Replication: Effects of Media on the Mental Models of Technical Users

Khadija Baig, Elisa Kazan, Kalpana Hundlani, Sana Maqsood, Sonia Chiasson
Carleton University
[*KhadijaBaig, ElisaKazan, KalpanaHundlani, SanaMaqsood*]*@cmail.carleton.ca*
chiasson@scs.carleton.ca

Abstract

Media has been observed to influence users' mental models in several domains. It was recently demonstrated that fictional television and movies have a strong influence on non-technical end users' mental models of security. We extended this study to explore its effect on 23 participants with technical backgrounds, given that misconceptions amongst this group could have important organisational impacts or could influence other non-technical end users. Our qualitative analysis reveals that technical participants sourced their mental models from both their academic or professional lives and from different forms of media (like news, cinema, forums, and social media). They were capable of identifying unrealistic depictions of hacking in the provided video clips and most could offer simplistic explanations about why these were problematic. We found that they generally had more nuanced understanding of the issues than non-technical end users, but they were not immune to misinformation from mass media.

1 Introduction

Users are regularly faced with decisions that impact their security or privacy online. The decisions of individuals in technical roles can impact entire networks, the robustness of software, or trusted advice given to non-technical end users. Many non-technical users look to technical individuals amongst their family, friends, and acquaintances for cybersecurity advice. Incorrect mental models by technical users could directly affect an organisation, and sharing incorrect information could affect the receiver's cybersecurity attitudes and practices. For this reason, technical users need accurate mental models of online security: how computer systems work, methods of protection, and risky behaviours.

Previous studies have shown that media can affect viewers' mental models, having been successfully used as an educational tool in the past (for example, to motivate students to study science [6], or as advertisement campaigns that act as Public Service Announcements [10]). It has also been seen that mental models of online security have been influenced by media in the past [30]. Depictions of cyber-security in media often involve certain tropes: fast-paced, dramatic depictions of hacking, use of technical jargon, decryption that occurs in a span of seconds, and cyber-security attacks mostly happening to large organisations, or individuals with wealth [20, 35, 36].

Incomplete, inconsistent, or inaccurate mental models of cybersecurity can lead non-technical end users to make negative decisions about how they handle their security and privacy online; for example, feeling that SMS and landline phone calls were at least as secure as end-to-end encrypted communication [2]. To understand how non-technical end users evaluate depictions of online security in media, and the effect it has on their existing mental models, Fulton et al. [14] conducted a study with 19 participants of different backgrounds. Fulton's study confirms that non-technical end users often turn to fictional media and its tropes to fill gaps in their technical knowledge. Participants often did not have enough technical knowledge to accurately evaluate a scene and would turn to existing tropes to justify realism; for example, many found technical jargon to be a sign of realism. They also turned to more environmental cues to inform their judgements, evaluating the perceived realism of the situation and characters, and drawing parallels to their own personal experience.

One would assume that users from technical backgrounds would be better informed in this domain, but this is not always the case. Computer Science students and developers alike have been found to have limited understanding of privacy and online security practices [5, 15, 34]. Given that Fulton's study did not control for technical expertise [14], we extend this study with users who have a technical background.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

23 participants took part in our study, which followed the protocol of Fulton et al. exactly. We conducted 60-minute sessions, consisting mainly of an interview supported by video clips of hacking portrayed in popular television shows or movies. In addition to the questions from the original study, we asked participants about their technical background. While there are several studies on looking at users' mental models of the Internet and cybersecurity [3] [40], to the best of our knowledge this is the first study exploring the effect of fictional television and movie media on technical users. We found that technical participants had more complete mental models of hacking and security than non-technical end users. They were generally able to assess the realism of hacking in video clips, but they still had misconceptions, and believed at least some of the inaccurate depictions presented.

2 Background

We discuss existing mental models of security, the effect these mental models have on software security, and the role media plays in information propagation overall.

Mental models of security: Online security is often linked to several digital systems and tools, such as anti-viruses, firewalls, encryption, and web security. When looking at users' mental models of computer security warnings, Bravo-Lillo et al. found that users with greater technical knowledge had more complex mental models than non-expert users [7]. Raja et al. found that users with higher levels of security knowledge often understood the general functionality of a firewall, but were unable to address key parts of its functionality (for example, being unable to identify the effect of choosing a network in their settings) [27]. In a study looking at general mental models of the Internet, it was found that more technical and non-technical users held similar beliefs [19], although technical users did perceive more privacy threats. These beliefs included the idea that attackers only go after high-value targets, and generally are too powerful to be stopped. Assal et al. found that while several developers agreed on the importance of software security, they mostly thought of their applications as not being a worthy target for attackers [4]. These types of beliefs have been found to affect users' security behaviours [18], such as failing to take precautions against broader, non-targeted attacks [14].

Interviews with smartphone app developers reveal concern over the lack of focus on security in technical-related education, with many developers simply turning to the Internet for answers when confronted with such obstacles in their work [5]. Similar sentiments were seen in Tahaei's interviews [34], where Computer Science students did not have holistic perceptions of computer security. These students often drew parallels to Hollywood hacking and cited media as a source for their mental models. Tahaei's study consisted of semi-structured qualitative interviews with Computer Science students, without the use of any external media.

Redmiles et al. surveyed a broad, census-representative US population to shed light on which factors influence users' rejection or adoption of security advice [28]. It is unclear whether their sample includes users with technical backgrounds. They found that the two major sources of online security advice were media and family or friends. 67.5% of respondents cited media as a source, and 60% of the advice given by family or friends were by people with background in Computer Science or IT. With users who received advice at work, more than 50% did so from someone with IT background. The study also found, however, that users with higher internet skill were 32% more likely to use media as a source of advice. Wash and Cooper [38] found that when being trained against phishing, users are more likely to benefit from security advice if provided by a security expert, and from relevant stories if provided by a peer. Given that several users turn to their more technically versed family, friends, and colleagues for advice, it is increasingly important that technical users have a sound understanding of online security lest they propagate inaccurate advice.

Software security: Millions of users have been affected by exploited vulnerabilities in software [13], despite the existence of best practices for incorporating security into the software development life cycle [22] [26]. Companies and developers have been reported logging unencrypted data in applications [9], and storing sensitive information (like passwords) in insecure areas [12], or storing them insecurely (e.g., unhashed or unencrypted)r [9]. Many posit that if developers had better, more complete knowledge of security, developed applications would be more secure as well [25]. To examine whether developers neglect to write secure code due to their mental models, Naiakshina et al. conducted a study examining whether Computer Science students would store passwords in a secure manner [24]. Their results show that none of the students did so without explicit prompting, and often had little understanding of cryptographic APIs. Students justified that if this was code being written for a real application, they would have done so without prompt. The study was repeated with freelance developers, who were hired to write code for what they believed was a startup-company [23]. These participants also mostly wrote insecure code either unless prompted, with several having misconceptions of password storage security and interchangeably using the terms *hashing* and *encryption*.

Role of media: The effect of media on the consumer has been noted in non-security related contexts, such as promoting knowledge of disease and healthcare. For example, Hether et al. found that exposure to breast cancer storylines affect users' attitudes and behaviours' to the illness, with exposure to multiple storylines being more effective than exposure to a single one [17]. Fulton et al. observed a similar effect on users' cybersecurity knowledge, and discussed how certain media events influence mental models of online security [14]. This further influences user behaviour, like whether they ignore obvious security practices based on the belief that there is no

Table 1: Technical experience. Numbers indicate count of participants per category.

Occupation	Student	10
	Project Manager	2
	IT	3
	Web Developer	1
	Software Developer/Engineer	2
	Network Maintenance	1
	UX Designer	1
	Instructor	1
	Retired	1
	Prefer not to answer	1
Programs of study	CS	9
	Engineering	7
	Business	2
	HCI	1
	Applied Science	1
	Project Management	1
	Prefer not to answer	2
Security exposure	None	10
	Work	6
	Study	4
	Study and Work	2
	No answer	1
Cyber-challenges	Completed	5
	No exposure	18

point. Conversely, the study also found that media could have positive effects on mental models if done correctly. We use their study protocol to evaluate how much media affects the mental models of technical users in this domain.

3 Methodology

Our methodology follows that of the Fulton et al. study [14], with extra questions in the post-test questionnaire. The interview script, post-test questionnaire can be viewed in the Appendix. The study was cleared by our Research Ethics Board. We pilot tested the study with an undergraduate Computer Science student who had reasonable knowledge and experience in cybersecurity; no changes were necessary.

3.1 Recruitment and Participants

Participants were recruited[1] via posters placed around our University campus. The study was also posted on a social media page advertising research studies by the university, and on online service-exchange platforms. We also used snowballing techniques. The eligibility criteria were: (1) being at least 18 years of age, (2) being fluent in English, (3) having normal or corrected vision, and (4) having a technical background.

[1]Note: the study was conducted before the COVID-19 pandemic.

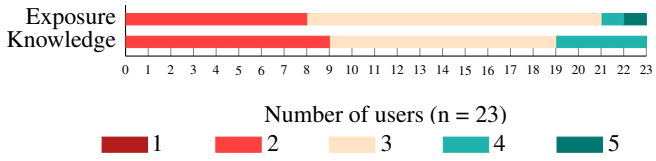

Figure 1: 5-point Likert-scale responses to cybersecurity exposure, knowledge (1 = none; 5 = very high)

We define "technical background" as having academic, work-related, or self-taught exposure to and experience in technical activities. This would include the field of Computer Science, Information Technology (IT), and Systems, Software, and Computer Engineering. It would also include IT and software project managers, freelance, and self-taught programmers. Participants were paid $15.

We initially recruited 26 participants (detailed demographics in Appendix A) but three were excluded due to an error during recruitment. This left us with 23 eligible participants: 11 identified as female and 12 as male. Excluding a participant who preferred not to answer, ages ranged from 18 years to 65 (M = 30.78, SD = 13.09).

All participants had completed post-secondary education. The majority had completed, or were enrolled in, either an undergraduate (n = 16) or a graduate degree/certificate (n = 6). Table 1, and Figure 1 provide more detail on participants' technical backgrounds, including their self-reported exposure (how often they hear about or discuss cybersecurity) and knowledge of cybersecurity (how much they know about cybersecurity). Participants generally reported similar levels of exposure and knowledge, only ever varying by one point.

Participants read and signed a consent form explaining the purpose and procedure for the study, and provided permission to be audio-recorded. Participants were assigned a pseudonym (e.g., P1-S3, P2-S3) that was not linked to their identity. The appended letters indicate participants' self-reported cybersecurity exposure: S1 (None), S2 (A little), S3 (Some), S4 (High), and S5 (Very high).

3.2 Procedure

The study involved completing an online screener questionnaire, followed by either an in-person or remote study session for those who qualified. All questionnaires used in the study were hosted on Qualtrics [2]. The questionnaires had a "prefer not to answer" option available for all questions.

Screener Questionnaire: Prior to being booked for a study session, potential participants completed an online screener questionnaire to assess eligibility. The screener had its own consent form embedded in it.

[2]https://www.qualtrics.com/

Study Session: Qualifying participants were invited to complete a 60-minute session which was audio-recorded with the participant's consent. In-person sessions were completed in our lab. Participants could also complete the study remotely through video-conferencing (e.g., Skype or Google Hangouts). The study session consisted of an interview and a questionnaire. During the interview, participants watched 6 different video clips and evaluated their perceived accuracy.

3.3 Interviews

The interview protocol mirrors the study by Fulton et al. [14], and is as follows:

Mental models: Participants answered questions to help assess their existing mental models of cybersecurity, hacking, and encryption.

Personal experience: Participants described incidents where they, or someone they knew, were being hacked.

Prior media exposure: Participants recalled whether they have seen any, or knew of, fictional TV/movies that contained content related to cybersecurity, hacking, and encryption.

Video clips: Participants watched 6 video clips. At the end of each clip, they answered: (i) whether they could identify the media or the scene, (ii) with a summary of the video clip, (iii) what they found realistic, and (iv) what they found unrealistic.

Realism in media: Participants described their general perceptions of (i) how realistic they find media in portraying these topics, (ii) media that portray these topics realistically, and (iii) media that portray these topics unrealistically.

3.4 Video Clips

We used the same video clips as the original study [14]. These were selected from television programs and movies to cover a wide variety of scenarios, tropes, and levels of realism.While we provide the source of the clip in the following descriptions, participants saw only the video clip without context of where it originated. Videos were played in random order.

1. Superman 3: An employee is disappointed with his first paycheck. A colleague tells him that in every big corporation, there are half-cents left over, but only the computers know where they go. Inspired by this, the employee stays after work and successfully hacks the system by typing in *Override all security*, and then using the command *Reroute all half-cents to above account* to add to his paycheck.

2. The Amazing World of Gumball: A blue and a pink character reach a locked door in a building with a computer terminal next to it. The blue one worries that they can't get in, but the pink one reassures him that she can break through. She types in the letters H-A-C-K, and presses enter. This opens the door, and the blue character is surprised. The pink character reveals she was joking, and explains in very technical terms how she actually hacked the door.

3. NCIS: A forensic team's computer is getting hacked. Several windows pop up and flash on the screen. An agent frantically types on the keyboard while exclaiming "they've broken through the NCIS public firewall!". Another agent joins the first agent in typing on the keyboard (four hands, one keyboard). Suddenly, the screen goes black, and the two are confused as to how the hack stopped, neither believing they were responsible. They look around and notice that another team member had unplugged the computer.

4. Blackhat: a high-level government agent receives an email asking him to change his password. The agent opens a file attached to the email, and downloads a keylogger by doing so. He can now see the new password being typed in by the agent in real time. The hacker then uses these credentials to successfully log in to the system.

5. Sneakers: a blind man sits in front of a computer, and asks another man to name places that are impossible to get into. They start with the federal reserve, and when they bring up its website, its "encrypted", with several nonsensical characters on the screen. Several people watch as the man uses a chip to decrypt everything. He replicates this with the national power grid. He describes encryption as a series of complex mathematical problems that can be broken like any code. Another man states that this chip is *the* code breaker, able to break any kind of encryption.

6. Skyfall: Two men stand in front of a giant computer screen which displays some sort of network that is constantly changing. A laptop is plugged into their computer infrastructure, which they are attempting to hack into. One man notices the name of a station amongst letters flashing on a screen, and asks his team member to use that as a "key". After doing so, the network rearranges to form a map of London. Suddenly several doors open, and they realise they've been hacked. The laptop flashes "Not such a clever boy after all", and while one man runs outside, the other frantically unplugs the laptop from their computer systems.

3.5 Analysis

In total, we recorded approximately 24 hours of audio from the interviews. The first author manually transcribed the interviews, and returned to the audio recordings and interview notes as needed during analysis to add any missing context.

Interview data was analysed using inductive thematic analysis [11]. We iteratively analyzed and created the codebook. Each transcript was reviewed multiple times, ensuring that every transcript was coded with the final codebook.

The first author conducted the interviews and was involved in all stages of the coding process. A second researcher helped code part of the data, and then left the project. A third researcher coded the remaining data and re-coded some

prior data. The detailed process unfolded as follows (see Appendix B). While editing the transcripts, the first author noted any initial themes occurring in the data. These 9 initial themes were then used as the basis for the first codebook. The first author coded two transcripts with this set of codes, then iteratively revised the themes until no new codes emerged, resulting in a second codebook consisting of 16 high-level themes and 87 sub-codes. This second codebook was used in the initial thematic analysis of the first ten transcripts by the first author.

The first author and a second researcher then coded three new transcripts together, and revised the codebook, resulting in a third codebook. The researchers then re-coded the 3 transcripts individually, as well as 3 additional transcripts, upon which a fourth and final codebook with 17 high-level codes and 95 sub-codes emerged. The percentage agreement between the two researchers for the codes on the overlapping transcripts was 98.67% overall.

A third researcher then continued the analysis process alongside the first author. The first author and the third researcher coded 3 transcripts individually using the fourth codebook, and met to clarify any misconceptions. No further revisions to the codebook were needed. Agreement between the two coders on the overlapping transcripts was 99%. All remaining transcripts were analysed or revised using the fourth codebook: the third researcher independently coded an additional 7 transcripts, and revised the codes for 10 transcripts. The first author also coded a further 3 transcripts.

4 Results

We found no overarching connections between technical backgrounds and mental models. After completing the analysis, we grouped participants based on their technical background (e.g., Computer Science, Project Management, Computer Engineering). We then compared results between group. This process was repeated with security knowledge, and security exposure. No patterns emerged in any of these comparisons. Given our small sample size (n = 23), we did not conduct statistical analysis. We present the results of our qualitative analysis, focusing on the main themes arising from the data.

4.1 Existing Mental Models

We first discuss participants' initial mental models and impression of how hacking is portrayed in the media, as described by participants *before* they viewed the video clips.

4.1.1 Profile of a hacker

Hacker persona: Many participants distinguished between ethical and malicious forms of hacking, acknowledging that a hacker could be hired by a company to ensure that their networks remain secure instead of having malicious intentions. Participants' main focus, however, was on those with malicious intentions.

Rather than having their own agenda, malicious hackers were believed to have been hired by others. Some participants explained that malicious data breaches were committed mostly by individuals who had been hired by an external organisation or a national agency, although they were unclear how this process unfolded. For example, P25-S2 expresses: *"a lot of people say they come from organisations overseas. I'm not sure how they'd find each other though; maybe through networks and contacts"*.

Hackers as individuals are mostly seen in a negative light. These were intelligent persons who had malicious intent, who were misguided, or who were suffering from psychological or social challenges. Hackers were described as users who enjoy the challenge of "code cracking" and problem-solving. Some users identified them as misfits or "outcasts" (P1-S3), suggesting they have "a psychological problem" (P22-S3), have "graduated from other forms of crime" (P19-S4), or have malicious intent. A few participants categorised hackers as thrill seekers, or power hungry, perhaps with the intent of creating a *"legacy that withstands time"* (P22-S3). Hackers might also simply be looking for a sense of community, perhaps in an attempt to fit in with a current friend group, or in search of a support network. P22-S3 distinguished between hackers who are "certified" and those who are self-taught, saying *"people who are self-taught are more dangerous; the intention to learn hacking is to go hack someone, otherwise I don't see the need for it"*.

A few participants viewed hackers with a sense of admiration. Hackers were individuals with tremendous skill. They were acknowledged as *"brilliant"* (P6-S3), *"talented"* (P6-S3, P10-S3) and *"intelligent programmers"*(P9-S3). This could possibly be justified based on certain characteristics of hacking seen in the media, like the speed or simplicity with which hacking occurs. As P14-S3 states: *"hackers are intelligent people, and their number of tries (to hack in) is probably way less than normal people. They can do things you can't even imagine"*.

Considering its general portrayal in media, some participants viewed hacking as a storytelling device that the media uses to convey to the audience that the character is *" smart or technical"* (P22-S3). Others expressed doubt over their portrayal: *"if it was the (hacker's) first try (hacking in)... no one's that much of a genius"* (P10-S3).

Hacker motives: Participants acknowledged money or information as a hacker's primary motives, and identified organisations (private and governmental) as the main intended targets since these were viewed as leading to higher rewards. P4-S3 also highlighted how newer companies or systems are more likely to get hacked: *"They haven't been around long so maybe they don't know who they need to be wary of"*. Hacking was viewed as a threat that organisations could learn to avoid with experience and attention. Three participants

considered individual persons to be secondary victims of an organisational breach: while not a direct target, the breached organisation's employees and customers were ultimately personally affected by breaches as well.

In cases where individual persons were noted as targets, three reasons were considered by participants. First, the target was a high-profile individual (n = 6) whose data could bring monetary or reputational rewards to the hacker. Second, participants thought that attacks could occur against random individuals (n = 4) and that the victim was simply the unlucky recipient of misfortune. And finally, participants noted that data breaches could be done for the purpose of *'stalking'* (P1-S3), and that this could occur towards someone the hacker personally knew, or towards an unfamiliar person if the hacker simply found a way to follow the victim's *'routine'*(P5-S5). Some level of victim blaming was apparent. Many felt that inexperienced users of the Internet, or those simply gullible by nature, would be targeted. As a participant explains: *"It's done to whoever seems most accessible... someone who signs up to a lot of things"*(P2-S3).

4.1.2 Human factors

When asked what makes someone an *easy* target for a hack (as opposed to *intended* target), all responses related to user behaviour or human factors instead of characteristics of the technology being used. More than half of participants (n = 13) expect *vulnerable* users to be the easiest targets. Vulnerability was often linked to inexperience, either due to age, general inexperience with technology, or general gullibility.

P5-S5 highlighted the effectiveness of social engineering for phishing, suggesting that anyone could become vulnerable under certain circumstances: *"Tired people who want to relax at the end of the day are more susceptible. People who multi-task and just want shortcuts could also gloss over a moment that could make them slip"*. With this quote, we note an underlying belief that the victim could have prevented the attack had they been more careful, partially holding the victim accountable for the attack. We found that this belief was pervasive and participants cited various security *behaviours* that could make users targets, such as having bad password habits (n = 7) (e.g., easy passwords, repeated use of passwords), not using certain security tools (n = 7) (specifically antivirus software, firewalls), and browsing the Internet carelessly (n = 6) (e.g., accessing sensitive information over public WiFi, visiting *"unhealthy"* (P10-S3) websites, not being careful when clicking on content online).

Most users who mentioned the victim's age as a factor considered the elderly to be most at risk. However, it appears that participants considered users at both extremes to be particularly vulnerable to hackers. P26-S2 mentioned "young kids who don't know they're giving away information that could make them easy targets", feeling that it would be "easy for people to trick them into dangerous situations".

4.1.3 Perceived origins of mental models

Many participants (n = 14) cited their academic or employment background as the primary source for their mental models and understanding of hackers. Some participants (n = 2) also cited their experience with cyber-challenges as affecting their perception: *"(Hacking) reminds me of cybersecurity challenges. It's just problem-solving; you either crack into it or you don't."* (P3-S3). Participants (n = 9) also did research of their own in cybersecurity (like reading articles online), and voluntarily engaged with others (family, colleagues, friends) on the topic: *"I've talked to people who are very interested in these kinds of things, and try to mimic being in the mind of a hacker"* (P5-S5).

Despite saying that media was generally an unreliable source of information, participants recognized that media played a significant role in forming of their mental models of hacking. Fourteen participants identified that their perceptions came from some form of media. Fictional TV or movies (n = 8) were noted as an important source of information. Online sources such as blogs, forums, Social Networking Sites (SNS), and YouTube (n = 14) were also mentioned. One participant explained: *"I watch horror stories on Youtube, and there's usually a hacker in there; that's where my perceptions of the deep web came from"* (P9-S3). News reports about *'data breaches'* or *'identity theft'* (n = 9) also commonly informed participants' mental models of cybersecurity and of hacking.

We noticed how these sources may have informed participants' responses, even prior to them watching the videos. For example, several participants identified a trope in crime/spy-based media, where there is often a technical person on the cast who responds to, or conducts, hacking. While participants generally said they believed these tropes to be inaccurate, their influence was suggested throughout the interviews. For example, when asked about a hacker's goal, P26-S2 responded *"I'm really into [detective show]: maybe in a hostage situation, you'd hack people to use their information to get people to act a certain way"*.

4.2 Characteristics of Realistic Media

In the second half of the interview, participants viewed each video clip and framed their responses with respect to the clips.

More than half of participants (n = 14) found the video clips to be heavily inaccurate. However, the clip from Blackhat was described as *"refreshing"* (P7-S2) by participants for its relatively accurate depiction of phishing. Participants' overall evaluation of each clip mostly hinged on whether the hack or defence seemed realistic. To supplement their evaluation, participants also used contextual and cinematic cues to assess realism. Several participants were critical of the speed and simplicity of the hacks, but some acknowledged that these aspects were probably *"dramatised for the audience"*.

4.2.1 Unplugging could happen but might not work

Participants' responses to unplugging the computer as a possible defence against hacking were dependent on the video and the participants' assumptions about the attack.

With the NCIS video, some reasoned that unplugging a single PC from its power source was ineffective in protecting against a network attack unless the network was disconnected as well. Others thought it was realistic, citing the commonly heard advice *"try turning it off and on again"*(P18-S2, P26-S2). A few participants clarified that this might only work if the hacker had not reached the network, while others explained that it was realistic in the context of that one specific system: *"when the system is off, how can someone hack into (it) if you're not connected to the Internet anymore?"* (P22-S3). P25-S2 observed that *"only (one) computer was being hacked, interestingly enough"*. Additionally, two participants found it unrealistic that unplugging a desktop computer would actually stop it from running. Like a laptop, they expected a backup battery to keep it running.

A similar scene was present in Skyfall, in which a system is hacked into while connected to a laptop. On realising they've been hacked, an actor unplugs the main system from the malicious laptop. Participants recognised that hackers could *"do a lot more if plugged in versus if not"* (P24-S2), and so unplugging in this case would be a *"a good move"*. However, a few were cynical of this action, unsure if *"(they'd) be able to stop it by that point"* (P25-S2).

Although no consensus was reached, participants' technical knowledge enabled them to assess each situation, reason about the conditions under which the attack may be plausible, and determine the extent of realism for themselves.

4.2.2 Hacker and victim profiles must fit

Hackers: Participants often used the characters' physical traits or personality when assessing realism. Participants relied on their own pre-conceived ideas of a typical hacker and found unrealistic any depictions that did not match their imagined hacker. In Skyfall, one character was referred to as *"a programmer dude"* (P3-S3) because he wore glasses and a sweater vest. In Blackhat, it was perceived as unrealistic that such *"attractive"* (P7-S2) and *"decent-looking"* (P6-S3) individuals could be hackers, and several found Gumball to be unrealistic because it was a cartoon, and because a little girl was a hacker. One participant, however, expected hackers to be younger individuals because they are more comfortable with technology. For example, when the main character in Gumball opens a door with the letters H-A-C-K, P6-S3 agreed that *"children can hack (in), so easily"*.

Security clearance: It was commonly believed that breaking through a system's security measures was difficult, so participants found scenes unbelievable if they perceived that the character wouldn't have adequate security clearance. For example, when Richard Pryor overrides all security access in Superman 3, participants were either suspicious or trusting based on their interpretation of his character. Some found it plausible that he would *"know the vulnerabilities"* (P20-S3) of the organisation simply by virtue of him being part of it. Others assumed he was part of the IT department ("he seems to be a programmer" (P3-S3)), and so accepted that he had some level of access. Several, however, didn't believe that *"the main character is smart enough to hack into the system and get the money out"* (P10-S3). Participants' mental models included some organisational understanding of who would have security clearance or administrator privileges, based on their own experiences, and used this practical knowledge in assessing the realism of the video clips.

Behavioural attacks: Participants were less forgiving of a victim who fell prey to phishing, especially one with high-level access as seen in Blackhat. Many believed that the scene was unrealistic because someone with that level of access would *"know better"*, and believed that anyone in that position would have received formal training addressing this topic. Some recalled their own experiences of having received similar training in the workplace. Interestingly, this contradicts participants' earlier explanation that anyone could be vulnerable due to inattention. This indicates that in contrast to non-technical end users, participants expect those handling sensitive information to not be susceptible to attacks leveraging human factors.

Participants thought that phishing attacks were unlikely to succeed in high-security organisations. Participants agreed that getting phishing emails was *"common"* (P3-S3, P16-S3) in the workplace, but explained that it *"shouldn't be that easy to get into someone's computer"* (P24-S2) and that other forms of security would separate the hacker from the system. Participant noted that security tools like firewalls and multi-factor authentication should hinder access by an attacker. Participants' technical background increased their skepticism in attacks that appeared too simple to be realistic.

4.2.3 Setting for the scene must be realistic

Situational context: Participants found cybersecurity events more realistic, when they matched the context of the organization in which they took place. Using Superman 3 as an example, P10-S3 explained: *"every company has this kind of situation where someone can hack in. A person is knowledgeable about Computer Science or networks, or does the payroll, and is knowledgeable about how to hack into other people's systems"*.

Exaggerations or obvious security lapses within the scenes triggered skepticism. P18-S2 conversely noted about Superman 3:*" I'm unsure how he's able to override the system, but the smaller scale seems more realistic"*. Similarly, in Gumball, some participants found it unrealistic that a door of high-value would be left unguarded.

Organisational values: Having the presence of several

people working together was seen as more realistic than watching a lone-wolf breach systems. For example, when watching Sneakers, P6-S3 explained *"people together trying to find a solution is realistic"*. P6-S3 was also critical of the field agent escaping at the end of the Skyfall clip, stating that no *"real leader"* would leave after a system breach. In participants' view, hacking and administering security were collaborative efforts where knowledge and responsibility was collectively shared among several individuals.

Some also found the lack of protocols in response to a system breach to be unrealistic. As P10-S3 stated: *"there are protocols or policies that need to be followed by leaders instead of running out and leaving the audience to imagine their own thing"*. This principle also applied to Blackhat, where a participant mentioned that a high-ranking organisation would probably have multi-factor authentication available for their systems. Again, participants had expectations with respect to how organisations handle security and breaches, and these were informed by their previous experiences or knowledge of how things "should be".

Timeline: Scenes set, or filmed, in the past were judged differently than those set in the present day. For example, P3-S3 found the decryption chip used in Sneakers to be unrealistic for its time because it was unlikely that this type of technology was available then. While watching the Superman 3 clip, some participants said it would be realistic for the company's systems to be insecure since *"they didn't care about cybersecurity back then"* (P7-S2). However, participants had limits to their allowances. Two participants explained that it was unlikely that systems were *"ever that unsafe"* (P15-S3).

4.2.4 Hacking is stealthy, malware is obvious

The distinction between malware and hacking was somewhat blurred by participants. For example, participants were divided on the accuracy of the NCIS scene where the system displayed several pop-ups after getting hacked. Most participants suggested that this appeared to be malware; their mental model of the association between malware and hacking determined their evaluation of the clip. If participants thought that malware equated to hacking, then pop-ups were to be expected. If participants thought hacking was distinct from malware, then the clip was a clear exaggeration.

Malware: Participants who identified a link between adware (and other malicious software) and hacking recognized the pop-ups, comparing it to their own experiences of visiting a *"bad website"* (P18-S2) or clicking a suspicious link. These participants expected obvious signs that the computer was being hacked: *"I think... malware tried to disrupt [the system]. I've never experienced this before, but I think this is what happens when a system's being hacked. It's a very astonishing thing when a system is being attacked"* (P13-S3). Another participant explained *"I can imagine, in reality, many things popping up as a system is being hacked, many things being stolen. "* (P16-S3). In these cases, the clip reinforced their (mis)understanding of how hacking typically occurs.

Stealth: Other participants were skeptical about whether a hacked computer would *"go that ham"* (P1-S3), possibly because hackers *"want to be undetected "* (P1-S3). Six participants were highly critical of the idea that a hack would have any visible effect, even if done via malware. Hackers would want to go unseen to avoid alerting the user while completing their task of interest. As P7-S2 states: *" Why would a hacker create code that would do that? To tip off the person being hacked?"*. In comparison, the Skyfall clip was more believable for this group of participants. In the clip, the hack was subtle and stealthy; the main characters mostly had no idea that they were being hacked.

Additionally, a few participants (n = 3) did not expect certain aspects of hacking to be *"broadcast to the public"* (P13-S3), for fear it might be *"dangerous"* (P13-S3). For example, a powerful decryption chip would be *"well hidden"* (P24-S2) if it existed, possibly only used by *"high profile (individuals and organisations) and underground cartels"* (P24-S2).

4.2.5 Hacking is complex

Participants expect breaching a system to be a complex process, and not just possible with *"one key-stroke"* (P3-S3). However, three participants noted an exception to this rule: breaching a system can be quick and simple if you have contacts or work for the organisation and are familiar with its vulnerabilities; in other words, insider attacks can be simple. Having a relationship with a *"higher-up"* (P10-S3) or using bribery to obtain information (P10-S3, P13-S3) would provide access to a system through relatively official channels, without need for complexity.

Participants believed organisations to have multiple layers of security in place for their systems. As such, a hacker would probably have to breach several protocols to successfully hack a system using conventional means. While Gumball was praised for its depiction by some participants, others were confused about how the pink character had enough time to truly hack in to the system while on screen. Regardless of these differences in perception, many agreed that the *"long list of things"* that needed to happen, as described by the character, were plausible.

The majority of our participants (n = 15) trusted encryption to be secure. When faced with a chip that destroyed all encryption simultaneously in Sneakers, many found it to be unrealistic. This was partially due to the hardware that would be required, with some feeling that this chip might only be possible *"in the future, maybe"* (P6-S3) and does not *"exist on this planet right now"* (P10-S3, P15-S3). One participant was entirely unconvinced: *"the amount of math you'd have to do would be... wow... in even existing or future computer hardware"* (P7-S2).

As part of a system's defence, participants expect a realistic

system to detect and log any attempted breaches. They criticised clips that showed hackers getting through undetected. Participants believe that most hacking attempts would be unsuccessful in real life. They further expect systems to flag most unauthorised attempts immediately and that these alerts would be immediately actionable by system administrators.

Two participants expressed that since not all organisations and businesses prioritise cybersecurity, some systems may actually be as simple to hack as portrayed. For example, after watching the scene in Gumball where typing H-A-C-K unlocks a door, P11-S2 expressed: *"I think a lot of places put very basic, easy passwords that are very easily guessed"*.

4.2.6 Media hacking is exaggerated, dramatised

Almost all participants (n = 21) commented on the cinematography and artistic liberties taken in the clips during their interview. Participants often expressed their disdain for cinematics, agreeing that while certain depictions *"make for good TV"* (P7-S2), they are often *"exaggerated"* (P9-S3). This includes situational context; As P24-S2 explained, they found the technology used by hackers in Blackhat to be *"too high-tech"* in comparison to the computer used by the victim of the hack, who was a government official. Other examples included the frantic hammering of keys on a keyboard, and random snippets of code flashing on the screen.

Interestingly, only five participants explicitly mentioned that two people were typing on the same keyboard in NCIS. These participants were either amused *"I don't think they're so close that they can finish each others' sentences"* (P3-S3), or instantly dismissed it as unrealistic *"Yeah, no. That's not going to work"* (P4-S3). A few others (n = 3) dismissed the entire clip as unrealistic.

4.3 Evaluating realism

Participants relied on their past experiences and their technical knowledge to assess realism.

Participants were quick to comment if they found certain parts of a video relatable. Some would draw on their technical experience to elaborate how they had *"seen this happen before"* (P3-S3, P7-S2) in the real world (either personally, or to someone else on the news). This was especially obvious with the scene involving a keylogger; 9 participants referred to real world examples. P22-S3 explained *"When you go to online support, they send you a file, and you install it and they are able to move your cursor for you, so it's possible"* (P22-S3).

Participants also used their technical experiences to dismiss certain scenes. For example, after watching the Skyfall video clip, P26-S2 commented *"I haven't experienced a program that has, once it's realised it's gotten hacked, that has a fail-safe measure to hack the hacker"*. When something technical is happening on the screen but participants don't understand it, many were confident enough to deem it unrealistic. The Blackhat clip includes a character dragging and dropping something towards the end of the scene. Participants who noticed this had *"no idea what was going on there"* (P3-S3), and responded by rejecting the premise entirely: *"It was confusing that they dragged and then a bunch of things happened on the screen. I don't know what kind of system does that stuff, so it's not too realistic."* (P4-S3). Others dismissed a scene because they became suspicious when they couldn't make sense of the technical jargon. Using Gumball as an example, P3-S3 stated: *"some stuff she said didn't seem right. It didn't connect, it just seemed like a list of things"*.

As we interviewed participants with a range of technical skills, we found that not all had the same level of cybersecurity knowledge, understanding, or past experiences. Some were able to use their past experiences and knowledge to correctly interpret the information presented in the video clips.

Others, however, were unable to do so. For example, when asked about which mechanisms hackers apply, some struggled to identify any methods beyond phishing, only stating that hackers somehow gain access to a network. When these participants were unsure of the technical nuances in a clip, they relied on their existing technical knowledge to assess its credibility, which was inadequate. Participants attempted to fill in the gaps whenever they were unsure of what was happening in the scene. This resulted in subjective interpretation of cues like technical jargon. Some participants chose to ultimately trust a scene, declaring: *"it could happen in real life"* (P13-S3); others were less committal in their phrasing, accepting that *"they seem to know what they're doing"* (P2-S3).

Others relied on their knowledge to make assumptions about feasibility. In one scene, P26-S2 felt that the *"the coding doesn't seem realistic"*. The participant then provided a counter-example: *"In The Matrix, the fact that they used binary is more realistic and the computer would understand it as opposed to human sentences"* (P26-S2). Similarly, in the Blackhat clip, a keylogger is downloaded onto an individual's computer when they click and open a PDF file. Some participants doubted this transmission vector and, as such, dismissed this threat. Similarly questionable claims were made on the topics of encryption, authentication, antivirus, and firewalls.

5 Discussion

Our study exploring the technical users' perceptions of cybersecurity in media resulted in three main findings:

1. Our technical participants appeared to have a semi-reasonable ability to assess the realism of hacking scenes. Due to their technical knowledge, they had more detailed background understanding, which they used to assess the realism of the clips. Specifically, their articulated reasons for why something was unrealistic were more detailed than those observed in Fulton et al.'s [14] study. However, an occasional gap in their mental models sometimes led them

Table 2: Comparison of non-technical end-users (from Fulton et al. [14]) and technical users' mental models. Section numbers for the associated results are provided for reference.

Topic	Non-technical users	Technical users
Unplugging	Unplugging the computer stops the hacker	[§4.2.1] Unplugging might stop the hacker, but it is more likely if unplugging from the network rather than the power source.
Detectability	Attacks and unsafe situations are obvious	[§4.2.4] **Malware** is what causes obvious pop-ups; hackers probably want to remain undetected
Encryption	Encryption is fragile and all security measures are futile	[§4.2.5] Encryption is nearly impossible to circumvent and security measures can be effective if used appropriately
Targets	Hackers have specific, important targets	[§4.1.1] Hackers have general financial or information goals and rarely target specific individuals.
Phishing	Users should be careful when evaluating suspicious links	[§4.1.2] Users should be careful, [§4.2.2] especially high profile victims who 'should know better'
Realism	To evaluate realism, non-technical end users use technical and non-technical knowledge, assess plausibility of plot and characters, consider cinematic cues	[§4.3] To evaluate realism, technical users use mostly technical knowledge, assess plausibility of plot, characters, location, context, and cinematic cues
Complexity	If it's too quick or easy, it's unrealistic.	[§4.2.5] Too quick and easy is unrealistic, except in cases of insider threats, organisations with lax security measures, and lax defence

to make inaccurate assumptions, which overlapped with those of non-technical, home computer users [37].

2. We found no consensus amongst participants over which of the characters' or systems' actions were unrealistic, demonstrating high variability in the aspects of a scene which they found believable or questionable. For all clips, at least some participants gave inaccurate explanations despite their technical backgrounds. Some participants had polar opposite impressions about the realism of an action.

3. Our data suggests that participants may also be influenced by media and believed at least some inaccuracies, though it is unclear if media informs or reinforces existing mental models. Despite their technical background, participants were not immune to misinformation.

5.1 Comparison with earlier results

Table 2 summarises our results compared to Fulton et al.'s original study [14]. We discuss the over-arching themes present in the two studies.

Unplugging: Some participants agreed that unplugging a device that's being hacked from its power source may be an effective way to stop a hack. However, many generally found unplugging from a network to be more effective at defending against a hack (unless the hack was local to the machine). This distinction was not present in the original results.

Detectability: non-technical end users believed that they would be able to recognize if a system was being hacked or if they encountered an unsafe situation online; the attack would be apparent to the user who could then take steps to mitigate the issue. Technical users believed that malware could cause pop-ups on the screen, but many believed that this was distinct from hacking. Hackers, they believed, would want to be stealthy so that they remain undetected.

Encryption: non-technical end users believed that encryption could be easily broken by skilled enough individuals. Hackers were seen as having an immense amount of power, encryption was futile because hackers could circumvent it, and the idea that hackers had a key that could decrypt everything seemed plausible. However, this point of view was not shared by our technical participants: some participants did believe hackers to be highly talented individuals, but many believed that encryption was strong and would require immensely powerful hardware to crack. The existence of such a "decryption" chip was placed in the far future.

Targets: When discussing intended targets of a breach, there is overlap between non-technical end users and our technical participant. Specific individuals, national organisations, and private businesses were viewed as plausible targets of attack by both groups. Our participants additionally felt that users and businesses with poor security practices were more susceptible to hackers and more likely to be targeted.

Phishing: Both non-technical end users and technical participants agreed that opening unknown and suspicious emails was a precursor to getting hacked. Many confirmed seeing such emails in their own inboxes, and were familiar with incidents of individuals or organisations being breached by way of phishing. Technical participants, however, placed significant responsibility on the victim in these situations, particularly those they considered "high-profile".

Realism: Methods of assessing realism were mostly con-

sistent between non-technical end users and technical participants. Both groups used personal experience, technical knowledge, context, and cinematic cues to evaluate the plausibility of cybersecurity portrayals in media. They were more likely to judge something as realistic if they had either experienced it themselves, or were familiar with someone who had. Use of technical knowledge in such appraisal, however, differs slightly amongst the two groups: technical participants were slightly more critical of technical jargon, expecting it to make sense, and they may have focused more on system vulnerability than non-technical participants. With respect to cinematics, technical participants focused on the realism of the set and how it fit with the context of the scene. For example, they considered what kind of organisation it portrayed and how the characters interacted with each other. non-technical end users, on the other hand, noted audio cues such as dramatic music in their assessment of realism.

Complexity: Hacking that was portrayed through quick, easy tasks was largely seen as unrealistic by both non-technical end users and technical participants. Technical participants commented that hacking is never that simple, unless it is done with help from a human insider. Our participants expected systems to be heavily defended using multiple protocols, and thus were critical of how hacking was portrayed as easy. This is in stark contrast to the original results: end users believed that hacking was easy but expected defence against it to be difficult.

Overall, we find that our technical participants had more nuanced understanding of hacking and security, based on their technical knowledge than the non-technical end users from the original study [14]. However, technical participants also appeared susceptible, although to a lesser degree, to misunderstandings and to believing that some of the fictional portrayals of hacking were realistic. Even participants who demonstrated reasonable knowledge of computer security concepts would occasionally mention *"you see it in the movies"*(P4-S3) as justification for penning a scene as realistic. The varied results of our study are concerning: our participants currently hold, or will soon hold, employment in technical positions. In these professional roles, they may make decisions regarding network configurations, they may administer systems, they may design and develop software, or they may make other decisions that could impact an organisation's susceptibility to security hazards like hacking or ransomware. They may also be in a position to recognize and act against possible security breaches. In any of these roles, accurate interpretations of hacking are especially important due to the potential consequences of their actions.

Our participants also hold informal roles as advisors, tutors, or troubleshooters of computer-related issues for the non-technical people in their lives. Any misconceptions about hacking held by our participants may get propagated amongst this wider circle of individuals who may not be equipped to counter them. Inconsistent or inaccurate advice could lead to further confusion and gaps in the mental models of non-technical users. Additionally, inaccurate advice that matches what is seen in fiction would reinforce the trust non-technical users place in (mostly inaccurate) media depictions.

As such, it is particularly dangerous for participants in technical fields to hold inaccurate, or conflicting, mental models, as it would not only affect them, but also others on both an individual and organisational scale.

5.2 Recommendations

Several suggestions for addressing these misconceptions have already been offered by Fulton et al. [14] for non-technical end users, and they likely largely apply to technical users too. We discuss these, along with additional recommendations.

R1. Security education: Much like Fulton et al. [14], we found that participants relied mostly on their technical knowledge in assessing realism. Participants also tended to adopt stereotypical beliefs about hackers and tended to 'victim-blame' end-users for security failures. This is problematic because technical users may propagate these attitudes in the workplace or to non-technical users that they advise. In both cases, this can undermine the implementation and maintenance of effective security mechanisms and practices [16, 31] Notably, participants had gaps in their mental models that sometimes led to inaccurate assumptions about encryption, the visibility of hacking attacks, who hackers target, how to mitigate threats, and the identity of hackers. As such, we advocate for a more thorough cybersecurity curriculum that addresses both technical details and human factors, and that explicitly tackles common stereotypes and misconceptions.

Individuals with a technical background may not have education specifically on cybersecurity topics. Others may find themselves in an occupation making technology-related decisions without related formal education(e.g., project management within a software team). As such, we suggest including mandatory cybersecurity education within the general education system or as part of workplace training. Prior research has found that the introduction of cybersecurity curriculum as early as elementary and middle school improves digital literacy and cybersecurity awareness [21, 41, 42]. We also urge the application of security in different platforms and services be included to provide a more holistic education (e.g., Abu-Salma et al. [1] found users' perceptions of private browsing mode to be mostly incorrect, while Wermke et al. [39] found users' security mental models of cloud services to be incomplete and undeveloped).

As mentioned by Fulton et al. [14], educators, designers, and developers who are more familiar with the nuances and depth of misconceptions held by target user groups would be able to better address them in their educational material. More broadly, we advocate for closer integration of cybersecurity content within core Computer Science/Engineering curriculum, so that upcoming generations of technical users have a

foundational understanding of secure computing.

R2. Fact-checking databases: We suggest adding educational information about classic television or movie tropes relating to cybersecurity and popular Hollywood hacking dramatizations to fact-checking websites such as Snopes [32]. In effect, we recommend bringing to the forefront these common misconceptions to make them easy for individuals to identify and to correct. Users are increasingly being taught to identify misinformation and verify the authenticity of online sources; we suggest that misinformation from television and movies be treated similarly (and given the popularity of streaming sites, the differentiation between television, movie, and online content is increasingly blurred). Making this information easily accessible online creates an opportunity to educate users when they specifically seek out the information (e.g., when searching about a particular scene or episode).

R3. Using media to educate: As discussed by Fulton et al. [14], we stress the need for collaboration between the entertainment industry and the cybersecurity community. Specifically, we emphasise using media as a tool to increase awareness of cybersecurity concepts. Research suggests that users ration the amount of effort put into security practices, and that asking them to follow certain existing security advice is unreasonable [33]. However, new security practices do exist that require less cognitive effort [16] (e.g., the use of password managers over traditional password security advice). Studies show that non-expert users' practices have remained largely unchanged, and that expert users also mostly employ these same practices [8] despite better knowledge of "best practices". Individuals may also need regular reminders to effectively retain and apply security information [29]. Therefore, a change might be required for how this advice is imparted to the general public. Media may be key to effectively educating users where previous methods have failed. If utilised, we might make progress in normalizing security best practices. For example, the show *Mr. Robot* is noted for its realism; many participants acknowledged its potential as an educational tool by employing realistic depictions of cybersecurity. It is, however, key that the entertainment industry utilizes reliable sources of cybersecurity expertise (as opposed to more general technical sources), to avoid propagating misconceptions such as those observed in our study.

5.3 Limitations

We have a relatively small sample (n = 23) and focused only on qualitative data. Additionally, participants' self-reported levels of cybersecurity knowledge and exposure may not be accurate, given its subjective nature. Our eligibility criteria may have primed participants to consider their technical background as a source for their mental models. Our interview may also have primed participants to: (i) suggest behavioural factors when asked for what makes someone an easy target, and (ii) explicitly look for unrealistic components within the video clips; it is possible that these same participants could have watched these television shows or movies in another context without even noticing or reflecting on their realism. As we followed the exact study methodology of Fulton et al., we similarly did not inquire about participants' perceptions of the actors in the video clips. Since Fulton et al. did not control for demographics, technical participants may have also been included in their study, so we are unable to assess the extent of overlap between the two populations.

5.4 Future work

It would be interesting to compare these results to users' perceptions of more realistic depictions of cybersecurity. Exploring alternate forms of media that our participants cited would also be helpful: blogs, forums, and videos seen on SNS (like YouTube). It also remains to be investigated whether participants "living" the experience through games that emulate hacking would evaluate their experience as realistic or not. The genre in which cybersecurity incidents are portrayed may also have an effect on users' perceptions of the topic. Finally, due to the qualitative nature of our study, we were unable to analyse whether there were links between participant demographics and how likely they were to source their mental models from media. A larger scale study would aid in answering some of these questions. Follow-up studies could make use of a true/false scheme for analysis, by having participants characterise whether media portrayals are accurate.

6 Conclusion

We conducted interviews with 23 participants with technical background to evaluate the effect of fictional television and movie media on participants' mental models of hacking and computer security. Participants were generally capable of determining the realism of hacking scenes, but gaps in their mental models sometimes lead to inaccurate assumptions. We also observed considerable variability among participants with regards to which actions participants identified as unrealistic and to the interpretation of the scenes. In comparison with the study of non-technical end users completed by Fulton et al., we found that our technical participants generally had a better informed or more nuanced assessment of the realism of the attacks. However, our participants were not immune to believing misinformation about hacking that they had previously seen in mass media.

Acknowledgments

We thank our participants and anonymous reviewers for their shared insight. This research was supported by NSERC Discovery Grant RGPIN 06273-2017; and the Canada Research Chairs program under Grant 950-231002-2016.

References

[1] Ruba Abu-Salma and Benjamin Livshits. Evaluating the end-user experience of private browsing mode. In *The 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2020.

[2] Ruba Abu-Salma, Elissa M Redmiles, Blase Ur, and Miranda Wei. Exploring user mental models of end-to-end encrypted communication tools. In *Workshop on Free and Open Communications on the Internet (FOCI)*. USENIX, 2018.

[3] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *Symposium on Security and Privacy (SP)*, pages 137–153. IEEE, 2017.

[4] Hala Assal and Sonia Chiasson. 'Think secure from the beginning': A survey with software developers. In *Conference on Human Factors in Computing Systems (CHI)*, page 289. ACM, 2019.

[5] Rebecca Balebako and Lorrie Cranor. Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy*, 12(4):55–58, 2014.

[6] Miri Barak, Tamar Ashkar, and Yehudit J Dori. Learning science via animated movies: Its effect on students' thinking and motivation. *Computers & Education*, 56(3):839–846, 2011.

[7] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[8] Karoline Busse, Julia Schäfer, and Matthew Smith. Replication: no one can hack my mind revisiting a study on expert and non-expert security practices and advice. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS) 2019)*, 2019.

[9] Pedro Canahuati. Keeping passwords secure. https://about.fb.com/news/2019/03/keeping-passwords-secure/, Last accessed: December 2019.

[10] Barbie Clarke and Catherine Gardner. Concerned children's advertisers leads the way. *Young Consumers*, 2005.

[11] Satu Elo and Helvi Kyngäs. The qualitative content analysis process. *Journal of Advanced Nursing*, 62(1):107–115, 2008.

[12] William Enck, Damien Octeau, Patrick D McDaniel, and Swarat Chaudhuri. A study of Android application security. In *USENIX Security Symposium*, 2011.

[13] Equifax. 2017 Cybersecurity Incident & Important Consumer Information. https://www.equifaxsecurity2017.com/frequently-asked-questions/, Last accessed: December 2019.

[14] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. The effect of entertainment media on mental models of computer security. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2019.

[15] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering*, 23(1):259–289, 2018.

[16] Cormac Herley. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *The 2009 Workshop on New Security Paradigms Workshop*, NSPW '09, page 133–144. ACM, 2009.

[17] Heather J Hether, Grace C Huang, Vicki Beck, Sheila T Murphy, and Thomas W Valente. Entertainment-education in a media-saturated environment: Examining the impact of single and multiple exposures to breast cancer storylines on two popular medical dramas. *Journal of health communication*, 13(8):808–823, 2008.

[18] Adele E Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. The psychology of security for the home computer user. In *Symposium on Security and Privacy*, pages 209–223. IEEE, 2012.

[19] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Symposium On Usable Privacy and Security (SOUPS)*, pages 39–52, 2015.

[20] Rhiannon L. Hacker's Game: 10 things Hollywood got wrong about computer hacking. https://www.hotbot.com/blog/10-things-hollywood-got-wrong-about-computer-hacking/, Last accessed: December 2019.

[21] Sana Maqsood, Christine Mekhail, and Sonia Chiasson. A day in the life of jos: A web-based game to increase children's digital literacy. In *The 17th ACM Conference on Interaction Design and Children*, pages 241–252, 2018.

[22] Microsoft. Microsoft Security Development Lifecycle (SDL). https://www.microsoft.com/en-us/securityengineering/sdl/, Last accessed: December 2019.

[23] Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, Emanuel von Zezschwitz, and Matthew Smith. " if you want, i can store the encrypted password": A password-storage field study with freelance developers. In *Conference on Human Factors in Computing Systems (CHI)*, page 140. ACM, 2019.

[24] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. Why do developers get password storage wrong?: A qualitative usability study. In *SIGSAC Conference on Computer and Communications Security*, pages 311–328. ACM, 2017.

[25] Duc Cuong Nguyen, Dominik Wermke, Yasemin Acar, Michael Backes, Charles Weir, and Sascha Fahl. A stitch in time: Supporting android developers in writingsecure code. In *The 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1065–1077. ACM, 2017.

[26] Berkeley Information Security Office. Secure coding practice guidelines. https://security.berkeley.edu/secure-coding-practice-guidelines#Secure%20coding%20principles, Last accessed: December 2019.

[27] Fahimeh Raja, Kirstie Hawkey, Pooya Jaferian, Konstantin Beznosov, and Kellogg S Booth. It's too complicated, so iI turned it off!: expectations, perceptions, and misconceptions of personal firewalls. In *Workshop on Assurable and Usable Security Configuration*, pages 53–62. ACM, 2010.

[28] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How I learned to be secure: a census-representative survey of security advice sources and behavior. In *SIGSAC Conference on Computer and Communications Security*, pages 666–677. ACM, 2016.

[29] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landesberger, and Melanie Volkamer. An investigation of phishing awareness and education over time: When and how to best remind users. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 259–284, 2020.

[30] Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala, and Kent Seamons. Weighing context and trade-offs: How suburban adults selected their online security posture. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 211–228, 2017.

[31] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19(3):122–131, 2001.

[32] Snopes. Snopes. https://www.snopes.com, Last accessed: February 2021.

[33] Elizabeth Stobert and Robert Biddle. The password life cycle: user behaviour in managing passwords. In *10th Symposium On Usable Privacy and Security (SOUPS) 2014)*, pages 243–255, 2014.

[34] Mohammad Tahaei, Adam Jenkins, Kami Vaniea, and Maria Wolters. "i don't know too much about it": On the security mindsets of computer science students. *Socio-Technical Aspects in Security and Trust (first ed.), Thomas Groß and Tryfonas Theo (Eds.). Springer International Publishing. https://www.springer. com/book/9783030559571*, 2020.

[35] TV tropes. Hollywood encryption. https://tvtropes.org/pmwiki/pmwiki.php/Main/HollywoodEncryption, Last accessed: December 2019.

[36] TV tropes. Hollywood hacking. https://tvtropes.org/pmwiki/pmwiki.php/Main/HollywoodHacking, Last accessed: December 2019.

[37] Rick Wash. Folk models of home computer security. In *The Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[38] Rick Wash and Molly M Cooper. Who provides phishing training? facts, stories, and people like me. In *The 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2018.

[39] Dominik Wermke, Nicolas Huaman, Christian Stransky, Niklas Busch, Yasemin Acar, and Sascha Fahl. Cloudy with a chance of misconceptions: Exploring users' perceptions and expectations of security and privacy in cloud office suites. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 359–377, 2020.

[40] Justin Wu and Daniel Zappala. When is a tree really a truck? Exploring mental models of encryption. In *Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 395–409, 2018.

[41] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction*, 13:10–18, 2017.

[42] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. I make up a silly name' understanding children's perception of privacy risks online. In *The 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

A Participant demographics

Table 3: Participant demographic details

Participant ID	Gender	Age	Occupation	Highest/Current level of education	Most recent program of study	Cyber challenges
P1-S3	Female	18-24	Student	Undergraduate	Prefer not to answer	No exposure
P2-S3	Female	35-44	Project Manager	Graduate degree	Project Management / Health Informatics	No exposure
P3-S3	Male	18-24	Student	Undergraduate	Computer Science	Completed one or more
P4-S3	Female	18-24	Student	Undergraduate	Computer Science	Completed one or more
P5-S5	Female	25-34	Student, web developer	Graduate degree	Computer Science	Completed one or more
P6-S3	Female	55-64	IT support specialist	Graduate degree	Control Systems Engineering	No exposure
P7-S2	Male	55-64	Contract Instructor	Graduate degree	No answer	No exposure
P9-S3	Male	18-24	Student	Undergraduate	Software Engineering	No exposure
P10-S3	Male	No answer	IT support specialist	Undergraduate	Engineering	No exposure
P11-S2	Female	25-34	Project Manager	Undergraduate	Business	No exposure
P12-S2	Male	65-74	Retired	Graduate degree	Applied Science (computer related)	No exposure
P13-S3	Male	25-34	Network Maintenance	Undergraduate	Computer Engineering	No exposure
P14-S3	Male	35-44	Software Engineer	Undergraduate	Computer Engineering	No exposure
P15-S3	Female	35-44	Software Developer	Undergraduate	Computer Science	No exposure
P16-S3	Male	18-24	Student	Undergraduate	Computer Science	No exposure
P18-S2	Female	18-24	Prefer not to answer	Undergraduate	Computer Engineering	No exposure
P19-S4	Male	25-34	IT support specialist	College	Information System Support Specialists	No exposure
P20-S3	Male	18-24	Student	Undergraduate	Computer Science	No exposure
P22-S3	Female	25-34	UX Designer	Graduate degree	Human Computer Interaction	No exposure
P23-S2	Male	18-24	Student	Undergraduate	Computer Systems Engineering	No exposure
P24-S2	Male	18-24	Student	Undergraduate	Computer Science (Minor: Entrepeneurship)	Completed one or more
P25-S2	Female	25-34	Student	Undergraduate	Computer Science	Completed one or more
P26-S2	Female	18-24	Student	Undergraduate	Computer Science (Stream: Software Engineering)	No exposure

B Data analysis timeline

Table 4: A summary of the data analysis process, and the researchers involved at each stage.

			Researchers involved		
Activity	**Codebook used**	**Transcripts coded**	**RS1**	**RS2**	**RS3**
Formed initial codebook of 9 items while editing all transcripts for accuracy	C1	–	x		
Coded two transcripts **(refined codebook)**	C1	T1-T2	x		
Re-coded two transcripts	C2	T1-T2	x		
Coded five transcripts	C2	T4, T6-T7, T10-T11	x		
Coded three transcripts **(refined codebook)**	C2	T3, T5, T9	x	x	
Re-coded transcripts	C3	T3, T5, T9	x	x	
Coded three transcripts **(codebook finalised)**	C3	T13, T15, T22	x	x	
Re-coded three transcripts (no changes)	C4	T3, T9, T15	x		x
Re-coded ten transcripts	C4	T1-T2, T4-T7, T10-T11, T13, T22			x
Coded seven new transcripts	C4	T12, T14, T16, T18-T20, T22-T23			x
Coded three new transcripts	C4	T24-T26	x		

C Post-test questionnaire

Q1 Please enter your Participant ID : _____

Q2 What gender do you most closely identify with?

- ○ Male (1)
- ○ Female (2)
- ○ Other: (3) _____
- ○ Prefer not to say (4)

Q3 What is your age? If you prefer not to say, please enter "prefer not to say": _____

Q4 Choose either the level of education for which you are **currently enrolled** or the highest level of education you have completed.

- ○ Elementary school (1)
- ○ High school (2)
- ○ College (3)
- ○ Technical, trade school, vocational training, or apprenticeship (4)
- ○ Undergraduate degree (Bachelor's) (5)
- ○ Post-graduate certificate or diploma (6)
- ○ Graduate degree or professional degree (7)
- ○ Other (8): _____
- ○ Prefer not to say (9)

Q5 What is your occupation?
If you prefer not to say, please enter "prefer not to say": _____

Q6 Please list all current and previously completed programs of study.
If you prefer not to answer, please write in "prefer not to answer": _____

Q7* Have you ever taken any technical **courses** or **training**? This would include courses from Computer

* Question not present in the original study's methodology.

Science, Information Technology (IT), Software Engineering, Systems Engineering, and many other fields.
Please list any other formal **training**, **courses**, or otherwise that may count as "technical".
If you prefer not to answer, please write in "prefer not to answer":

_____

Q8 Which option best describes your current employment status?

- ○ Working for payment or profit (1)
- ○ Unemployed (2)
- ○ Home-maker (looking after home/family) (3)
- ○ Student (no other form of employment) (4)
- ○ Retired (5)
- ○ Unable to work due to permanent sickness/disability (6)
- ○ Other (specify): (7) _____
- ○ Prefer not to say (8)

Q9* Do you study or work in a field that links closely to some form of computer **security**? (E,g: involving encryption, hacking, authentication)

- ○ Study only (please provide details into your program/area of study): _____
- ○ Work only (please provide details into your area of work): _____
- ○ Both study and work (please provide details into your area of study and work:) _____ (3)
- ○ Neither study nor work (4)
- ○ Prefer not to say (5)

Q10* Have you ever participated in hackathons or other security-oriented coding challenges?

- ○ Yes (please list what kinds of challenges you've participated in:) _____ (1)
- ○ No (2)
- ○ Prefer not to say (3)

Q11* Please list any courses you have taken pertaining to computer security.
If you prefer not to answer, please write "Prefer not to answer": _____

* Question not present in the original study's methodology.

Q12* Are you currently a student (part-time or full-time)

- ○ Yes (1)
- ○ No (2)
- ○ Prefer not to say (3)

Display The Question Below: If "Are you currently a student??" is "Yes"

Q13 Please select the level of education you are **currently completing**.

- ○ Undergraduate degree (1)
- ○ Master's degree (2)
- ○ PhD degree (3)
- ○ Post-doc (4)
- ○ Diploma (5)
- ○ Other (please list): _____ (6)
- ○ Prefer not to say (7)

Display The Question Below: If "Are you currently a student?" is "Yes"

Q14* Please enter which year of study you are currently in (e.g: 1st year, 2nd year, etc).
If you prefer not to answer, please write "Prefer not to answer": _____

Q15* Please select the statement that best describes your **exposure** to topics of computer security (encryption, hacking, authentication, etc) **in the past one year**.

- ○ No exposure at all (1)
- ○ A little exposure (2)
- ○ Some exposure (3)
- ○ High exposure (4)
- ○ Very high exposure (5)
- ○ Prefer not to say (6)

* Question not present in the original study's methodology.

Q16* Please select the statement that best describes your **level of knowledge** of computer security (encryption, hacking, authentication, etc).

- ○ No knowledge at all (1)
- ○ A little bit of knowledge (2)
- ○ Some knowledge (3)
- ○ High level of knowledge (4)
- ○ Very high level of knowledge (5)
- ○ Prefer not to say (6)

Q17 Please enter the number of hours you typically spend on each of the following activities in the specified time range.
If you prefer not to say, please enter the letter **X**.

- Recreational TV: ____ hours/week (1)
- Newspapers: ____ hours/week (2)
- Podcasts: ____ hours/week (3)
- Social media: ____ hours/**day** (4)
- Movies: ____ hours/**month** (5)
- TV news: ____ hours/week (6)
- Magazines: ____ hours/week (7)

Q18 Please select which of the following genres you enjoy consuming media in (select as many as apply).

- ☐ Action (1)
- ☐ Comedy (2)
- ☐ Romance (3)
- ☐ Documentary (4)
- ☐ Horror (5)
- ☐ Drama (6)
- ☐ Kids (7)
- ☐ Adventure (8)
- ☐ Sci-fi (9)
- ☐ Fantasy (10)
- ☐ Thrillers (11)
- ☐ Spy-films (12)
- ☐ Other (please list): _____ (13)
- ☐ Prefer not to say (14)

* Question not present in the original study's methodology.