# IMPROVING MENTAL MODELS OF COMPUTER SECURITY THROUGH INFORMATION GRAPHICS

by
Leah Zhang-Kennedy

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF APPLIED SCIENCE

School of Computer Science

at

CARLETON UNIVERSITY

Ottawa, Ontario
August, 2013

## Abstract

Many users have difficulties making effective security decisions. Education is one way to improve users' mental models of computer security, but a common challenge is that users are not motivated to learn about security. We propose that a visual approach to education can improve comprehension and engagement with security information. This thesis examines whether information graphics form an effective, memorable, and persuasive method of communication to increase computer security understanding and improve user behaviour. Guided by visual-textual strategies developed in education literature, we designed seven pieces of instructional materials that help end-users learn about password guessing attacks and antivirus protection. These include five infographic posters and two online interactive comics. Five one-week user studies with a total of 145 participants show that information graphics led to superior learning outcomes and a better user experience than existing text-alone approaches. Participants showed an increase of comprehension, retention, and improved behaviour after one week.

## Acknowledgements

First and foremost, I would like to express my gratitude to my supervisors. Without their encouragement and guidance this thesis would not have materialized. I would like to thank Sonia Chiasson for her extraordinary dedication to her students. You helped me in my journey to complete a Masters degree in every way possible, and I can't say thank you enough for your tremendous support and help. I would like to thank Robert Biddle for sharing his inspiration, insight, and passion for research. Your wisdom and the advice you gave me kept me on the right track throughout my degree.

Many thanks to the members of my committee, Ali Arya, David Mould, and Dwight Deugo, for your time and feedback.

I would like to thank my parents for their love and support in pursuing all of my life's passions and interests.

Lastly, I would like to thank my husband Matt, who turned out to be an excellent unofficial graduate guidance counsellor. Thank you for believing in me. I cherish your love and continuous support.

Parts of this project were funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC.

# Table of Contents

## List of Tables

## List of Figures

# Chapter 1

# Introduction

## 1.1 Research Question

Usable security [26] is a field of research that aims to increase the usability of computer security systems. Research in usable security [5,105] suggests that end-users typically have poor mental models of security threats. Education is one way to help end-users be more vigilant online. A number of online security education resources are available, but they appear to have limited effects on affecting user behaviour. Many approaches to security education focus on delivering information in plain text format, which falls behind to what is considered to be today's *massively visual society* [37], in which the public are exposed to visual and interactive communication media in almost every aspect of their lives. Yet, despite available evidence in popular media and traditional education literature [18,19,70] of the effectiveness of visual communication, few works in usable security [60, 65, 95] have explored whether visual information delivery methods can influence comprehension and persuasiveness of security advice. This thesis investigates whether visual communication strategies can help to address common challenges in security education. Specifically, our research questions are as follows:

> Do integrated visual-textual education strategies form an effective, memorable, and persuasive approach for computer security understanding by altering user perception and improving user behaviour? If so, does a richer interactive user experience help to further enhance the learning process and effect positive behavioural change?

This thesis includes the rationale, design, user studies, and learning outcomes of two visual communications media, infographic posters and interactive comics, at teaching end-users about password guessing attacks and anti-malware software.

## 1.2 Motivation

How to stay safe online is essential knowledge for users in today's connected world. The growing number of online services means individuals are moving online to manage large networks of personal, social, and business relationships. The average user juggles 25 online accounts [39]. These accounts store valuable personal and financial information, and are prone to unauthorized access and exploits [45]. Organizations, financial institutions, and business are becoming increasingly aware that security solutions must involve human factors. Many businesses offer customers security resources and advice, such as how to create strong passwords, install antivirus software, protect online privacy, and practice safe Internet habits. For instance, websites like Ebay [35], Microsoft [73], Google [49], Paypal [85], financial institutions [6, 21], government and organizational initiatives [46, 96] have dedicated extensive sections on security and protection to help to their users. There is certainly no lack of information available to users, although they appear to be insufficient at affecting behaviour.

Research from usable security [5, 105] suggest that end-users typically have poor mental models of security threats. A *mental model* is a simplified internal concept of how something works in the real world [24]. People rely on the reasoning of their mental models to anticipate the outcome of their actions in real life. That is to say, a mental model can help to solve problems, and in turn, shape long-term behaviour. We suggest that when users have incomplete mental models of security, it can hinder their motivation and ability to maintain good security. In this thesis, we focus on helping end-users build security understanding about two distinct threats, password guessing attacks, and malware protection.

**Password guessing attacks:** In knowledge-based authentication, users are required to remember data created for authentication purposes. Text passwords and personal identification numbers (PINs) remain popular, despite the growing number of alternative graphical and textual schemes [5, 38]. Among many problems, text-based passwords are difficult to remember and are frequently forgotten [38, 104]. Some users cope by creating short, easy to remember passwords. Such weak passwords are vulnerable to dictionary, brute-force, and targeted guessing attacks [5, 38].

**Antivirus protection:** Installing antivirus software, and practicing safe internet

habits are users' best practices to defend against malware. However, many users fail to maintain an up-to-date antivirus [13], diminishing the software's effectiveness against malware protection. When antivirus is severely out of date, some users install additional antivirus software, rationalized by the thought that multiple antivirus provides better security, where in reality multiple incompatible software could degrade the software's performance [68]. Unprotected computers are vulnerable to various types of malware, including computer viruses, worms, trojan horse, adware, and spyware.

Improving end-user security is difficult because of several unique challenges. End-users regard security as a secondary task that they must complete in order to perform a more relevant primary task. For example, users may be forced to enter a password before they can gain access to an email account. Email is users' primary concern while the process of authentication is considered a secondary task. Understandably, when security tasks become difficult, time-consuming, or burdensome, users avoid security or develop coping strategies that allow them to bypass security mechanisms to focus on their primary task. Since security is regarded as a secondary concern, users are not motivated to read security information or take the time to educate themselves about the threats. Research in human factors of security [5, 105] found that users seldom understand the nature of good defence. They may at times act insecurely without realizing that their decisions can have later consequences. Since people rely on the reasoning of their mental models to make decisions, Camp [14] suggested using mental models to help end-users build understanding of security threats.

There is no lack of publicly available security resources for end-users, but it is often seen as overly technical, time-consuming to read, and impractical to adopt into daily practices [55]. Security advice tends to focus on what users should or should not do, but does not help them build an understanding of *why* the advice is necessary and *how* certain actions result in better security than others. For example, users are used to hearing advice such as "do not download from peer-to-peer sharing sites," or "your password should be a minimum of 8 characters consisting of alpha numeric and special characters." This advice either conflicts with users' primary goals (e.g., user wants to download a particular movie), or has cost-benefit tradeoffs (e.g., strong passwords are more difficult to remember). Herley [55] argues that users often reject security

advice because it offers poor cost-benefit tradeoffs. Without an understanding of the threat, users cannot make robust decisions, and so intentionally choose to ignore good advice if they believe that the benefits are moot.

We argue that users need to develop some basic knowledge of the threats through education in order to be convinced why certain security advice is necessary, and propose that visual communication strategies can help facilitate understanding of security information. Research in education literature provides strong evidence that integrating visual and verbal strategies facilitates better learning than text-only [18, 54, 70], especially when prior knowledge is low [19]. Visual communication strategies used in marketing and advertising to reach the general public are widely deployed in a number of areas. For example, success has been seen in the public health sectors to prevent the flu by disseminating messages to the public advocating hand washing. In computer security research, however, visual information delivery methods that can be used to reach the general public have received very little attention. Only a few works in usable security like *Anti-Phishing Phil* [65], *Security Cartoon* [95], and *A Nutrition Label for Privacy* [60], have tapped into the power of visual communication.

In this thesis, we propose computer security education should include information graphics to help end-users build security understanding. We investigate visual design strategies in context of two computer security topics, password guessing attacks and antivirus protection. Our research approach is as follows. To address our research question, we designed and built educational prototypes in two established visual communication forms, infographics and comics. We utilized the ADDIE instructional design process to guide the development of the prototypes. Next, we performed empirical studies to evaluate the learning outcomes of the prototypes. The empirical studies utilized controlled experimental studies that test specific hypotheses to assess the learning effects of the visualization prototypes at teaching users about computer security, and interviews to gain an understanding of users' mental models of password guessing attacks and antivirus protection.

## 1.3 Contribution

The main contributions of this thesis are:

1. The design and implementation of 5 infographic posters and 2 educational interactive online comic books.

2. Empirical results showing improved effectiveness of infographics and comics over text-only advice in one-week user studies with a total of 145 participants.

3. Qualitative analysis of users' mental models of password guessing attacks and antivirus protection with a total of 29 participants.

4. Comic eye-tracking experiment making possible connections between user attention and comprehension.

5. Discussion and recommendations of 6 design strategies for computer security education supported by our empirical results.

**1. The design and implementation of 5 infographic posters and 2 educational interactive online comic books:** We designed and implemented tangible educational materials to help users improve their understanding about password guessing attacks and antivirus protection, including 5 infographic posters, and 2 full-length online interactive comic books. All prototypes were hand drawn by the primary researcher and implemented using Adobe graphics software. The infographics provide users with a quick-to-read lesson of the threats and actionable harm reduction advice. The designs explore various metaphors of risk communication adapted from existing literature and online resources. The comics inherited some of the most successful elements from the infographic designs, but provided users with a more in-depth and comprehensive lesson of the topic. The comics were designed to achieve user engagement through narrative, character development, humour, and interactivity.

**2. Empirical results showing improved effectiveness of infographics and comics over text-only advice in one-week user studies with a total of 145 participants:** We conducted between-subject in-lab user studies with a total of 145 participants to evaluate our prototypes. The user studies utilized mixed qualitative and quantitative methodology, including multi-session one-on-one interviews, questionnaires assessing pre and post knowledge of the topic, prototype evaluations,

eye-tracking measurements, and online follow-ups. The user studies allowed empirical evaluations of our prototype designs. The results provide positive evidence of the effectiveness of information graphics at educating users about computer security.

Summary of user studies:

- Password infographic study — 55 participants
- Password comic study — 21 participants
- Password comic eyetracking and interviews — 13 participants
- Antivirus infographic study — 40 participants
- Antivirus comic study and interviews — 16 participants

**3. Qualitative analysis of users' mental models of password guessing attacks and antivirus protection with a total of 29 participants:** We build on prior work in usable security [4, 14, 87, 103] to identify users' mental models of security threats, focusing primarily on password guessing attacks and antivirus protection. Our results show links between incorrect or incomplete mental models and effects on users' ability to make secure decisions. Specifically, we uncovered a *Target* mental model for password guessing attacks that dictates how users create their passwords, prioritize accounts, and make decisions based on context. We identified three basic models of how antivirus software works: *inclusionary*, *exclusionary*, and *risk assessment* models, and several models of malware, including *"Viruses" are more harmful than "malware"*, *viruses are like pests*, *viruses are like a infectious disease*, *viruses cause computers to mechanically break down*, and *viruses are pieces of code*. We also found that many users were unable to distinguish the difference between "clean", "quarantine", and "delete" actions in antivirus software.

**4. Comic eye-tracking experiment making possible connections between user attention and comprehension:** We performed an eye-tracking evaluation of the interactive password comic as a tool to teach users about security threats. Comics have the ability to demonstrate complex topics progressively, through the use of

narrative and characters. To understand how users progress through our educational content, we used eye-tracking to evaluate the password comic and provide an analysis of how information is processed through comic media and make possible links between users' attention and comprehension. The results suggest that the combination of text and graphical elements help to facilitate comprehension of the information, and encourages learnability and engagement of security topics.

**5. Discussion and recommendations of 6 design strategies for computer security education supported by our empirical results:** This research advances our knowledge of how to improve users' mental models and influence user behaviour by providing empirical evidence of what visual approaches are effective at conveying information about security. We propose 6 visual design strategies and discuss their effectiveness based on empirical results from evaluating our prototype designs.

## 1.4 Thesis Outline

This thesis is organized as follows: In chapter 2, we review prior work in usable security related to user education and mental model research; In chapter 3, we describe visual communication strategies grounded in traditional education literature, and propose 6 ways that information graphics can be used to facilitate computer security understanding; In chapter 4, we explain our creative process and provide detailed rationales of our prototype designs; in chapters 5 and 6, we report the results of our user studies for two security topics, password guessing attacks and antivirus protection; and lastly, chapter 7 discusses the effectiveness of visual design strategies on security education based on our empirical results, as well stating the limitations and future work.

# Chapter 2

# Background

In this chapter, we give background on the field of usable security. We specifically focus on literature in mental models research and security education. We highlight successes as well as challenges faced by security professionals to teach end-users security information. Lastly, we give background on two security threats that are the focus of this thesis, password guessing attacks and antivirus protection.

## 2.1 Usable Security

Usable computer security [26] is a multidisciplinary area of research that combines computer security with human-computer interaction (HCI). It aims to improve the usability of secure systems while maintaining or advancing system security.

Achieving a balance in usability and security of computer systems poses a complex challenge, involving both the "user" and the "attacker". Security systems should be easy to use for end-users, but difficult to hack for attackers. There is increasing awareness in computer security that secure solutions should include human factors. Usable computer security recognizes that even the most secure system could fail when it is used incorrectly or dismissed by users. Research in the field has revealed that users' mental models can impact usability and have negative consequences with respect to security. Specifically, users tend to have poor mental models of security threats [103]. They seldom understand the nature of potential risks and what to do in defence, and make security decisions based on misconceptions that can lead to negative consequences.

Users are sometimes regarded as the "weak link" in security systems [2]. One difficulty is that users are typically uninterested in security. Security is regarded as secondary while users perform some kind of primary task [105], such as accessing an online bank account or downloading music. Users may be momentarily delayed by

entering a password before gaining access to an online account, but they are uninterested in the process of authentication. Understandably, users try to minimize time and effort spent on security [55] to focus on their primary tasks. Secondly, security systems are technically complex for end-users to understand. Security systems need to be designed so that users can meaningfully interact within context of the system's expected behaviour [43]. Poorly designed user interfaces tend to give inconsistent and arbitrary feedback, and do not provide adequate information to guide users to make secure decisions (e.g., [47, 105]). Usable security design guidelines are intended to improve security-oriented systems [109].

There are three high-level strategies in usable security [25] that help to protect users from security threats: 1) build security systems that just "work" without user intervention, 2) make security intuitive and easy to use, and 3) train users about security. This thesis focuses on the third strategy. The idea is not to single out user education as the "best" approach, but to build and expand on education strategies as part of an integrated effort to secure system usability. Some experts argue that education does not have positive effects on user behaviour [50], and that security experts should not put the burden on users [77]. On the contrary, empirical evidence in usable security [64, 92] has suggested that exposure to education materials can raise awareness and enhance understanding of security topics, and even affect behaviour.

## 2.2 Mental Model Research in Usable Security

A *mental model* is a simplified internal concept of how something works in the real world [24]. People rely on the reasoning of their mental models to discriminate new concepts, solve problems, make predictions, and interpret information in their surroundings. Humans rely on mental models to perform everyday activities. Therefore, mental models are applicable to the design of everyday things [79]. By gaining an understanding of what users know about the system and how they interact with it from the provided interface, it is possible to improve the design to support appropriate user mental models.

The theory of mental models was first formulated by Kenneth Craik in the 1940s [24]

as a basis for understanding human thought. Two decades later, Young [110] suggested that users' mental representation of their interaction with complex devices are made through mental models. In 1998, Laird *et al.* [58] further stated that humans use a working model of a certain phenomenon in order to understand it. People solve new problems by using prior knowledge of similar problems if there are similarities between them. Mental models may include the minimum functionality required to understand the subject, and people make assumptions based on their mental models to fill in gaps in their lack of knowledge.

In usable security, several researchers have tried to understand end-users' mental models in order to help users shape good security behaviour. Early research investigated users' attitudes toward security and network administration in home and work environments. Dourish *et al.* [34] examined how corporate workers experience and handle security issues. They argued that a major obstacle to the development of secure systems is that these systems often match poorly in ways people need to use them. They concluded that "any technology for secure communication is only as secure as the settings within which it is deployed" [34]. In a related study, Gross and Rossum [52] studied end-users' knowledge of security in organizational contexts. Supported by an analysis of end-users' perspectives on security management, the authors argued that good system design should bridge the knowledge gap of users when necessary and mask complexities where possible. Insights of home network administration practices were gained through interviews conducted by Grinter *et al.* [51]. They found that users require considerable efforts to setup, maintain, and coordinate home networks. These papers offer insights into what security issues users face in home and corporate contexts, but do not dig deeper into why users make certain security decisions.

In 2009, Camp [14] enumerated five conceptual models frequently used in computer security literature. The conceptual models use analogies or metaphors to communicate complex security risks to the general population: physical security, medical infections, criminal behaviour, warfare, and economic failure. Physical security is implicit in descriptions of physical objects like "locks" and "keys", and signifies individualized and localized control. The medical infection model of security mirrors the

epidemic of infectious diseases. Criminal behaviour models computer security as risks of being a victim of crime where users or machines are targeted. The warfare concept implies the existence of a determined implacable enemy. Lastly, security vulnerabilities can be seen as economic failures, such as security failures causing downtime and costs. These conceptual models had been used as the basis for further research into users' mental models.

Asghapour *et al.* [4] performed a formal evaluation of Camp's conceptual models in a card sorting experiment. They found strong differences in security mental models between experts and novice computer users. Traditionally, it has been thought that since experts are more knowledgeable about the technical definition of the risks, their mental models should provide the foundation for designing risk communication instruments for non-experts. On the contrary, findings by Asghapour *et al.* [4] suggest that the gaps between the mental models of expert and novice groups can lead to ineffective and poor communication of the risks. The experiment suggests that the effectiveness of risk communication could increase if it is adjusted to fit the mental models of non-experts, and that end-users do not necessarily have to learn all the technical details of the risks to respond effectively.

Wash [103] went beyond prior research on assumptions of the usefulness of mental models, and investigated end-users' actual mental models through interview methods and qualitative analyses. He identified eight "folk models" that are used by end-users to decide what security advice to follow and which security software to use. Four of these models are end-users' conceptualization of "hackers" that break into computers. Some believe hackers are digital *graffiti* artists that cause mischief, while others thought hackers are criminals like *burglars* who break into computers, or are *contractors* who support organized crime. Some thought hackers only target *"big fish"*, where ordinary people are unlikely victims. Four other models Wash identified are end-users' conceptualization of "viruses" and other types of malware. Users with under-developed models believe viruses are generally *bad*, but could not describe how they are bad. Some believe that a virus needs to be intentionally placed on the computer. It behaves like any other software except that it is *buggy software*. A number of users believe that the intention of viruses is to cause *mischief*, while others

believe they *support crime*. These models help to explain why end-users follow some expert security advice while ignoring others.

## 2.3 Training Users about Security

As of 2013, there are approximately 2.75 billion users online worldwide [56], almost twice as many compared to 5 years earlier. Internet users are susceptible to password guessing attacks, malware, botnet applications, and social engineering. One way that the security community responded against these threats is to protect end-users through user education. Users are provided with self-help instructions and advice from security professionals to learn how to protect themselves and their computers. Most large websites and software providers offer users security resources and advice, such as how to create strong passwords, install antivirus software, protect online privacy, and practice safe Internet habits. For instance, websites like Ebay [35], Microsoft [73], Google [49], Paypal [85], and financial institutions [6, 21], have dedicated extensive sections of their websites to security education in an effort to help protect their users. However, advice usually focuses on what users should or should not do, while offering little insights on *why* the advice is necessary and *how* certain actions result in better security than others. Users are accustomed to hearing advice such as "do not download from peer-to-peer sharing sites," or "your password should be a minimum of 8 characters consisting of alpha numeric and special characters." This advice either conflicts with users' primary goals (e.g., user wants to download a movie), or appears impractical (e.g., strong passwords are more difficult to remember). There is no lack of resources available to learn about security, although they appear to be insufficient at affecting behaviour. Through usable security research, we learned that security is a secondary task for users [105], and that low motivation and poor understanding of the threats lead users to be noncompliant with security guidelines, such as password security policies [2].

Research into users' mental models [103] suggests that one major problem with security education is that it does not adequately explain the threats people face. Therefore, end-users intentionally choose to ignore security advice that they perceive

will not help. This problem is visible in mainstream security education efforts; although abundant, they are often seen as arbitrary and impractical to adopt into daily practices. In 2009, Herley [55] proposed that users reject security advice because it offers poor cost-benefit tradeoffs. Without an understanding of the threat, users cannot make robust decisions, and so intentionally choose to ignore good password advice if they believe the benefits are moot. He continues to argue that although security education is important, the current state of advice given to users is overwhelmingly complex and growing, and require much cost in user time and effort. As a result of these challenges, many approaches were introduced in the usable security community to reduce the cost of teaching users.

"Anti-Phishing Phil" [92] takes an interactive game-based approach to teach users how to avoid falling for phishing attacks. It tries to motivate users by engaging them in game activities while instructing them how to distinguish legitimate links from fraudulent ones. Similar efforts in phishing education include "PhishGuru" [65], an email-based anti-phishing education system that teaches users after they have responded to a fake phishing message, and the APWG CMU-Cylab's phishing education landing page program [86]. It also aims to instruct users at the "most teachable moment" when they have just fallen for a phishing communication.

Two education approaches have looked into whether users can benefit from security education embedded into an entertaining primary task. In "Control-Alt-Hack" [30], three to six players can engage in a hacker-themed strategy card game. Security concepts are embedded into the game to increase awareness and understanding of high-level computer security topics among those who play the game. "Auction Hero" [20] is a computer game that is modelled after life online. Making profitable transactions through buying and selling robot parts while avoiding various computer security attacks is the primary game mechanic. Both works are founded on the idea that learning about computer security should be a secondary task because that is how users manage security in real life.

To the best of our knowledge, the only extensive exploration of the comic media in computer security education is *Security Cartoons* [95]. It uses a series of comic strips to improve non-expert users' understanding of various risks. The authors argue

that a cartoon-based approach will more likely produce better long-term effects than currently practiced education efforts. This is because presenting a serious topic like computer security as cartoons can help users to overcome the initial "intimidation factor," help users immerse in the learning material, reach a large readership, and communicate changing threats quickly at low production costs. Mainstream comics that sometimes include security advice are Dilbert [3] and XKCD [75]. Another related example is the online Google Chrome comic [48]. The 39-page instruction manual, delivered entirely in comic book format, teaches users about the inner workings of the Google Chrome browser, including key security concepts and benefits. Although these resources exemplify that the use of comic media is a promising approach to educate users about security, empirical evidence is needed to support the actual effectiveness of comics in the context of computer security education.

Some work in usable security has shown that users can benefit from visual metaphors and good information design. In the design of firewall warnings, Raja *et al.* [87] found that a personal firewall visualized based on a physical security metaphor facilitates better comprehension, risk communication, and increased likelihood of safe behaviour than warning messages from existing firewall software. In *A Nutrition Label for Privacy* [60], Kelley *et al.* explored information design to improve the visual presentation and comprehensibility of online privacy policies. The authors designed an easy to read privacy label drawing from design elements and principles from nutrition, warnings, energy labelling, and banking privacy notifications. Results show that participants found information more quickly and accurately on the proposed privacy label compared to existing natural language privacy policies. Interestingly, good information design also enabled participants to have a more enjoyable information seeking experience.

One common feature that is shared by many works described above is that security training is embedded into a fun activity, such as reading comic strips in *Security Cartoons* [95], playing a table card game in *Control-Alt-Hack* [30], or engaging in computer games like *Anti-Phishing Phil* [92] or *Auction Hero* [20]. The entertaining and interactive features of these works allow the use of stories to illustrate complex process [95], keep users engaged in learning through multimedia [92], allow a deeper

understanding of security risks through interactivity [92], and leverage fun and entertainment to help spread security awareness [30].

Study found that the majority of users are indeed security conscious if they perceive the need for secure behaviours [2]. Therefore, education is useful beyond teaching essential security knowledge, but can also motivate the need for security. Recognizing the importance of raising awareness about secure online behaviour, several government initiatives are in place. *Get Cyber Safe* [46] is a national awareness campaign that aims to educate Canadians to be "responsible digital citizens." Extensive online resources span across various aspects of internet security that offer tips to help people stay safe online. On a larger scale, *Stop. Think. Connect.* [96] is a global cyber security awareness campaign with international partners in Canada, United States, Panama, and Paraguay. Launched in 2010, it is led by the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG). It also aims to raise awareness about online security by providing resources and support to help the public stay vigilant online. Current campaigns include subway posters developed for the national cyber security awareness month, online safety posters, public safety announcements, the *Keep a Clean Machine* campaign, and *CYBERSMART!* classroom activities and posters. These campaigns aim to engage the public, private sectors, and governments to improve cybersecurity.

## 2.4 Selected Security Topics

For this thesis, we focus our efforts on two security topics faced by end-users on a daily basis: password guessing attacks and antivirus software. We provide background on each topic to better frame our design decisions in later chapters.

### 2.4.1 Overview of Online Password Guessing Attacks

In knowledge-based authentication, users are vulnerable to *online password guessing attacks* when they set up "weak" passwords that can be easily predicted by attackers. While *offline* guessing attacks are also possible (e.g., when attackers gain access to databases), our prototypes focus on the threat of online attacks. Online guessing attacks rely on interaction with the live system to determine if a guess is correct.

After a series of unsuccessful password entry attempts, some sites will increase system response delay times or disable future attempts. Although these security mechanisms help to reduce password guessing, they also run the risk of locking out legitimate users who forget their passwords, and could enable a denial-of-service attack to purposely lock user accounts.

Users cope with the challenge of remembering passwords by making them short and easy to remember. They also reuse or create variations of the same password [45]. This puts users at risk of three types of online guessing attacks: exhaustive brute-force, dictionary, and targeted attacks. Tools are readily available online to help launch automated attacks. Sophisticated large-scale attacks may require expertise, but many attacks could easily be replicated by "script kiddies" with basic computer hacking skills.

**Exhaustive Brute-force Attack:** Brute-force attacks consist of guessing every possible password in a theoretical password space [1]. All passwords can eventually be cracked by brute force, but the size of the search space, time, and processing power can make it infeasible to crack strong passwords. Users' best defence against brute-force attacks is to create long, random-looking passwords containing alphanumeric and special characters to maximize the search space, thus minimizing attackers' chance to crack passwords using brute force.

**Dictionary Attack:** Dictionary attacks use pre-compiled or computerized lists of high probability candidate passwords to guess the target password. Attackers exploit the fact that people like to use whole words or a string of words to create their passwords. Attackers also search for predictable patterns in user behaviour supported by empirical data, such as commonly used character substitutions (e.g., @ for a), popular passwords (e.g., qwerty123), or predictable character distribution and composition (e.g., P@ssword1). Such pre-compiled lists are easily computed, available online, and shared amongst attackers [31].

**Targeted Attack:** In a targeted attack, the attackers try to obtain information about a specific user. Attackers exploits the fact that people use personal information as their passwords to cope with memorability challenges [45]. For example, names,

[1] The set of all possible password combinations for a given system configuration

birth dates, hobbies, pets, or phone numbers are frequently used as passwords, and could be traced back to the user. This information is often readily available online, such as on social media sites, making it easy for attackers to gather user information even if they do not personally know their victims.

### 2.4.2 Overview of Antivirus Protection

Antivirus (also known as "AV") is software that that prevents, detects, and removes malicious software programs like computer viruses, worms, trojan horse, spyware, adware, and other types of malware from computer systems. Many subscription-based antivirus as well as free software are available to users, including popular brands like Norton, McAfee, Avast, Avira, and AVG. Generally, approaches to detection and removal methods can be distinguished into two categories: signature-based and heuristic-based detection.

**Signature-based Detection Method:** Signature-based antivirus software contains a library of known virus information, called the virus *fingerprint* or *signature* [90]. In the process of scanning, the antivirus compares contents of the program with its database of virus signatures. If a match is found, the antivirus alerts the user that a possible virus has been found and future actions can be taken to resolve the infection. This method of detection is effective against existing viruses that are contained in the antivirus database.

**Heuristic-based Detection Method:** Sometimes virus codes are modified to evade signature-based detection. The heuristic-based detection method examines programs based on a database of virus behaviours previously seen [90]. This method of detection is most effective against variants of known viruses, and may also detect some *zero-day* viruses [2].

**Maintaining Antivirus Software:** Running regular updates is essential to maintain the optimal effectiveness of antivirus software. The majority of antivirus programs enable users to update their software directly through the software. In addition to performing regular updates, subscription-based antivirus providers require the

[2] A previously unknown computer virus or other malware for which specific antivirus software signatures are not yet available

user to renew their software at the end of each subscription period (usually yearly). Most antivirus software checks for updates automatically and send users subscription renewal reminders, but installing updates or renewing the software may require users' attention. As a result, users may choose to ignore prompts and reminders to update for prolonged periods of time. A survey with 415 end-users found that while 87% of users have antivirus software installed, only about 34% update regularly [13]. The study revealed that although users feel confident and believe they have heightened awareness of security threats, their antivirus software are not updated regularly enough to provide sufficient protection. When users fail to update regularly, antivirus software can quickly become out-of-date and ineffective against new threats.

## 2.5 Summary

Research in usable security has found that end-users typically have poor mental models of security threats. One of the approaches to improve mental models is through user education. We reviewed past education efforts in the usable security field, as well as summarized materials developed by large websites, and by organizations and government initiatives. One main challenge we described was security is a secondary task for end-users and motivation to learn is low. Other observations we identified was publicly available resources often do not adequately explain the threats users face, and compliance requires much cost in time and effort. In the next chapter, we describe how some of these challenges can be addressed through visual design strategies, and outline ways they can be applied to security education.

# Chapter 3

# Building Mental Models through Visual Communication

In Chapter 2, we showed security education is difficult because users typically rely on poor mental models to make security decisions. In this chapter, we propose integrating visual communication strategies in security education, and provide an overview of how information graphics can help support improved mental models that aid learning. We draw on a body of work in education to help to inform the design and evaluation of our prototypes, presented later in Chapter 4. We end with a summary of six ways that information graphics can help educate users about security.

## 3.1 Visual Information for Learning

Researchers have several theories to support the positive effects of visuals on learning. One is Paivio's dual coding theory [82] that suggests graphics and text are coded into memory differently. People process text in their phonetic working memory, while images are encoded in visual working memory. The theory implies that the combination of related text and images helps to enhance comprehension, and increases long-term memory.

Theories in education literature show that the use of visual-textual strategies in learning is more effective than text alone [18, 54, 70]. Scientific textbooks, for example, incorporate illustrations of theories and diagrams to support text explanations. *Graphic design* is applied to the page layout to make reading and finding information more intuitive and accessible. *Information design* (introduced in Chapter 4) is utilized to visually represent information or data in figures or diagrams so that it is readily understandable.

Empirical evidence in learning proposes several ways that graphics can help build mental models. First, visuals that depict the content of accompanying text may facilitate the construction of a mental model [54]. In one study [54], researchers

compared the effects of text-only, text accompanied by visuals that only represented elements described in the text, and text accompanied by visuals that represented the relationships of elements described in the text. In all cases, visuals returned higher accuracy and response times in recognition and problem solving than text-only. Secondly, visuals that show relationships between elements being described in the text are the most beneficial [54]. This suggests that visual information would be more effective if it offers additional insights by highlighting relationships between the objects being described in the text.

Another study [27] offers further evidence that visual aids like diagrams help build mental models in the learning process. Cuevas *et al.* [27] compared learning of aviation lessons between text-only and text with diagrams. The study found that participants who learned through text and diagrams scored higher on tests than participants who viewed the text-only tutorial. The authors concluded that diagrams presented with text in tutorials could improve learning efficiency, and consequently lend further evidence of the benefits of visuals to help build mental models.

According to Clark and Lyons [22], there are four graphic types used to build mental models: organizational, relational, transformational, and interpretive. Organizational graphics are visuals that qualitatively show relationships between content elements. For example, boxes, lines and arrows are used in flow charts to group concepts and show flow of information. Relational graphics show quantitative relationships, such as data visualized in charts and graphs. Transformational graphics show movements in time and space, and help to build temporal, and cause-and-effect mental models. Lastly, interpretive graphics demonstrate theoretical or abstract relationships, thus help to show cause-and-effect relationships. Please refer to table 3.1 for a summary of graphic types.

## 3.2 Visual Communication Forms

Visual communication attempts to communicate ideas and information through visual media. It is primarily presented or expressed through an integration of text and images. Effective visual communication materials are mainly based on measuring comprehension by the audience, and not based on personal aesthetic preferences [42].

| Graphic Type | Description | Example | Used to Build |
|---|---|---|---|
| Organizational | A visual that shows the qualitative relationships among content elements | A graphic organizer (i.e., boxes, lines, arrows) | Mental models of the relationships among facts and concepts |
| Relational | A visual that communicates quantitative relationships | A bar chart, or a pie chart | Cause and effect mental models |
| Transformational | A visual that shows movement and change in time and space | An animated diagram of how to perform a procedure, or a flow chart of how photosynthesis happens | Temporal mental models; cause-and-effect mental models |
| Interpretive | A visual that illustrates theoretical or abstract relationships | A schematic diagram or a simulation of molecular movement | Cause and effect mental models |

Table 3.1: Four graphic types used to build mental models. Table adapted from [22]

In this thesis, we focus on two types of established visual communication forms: information graphics and comics. Although there are other ways to express information visually that are not explored in the thesis, such as film or animation, we chose to focus on information graphics and comics because these two types of media have several distinctive advantages. First, information graphics and comics have lower production costs than film and animation. Many businesses offer customers security resources and advice to help minimize security failures that could cause downtime and costs. We argue that the cost of graphic design work involved in the production of visualization materials is very small compared to the possible payback in increased security and a better user experience. Since many users have low interest to learn about security, it is necessary to create materials that attract attention, quick to read, and enjoyable to learn. Visual forms of communication have greater potential to achieve this goal than text-only approach. Secondly, information graphics and comics are quicker to produce than film or animation. Therefore, these media types are more likely to reach the audience in a timely manner. As security threats constantly change, education materials need to rapidly adapt to new threats. Thirdly, information graphics and comics enable the audience to consume information at their own pace. For example,

the audience can easily flip through pages in a comic book, and control the order and speed in which the comic book is read.

### 3.2.1 Information Graphics

Information graphics are visual representations of information, data, or knowledge [93]. Information graphics have historical roots from scientific diagrams, statistical graphs, geographic renderings, and maps. In the 21st century, information graphics gained a large web presence through the popularity of social media. They are shared between users as static images or simple interactive interfaces spanning across a wide range of topics. Information graphics are effective because of their visual element, and are faster to consume than text because the brain process visual information simultaneously, whereas text is processed in a linear fashion [93]. Furthermore, information graphics are a suitable communication media for a large portion of the population. Research estimated that approximately 65% of the population are visual learners, as opposed to auditory or kinesthetic [9]. The media intends to present complex information quickly and clearly, by utilizing the human visual system's ability to see patterns and trends to enhance cognition [15]. Information graphics are capable of transforming abstract, complex, or otherwise difficult to understand concepts into intuitive, instant knowledge [93]. The term *information graphics* is sometimes used interchangeably with *infographics* in popular media. In this thesis, we refer to *information graphics* as the umbrella term for visual representation of information. We refer to our poster prototype designs as *infographics* because it is the popular web term used to describe this type of media.

The design of information graphics should support three basic provisions of communication: appeal, comprehension, and retention [25]. Appeal refers to the need to initiate interest from the audience to engage in the material, and can be achieved through visual design. Comprehension implies that the audience should be able to understand the information quickly and clearly. Successful manipulation of information and data can be achieved through information design. The goal of successful information design is to portray information and/or data effectively and efficiently for people to understand. Rendering of text and graphics are intended to deliver the

information efficiently, rather than for decoration or illustration. Modern pioneers of information design include Edward Tufte. He argues that the objective of conveying specific information should be the main guide in the design decision behind visualizations [99]. Information design is useful because the presentation of opinion and facts can be improved with graphics and thoughtful compositions of visual information. Tufte cautioned against false data visualization that might mislead the user or hinder the proper interpretation of data, and against "chart junk" [99], which are unnecessary manipulations of graphics that add no value to the visualization. When choosing how to convey information, the purpose of the information and its intended message and audience must be considered. On a more granular level, information design relies on good graphic design to provide a logical development of the topic and create emphasis on what is important. The application of graphic design principles [1], typography, and clear writing are essential aspects of good information design. Lastly, the audience should be able to remember the information presented. Retention of visual information is supported by the picture superiority effect [74], meaning people remember images better than text.

### 3.2.2 Comics

Comics are a form of "sequential art" [36] that use a series of images to deploy graphic storytelling and to convey information. Although the history of comics has followed divergent paths in different cultures, several distinctive characteristics remain similar. The comic form is an established media to communicate ideas via juxtaposed sequences of panels with images. Textual devices such as speech balloons, captions, and symbolic sound effects are usually placed beside images to indicate dialogue, narration, and other types of information. Size and placement of panels control the flow of the narrative and pacing. There are several advantages to comic media. First, comics offer an enormous breadth of control to create customized content through a full range of visual symbols, and pairing of words and images to construct a convincing story [71]. Secondly, comics are able to demonstrate complex processes progressively, through the use of stories and characters. Thirdly, it has a greater potential to reach non-technical Internet users than traditional educational efforts, because the reading

format is lightweight, easy to consume, and appears less daunting to read [95]. We argue that presenting security topics as a comic can generate interest and motivate learning. The comic media has attracted the attention of educators because of its potential to foster students' interest in science and help with retention of knowledge [76]. Comics can draw on the functions of humour to enhance communication of serious topics [33]. Using humour can also enhance persuasion, and increase the comprehension and retention of information [33]. Graphically, comics share many advantages with infographics. They deliver information through a juxtaposition of text and images, and break down complex concepts visually to aid comprehension.

## 3.3 Metaphors to Support Mental Models

From a cognitive linguistic point of view, a *metaphor* is defined as understanding a target domain in terms of other source domains [67]. Analogies and metaphors are often used to help users understand computer security risks. For example, the concept of firewalls can be explained in terms of physical barriers [87].

Mental models are often constructed from metaphors. A breadth of research on the benefits of using metaphors exist in the HCI community, but Marcus [69] cautions that relying solely on metaphors could be limiting, and may not give users a complete mental model of the concepts. For example, when a physical security metaphor is used, the concept could be limited by physical barriers, such as a wall, whereas Internet security does not have such limits [87]. When a metaphor is unfit to represent the target domain, it can cause users to make errors or to have a false sense of security. Metaphorical references can also vary over time across technological and cultural shifts [69]. However, Marcus [69] goes on to argue that even though some metaphors cannot support a complete mental model, they can help to fill in the details from users' experience.

In the previous chapter, we showed that even among security experts, there is discrepancy on the "correct" model that non-expert users should use to think about computer security. However, previous work has proposed possible metaphors that could be used to support mental models based on existing literature and empirical evidence, such as the framework proposed by Camp [14]. There is evidence that

metaphors can increase the pace of learning, memorization, ease of use, and engagement because they leverage concepts that are familiar to users [69]. In computer security, metaphorical references are common in software and user interface design, such as the concepts of physical security depicted through keys, locks, and walls.

## 3.4 Measuring Learning Outcomes

According to Schmidt and Bjork [91], effective education should help learning in three ways: *knowledge acquisition*, *knowledge retention*, and *knowledge transfer*. *Knowledge acquisition* determines how well the learner can process and extract knowledge. Graphics can be used to illustrate relationships and highlight key concepts through figures and diagrams. According to Carrol *et al.* [16], technical self-instruction manuals should aim to present the material as briefly as possible to make the training unimposing. Images are quicker to consume than text. To this end, we can use visuals to minimize text content in instructional materials. *Knowledge retention* measures learners' ability to retain and recall information after some time has passed since the initial knowledge acquisition. *Knowledge transfer* is the learner's ability to apply acquired knowledge to different situations. Research has shown that humans remember images better than they remember textual information [83]. Therefore, graphics can be applied to educational materials to aid knowledge transfer after learning and prolong information retention. Graphics support *near* and *far* transfers [40, 101]. *Near* transfer is the learner's ability to apply acquired knowledge to a closely related context. Graphics can be used to support step-by-step "how-to" skills by showing visual examples such as teaching users how to create a strong password. *Far* transfer is the learner's ability to apply knowledge to different situations. Tasks such as problem solving rely on *far* transfer skills. Graphics could be used to represent abstract idea more concretely, and help learners build richer mental models that could guide them in decision making.

## 3.5 Other factors that Could Help Users Learn

**Motivation:** Before knowledge acquisition, retention, and transfer can occur, we first need to get users to pay attention to the learning material. As described in Chapter 2, users have low motivation to learn about computer security because it is a secondary task [105]. Presenting security information graphically might help to draw attention and interest, and prolong engagement with the material. If people dislike reading technical, text-heavy security content, graphic design might make the information more interesting, accessible, and quicker to read. Higher interest and greater learning are correlated [102], meaning if people are interested in what they are learning, they take more care into processing the information. Graphics is one way to help engage users' interest in technical instruction materials.

**Humour:** Research in serious games found that the use of humour can help to ease the social, emotional, and cognitive challenges of serious topics, and enrich the overall user experience [33]. Some users are intimidated by technical topics like security. Humour can help to relieve the stress of learning about a complex topic while reducing anxiety or frustration [33]. Socially speaking, humour helps to break down barriers between the mentor-student relationship when it is used. Characters designed with a sense of humour are perceived to be well-rounded, interesting, and more believable [78]. In addition to social and emotional benefits, research in education has found that using humour can enhance persuasion, and increase comprehension and retention of information [44].

**Persuasion:** Research in persuasive games suggests that the interactive nature of computer games affords a new approach to rhetoric called "procedural rhetoric" [7]. It suggests that rhetorical appeal is discovered by users through interaction with the software. In essence, procedural rhetoric is the practice of effective persuasion. In computer security, advice is given to inform and persuade users to behave securely. Graphics and interactivity may be incorporated into security education to help to create meaning and construct arguments.

## 3.6 Proposed Design Strategies

Based on our literature review of mental models and educational research, we propose that information graphics can be used to help educate users about computer security in several ways. We frame these as design strategies that can provide theoretical background for the design of educational material. Our six design strategies are articulated below, along with section numbers pointing to the associated literature.

1. Integrate graphics with text to gain and sustain user attention, and assist in comprehension of related textual explanations to facilitate knowledge acquisition. (Section 3.1)
2. Apply information design theory to organize content that enables users to find information quickly and accurately. (Section 3.1)
3. Depict metaphors visually to increase the persuasiveness and memorability of metaphorical rhetorics. (Section 3.3)
4. Use visuals, interactivity, and humour to add interest and engagement in learning materials. (Section 3.5)
5. Combine visuals and text to help communicate operational implications among content objects to assist the transfer of knowledge in the form of a mental model. (Section 3.1, 3.3)
6. Maintain high ratio of visual to textual content to help reduce memory load and increase the retention of information. (Section 3.1, 3.4)

We will use these design strategies to inform and guide our design decisions while developing our educational material to teach users about password guessing attacks and antivirus protection.

## 3.7 Summary

We reviewed a body of work in education that shows information graphics help build mental models. We proposed six design strategies that will inform the design decisions of our educational prototypes, described in the following chapter. Next, we discuss

the design rationale for each of our educational prototypes founded on information graphics theory.

# Chapter 4

# Design of the Infographics and Interactive Comics

To explore the learning effects of information graphics on security education, we devised education prototypes in two distinct formats: infographics and interactive comics. We choose these two media types because they are highly visual, quick and easy to consume, and popular in mass media. In this chapter, we give rationales for the prototype designs used to educate end-users about password guessing attacks and antivirus protection. We describe the ADDIE instructional design model that guided the process of our designs, and give detailed rationales for our design decisions that went into the creation of the educational material.

## 4.1 The ADDIE Instructional Design Model

Instructional design models were developed to guide the effective design of instructional materials. ADDIE [53] is an acronym that stands for the 5 phases of instructional design: analyze, design, develop, implement, and evaluate. The ADDIE model was first introduced in 1975 [10] as the process involved in an instructional systems development (ISD) program for military service training, but became applicable to other areas of instructional design. Over the years, ADDIE has developed from a linear waterfall model to a dynamic iterative process, where the designer can assess and iterate the material at each stage of development. Figure 4.1 shows the most commonly used version of the ADDIE process as we understand it today. There are five phases involved:

**Analysis:** The problem space is first analyzed to gather information about the target audience, project objectives, constraints, and desired learning outcomes. The instructional designer consolidates the information and considers delivery options.

**Design:** In the design phase, the instructional designer identifies types of activities required for users to achieve the goals identified in the *analysis* phase. The

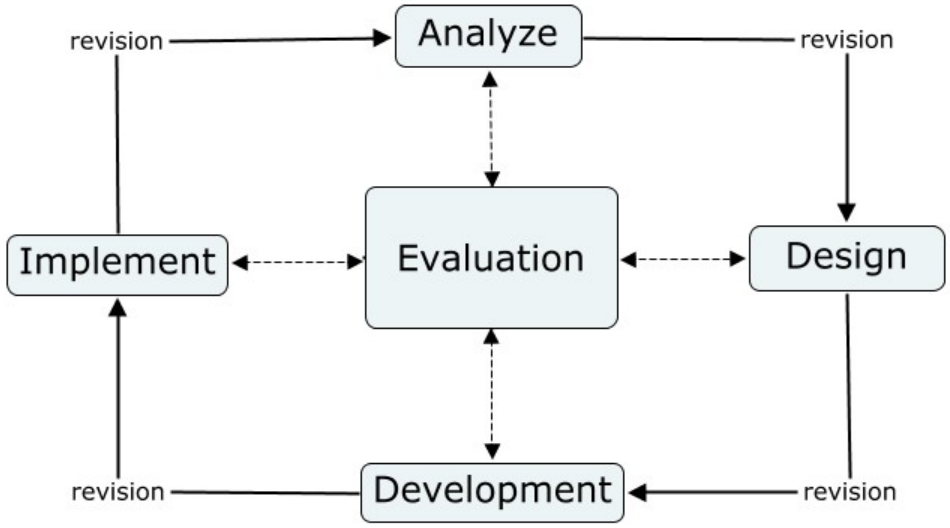



Figure 4.1: The ADDIE instructional design process. Diagram adapted from Wikimedia Commons [23]

instructional designer plans the lesson and content. At this phase, learning strategies (discussed in Chapter 3) are applied to meet the desired behavioural outcomes. The designer starts to sketch the user interface and plan the user experience. Low-fidelity prototypes or concept art may be developed to iterate design ideas quickly at low cost. Graphics design principles [1] are considered to maximize the effectiveness of the visual design. At the end of the design phase, a "blueprint" is created to take the design into the development stage.

**Development:** The instructional designer assembles content laid out in the blueprint from the *design* phase. The designer create storyboards and sample graphics to get feedback and iterate the design accordingly.

**Implementation:** After the design is fully developed, it is implemented. This phase enables the instructional designer to test all completed material before it is shown to the intended audience and evaluated. The phase ensures that the implemented material is fully functional, and free of bugs and mistakes like spelling errors.

**Evaluation:** This phase consists of *formative* and *summative* evaluations. *Formative* evaluations are involved in every stage of the ADDIE process, and typically involve qualitative feedback rather than quantitative testing. The evaluation may

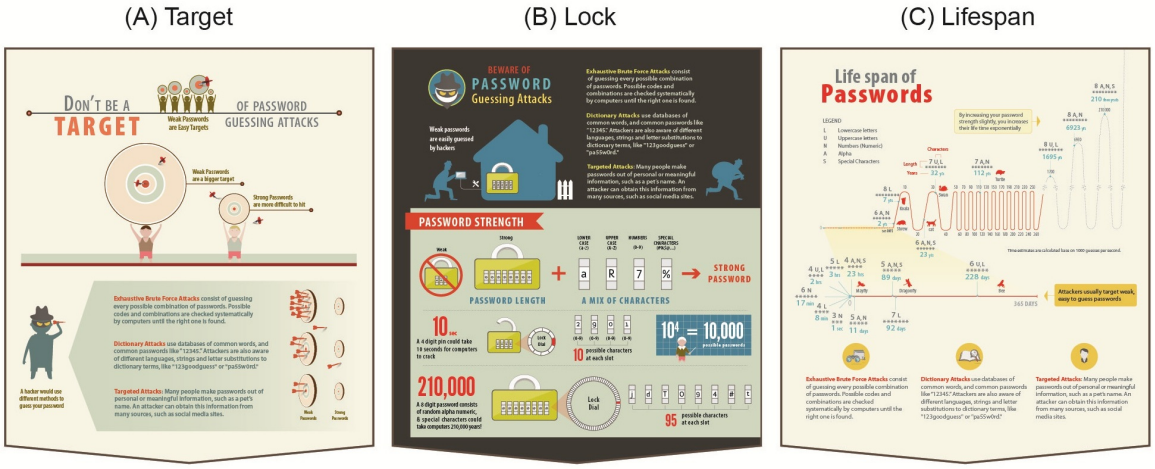



Figure 4.2: The portion of our three infographic designs explaining how password guessing attacks work

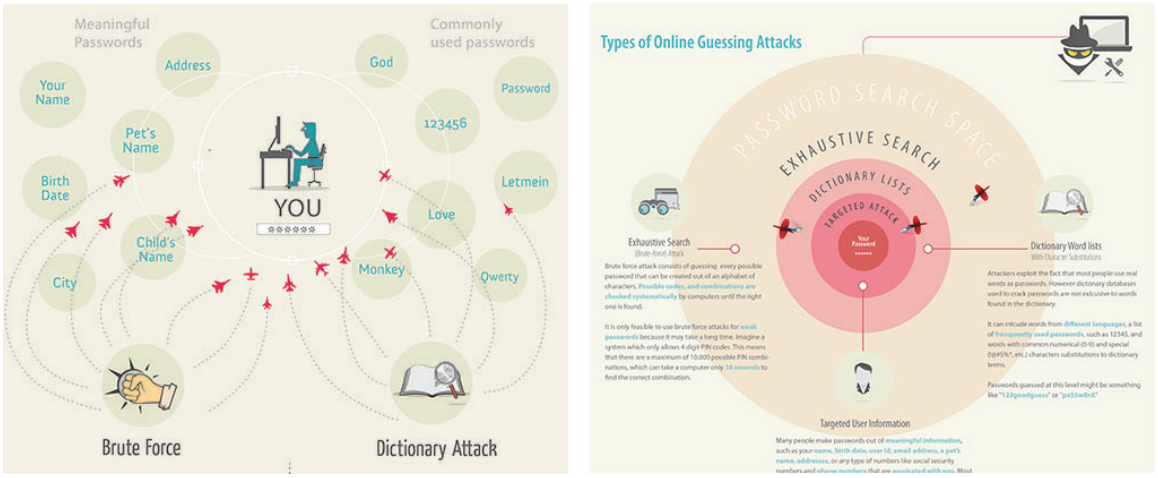



Figure 4.3: A portion of two early exploratory layouts for the *Target* concept

be formal or informal (e.g., from pilot testing a prototype to getting informal feedback from a colleague). *Summative* evaluations seek to monitor learning outcomes after a particular time has passed, and aims to summarize learning up to that point. *Summative* evaluations are typically done at the end of the *implementation* phase.

## 4.2 Password Guessing Attacks Infographic Designs

We used infographics to communicate to end users about the threat of password guessing attacks (Appendix A.1). Our prototypes aim to deliver knowledge and ideas

visually, so users can understand them quickly. In the *analysis* phase of the ADDIE process, we began by researching the problem space by exploring both academic and public resources to identify common problems. For example, we explored public security advice resources available to end-users, misconceptions users may have, popular analogies and metaphors used to explain the risks, and challenges end-users face while learning about the topic. After gaining an understanding of the challenges, we focused on what might be the most helpful information to give end-users. We narrowed down several ideas that have the most potential and selected three metaphors for our infographic prototypes, *Target*, *Lock*, and *Lifespan* (see figure 4.2 A, B, and C, and available online at [111]). They were selected because they represent a sample of metaphors commonly used in public communications media (e.g., [89], [41], [72]), or in computer security literature (e.g., [14], [87], [103]). In the *design* and *development* phase, we refined the ideas and determined how to present them to end-users visually. Sketches and exploratory layouts were produced. Figure 4.3 shows two clippings of the initial exploratory layouts for the *Target* concept. After receiving feedback from members of our lab, we iterated the layout several times. Lastly, we implemented the designs using Adobe Illustrator. During the *evaluation* phase, we printed the infographics on large format posters. To ensure that our findings are not specific to one design, we tested three different visualizations and compared their effectiveness with a text-only condition. We provided the same basic textual information on all three prototypes, first teaching about *how* guessing attacks work, by describing brute-force, dictionary, and targeted attacks. Secondly, we gave advice on creating and managing secure, memorable passwords. We used a metaphorical explanation unique to each infographic accompanied by graphic devices that most powerfully represented each metaphor. The amount of information included on each infographic varies from the least complex (*Target*), to moderately complex (*Lock*), to the most complex (*Lifespan*). All of our prototypes are available online at *http://www.versipass.com/edusec*. In the next few sections, we provide detailed rationales of our prototype designs.

### 4.2.1 Selected Metaphors for Password Guessing Attacks

**Target Metaphor:** "Don't be a target" is a common tagline used in public safety and security communications media. For example, financial institutions like Royal Bank of Canada have used this approach to raise awareness about theft prevention in public settings [89]. Similarly, our *Target* concept promotes risk reduction. It communicates the message that weak passwords are easier to crack than strong passwords, therefore users with weak passwords are bigger targets for attackers. We illustrated the idea by showing a hacker taking aim at dartboards of various sizes (figure 4.2 A). Weak passwords are represented by large dartboards, and strong passwords by smaller ones, suggesting that weak password are more vulnerable to password guessing attacks because they are easy targets.

**Lock Metaphor:** The lock is a widely used security metaphor, due to users' familiar understanding of padlocks and keys in the physical world. Most security programs like antivirus software, encryption software, and SSL certificates use the lock as a verbal and visual metaphor. In "A Brick Wall, a Locked Door, and a Bandit" [87], the concept of a locked door was tested as one of the physical security metaphor for firewall warnings. In our prototype, we illustrated the concept through burglary, which is one of non-expert users' mental models of hackers [103]. We use combination locks to visually depict password strength (figure 4.2 B). Length is portrayed by the number of dials on the lock, while strength is portrayed by the size of each dial and how many characters it contains.

**Lifespan Metaphor:** In password policies, the "lifespan" of a password usually refers to the period of time before the password of a user account expires [72]. In our *Lifespan* prototype, we used a similar metaphor to refer to password cracking, where weak passwords that are easily guessed by attackers are represented by short lifespans, and strong passwords represented by exponentially longer lifespans. Based on our experience in authentication research, users often underestimate the length of time it takes hackers to crack passwords, because they assume most passwords would be difficult for humans to guess [45]. According to research conducted by Deloitte Canada, more than 90% of user-generated passwords would be vulnerable to hacking in 2013 [29]. The "life expectancy" of passwords can demonstrate how long it would

take to crack [41]. We illustrated this concept on a line graph with passwords plotted over the time it takes to crack them (figure 4.2 C). We overlaid animal icons on the graph to give users a reference to animal lifespans. Our calculations are based on the estimated theoretical password space of attacks with the computational power of delivering 1000 guesses per second.

### 4.2.2 Password Advice

There is a body of evidence indicating that typical computer users suffer from "password overload" [80]. In order to cope with remembering multiple passwords, users turn to unsafe practices such as password reuse. Standard password advice recommends that users create passwords that are unique to each account, at least 8 characters long, and consists of alphanumeric and special characters. Although this is ideal practice, cognitive challenges of remembering complex passwords mean users often ignore the advice and continue to use unsafe alternatives. We believe that in addition to giving users security advice, users should be given practical coping strategies for remembering their passwords. With this in mind, our password advice is based on the following considerations:

- Use a strategy like a pass-phrase
- Prioritize strong passwords for high-value accounts
- Use passwords that are long enough to be secure
- Choose passwords that are hard to guess

The infographics recommend that users create a personal strategy to help them remember passwords. An example of our recommendation is to use a pass-phrase such as *"My sister Peggy's 29 years old"* to make the password *"MsP'29yo"* (see figure 4.4). Passwords created from a personalized pass-phrase can help to ease the memorability challenges of strong passwords [59], but they should be personalized rather than using popular slogans, song lyrics, or other sources that are easily accessible by attackers building attack dictionaries [66]. We further recommended to users that they should prioritize strong passwords, and always create unique, strong passwords for high-value accounts like banking and email.

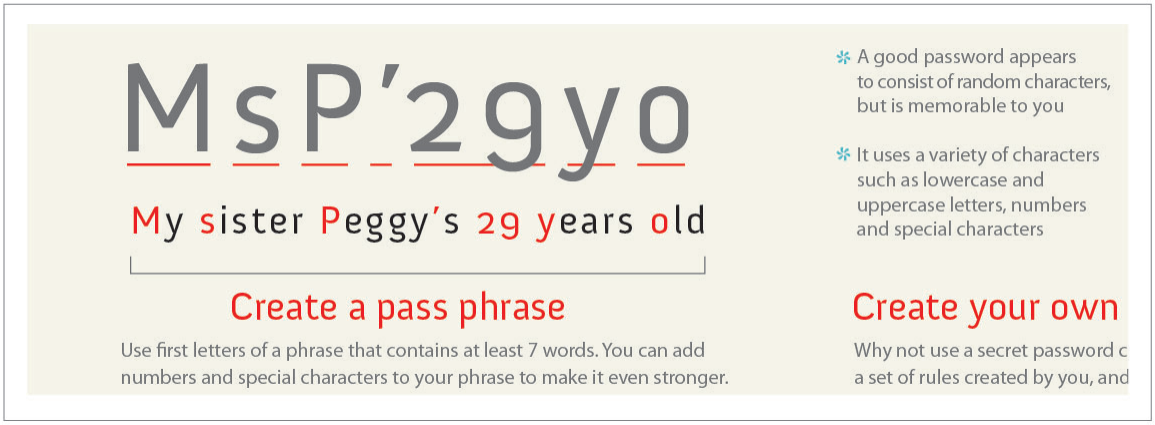



Figure 4.4: A portion of the password creation advice common to the infographics

## 4.3 Antivirus Infographic Designs

We created two infographics to educate users about antivirus protection (Appendix A.2). In the *analysis* phase of the ADDIE process, we explored antivirus protection resources publicly available for end-users, such as antivirus software sites and blogs, as well as antivirus and risk communication literature in computer security. We selected two metaphors, *Surveillance* and *Medical* to help users understand antivirus concepts. The metaphors were depicted visually in conjunction with text information. *Surveillance* is inspired by physical security metaphors (ie., [14], [87]), and *Medical* is inspired by biological models used to predict computer virus outbreaks [62, 84]. Each metaphor was incorporated into an infographic to test its effectiveness against text-only advice with no metaphors. Comparing two different infographics to one text-only condition helps to ensure that our findings are not specific to one design. We provided identical textual information on both infographics, first describing *how* antivirus software works, followed by a tips and myths section. We explored how to depict the two concepts visually during the *design* and *development* phase and presented them to members of our lab to get feedback. Figure 4.5 show initial exploratory designs for the two infographics. The feedback we received suggested that our initial designs may be too abstract to demonstrate the concept concretely. In the final designs, we made the idea of physical security more prominent in *Surveillance*, and opted for a clinical-like design for *Medical*.

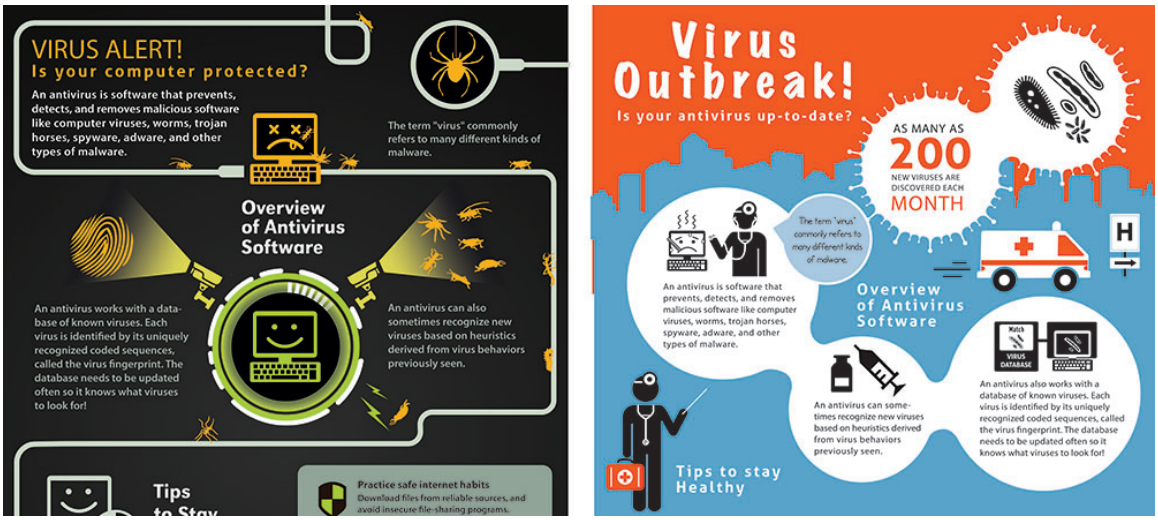


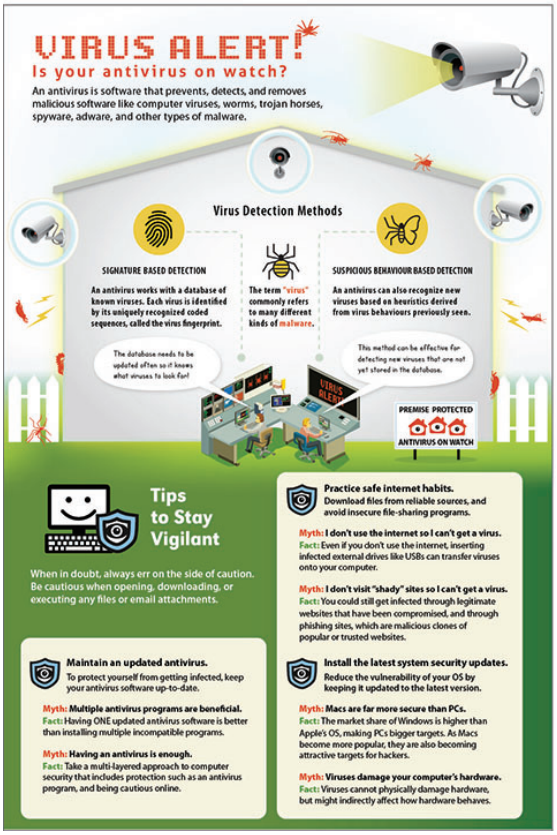

Figure 4.5: A portion of two early exploratory layouts the *Surveillance* and *Medical* concept

Keeping an up-to-date antivirus is an important step in antivirus management to ensure the optimal effectiveness of the software, yet many users overlook the importance of updating. We believe providing end-users with a basic understanding of how antivirus works can help to justify why updates are necessary. In the infographic prototypes, we provided basic explanations of signature-based and heuristic-based virus detection methods. In signature-based detection, we emphasized that the antivirus works with a database of known viruses, identified by each virus' unique code sequence. Without regular updates, the antivirus would be unable to recognize new viruses. We described heuristic-based detection as "suspicious behaviour" based detection, where the antivirus looks for previously seen virus behaviours. It may help to detect new viruses that are not yet stored in the antivirus database.

### 4.3.1 Selected Metaphors for Antivirus Protection

**Surveillance Metaphor:** The *Surveillance* infographic leverages people's understanding of physical security, and familiar imagery of virus as bugs (figure 4.6 A). In popular media, it seems that computer viruses are often visually portrayed as some form of bug. Worms, spiders, cockroaches, and other types of hybrid-bugs appear to be the most popular. For one of our infographic designs, we chose to depict malware

(A) Surveillance




(B) Medical

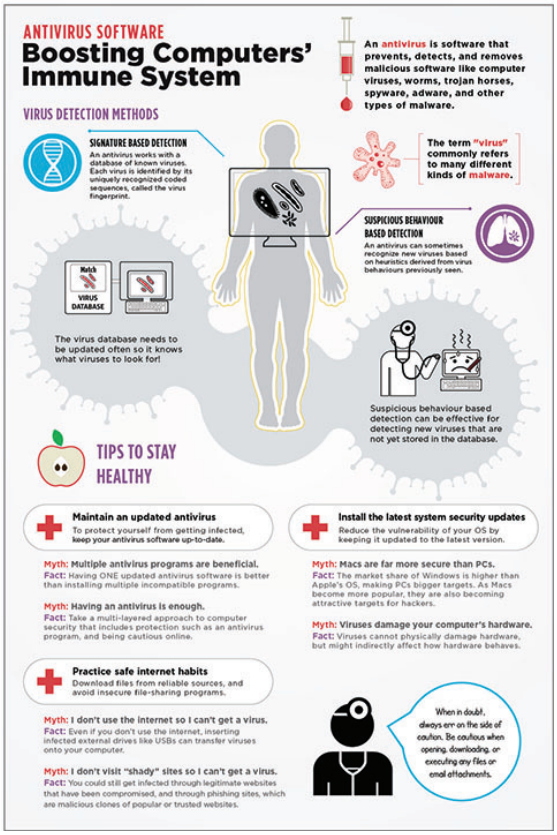



Figure 4.6: Two infographics explaining how antivirus software work, using surveillance and medical metaphors

as insects and show the threat of an infection through physical security. Malware are illustrated as bugs that are invading a house. The antivirus acts as a surveillance system that monitors anything that looks malicious and keeps the premise clean of bugs. Since the antivirus works like a surveillance system, it needs to know how to identify malicious bugs. We explained that the antivirus works with a database containing virus "fingerprints" and it needs to be updated to recognize new viruses. The antivirus also checks for suspicious behaviour. We illustrated a suspicious looking butterfly with half wing, half spider legs, to imply that the antivirus will likely catch a bug that appears to be malicious, but is previously unknown.

**Medical Metaphor:** Metaphors inspired by biology are probably the most widely used to portray malware. The term "virus" itself has roots from biology and mirrors similarity in ways it is spread. Since "virus" is a widely used term, Wash [103]

found that users tend to rely on medical terminology to describe malware actions, such as to be "infected" with a virus means that your computer has "caught" a virus. Many researchers have looked into ways antivirus software can be modelled based on biological systems, such as animal immune systems [61, 94].

In the *Medical* infographic, we portrayed how malware can infect computers like a biological virus, and the antivirus is the medicine or vaccine that could cure the body and prevent future infections (figure 4.6 B). We were inspired by traditional medical posters of human anatomy that are often seen in doctors' offices. The intention is to give the infographic a "clinical" feel and convey the seriousness of the issue from a health care perspective. We overlaid a wireframe computer monitor onto a silhouette of a human body. Where the two shapes overlap, it is as if the screen is performing a scan of the human body and the viruses become visible. Overlaying the two elements together implies that computers can "catch" a virus like a human, and having an antivirus is like performing a scan that reveals infections which can then be addressed. Each virus has a unique code sequence like DNA. The antivirus can identify viruses by their unique DNA if they are stored in the database. Outdated DNA libraries cannot protect against new viruses. Therefore, the antivirus database needs to be updated often with new virus DNAs. The antivirus can also look for suspicious virus behaviour, just like how doctors diagnose patients based on previously seen symptoms.

### 4.3.2 Malware Protection Advice

Although antivirus software is effective for malware prevention, it is not a foolproof solution to protect users. Many viruses are spread through social engineering, such as phishing emails and spoofing. According to Wash's "folk models" [103], many misconceptions surrounding viruses exist, including but not limited to: Macs are immune to hacking problems; intentional downloading and clicking on links is necessary to get a virus; and viruses can be prevented by avoiding the "bad" parts of the internet. We believe that in conjunction to promoting the need for antivirus software, it is important to help users correct common misconceptions that could lead to insecure actions.

In both antivirus infographics, we presented advice in three categories to promote

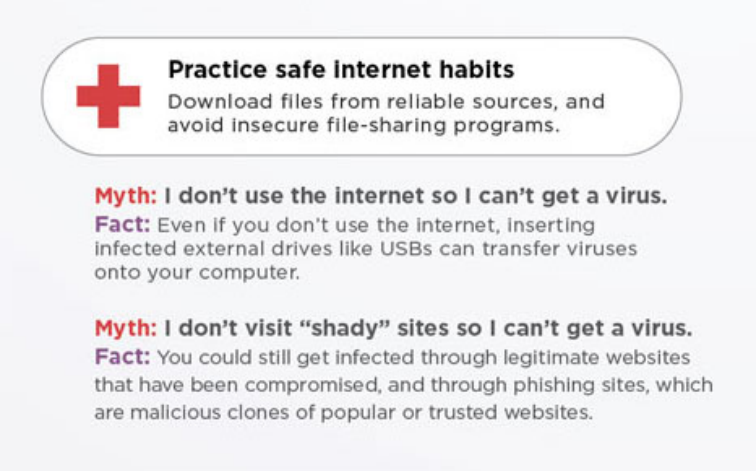



Figure 4.7: One section of tips and advice given on each antivirus infographic

a multilayered approach to security: antivirus management, internet safety, and system security. We then summarized common myths surrounding each category. For example, many people believe they could not get viruses if they do not use the internet or if they only go to trusted websites [103]. Under "Practice safe internet habits", the infographics point out the two myths "I don't use the internet so I can't get a virus," and "I don't visit shady sites so I can't get a virus," immediately followed by "facts" to counter each myth. Please refer to figure 4.7 for an example of the advice.

## 4.4 Design of the Interactive Comics

As detailed in Chapter 5 and 6, the infographic studies highlighted that most users prefer to learn visually. Building on this idea, we explored whether a richer visual experience would enhance learning. We chose a comic book format as the teaching media, and developed online comics to educate users. The comic prototypes are available online [111] (note: Adobe Flash player is required to view the comic). In addition to metaphors, we included various stimuli to engage the user; for example, characters, narrative, humour, and interactivity. See figure 4.8 for two example pages from the password comic.

To the best of our knowledge, the only extensive exploration of the comic medium in computer security education is *Security Cartoons* [95]. It uses a series of short 2 to 3 panel comic strips to improve non-expert users' understanding of various risks [95].


Figure 4.8: Two individual panels from the password comic

Mainstream comics that have security advice include Dilbert [3] and XKCD [75]. Although these resources exemplify that the use of comic media is a promising approach to educate users about security, they mostly provided fairly shallow, prescriptive advice. Furthermore, no empirical evidence is available to support the actual effectiveness of comics in the context of computer security education. We fill in the gap by formally evaluating our comic prototypes, and providing empirical results of their effectiveness at altering user perceptions and changing user behaviour.

We created three main characters for the comics. *Jack* and *Nina* are agents of computer security. They solve computer security crimes and protect users against *Hack*. As the name implies, Hack's mysterious character embodies all computer security crimes. Jack and Nina take on the role of mentors who teach users about password guessing attacks and antivirus protection. Characters are designed with a sense of humour to make them seem well-rounded, interesting, and believable [78].

As part of the online comics, we explored interactivity to offer users additional insights. For example, in the "Types of Attacks" section of the password comic, users can rollover silhouettes of people to see examples of strong and weak passwords. People with weak passwords are highlighted with a target icon, indicating that they are vulnerable to password guessing attacks. At the end of each comic, users have the option to play a "test your knowledge" mini game. The purpose of the mini game is to review and practice important concepts that were taught in the comic.

The prototypes use original artwork drawn by us in Adobe Illustrator using a Wacom Intuos 5 tablet and programmed in Adobe Flash. In the *design* phase, we first created written scripts of the comic dialogue and storyline. After the completion of the scripts, we designed the characters and produced storyboards drawn on paper to plan out the narrative and interactions. During the *development* phase, the sketches were scanned and imported into Adobe Photoshop and overlaid with text dialogues to test whether the images and text pairings work together in each frame. At this stage, the designs were iterated several times until we arrived at the final storyboards. For *implementation*, the storyboards were imported into Adobe Illustrator, and each screen was drawn and coloured with a graphic tablet in vector format. The interactive elements in the comics were also drawn in illustrator, and later imported into Adobe Flash. We follow the same design process for the password comic and the antivirus comic. Figure 4.9 and 4.10 shows storyboards from the *implementation* stage and screens from the final comic designs. Participants viewed the both comics as .swf files on a Macintosh laptop computer during the studies. After study completion, we made the comics accessible to the public online [111].

### 4.4.1 Password Guessing Attack Comic

The password guessing attack comic has three main sections: password guessing, types of attacks, and tips/advice, preceded by an introduction and concluding with a mini game (Appendix C.1). The comic begins by introducing common challenges of managing multiple password-protected accounts and the importance of protecting passwords. We use a physical security metaphor to support the burglar mental model [103] to convey the risk of compromised passwords. Then, users are taught about three types of online password guessing attacks: exhaustive brute-force, dictionary, and targeted attacks (figure 4.11 A). In the tips and advice section, we taught users how and why they should use strong passwords. Since participants responded positively to the pass-phrase strategy used in the infographic studies, we repeated the same strategy in the comic and showed additional examples of how to make pass-phrases (figure 4.11 B). Lastly, the mini drag-and-drop game tests users' judgement of the strength of sample passwords based on what they have learned. The game

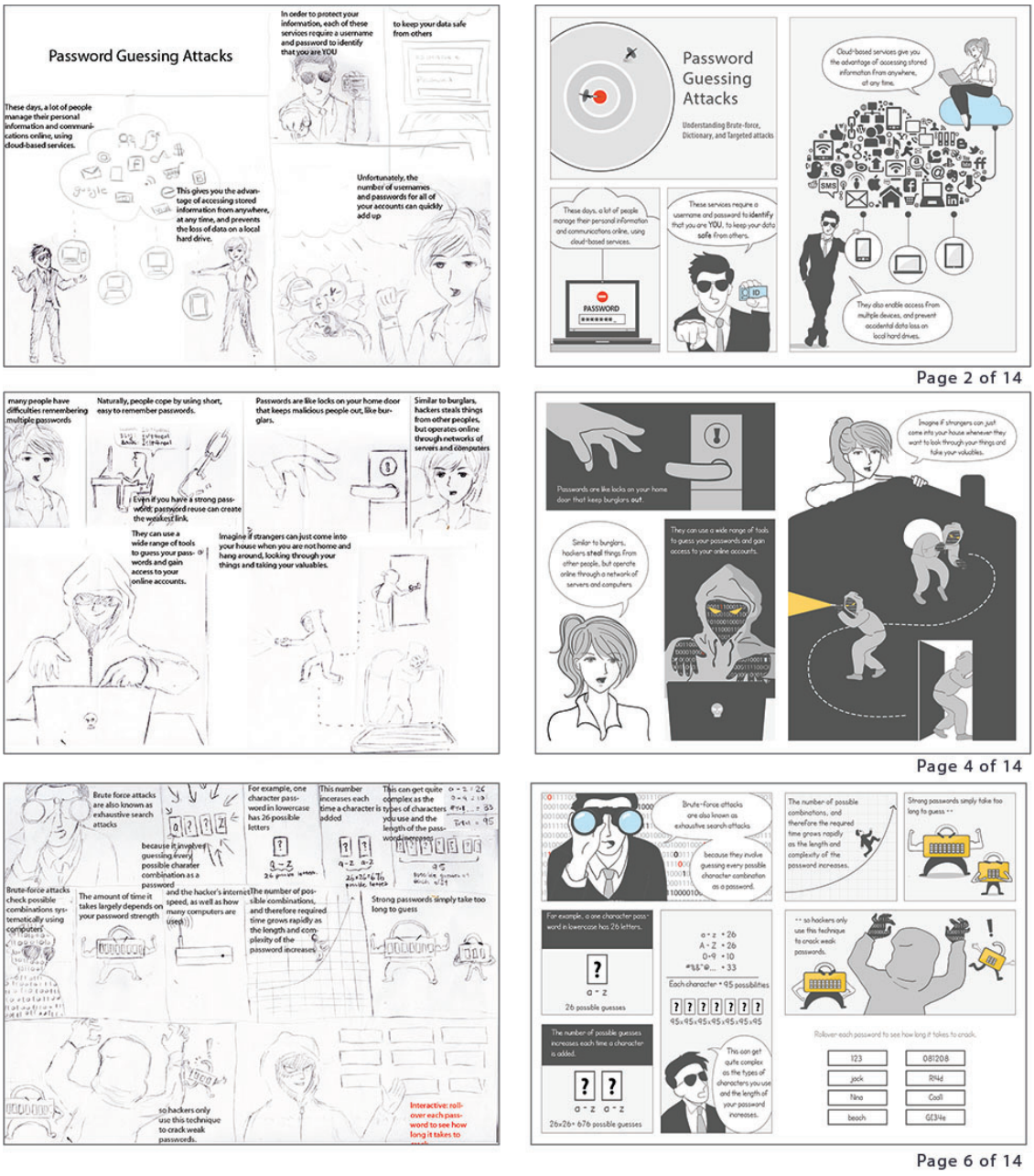



Figure 4.9: Examples of storyboards (left) used to plan the password comic

offers immediate user feedback after each right or wrong answer to help to reinforce lessons taught in the comic.

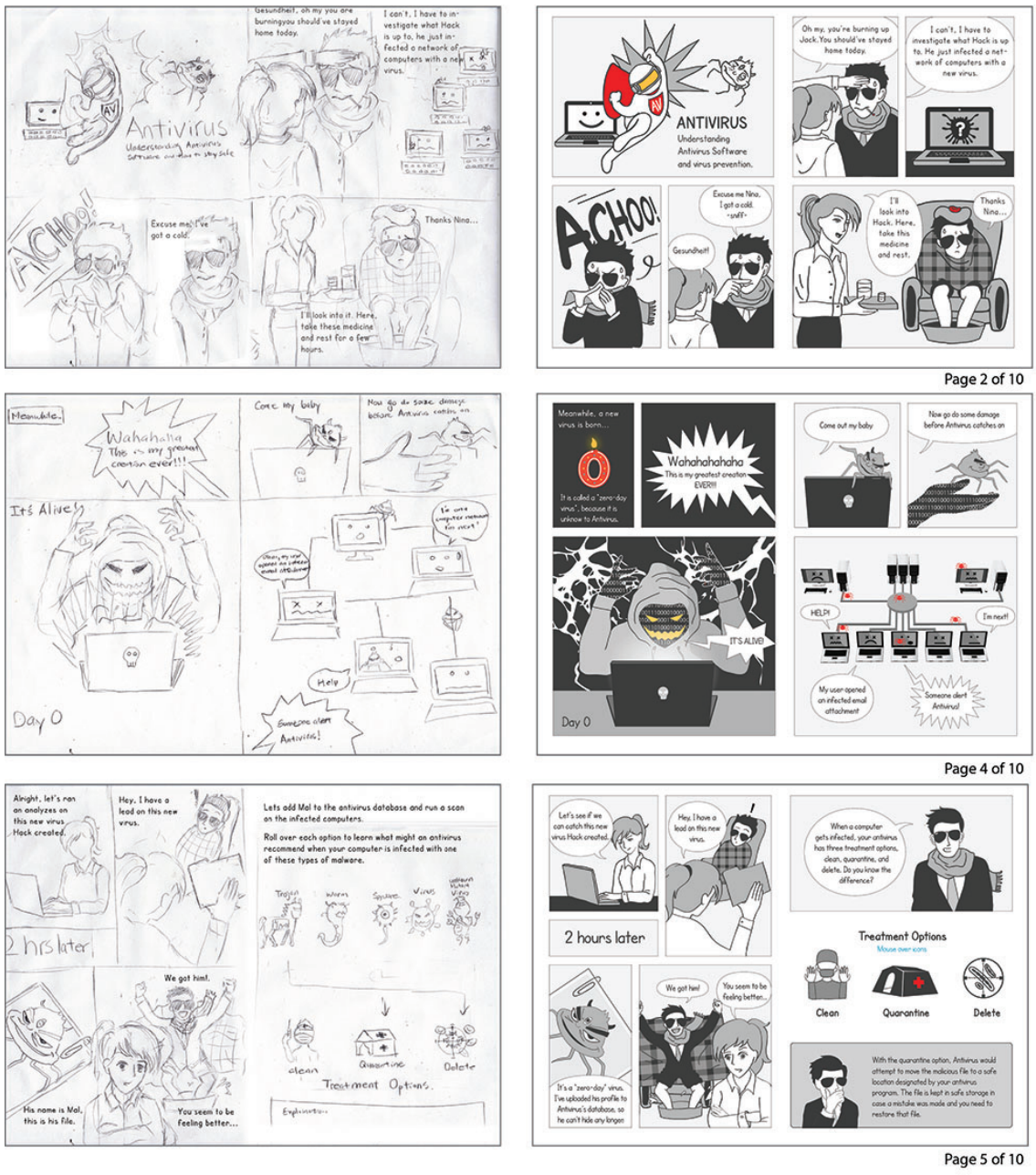



Figure 4.10: Examples of storyboards (left) used to plan the antivirus comic

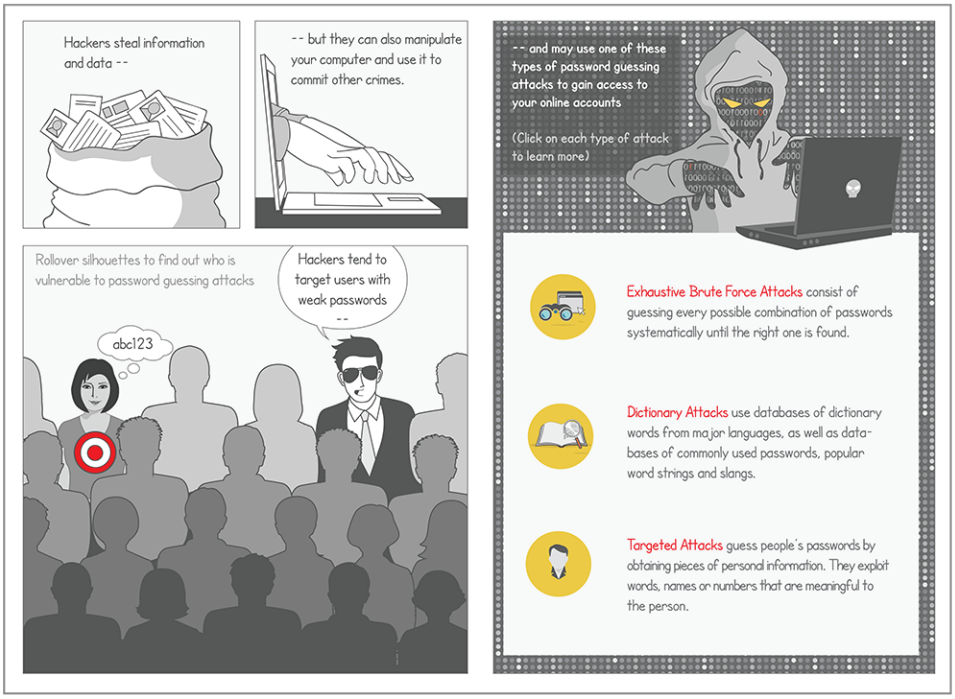
### 4.4.2 Antivirus Protection Comic

We followed the same storytelling format for the antivirus comic. The comic has three main sections: types of malware, how antivirus works, tips and advice, preceded by an introduction and concluding with two mini games (Appendix C.2). We used a

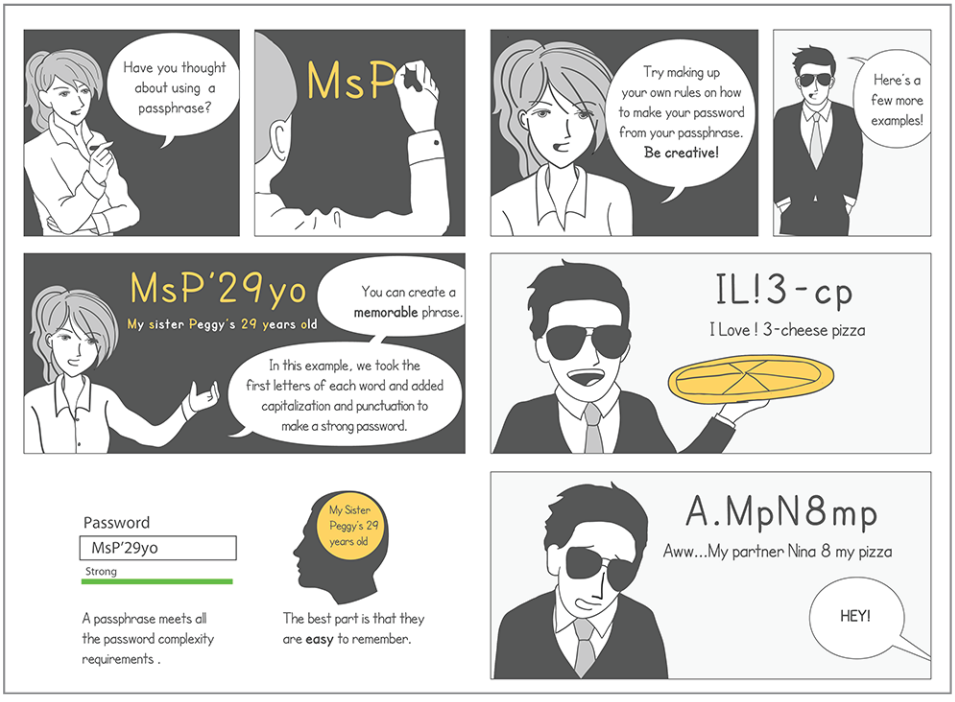
medical theme to help explain the concepts. At the beginning of the narrative, one of the main characters catches a cold, while *Hack* infects a network of computers with viruses. This alludes to the medical theme and it is carried throughout the comic. Feedback from our infographic study indicated that users have an interest in learning about different types of malware. We specifically dedicated one page of the comic to explain the difference between virus, worm, trojan horse, spyware, and hybrid malware (figure 4.12 A). The following section of the comic teaches users about how antivirus software works (figure 4.12 B). In addition to explaining signature and heuristic detection methods, we clarified the difference between clean, quarantine, and delete options used in most antivirus software. Again, we used a medical concept to illustrate these concepts. The tips and advice section aims to dispel common myths among antivirus users. Lastly, the comic ends with two mini games. The first mini game tests whether users can identify the difference between different types of malware, and the second game helps to correct any myths that the participants still hold.

## 4.5 Summary

We provided design rationales for our infographics and comic prototypes that teach users about password guessing attacks and antivirus protection. After the design process was completed, we conducted several user studies to evaluate their effectiveness. In the following chapters, we present the study results.




A




B

Figure 4.11: Two pages from the password comic (A: How attacks work, B: Passphrase)


Figure 4.12: Two pages from the antivirus comic (A: Types of malware, B: How antivirus works

# Chapter 5

# Improving Mental Models of Password Guessing Attacks

We conducted three between-subject user studies with a total of 89 participants to evaluate the prototypes we developed for teaching users about password guessing attacks. We first report our password infographic study results, followed by the password comic results. We analyze participants' answers from online questionnaires and performed statistical tests to evaluate the effectiveness, usefulness, memorability, and persuasiveness of the prototypes. Next, we report the findings of a eye-tracking experiment using our password comic. Lastly, we provide qualitative analysis of the interview data that identifies perceptions and mental models surrounding password guessing attacks.

## 5.1 Password Infographics User Study

### 5.1.1 Study Design

We performed a user study to test the effectiveness of our three infographics with corresponding metaphors to communicate to users about password guessing attacks, as well as a text-only condition with no metaphor. We will refer to each infographic by the metaphor they present: *"Target"* for infographic A, *"Lock"* for infographic B, and *"Lifespan"* for infographic C. The text condition will simply be referred to as "*Text*". To recap design rationales provided in Chapter 4: *Target* focuses on the message that people who have weak passwords are bigger targets for hackers, *Lock* illustrates the threat through a physical security concept, burglary, where the malicious intention of hackers is explicitly shown, and *Lifespan* makes the case that passwords have a life expectancy, based on how long it takes for hackers to crack them. The three concepts were presented to participants on posters measuring $20 \times 30$ inches each.

The text-only condition was taken directly from Wikipedia's description of how

"password cracking" works [107], including a section giving advice on how to create passwords that are "easy to remember" but "hard to guess" (Appendix B.1). Although much password advice is available online, we selected content from this source because Wikipedia is a publicly accessible and popular learning resource, and the type of content provided on password guessing attacks is closely comparable to our infographics. We kept typographic styles such as headings, bold, and italics, and presented the information on letter size printouts, in 12pt font across 2 pages. To avoid learning effects between conditions, we used a between-subject design to assess which condition best facilitates learning about the subject. Testing was conducted through one-on-one sessions with the experimenter. The study was approved by the Research Ethics Board at Carleton University. The components of the study are described below. In the following descriptions, "prototype" refers to the user-assigned infographic poster or text printout.

The independent variable in the study was the visual communication form of infographics. We wish to study whether infographics produce a more positive learning experience, and significantly increase knowledge transfer and retention compared to the text-only condition. As explained above, the four study conditions include three graphical conditions: *"Target"* infographic, *"Lock"* infographic, *"Lifespan"* infographic, and a baseline condition of plain text that contains no graphics and metaphors. Three different graphical conditions help to ensure that the results are not specific to a single infographic design. The dependent variables were participants' evaluations of the prototypes based on the learning experience. Participants completed a online evaluation questionnaire that consisted of Likert scale questions. They gave ratings to statements pertaining their perception of the prototype's effectiveness and the learning experience immediately after viewing a assigned infographic or text condition. One week later, participants completed a followup questionnaire to assess whether knowledge about password guessing attacks significantly changed before and one week after viewing a prototype.

Based on previous work in education literature on the effect of visual information for learning, we formed the following hypotheses:

1. The teaching media of the three infographic conditions will be perceived as more

effective at educating users about password guessing attacks than the text-only approach.

2. Information visualized in the three infographic conditions will be perceived as more useful at conveying password guessing attacks than text-only information.

3. Advice from the three graphical conditions will be perceived as more persuasive at convincing users to change weak passwords than text-only advice.

4. Information presented in the three infographic conditions will be perceived as easier to remember than text-only.

5. Knowledge about password guessing attacks will increase one week after viewing the three infographic conditions, and no significant increase for the text-only condition.

We used the non-parametric Kruskal-Wallis and Mann-Whitney U significance tests to analyze participants' Likert scale evaluations of the prototypes, based on participants' perceptions of the prototypes' effectiveness, usefulness, persuasiveness to change passwords, and memorability. McNemar significance tests were used to assess whether knowledge about the security topic significantly changed before and one week after the experiment. See table 5.1 for a summary of statistics used in the thesis.

### 5.1.2 Materials

**Pretest questionnaire:** Before prototype viewing, we gave participants a pretest questionnaire to have a base understanding of their current knowledge of password guessing attacks, as well as their present password behaviours. This data enabled us to make meaningful comparisons with the followup questionnaire completed a week later. All questionnaires were administered online using LimeSurvey [17], which stored data on our local server.

**Demographic questionnaire:** The demographic questionnaire collected standard demographic information about the participants, such as age, gender, education,

| NAME | DESCRIPTION | USAGE IN THE THESIS | EXAMPLES & VARIABLES |
|---|---|---|---|
| Kruskal-Wallis | Non-parametric test that compares the ordinal distributions between more than two groups. | Significance tests of participants' post-prototype viewing Likert scale evaluations of the conditions. | $H(a) = n$, $p < .05$<br><br>$a$ = degrees of freedom,<br>$n$ = value of the $H$ statistic, used to determine $p$,<br>$p$ = significance level |
| Mann-Whitney U | Non-parametric test that compares the ordinal distributions of two samples of data. | Significance tests that compare the distribution of Likert scale data in sample pairs. | $U = n$, $p < .05$<br><br>$n$ = value of the U statistic, used to determine $p$,<br>$p$ = significance level. |
| McNemar | Compares two correlated proportions that are based on the same sample of subjects or on matched-pair samples. | Significance tests of whether knowledge about the security topic significantly changed before and one week after the experiment. | $X^2(a) = n$, $p < .05$<br><br>$a$ = degrees of freedom,<br>$n$ = value of the $X^2$ statistic, used to determine $p$,<br>$p$ = significance level. |

Table 5.1: Summary of statistics used in the thesis

and background. Participants also provided information about whether they had prior training on password guessing attacks.

**Prototype viewing:** Participants were told that they could take as much time as they want to view the prototype. The infographics took on average 2 minutes to read, and the text condition took on average 6 minutes to read. The experimenter noted immediate reactions from the participant. Afterwards, we had a brief interview with each person to openly discuss their opinions of the prototype. Participants were encouraged to be honest and point out if there is anything difficult to understand or confusing about the concepts. The experimenter took notes of the comments made by the participant, and any misunderstandings of the metaphors, layouts, and other graphical elements on the infographics, and comments about the information presented in the text condition.

**Post-viewing questionnaire:** After prototype viewing, participants were asked

to complete a questionnaire about the prototype. It had 14 Likert scale questions, on a scale of 1 (strongly disagree) to 10 (strongly agree). Participants were asked to give a rating to each statement about the prototype. We reversed the direction of a few questions to avoid bias.

**One-week followup questionnaire:** Participants were emailed a link to an online followup questionnaire one week after their scheduled lab session. The purpose of the questionnaire is to assess information retention. We intended to compare the results to the pretest questionnaire to evaluate if there are improvements in users' understanding of guessing attacks. We included one question verbatim from the pretest questionnaire, which asked users to describe in their own words how password guessing attacks work. This enabled us to compare answers from the two occasions. To assess if participants learned useful password strategies, we asked them to create two strong passwords and explain how they created them. Additionally, we created a knowledge quiz with 7 true and false questions and a multiple-choice question.

### 5.1.3 Participants

We recruited 55 participants from our university. We randomly assigned 15 users to each infographic prototype and 10 users to the text-only condition. Participants were recruited through flyers posted on bulletin boards across campus, and through a faculty and staff subscribed email newsletter. Participants were given a $10 honorarium.

We did not specify a knowledge level of computer security to qualify for the study. According to our pretest questionnaire, our randomly selected participants' behaviour for creating and maintaining passwords are in line with past research on the challenges of text-based authentication schemes [45, 108]. 50 out of 55 (91%) of our participants said they have difficulty remembering passwords. Other strategies used by our participants also correspond to past findings [45,108], including password reuse (32 participants, 58%), use of personal information in passwords (24 participants, 44%), and writing down passwords (11 participants, 20%). Ten participants said they use a password manager (18%), 4 (7%) use variations of the same password, and 2 (4%) make passwords based on account information.

For current passwords, 47 (85%) participants reported using 6-8 alphanumeric

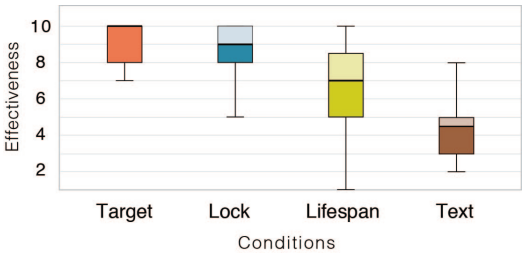



Figure 5.1: Password infographics: Likert scale responses assessing the *effectiveness of each prototype at conveying information* (10 = most effective, 1 = least effective)

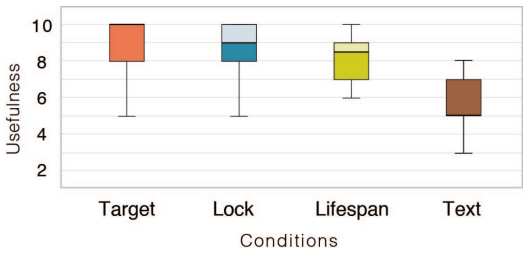



Figure 5.2: Password infographics: Likert scale responses assessing the *usefulness of the presented information* (10 = most useful, 1 = least useful)

characters or longer, and the remainder reported using insecure passwords that are less than five characters. Lastly, participants self-rated their knowledge about how password guessing attacks work. More than half (32 participants, 58%) self-declared to have very little or no idea about how the attacks work. Only three participants considered themselves to be very knowledgeable, and 20 (36%) participants said they have some ideas about how password guessing attacks work.

### 5.1.4 Password Infographics Study Results

In this section, we report the results of the post-viewing questionnaire and the one-week followup questionnaire. In what follows, all Likert scale data is presented positively for readability, with 10 = most positive and 1 = least positive. To analyze the Likert-scale responses, we used the non-parametric Kruskal-Wallis and Mann-Whitney significance tests to evaluate whether any differences were apparent between the four conditions. In all cases, $p < 0.05$ is considered significant.

#### Post-Viewing Questionnaire Results and Feedback

Participants evaluated their learning experience in a questionnaire immediately after viewing the material. We focus on four particular comments from the questionnaire and user feedback: effectiveness of the visualization, usefulness of the information, persuasiveness to update current passwords, and memorability of the information.

**Effectiveness for learning:** Most of our study participants (84%) said they are

visual learners. Less experienced users perceived visualizing the process of password guessing attacks to be the most helpful. Although knowledgeable users felt that they did not learn new information, they agreed that visualization was a good way to teach novice users. Participants commented that they liked the graphics in *Target* and *Lock* infographics and thought the metaphors were effective. The *Lifespan* infographic was generally perceived to be the least effective because participants did not easily comprehend how the metaphor is associated with passwords.

Figure 5.1 shows the Likert scale responses for users' perceived effectiveness of each of the infographics compared to the text-only condition at communicating about password guessing attacks. From the figure, it appears that the *Target* (median 10/10) and *Lock* (median 9/10) infographics are more effective than the *Lifespan* infographic (median 7/10), but all three infographics were considerably more effective than the text-only condition (median 4.5/10). To confirm this result, a Kruskal-Wallis test showed a statistically significant difference between perceived effectiveness of the four conditions ($H(3) = 22.5$ with $p < 0.001$). To determine where the differences lay, Mann-Whitney tests with a Bonferroni-corrected p-value of ($p < 0.05/4 = 0.013$) were used. All three infographics are perceived to be more effective than the text-only condition: *Target* ($U = 4.5, p < 0.001, r = -0.804$), *Lock* infographic ($U = 17, p = 0.001, r = -0.651$), and *Lifespan* ($U = 38, p = .038, r = -0.416$). Results suggest that infographics are perceived to be significantly more effective by users than text-only information.

Based on verbal feedback, participants responded most positively to the *Target* infographic and found the *Lifespan* infographic most confusing. They found the concept of *Lifespan* to be too abstract for depicting password security. The information in *Lifespan* also took longer to read than the two other infographics. Participants did not find password cracking times relatable to animal lifespans, since most people admit to have only vague ideas of how long animals live. Conversely, participants said that the *Target* poster took very little effort to read and understand. They felt that the concept is concise, "simple but informative." It is "easy to understand" and the communication of the key message is immediate. One participant said "even if I only have the time to look at the poster for a moment, I would at least walk away

with the message that weak passwords are bigger targets for hackers." For the *Lock* infographic, participants said the visuals successfully captured the intentions of hackers, and depicted password strength well. In general, participants commented that they liked the graphics in the *Target* and *Lock* poster and thought the metaphors were effective. Participants thought average users would not read the *Text* condition with interest on their own time. Some participants found the information "a lot to take in at once", "too technical", or "boring" to read.

**Usefulness of the information:** We received positive evaluations across all three infographics on the usefulness of the material. Novice users found the information particularly helpful. Knowledgeable users agreed that the information would be suitable to teach average end-users. One participant said "I already know most of the information, but I think something like this would be great for my parents."

Responses to the Likert scale question about the usefulness of the information are available in Figure 5.2. Based on the responses, we could not determine which infographic participants found to be the most useful. Kruskal-Wallis test showed no statistically significant difference in the perceived usefulness of the information between the three infographics ($H(3) = 2.66$ with $p = 0.26$). However, when comparing the three infographics to text-only, participants perceive the infographics to be significantly more useful ($H(3) = 16.53$ with $p = 0.001$). Mann-Whitney tests show the difference between each of the infographic when compared to the text-only condition are ($U = 9.5, p < 0.001, r = -0.745$) for *Target*, ($U = 23, p = 0.003, r = -0.586$) for *Lock*, and ($U = 21.5, p = 0.004, r = -0.579$) for *Lifespan*.

During open-ended feedback, participants commented that depicting password strength visually through various sizes of combination locks in the *Lock* infographic is very informative. They thought the graphic successfully "depicts what the hacker is trying to do". The *Target* infographic demonstrated password strength on a more abstract level, linking weak passwords with bigger targets. Although participants thought the message was straightforward and clear, they did not learn what constitutes password strength. Once again, participants found the *Lifespan* infographic visually complex, and took more effort to decipher the message. Participants also found that *Lifespan* is not a familiar concept to describe passwords. *Text* took longer

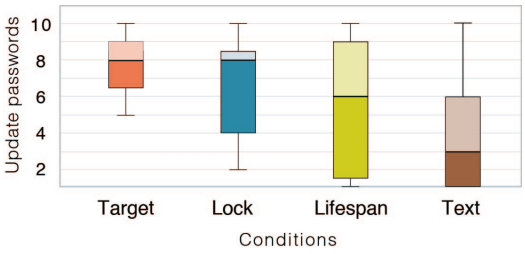



Figure 5.3: Password infographics: Likert scale responses assessing the *likelihood to update current passwords* (10 = most likely, 1 = least likely)

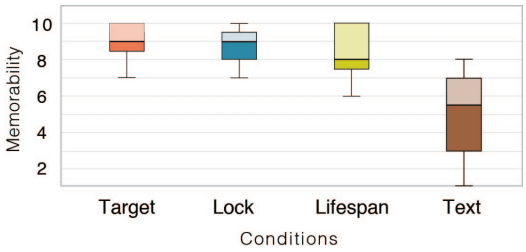



Figure 5.4: Password infographics: Likert scale responses assessing *how likely participants will remember the information* (10 = most likely, 1 = least likely)

and more effort to read than all three infographics. Participants commented that it would be challenging for users to remember information from text descriptions.

**Likelihood to update current passwords:** Participants evaluated how likely they were to update their passwords after reading the material. We found a significant difference between the persuasiveness of the 4 conditions ($H(3) = 8.186, p = 0.042$). Mann-Whitney tests show that the *Target* and *Lock* infographics are significantly more persuasive than text-only, ($U = 23.5, p = 0.004, r = -0.577$) and ($U = 36, p = 0.029, r = -0.4376$). We found no statistical difference between the *Lifespan* infographic and text-only condition ($U = 55.5, p = 0.272, r = -0.22$). Results of the Likert scale question are provided in Figure 5.3. During the study session, we heard comments such as "I need to change my passwords", and "I will Google more about this". The evaluations show that *Target* and *Lock* infographics have greater potential to be more persuasive than text advice.

**Memorability of information:** Participants rated the likelihood of remembering learnt information. A Kruskal-Wallis test showed a statistically significant difference between the memorability of the four conditions ($H(3) = 20.369, p < 0.001$). Mann-Whitney tests show that all three infographics are significantly more memorable than text-only, ($U = 3.5, p < 0.001, r = -0.161$) for *Target*, ($U = 16.5, p = 0.001, r = -0.131$) for *Lock*, and ($U = 12, p < 0.001, r = -0.142$) for *Lifespan*. Results of the Likert scale question are provided in Figure 5.4. We assess the actual information retention of the four conditions in the following section.

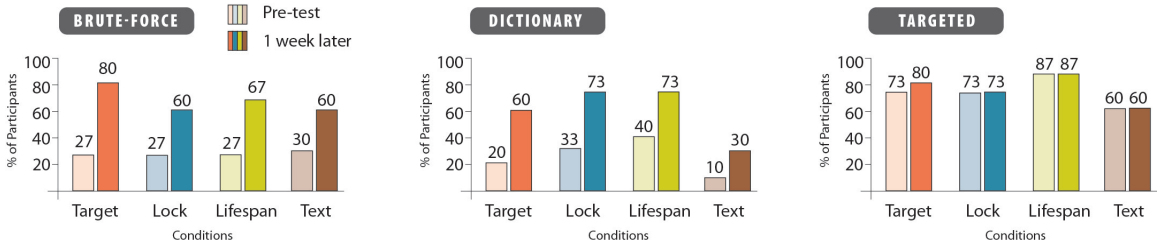



Figure 5.5: Password infographics: participants' ability to describe different types of attacks before and after viewing instructional material

| | | |
|---|---|---|
| Brute-Force Attack | Target | $(\chi 2(1) = 1.364, p = 0.008)$ |
| | Lock | $(\chi 2(1) = 3.636, p = 0.063)$ |
| | Lifespan | $(\chi 2(1) = 2.727, p = 0.031)$ |
| | Text | $(\chi 2(1) = 5.625, p = 0.25)$ |
| Dictionary Attack | Target | $(\chi 2(1) = 2.5, p = 0.031)$ |
| | Lock | $(\chi 2(1) = 2.727, p = 0.031)$ |
| | Lifespan | $(\chi 2(1) = 3.636, p = 0.063)$ |
| | Text | $(\chi 2(1) = 4.286, p = 0.5)$ |
| Targeted Attack | Target | $(\chi 2(1) = 10.313, p = 1)$ |
| | Lock | $(\chi 2(1) = 15, p = 1)$ |
| | Lifespan | $(\chi 2(1) = 15, p = 1)$ |
| | Text | $(\chi 2(1) = 15, p = 1)$ |

Table 5.2: Statistics for the password infographic comparing participants' ability to describe attacks on the pretest and one week later

### 5.1.5 Information Retention

Prior to viewing the study material, we gave participants the opportunity to describe, in their own words, the ways in which hackers try to guess passwords. For comparison, this question was also asked verbatim one week later in an emailed online questionnaire. We received 52 completed responses in the pretest, and 54 completed responses one week later. Blank answers were considered as "I don't know."

We evaluated the answers based on correct descriptions of attacks, not based on participants' ability to define technical terms used in computer security. We assigned a corresponding meaning unit to each correct statement. For example, we attributed participants' answer to "targeted attack" when they wrote "birthdays, names of close family member, and pets", even though they did not identify the name of the attack.

Figure 5.5 shows a summary graph of participants' ability to describe brute-force,

dictionary, and targeted attacks in the pretest questionnaire compared to results from the one week later followup questionnaire. The graph shows that most participants were able to identify targeted attacks across all four conditions in the pretest, but had trouble describing brute-force and dictionary attacks. One week later, participants who viewed an infographic condition showed more dramatic increase in knowledge of brute-force and dictionary attacks than from the text-only condition. Since participants were already familiar with targeted attacks prior to learning, there is little or no change one week later.

To find if the increase in knowledge was statistically significant, we conducted McNemar tests comparing the results from the pretest questionnaire to the one week later followup questionnaire. Refer to Table 5.2 for a summary of the results. We found a statistically significant increase in participants' ability to describe brute-force and dictionary attacks across *Target*, *Lock*, and *Lifespan* infographics after one week. For the *Text* condition, we found no significance. As expected, there were no statistical significant differences for targeted attacks across all four conditions. Most participants had no trouble explaining the idea of targeted attacks prior to learning, and therefore user education had little influence. We discovered from the pretest questionnaire that participants have very limited knowledge of brute-force and dictionary attacks. These result suggest that one week after learning, participants were able to remember the information better from the infographics than from text-only.

In the one-week followup questionnaire, we also asked participants to generate two unique passwords. We did not specify the length of the password or how to create them. We emphasized that the password should be something they can remember. 98% of the participants who viewed an infographic prototype created passwords that were at least 7 characters long. Most created strong passwords using a personally meaningful passphrase. None replicated our example *"My sister Peggy's 29 years old"* from the infographics, although three participants used a passphrase with references to a sister's name and age. 60% of participants who viewed the text-only

condition used variations of passphrase to create passwords. Even though the passwords were at least 7 characters long, half of these participants created weak passwords using strings of whole words and sequential numbers. A few other participants who viewed the text-only condition created passwords from combinations of people's names, strings of unrelated words, and non-English words combined with numbers and special characters.

## 5.2 Password Comic User Study

### 5.2.1 Study Design

For the comic study, we report the results of the post-viewing questionnaire and the one-week followup questionnaire. We use same study protocol, questionnaires as the password infographic study. McNemar significance tests were used to assess whether knowledge about the security topic significantly changed before and one week after the experiment.

The independent variable in the study was the visual communication form of our password interactive comic. We wish to study whether our interactive comic produces an enjoyable learning experience, and positive effects on knowledge transfer and information retention one week later. The dependent variables were participants' evaluations of the prototypes based on the learning experience. Participants completed a online evaluation questionnaire that consisted of Likert scale questions. They gave ratings to statements pertaining their perception of the comic's effectiveness and the learning experience immediately after viewing the comic. One week later, participants completed a followup questionnaire to assess whether knowledge about password guessing attacks significantly changed before and one week after viewing the comic.

Our hypotheses were:

1. The comic will be perceived as an effective teaching tool at educating users about password guessing attacks.

2. Information visualized in the comic will be perceived as useful at conveying password guessing attacks.

3. The comic will persuade users to update weak passwords.

4. Information presented in the comic will be perceived as easy to remember.

5. Knowledge about password guessing attacks will increase one week after reading the comic.

### 5.2.2 Participants

An additional 21 participants were recruited for the comic user study. To prevent overlap in learning outcomes, participants from the infographic study were excluded. 20 out of 21 participants reported having difficulties remembering passwords (95%). 11 (52%) participants practice password reuse, 8 (38%) use personal information, 7 (33%) write down passwords, 2 (10%) use a password manager, and 1 (5%) stores passwords in email.

In the pretest questionnaire, we received answers from 20 out of 21 participants who self-rated their current knowledge of password guessing attacks. 9 participants considered themselves to be somewhat knowledgeable, and another 10 believed they knew very little. Only one declared to be very knowledgeable. Nine participants reported that the typical length of their passwords is 6 to 8 characters, and an additional eight said they were using passwords that are longer than 8 characters. Two participants said the length of their passwords depends on the minimum allowed by the site. Six participants said they are currently using alphanumeric characters, and an additional 11 are using alphanumeric with special characters. Only two participants reported regularly using weak passwords (e.g., numbers only).

### 5.2.3 Post-viewing Questionnaire Results and Feedback

Results of the four Likert scale questions, assessing the effectiveness, usefulness, likelihood to update current passwords, and perceived memorability of the information are presented in Figure 5.6. Overall, participants thought the comic was “enjoyable” and “fun”. They thought people would identify with the characters and wanted to learn more about them. One participant commented “I think it’s great and some

parts are really funny, I never thought that you could present security information like this before."

**Effectiveness for learning:** Teaching users about password guessing attacks through a comic book format was overall well received, with an average score of 9.2 for effectiveness. Most participants found the comic to be visually appealing and said it was enjoyable to read. A participant said "any time you have characters and a story, everything becomes more relatable." Several of the participants chuckled while reading the comic, which is a reassuring response that the use of humour was appreciated. A few participants were unsure of the reading direction at first and offered layout suggestions for future iterations.

**Usefulness of the advice:** Users said they gained useful knowledge from reading the comic ($Mean = 9.2$). As explained by one participant, "I've heard some of this advice before, but never in a cohesive fashion like this." Many users were familiar with the advice concerning password strength, but gained practical information about password guessing attacks. Participants found the coping strategies to be particularly useful to help them remember passwords. They thought that prioritizing strong passwords for important accounts was practical advice and that the passphrase is a "smart" technique.

**Likelihood to update current passwords:** Participants rated the likelihood to update their current password after viewing the comic. 80% of participants said they would most likely update their current passwords. These participants thought that their current passwords were insecure or moderately secure based on the information provided.

**Memorability of information:** The information provided in the comic was perceived to be strongly memorable ($Mean = 9.0$). Participants were surprised by the visualization of how quickly computers can crack weak passwords. Some said seeing how a single character can significantly increase the time to crack a password has motivated them to make their passwords longer in the future. Participants thought the tips and advice section to be particularly memorable, because it shows practical coping strategies that can be easily adopted.

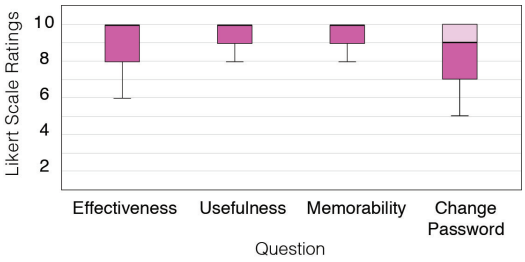



Figure 5.6: Password comic: Likert scale responses for four questions (10 = most positive, 1 = least positive)

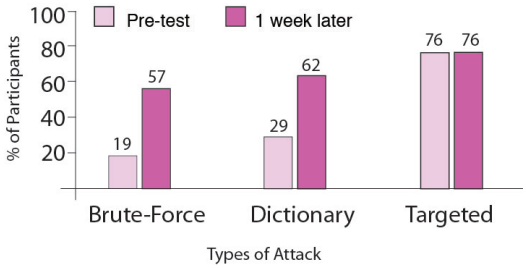



Figure 5.7: Password comic: participants' ability to describe different types of attacks before and after viewing the instructional material

### 5.2.4 Information Retention

Participants' ability to describe brute-force, dictionary, and targeted attacks was measured in the pretest and in the followup questionnaire (Figure 5.7). Again, most participants could describe targeted attacks on the pretest. On the followup questionnaire, participants were more successful at describing all three attacks.

We conducted a McNemar test to analyze participants' ability to describe the attacks pretest compared to one week later. Similar to the infographics study, we found a statistically significant increase in participants' ability to describe brute-force ($\chi 2(1) = 3.706, p = 0.004$) and dictionary attacks ($\chi 2(1) = 5.169, p = 0.008$) one week after viewing the prototypes. Participants were able to successfully describe targeted attacks on both occasions ($\chi 2(1) = 21, p = 1$) and the statistical test showed no difference.

## 5.3 Interview and Eye-Tracking Study of the Password Comic

In the previous infographic and comic study, we explored visual strategies to communicate to users about password guessing attacks and built infographics and a comic to test their effectiveness. In the current section, we present a two-part follow-up study of our interactive educational comic prototype. The goal is to gain more in-depth understanding of users' mental models for creating passwords using one-on-one semi-structured interviews. Our qualitative analysis shows that prior to viewing the comic, users' perception of password guessing attacks is based on a *Target Model*,

leading to a number of implications for password creation, account prioritization, and context of use. Secondly, we report the findings of an eye-tracking experiment that measures how users read and interact with our comic as an learning tool. Use of eye-tracking data is consistent with other multimedia learning studies (e.g., [100]). Our study confirms prior comic eye-tracking studies [57, 81] that elements in comic panel design help to direct reading pattern and user attention. Although several comic eye-tracking studies gave insights into how people read comics, there is little research available on reading comprehension, except for a eye-tracking study by Kinzer *et al.* [63] that examined the effects of text and images in comics and video games on story comprehension of 6th graders. In our eye-tracking experiment, we make possible connections between visual attention and comprehension of the information. Lastly, we report the learning outcome of the comic through analysis of follow-up interviews conducted one week later, and participants's feedback of their learning experience.

### 5.3.1 Methodology

Thirteen people from the university community participated in our study. Based on self-reported evaluations, nine participants had a low of level knowledge about how password-guessing attack work, three have intermediate level knowledge, and one had expert level knowledge.

This two-part study included questionnaires, semi-structured interviews, and prototype viewing on an eye-tracking computer. To pre-assess current habits and knowledge, participants answered a pre-test questionnaire and a one-on-one semi-structured interview. The questionnaire gave a general assessment of participants' demographics, current password strengths, and password coping strategies, while the interview provided an in-depth look at users' understanding of passwords and guessing attacks. Next, participants viewed the prototype on an eye-tracking computer. The primary purpose of incorporating eye-tracking into our comic study is to evaluate how users read security information in comic format, how they use the interactive elements, and how long they spend on various visual elements.

21 two-part interviews were audio recorded and transcribed verbatim by the experimenter. Data was coded using the online data analysis application Dedoose [28].

| DATA EXTRACT | CODES | THEME |
|---|---|---|
| "I changed one for Hotmail, I change one for facebook, which I consider email, and I changed one for Yahoo mail so." | • Update passwords for email accounts.<br>• Facebook is treated like email. | Prioritize strong passwords for high value accounts |
| "The ones that are important, so my banking, OGS, all those type of email passwords, I don't have my computer remember them. But facebook, the computer remembers it." | • Memorize passwords for financial accounts and email.<br>• Computer auto-remembers password for facebook. | |
| "My emails are more secure, because that's pretty important, I use it for work, I use it for job interview, I used it for work purposes." | • Use stronger passwords for emails.<br>• Email is important for work. | |
| "My Carleton account is far more secure than my facebook account, just because nothing important goes on facebook versus Carleton is my official communication with the university. My password is longer, my password is more elaborate, they are not written down because I used them so many times that I have them memorized by now." | • No important information on facebook.<br>• Accounts for official communication are more important than social media.<br>• Use longer and more elaborate passwords for important accounts.<br>• Frequently used passwords are stored in memory. | |
| "If it's something more like my personal information is not going to be on there, or like personal messages or anything like that I don't really care what the password is, so I'd just like choose my simplest password." | • Use simple passwords for accounts that do not contain personal information. | |

Table 5.3: Password interview data analysis: sample data extracts with corresponding codes and theme.

Open coding [97] was used to look for emergent themes. A theme captures something important about the data and represents some level of patterned response or meaning within the data set [11]. First, we read the transcribed interview data several times for overall understanding and generated initial codes. Codes identify a feature of the data that appears interesting to the analyst, and refer to the "most basic segment, or element, of the raw data or information that can be assessed in a meaningful way" [8]. We then applied the codes systematically to the entire data set, organizing data relevant to each code. Our goal was not to disrupt the original meaning of the verbatim statements, but to apply interpretative analysis to the meaning of the statements and organize them into coded units. For each significant statement, we applied a code for the data. Table 5.3 shows examples of codes applied to short segments from a set of 37 data extracts regarding users' classification of high value accounts and rationales of why they chose to use weak passwords. Next, we analyzed and merged similar codes into potential themes. For the example shown, the codes were categorized into a theme that users prioritize strong passwords for high-value accounts. Lastly, we looked for cause and effect relationships between the themes and the overall story the analysis tells in relation to users' mental models. In the case of password guessing attacks we synthesized the themes into an emergent "Target" mental model.

A Tobii 1750 eye-tracking system and Tobii Studio software was used to collect real-time data. The Tobii eye-tracking system uses an infrared camera embedded at the bottom of the computer screen to track eye movements and fixations. The participant sat in front of the eye-tracking computer screen in a normal sitting pose that enabled them to use a mouse to navigate through the comic. A short calibration process enabled the system to recognize each participant's gaze. Participants were simply asked to sit still while following a moving dot across the screen with their eyes. After the initial calibration, participants read the comic on-screen, and were told to interact with screen elements in any way they like. Tracking of eye movement was recorded on screen and outputted as AVI videos. Eye movements were analyzed using these video recordings and time stamps for each participant. We first calculated time spent reading each page and time spent on interactive elements. We also noted reading direction and general characteristics of fixation sequences on each page by

identifying corresponding eye positions on images of the comic. The eye-tracking data tells us in what order and how many times participants fixated their eyes on screen, and which panels were skipped. We also counted the number of times users back-tracked to previously viewed screens, which means participants clicked back to a previously viewed panel to re-read the contents before continuing forward. Lastly, we consolidated results by analyzing reoccurring eye patterns, and average time spent reading.

### 5.3.2 Qualitative Analysis Results

In this section, we summarize our pre-test interview results of user's prior knowledge and perceptions about password management. We uncovered the presence of a *Target* mental model that seemed to impact users' perceptions, misconceptions, and understanding of "good passwords". Users with this model feel that attackers target specific users and that they are not usually likely targets. Users' understanding of password guessing attacks was mostly restricted to targeted attacks, with little knowledge of dictionary and brute-force attacks. When mentioned, users mistakenly envisioned attackers targeting specific users in brute-force and dictionary attacks. This misunderstanding may strongly influence users' ability to make the right password choices.

Users are more likely to create stronger passwords for accounts that they consider high value because these are bigger targets. Even the most cautious users reported sometimes practicing unsafe behaviours, such as password reuse. Participants emphasized that they make an extra effort to use strong passwords for accounts that they consider important. Their passwords for these accounts are longer and more elaborate, and are committed to memory. There is consensus that financial information has top priority, followed by primary email accounts. Interestingly, participants who considered Facebook to be a form of email communication said it was important. Those who saw Facebook as a social tool deemed it unimportant. For those who had several email accounts, primary accounts used for formal communication are perceived to contain more sensitive information than secondary accounts used for personal messages. Participants classified "unimportant" accounts as sites that do not request personal information and accounts that are accessed only occasionally.

These types of accounts include entertainment and gaming sites, and forums. Participants perceive these accounts to contain very few assets and therefore, are unlikely targets for hackers.

Users' definition of a "good" password is a long password with a mix of different types of characters. Users justify passwords such as "P—a—s—s—w—0—r—d" as strong based on the length and types of characters, and whether it would be easy for humans to guess. Passwords associated with personal information are generally considered to be "bad" because attackers could target them and uncover this information. However, users included only the most obvious personal information like birth date, place of birth, current phone numbers, and information associated with immediate family and close friends. Participants considered outdated information to be personal secrets that are not available to the public, and therefore safe to use as passwords.

Some users created weak passwords because they felt the benefit to attackers from breaking into their accounts is extremely low. This belief that attackers only target wealthy and famous people coincides with Wash's "big fish" model [103]. In some instances, even high-value accounts are considered less important when they have few assets. For example, an online banking account is perceived as low value if it contains little money. There would be little motivation for users with this mental model to make extra effort to use strong passwords because they feel they have nothing to lose.

### 5.3.3 Eye-Tracking Results

Through eye-tracking measurements, we evaluated how users' attention was divided, reading times, and fixation patterns to gain insights into the possible connection between users' attention and their comprehension of the content.

#### Path and pattern of fixation

In comics, graphics take up much more space on the page than text, but text attracts attention before graphics. In our comic, headings and text blocks get eye fixations first. The only exception is if a graphic takes up most of the real-estate on the page. Interestingly, text that is graphically rendered as typographic elements attracts the

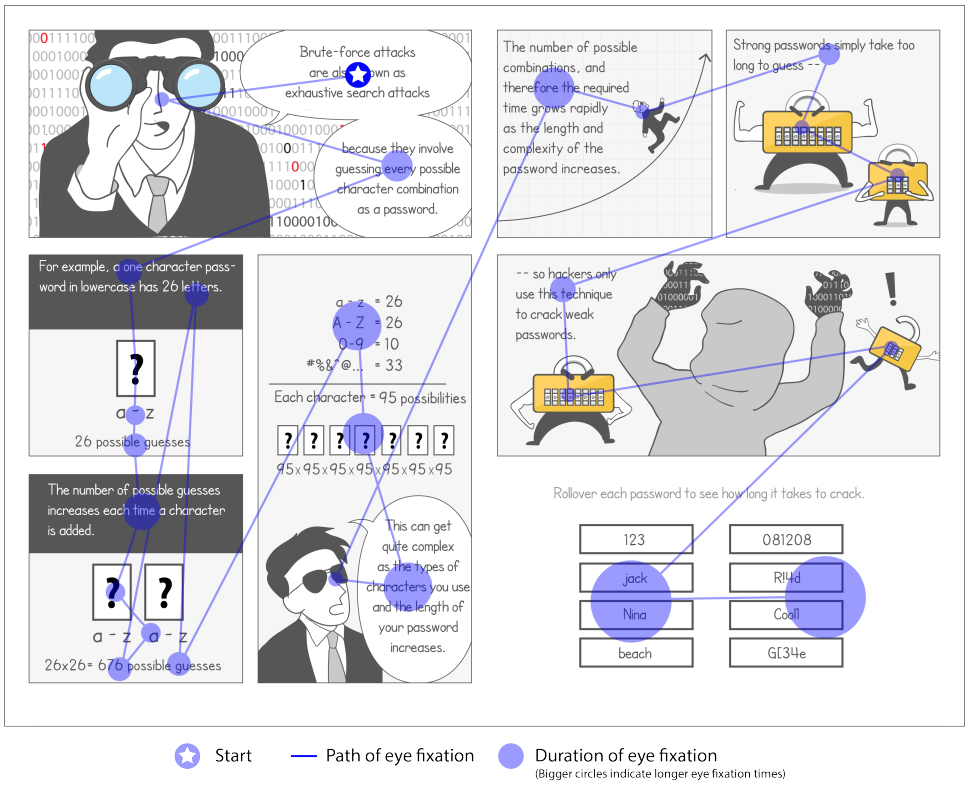



Figure 5.8: Eye-tracking for page 6 of the password comic

most eye fixations. For example, on page 10 of the comic, the password "abc" is illustrated as personified characters with googly eyes holding hands (see figure 5.9). On this page, participants spent the most time looking at this graphic.

The path of fixation starts with headings, text blocks, and then graphics. After a text block is read, users' eyes move to the nearest graphic. Images typically get eye fixation for $\leq$ 1 second between frames. We observed a consistent back and forth reading pattern of text and images between participants. Our observations also show that some participants re-read text after looking at the images. This re-viewing behaviour suggest deeper comprehension of text after looking at the accompanied images. Figure 5.8 shows an example of one participant's gaze pattern for page 6 of the comic. We obtained this data from the original screen recording, and output it as an image using graphic software. This participant spent a total of 101 seconds on the page. We choose this particular result as an example because it represents a common reading pattern we observed for this page. Page 6 also has interactive

elements, displayed at the lower right of figure 5.8. These are simple rollovers that reveal the amount of time it takes to crack each password. Blues lines in figure 5.8 represent the reading path, and blue dots represent the time spent on each fixation point. Larger dots represent longer fixation times. The data shows the participant spent much longer looking at the password rollovers. Most participants moused-over all password examples on this page at least once. We also observed back-tracking behaviour for 4 participants. These participants reviewed contents on previously read frames or pages after looking at an image or interactive example. This behaviour again suggests deeper comprehension of the content.

Participants generally focused more on characters' faces. Eyes especially drew attention. We noticed that on page 10, the example password "abc" received longer eye fixations than "Ae8%!" (refer to figure 5.4 for a screenshot). Both typographic images have personified characteristics, but the "abc" graphic included eyes. We did not find that the sporadic use of colour affected users' attention. However, circular objects drew eye fixation, especially when they are highlighted with colour. We did not find any major differences in reading patterns between non-comic readers and participants who read comics for leisure.

| Page # | 1 | 2 | 3 | 4 | 5* | 6* | 7 | 8* | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Time (s) | 37 | 53 | 58 | 45 | 104 | 101 | 91 | 76 | 89 | 69 | 87 | 52 | 34 |

Table 5.4: Mean time in seconds spent on each page of the password comic, excluding the mini-game. Pages denoted with "*" contain interactive elements

### Time Spent Looking at Display Elements

Participants spent an average of 9 minutes interacting with the comic. Average viewing times per page varied from 34 seconds to 104 seconds. Table 5.4 shows the average time participants spent on each page of the comic. Pages 5, 6, and 8 contain interactivity. Our results show that participants spent as much as 60% longer on interactive pages. For instance, participants spent on average 104 seconds on page 5, while the first page of the comic took on average 37 seconds to read. On occasions where the interactive elements reveal cause-effect relationships, participants moused over objects more than twice to make comparisons of the two states.

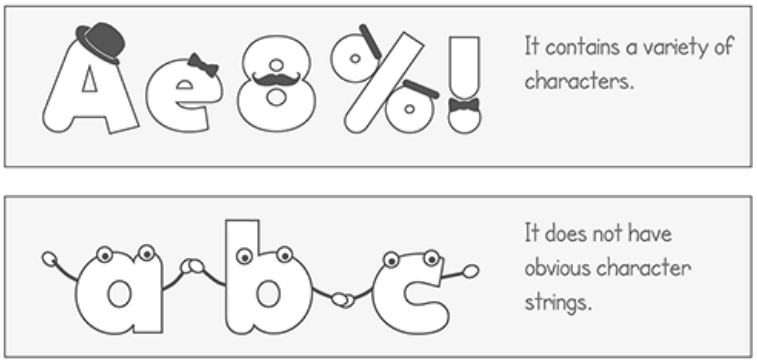



Figure 5.9: Explanation of what constitutes a good password. Introduced on page 10 of the password comic

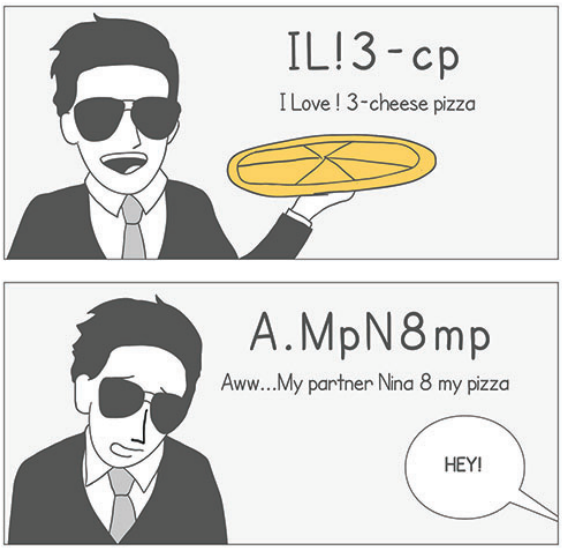



Figure 5.10: Passphrase examples. Introduced on page 11 of the password comic

| Self assessed password strength | Changed passwords? | Use Pass-phrase in the future? | User ID | Participants' Reasons for changing OR not changing passwords |
|---|---|---|---|---|
| Weak | Yes | Yes | C-02 | It was powerful enough to move me forward |
| | Yes | Yes | C-04 | Different methods to crack impressed me |
| | Yes | Yes | C-09 | My passwords are not as good as I thought |
| | Yes | Yes | C-12 | Time it takes to crack short passwords is scary |
| | No | Yes | C-13 | Laziness |
| Moderate | No | Yes | C-05 | Would not change without prompting |
| | No | Yes | C-01 | Accounts have never been hacked |
| | No | Maybe | C-10 | Too busy |
| | No | Yes | C-11 | I considered it, but haven't had time |
| Strong | No | Yes | C-03 | My current passwords are strong |
| | No | Yes | C-06 | My current passwords are strong |
| | No | No | C-07 | My current passwords are strong |
| | No | No | C-08 | My current passwords are strong |

Figure 5.11: Summary of learning outcomes for the password comic eye-tracking study

For static examples, participants also spent more time looking at the graphics. For instance, page 11 teaches users how to use the passphrase strategy. Participants spent as much as 6 seconds looking at the example "IL!3-cp" made from the passphrase "I love ! 3-cheese pizza", and up to 19 seconds looking at the example "A.MpN8mp" made from the passphrase "Aww...my partner Nina 8 my pizza" (Refer to figure 5.10 for a screenshot). The behaviours observed support prior findings that text explanations complemented by visuals could help to facilitate better comprehension [54].

In summary, we observed several reading behaviours in the eye-tracking experiment that suggest image and text pairings help to facilitate transfer of knowledge and increase engagement in the content.

- Participants' eye fixations jumped back and forth between text and images.
- Participants prolonged eye-fixations on visual examples.
- Participants prolonged eye-fixations on interactive elements.
- Participants exhibited back-tracking reading behaviour.

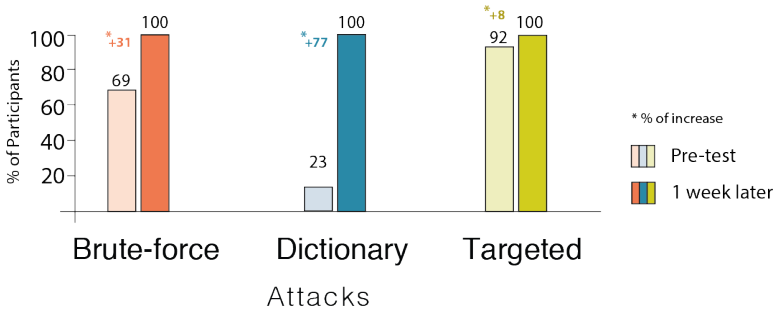



Figure 5.12: Participants' ability to describe how password guessing attacks work in the pre-interview and one-week later interview

### 5.3.4 Learning Outcomes

Participants returned one week later for a short followup interview. We asked them whether they changed their passwords. We grouped participants' responses based on their self-evaluated password strength. Our results show that 4 out of 5 participants with weak passwords changed them at home after the initial learning session. All 4 participants used the passphrase strategy to create their new passwords. 8 participants, who self-assessed their passwords as strong or moderately strong, did not change their passwords. These respondents felt that they were already maintaining good passwords for high-value accounts, and were not motivated to change other passwords. 85% of our study participants said they would use the passphrase strategy in the future. Please see figure 5.11 for a result summary. As with our earlier studies, we asked participants to recall and describe how password guessing attacks work to assess information retention. All participants were able to identify and describe brute-force, dictionary, and targeted attacks (see figure 5.12). The interview results are consistent with our previous questionnaire results, where we identified that most participants have a poor prior understanding of brute-force and dictionary attacks. Participants had the most trouble identifying dictionary attacks from both studies prior to learning, but this improved dramatically after viewing the comic.

### 5.3.5 Limitations of the Eye-Tracking Experiment

In our experiment, users gave us their full visual attention to read the comic. We did not find users skimming or skipping content. In fact, some users read certain

sections more than once. However, there are several limitations to eye-tracking in the lab environment. The most obvious is that during the calibration stage, users were told that their gaze is tracked while they read the comic. This could have influenced participants' natural reading behaviour. Some might felt obligated to read the whole comic, even though they were told to interact with the comic in any way they like. In real life, users might not dedicate as much time to reading the comic. When inquired about this afterwards, users suggested that it would be appropriate to present the comic as a tutorial at the account sign-up stage, or include it in the password advice sections of websites. Participants commented that they would much rather read the information in comic format than from text documents, which is the typical format available to users.

## 5.4 Summary

In this chapter, we presented the user study results evaluating our prototype designs that teach users about password guessing attacks. Three infographic posters and a text condition were evaluated based on their effectiveness, usefulness, memorability, and persuasiveness. We followed up with participants one week later through a emailed online questionnaire to assess learning outcomes and retention. Next, we evaluated the password comic following a similar methodology and reported the results. To gain a perspective of users' mental models and how the interactive comic is read and processed cognitively, we conducted one-on-one interviews and eye-tracking measurements. We later followed up with participants in an in-lab interview one week. Both studies showed promising results that our prototypes are effective teaching tools to help users develop an understanding of the threats. In the next chapter, we report our findings for another set of prototypes designed to teach users about antivirus protection.

# Chapter 6

# Improving Mental Models of Antivirus Protection

We repeated the previous methodology and conducted two between-subject user studies with a total of 56 participants to evaluate the prototypes we developed for teaching users about antivirus protection. Some minor differences exist between the two studies. For clarification, we outline the differences in the antivirus study design.

## 6.1 Antivirus Infographics User Study

### 6.1.1 Study Design

A user study was conducted to evaluate the two antivirus infographics with corresponding metaphors and one text-only condition striped of metaphors and images. We will refer to each infographic by the metaphor it presents: *"Surveillance"* for infographic A, and *"Medical"* for infographic B. The text condition will be referred to as "*Text*". The two infographics were presented to participants on posters measuring $20 \times 30$ inches each. In the text condition, we combined pieces of information from three resources to closely match the information to our infographics (Appendix B.2). To describe how antivirus works, we used the first two paragraphs of Wikipedia's description of antivirus software [106], which includes brief explanations of signature and heuristic detection methods. For the tips and myths section, we used comparable online resources from Logical PC solutions [68] and a security blog [98]. We use 4 myths verbatim from Logical PC Solutions, and 2 myths from the security blog to match the myths presented in our infographics. We presented the information on a letter size printout, in 12pt font. A between-subject design was used to assess which condition best facilitates learning about the subject. Testing was conducted through one-on-one sessions with the experimenter. The study was reviewed and approved by the Carleton University Research Ethics Board.

The independent variable in the study was the visual communication form of infographics. We wish to study whether infographics produce a more positive learning experience, and significantly increase knowledge transfer and retention compared to the text-only condition. As explained above, the three study conditions include two graphical conditions: *"Surveillance"* infographic, *"Medical"* infographic, and a baseline condition of plain text that contains no graphics and metaphors. The dependent variables were participants' evaluations of the prototypes based on the learning experience. Participants completed a online evaluation questionnaire that consisted of Likert scale questions. They gave ratings to statements pertaining their perception of the prototype's effectiveness and the learning experience immediately after viewing a assigned infographic or text condition. One week later, participants completed a followup questionnaire to assess whether knowledge about password guessing attacks significantly changed before and one week after viewing a prototype.

Our hypotheses were:

1. The teaching media of the two infographic conditions will be perceived as more effective at educating users about antivirus protection than the text-only approach.

2. Information visualized in the two infographic conditions will be perceived as more useful at conveying antivirus protection than text-only information.

3. Advice from the two graphical conditions will be perceived as more persuasive at convincing users to update antivirus software than text-only advice.

4. Information presented in the two infographic conditions will be perceived as easier to remember than text-only.

5. Knowledge about antivirus protection will increase one week after viewing the two infographic conditions, and no significant increase for the text-only condition.

We used non-parametric Kruskal-Wallis and Mann-Whitney U significance tests to analyze participants' Likert scale evaluations of the prototypes, based on participants' perceptions of the prototypes' effectiveness, usefulness, persuasiveness to

change passwords, and memorability. McNemar significance tests were used to assess whether knowledge about the antivirus protection significantly changed before and one week after the experiment.

### 6.1.2 Materials

**Pretest questionnaire:** Before prototype viewing, we gave participants a pretest questionnaire to gain a base understanding of their current knowledge and behaviour. Specifically, we asked about antivirus management, malware, and how antivirus works.

**Demographic questionnaire:** The demographic questionnaire collected standard demographic information about the participants, such as age, gender, education, and background.

**Prototype viewing:** Participants were told that they could take as much time as they want to view the prototype. Each infographic took on average 2 minutes to read. The text condition took on average 4 minutes to read. The experimenter noted immediate reactions from the participant. Afterwards, we conducted a brief interview with each person to openly discuss their opinions of the prototype. Participants were encouraged to be honest and point out if there is anything difficult to understand or confusing about the concepts. The experimenter took notes of the comments made by the participant, and any misunderstandings of the metaphors, layouts, and other graphical elements on the infographics, and comments about the information presented in the text condition.

**Post-viewing questionnaire:** After prototype viewing, participants were asked to evaluate the prototype in a questionnaire consisted of 19 Likert scale questions, on a scale of 1 (most negative) to 6 (most positive). Participants were asked to give a scaled rating to each statement about the prototype. We randomly reversed the direction of some questions to avoid bias.

**One-week follow-up questionnaire:** Participants were emailed a link to an online follow-up questionnaire one week after their scheduled lab session. The purpose of the questionnaire was to assess information retention. We intended to compare the results to the pretest questionnaire to evaluate if there are improvements in users'

understanding. We included several questions verbatim from the pretest questionnaire in the follow-up. Users were first asked to describe in their own words how antivirus software works, followed by 7 true or false questions surrounding "myths" about virus prevention. This enabled us to compare answers from the two occasions.

### 6.1.3 Participants

40 participants were recruited from Carleton University, through posters, an email newsletter, and an email contact list of volunteers. 15 participants were randomly assigned to one of two infographic prototypes, and 10 participants were randomly assigned to a plain text condition. Each participant was given a $10 honorarium.

During the study session, participants first completed a demographic questionnaire. 21 undergraduate students, 7 graduate students, and 12 university staff participated in the study. The mean age was 30 years, with 19 male, and 21 female. Participants had diverse academic backgrounds in the sciences (9), social science (9), business (3), arts (9), and engineering (8). 2 participants who were university staff members did not provide previous academic backgrounds.

Secondly, participants completed a pretest questionnaire about their current knowledge and perceptions of antivirus software, types of malware, and malware prevention. Participants' self-rated their knowledge about how antivirus software works on a Likert-scale of 6, where 1 is very low knowledge, and 6 is expert knowledge. 15 participants gave self-ratings between 1 and 2, 18 participants gave ratings between 4 and 5, and 5 participants gave a rating of 5. There were no ratings above 5, and 2 participants did not give a self rating. The participants were assigned to one of the three condition randomly. The average knowledge between conditions are 3.4 for *Surveillance*, 2.7 for *Medical*, and 2 for *Text*. Self evaluations show that participants in the *Surveillance* group considered themselves to be more knowledgeable about how antivirus software works than the two other conditions. This is consistent with our follow-up findings, where participants' learning outcomes increased in proportion to their prior knowledge. There were 9 Macintosh users and 31 Windows users for the primary computer used. The majority of participants (83%) considered themselves to be visual learners.

Out of the 40 participant recruited, 2 did not have antivirus software installed. When asked about the frequency of updates for the 38 participants who had an antivirus, 19 said their antivirus is set on "automatic" updates, with no specification of the frequency. Only 3 participants updated daily, and another 3 updated weekly. The rest updated somewhere between 1 month to 1 year. For renewing antivirus subscriptions, more than half of the participants (61%) with antivirus installed had either expired subscriptions that are more than 2 years old, or do not know whether their subscription has been renewed.

We asked participants to rank which operating system they thought to be the most secure. A common myth among users is that Macs are immune to viruses [103]. The perceptions among our participants support this misconception, where Windows is ranked by 55% of the participants to be the least secure, followed by Linux (38%) and only 5% for Macs.

A section of our education prototypes helps to correct numerous misconceptions regarding virus prevention, including the following myths:

- Viruses can damage your computer's hardware.
- Running multiple Antivirus programs on the same computer is beneficial.
- Having an Antivirus is enough to be secure.
- I can't get a virus if I'm not connected to the Internet
- I can't get a virus if I don't download anything.
- I can't get a virus if I don't visit "shady" sites, such as porn, gambling, or file sharing websites.
- Mac is far more secure than Windows

Participants from our study hold the strongest misconceptions that viruses can damage computer's hardware (50%), followed by Macs are more secure than Windows (38%), and having multiple antivirus is beneficial (25%).

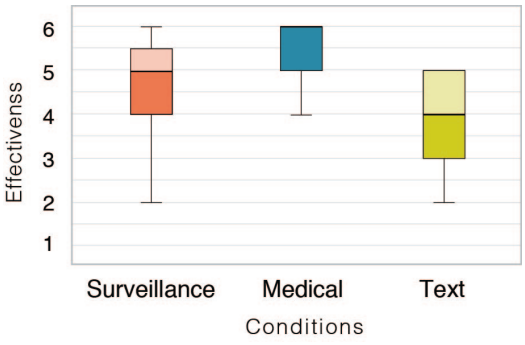



Figure 6.1: Antivirus infographics: Likert scale responses assessing the *effectiveness of the prototype at conveying information* (6 = most effective, 1 = least effective)

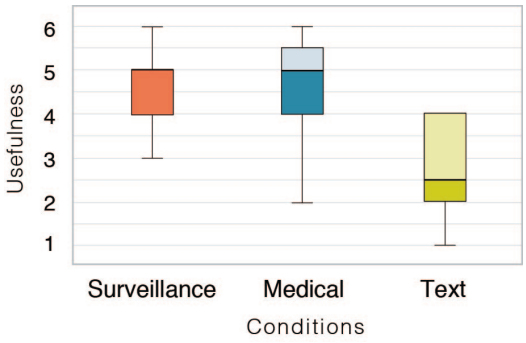



Figure 6.2: Antivirus infographics: Likert scale responses assessing the *usefulness of the presented information* (6 = most useful, 1 = least useful)

### 6.1.4 Post-Viewing Questionnaire Results and Feedback

Participants completed an evaluation questionnaire regarding the prototype and learning experience immediately after viewing. We highlight four particular areas of user evaluation and comments: effectiveness of the visualization, usefulness of the information, persuasiveness to maintain an up-to-date antivirus, and memorability of the information. All Likert-scale data is presented positively for readability, with 6 = most positive and 1 = least positive. To analyze the Likert scale responses, we used the non-parametric Kruskal-Wallis and Mann-Whitney significance tests to evaluate whether any differences were apparent between the three conditions. In all cases, $p < 0.05$ is considered significant.

**Effectiveness for Learning:** Participants gave a Likert-scale rating for the effectiveness of the prototype they saw at teaching them about antivirus protection. The material was either presented them visually as one of the two infographic posters or a text-only document. Figure 6.1 shows participants' responses for the effectiveness of the two infographics and the text-only condition. *Surveillance* (mean 4.8) and *Medical* (mean 5.3) received higher ratings than *Text* (mean 3.3). A Kruskal-Wallis test showed a statistically significant difference between perceived effectiveness of the three conditions ($H(3) = 17.85$ with $p < 0.001$). To determine where the differences lay, Mann-Whitney tests with a Bonferroni corrected p-value of ($p < 0.05/2 = 0.25$)

was used. Participants perceived both infographics to be more effective than the text-only condition: ($U = 18, p = 0.001, r = -0.648$) for *Surveillance* and *Text*, and ($U = 6.5, p < 0.001, r = -0.783$) for *Medical* and *Text*. There is no statistical difference between *Surveillance* and *Medical*. The results suggest that participants perceive visual communication through infographics more effective than learning from plain text.

Participants found the metaphor used in the *Medical* infographic to be the most intuitive. A participant said "If you just portray computers, people may not understand what it means because it's technical. Everybody understand how germs and viruses can affect the human body, so they can make meaningful comparisons with how computer viruses work." The term "virus" is widely used other than in computer security. Therefore, participants found the Medical concept "familiar" and "relatable." Participants also pointed out that presenting a computer topic directly might not interest people, but disguising it as a health issue might prompt people to read it. This is also true for the *Surveillance* infographic. A participant said "I might've not known that it's about antivirus because of the graphics, but it could help get people's attention if they are not interested in computer security." Participants who viewed the *Surveillance* infographic found the bug imagery captures how viruses can "creep in without you noticing it." Participants thought illustrations of the house, fence, and security cameras offered a simple understanding of the detection purposes of antivirus software.

**Usefulness of the information:** On each infographic, we focused on providing participants with actionable advice on how to stay safe, along with correcting common myths surrounding each advice. Similarly, the available online resources we used in the text condition also help users to correct common myths, but are not always paired with actionable advice. When comparing the three conditions for participants' responses for usefulness of the information (See figure 6.2), we found a highly significant difference: $H(3) = 10.394$ with $p < 0.004$. Mann-Whitney tests show a statistic significance between *Surveillance* and *Text* ($U = 27, p = 0.013, r = -0.503$), and *Medical* and *Text* ($U = 20, p = 0.001, r = -0.627$), but not between *Surveillance* and *Medical*. This suggests that participants perceived the information shown on both

infographics to be more useful than the information shown in the text condition. Interestingly, the infographics provided the same myths as the text condition. This result may indicate that when security information is paired with actionable advice, participants perceive them to be more useful. Participants commented that the myths "Macs are far more secure than PCs," and "Having multiple antivirus programs are beneficial" were most useful to help them correct misconceptions.

**Likelihood to update antivirus as a result of learning:** The questionnaire asked participants whether the information has convinced them to maintain an up-to-date antivirus. The results suggest the infographics have more persuasive power to influence user behaviour than information written in plain text (See Figure 6.3) We found a statistically significant difference between the infographics and the text condition. Kruskal-Wallis test showed $H(3) = 6.352$ with $p < 0.039$. Mann-Whitney tests found that participants thought the *Medical* infographic is more persuasive than *Text* ($U = 30.5, p = 0.019, r = -0.47$). A participant commented "comparing the computer with the human body is vivid, and makes it easy to consider the importance to protect our computer from viruses. It also makes it easy to draw parallels around how computer viruses are spread, from host to host." We did not find a statistically significant difference between *Surveillance* and *Text*, or *Surveillance* and *Medical* infographics. For the *Surveillance* infographic, participants said that bugs are recognizable imagery for viruses, and the surveillance cameras are a well understood concept of physical security. However, some participants said they associate home security more vividly with burglars. Bugs seem "less threatening" than burglars in the context of a "home invasion."

**Likelihood to remember the information:** Participants evaluated how likely they were to remember the information (See Figure 6.4) . Participants' feedback suggest that they perceive content from the infographic posters easier to remember than plain text, but Kruskal-Wallis test showed no significant statistical difference between the three conditions, $H(3) = 5.68$ with $p < 0.056$. A participant said, "graphics would get more attention and draw more people in. It is also easier to commit to memory when there are graphical parallels you can draw upon." Another said, "I definitely think it would be a lot more interesting to read, which would

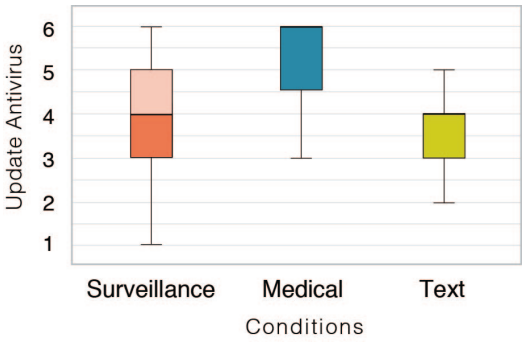



Figure 6.3: Antivirus infographics: Likert scale responses assessing the *likelihood to update antivirus* (6 = most likely, 1 = least likely)

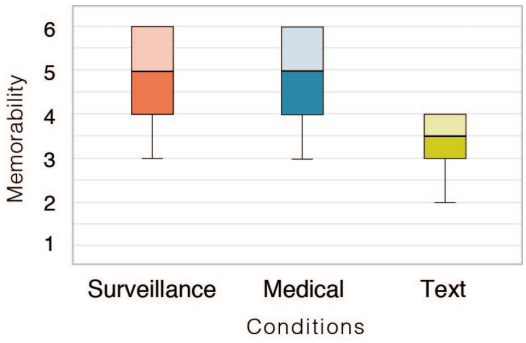



Figure 6.4: Antivirus infographics: Likert scale responses assessing *how likely participants will remember the information* (6 = most likely, 1 = least likely)

subsequently make the info more memorable. Text can be very daunting to read, so a more visually interesting method of display with pictures and colours would be a lot more useful." Participants also commented that they would more likely to remember the main take-away message from the infographic posters, which is to keep their antivirus up-to-date, even if they cannot remember the textual details.

### 6.1.5 Information Retention

All three conditions taught users how antivirus software works and why they need to perform regular updates. Prior to viewing the study material, we gave participants the opportunity to describe, in their own words, how they thought antivirus software works to detect malware. For comparison, this question was also asked verbatim one week later in an emailed online questionnaire. We received 40 completed responses in the pretest, and 38 completed responses one week later. Blank answers were considered as "I don't know."

| | |
|---|---|
| Surveillance | $(\chi 2(1) = 8.182, p = 0.5)$ |
| Medical | $(\chi 2(1) = 1.224, p = 0.031)$ |
| Text | $(\chi 2(1) = 10.313, p = 1)$ |

Table 6.1: Antivirus infographics: statistics comparing participants' ability to describe attacks on the pretest and one week later

We evaluated the answers based on participants' ability describe the fundamental idea of how antivirus software detects malware. An example of a correct answer is "The antivirus software has a library of suspect code that is used to find matches in the code of files being scanned." The goal is not to evaluate users' ability to describe technical aspects of detection methods, but to identify their basic understanding of how antivirus works.

In the pretest, a total of 13 out of 40 (33%) participants held correct mental models of how antivirus works. The rest offered descriptions of the general purpose of antivirus and the scanning process, with no insights on how antivirus can achieve these tasks. These include protecting users against viruses, alerting the user after the scanning process, and help users to eliminate viruses from computers. Since participants were assigned to a condition randomly, the number of correct answers between conditions varies in the pre-test. 13 participants with correct mental models were distributed across the three conditions as follows: 60% (9/15 participants) for *Surveillance*, 7% (1/15 participants) for *Medical*, and 30% (3/10 participants) for *Text*. One week later, we evaluated the percentage of increase for each condition in participants' ability to describe how antivirus works. Please refer to figure 6.5 for a summary of pre-test versus one-week later results.

We conducted McNemar tests to analyze participants' ability to describe how antivirus software detect malware in the pretest compared to one week later. 60% of participants from the *Surveillance* condition were able to describe how antivirus works in the pretest questionnaire, compared to 7% for *Medical* and 30% for *Text*. We found a 25% increase for the *Surveillance* condition one-week after learning, 40% for *Medical*, compared to only 10% for *Text*. The results suggest that our infographics prototypes help users learn and remember the information better than text-only descriptions, especially when prior knowledge is low. Statistically, there is a significant increase in knowledge for *Medical* ($\chi 2(1) = 1.224, p = 0.031$), but not for *Surveillance* or *Text*.

## 6.2 Antivirus Comic User Study

We designed a second educational comic to help users' build mental models of how antivirus software works, and best practices for malware protection. The antivirus

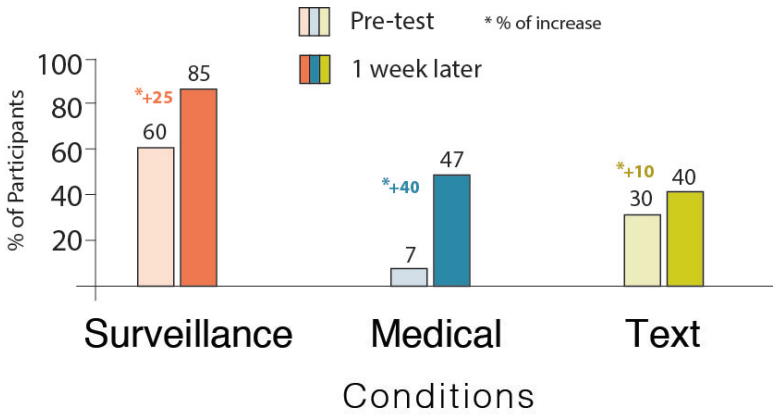



Figure 6.5: Antivirus infographics: summary of participants' ability to describe how antivirus software works before and after viewing the instructional material

comic further develops the narrative and characters introduced in the password comic. It is 10 pages long, including two self-test mini games. We described the comic design in detail in section 4.3. Reading times of the comic varied from 5 to 8 minutes, depending on each participants' individual reading speed.

### 6.2.1 Study Design

This was a two-part user study with sessions conducted one-week apart to assess users' current knowledge and the learning outcome of the comic prototype one-week later. Participants first answered a demographic questionnaire, followed by a 20 minute one-on-one semi-structured interview with the experimenter. The questionnaire gave a general assessment of participants' demographic and self evaluations of current knowledge about the topic. The purpose is to gain an in-depth understanding of users' mental models for using antivirus software, as well as perceptions of malware. The interviews allowed us to dig deeper into the user perceptions we explored in the infographic study. Participants viewed the comic prototype on a laptop computer. After viewing the comic, participants completed a post-viewing questionnaire similar to the one used in the antivirus infographic study. Participants returned to our lab one week later for the second follow-up interview. The purpose of the follow-up interview is to assess retention of the comic and whether learning the information helped participants build mental models. We also inquired about whether reading

| DATA EXTRACT | CODES | THEME |
|---|---|---|
| "Like a bug, or a worm. Just some type of pest that's invasive that might get inside your house or something. So if I were to visualize it it's something that got inside my computer that's eating things up." | • Viruses are invasive.<br>• Like bugs that get inside of the house.<br>• They "eat" up my computer. | Viruses are like pests |
| "It's annoying. A bug? I would connect it with bed bugs. Like even if you want to kill it you can't destroy it. Like it's tough." | • Viruses are annoying.<br>• Viruses are difficult to get rid off (like bed bugs). | |
| "I don't know it kind of just takes on a life of its own, that's kind of how I always thought. Its like a little worm." | • Viruses have a life of it's own.<br>• Viruses are like a living worm. | |
| "I think about a worm moving around." | • Viruses are like a living worm that moves around. | |
| "Something like a worm I think? Something that pops out. Your screen turns red or black. I don't know something not what you expect I perceive it as a virus." | • A worm that crashes the computer. | |
| "Little bugs that's gotten in there." | • Small bugs that got through the cracks. | |

Table 6.2: Password interview data analysis: sample data extracts with corresponding codes and theme.

the comic prompted changes in security behaviour within the period of one week. The follow-up interview took approximately 15 minutes.

16 two-part interviews were audio recorded and transcribed verbatim by the experimenter. We used the same data analysis methodology as described in Chapter 5, section 5.3.1. To recap, open coding [97] was used to look for emergent themes.

We then applied the codes systematically to the entire data set, organizing data relevant to each code. Next, we analyzed and merged similar codes into potential themes. Lastly, we looked for cause and effect relationships between the themes and the overall story the analysis tells in relation to users' mental models. Table 6.2 shows examples of chucks of interview data and their corresponding codes used to find the theme "viruses are like pests."

### 6.2.2 Participants

We recruited 16 participants for the antivirus comic study. On a scale of 1 to 6 (1 - novice, 6 - expert) the average self-rating for prior experience with antivirus software was 2. The majority of the participants were Windows users, with the exception of one Mac user. The mean age was 22 years, and there were 11 female and 5 male participants. All participants were students from our university, with 13 undergraduate and 3 graduate students.

### 6.2.3 Mental Models of Malware and Antivirus Software

From the pre-test interviews and qualitative analysis, we identified that users have several misconceptions surrounding malware and antivirus software as a consequence of poor mental models. They are:

#### "Viruses" are more harmful than "malware"

Among end-users, "virus" is a general term widely used to describe various types of malware. We were interested to find whether participants realize that computer viruses are a type of malware. Interestingly, when asked about the term "virus" and "malware", half of the participants perceived them as distinct threats. None of the participants were able to identity that a virus is a class of malware. Participants' descriptions of harm caused by "malware" and "virus" varies in degrees of seriousness (see Figure 6.6), where "malware" was perceived to be less serious than "virus." Damages from "malware" were described to cause minor irritation and annoyance, such as ads popping up and user information getting stolen. "Virus" on the other hand,

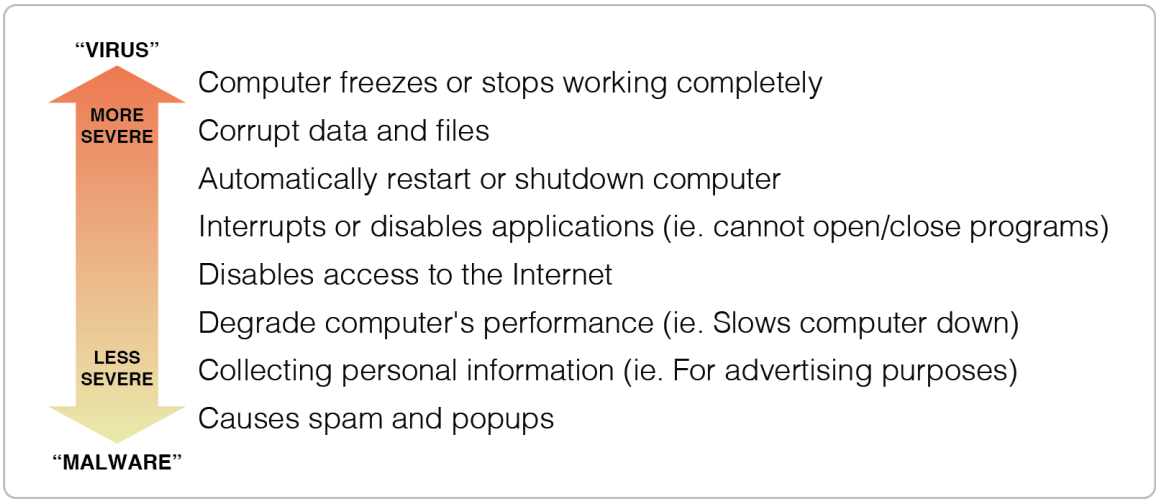



Figure 6.6: Pretest perception of harm caused by viruses and other types of malware

causes more serious damage that could be devastating for users. These may include corrupting data, and compromising or entirely disabling systems and networks.

Half of our participants believe that "virus" is more serious than "malware". Figure 6.6 shows a summary of harm described by participants, organized in order of how serious they perceive them to be. Types of harm near the top of the list were perceived to be more severe, and more likely to be caused by a "virus." Participants perceived types of harm caused by "malware" less severe. AC9 said, "to me the word virus just sounds like it could be worse. Malware kind of sounds like it's just a pain, like something that is added-on." AC2 associated malware to spam: "From what I heard, a virus can basically...sometimes it can prevent you from opening your files. Compared to malware...I usually call that spam." Many participants with this perception believe that malware does not cause harm directly to the computer, but instead the purpose is to disturb users. For instance, AC1 said, "Virus is more dangerous. It damages your whole computer. Malware just distracts you." Only one participant (AC5) believed malware is more dangerous than a virus.

5 participants (31%) perceived "virus" and "malware" to be nearly the same thing, but were unable to explain exactly what malware is. These participants generally feel that both things are "bad" and should be avoided. For example AC15 said, "To me they aren't really different. To me it's a lament basically. They are all things that I

| Perception | # of Participants |
|---|---|
| Virus is more harmful than malware: | 8 |
| Malware is more harmful than virus: | 1 |
| Both are equally harmful: | 5 |
| Don't know: | 2 |

Table 6.3: Pretest summary of perceptions of "virus" and "malware"

don't want to have. They are all things that I would worry about somehow wrecking my experience with the computer. So whether they are officially classified as viruses or not, I treat them the same way. If someone said you have a virus, or you have malware, I say oh, dammit." 2 participants (12%) said they have no idea whether the term "virus" and "malware" would mean the same thing or are different. Please refer to table 6.3 for a summary of participants' perceptions.

### Malware: Virus, Trojan Horse, Worm, Adware, and Spyware

Participants were asked to describe each of the following malware: virus, trojan horse, worm, adware, and spyware. As mentioned earlier, "virus" is the popular term among end-users to describe different kinds of malware. When asked about how computer viruses differ from other types of malware, participants were unable to give clear answers. They described the general harm that can be caused by viruses, such as damaging files, programs, and the OS, but none were able to describe exactly how a virus can achieve those things. A good example is what AC12 said, "I would say a virus is software that doesn't do what you expect. It slows down your computer; messes up functions, and generally just make a mess of things."

Computer worms were generally perceived as the same thing as a virus. AC15 said, "I don't know if I'm familiar with that as a specific thing. So to me if I've heard of someone say computer worm, I would just think oh, do you mean a virus." Participants were not able to distinguish the difference between worms and viruses and how they propagate and spread.

Participants had an easier time describing how trojans work, especially for those who were familiar with the trojan horse in Greek mythology . Most participants were able to guess how trojans are spread based on mythology. For instance AC10

said, "I've heard of this one mainly because of mythology. It basically masks itself as one thing but there is something deadly inside." To most participants, trojans were a type of virus in disguise: "I guess the analogy of it is just being appearing as something but being something else, so maybe downloading a file and it's actually something else."

Adware and spyware sounded like familiar terms to some participants, but were perceived as types of "malware," mainly because of the perception that they cause annoyance rather than real harm to computer systems. A few participants also mentioned that the spelling of adware and spyware were similar to malware, so they perceive them as the same. Although most users admittedly to have heard of the terms before, few were able to describe exactly what they are. When participants offered explanations, adware was directly associated with "annoying popup ads". Spyware was described as "when someone can hack into your computer and see what you are doing," or to "steal your information."

### 6.2.4 Pictorial Metaphors: Visual Depictions of Malware and Antivirus

In the pretest interviews, we asked participants to describe types of imagery they associate with the term "virus" to better understand users' mental models of viruses and other types of malware. We were able to summarize user's description into four models. The first two models, *biology* and *pest* are descriptive of how one can get infected based on an understanding of how infectious diseases and pests spread. Participants who described *mechanical failures* or the *code* model offered more general explanations of the type of harm viruses can cause, or descriptions of the outcome of being infected. See table 6.4 for a summary of the results.

**Viruses are like pests:** 6 participants (38%) pictured viruses as some form of pest, like a bug or a worm. Participants imagined them to have "somehow got through the cracks" of a computer, much like how pest can slip through the cracks of a house to get inside. AC15 describes it as "a bug or a worm or some type of pest that's invasive that might get inside your house." Visually, the participant imagined a virus getting inside the computer and "eating things up." Viruses also "take on a life of its own... like a little worm." Malware were generally perceived to cause

| Visual Depiction | # of Participants |
|---|---|
| Pest | 6 |
| Biology | 4 |
| Mechanical | 4 |
| Codes | 2 |

Table 6.4: Pretest summary of visual depictions of viruses

annoyance but can range in severity depending on the type. Participants who hold the *pest* model perceived viruses to be difficult to remove. For example AC13 said "I would connect it with bed bugs. Like even if you want to kill it you can't destroy it." Several participants with this model believe that the only way to completely get rid of a virus is to reformat the hard drive.

**Viruses are like an infectious disease in a human body:** Another common virus imagery held by 4 participants (25%) is infectious viruses in living organisms. To visualize what viruses might look like, participants associate them with images of actual viruses under a microscope, such as AC12's description of a "sphere with the little bumps on it." Viruses can grow and take over the host. AC3 said, "I have no idea how it works on computers. Viruses seem like, from TV shows, cancer cells that just convert everything." Participants with this model imagine that computer viruses can be spread from host to host just like a real virus.

**Viruses cause computers to mechanically break down:** When asked about what types of imagery the term virus inflicts, 4 participants (25%) offered much more general descriptions. These participants' literally visualized computers breaking down and not working properly. Participants such as AC2 described that viruses can "basically damage my work and my computer," but were not able to specify how that can be achieved.

**Viruses are pieces of code:** 2 participants (12%) described viruses as pieces of codes or programs. Visually, the participants pictured viruses to look like binary codes. As AC14 described it, a virus is "some code, some program, 0101010, numbers."

| Perception | # of Participants |
|---|---|
| Inclusion Model | 5 |
| Exclusion Model | 6 |
| Risk Assessment Model | 2 |
| Don't know: | 3 |

Table 6.5: Pretest summary of mental models of how antivirus software works

### 6.2.5 Mental Models of How Antivirus Software Works

Prior to viewing the comic, we discovered that our users hold three types of mental models of how antivirus software works (See table 6.5). Only 2 participants (13%) were able to correctly describe signature-based or heuristic-based detection methods, and point out the need for updates to accommodate for new malware. 3 participants (19%) said they had no idea how the software works at all. The rest gave abstract descriptions of the scanning process within the software they own, such as the scan progress bar, alerts and prompts they receive through the antivirus software. We were able to group participants' perceptions into three basic models of how antivirus "catches" viruses. The *Inclusion Model* is closely related to how antivirus software actually works. The antivirus has a database of previously known viruses. When a file matches a known virus, antivirus alerts the user. In the *Exclusion Model*, participants believe antivirus somehow catalogues legitimate programs and exclude malicious ones. When a file does not match the antivirus' list of "good" programs, it flags it as a virus. In the *Risk Assessment Model*, a small number of participants believe that downloaded files are somehow linked to the source, and the antivirus tracks the origin of both legitimate and malicious files.

**Inclusion Model:** The *Inclusion Model* is held by 5 participants (31%). The model describes antivirus as a database that contains a library of known viruses. During the scanning process, the antivirus compares the file to its library of virus signatures. For example AC12 said, the antivirus has "a database of files categorized that are virus files, and checks to see if you got any on your computer, and if there's a match they will try to delete it or isolate it somehow." Another example by AC5 says "it has a database on it's own since it keeps updating itself. Each time it increases, it scans the computer and sees if there is any files that are the same, then it detects it

as a virus." These participants had a basic understanding that antivirus works with a library or database that needs to be updated to recognize new viruses.

**Exclusion Model:** The *Exclusion Model* also recognizes the existence of a database, but instead of storing a library of virus signatures, it stores a database of pre-approved legitimate files or programs. Some participants with this model imagined antivirus to work like a filter, where it separates legitimate files from unwanted malicious ones. Antivirus distinguishes the file by the code associated with it. If the file meets certain attribute recognized by the software, it is allowed to pass through. In other words, antivirus creates a filter that only lets the "good" content recognized by its database pass through. As AC15 described it "if I were to visualize it might be some kind of net and only certain shapes fit through, and the viruses are not shaped properly and that it catches them. Perhaps that shape has something to do with the data or code or something like that. That's how I would interpret it."

**Risk assessment model:** A small number of participants (12%) believe antivirus assesses the risk of files by tracing them back to their source. One participant believes antivirus scans and checks the risks of the site that he is downloading from. Another participant believes that there is an active link between files and their source, especially from peer-to-peer sharing sites. AC9 said, "it's still connected to a IP address. If you just download a file, the file is on your computer and that link is cut from where it came from, but if it was a peer-to-peer sharing site with a virus, it is still be connected to different computers. It's looking for atypical files." In short, the antivirus assesses the origin of the file and evaluates the risks. Once the user accepts the file and downloads it, the active link is cut.

### 6.2.6 User Perceptions of "Clean", "Quarantine", and "Delete"

Research in security warnings [12, 87] have found that security warning often fails to communicate to users what they should do in the presence of a risk. Antivirus software will generally give users three options when it encounters a virus-infected file: clean, quarantine, and delete. A mishap of selecting the wrong option can sometimes lead to frustrating and damaging outcomes, such as mistakenly deleting an entire program.

When antivirus "cleans" a file, it attempts to detach and remove the infection from the file. This action is best used for true viruses, where a legitimate file has been "infected" with a virus. By choosing to "clean" a file, the virus can be removed without having to delete the infected program. It would not be possible to "clean" some types of malware like worms, because they are standalone malicious programs. The quarantine option disables and removes the file to a safe location managed by the antivirus software, and is reversible if the file needs to be recovered later. In contrast, the delete option removes the file completely from the system.

During the interview, we asked participants to distinguish the difference between clean, quarantine, and delete. We found that users most often choose to "delete" when their antivirus prompts them to carry out an action. This is not surprising considering it is the most well understood option among our users. 13 participants (81%) thought delete is the most obvious and straightforward option. When asked about why they would choose to delete the infected file rather than to clean or quarantine it, the main reason participants gave was because they feel delete is the most effective solution. AC8 said, "I feel like quarantine wouldn't fix it. I feel like deleting it just gets rid of it the best. Cleaning it... stuff could be left." Participants also saw no reason to keep an infected file around and want to get it out of their computer as soon as possible. They responded by saying "what's the point of keep it there for a while" (AC4); "I usually say delete, just get it out of my computer" (AC1); "I don't want it there. It saves space I guess" (AC5). Most participants had no trouble identifing what delete is. However, 3 participants were unsure whether delete meant deleting the file or deleting the virus that is attached to the file.

Participant had a lot of trouble describing what "cleaning" can do. Only 38% were able to describe the effects of cleaning a file. Some had no idea how it works, while others gave varied answers like it "scans the whole system" (AC11), "track the virus down to its sender" (AC3), or "suggesting you to delete it" (AC13).

More than half of the participants (56%) were able to identify what "quarantine" does. AC15 said "I know what the word quarantine means, as though it's taken from here and remove it to here to be watched over, kept separate from the rest of the people or files." The participant assumed that antivirus would quarantine malicious

files the same way. However, a few participants believed that antivirus would only quarantine a file if it cannot delete it. AC12 said "I guess it would be for whatever reason the antivirus can't delete the file, maybe I don't know if it doesn't have access or user privilege, it's just trying to... I don't know how but prevent it from doing actual damage without actually deleting it." Others believed that quarantine, clean, and delete is a three-step process. Antivirus would proceed from quarantine to clean, then delete it if it has no other choice. This is described by AC10: "Quarantine would be segregating it off of it the network and off of everything and actually looking at it more carefully to see if they can clean it. If they can't detach it then delete it later."

### 6.2.7 Post-Viewing Questionnaire Results and Feedback

After the interview, participants viewed the antivirus comic prototype. We used same study protocol and questionnaires as the antivirus infographic study. We asked participants for immediate feedback after reading, and took notes of the comments. Participants then evaluated their experience in an online questionnaire. The questionnaire consisted of Likert-scale ratings from 1 to 6. The data is presented here positively for readability, where 6 = most positive and 1 = least positive.

The independent variable in the study was the visual communication form of our antivirus interactive comic. We wish to study whether our interactive comic produces an enjoyable learning experience, and positive effects on knowledge transfer and information retention one week later. The dependent variables were participants' evaluations of the prototypes based on the learning experience. Participants completed a online evaluation questionnaire that consisted of Likert scale questions. They gave ratings to statements pertaining their perception of the comic's effectiveness and the learning experience immediately after viewing the comic. One week later, participants completed a followup questionnaire to assess whether knowledge about password guessing attacks changed before and one week after viewing the comic.

Our hypotheses were:

1. The comic will be perceived as an effective teaching tool at educating users about antivirus protection.

2. Information visualized in the comic will be perceived as useful at conveying antivirus protection.

3. The comic will persuade users to update antivirus software.

4. Information presented in the comic will be perceived as easy to remember.

5. Knowledge about antivirus protection will increase one week after reading the comic.

As with the infographics, we report on four results from the Likert-scale questions: 1) effectiveness of visual learning, 2) usefulness of knowledge gained about AV, 3) likelihood to remember, and 4) persuasiveness to maintain an up-to-date antivirus. Figure 6.8 shows a box plot of the results.

**Effectiveness of visual learning:** There is consensus among our participants that presenting the information visually as an comic was easy to read and understand. Participants believed teaching about antivirus and virus prevention visually is an effective method to communicate about this topic. The average rating given by participants was 5.3. AC4 said, "If I came across security information and it takes me 30 minutes to read, I probably wouldn't read it. This was quick and easy." AC7 believed the content would be suitable for a lot of different age groups because comics are very popular. AC10 commented that the characters in the comic made the topic more relatable.

We used a medical theme to explain many of the antivirus protection concepts to users. Participants found the medical concept intuitive to understand. AC9 commented, "it's what first comes to mind when I think of a virus." In the comic narrative, we subtly alluded to the medical theme at the start of the comic, when "agent Jack" catches a cold, while "Hack" infects a network of computers with a computer virus (figure 6.7). Although a few participants did not get the analogy at the start, the repetitive use of the medical concept throughout the comic helped to reinforce the message.

Participants described the comic as "fun", "cute," and "pleasant" to read. Several participants wanted to share the information with family and friends, and asked


Figure 6.7: A portion of page 1 of the antivirus comic

whether it would be available online. Participants reported that they had a pleasurable experience reading the comic. The visual content and interactivity kept them entertained while they learned useful information.

**Usefulness of knowledge gained about AV Protection:** After reading the comic, most participants believed they gained useful knowledge about antivirus protection (Mean = 5.3). Participants thought the comic was most useful for them to clarify common "myths". AC4 said, I think I knew some of this information, but it helped to confirm my suspicious about the myths." Many antivirus and malware related terms sounded familiar to users. However, even though most participants have heard of the terms many times before, many initially could not describe what they mean. For example, when asked about types of malware in the pretest, many cannot describe the differences between them, even though most people heard of the terms before. After reading the comic, most participants were able to recognize the importance of updates. This suggests learning about how antivirus works could help users determine why regular updates are necessary.

**Likehood to remember:** Participants evaluated how likely they were to remember the information after some time has passed. The comic received a mean value of 5.3 for memorability. In the post interview, several participants used scenes from the comic to describe how antivirus software works, such as using a medical anology, describing virus signatures as "DNA" sequences, and referring to hackers as the

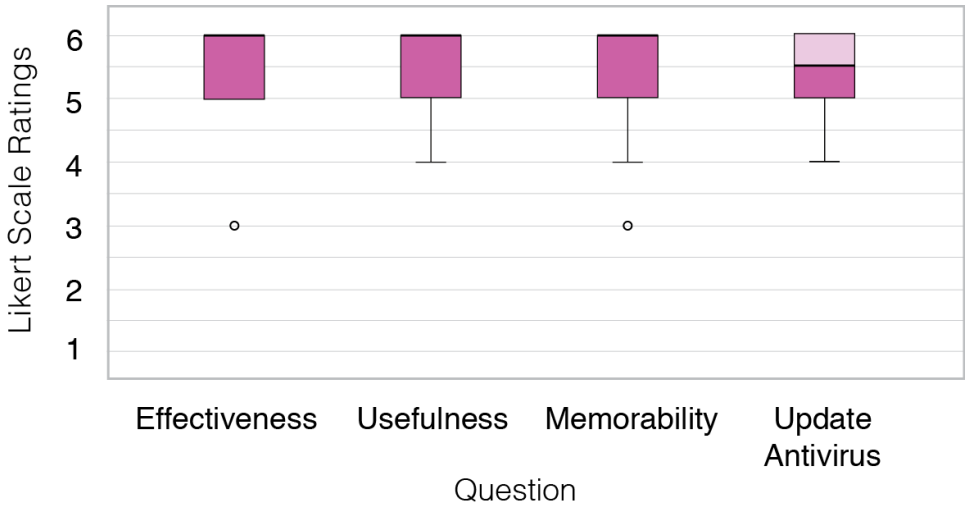



Figure 6.8: Antivirus comic: Likert scale responses for four questions (6 = most positive, 1 = least positive)

"villain."

Participants believed presenting the information as a comic had positive effects on how well they could remember the contents. For instance, AC11 said, "I might read the information but I wouldn't remember it normally, but I think I would remember what I read in the comic." The interactive nature of the comic could have also contributed to the memorability of the content. Several participants found the interactive elements useful to expand on what they have read. Several participants also provided positive feedback regarding the mini-games at the end of the comic. Participants said they helped to reinforce what they have just learned.

**Persuasiveness to maintain an up-to-date antivirus:** One question asked participants whether reading the comic has convinced them to maintain an up-to-date antivirus. We evaluate participants' actual behaviour from our follow-up results in the next section. In the mean time, the questionnaire assesses participants' perception of the persuasiveness of the comic. The average rating participants gave was 5.1. This is an encouraging result if the comic is able to affect user behaviour. Even though we cannot prove the actual efficacy of the comic at this stage of the study, participants' feedback suggests that the comic was at least able to heighten awareness about antivirus protection. Several participants expressed intent to take further

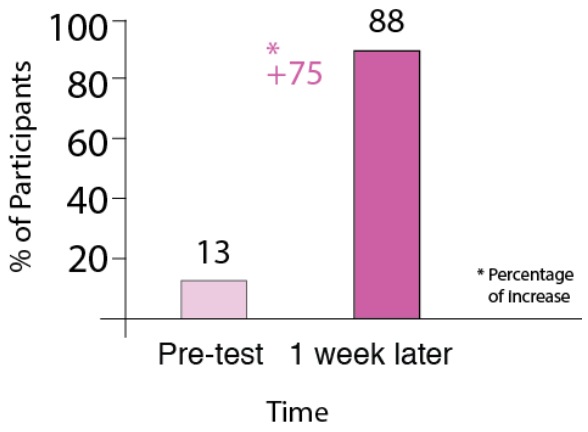



Figure 6.9: Antivirus comic: participants' ability to describe how antivirus works before and after viewing the instructional material

action after the study. For example, AC2 wanted to know why people create viruses and thinks she is going to look it up on her own. AC3 said he is going to check his antivirus setting when he gets home. AC11 and AC15 said they would look up more about different types of malware on their own time.

### 6.2.8 Learning Outcomes

The study participants returned to our lab one week later for an in-person follow-up interview. We asked participants to describe the various contents of the comic to assess information retention, as well as the effect of learning on user perception of computer security and influences on user behaviour.

In the pre-test interview, only 13% of our participants were able to correctly describe how antivirus works. We believe the lack of knowledge could have consequences on users' ability to properly manage their antivirus software. The pre-test interview showed that most users do not keep an updated antivirus. Some held the belief that antivirus software can still maintain good security without regular updates. To help to correct this misconception, one section of our comic taught users the basics of how the antivirus detects viruses. We described to users that each virus has a unique code sequence, like "DNA" sequences. The antivirus works with a database of known virus signatures or looks for virus behaviours previously seen. Therefore,

the antivirus needs to be updated often so it can recognize newly released viruses. One-week after interacting with the comic prototype, 88% of participants were able to describe how antivirus works, compared to just 13% before learning (See figure 6.9). In addition, 81% of the participants were also able to describe why it is important to perform regular updates. Participants like AC13 and AC10 said, "I didn't know that by updating it's actually able to catch more things," and "it now actually allows me to understand how it's worked and why is it so important to keep it up to date." 6 participants specifically referred to the images in page 12 of the comic to describe how antivirus worked, such as "it detects the DNA of the virus" (AC16), and "it analyses the sequence, so I guess the code sequence just like an DNA in a human" (AC11). Interestingly, AC7 added, "Because the villain is constantly coming up with new ones, spreading them out to get information, to send more spam. So to update it is to recognize the ones that are being put out on an ongoing basis." Here, the participant is referring the scenes depicted in page 8 and 12, and the "villain" refers to the character "Hack". This suggest that visual narratives of malicious intentions of hackers can help users understand the risks.

To assess learning effects of the comic on user behaviour, we asked participants to describe habitual changes over the course of a week after reading the comic. Table 6.6 provides a summary of the results. 31% of participants performed updates during the week. AC15 said "I did go update Avira after out first meeting. I thought I might as well just go and do it, it's not going to be that hard, and I suppose it probably made me more cautious of things that could infect my computer. Although I don't think that I've experienced any potential threats, I might think a little bit more about what I do." AC10 said, "It makes me realize that I need to be more aware and actually, you know I went back to my computer and I looked at my antivirus software that I had (at work) and I went home and I looked at my antivirus and made sure that it was up to date. Made sure everything was working on it." Several other participants also described how learning the information had made them more conscientious and cautious about what they are doing. 38% of participants said that learning about malware has made them more cautious when browsing on the Internet and/or downloading files. Another 19% said they became more conscious of security

| Effects of Learning | # of Participants |
|---|---|
| Updated antivirus within one week | 5 (33%) |
| More conscious of security warnings | 3 (19%) |
| More cautious when browsing and downloading | 6 (38%) |
| Shared knowledge | 8 (69%) |
| No effect | 2 (13%) |

Table 6.6: Antivirus comic: effect of learning on user behaviour

warnings, and would now try to read the entire warning message before performing an action. Within the time period of a week, 69% of participants shared the information they have learned with friends and family. For example, AC4 shared the information with her parents: "Yeah I was explaining it to my parents, especially my dad he has a whole bunch of antivirus on the computer so it made it really slow. So I was trying to explain to him that he doesn't need that many antivirus, he only needs one."

## 6.3 Summary

In this chapter, we presented the study results evaluating our prototype designs that teach users about antivirus protection. Results from a user study that compares our two infographic posters with a text condition were analyzed based on questionnaires evaluating their effectiveness, usefulness, memorability, and persuasiveness. We followed up with participants one week later through an emailed online questionnaire accessing learning outcomes and retention. Results for the antivirus comic were also evaluated based on questionnaires, but additionally collected interview data to gain an understanding of users' mental models of antivirus protection. We reported the questionnaire results, as well as qualitative analyzes of user perceptions and mental models of malware and antivirus software. In the next chapter, we discuss whether the results from chapter 5 and 6 support the six design strategies we proposed at the end of chapter 3.

# Chapter 7

# Discussion and Conclusion

Our research question for this thesis was:

> Do integrated visual-textual education strategies form an effective, memorable, and persuasive approach for computer security understanding by altering user perception and improving user behaviour? If so, does a richer interactive user experience help to further enhance the learning process and effect positive behavioural change?

To address this question, we investigated a visual design approach and performed empirical studies to evaluate our prototypes. In this chapter, we revisit our proposed design strategies and examine whether they were supported by our empirical and statistical results.

## 7.1 Effectiveness of Our Design Strategies

Publicly available computer security resources are frequently text intensive, complex, and inconsistent. Existing approaches to security advice tend to focus on instructing users how to follow certain security heuristics, and are not based on helping them to develop an understanding of the threats. We argue this approach to security education could limit end-users' ability and motivation to make informed security decisions.

Our research proposes that security education should incorporate information design strategies to help end-users learn security information. We believe that having a basic understanding of security risks could empower users, help in harm reduction, and improve user behaviour. We chose to break down security concepts visually by using infographics and comic media, and make the information easy and enjoyable to learn. We minimized content by avoiding overly technical information, and focused on graphical methods of delivery that illustrate conceptual models visually so users

can develop an understanding of the risks quickly. In Chapter 3, we proposed that one way to help address common challenges in end-user security education is to incorporate visual communication strategies. As a proposed solution, we outlined six design strategies to guide our design and development of the prototypes:

1. Integrate graphics with text to gain and sustain user attention, and assist in comprehension of related textual explanations to facilitate knowledge acquisition.
2. Apply information design theory to organize content that enables users to find information quickly and accurately.
3. Depict metaphors visually to increase the persuasiveness and memorability of metaphorical rhetorics.
4. Use visuals, interactivity, and humour to add interest and engagement in learning materials.
5. Combine visuals and text to help communicate operational implications among content objects to assist the transfer of knowledge in the form of a mental model.
6. Maintain high ratio of visual to textual content to help reduce memory load and increase the retention of information.

For the remainder of this chapter, we revisit each strategy, summarize our empirical evidence, and discuss our experience and thoughts in relation to each strategy.

### 7.1.1 Integrate graphics with text to gain and sustain user attention, and assist in comprehension of related textual explanations to facilitate knowledge acquisition

**Application of the Strategy:** Our infographic and comic prototypes rely on the use of graphic/text pairings to support knowledge acquisition. This strategy is grounded in education literature that states the combination of text and images facilitate learning more efficiently than text-only [54]. We used graphics to support knowledge acquisition in two ways: to accompany text content so users can understand them more easily, and to illustrate abstract concepts concretely using visuals.

For supporting text content, we used graphics to extend the meaning of text explanations. For instance, we included both text and visual elements to help to explain how to create a passphrase. The passphrase "My sister Peggy's 29 years old" was explained visually through typographic treatments as well as text explanations. Secondly, we used graphics to help explain abstract concepts, such as in the *Lock* infographic. We used a combination lock to explain password strength to users. Password strength is portrayed through the size of the lock, complexity, and length of lock dials.

**Empirical Evidence:** Our experiments demonstrated that using visual content is beneficial to improve knowledge acquisition. Statistical analysis of data from the infographic studies supported the assertion that the infographics were perceived as significantly more effective for learning than text-only. In fact, statistics showed that infographics from both the password and antivirus studies were preferred to text-only material. We also have statistical evidence supporting improvement in knowledge acquisition and retention in the infographic conditions one week after viewing the material. Users who viewed the infographics were significantly more proficient at describing password guessing attacks and how antivirus software works.

The eye-tracking study of the password comic provided measurements and observations of how users' attention was divided to gain insights into possible connections between participants' attention and their comprehension of the content. Eye-tracking analysis showed that graphics function as references that aid in comprehension of textual information. Participants indeed refer to image and text content back and forth between eye fixations. Text usually gets eye fixation first, then the closest surrounding image. Interestingly in some frames, participants went back to reading text a second time after looking at the images. Additionally, our data showed greater improvements in comprehension when graphics and text were integrated with interactivity. Results from the eye-tracking study showed that after prolonged eye fixations on an interactive element, 25% of participants back-tracked to previously viewed frames, pages, or sections and re-read content.

From the pre-test questionnaire results of 145 participants, 78% reported being visual learners. This provides evidence that the majority of users are visual learners, and support the notion that most people would benefit from learning new information

visually. Our result is slightly higher than a prior finding [9] that reported 65% of the population are visual learners. Only 11% of our participants said they prefer to learn from plain text. We predicted participants' learning preferences might influence how well they learn from information graphics. However, our results did not reveal differences in learning outcomes between visual-learners and non-visual learners. In future prototypes, customizable multimedia preferences could be taken into consideration to accommodate text, visual, or audio learning preferences. In the mean time, we believe visual learning methods are the most practical approach because they accommodate the preferred learning style of at least 65% of the population [9].

**Discussion:** Participants with low prior knowledge preferred to learn visually from our educational material than participants with expert knowledge. Feedback suggests information graphics were most beneficial for users with low security knowledge. After interacting with our prototypes, most participants gained a basic understanding of how things worked and why they needed to protect themselves against the risks. There was little increase in the learning outcome of expert users. These participants wanted more details in the information presented, and some preferred to learn the information by reading text instead. Understandably, they also felt they did not gain new knowledge on the topic. However, we received positive feedback from these participants that our education materials would be very suitable for end-users with lower security knowledge. For example, one expert participant said "I already know most of the information, but I think something like this would be great for my parents."

### 7.1.2 Apply information design theory to organize content that enables users to find information quickly and accurately

**Application of the strategy:** We used graphical elements to organize the layout in our infographic posters. We applied graphic design to create a visual theme that is the most appropriate for each infographic. Design decisions such as colour, typography, and style were made based on the chosen theme. For example, one of the antivirus infographic (*Medical*) was inspired by medical posters. Therefore, we gave the infographic a clinical look through the use of medical-related graphics and colour

schemes. We used other types of graphics for reference purposes, such as icons and typographic headings. Reference graphics help to direct user attention to particular content. Lastly, we used graphics like boxes, lines, and colour blocks to group and organize information. The comic layouts use traditional comic book panels to organize content. Each panel is subdivided into small panels, each of which displays an image in the story, and helps to guide the reading sequence. Word balloons are used to show dialogue.

**Empirical Evidence:** Observations from the infographic studies support the notion that information graphics have organizational benefits that ease reading and finding of information. However, participant feedback indicates that personal interest may influence the order in which content from the infographics are read. For example, users might first scan the page with their eyes to identify areas of interest, then read the information in smaller chucks. Empirical evidence show that graphical cues (i.e., icons, arrows, boxes, shading, and white space between elements) directs user attention to various areas of interest, and allow users to visually search information quickly. A future eye-tracking study of infographic posters would help to confirm these observations.

Empirical evidence from the eye-tracking study of the password comic shows that headings get eye fixations first, followed by text blocks, then graphics. Some elements drew longer eye-fixations than others. Data analysis of the eye-tracking data revealed that elements that drew attention were circular objects, eyes, interactive images, and typographic images. Participants read the comics in a traditional top-to-bottom, left-to-right direction. We did not find users actively searching for information across pages while reading the comics. Although some participants "browsed" images on the current page, they quickly returned to the traditional reading pattern.

**Discussion:** Our infographic user studies show that users do not always process graphical information the same way they would read a text document. Reading plain text information appears to be more linear (i.e., people read from left to right / top to bottom). When participants were presented with an infographic poster, they first visually searched the information, then proceeded to reading smaller areas of interest.

Graphical elements that create visual cues could help to make important points in the instructional content stand out, and build hierarchal relationships between elements. In comics however, users fall back to the traditional reading pattern.

Through eye-tracking measurements of the password comic, we found that our first attempt in the organization of panels in landscape format affected reading direction on some pages. A few participants were unsure of the direction of flow for some panels. In the second iteration of the password comic, we re-arranged the panels to traditional left-page, right-page open book format, and applied this page format for the design of the antivirus comic. Results from the antivirus comic study indicate that this format was more intuitive for users.

### 7.1.3 Depict metaphors visually to increase the persuasiveness and memorability of metaphorical rhetorics

**Application of the Strategy:** In our prototypes, we relied on metaphors to help explain some key concepts of password guessing attacks and antivirus protection. The purpose of using metaphors was to help users build computer security mental models in terms of other well-understood concepts. Each infographic condition relied on one metaphor to communicate the risks. We took the most successful metaphors from the infographic studies and incorporated them into the comic designs. For example, to portray the importance of password strength, one of our infographic posters used a lock metaphor to illustrate the need for strong locks to protect physical assets from burglars. In the password comic, we further developed this metaphor by personifying the lock illustration as a secondary character to teach users about password strength.

**Empirical Evidence:** The assertion that visual metaphors improve security understanding is supported by our results from both the password and antivirus studies. Participants' feedback of the prototypes showed that metaphors embedded in the instructional material facilitated improved understanding of the security topic. Metaphorical concepts used in our educational material were described by participants to be "familiar" and "relatable". For instance, the medical metaphor from the antivirus studies provided participants with meaningful comparisons of computer

viruses and biological viruses. An already well-understood concept of how biological viruses can affect the human body and spread in epidemic proportions improved the understanding of computer viruses and emphasized their seriousness. Participant evaluations of the persuasiveness of the infographics were statistically more positive compared to text information that made no metaphorical references. The infographics and comics were thought to be more relatable than the text-only condition. Data analysis of followup interviews from both the password and antivirus comic studies shows evidence that visual metaphors support deeper comprehension of the risks. Participants directly applied metaphors used in the comics to their descriptions of security concepts one week later. Result indicate that the use of visual metaphors were the most beneficial for users with low security knowledge.

**Discussion:** Our results suggest that the use of visual metaphors help to make abstract security concepts more concrete for users to understand. For example, the lock metaphor from the password studies relied on the concept of physical security. We used the analogy that locks are like passwords that act as barriers to keep dangerous people out. We illustrated this through a burglar scene in one of the password infographics and the comic. Participants thought the illustration has successfully depicted the malicious intent of hackers in cyberspace through the analogy that people need to protect their online spaces just like how they would protect physical spaces.

We selected different metaphors to help users build mental models of the threats. Our studies suggest not all metaphors are equally effective. When the metaphor used is overly complex, it can be counterproductive to help users learn new information. For instance, one password infographic showing the concept of animal lifespans proved to be unsuccessful at communicating the amount of time to crack passwords. Feedback indicate that participants had no concrete idea of how long animals live, and therefore could not make meaningful comparisons between animal lifespans and password cracking times.

### 7.1.4 Use visuals, interactivity, and humour to add interest and engagement in learning materials

**Application of the Strategy:** Infographics and comics have the potential to draw interest to security information because they are highly visual, do not appear intimidating, and require less effort and time commitment to read than text. Images are typically faster to consume. We used graphical explanations whenever possible to reduce the amount of text needed. The infographic were designed to improve security understanding through the use of metaphors. Metaphors help users gain understanding of new information in terms of other well-understood concepts. We avoided overly technical information, and focused on building mental models of understanding. For our comic prototypes, we embedded entertainment and interactivity when they become relevant to the lesson content. Interactive elements extend comprehensibility of the content by giving users additional examples, portray cause and effect relationships, and apply acquired knowledge in interactive mini-games.

**Empirical Evidence:** Empirical evidence from participants' post-viewing prototype evaluations show that graphical learning materials provide a more enjoyable user experience than text-only. 78% of our participants prefer to learn visually from one of our prototypes over reading a text document with the same information. In the password infographic study, participants gave all three graphic conditions higher evaluations than the text only condition. Similarity, the antivirus infographic posters also received higher evaluations for enjoyment. For the text conditions, participants felt they gained useful information, but reported a less pleasurable learning experience than the infographic posters or the comics.

The comics also received high evaluations for enjoyment. Participants thought the comics were "visually appealing", "enjoyable", and "fun" to read. Participant feedback indicated the inclusion of characters and stories had made the topics more relatable and interesting. Humour within the comic was particularity welcomed. Our in-lab observations found several participants chuckling out loud while reading. Results show the use of humour was successful at creating user interest in the lesson content.

Our eye-tracking data provided evidence that interactive elements prolong cognitive interest in the lesson. Users spent as much as 60% longer on pages with interactivity. We also received positive feedback regarding the interactive mini-games at the end of each comic. They helped participants review and reinforce the information they just learned.

One encouraging finding from the antivirus comic study is that many of our participants shared the information they learned with family and friends. 69% of our participants reported sharing behaviour, mostly through word-of-mouth. Participants were also interested to send our prototypes to family and friends when they become available to the public online.

**Discussion:** We know from literature in education [102] that one important source of motivation for learning is interest. Graphics and multimedia are a few tools that are commonly used to engage students in lesson content. We believe security education could also leverage the positive effects of visual communication methods to help end-users learn. However, a study in 1990 [32] cautions against the assumption that greater entertainment will always lead to greater learning. Excessive entertainment could potentially distract users' from learning. For our comic prototypes, we have taken this into consideration during the design process and embedded entertainment and interactivity only when they are relevant to the lesson content, and when we felt they would help to enhance comprehension of the subject.

Our studies show learning certain aspects of security information could influence users' motivation to behave securely. In the password studies, participants were particularly surprised and impressed to learn how quickly computers can be used to guess short passwords. The fact that a single character added to a password can make guessing it exponentially harder has motivated users to make their passwords longer. 80% of users with previously weak passwords were motivated to update their passwords at home. Showing users that little changes can make a big difference can motivate users to adopt these behaviours more efficiently than giving advice that is difficult to achieve.

One issue we found was that a few participants skipped the interactive components on some pages. Eye-tracking data revealed that some users skipped them because

they did not realize the components were interactive. In future iterations of the comic, small animated visual cues could be added to highlight areas of the page with interactivity. The mini-games included in the comics were not scored. Participants suggested that including a summary of correct and wrong answers might motivate them to replay the game.

Our results show images and interactivity help to prolong interest in the lesson content. However, context will most likely play a role in how long users would engage with the learning material. Since our studies took place in a lab setting, contextual factors could not be measured (we discuss this as a limitation in section 7.2). However, many participants offered suggestions for deployment. For the infographic posters, participants said they would most likely read them in situations where they have to wait. A few locations participants suggested are bus/subway stops, offices, and waiting areas. For the educational comics, participants suggested including them with existing software, embedding them in the installation process, featuring them on online safety learning sites, or showcasing them on security help sections of company websites.

An unexpected but positive observation from the antivirus infographic study is that a highly interesting but unrelated topic could help users pay attention to security information. In the *medical* infographic, we presented antivirus protection information visually to look like a health-related poster. Participants said that they did not first expect the content to be about antivirus. They considered medical issues a high-interest topic, and commented that the poster will most likely draw their attention. Once they realized the poster was about antivirus protection, they thought the use of the medical metaphor was clever and relevant. One participant said "If I knew the poster was about computer security, I probably wouldn't read it, but the health related graphics made me curious." Future security education tactics could consider using a high public interest topic to create initial engagement in security information.

### 7.1.5 Combine visuals and text to help communicate operational implications among content objects to assist the transfer of knowledge in the form of a mental model

**Application of the Strategy:** Our instructional materials helped users build mental models. We focused on explaining the basic process of how things work to justify the need for security. For example, by learning about antivirus detection methods, users may be motivated to update their antivirus because they gained knowledge about *why* they should update. The comics took this a step further by giving users a more in-depth lesson. We believe that helping users build mental models of security risks is an important step towards developing long-term problem solving skills. Since not all security threats will occur in the same way each time (e.g., phishing emails), users with a robust mental model would be able to adapt to changing threats and make security conscious decisions.

**Empirical Evidence:** Empirical results from both the password studies and antivirus studies support our assertion that graphics help to build mental models by highlighting cause and effect relationships, and therefore support knowledge transfer. For example, one of the password infographics use a (*Lock*) metaphor to speak to end-users about the threat of password guessing attacks. We illustrated a burglar theme and used a dark colour scheme in the background. This scene generate an overall mood and demonstrate the malicious intent of attackers using a physical security metaphor. A strong lock, hence a strong password prevents unauthorized entry.

It is evident from our pretest assessment of participants' password practices that mental models of password guessing attacks are primarily understood among end-users as targeted attacks. One week after viewing a graphical prototype, participants were statistically more proficient at describing how the three types of online password guessing attacks work, and were also able to apply their new knowledge to create strong sample passwords that evade these attacks. Our analysis of the study results showed connections between an increase of knowledge about attacks and users' ability to create strong passwords.

Pretest results from the antivirus infographic user study show that users have an limited understanding of how virus detection works. Although 95% of our participants have antivirus installed, only 15% updated them once a week. Many also had expired antivirus software subscriptions that were at least 2 years old. Our interview analysis found that end-users have an underdeveloped mental model of *why* they should update antivirus software regularly. Specifically, we uncovered four pre-existing mental models of viruses and other types of malware, and three pre-existing mental models of how antivirus software works. One week after viewing the *Medical* infographic prototype, participants were statically more proficient at describing how antivirus software detection methods work and why they should keep an updated antivirus software. The antivirus comic study showed evidence of positive behavioural outcomes one week after learning about how antivirus works. 33% of our study participants went home and updated their antivirus. An additional 57% said learning about antivirus protection had made them more conscious and cautious. Users commented that learning has brought the risks to the forefront of their minds and prompted them to ask critical questions like "am I vulnerable?" Even though some users did not change their behaviour within the period of a week, they credited the experience for making them more aware of the risks.

**Discussion:** There is evidence from our studies that end users have misconceptions about the nature of security threats. Furthermore, our pretest questionnaire allowed us to gain valuable insights into end-users' mental model of password guessing attacks and antivirus protection.

From the password studies, we found users knowledge is largely restricted to targeted attacks. We argue that a lack of awareness of brute-force and dictionary attacks could impede users' ability to choose good passwords. In our password studies, the majority of participants self-reported that they use strong passwords outlined by standard password advice, such as creating passwords that are at least 7 characters long with uppercase, lowercase, numbers and special characters. There seems to be, however, confusion about what constitutes a "good password". A participant commented "I think my passwords are strong by my own standards, but after reading [the comic] I don't feel they are very strong." Another participant admitted "things

I thought were strong weren't. I use my name with a number at the end. I thought that was strong enough." This suggests that when users sometime choose weak passwords, they mistakenly think they are strong enough. Our users initially justified passwords such as "Ashley10" as strong, based on the length and types of characters, not based on whether they are susceptible to password guessing attacks. Our experiment showed that traditional password advice given to home users does not adequately explain why users should follow the advice or explain how the process of password cracking works, thus limiting users' ability to create strong passwords. Our studies also revealed that end-users are under-educated about brute-force and dictionary attacks. We propose that more user education on *how* attacks work would be beneficial.

From the antivirus studies, we found users have incomplete mental models about virus detection, and therefore this undermines the importance of regular updates. Interview data also revealed that most users have little understanding of the difference between types of malware and how to protect themselves against them. Feedback from the antivirus infographic study shows that there was an interest learning about various types of malware. We included a page designated to malware in the antivirus comic. One week after reading the comic, most participants were able to distinguish that virus is a class of malware. Participants particularly had trouble distinguishing between viruses and worms prior to learning. After reading about them, some confusion still persisted. A few participants also had trouble remembering the differences between types of malware. In future iterations, more visual explanations could to be included to demonstrate how each malware infects and propagates computer systems.

### 7.1.6 Maintain high ratio of visual to textual content to help reduce memory load and increase the retention of information

**Application of the strategy:** All of our prototypes rely on text and graphics to communicate security information to end-users. Our application of visual communication strategies is grounded on prior research that humans remember images better than they remember textual information [83]. We included a text-only condition as the baseline to compare the retention rates of the graphic conditions.

**Empirical Evidence:** We have statistical evidence supporting improvements in information retention one week after viewing an infographic. For the password user studies, participants recalled information about brute-force and dictionary attacks one week later. Since we found that targeted attacks were already well-understood, there was little improvement in retention. The text condition showed no significant improvement in participants' ability to describe any of the three types of attacks. For the antivirus user studies, we evaluated participants' ability to recall how antivirus works to detect malware. The results show a 25% increase in knowledge for the *Surveillance* condition, 40% for *Medical*, and only 10% for *Text*. Statistical tests showed the *Medical* infographic was the most successful in retention rates. These results show evidence that visual-textual communication improves retention of security information.

**Discussion:** Although images can help reduce cognitive load, we found that graphics with a lot of visual noise can be counter-productive. We presented posters in three levels of complexity in the password infographic study. The *Target* infographic was the least visually complex, *Lock* was moderately complex, and *Lifespan* was the most complex. We found that *Lifespan* was the least preferred infographic of the three and least effective at communicating about password guessing attacks. *Lifespan* took longer to read than the other conditions. Participants found it to be complicated and it required some effort to understand. Legends, symbols and icons were used in *Lifespan*, and graphics were presented more abstractly than the other infographics. Participants found that they first needed to learn how to read the legends before beginning to understand the content. This process actually increased their memory load and interfered with the learning process. In contrast, the *Target* and *Lock* infographic achieved a good balance in the amount of content presented and visual complexity.

### 7.1.7 Recommendations for Using Visual Communication Strategies in Computer Security Education

We give recommendations for using information graphics in security education based on our experiences designing these instructional materials for end-users, and on the

empirical evidence we collected through our user studies. We believe these strategies can help to improve computer security understanding and provide an efficient method for end-user communication.

Our first strategy states that graphics that accompany text support knowledge acquisition. Results for the majority of our prototypes support this claim, except for graphics that have a lot of visual noise, which can actually disrupt the learning process. Our experiments showed that although graphics that illustrate an instructional text can improve learning, not all visual are equally effective. Complex visuals that requires high memory load should be avoided. Our second strategy states that graphics can organize layout to making reading intuitive. Our results show that although best practices for graphic design can be applied to maximize the readability of security content, users may not always follow the reading path laid out for them. User interest may dictate what content will get read first. We recommend presenting security material from users' interest point of view and what may be the most useful content for them. The third strategy states that visual metaphors can help users understand security concepts. Our results strongly support this claim. Graphical metaphors are particular effective to depict abstract security concepts (i.e., password strength) visually to users with low security knowledge. The fourth strategy we proposed was that graphics prolong interest and motivate learning. Our results show that visual learning methods are the preferred learning style of most users. Participants had a more enjoyable learning experience interacting with a graphic prototype than reading from text. Since security is regarded as a secondary task, we recommend using visuals methods to communicate to end-users because they can help to initiate interest and prolong engagement in a low interest topic like computer security. The fifth strategy states graphics support knowledge transfer. Our studies show that visuals are much more effective at building a understanding of how something works than text explanations, especially when users' prior knowledge is low. Therefore, we recommend using graphical methods of communication for end-users with low security knowledge because they help to build mental models. The last strategy states that graphics help to support information retention. The studies showed participants who viewed a graphic prototype were able to recall information more successfully, thus

supports prior findings that humans are able to recall images better than text [83]. We further recommend the use of graphics in computer security education to help to reduce cognitive load and maximize users' ability to remember the information.

Teaching formats of our infographics and comics led to different user experiences. The infographics were quick to read and provided helpful actionable advice, while the comic provided users with an in-depth contextual understanding of the attacks and a richer user experience. We recommend using infographics for rapid communication and to raise awareness of security threats, and interactive comics for developing a deeper understanding.

## 7.2 Limitations and Future Work

### Contextual factors

Although we have stressed that the use of visuals have many communication and psychological functions, one limitation of evaluating educational material in a lab environment is that users cannot experience the learning materials in context of which they will be displayed and used. Environmental factors such as placement, location, format, size, and time, and the technological platform may influence how the material is absorbed by end-users. The next step of this research is to evaluate the educational material with end-users in their own environment. In future work, we would like to partner with organizations to explore venues for deployment, and gather additional empirical data through field studies.

### Effect of Control Condition

Text was used as a control condition to compare the effectiveness of the infographic prototypes. We chose text information comparable to content from our prototype designs. We did not replicate exact text from our infographics to use it as a control condition because it was custom written to work in conjunction with the visuals. As an alternative, we chose to adapt text information from well-known resources used by end-users to learn information like Wikipedia. The resources we used were written in plain language with minimal technical jargon. Although we tried closely match

the contents of the control condition to our infographics, differences still existed, like the choice of words, writing style, and the amount of information covered through text. Since our infographics heavily rely on the use of images, text content is reduced to a minimum. The infographics were quicker to read than the text conditions, but conveyed similar types of information. For the antivirus study, we had to adapt text from several resources to match them with our infographics. This was not ideal, but no single reputable resource was available to provide a close match. The sufficiency of the control condition cannot be proved. Differences in types of resources could influence the effectiveness of the control condition.

### Scalability

We have shown in our users studies that most participants were able to retain information from our educational material and reported positive behavioural change one week after learning. The third limitation of our studies is that it does not measure knowledge retention and knowledge transfer beyond one week. Research into end-users' password management strategies have found that there is discrepancy between what users know and what they actually do [88]. Although many of our participants reported positive behavioural change over one week, it is unknown whether they will continue with these practices in the long term. In future work, longitudinal studies are needed to followup with participants at longer time intervals.

## 7.3 Conclusion

This thesis examined the learning effects of visual design strategies to increase computer security understanding. In our five user studies with a total of 145 participants, we evaluated the effects of educating users visually through infographic posters and online interactive comics about password guessing attacks and antivirus protection. Infographics that rely on visual-textual communication were compared to a text-only condition. We later experimented with interactive comics to extend the power of information graphics through a richer interactive user experience.

In summary, our contributions of this thesis are:

1. The design and implementation of 5 infographic posters and 2 educational interactive online comic books.

2. Empirical results showing improved effectiveness of infographics and comics over text-only advice in one-week user studies with a total of 145 participants.

3. Qualitative analysis of users' mental models of password guessing attacks and antivirus protection with a total of 29 participants.

4. Comic eye-tracking experiment drawing possible connections between user attention and comprehension.

5. Discussion and recommendations of 6 design strategies for computer security education supported by our empirical results.

The between-subject infographic studies took place both in-lab and at home over a one week period. The comic studies took place in two lab sessions, also set one week apart. Participants perceived both the infographics and comics to be more effective, useful, memorable, and persuasive than learning from text-only. They are *effective* because they support knowledge acquisition and knowledge transfer by building conceptual mental models. They are *useful* in helping end-users read and find information efficiently. They are *memorable* due to the picture superiority effect [83]. In addition, the use of visual metaphors help users learn new information through familiar contexts. Lastly, they are *persuasive* because they help to heighten personal awareness, create motivation, and prolong interest in learning about security information.

Future work in this area seeks to investigate some of the limitations, including context, scalability, and the control condition. A field study could possibly gain insight into the effectiveness of the prototypes in various learning environments. Longitudinal measurements of knowledge retention and transfer could provide insight into the persistence of the security knowledge and behaviour.

In conclusion, our research question asked:

> Do integrated visual-textual education strategies form an effective, memorable, and persuasive approach for computer security understanding by altering user perception and improving user behaviour? If so, does

a richer interactive user experience help to further enhance the learning process and effect positive behavioural change?

The design, prototyping, and empirical work in the thesis demonstrated positive outcomes. Participant evaluations and feedback show that learning graphically is perceived to be effective, useful, memorable, and persuasive. The followup results were able to confirm improved user behaviour after one week. Most participants showed a increase in knowledge about the security topic, improved personal awareness of the threats, and reported active changes in behaviour. Our results also positively support that a richer interactive user experience helps to further enhance the learning process and effect positive behavioural change. The inclusion of a narrative, characters, humour, and interactivity create interest and engagement in the instructional content. Therefore, we conclude that visual communication is a viable and effective approach for conveying security information, and for helping end-users form better mental models of computer security.

## Bibliography


[1] about.com. Principles of Design, Accessed June 2013. `http://desktoppub.about.com/cs/basic/g/principles.htm`.

[2] A. Adams and M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[3] Adams, S. Dilbert, Accessed December 2012. `http://search.dilbert.com/comic/Security`.

[4] F. Asgharpour, D. Liu, and L. Camp. Mental models of security risks. *Financial Cryptography and Data Security*, pages 367–377, 2007.

[5] Robert Biddle, Sonia Chiasson, and Paul C. van Oorschot. Graphical passwords: learning from the first twelve years. *ACM Computing Surveys*, 44(4), 2012.

[6] bmo.com. Your Security Online: Protecting Yourself, Accessed June 2013. `http://www.bmo.com/home/about/banking/privacy-security/protecting-yourself?nav=left`.

[7] I. Bogost. *Persuasive games: The expressive power of videogames*. MIT Press, 2007.

[8] R. E. Boyatzis. *Transforming qualitative information: Thematic analysis and code development*. Sage, 1998.

[9] W.C. Bradford. Reaching the visual learner: Teaching properly through art. *The Law Teacher*, 11, 2004.

[10] R. K. Branson, G. T. Rayner, J. Cox, J. P. Furman, and F. J. King. Interservice procedures for instructional systems development. executive summary and model. Technical report, DTIC Document, 1975.

[11] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[12] C. Bravo-Lillo, L. F. Cranor, J. S. Downs, and S Komanduri. Bridging the gap in computer security warnings: A mental model approach. *Security & Privacy, IEEE*, 9(2):18–26, 2011.

[13] P. Bryant, S. M. Furnell, and A. D. Phippen. Improving protection and security awareness amongst home users. *Advances in Networks, Computing and Communications 4*, page 182, 2005-2006.

[14] L.J. Camp. Mental models of privacy and security. *Technology and Society Magazine, IEEE*, 28(3):37–46, 2009.

[15] S. K. Card, J. D. Mackinlay, and B. Shneiderman. *Readings in information visualization: using vision to think*. Morgan Kaufmann Pub, 1999.

[16] J. M. Carroll, P. L. Smith-Kerker, J. R. Ford, and S. A. Mazur-Rimetz. The minimal manual. *Human-Computer Interaction*, 3(2):123–153, 1987.

[17] S. Carsten. Limesurvey: The open source survey application, Accessed June 2013. `http://www.limesurvey.org`.

[18] L.J. Chanlin. The effects of verbal elaboration and visual elaboration on student learning. *International Journal of Instructional Media*, 24(4):333–39, 1997.

[19] L.J. Chanlin. Animation to teach students of different knowledge levels. *Journal of Instructional Psychology*, 1998.

[20] S. Chiasson, Manas M., and R. Biddle. Auction hero: The design of a game to learn and teach about computer security, Accessed July 2013. `http://hotsoft.carleton.ca/~sonia/content/Chiasson_Auctionhero_ELearn2011.pdf`.

[21] citi.com. How to Protect Yourself, Accessed June 2013. `https://online.citibank.com/US/JRS/pands/detail.do?ID=ProtectYourSelf`.

[22] R. C. Clark and C. Lyons. *Graphics for learning: Proven guidelines for planning, designing, and evaluating visuals in training materials*. John Wiley & Sons, 2010.

[23] Wikimedia Commons. Addie model of design, Accessed July 2013. `http://upload.wikimedia.org/wikipedia/commons/d/d3/ADDIE_Model_of_Design.jpg`.

[24] K. Craik and W. James. *The nature of explanation*. Cambridge University Press, 1967.

[25] L. F. Cranor. A framework for reasoning about the human in the loop. *USENIX*, 8:1–15, 2008.

[26] L. F. Cranor and S. Garfinkel. *Security and usability: Designing secure systems that people can use*. O'reilly Media, 2008.

[27] H. M. Cuevas, S. M Fiore, and R. L. Oser. Scaffolding cognitive and metacognitive processes in low verbal ability learners: Use of diagrams in computer-based training environments. *Instructional Science*, 30(6):433–464, 2002.

[28] dedoose.com. Dedoose research application, Accessed June 2013. `http://www.dedoose.com`.

[29] Deloitte. P@$$1234: the end of strong password-only security, Accessed March 2013. http://www.deloitte.com/view/en_GX/global/industries/technology-media-telecommunications/tmt-predictions-2013/tmt-predictions-2013-technology/9eb6f4efcbccb310VgnVCM1000003256f70aRCRD.htm#.UfVzT5WPD_M.

[30] T. Denning, T. Kohno, and A. Shostack. Control-alt-hack: a card game for computer security outreach and education. In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, pages 729–729. ACM, 2013.

[31] M.M.A. Devillers. Analyzing password strength. *Radboud University Nijmegen, Tech. Rep*, 2010.

[32] N. M. Dixon. *Evaluation: A tool for improving HRD quality*. University Associates San Diego, 1990.

[33] C. Dormann and R. Biddle. A review of humor for computer games: Play, laugh and more. *Simulation & gaming*, 40(6):802–824, 2009.

[34] P. Dourish, R. E. Grinter, J. D. De La Flor, and M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[35] ebay.com. Ebay Security Center, Accessed June 2013. http://pages.ebay.com/securitycenter/index.html.

[36] W. Eisner. Comics & sequential art. 1985.

[37] M. Emmison and P. Smith. Researching the visual: Images, objects, contexts and interactions in social and cultural enquiry, 2000.

[38] D. Florêncio and C. Herley. Where do security policies come from. In *Proceedings of the 10th Symposium on Usable Privacy and Security*, 2010.

[39] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *WWW '07: Proceedings of the 16th Internation Conference on World Wide Web*, New York, USA, 2007. ACM.

[40] G. T. Fong and R. E. Nisbett. Immediate and delayed transfer of training effects in statistical reasoning. *Journal of Experimental Psychology: General*, 120(1):34, 1991.

[41] Fontana, J. Password life expectancy down to seconds, Accessed March 2013. http://www.zdnet.com/password-life-expectancy-down-to-seconds-7000009851.

[42] J. Frascara. Communication design, principles, methods and practice. 2004.

[43] S. Garfinkel, G. Spafford, and A. Schwartz. *Practical UNIX and Internet security*. O'reilly, 2003.

[44] R. L. Garner. Humor in pedagogy: How ha-ha can lead to aha! *College Teaching*, 54(1):177–180, 2006.

[45] S. Gaw and E.W. Felten. Password management strategies for online accounts. In *Proceedings of the 2nd Symposium on Usable Privacy and Security*, pages 44–55. ACM, 2006.

[46] getcybersafe.gc.ca. Get Cyber Safe, Accessed June 2013. `http://www.getcybersafe.gc.ca/index-eng.aspx`.

[47] S. Good and A. Krekelberg. Usability and privacy: a study of kazaa p2p file-sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 137–144. ACM, 2003.

[48] Google Chrome Team, McCloud, S. Google Chrome, Accessed June 2012. `http://www.google.com/googlebooks/chrome`.

[49] google.ca. How you can stay safe and secure online, Accessed June 2013. `http://www.google.ca/goodtoknow/online-safety/`.

[50] S. Görling. The myth of user education. In *Virus Bulletin Conference*, volume 11, page 13, 2006.

[51] R. E. Grinter, W. K. Edwards, M. W. Newman, and N. Ducheneaut. The work to make a home network work. In *ECSCW 2005*, pages 469–488. Springer, 2005.

[52] J. B. Gross and M. B. Rosson. Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 Symposium on Computer Human Interaction For the Management of Information Technology*, page 10. ACM, 2007.

[53] K .L. Gustafson and R. M. Branch. What is instructional design? *Trends and Issues in Instructional Design and Technology*, pages 16–25, 2002.

[54] V. Gyselinck and H. Tardieu. The role of illustrations in text comprehension: What, when, for whom, and why? 1999.

[55] C. Herley. So long, and no thanks for the externalities. In *New Security Paradigms Workshop (NSPW)*, 2009.

[56] internetworldstats.com. Internet Growth Statistics, Accessed July 2013. `http://www.internetworldstats.com/emarketing.htm`.

[57] E. Jain, Y. Sheikh, and J. Hodgins. Inferring artistic intention in comic art through viewer gaze. In *Proceedings of the ACM Symposium on Applied Perception*, pages 55–62. ACM, 2012.

[58] P. N. Johnson-Laird, V. Girotto, and P. L. Mental models: a gentle guide for outsiders. *Sistemi Intelligenti*, 9(68):33, 1998.

[59] M. Keith, B. Shao, and P. Steinbart. A behavioral analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems*, 10(2):63–89, 2009.

[60] P.G. Kelley, J. Bresee, L.F. Cranor, and R.W. Reeder. A nutrition label for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 4. ACM, 2009.

[61] J. O. Kephart. A biologically inspired immune system for computers. In *Artificial Life IV: Proceedings of the 4th International Workshop on the Synthesis and Simulation of Living Systems*, pages 130–139, 1994.

[62] J. O. Kephart, G. B. Sorkin, W. C. Arnold, D. M. Chess, G. J. Tesauro, S. R. White, and T. J. Watson. Biologically inspired defenses against computer viruses. In *IJCAI (1)*, pages 985–996, 1995.

[63] C.K. Kinzer, S. Turkay, D. L Hoffman, N. Gunbas, P. Chantes, A. Chaiwinij, and T. Dvorkin. Examining the effects of text and images on story comprehension: An eye-tracking study of reading in a video game and comic book. pages 259–275, 2012.

[64] P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. F. Cranor, and J Hong. Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, pages 70–81. ACM, 2007.

[65] P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor, and J. Hong. Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):7, 2010.

[66] C. Kuo, S. Romanosky, and L. F. Cranor. Human selection of mnemonic phrase-based passwords. In *Proceedings of the 2nd Symposium on Usable Privacy and Security*, pages 67–78. ACM, 2006.

[67] G. Lakoff and M. Johnson. The metaphorical structure of the human conceptual system. *Cognitive Science*, 4(2):195–208, 2010.

[68] logicalpcs.com. 5 Popular Computer Virus Misconceptions, Accessed June 2013. `http://www.logicalpcs.com/2012/03/07/5-popular-computer-virus-misconceptions/`.

[69] A. Marcus. Metaphor design for user interfaces. In *CHI 98 Cconference Summary on Human Factors in Computing Systems*, pages 129–130. ACM, 1998.

[70] R.E. Mayer, W. Bove, A. Bryman, R. Mars, and L. Tapangco. When less is more: Meaningful learning from visual and verbal summaries of science textbook lessons. *Journal of educational psychology*, 88(1):64, 1996.

[71] S. McCloud. *Reinventing comics: How imagination and technology are revolutionizing an art form*. William Morrow Paperbacks, 2000.

[72] Microsoft Developer Network. Password Policy, Accessed March 2013. `http://msdn.microsoft.com/en-us/library/ms161959.aspx`.

[73] microsoft.com. Safety and Security Center, Accessed June 2013. `http://www.microsoft.com/security/default.aspx`.

[74] Miriam Z. Mintzer and Joan Gay Snodgrass. The picture superiority effect: Support for the distinctiveness model. *The American Journal of Psychology*, 112(1):113–146, 1999.

[75] Munroe, R. XKCD: a webcomic of romance, sarcasm, math, and language, Accessed December 2012. `http://xkcd.com/936/`.

[76] A. Negrete and C. Lartigue. Learning from education to communicate science as a good story. *Endeavour*, 28(3):120–124, 2004.

[77] J. Nielsen. User education is not the answer to security problems. *Alertbox, October*, 2004.

[78] A. Nijholt. Embodied agents: A new impetus to humor research. In *The April Fools' Day Workshop on Computational Humour*, volume 20 of *Twente Workshops on Language Technology*. University of Twente, 2002.

[79] Donald A Norman. *The design of everyday things*. Basic books, 2002.

[80] G. Notoatmodjo and C. Thomborson. Passwords and perceptions. In *Proceedings of the 7th Australasian Conference on Information Security-Volume 98*, pages 71–78. Australian Computer Society, Inc., 2009.

[81] T. Omori, T. Ishii, and K. Kurata. Eye catchers in comics: Controlling eye movements in reading pictorial and textual media. In *28th International Congress of Psychology*, 2004.

[82] A. Paivio. Dual coding theory: Retrospect and current status. *Canadian Journal of Psychology/Revue Canadienne de Psychologie*, 45(3):255, 1991.

[83] A. Paivio, T. B. Rogers, and P. C. Smythe. Why are pictures easier to recall than words? *Psychonomic Science*, 1968.

[84] R. Pastor-Satorras and A. Vespignani. Epidemic spreading in scale-free networks. *Physical Review Letters*, 86(14):3200, 2001.

[85] paypal.com. How to Stay Protected and Secure, Accessed June 2013. `https://www.paypal.com/ca/webapps/mpp/security/online-security-center`.

[86] phish-education.apwg.org. APWG CMU-Cylab phishing education landing page program, Accessed June 2013. `http://phish-education.apwg.org`.

[87] F. Raja, K. Hawkey, S. Hsu, K.L.C. Wang, and K. Beznosov. A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In *Proceedings of the 7th Symposium on Usable Privacy and Security*. ACM, 2011.

[88] S Riley. Password security: What users know and what they actually do. *Usability News*, 8(1), 2006.

[89] Royal Bank of Canada. Don't be a Target, Accessed March 2013. `http://www.rbc.com/privacysecurity/ca/popup-dont-be-a-target.html`.

[90] D. J. Sanok Jr. An analysis of how antivirus methodologies are utilized in protecting computers from malicious code. In *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, pages 142–144. ACM, 2005.

[91] R. A. Schmidt and R. A. Bjork. New conceptualizations of practice: Common principles in three paradigms suggest new concepts for training. *Psychological Science*, 3(4):207–217, 1992.

[92] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J. Hong, and E. Nunge. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pages 88–99. ACM, 2007.

[93] M. Smiciklas. *The Power of Infographics: Using Pictures to Communicate and Connect With Your Audiences*. Que Publishing, 2012.

[94] A. Somayaji, S. Hofmeyr, and S. Forrest. Principles of a computer immune system. In *Proceedings of the New Security Paradigms Workshop (NSPW)*, pages 75–82. ACM, 1997.

[95] S. Srikwan and M. Jakobsson. Using cartoons to teach internet security. *Cryptologia*, 32(2):137–154, 2008.

[96] stopthinkconnect.org. Stop. Think. Connect, Accessed June 2013. `http://stopthinkconnect.org`.

[97] A. Strauss and J. Corbin. Open coding. *Basics of qualitative research: Grounded theory procedures and techniques*, 2:101–121, 1990.

[98] Tembhurne, R. 15 Myths and Misconceptions about Viruses and Security Applications, Accessed June 2013. `http://rakesh.tembhurne.com/15-myths-and-misconceptions-about-viruses-and-security-applications/`.

[99] E. R. Tufte and P. R. Graves-Morris. *The visual display of quantitative information*, volume 2. Graphics Press Cheshire, CT, 1983.

[100] T. Van Gog and K Scheiter. Eye tracking as a tool to study and enhance multimedia learning. *Learning and Instruction*, 20(2):95–99, 2010.

[101] J. J. Van Merrienboer, M. B. De Croock, and O. Jelsma. The transfer paradox: Effects of contextual interference on retention and transfer performance of a complex cognitive skill. *Perceptual and Motor Skills*, 84(3):784–786, 1997.

[102] S. E. Wade. Research on importance and interest: Implications for curriculum development and future research. *Educational Psychology Review*, 13(3):243–261, 2001.

[103] R. Wash. Folk models of home computer security. In *Proceedings of the 6th Symposium on Usable Privacy and Security*. ACM, 2010.

[104] D. Weirich and M.A. Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the New Security Paradigms Workshop (NSPW)*, pages 137–143. ACM, 2001.

[105] Alma Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium*, volume 99, Washington, USA, 1999.

[106] Wikipedia. Antivirus Software, Accessed June 2013. `https://en.wikipedia.org/wiki/Antivirus_software`.

[107] Wikipedia. Password Cracking, Accessed March 2013. `http://en.wikipedia.org/wiki/Password_cracking`.

[108] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: Empirical results. *Security & Privacy, IEEE*, 2(5):25–31, 2004.

[109] K. Yee. *User interaction design for secure systems*. Springer, 2002.

[110] R. M. Young. Surrogates and mappings: Two kinds of conceptual models for interactive devices. *Mental models*, pages 35–52, 1983.

[111] Zhang-Kennedy, L. and Chiasson, S. and Biddle, R. Versipass. `http://www.versipass.com/edusec/`.

# Appendix A

# Infographic Prototypes

## A.1 Password Guessing Attacks Infographic Prototypes

## A.2 Antivirus Protection Infographic Prototypes

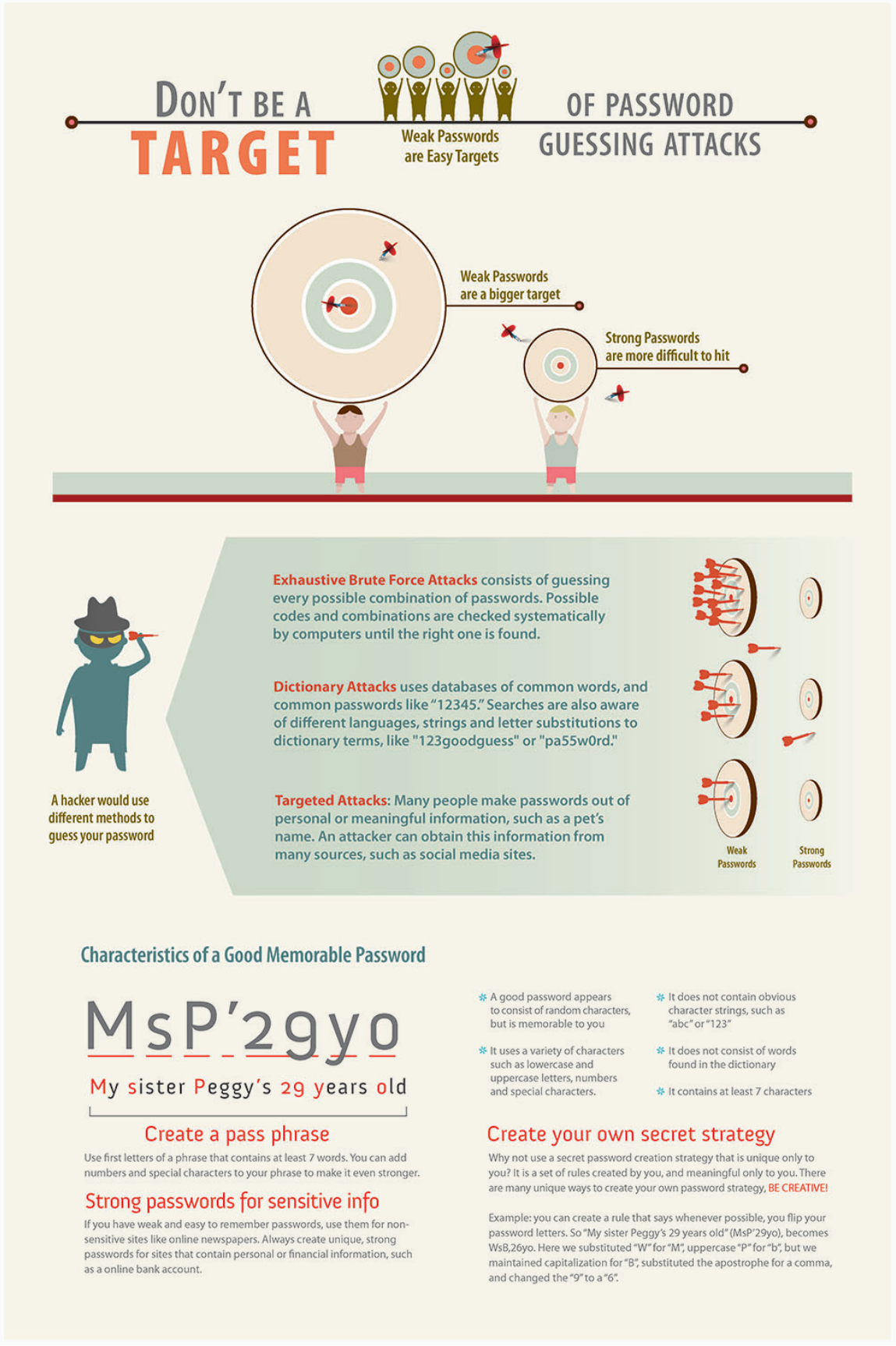



Figure A.1: Password guessing attacks infographic prototype A: *Target* Infographic

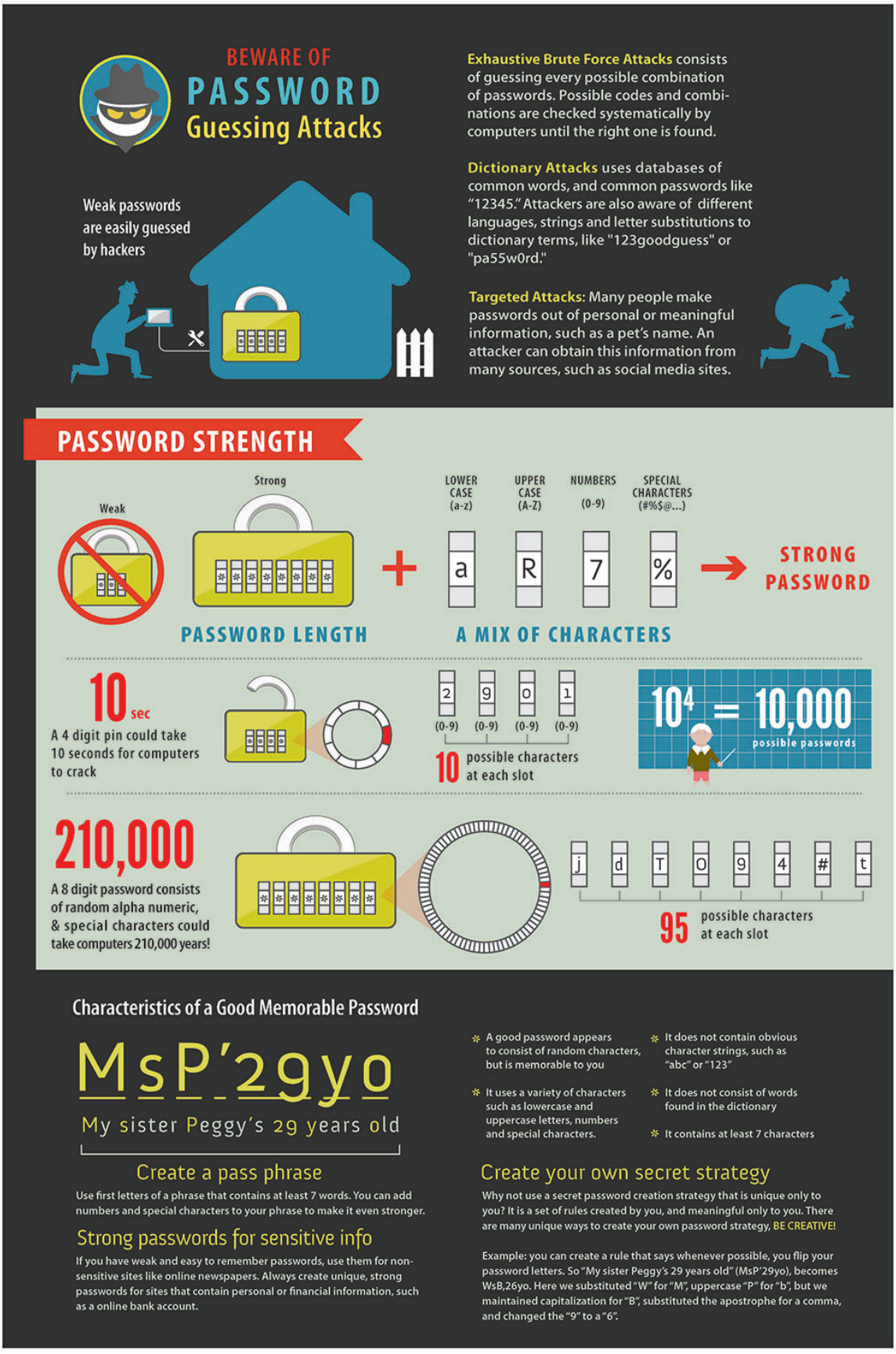



Figure A.2: Password guessing attacks infographic prototype B: *Lock* Infographic

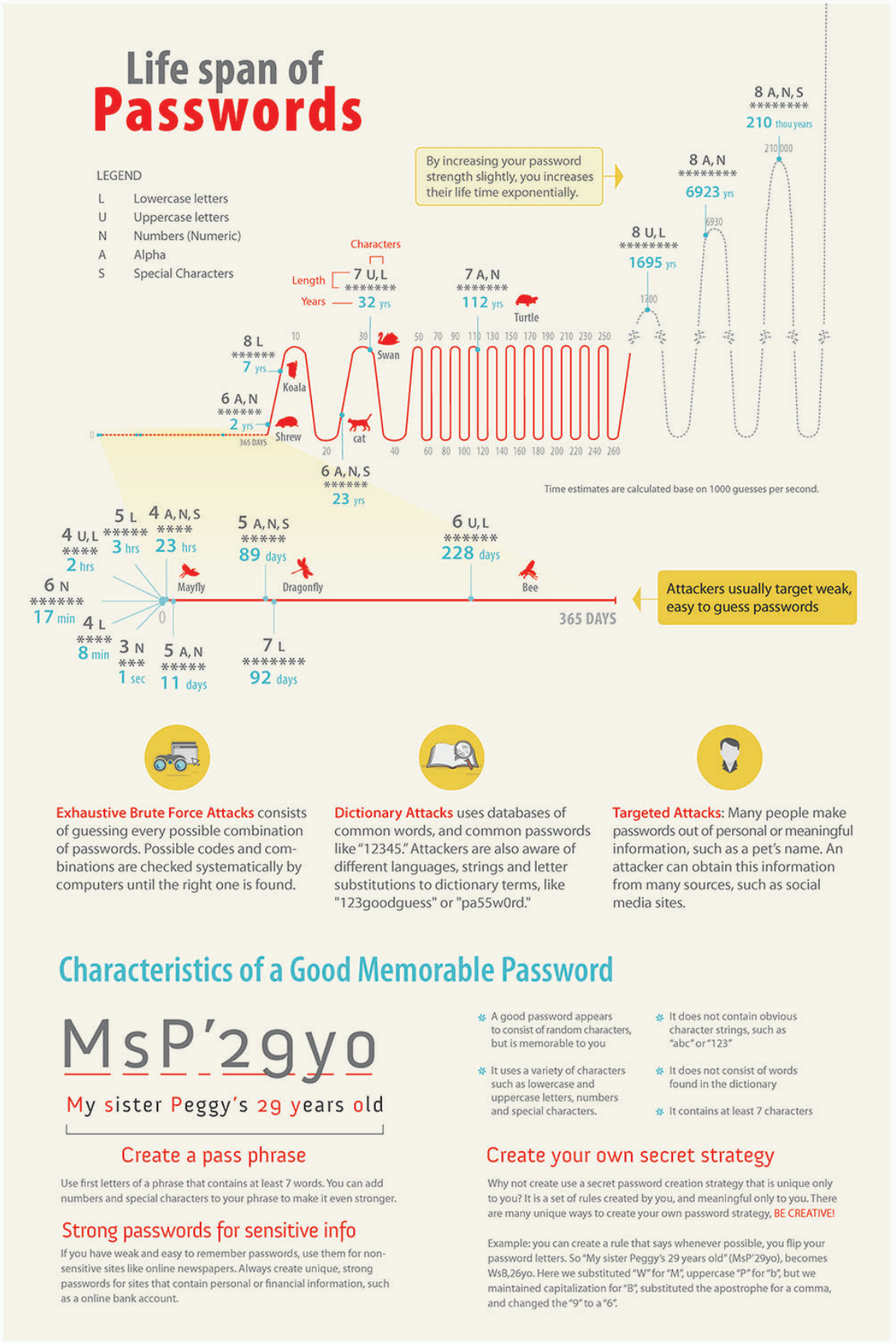



Figure A.3: Password guessing attacks infographic prototype C: *Lifespan* Infographic

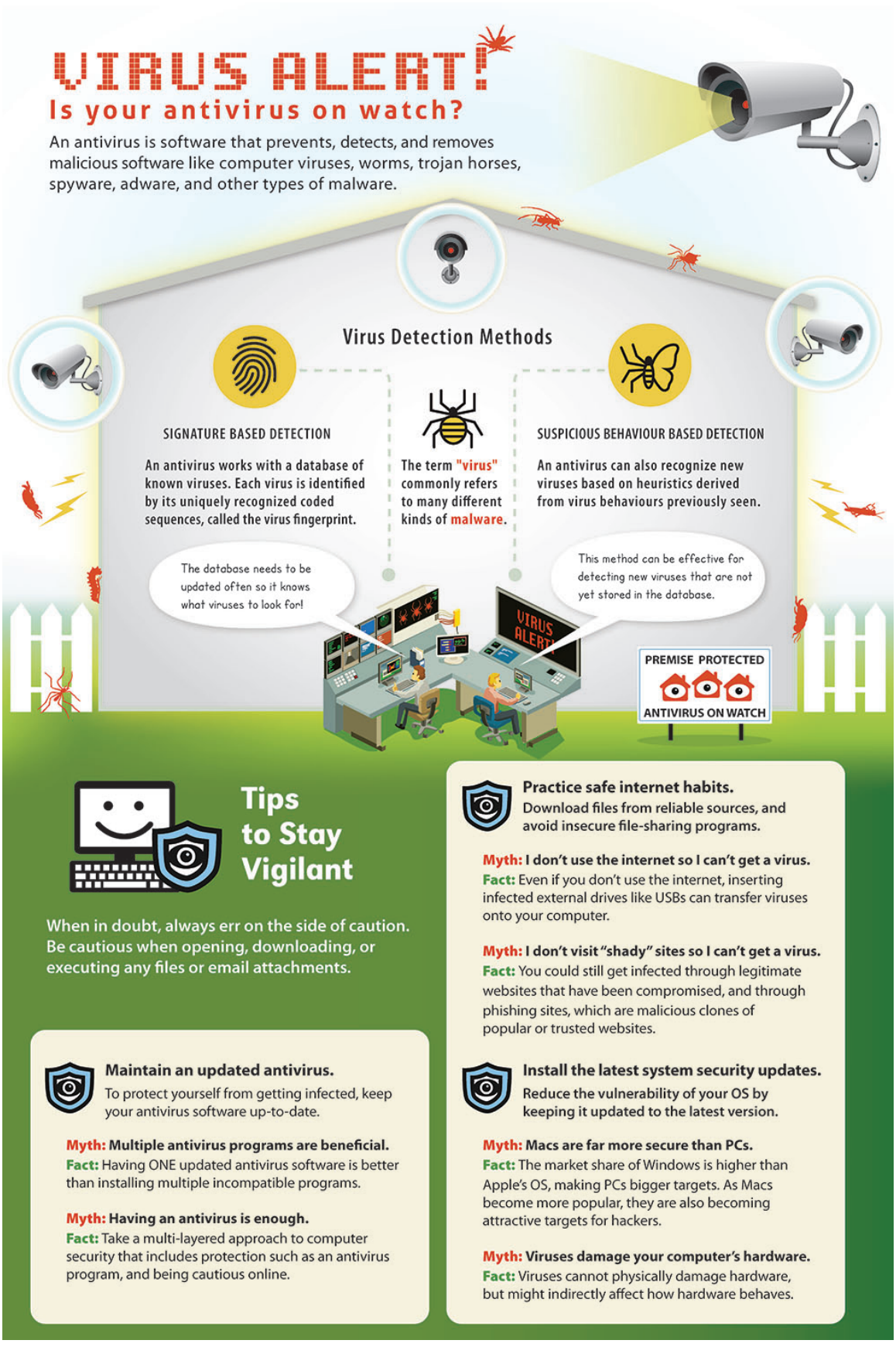



Figure A.4: Antivirus protection infographic prototype A: *Surveillance* Infographic

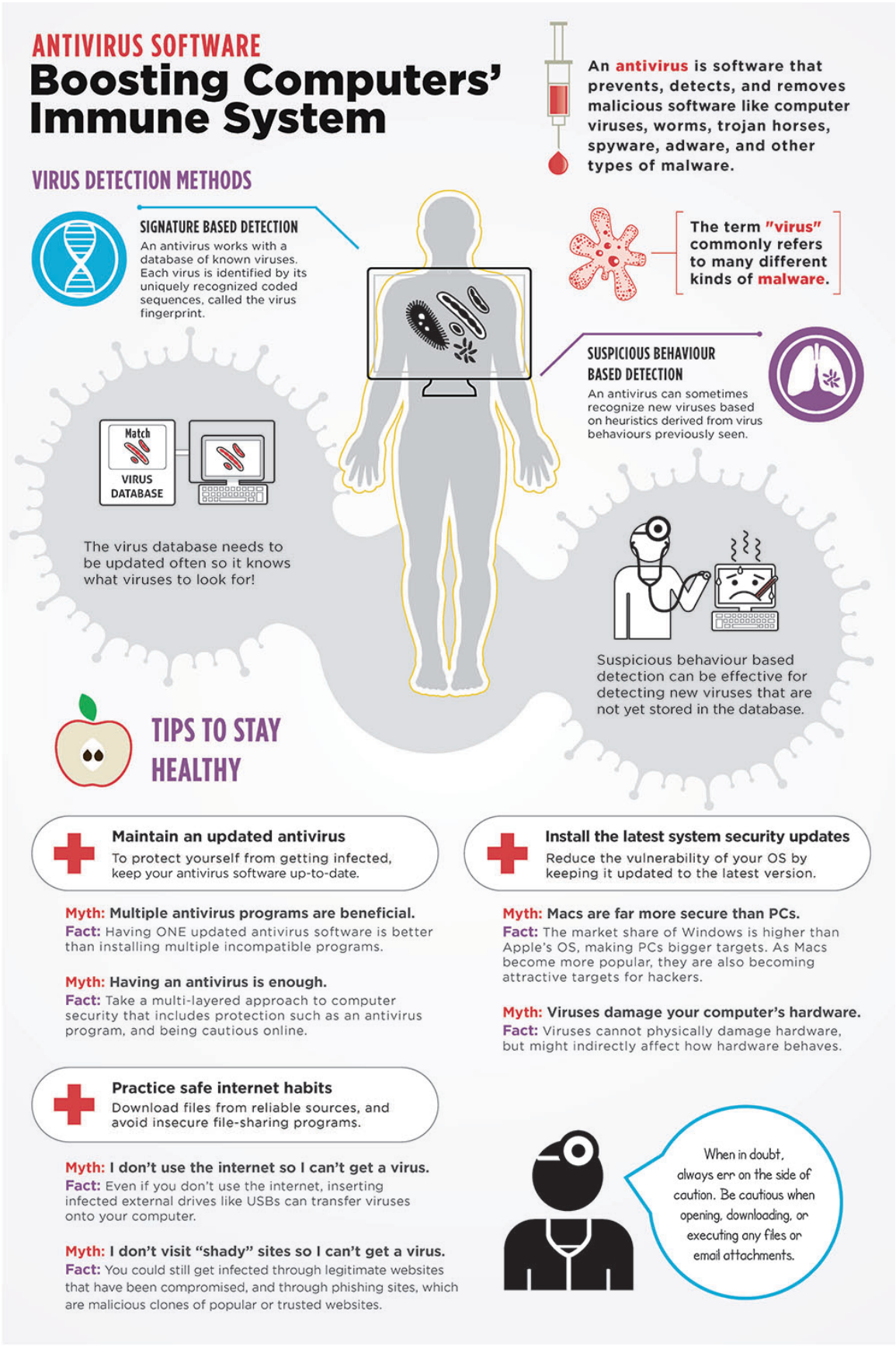



Figure A.5: Antivirus protection infographic prototype B: *Medical* Infographic

# Appendix B

# Text Conditions

## B.1 Password Guessing Attacks Infographic Study Text Condition

### Time needed for password searches

The time to crack a password is related to bit strength; which is a measure of the password's information entropy. Most methods of password cracking require the computer to produce many candidate passwords, each of which is checked. One example is brute-force cracking, in which a computer tries every possible key or password until it succeeds. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc., attempt to reduce the number of trials required and will usually be attempted before brute force. Higher password bit strength increases exponentially the number of candidate passwords that must be checked, on average, to recover the password and reduces the likelihood that the password will be found in any cracking dictionary.

The ability to crack passwords using computer programs is also a function of the number of possible passwords per second which can be checked. If a hash of the target password is available to the attacker, this number can be quite large. If not, the rate depends on whether the authentication software limits how often a password can be tried, either by time delays, CAPTCHAs, or forced lockouts after some number of failed attempts. Another situation where quick guessing is possible is when the password is used to form a cryptographic key. In such cases, an attacker can quickly check to see if a guessed password successfully decodes encrypted data. For example, one commercial product claims to test 103,000 WPA PSK passwords per second.

Ordinary desktop computers can test over a hundred million passwords per second using password cracking tools that run on a general purpose CPU and billions of passwords per second using GPU-based password cracking tools. A user-selected

eight-character password with numbers, mixed case, and symbols, reaches an estimated 30-bit strength, according to NIST. 230 is only one billion permutations and would take an average of 16 minutes to crack. When ordinary desktop computers are combined in a cracking effort, as can be done with botnets, the capabilities of password cracking are considerably extended. In 2002, distributed.net successfully found a 64-bit RC5 key in four years, in an effort which included over 300,000 different computers at various times, and which generated an average of over 12 billion keys per second. Graphics processors can speed up password cracking by a factor of 50 to 100 over general purpose computers. As of 2011, available commercial products claim the ability to test up to 2,800,000,000 passwords a second on a standard desktop computer using a high-end graphics processor. Such a device can crack a 10 letter single-case password in one day. Note that the work can be distributed over many computers for an additional speedup proportional to the number of available computers with comparable GPUs.

**Easy to remember, hard to guess**

A password that is easy to remember is generally also easy for an attacker to guess. Passwords that are difficult to remember will reduce the security of a system because (a) users might need to write down or electronically store the password, (b) users will need frequent password resets and (c) users are more likely to re-use the same password. Similarly, the more stringent requirements for password strength, e.g. "have a mix of uppercase and lowercase letters and digits" or "change it monthly", the greater the degree to which users will subvert the system. In "The Memorability and Security of Passwords", Jeff Yan et al. examines the effect of advice given to users about a good choice of password. They found that passwords based on thinking of a phrase and taking the first letter of each word are just as memorable as naively selected passwords, and just as hard to crack as randomly generated passwords. Combining two unrelated words is another good method. Having a personally designed "Algorithm" for generating obscure passwords is another good method. In the latest improvements, more and more people are noticing change in the way that passwords are secured.

## B.2 Antivirus Protection Infographic Study Text condition

**Antivirus or anti-virus software** is software used to prevent, detect and remove malware (of all descriptions), such as: computer viruses, malicious BHOs, hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. Computer security, including protection from social engineering techniques, is commonly offered in products and services of antivirus software companies. This page discusses the software used for the prevention and removal of malware threats, rather than computer security implemented by software methods.

A variety of strategies are typically employed. Signature-based detection involves searching for known patterns of data within executable code. However, it is possible for a computer to be infected with new malware for which no signature is yet known. To counter such so-called zero-day threats, heuristics can be used. One type of heuristic approach, generic signatures, can identify new viruses or variants of existing viruses by looking for known malicious code, or slight variations of such code, in files. Some antivirus software can also predict what a file will do by running it in a sandbox and analyzing what it does to see if it performs any malicious actions.

**Myths and Tips:**

**1. PCs are far less secure than Macs.**

Apple and some over-zealous Mac users are primarily responsible for pushing this misconception. While the rates of infection are generally higher with PCs, the actual reason for this is the market share between Windows and Apple's OS. It's estimated that in the US only 10-11% of computers are using an Apple OS, with Windows coming in at nearly 87%. From the perspective of virus and malware authors, this imbalanced market share makes Windows-based viruses a far more attractive endeavour.

**2. Viruses damage your computer's hardware.**

While it's certainly feasible that a virus could damage or destroy the functionality of a computers software foundation, the chances that they are able to damage the physical components is exceptionally low. There have been some cases where a virus was able to alter hardware settings to levels that could potentially cause damage, but again, this is extremely rare, and not even possible on the bulk of PCs in circulation. More often, unrelated hardware issues are uncovered during diagnostic procedures when the virus is being professionally removed.

**3. Multiple Anti-virus programs are beneficial.**

While it may seem reasonable to assume that multiple anti-virus programs would enhance a PCs security, this is almost NEVER true. In most cases the presence of multiple anti-virus programs will actually cause the PC to be less secure in addition to causing degraded performance. Even trace amounts of left over files from a previous anti-virus can cause issues. There are some security programs that can be used in conjunction with an anti-virus suite, but it's recommended that you consult an IT professional before installing any such program.

**4. Having an Anti-virus is enough to be secure.**

This may be the biggest misconception of all. While having an up-to-date anti-virus is paramount to a PCs overall security, it is only 1 piece of the puzzle. Additional steps, such as keeping the operating system up-to date, avoiding P2P/File-sharing programs, and employing safe web browsing habits are also necessary to keep the PC secure.

**5. I do not use Internet on my computer, so no chance of getting infected.**

Internet is not only the place from where your computer will get viruses and other malwares. USB drives, CDs, DVDs are other popular mediums through which infections spread. Malwares may also be present in some of the softwares, games or files you are using, even if they are popular and trusted but taken from untrusted sources

like your friend's computer.

**6. If I do not open Porn / Adult Websites, my PC will not get infected.**

If you are thinking only porn, adult or gambling websites run bad scripts in the background, you should definitely read my last blog post, Facebook applications that might annoy your friends. You must have already heard about Phishing websites, which are nothing but clones of popular websites, especially banks and financial websites, to trick you. Email attachments are also one of the common way to get infected. I have also seen some people hiding one fine inside other files. For example, I saw someone to hide a video inside a image file. If you open that file, image will show up as it generally does, but very few knew how to see that hidden video inside that image file.

# Appendix C

# Comic Prototypes

## C.1 Password Guessing Attack Comic Prototoype

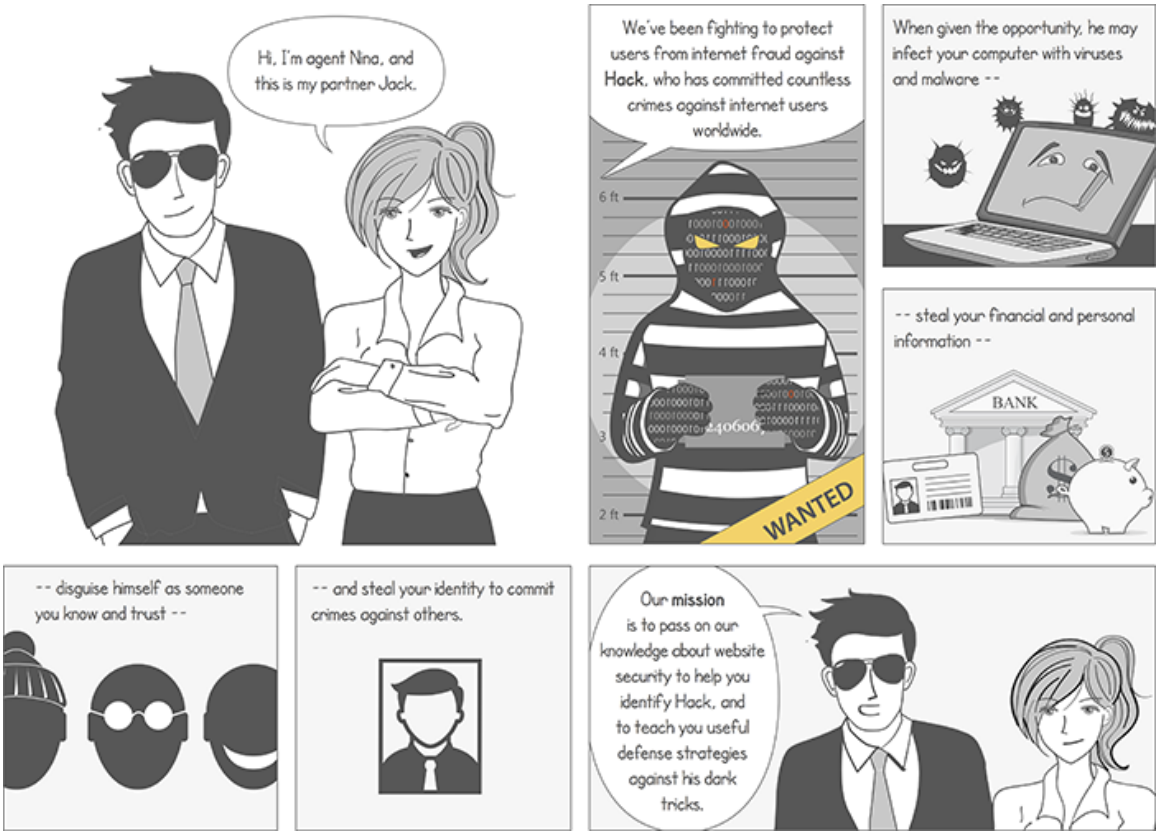



Figure C.1: Introduction common to the password and antivirus comics

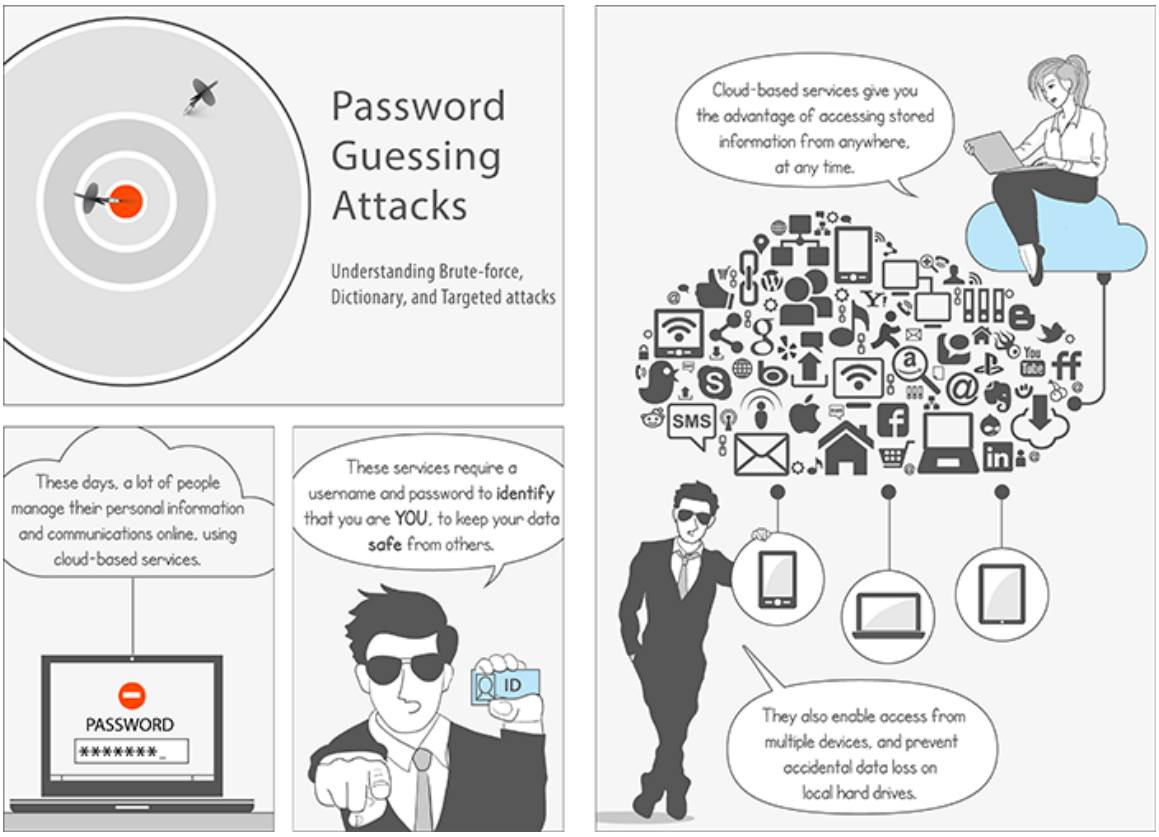



Figure C.2: Password comic: page 1 of 13

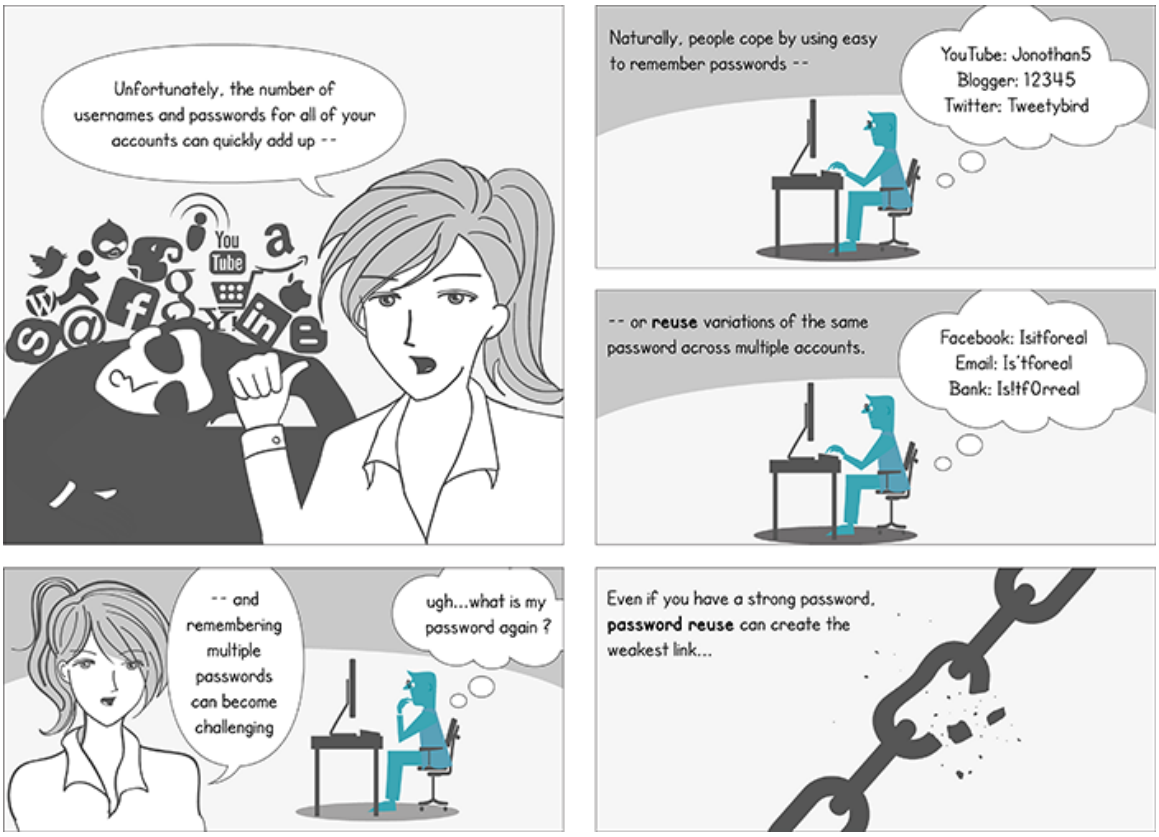



Figure C.3: Password comic: page 2 of 13

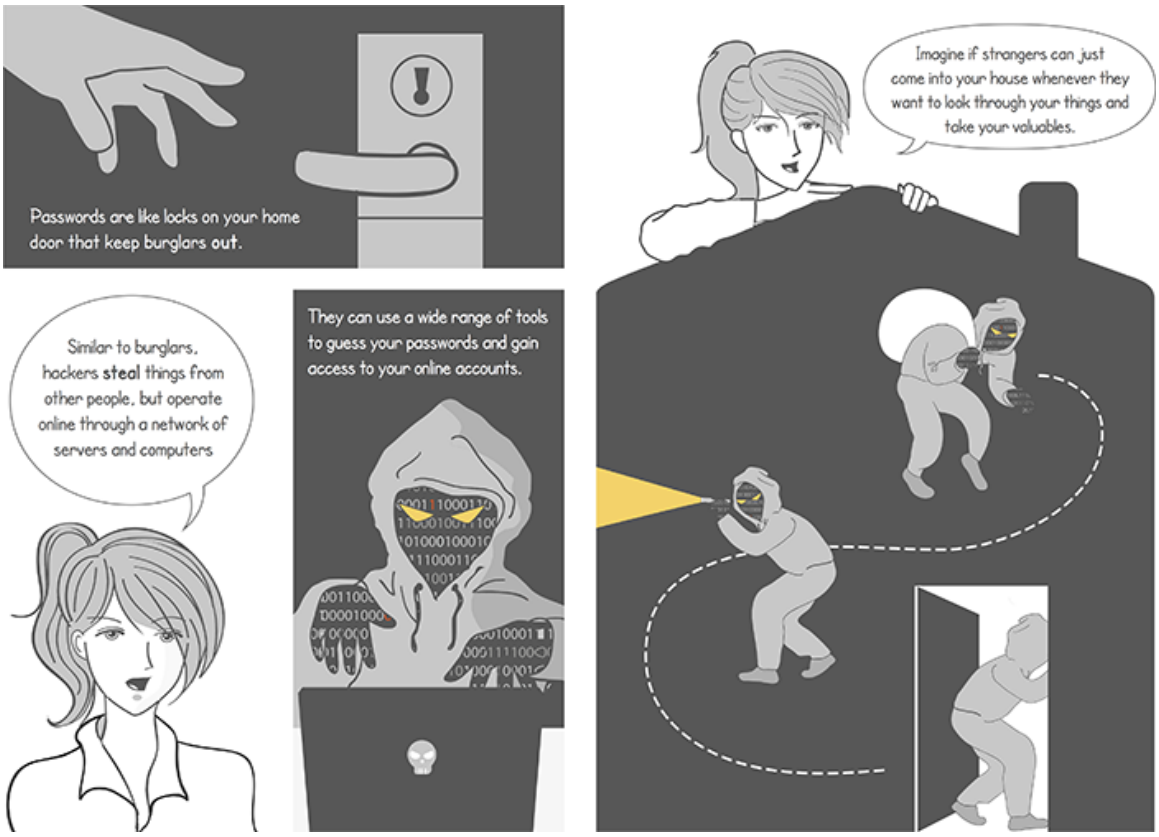



Figure C.4: Password comic: page 3 of 13


Figure C.5: Password comic: page 4 of 13

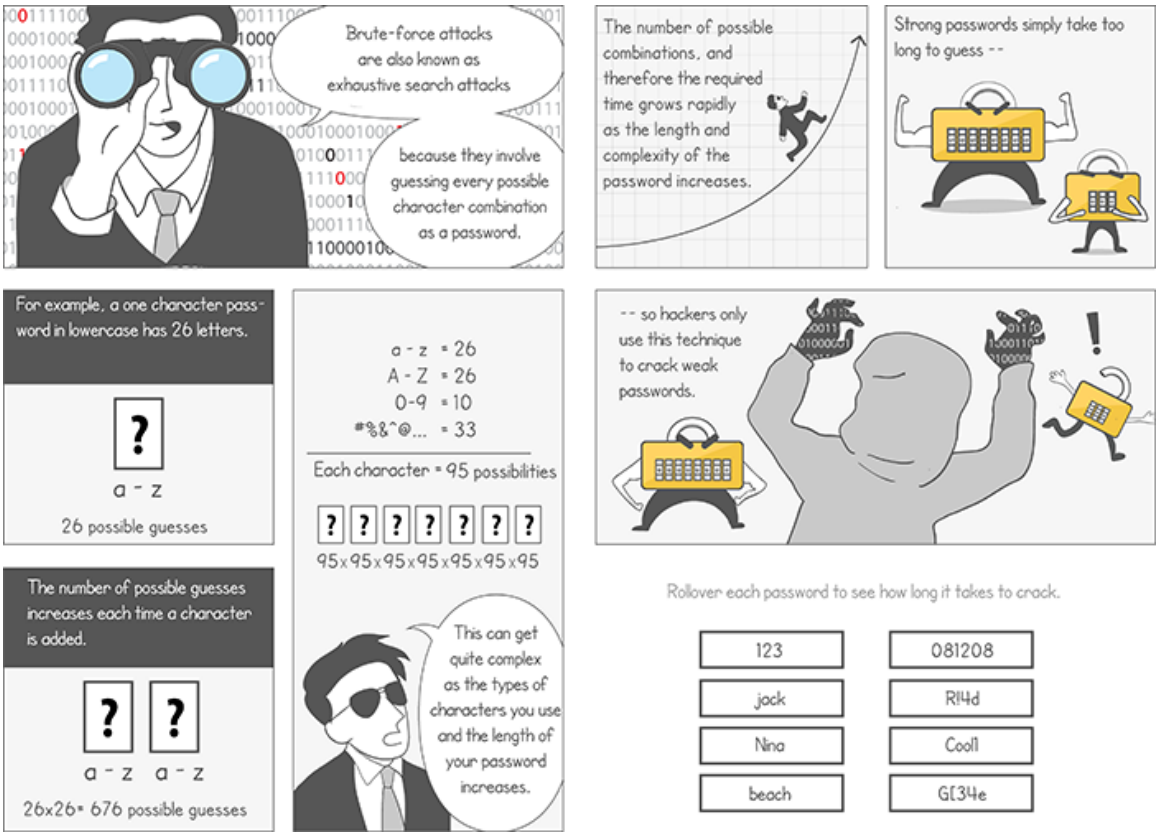



Figure C.6: Password comic: page 5 of 13

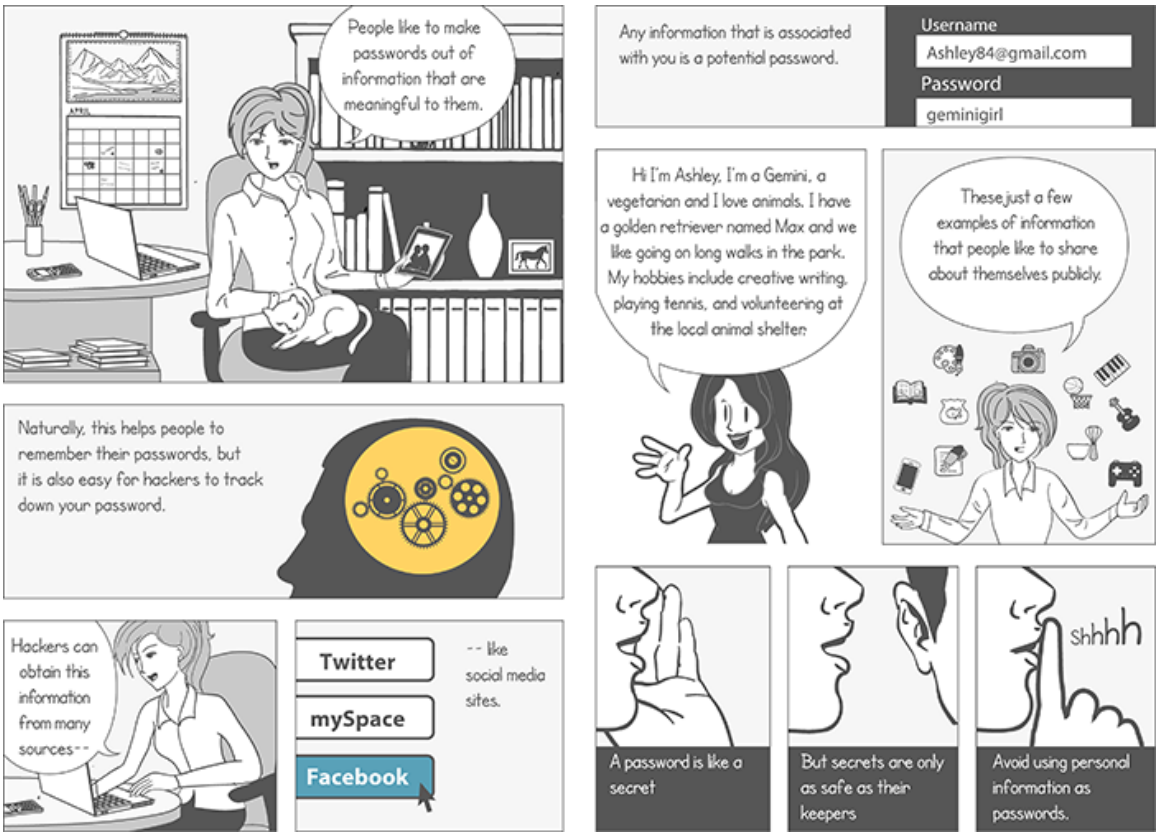



Figure C.7: Password comic: page 6 of 13


Figure C.8: Password comic: page 7 of 13

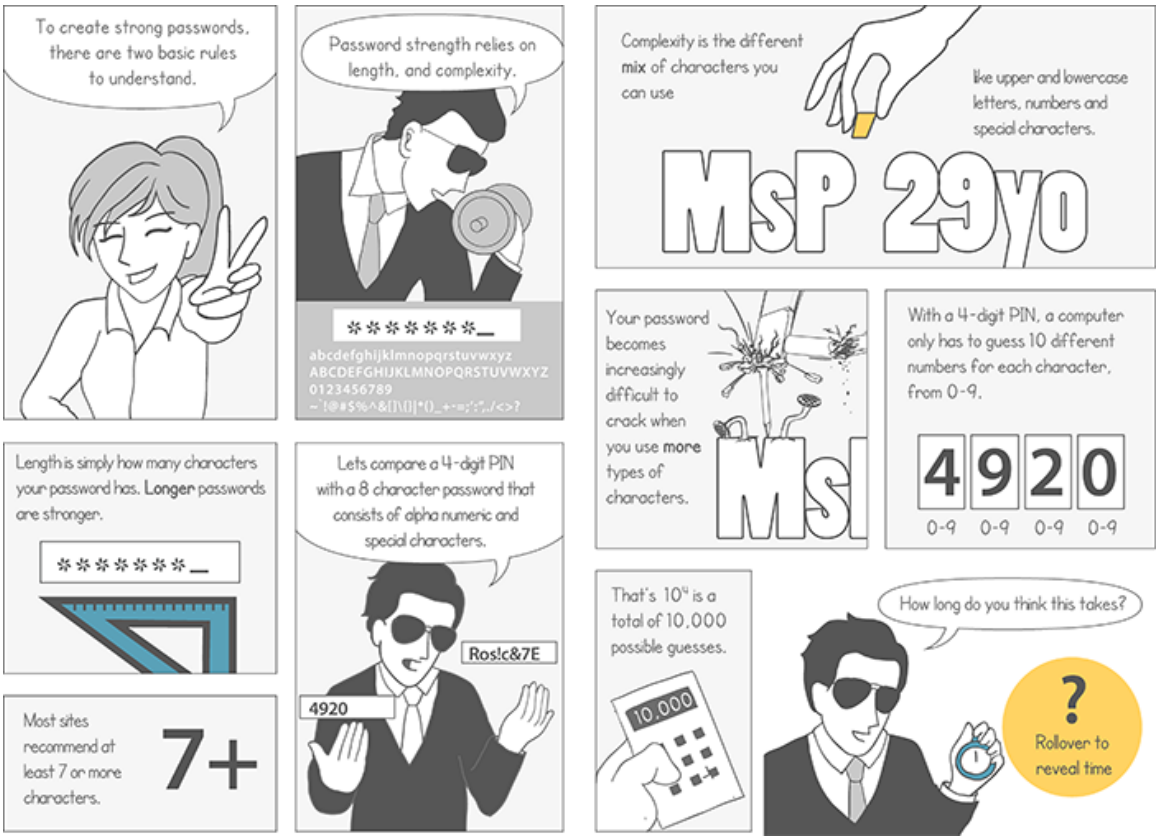



Figure C.9: Password comic: page 8 of 13

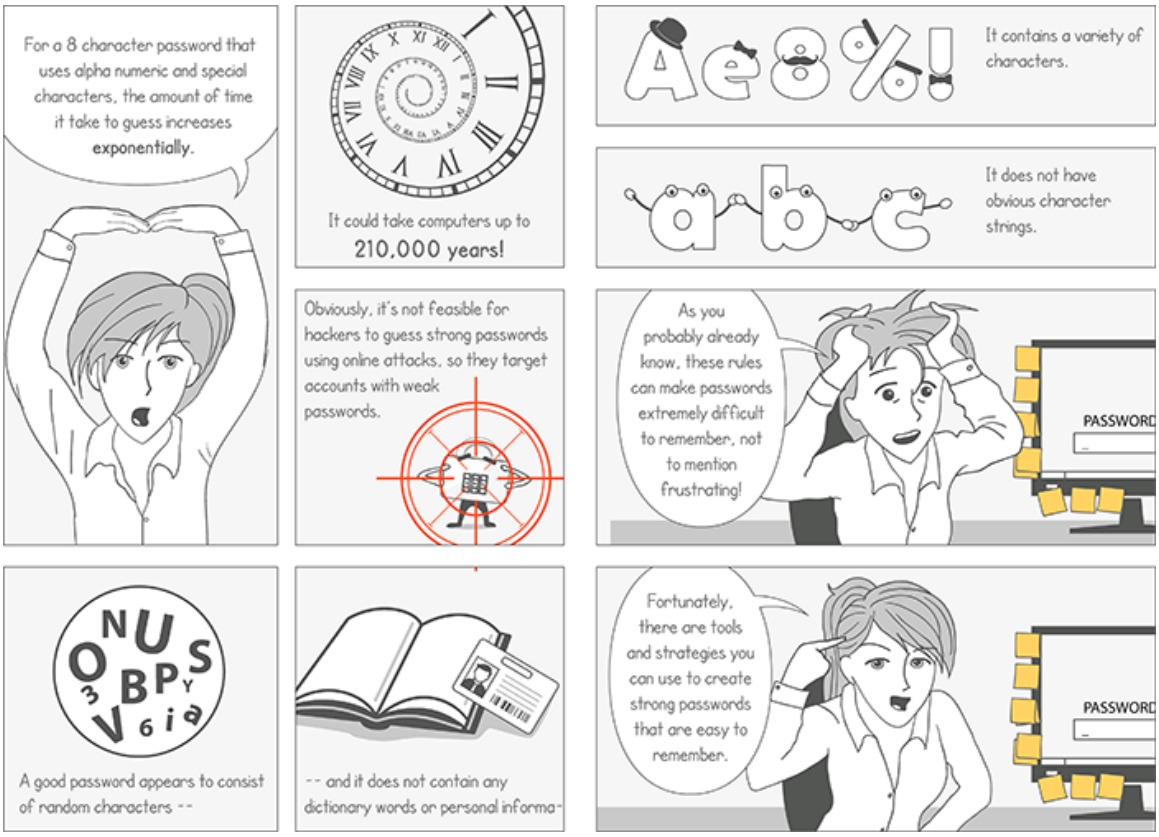



Figure C.10: Password comic: page 9 of 13

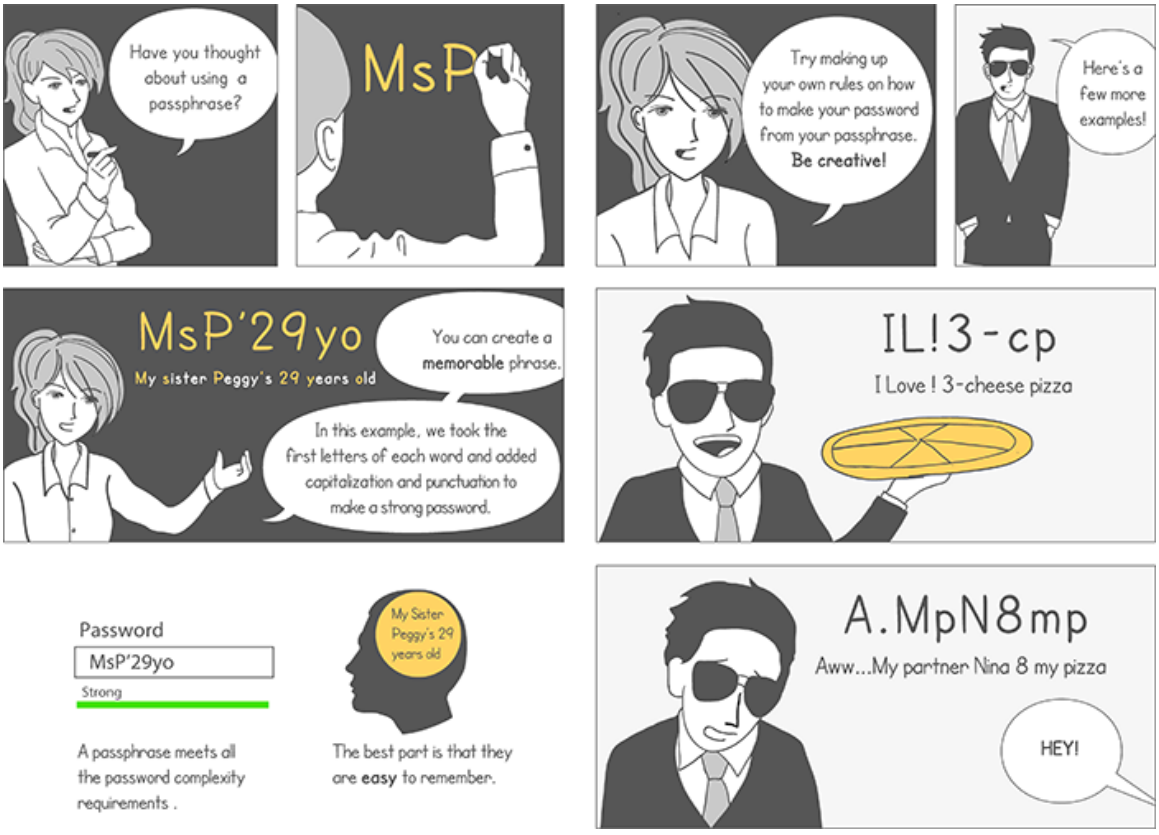



Figure C.11: Password comic: page 10 of 13

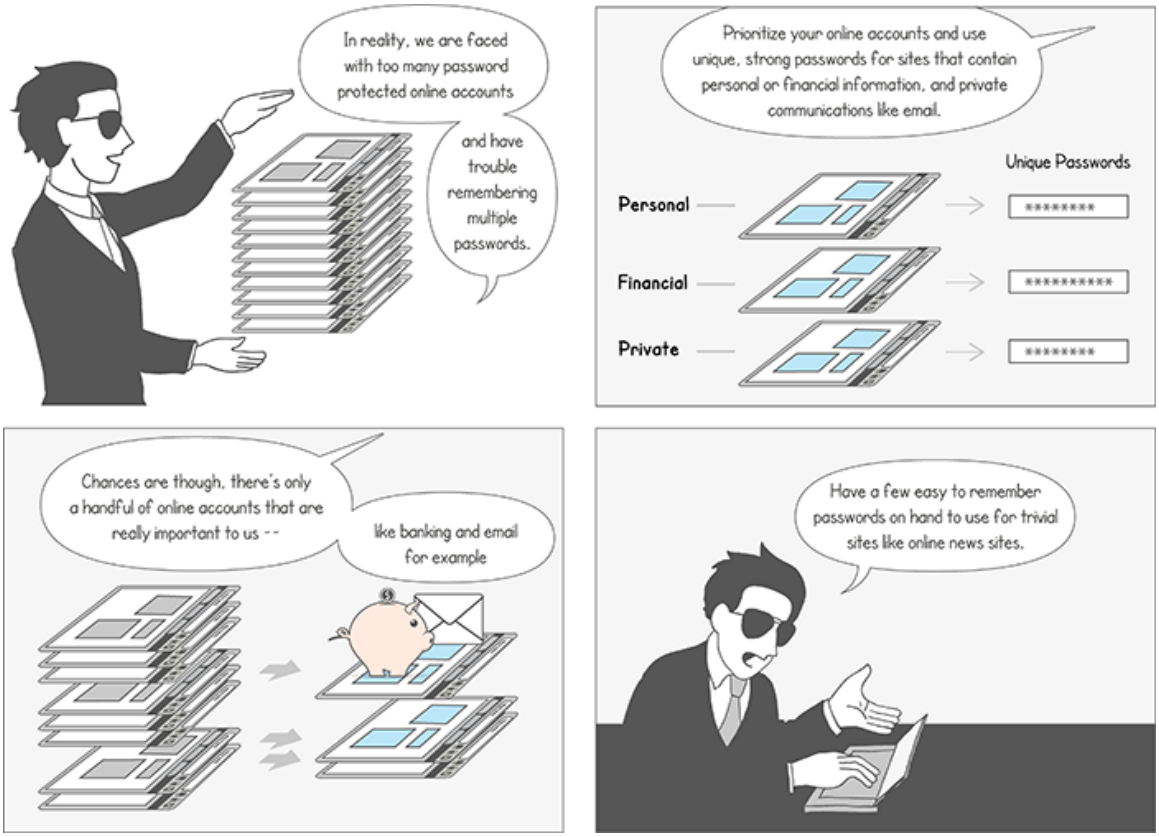



Figure C.12: Password comic: page 11 of 13


Figure C.13: Password comic: page 12 of 13


Figure C.14: Password comic: page 13 of 13

## C.2 Antivirus Protection Comic Prototype

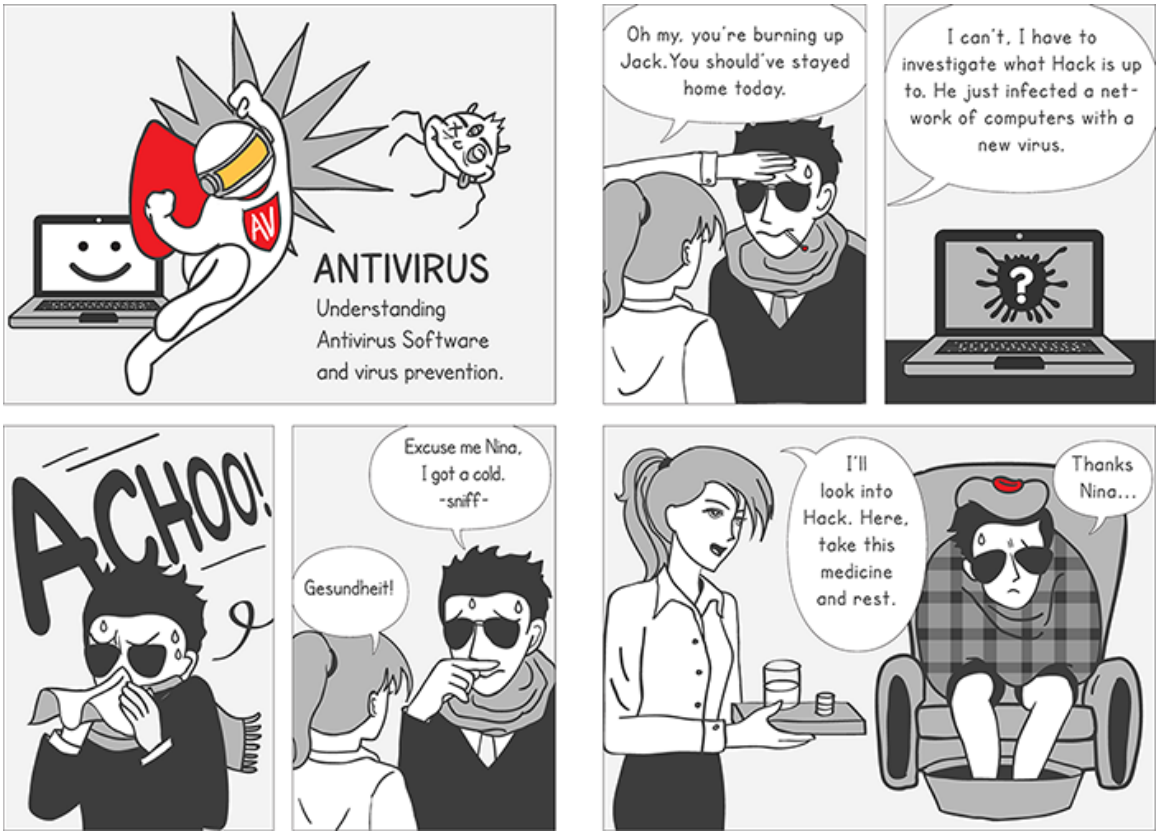



Figure C.15: Antivirus comic: page 1 of 9

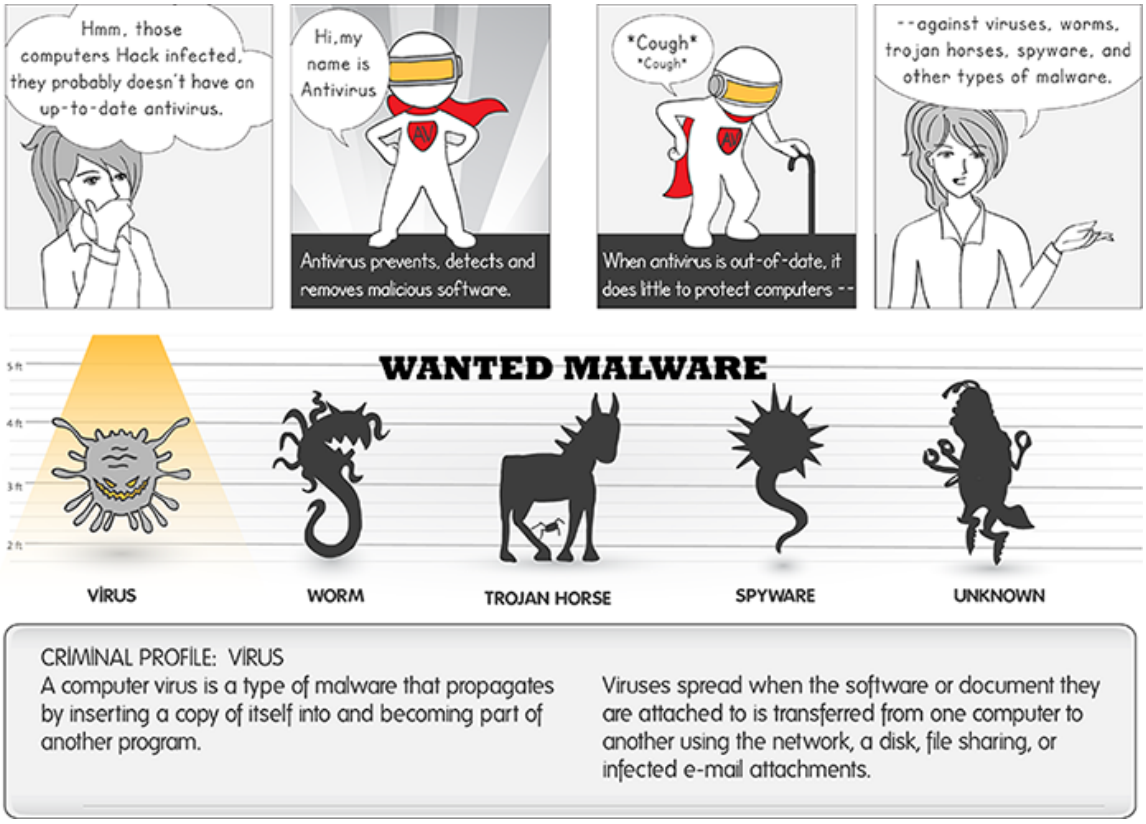



Figure C.16: Antivirus comic: page 2 of 9

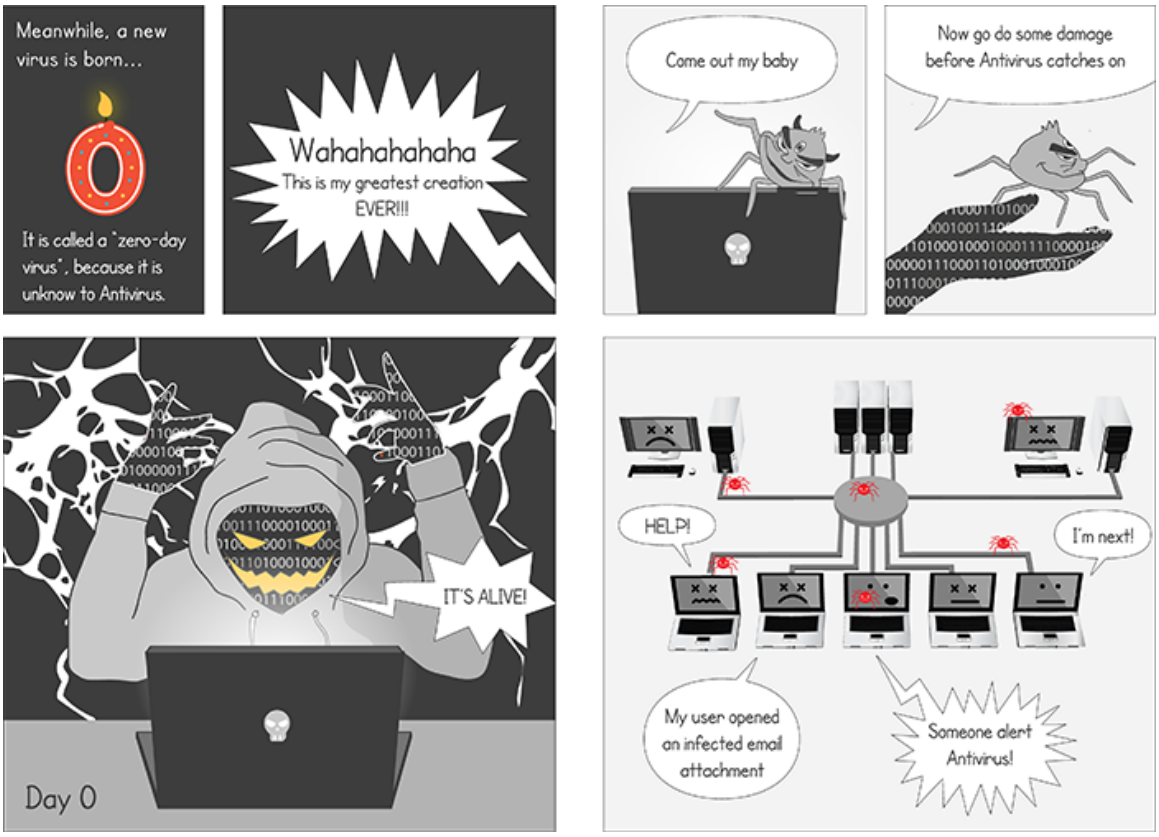



Figure C.17: Antivirus comic: page 3 of 9

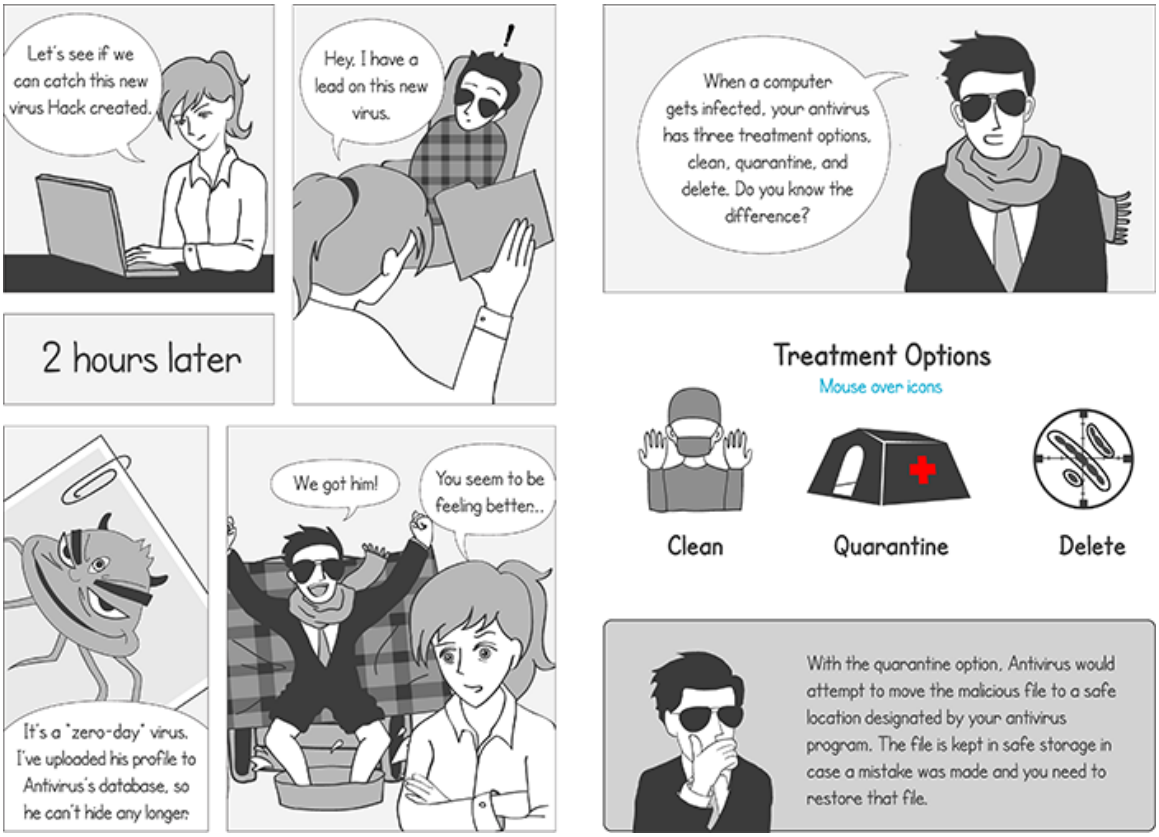



Figure C.18: Antivirus comic: page 4 of 9

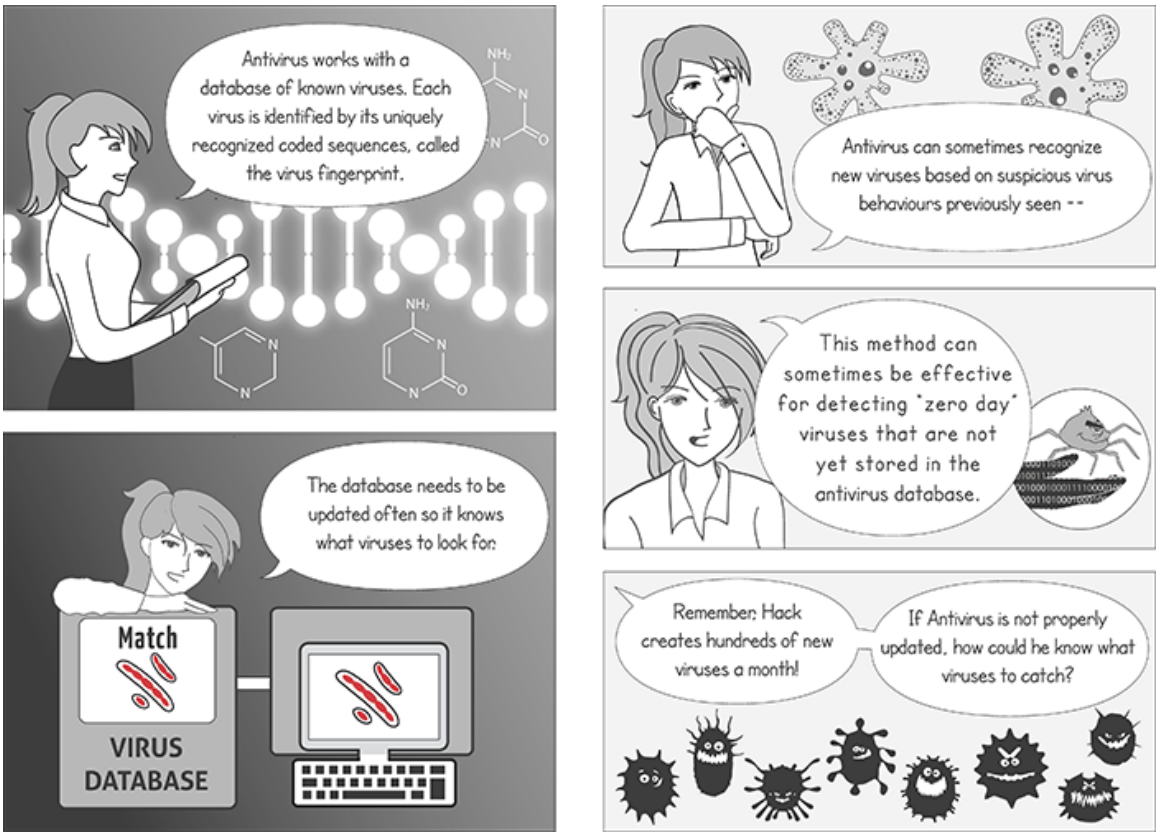



Figure C.19: Antivirus comic: page 5 of 9

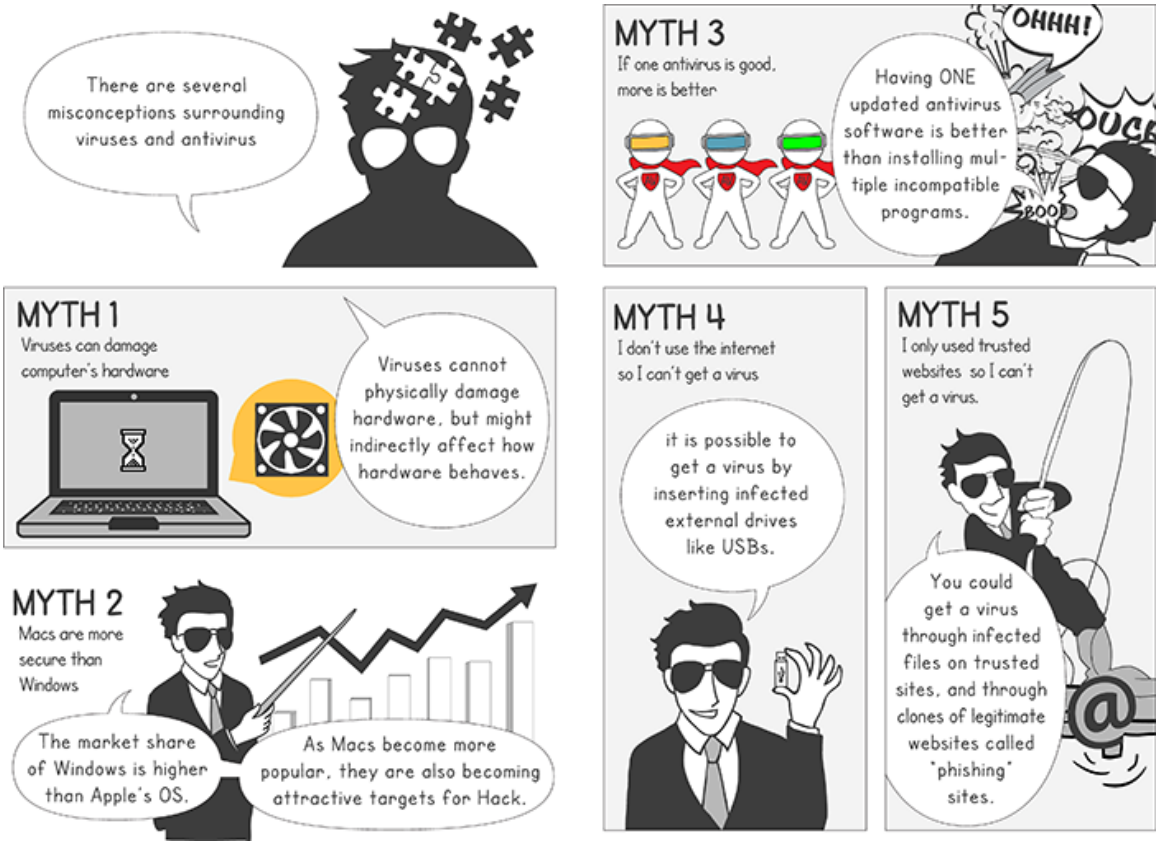



Figure C.20: Antivirus comic: page 6 of 9

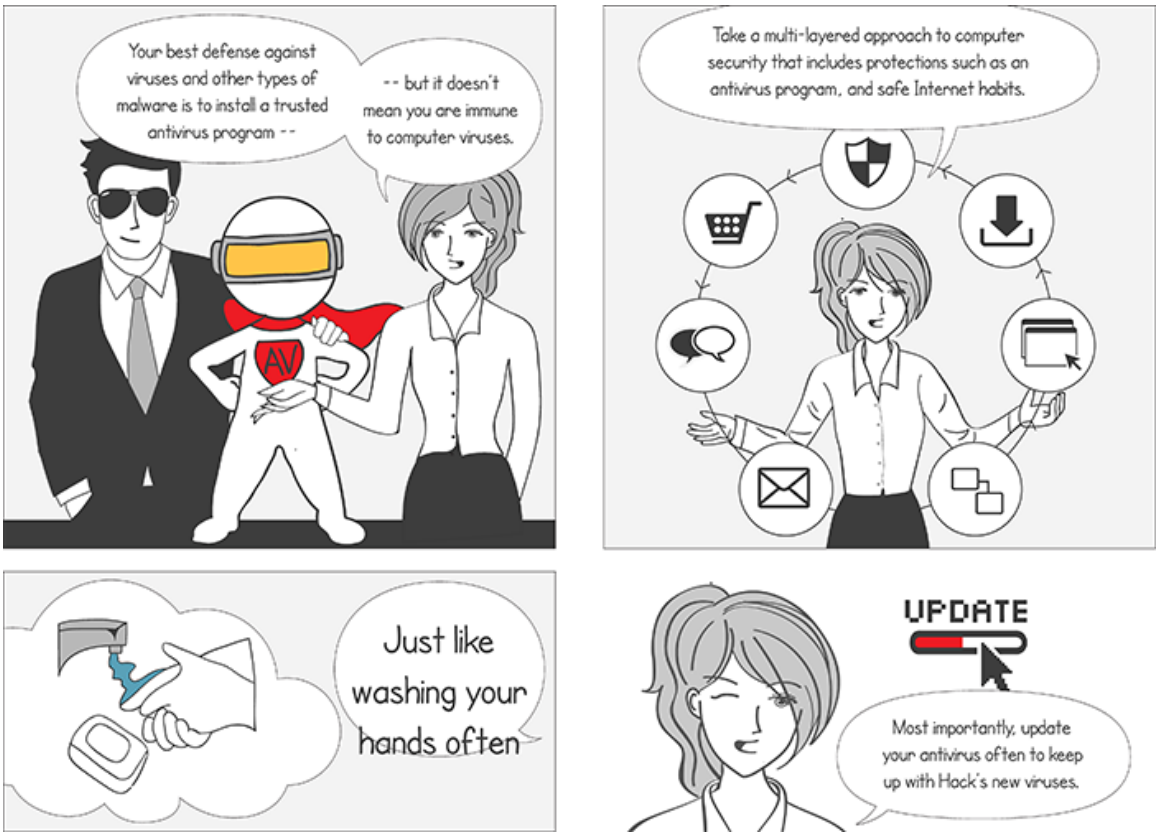



Figure C.21: Antivirus comic: page 7 of 9

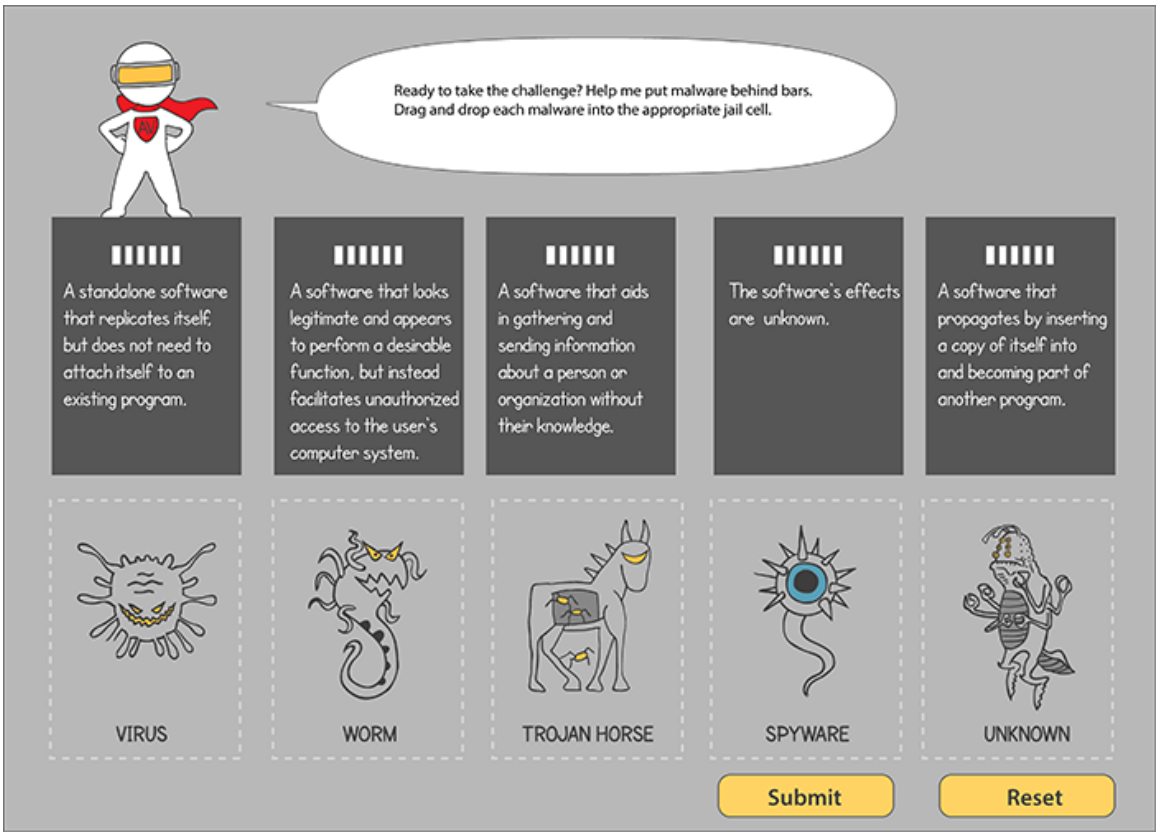



Figure C.22: Antivirus comic: page 8 of 9

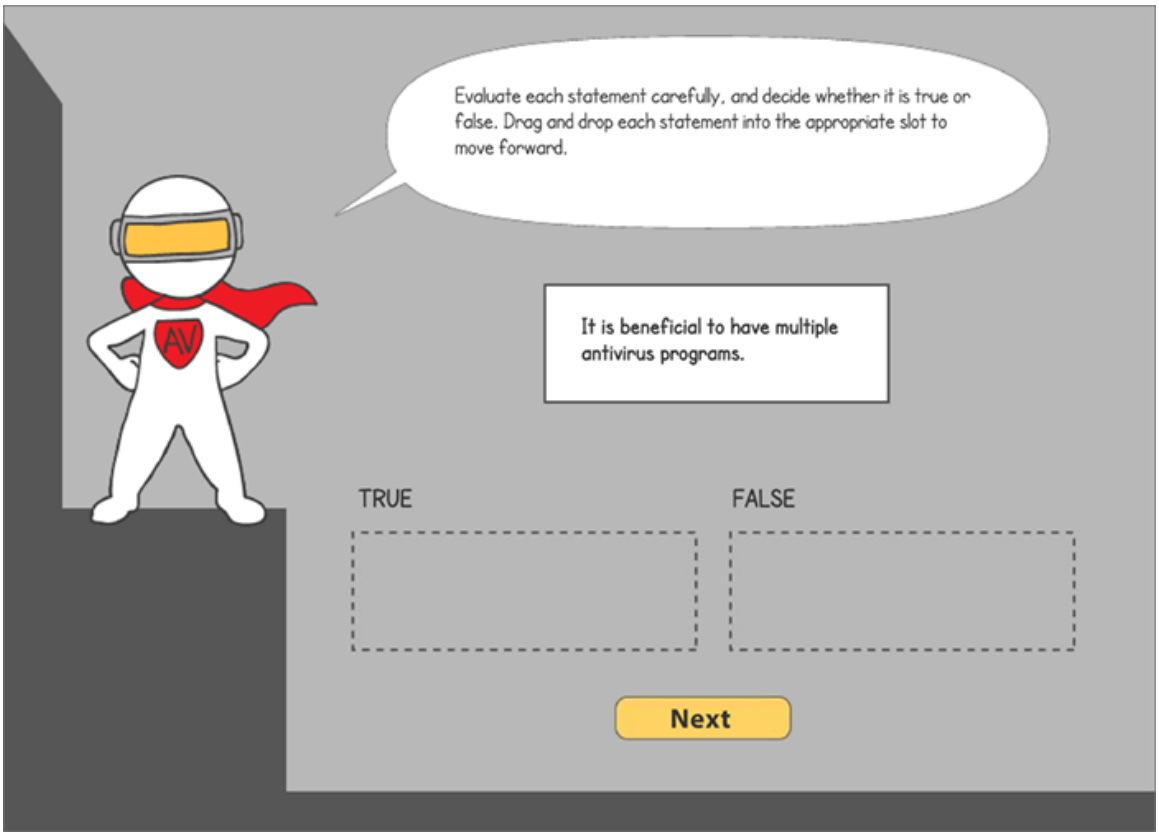



Figure C.23: Antivirus comic: page 9 of 9