A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education

LEAH ZHANG-KENNEDY, University of Waterloo Stratford School of Interaction Design and Business, Canada
SONIA CHIASSON, Carleton University School of Computer Science, Canada

We conduct a comprehensive review covering academic publications and industry products relating to tools for cybersecurity awareness and education aimed at non-expert end-users developed in the past 20 years. Through our search criteria, we identified 119 tools that we cataloged into five broad media categories. We explore current trends, assess their use of relevant instructional design principles, and review empirical evidence of the tools' effectiveness. From our review, we provide an evaluation checklist and suggest that a more systematic approach to the design and evaluation of cybersecurity educational tools would be beneficial.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**; *Usability in security and privacy*;

Additional Key Words and Phrases: Cybersecurity educational tools, cybersecurity awareness and education

ACM Reference format:
Leah Zhang-Kennedy and Sonia Chiasson. 2020. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Comput. Surv.* 54, 1, Article 12 (December 2020), 39 pages.
https://doi.org/10.1145/3427920

1 INTRODUCTION

Cybersecurity is both a technical problem and also one that is significantly impacted by non-expert end-users who interact with online content. Due to the ever-changing and nuanced nature of security, technological countermeasures alone are rarely enough to protect these users from online threats. For example, users are responsible for adjusting their privacy settings, choosing strong passwords, and complying with security policies. These decisions require informed decision making, foresight, and tradeoffs based on users' existing knowledge about online risks and the technology they use [8, 71, 76, 85, 199, 200]. Therefore, improving non-expert end-users' knowledge and awareness is an essential step towards cybersecurity.

Researchers and practitioners have developed a variety of multimedia educational tools targeted at non-expert end-users over the last couple of decades to increase awareness and address a knowledge gap in cybersecurity. We define "multimedia educational tools" as *learning content that uses*

S. Chiasson received funding from Canada's Natural Sciences and Engineering Research Council through the Discovery Grant and Canada Research Chair programs.
Authors' addresses: L. Zhang-Kennedy, University of Waterloo Stratford School of Interaction Design and Business, 125 St. Patrick Street, Stratford, Ontario, Canada; email: lzhangkennedy@uwaterloo.ca; S. Chiasson, Carleton University School of Computer Science, 1125 Colonel By Drive, Ottawa, Ontario, Canada; email: chiasson@scs.carleton.ca.

0360-0300/2020/12-ART12 $15.00
https://doi.org/10.1145/3427920

more than one mode of communication, which may include a combination of text, images, audio, animation, video, and interactive content. Based on the educational literature, multimedia can increase a learner's motivation, engagement, and comprehension of educational content [36, 107]. For this article, we chose to explore how such tools are used to teach about security. Our review focuses on multimedia educational tools developed for people with general or limited computing and security knowledge, including end-users, students, consumers, corporate users, children, youth, and young adults. We synthesize current trends and the impact of these educational tools by systematically reviewing existing work. The objective of our research is to provide an overview of the tools, synthesize their design methodology, and assess their effectiveness at improving users' cybersecurity awareness and knowledge. Our research questions address the following: *(1) What are the current trends in using multimedia tools for educating users about cybersecurity? (2) Which design principles are utilized in the tools? (3) How are the tools evaluated, and what is their educational impact?* Our review consolidates existing research in the area, includes analysis of *119 cybersecurity educational tools*, and guides future research efforts by identifying gaps and open research issues.

We first summarize existing literature reviews in Section 2, then outline our method of data collection and analysis in Section 3. The rest of the article consecutively answers our three research questions. In Section 4, we describe the current trends in using cybersecurity educational tools, focusing on identifying the types of media, the educational subjects, and target audiences. In Section 5, we present an analysis of the instructional design principles employed in existing educational tools. Section 6 identifies the evaluation methodologies used and empirical evidence available regarding the tools' effectiveness and usability. The final section further discusses the state of cybersecurity awareness and education, and provides considerations for the future research.

2 RELATED WORK

To the best of our knowledge, our literature review is the most extensive and complete analysis of general cybersecurity awareness and educational tools for non-expert end-users. For context, we begin by briefly discussing the scope of other reviews that have explored subsets of the space.

A widely practiced educational approach is to use games and gamification. Shostack [177] provides an extensive online compilation of such efforts but offers no accompanying analysis. While researchers of previous literature reviews [3, 15, 43, 46, 75, 77, 100, 153] found games to be an effective media for creating cybersecurity awareness and education, they also identified some serious limitations, as discussed next.

Alotaibi et al. [3] examined 12 academic papers on game-based cybersecurity studies and ten popular industry games. They observed that the focus of industry games is general cybersecurity, compared to the more domain-specific topics (e.g., phishing, malware, passwords) used in games for academic research. The authors concluded that games had positive results for training users and creating cybersecurity awareness, but highlighted a need for in-depth and robust evaluations with larger sample sizes. Similarly, Hendrix et al. [75] found it difficult to draw definitive conclusions about effectiveness of games at altering users' security practices in the long-term. In another review of seven cybersecurity games, Herr and Allen [77] found the games do not provide comprehensive cybersecurity training and collaborative learning. Furthermore, a review of eleven serious games for information assurance and cybersecurity by Compte et al. [100] presented a framework for designing games to raise novice users' security awareness and knowledge. They observed the pedagogic potential of games, but concluded that their use is limited to formal learning contexts. Cullinane et al. [46] evaluated seven existing games through a scoring and ranking process based on replay value, progression qualities, and interface accessibility. They found that games with strong gameplay elements ranked higher in those categories, and proposed new game designs to

convey cybersecurity concepts to minors. Pastor and Díaz [153] examined thirteen information security simulation systems for information security and information assurance education, training and awareness. Battistella et al. [15] conducted a systematic review of games used in higher education curriculum across computing knowledge areas, and Connolly et al. [43] conducted a systematic literature review of empirical evidence on computer games and serious games, but neither reviews focuses on cybersecurity.

Prior work identified significant limitations in cybersecurity education. We confirm a few patterns found in earlier reviews, such as focusing on general cybersecurity subjects [3] and limited rigorous evaluations [3, 75]. However, prior reviews concentrate on games and do not provide sufficient analysis and insights on multimedia trends, design, and evaluation. Our work fills this research gap by extending existing reviews, synthesizing prior findings, and providing new analysis. We broaden the educational tools' scope to include digital games, tabletop games, comics, film and animation, and learning modules.

In the next section, we describe our search strategy for identifying tools, exclusion criteria, and method of data collection and analysis.

3 TOOLS SELECTION AND ANALYSIS METHODOLOGY

The literature search began in June of 2018 and were updated in June 2019. Our initial cataloguing of tools included any work that has a cybersecurity educational goal and that was created after January 2000. Our search was conducted online; we did not specify geographic limitations but covered only English-language tools, though some tools are also available in other languages. The literature search began with cataloguing works from existing literature reviews described in Section 2 and this yielded 58 unique tools. We read all of the related academic papers, tech reports, and white papers referenced. Next, we used Google's search engine, Google Scholar, Apple Apps Store, Google Play Store, and the video-sharing service YouTube to conduct a comprehensive search. The search terms we used are combinations of the search string *subjects* AND *learning* AND *media*:

- Subject terms: "security" OR "cybersecurity" OR "privacy" OR "phishing" OR "digital citizenship" OR "digital literacy" OR "online safety"
- Learning terms: "education" OR "educational" OR "awareness" OR "game-based learning" OR "e-learning" OR "mobile learning" OR "training" OR "learning"
- Media terms: "game" OR "serious game OR "simulation" OR "visualization" OR "information graphic" "infographics" OR "animation" OR "video" OR "comic" OR "graphic novel OR "board game" OR "tabletop game" OR "module" OR "tool"

3.1 Exclusion Criteria

We collected approximately 170 candidate tools. Next, we developed and refined the exclusion criteria described below through repeated discussions with usable security researchers from our lab. We focused our review on educational tools for people with general or limited computing and security knowledge. These may include end-users, students, consumers, corporate employees, children, and youth, but exclude security experts or those formally training to be cybersecurity professionals. Applying the exclusion criteria to our search results narrowed the scope to 119 tools.

Tools falling within the following exclusion criteria were omitted from our review:

(1) Tools for testing and training cybersecurity professionals, information technology (IT) experts, and system administrators, including threat modelling and information assurance simulation systems for users with profound technical backgrounds. Examples: Elevation of Privilege [176]; The Security Cards [48]; Operation Digital Chameleon [164].

(2) Tools for eliciting security and system design requirements. Examples: Cornucopia [151]; Social Engineering Requirements Game [16]; Design with Intent Toolkit [103]; Privacy Ideation Cards [48].
(3) Tools for testing computer security knowledge and hacking skills, such as software used in security competitions, a.k.a., CTFs. Example: CMU's PicoCTF computer security game [22].
(4) Security-themed games and hacking games that do not have a core educational purpose. Examples: Watch Dogs [196]; Uplink [82]; Hack Evolution [58].
(5) Tools that are not free and accessible to educators, including internal training material for employees, training tools for company-specific products, and paid commercial products and subscriptions. Example: teachprivacy.com [179].
(6) Tools that do not function as stand-alone learning resources[1] and require extensive external instruction and scaffolding, such as instructor support tools for classroom use. Examples: GRASP [171]; ICV [172]; Cryptool [105].
(7) Tools that have insufficient primary or secondary information accessible in the public domain for us to clearly grasp their characteristics and mechanics to conduct a thorough analysis. Example: CyberNEXS [129], infographics that do not have supporting documentation of the design process.
(8) Cybersecurity learning activities and exercise that are not multimedia tools, including gamified cybersecurity exercises, frameworks, conceptual learning activities, and alternate reality games (ARGs). Examples: Protection Pocker [205]; NeoSens [166]; Phishing Game Design Framework [7]; InfoSec Cinema [17]; Cryptomancer [198]; Computer Security Alternate Reality Game [127].
(9) Works that do not have a functional prototype or end product, such as game proposals and conceptual models. Examples: Cybersecurity Awareness Game [98]; Privacy Doodle Jump [95].

3.2 Data Collection and Analysis Process

We systematically extracted and catalogued 14 types of data for each tool in Microsoft Excel: (1) title, (2) description, (3) URL (if the tool is available online), (4) release date, (5) category and type (e.g., game–simulation; tools are assigned to only one category per dimension), (6) educational subject, (7) number of players (or users) supported per use, (8) design goals; (9) design methodology, (10) development information, (11) primary target audience, (12) companion materials (e.g., lesson plans), and if applicable, (13) the evaluation methodology, and (14) the main empirical findings. The information is extracted directly from the sources and accompanying materials when available. In some cases, we had to infer data based on secondary sources. For example, we could not find the release dates for some tools directly from their source, so we deduced the information from external websites like YouTube. Each tool and related resources were inspected at least twice to ensure they passed our exclusion criteria.[2]

For the release date, we documented the year that the tools were first made publicly available. For example, Hector's World [139] is an animated series created in 2003 with episodes running up until 2008; we recorded 2003 as the release date. Tools used for academic research are listed using the year that they were created, but we used paper publication dates if the release information for the tools is unavailable.

[1]We included some multimedia resources from teaching curriculums that could function as individual learning tools.
[2]We were very diligent in data compilation, but we apologize for any inadvertent omissions or errors, particularly when we had to infer data.

After identifying the list of sources, we read and analyzed the material relating to the tools. It included academic papers, instruction manuals, articles, website summaries, teaching guides, and other resources. We directly interacted with the tools to gain a good understanding of the content and mechanics if they are available online. If a working version of the tool was unavailable, then we based our analysis on published descriptions and related secondary resources, such as trailers, demos, and tutorials. We assigned a category to each tool based on our assessment of their content. For example, although some of the interactive modules were called "games" by their creators, we placed these in the Module category, because they most closely fit our definition of Learning Modules.

4 TRENDS IN CYBERSECURITY AWARENESS AND EDUCATION

Addressing our first research question, we report general trends in cybersecurity awareness and education using multimedia tools. Due to the breadth of our sample, we organize the tools into five dominant multimedia categories and use a small number of representative examples. We do not necessarily endorse these tools as the "best" in the category but merely present them as good exemplars that reasonably capture the unique characteristics of the multimedia type discussed. A few of the tools discussed in this review are created by us. To keep analysis as objective and transparent as possible, we overtly indicate the tools by name (i.e., Zhang-Kennedy et al.) or set the names of the tools in *italicized* text (e.g., *Secure Comics* [213], *Cyberheroes* [209]).

We identified 119 tools for educating users about cybersecurity and privacy created between January 2000 and June 2019. An overview of the name, type of tool, educational subject, and target audience is provided in Section 5.3, Tables 2, 3, and 4. Figure 1 shows a heatmap chart of the number of tools found for each year. There are 54 digital games, 34 films and animation, 10 tabletop games, 9 learning modules, 9 comics, and 3 falling into other types of media. Evident in Figure 1, few tools existed in the early 2000s but there is growing use of multimedia tools after 2005. The majority of the tools ($n = 91$) are accessible online. Figure 2 shows that educational subjects have broadened over time. We assigned the subject categories based on our assessment of the tools' educational content. Tools that teach a range of cybersecurity topics are placed under the subject of general cybersecurity ($n = 30$), while tools that focus teaching a specific cybersecurity sub-topic or other closely related topics are placed into their own subjects. These include e-safety ($n = 28$), and e-privacy ($n = 18$), digital citizenship and literacy ($n = 18$), data security ($n = 12$), network security ($n = 4$), software security ($n = 3$), and phishing ($n = 6$). For example, Security Cartoons [181] is categorized as "general cybersecurity" in our analysis, because the educational comic strips cover a wide range of cybersecurity sub-topics like spoofing, malware, phishing, pharming, and passwords. In comparison, MediaSmarts' interactive comic, Top Secret [116], specifically teaches about the benefits and drawbacks of sharing information online and is therefore categorized under the subject of "e-privacy" in our analysis.

Digital games, particularly web-based games, and films and animation stand out as the predominant pedagogical approaches. The tools are created for a wide range of demographics, including both adults ($n = 68$) and children and youth ($n = 51$). The majority of educational tools for children and youth focus on teaching digital citizenship, e-privacy, and e-safety. In our article, we refer to audiences 18 and over as "adults" and those under 18 as "children and youth." In some cases, we specifically refer to "children," which are individuals under 13 years of age.

4.1 Digital Games

Digital games, including web-based games ($n = 42$) and computer games ($n = 11$), are the most widely used type of tools. Five web-based games are also available as mobile apps. We found only one game [18] released exclusively on mobile devices. Web-based games are instantly accessible

Year	Game	Film	Tabletop	Module	Comic	Other	Total
2000	1	0	0	1	0	0	2
2001	0	0	0	0	0	0	0
2002	0	0	0	0	0	0	0
2003	0	1	0	0	0	0	1
2004	0	0	0	0	0	0	0
2005	1	2	0	1	1	0	5
2006	2	2	0	0	1	0	5
2007	2	0	0	0	1	0	3
2008	1	1	0	0	1	0	3
2009	1	0	0	0	0	0	1
2010	4	0	0	0	0	0	4
2011	1	4	0	2	0	0	7
2012	8	3	1	0	1	0	13
2013	2	2	2	1	0	1	8
2014	4	4	1	1	1	0	11
2015	6	1	0	1	0	1	9
2016	3	4	2	2	1	1	13
2017	11	7	3	0	1	0	22
2018	7	2	1	0	1	0	11
2019-Jun	0	1	0	0	0	0	1
Total	**54**	**34**	**10**	**9**	**9**	**3**	**119**

Number of tools by media

Total number of tools by year

No tools

Fig. 1. Number of cybersecurity educational tools between January 2000 to June 2019. Higher intensity colours represent a larger number of tools.

online and require minimal loading time, while computer games and mobile games must be downloaded onto the users' computer or mobile device before playing. Security-themed console games exist (e.g., Watch Dogs [196]), but are created for entertainment rather than educational purposes.

Figure 3 shows an example of a web-based game that teaches users how to identify phishing URLs. Created over a decade ago, the game Anti-Phishing Phil [175] remains one of the most referenced tools for teaching phishing prevention. The player takes the role of a young fish named "Phil" who needs to eat real worms (representing URLs of legitimate websites) and avoid fake worms (representing phishing URLs). Phil's father, an experienced fish, advises the player on how to identify phishing attacks. The game includes four rounds with increasing difficulty, each focusing on different types of deceptive URLs.

Game genres adapted for cybersecurity and privacy education include quiz and puzzle (n = 17), adventure (n = 12), simulation (n = 8), strategy (n = 8), action (n = 2), serious game (n = 6),

Year	General Cybersecurity	E-safety	E-privacy	Digital Citizenship	Data Security	Phishing	Network Security	Software Security	Total
2000	0	1	0	1	0	0	0	0	2
2001	0	0	0	0	0	0	0	0	0
2002	0	0	0	1	0	0	0	0	1
2003	0	0	0	1	0	0	0	0	1
2004	0	0	0	0	0	0	0	0	0
2005	0	2	1	2	0	0	0	0	5
2006	3	1	0	0	1	0	0	0	5
2007	1	0	0	0	0	2	0	0	3
2008	1	0	0	1	0	1	0	1	4
2009	0	1	0	0	0	0	0	0	1
2010	1	0	1	0	2	0	0	0	4
2011	1	4	1	0	1	0	0	0	7
2012	3	2	5	1	2	0	0	0	13
2013	2	1	0	3	0	0	1	0	7
2014	3	3	2	1	0	0	0	1	10
2015	2	4	0	1	3	0	1	0	11
2016	4	4	4	0	0	2	0	0	14
2017	6	2	2	4	2	1	1	1	19
2018	3	2	2	2	1	0	1	0	11
2019-Jun	0	1	0	0	0	0	0	0	1
Total	**30**	**28**	**18**	**18**	**12**	**6**	**4**	**3**	**119**

Number of tools by subject

Total number of tools by year

No tools

Fig. 2. Number of tools by the educational subject between January 2000 to June 2019. Higher intensity colours represent a larger number of tools.

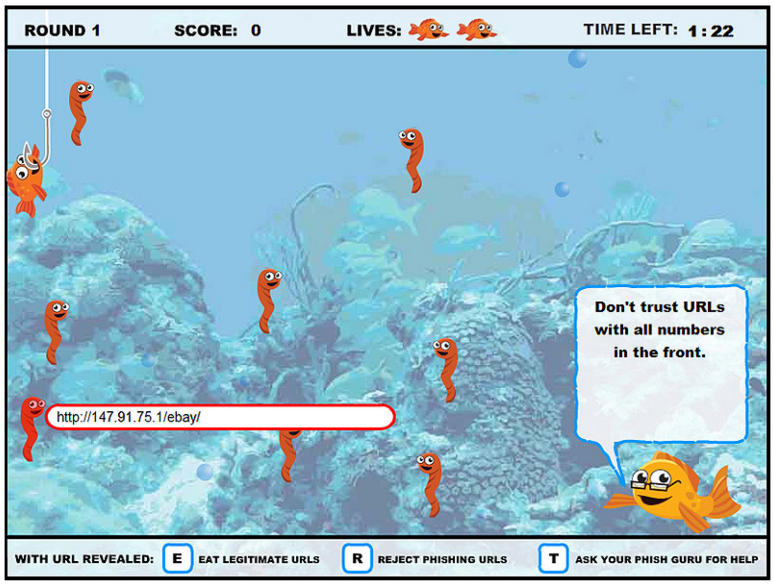

Fig. 3. A screenshot from the game Anti-Phishing Phil [175] showing a URL (lower left) and advice provided by a fish character (lower right).

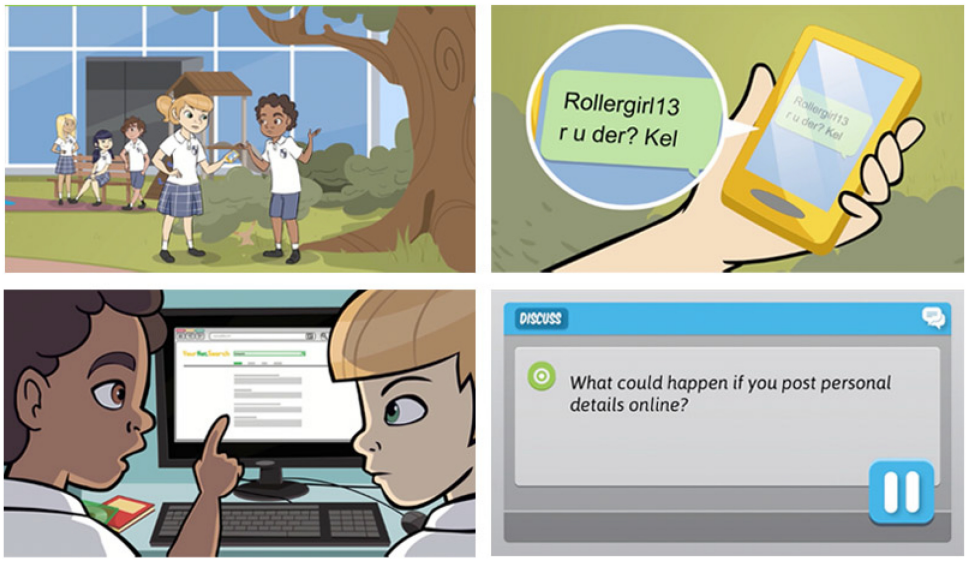

Fig. 4. Screenshots from Cybersmart Detectives that is a part of the Cybersmart Challenge [143] animated video series. The characters find a lost mobile phone (top left); The phone receives a text message to "Rollergirl13" (top right); the characters find Rollergirl13's personal information online (bottom left); a discussion screen interrupts the narrative (bottom right).

and card game ($n = 1$). The games are usually designed to balance the educational aspects with entertainment and gameplay. *Quiz games* range from traditional test-your-knowledge quizzes to quiz questions embedded into other forms of gameplay to increase engagement, such as in the platform game Share Jumper [38]. *Adventure games* include role-playing (RPGs), choose-your-own-adventure (CYOA), action-adventure, and story-based adventure. *Simulation games* challenge players' theoretical and practical knowledge by placing them in game-based environments that replicate real-world contexts. *Strategy games* involve players in tactical decision-making to outwit the presented cybersecurity challenges. Even though many of the games have a primary purpose other than pure entertainment, a few games explicitly identify with the *serious game* genre. We also found a small number of *action games* and a *card game*.

Educational digital games are used to educate both adult and children audiences. We found 27 games for adults and 27 for children and youth, suggesting educational games are prevalent for both groups. The target audience of the games created for adults range from specific (e.g., healthcare providers; corporate users) to general (e.g., end-users; general public). In contrast, all games created for children and youth specify an age range, with the youngest being five years old.

4.2 Short Films and Animation

Short films are the second most widely used types of tools we encountered. We found 34 films. Most resources are 2D animations, and six are live-action films. 3D films are rarely used for cybersecurity education. There are 25 short films created for children and youth compared to just nine films for adults, suggesting that young people are the primary target audience of educational films.

Short films are commonly released as multi-part series. For example, Figure 4 shows a part of a suite of animated videos [143] for educating primary school students about e-safety issues. Topics include protecting personal information, cyberbullying, and sharing images online. The videos are

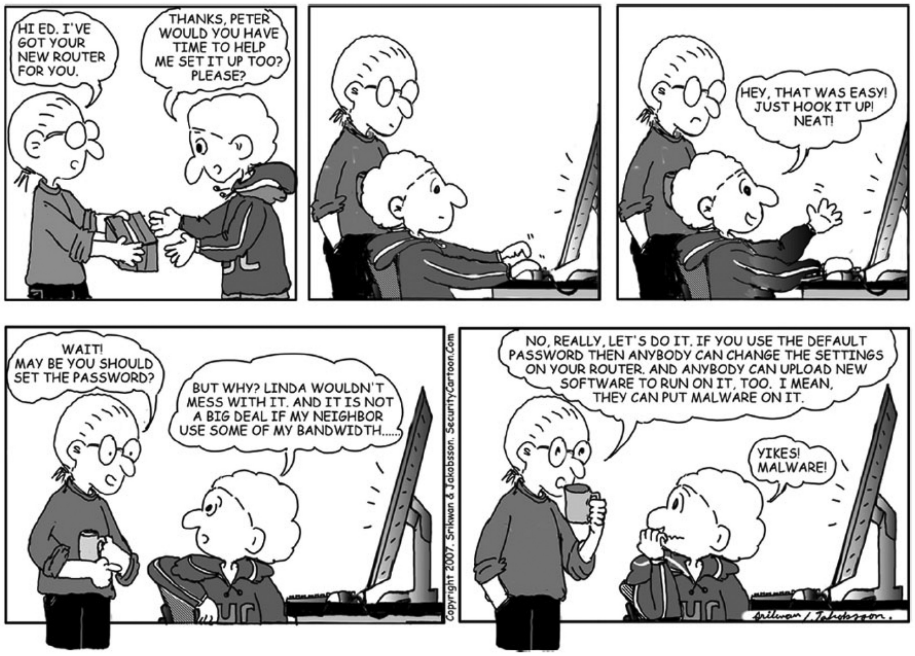

Fig. 5. Sample comic from Security Cartoons [181].

supplemented with teacher-led activities and lesson plans. We found that including supplementary material is relatively common. Seventy-one percent of the films include companion resources such as teaching guides, lesson plans, and other educational resources, suggesting that the primary purpose of short films is to scaffold other education efforts. Furthermore, due to their short lengths (30 s to 10 min, *Median* = 3 minutes), they raise general awareness about Internet safety, digital citizenship, cybersecurity, and online privacy rather than provide in-depth educational information about these topics. Most of the films we identified are less than three minutes long and aimed to raise the viewers' awareness about a specific cybersecurity or privacy topic. They use visual images, audio narration, and sounds to engage users.

4.3 Comics

We found nine educational comics, including comic strips, graphic novels, and interactive comics and narratives. Four were created for adult users and five for children and youth. To the best of our knowledge, Security Cartoons [181], shown in Figure 5, was the first major online adaptation of comics to educate end-users about Internet risks. Created in 2006, it aimed to improve security awareness and understanding via a series of short black-and-white comic strips addressing topics like spoofing, malware, phishing, pharming, and passwords. In contrast, graphic novels are single book-like narratives, such as the Social Smarts [147] graphic novel created for tweens and teens. We saw a trend in increased interactivity over the years, possibly due to the growing popularity of online comics. Digitized comics enable the addition of interactive elements over images, text, and the narrative. Compared to traditional comics, interactive comics enable user experimentation with the content and narrative and produce a game-like experience. For example, *Secure Comics* [213] include mouse-over images and text to supply the reader with additional content to portray cause-and-effect relationships and to deliver important messages in the narrative. Cyber Chronix [185]

Fig. 6. Ten Principles for Online Privacy from the Teaching Privacy Curriculum [53].

prompts the user to make several different choices that will affect the storyline and the eventual outcome of the narrative. Most comics are created for online distribution only, except for a few titles (e.g., Social Smarts [147]) that are downloadable as printable PDFs.

4.4 Learning Modules

We found nine learning modules; seven modules were created by non-profit organizations for youth ranging between preschool to high school. For example, MediaSmarts' learnings modules such as Co-Co.'s AdverSmarts [118], Click if you Agree [120], and Privacy Pirates [117]) aim to improve children's digital and media literacy. All of MediaSmarts' modules for children are guided by a pedagogical character like the cereal character "Co-Co Crunch" from Co-Co.'s AdverSmarts [118], the robot character from Click if you Agree [120], and the pirate character from Privacy Pirates [117]. Learning modules for children are sometimes branded as "games," but they are not true computer games, because they lack a system of rules and other gameplay characteristics [89]; more accurately, they use game-based learning to increase motivation and engagement [168] rather than being games in and of themselves.

We found very few free learning modules for adult use; most of the resources we encountered required paid subscriptions, and, therefore, did not meet our inclusion-exclusion criteria. Similar to films, the majority (90%) of learning modules are supported by companion resources. For example, Figure 6 shows the Teaching Privacy learning module [53] that instructs high school and undergraduate students about Ten Principles for Online Privacy; it features classroom activities that teachers could incorporate into a customized lesson plan.

Fig. 7. Control-Alt-Hack [49] box set and playing cards. The cards show (from left to right) a Hacker character card with skills, a Mission card based on security for cars, a Mission card incorporating network intrusion and humour, and a Mission card on misconceptions about hacking.

4.5 Tabletop Games

Traditional tabletop card and board games occasionally emerge as tools to teach users about cybersecurity and privacy. We included ten educational tabletop games; seven are created for adults, and three are created for school aged students. Most games require that the games pieces be downloaded, printed, and assembled, but three games have digital tabletop versions. All tabletop games we encountered have multiplayer support. They accommodate co-operative learning and encourage discussion in social settings as players uncover security lessons in the context of their actions. For example, Figure 7 shows a three to six multiplayer tabletop card game, Control-Alt-Hack [49]. The game is centred around 56 missions that introduce players, who take the role of ethical hackers, to security concepts.

4.6 Other Tools

Three cybersecurity educational tools created for academic research did not fit into the other categories but are also included in our review; they are: an interactive robot [34], an information visualization [214], and security infographics [122, 211, 212]. Ada [34] is an open-source cybersecurity education robot developed by the University of New Haven's Cyber Forensics Research and Education Group. It is capable of reading tweets and RSS feeds, checking if email accounts have been hacked, providing tips, prompting quizzes, telling jokes, and showing articles that give users cybersecurity tips and information in an interactive way. A tool called *Geo-Phisher* [214] visualizes data from a large phishing blacklist database to provide context for phishing crimes

while providing phishing prevention advice. Last, *security infographics* [122, 211, 212] with visual metaphors are used to educate users about passwords, malware, and mobile online privacy.

4.7 The Implication of Media Type for Cybersecurity Education

Our results clearly show a growing interest in using multimedia to teach users about cybersecurity and privacy. We identified five predominant media types.

For digital games, factors like fun, engagement, feedback, choice, and narrative could contribute to their success. Still, the empirical evidence thus far has not reliably identified which of these factors consistently result in successful educational outcomes [101]. Others have suggested that the rhetorical messages discovered by players through rule-based representations during gameplay (i.e., procedural rhetoric [19]) are a powerful persuasion tool. Researchers [27, 106] who have used procedural rhetoric in the design process of cybersecurity educational games found it useful at influencing security behaviour.

Unlike digital games, traditional tabletop games also support physical interactions between players [49]. Social play in a co-located space is more likely to meet players' expectations for social interaction than multiplayer online games [68]. Tabletop games are more accessible than digital games, because they can engage people with low computer literacy and are inexpensive to use in the classroom compared to computer games (e.g., require no computer lab) [68]. The game rules can be modified and adapted by players, which could help them critically and personally engage with the game content [68].

Film-based learning has led to mixed results when evaluating its effectiveness. While some researchers (e.g., Reference [110]) suggest that animation can promote understanding, others (e.g., Reference [195]) argue that animations may distract from the learning activity and they are often too complex or too fast to be perceived accurately. Films do not promote user interaction with the content and therefore support passive rather than active learning. However, short animated films usually require less time commitment from users than other educational formats.

Comics could offer greater accessibility [181], build mental models (e.g., Reference [213], increase user engagement, comprehensibility, and memorability of security and privacy information (e.g., References [93, 96, 97, 183, 207]. Comics are also used to highlight important privacy information in a user interface, but their primary purpose in those instances is to inform users about terms of service agreements (e.g., References [93, 183]) rather than to educate users.

Learning modules are characterized by grouping information into learner-paced chunks, usually presented sequentially to aid absorption of the information [168]. They rely heavily on multimedia to deliver educational content. Although learning modules support both individualized learning and collaborative learning [168], they are particularly well-suited for a classroom context [53]. This is because we found companion materials and resources like teachers' guides, lesson plans, and activities for most learning modules, suggesting that their use is mainly in a facilitated environment like a classroom. Learning modules with interactive elements and activities are sometimes referred to as "games," but they are not real computer games, because they do not incorporate rule-based game mechanics. Instead, they use game-based learning to increase motivation and engagement [168].

5 DESIGN PRINCIPLES USED IN CYBERSECURITY EDUCATIONAL TOOLS

Addressing Research Question 2, we next look at the design approaches taken by these tools. There are several broad approaches and theoretical foundations applied to the design of the tools, thus making close comparisons of the design methods difficult. They range from general instructional design models like ADDIE [41] and Instructional Design (ID) [123] (also known as Instructional Systems Design), and using design processes like user-centred design, participatory

design, iterative design, and simply gathering feedback from participants. Psychological models like PERMA [174] and security frameworks like the Information Assurance (IA) model [104] are also used. Others reference research from game design, gamification, and game-based learning. Furthermore, only 37% of tools identified any design methodology.

It became clear that work to systemize the design approaches was needed. We conducted a systematic analysis, evaluating each educational tool against established instructional design principles from the field of learning science, a body of work that aims to understand how people learn as well as to improve the design and implementation of learning technologies. In this section, we describe the method for our analysis and present the results.

5.1 Instructional Design Principles

Researchers in education have developed a large set of instructional design principles to guide the design of effective and appealing instructional materials [65]. Detailed in Table 1, we selected the ten basic principles most applicable to cybersecurity training, as proposed by Zhang-Kennedy et al. [209, 213], Kumaraguru et al. [96], and Sheng et al. [175].

The *multimedia* instruction design principle introduced in this section specifically describes the use of words and graphics together to increase learning rather than in isolation (see Table 1 for a full description). It is distinct from our general use of the word multimedia in the context of educational tools, where it describes a broader range of media combinations (e.g., audio, animation, video, interactive content). When referring to the instructional design principle, we use *italicized* text.

5.2 Method for Evaluation Using ID Principles

We conducted a systematic evaluation of the cybersecurity educational tools using the ten principles described in Table 1. To ensure a consistent analysis, we determined that a tool applied a given principle if the following five criteria were met:

- *Consistency:* The principle is consistently used. For example the *signalling* principle is identified if the tool highlights important information consistently throughout the tool; it is not used only sporadically in only parts of the tool.
- *Integrity:* The tool retains the integrity of the principle. For example, we attribute the *learning-by-doing* principle if the user performs tasks that closely reflect real-world situations (e.g., the tool presents the user with a sample phishing email/message); we do not attribute the principle if the task is presented as a description of a hypothetical scenario, such as a quiz question (e.g., "What would do you if you received an email that asks you to click on a link?").
- *Educational:* We recognize use of the principle if it is used primarily for learning purposes (e.g., the *immediate feedback* principle informs users how well they are learning; it is not used for extraneous entertainment).
- *Explicit or inferred:* We attribute the principle if the tool clearly exhibits characteristics of the principle or the creator of the tool explicitly states the use of the principle in their design. If the tool is not accessible online, then we attribute the principle if it can be inferred from available evidence (e.g., descriptions of the mechanics of the tool clearly exhibit characteristics of the principle).
- *Stand-alone assessment:* We recognize application of the principle if the tool itself exhibits characteristics of the principle, without reliance on related educational curricula or supporting materials.

Table 1. Summary of Instructional Design Principles from Learning Science

Name	Instructional Design Principle	Description
Segmenting	Segmenting lessons into learner-paced chunks rather than as a continuous unit helps people learn better.	Segmenting means breaking down complex lessons into smaller parts and present the smaller segments one at a time [36]. A classic user interface example is the "continue" button, which causes the user to pause and process the information before moving on to the next step. A study showed that learners performed better after viewing segmented lessons separated by continue buttons compared to a continuous lesson [109].
Contiguity	Aligning words to corresponding graphics increases learning performance.	Mayer et al. [108] proposed that when text and audio information are presented contiguously to related visuals instead of in isolation, the effectiveness of computer-aided instruction increases. For example, an experiment found that students performed better when text and animations were placed close to each other rather than far apart [128].
Reflection	Providing users with opportunities to reflect on what they learned increases learning.	Reflection is a form of mental processing by which the learner is given opportunities to reflect on what they have learned [156]. Research shows that learning increases when learners are prompted to stop and think about what they are doing [156].
Immediate Feedback	Giving immediate feedback helps users to assess how they are doing and provides efficient guidance in learning.	Providing learners with immediate feedback during the process of learning promotes efficient knowledge acquisition and guidance towards a target behaviour [5, 170]. Hattie and Timperley [73] suggest that supplying learners with concrete explanatory feedback that helps them improve is more useful than corrective feedback that merely states whether the learner's response is correct or incorrect.
Narrative	Presenting training material within the context of a story establishes an emotional connection with learners.	Presenting the training material within the context of a story enhances learning [107]. Mcquiggan et al. [112] showed that the motivational benefits of story-based learning on learner interest, presence, and self-efficacy are substantially more than traditional instructional approaches, suggesting that the value of story-based learning lies in the emotional connection created by stories between learners and the instructional material.
Signalling	Directing user attention to key messages in the lesson helps with information discovery and understanding.	People learn more efficiently when cues highlighting the organization of the material (e.g., bold, highlight, arrows) are added to call to attention the essential content [107]. For example, an experiment with computer security dialogues found that users are more likely to make an informed decision after viewing dialogues with visual signalling cues to draw attention to important security information [20].
Personalization	Using conversational style language and pedagogical agents create engagement and increase learning.	This principle suggests that attributing social characteristics to the user interface that resemble human-to-human interaction help people learn. Clark and Mayer [36] recommends using conversational style such as "I," "you," "we," rather than formal language in the delivery of instructional materials. Furthermore, the use of a pedagogical agent that offers instructional advice can help focus learner attention [36].
Multimedia	Combining words and images is more conductive to learning than words alone.	The multimedia principle states that using words and graphics together is more conducive to learning than when each is used in isolation [36]. The idea is based on the Dual Coding Theory [35], which suggests that graphics, text, and audio are coded into memory via separate channels. Studies have shown that the combination of related text and images creates better comprehension and increases long-term memory than text alone [108].
Conceptual-Procedural	Showing causal relationships between conceptual knowledge and procedural knowledge increases understanding of a concept.	Conceptual knowledge (i.e., a mental representation of an idea) [37], and procedural knowledge (i.e., clearly defined steps to solve a problem or complete a task) [37] mutually support one another in the construction of new knowledge [165]. For example, in an experiment to understand how students solve mathematical equivalence problem, Rittle-Johnson and Koedinger [165] found that students performed better when conceptual and procedural lessons are interleaved compared to presenting all of the conceptual lessons first and then all of the related procedures.
Learning-by-doing	Practice (by doing) strengthens acquired knowledge and skills.	"Learning-by-doing" was theorized by John Dewey [50] and refers to a form of active learning that enables learners to apply the newly acquired knowledge or skills. Research shows that learners who are given opportunities to practice what they have just learned had improved knowledge transfer and performed better in the long term than those who do not [2, 170].

ID Principle	Game	Film	Tabletop	Module	Comic	Other	Mean for All Tools
Segmenting	81	79	90	89	100	67	83
Contiguity	20	17	10	11	89	33	23
Reflection	70	17	70	22	89	33	52
Immediate feedback	81	6	80	89	67	67	58
Narrative	85	79	70	67	78	0	78
Signalling	33	29	30	33	44	33	33
Personalization	80	63	40	89	56	67	71
Multimedia	76	100	60	89	100	100	85
Conceptual-procedural	56	69	30	67	67	67	60
Learning-by-doing	67	0	30	67	44	0	41

Percentage of principles used by media

Mean percentage of principles used for all tools

No principles used

Fig. 8. Percentage of tools that exhibit each instructional design principle.

The tools were independently reviewed by two researchers using the evaluation criteria to reduce variability and bias. One researcher analyzed all 119 tools in the first round and a second researcher randomly selected and analyzed 50 tools that are accessible online in the second round. We directly interacted with the tools and read related content to identify the instructional design principles. If a tool is inaccessible online, then we identified the principles to the best of our ability from secondary sources (e.g., reading academic papers and online information; watching tutorials and demos). We attributed the instructional design principles if the tools showed clear characteristics of the principles and met our evaluation criteria. The results were recorded in Microsoft Excel. We used Cohen's Kappa (k) test to check the agreement between the two researchers and found good agreement; $k = 0.654$ (95% CI, .591 to .717), $p < 0.0005$. In the final stage of the analysis, the two researchers met to resolve the disagreements and consolidated the results. Constructive discussions between the researchers found that most of the discrepancies were due to how stringently each researcher applied the evaluation criteria. To resolve the differences, the researchers openly compared and discussed the rationale for their analysis and reached an agreement. The primary researcher re-assessed the remaining tools to align with the decisions from these discussions. The final results are summarized in the last columns of Tables 2, 3, and 4.

5.3 Application of Instructional Design Principles

The majority of the tools (70%) use between four to seven instructional design principles, but fewer than 5% use all ten principles. Figure 8 shows a heatmap that summarizes the percentage of tools from the five media categories that exhibit each instructional design principle, and the mean percentages for all tools. Furthermore, we found the percentage of tools exhibiting the principles differed when we considered those designed for adults compared to those designed for children, as summarized in Figure 9. In the following sections, we discuss which principles are commonly applied and how these differ between tool categories and target audiences.

5.3.1 Frequently Applied Principles. The four most applied instructional design principles in cybersecurity and privacy educational tools are *multimedia*, *segmenting*, *personalization*, and *narrative*. The *multimedia* principle is exhibited in 85% of the tools, indicating its use to explain cybersecurity concepts is standard practice. However, most tools other than comics do not place

Table 2. Summary of Cybersecurity Educational Tools from 2000 to 2012 and Instructional Design Principles Found in the Tools

Title	Category: Type	Subjects	Primary Audience	Reference	*Segmenting*	*Contiguity*	*Reflection*	*Immediate feedback*	*Narrative*	*Signalling*	*Personalization*	*Multimedia*	*Conceptual-Procedural*	*Learning-by-Doing*
2000 – 2005														
2025 Exmachina	Game: Serious game	E-safety	Ages 12–17	[191]	●	●	●	●	●	●	●	●	●	●
Jo Cool or Jo Fool	Module: Quiz	Digital citizenship	Grades 6–8	[113]	●			●	●		●	●		●
Jenny's Story	Film: Live-action	E-safety	High school	[31]		●	●		●		●	●		
Hector's World	Film: 2D animation	Digital citizenship	Ages 5–7	[139]	●				●		●	●	●	
NetSmartz Videos	Film: 2D/3D series	E-safety	Elementary–high school	[133]	●				●		●	●	●	
Allies and Aliens	Module: Game-based	Digital citizenship	Grades 7–8	[114]	●			●	●		●	●		
CyberPig Adventures	Game: Adventure	Digital citizenship	Ages 8–10	[115]	●		●	●	●		●	●	●	
Top Secret!	Comic: Interactive	E-privacy	Grades 6–8	[116]	●	●	●	●	●			●		
2006 – 2007														
CyberCIEGE	Game: Simulation	Cybersecurity	Post-graduate students	[190]	●		●	●	●		●	●	●	●
NSTeens Videos	Film: 2D animation	E-safety	Ages 8–17	[134]	●				●			●	●	
OnGuard Online Games	Game: Quiz	Cybersecurity	Teens	[61]	●			●	●		●	●		
OnGuard Online Videos	Film: 2D animation	Data security	Teens	[62]	●	●					●	●		
Security Cartoons	Comic: Comic strip	Cybersecurity	End-users	[181]	●	●			●			●	●	
Anti-Phishing phil	Game: Simulation	Phishing	End-users	[175]	●	●	●	●	●	●	●	●	●	●
Carnegie Cadets	Game: Simulation	Cybersecurity	Grades 4–6	[21]	●	●	●	●	●	●	●	●	●	●
PhishGuru	Comic: Comic strip	Phishing	Corporate users	[96]	●	●	●	●	●	●	●	●	●	●
2008 – 2009														
Antiphishing Program	Comic: Comic strip	Phishing	End-users	[6]	●	●	●	●		●	●	●	●	●
hACME Game	Game: Simulation	Software security	Software developers	[131]	●			●						●
Let's Fight It Together	Film: Live-action	E-privacy	Ages 11–15	[32]	●			●						●
Wild Web Woods	Game: Adventure	E-safety	Ages 7–10	[137]	●		●	●	●		●	●	●	
2010														
Cash City*	Game: Strategy	Data security	Corporate users	[126]	●				●				●	
Cyber Security Games	Game: Quiz	Cybersecurity	Students/faculty/staff	[184]	●		●	●	●	●	●	●		●
Data Security	Game: Simulation	Data security	Corporate users	[159]	●		●	●	●		●	●	●	●
Smokescreen	Game: Simulation	E-privacy	Teens 14–16	[178]	●		●	●	●		●	●		●
2011														
Counter Measures*	Game: Serious game	Cybersecurity	CS/STEM Students	[88]	●			●	●		●		●	●
I-SEE*	Module: Game-based	Data security	Post-secondary students	[169]				●			●	●	●	●
Internet Safety for Kids	Film: 2D animation	E-safety	K–3	[80]	●				●	●	●	●	●	
Lee and Kim	Film: 2D animation	E-safety	Ages 5–7	[28]					●		●	●	●	
NetSafe Utah Project	Film: 2D animation	E-safety	Kids, teens	[132]	●				●		●	●	●	
Privacy Pirates	Module: Game	E-privacy	Ages 7–9	[117]	●			●	●	●	●	●	●	
Safemoods Adventures	Film: 2D animation	E-safety	Children	[64]	●				●	●	●	●	●	
2012														
Agent Surefire	Game: Adventure	Data security	Ages 13+	[81]			●	●	●	●	●	●	●	●
Child Focus 'E-safety'	Film: 3D animation	E-safety	Ages 4–8	[45]				●	●	●		●	●	
Cybersecure	Game: Serious game	Data security	Healthcare providers	[74]	●		●	●	●		●	●		
Ministry of Sharing Test	Game: Quiz	E-privacy	General public	[187]			●	●	●	●	●	●	●	
NSTeens Games	Game: Action	Digital citizenship	Tweens and teens	[135]	●				●	●	●	●		
Identity Risk Calculator	Game: Quiz	Cybersecurity	Consumers	[44]			●					●		
Privacy Game (Print)	Tabletop: Card game	E-privacy	End-users	[12]			●	●	●	●	●	●		
Privacy Game (Web)	Game: Card game	E-privacy	End-users	[186]			●	●	●	●	●	●		
Social Smarts	Comic: Graphic novel	E-Safety	Tweens and teens	[147]	●	●	●		●			●	●	
Werewolves	Game: Strategy	Cybersecurity	Post-secondary students	[56]			●		●				●	●
Protect Your Online Rep	Film: Live-action	E-privacy	Teens	[148]	●						●	●	●	
Risk Communication Videos	Film: Live-action	Cybersecurity	End-users	[86]	●		●		●			●	●	
Zippep's Astro Circus	Game: Adventure	E-Safety	Ages 5–7	[11]	●	●	●	●			●	●	●	●

Undeployed tools are indicated with an asterisk (*). A circle symbol (●) under the instructional design principles indicates that the tool demonstrates characteristics of the principles.

Table 3. Summary of Educational Tools and Instructional Design Principles Applied (Indicated by ●) from 2013 to 2016

Title	Category: Type	Subjects	Primary Audience	Reference	*Segmenting*	*Contiguity*	*Reflection*	*Immediate feedback*	*Narrative*	*Signalling*	*Personalization*	*Multimedia*	*Conceptual-Procedural*	*Learning-by-Doing*
2013														
[d0x3d!]	Tabletop: Card game	Network security	CS/STEM students	[67]	●	●	●	●		●		●		
Auction Hero*	Game: Simulation	Phishing/Malware	Young adults	[27]	●	●	●	●	●		●	●		●
Co-Co's AdverSmarts	Module: Game-based	Digital citizenship	Ages 5–8	[118]	●			●	●		●	●		●
Control-Alt-Hack	Tabletop: Card game	Cybersecurity	CS/STEM students	[49]	●		●	●	●		●	●		
CyberSmart CyberSAFE	Film: 2D/3D	E-safety	Youth	[102]	●				●		●	●		
Digital Citizenship Lessons	Film: 2D/live-action	Digital citizenship	Elementary	[39]	●	●			●	●	●	●	●	
Digital Passport	Game: Puzzle & quiz	Digital citizenship	Grades 3–5	[38]	●		●	●	●	●	●	●	●	
Security Infographics	Other: Infographic	Cybersecurity	End-users	[211]			●	●		●	●	●		
2014														
#GAMEON	Film: Live-action	E-safety	High school	[141]	●				●			●		
B4UClick	Film: 2D/live-action	E-safety	K–12	[33]	●				●			●		
Be Deadly Online	Film: 2D animation	E-safety	High school	[140]	●	●	●		●	●	●	●	●	
Cybersecurity Lab Game	Game: Strategy	Cybersecurity	Grade 6–12	[154]	●		●	●	●			●	●	●
Cybersecurity Lab Videos	Film: 2D animation	Cybersecurity	Grade 6–12	[155]	●				●		●	●		
Friend Inspector	Game: Serious game	E-privacy	SNS users	[25]			●	●			●	●	●	●
Internet Hero*	Game: Strategy	Digital citizenship	Ages 9–12	[90]	●			●	●		●	●		●
NSTeens Comics	Comic: Interactive	Digital citizenship	Ages 11–17	[136]	●	●	●	●	●			●		●
Security Shepherd	Module: Game-based	Software security	Software engineers	[150]	●			●					●	●
Security Empire*	Game: Strategy	Cybersecurity	High school	[149]			●	●	●		●	●	●	●
The Watchers	Tabletop: Hybrid	E-privacy	Ages 11–12	[162]	●		●	●	●		●	●	●	
2015														
Ada Cybersecurity Robot	Other: Robot	Cybersecurity	End-users	[34]	●			●			●	●		
Cyber Café	Module: Game-based	E-safety	Ages 8–10	[189]	●		●	●	●	●	●	●	●	●
Digital Compass	Game: Adventure	Digital citizenship	Grades 6–8	[40]	●		●		●		●	●		●
Happy Onlife (Print)	Tabletop: Quiz	E-safety	Ages 8–12	[26]	●			●						
Happy Onlife (Web)	Game: Quiz	E-safety	Ages 8–12	[26]	●			●						
How Cyber-Savvy Are You?	Game: Quiz	Cybersecurity	Ages 5–8	[119]	●		●		●		●			
Lock Down	Game: Quiz	Data security	Unknown	[180]	●			●	●		●			●
SIRET Security Game*	Game: Serious game	Data security	Corporate users	[47]	●			●	●		●	●	●	●
Targeted Attacks	Game: Adventure	Network security	Corporate users	[192]	●		●		●		●	●	●	●
The Weakest Link	Game: Quiz	Data security	Corporate users	[84]	●			●	●	●				
Webwise Ireland	Film: 2D/live-action	E-safety	Youth	[201]	●				●			●		
2016														
Click If You Agree	Module: Game-based	Privacy notices	Ages 12–14	[120]	●		●	●	●	●	●	●	●	●
Comic Book Capers	Game: Quiz	E-safety	Ages 6+	[142]	●	●	●	●	●	●	●	●	●	●
Cyber-Five	Film: 2D animation	E-safety	Grade 3	[1]	●		●		●	●		●	●	
Cyber Threat Defender	Tabletop: Card game	Cybersecurity	High school	[23]	●			●	●			●		●
Cybersmart Challenge	Film: 2D animation	E-safety	Ages 8–10	[143]	●		●		●	●	●	●	●	
Data Privacy in Education	Film: 2D animation	E-privacy	K12 teachers	[79]	●						●	●	●	
*Geo-Phisher**	Other: Visualization	Phishing	General public	[214]	●		●	●				●	●	
How Cybersmart Are You?	Game: Quiz	E-safety	Ages 6+	[144]	●	●	●	●	●	●	●	●	●	●
Lock Down Your Login	Film: 2D animation	Cybersecurity	Consumers	[182]							●	●	●	
Secure Comics	Comic: Interactive	Cybersecurity	End-users	[213]	●	●	●		●	●	●	●	●	
Security Awareness Games	Game: Quiz	Cybersecurity	Students & staff	[188]	●		●	●	●		●			●
Smells Phishy?*	Tabletop: Board game	Phishing	End-users	[14]	●		●	●	●	●	●	●	●	●
Teaching Privacy	Module: Web-based	E-privacy	High school	[53]	●	●					●	●	●	

associated words and graphics close together, thus violating the *contiguity* principle. Text-only interfaces are found exclusively in quiz-based tools where the user is presented with multiple-choice and true-and-false questions. Eighty-three percent of tools use the *segmenting* principle to make the lessons more accessible to learners. Seventy-one percent of tools provide *personalization*, either by communicating with conversational style language or through a pedagogical agent. *Personalization* is used consistently across different media types but is more frequent in learning

Table 4. Summary of Educational Tools and Instructional Design Principles Applied (Indicated by ●) from 2017 to June 2019

Title	Category: Type	Subjects	Primary Audience	Reference	*Segmenting*	*Contiguity*	*Reflection*	*Immediate feedback*	*Narrative*	*Signalling*	*Personalization*	*Multimedia*	*Conceptual-Procedural*	*Learning-by-Doing*
2017														
Agile App Security Game	Tabletop: Card game	Software security	Novice & expert users	[202]	●		●		●				●	
Amaze Org Internet Safety	Film: 2D animation	E-safety	Ages 10–14	[4]	●		●	●	●		●	●	●	
Cloud Defense	Game: Strategy	Cybersecurity	Corporate users	[72]	●		●	●	●	●	●	●	●	●
Cyberheroes	Comic: Interactive	E-privacy	Ages 7–9	[209]	●	●	●	●	●	●	●	●	●	
Data Center Attacks	Game: Adventure	Data Security	General public	[193]	●		●		●		●		●	●
Digital Citizenship & Safety	Film: 2D animation	Digital citizenship	Teachers	[70]	●						●	●	●	
Digizen Game	Game: Adventure	Digital citizenship	Ages 11–15	[51]	●						●	●	●	
Enter IT Security Game	Game: Puzzle	Data security	Corporate users	[18]	●		●	●	●	●	●	●		●
FBI Safe Online Surfing	Game: Puzzle & quiz	Digital citizenship	Grades 3–8	[60]	●	●	●	●			●	●		
GeoCTF	Game: Strategy	E-privacy	High school & college	[208]			●	●	●	●		●	●	●
Interland	Game: Adventure	Digital citizenship	Children	[69]	●		●	●	●		●	●		
Netsim	Game: Simulation	Network security	High school	[9]	●						●		●	●
Parliamentary Digital Service	Film: 2D animation	Cybersecurity	General public	[152]	●				●			●		
Play Like Share	Film: 2D animation	E-safety	Ages 8–10	[29]	●				●			●		
Privacy Board Game	Tabletop: Board game	E-privacy	Web users	[13]	●		●	●	●					
RBC Be Cyber Smart	Film: 2D animation	Cybersecurity	RBC Clients	[167]	●				●	●		●	●	
Securing Your Identity	Film: 2D animation	Cybersecurity	Corporate & end-users	[125]		●				●	●	●	●	
What.Hack	Game: Simulation	Phishing	Unknown	[203]	●	●		●	●	●	●	●		●
World Password Day Game	Game: Adventure	Cybersecurity	General public	[111]				●	●			●		●
Your Privacy Online	Film: Live-action	E-privacy	Teens	[94]	●						●	●	●	
2018–June 2019														
A Day in the Life of the Jos	Game: Adventure	Digital citizenship	Ages 11–13	[106]	●	●	●	●	●	●	●	●	●	●
Act eSafe	Film: 2D animation	E-safety	Ages 8–11	[145]		●			●	●	●	●	●	
Band Runner	Game: Action	E-safety	Ages 8–10	[30]				●	●	●		●		
Cyber Chronix	Comic: Interactive	E-privacy	Youth	[57]	●		●	●	●		●	●		●
Cyber Threat Defender (PC)	Game: Strategy	Cybersecurity	Middle–high school	[24]	●			●	●			●		
Data Defenders	Game: Puzzle	Data security	Grades 4–6	[121]	●		●	●	●		●	●	●	
GAP*	Game: Serious game	Password security	End-users	[194]	●		●	●					●	●
Jessie & Friends	Film: 2D animation	E-safety	Ages 4–7	[130]	●				●			●	●	
King GAFA	Film: 2D animation	E-privacy	End-users	[78]	●				●			●		
Permission Impossible*	Game: Puzzle	Network security	Various users	[173]	●	●		●	●		●	●		●
Project Config.Play	Tabletop: Board game	Cybersecurity	CS students	[55]	●									●
The Lost Summer	Game: Adventure	Digital citizenship	Ages 11–14	[146]	●		●	●	●		●	●	●	●

modules and digital games. The *multimedia*, *segmenting*, and *personalization* principles are exhibited in tools created for audiences of all ages: *personalization* is used in 66% of adults' tools and 74% of children's tools; the *segmenting* and *multimedia* principles are used in the majority of children's products (88% and 94%), but comparatively less for adults (77% and 74%). Seventy-eight percent of tools exhibit the *narrative* principle. In some cases, the educational content is fully integrated into a story, while others use mini-narratives to supplement the educational content. Generally, children's tools contained more elaborate and detailed stories than the tools targeted at adults.

5.3.2 Moderately Applied Principles. More than half of the tools exhibit *immediate feedback* (58%), *reflection* (52%), and the *conceptual-procedural* principle (60%). Unfortunately, generic feedback like "correct" or "please try again" is common in our dataset. More useful feedback supports learners constructively to explain why a particular action was taken. For example, the digital literacy game A Day in the Life of Jos [106] presents players with a review screen after completing each

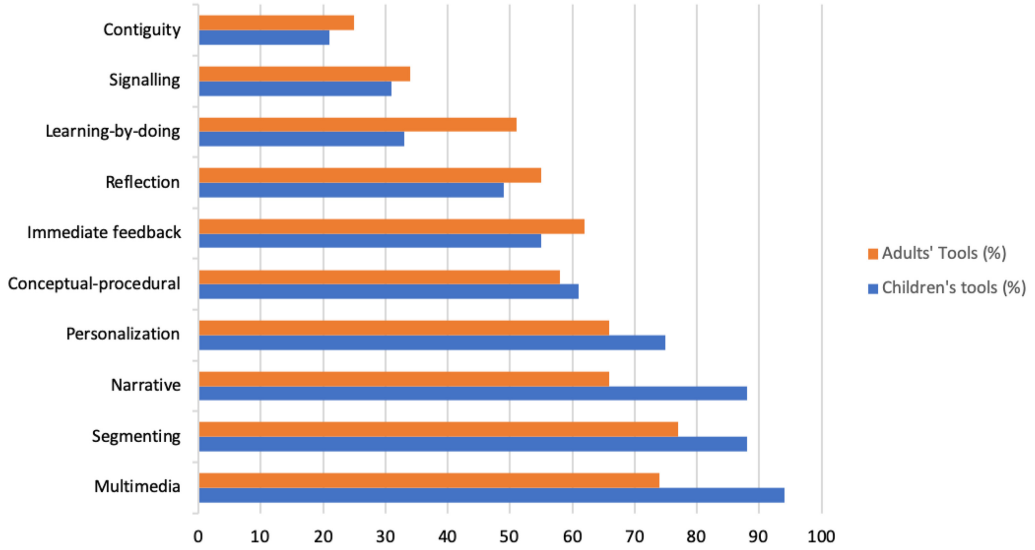

Fig. 9. Percentage of tools exhibiting each instructional design principles divided by target audience.

game level to reflect on whether they made the most appropriate choice for the characters' digital lives and provides advice on appropriate alternatives. Although generic, positive conditioning like "great job!" can also be beneficial in some circumstances, because it praises learners for the correct behaviour and thus provides encouragement. Time-bound media like films (6%) provide little or no opportunities for *Immediate feedback*, because it is typically viewed as one continuous chunk.

Half of the tools use *reflection*, often paired with feedback. Reflective moments are implemented as mini-games, interactive elements, corrective feedback, discussion prompts, and debriefing summaries. Furthermore, several tools use procedural rhetoric for reflection. For example, some educational games (e.g., References [27, 106]) enable players to make choices and explore the consequences of their actions, causing moments of reflection as the player discovers the educational message progressively through gameplay.

More than half of the tools exhibit the *conceptual-procedural* principle. For example, an anti-phishing game [97] first describes how using a search engine is a good method to identify phishing websites (i.e., conceptual knowledge), then provides tutorials about how to search for brands or domains and how to recognize fraudulent search results (i.e., procedural knowledge). We found that comics, learning modules, and films combine conceptual and procedural knowledge more frequently than digital games or tabletop games.

5.3.3 Least-applied Principles. *Learning-by-doing* (41%), *signalling* (33%), and *contiguity* (23%) are the least-used principles in cybersecurity educational tools. The *learning-by-doing* principle is sometimes used in digital games and game-based learning modules. Simulation games, in particular, provide the player with opportunities to practice and strengthen learned knowledge and skills. Half (51%) of adults' educational tools incorporate *learning-by-doing* compared to just 33% of children's tools. The *signalling* principle is more commonly exhibited in tabletop games and comics to highlight important information. Thirty-four percent of adults' tools use the *signalling* principle compared to 31% for children. Additionally, 25% of adults' tools use the *contiguity* principle compared to 21% for children;

5.4 Implications Relating to Instructional Design Principles

While prior literature from learning science suggests how instructional design principles could generally be used (e.g., Table 1), we believe it is essential to identify how the principles can also address the unique challenges in cybersecurity learning. From our review, the use of principles in this context appears to focus on three areas: creating user engagement, increasing learning by facilitating the development of appropriate mental models, and improving the tools' usability. Educators frequently utilize *multimedia*, *personalization*, *narrative* principles to activate learning and create engagement to address the problem that users typically have low motivation to learn about security [204]. "Fun and engaging" is a widely stated goal among the tools we evaluated, where the aim is to capture users' interest through a visually appealing user interface and interactive content. Instructional design principles like *segmenting* lessons into digestible pieces, providing users with *immediate feedback*, and using *signalling* to highlight essential content can all help with usability and learnability of the content. The *reflection*, *conceptual-procedural*, *contiguity*, and *learning-by-doing* principles are used to induce reasoning and problem solving among learners to address the problem that users have poor mental models of online risks and how security mechanisms work [199]. Unfortunately, design principles that aid in building mental models are only moderately used, or not used at all, in many of the tools we evaluated.

Furthermore, we note that some instructional design principles exhibited in the tools may have been incidental applications, since these were not explicitly mentioned in the publicly available information. While an instance of a principle can be effective regardless of whether it was intentionally followed, opportunities will be missed through this haphazard approach. Therefore, we propose that deliberate and thoughtful application of instructional design principles could aid the design of cybersecurity educational tools. Our analysis shows that many tools intentionally or inadvertently utilize principles that provide user engagement and content usability but neglect the principles that help users build mental models. Future designs should consider that security instruction alone might not sufficiently motivate users to practice secure behaviour; educational tools should guide users towards understanding *why* specific actions are necessary to transfer the learned knowledge to different real-life situations.

We caution that some principles may need to be applied differently for different audiences, or may have limited usefulness for some populations. For example, the *learning-by-doing* principle was found infrequently in children's tools compared to adults'. This could be because assessing online risks often involves cognitively complex processing that younger children are not developmentally equipped to handle [124]. In fact, our analysis found several other design differences between adult and children's tools. Specifically, *personalization*, *segmenting*, *multimedia*, and *narrative* principles are frequently used in children's products to support their short attention spans [161], limited memory and processing capabilities [157, 158], and low literacy skills [52]. These patterns suggest that many designers were mindful of creating age-appropriate tools that support children's developmental needs. In all cases, consideration of characteristics such as the abilities, skills, and experiences of the target audience will guide the choice of principles and how they should be applied.

6 EVALUATIONS AND EMPIRICAL DATA

Evaluating whether an educational tool meets its instructional objectives should be done through empirical data assessing its effectiveness and usability. Yet, we found that only 30% (36/119) of the tools had been evaluated. Most categories had fewer than five evaluated tools. Only 33% (3/9) of existing comics and 22% (2/9) of learning modules were evaluated. Digital games account for the largest number of existing cybersecurity educational tools, so it is unsurprising that it also had the

most evaluations. Upon closer inspection, however, only 33% (18/54) of existing games have been evaluated. In contrast, a small number of tabletop games exist, but 70% (7/10) have been evaluated. The majority of evaluated tools were part of academic research; few non-academic tools have been evaluated. Furthermore, we found that although 91% (108/119) of tools are disseminated online as learning resources, only 23% of these resources were evaluated.

A summary of the evaluation methodology used for each tool is presented in Tables 5 and 6. When available, we note the type of study (e.g., lab study), the study design with the number of conditions (e.g., between-group (×2)), and the number of sessions and the duration of the study in weeks (e.g., 2ses/2wks). Tools with more than one study are enumerated. For example, in Table 5, researchers conducted four studies to evaluate Anti-Phishing Phil—the first consisted of a lab pilot study with eight non-expert participants, and used the think-aloud protocol. This section first describes the different evaluation approaches used, including the types of evaluation, study design, and participants, then summarizes the empirical data collected to-date.

6.1 Types of Evaluation

Research methods used to evaluate the tools typically consist of lab studies conducted in a controlled environment, field studies conducted with a group of participants in their environment over some time, and web-based studies conducted completely online with no in-person contact with the participants. Data collection methods include observation, interview, pre-post tests, survey, questionnaire, eye-tracking, in-tool automated metrics, wizard-of-oz protocol, think-aloud protocol, feedback, and note-taking. Researchers often mix evaluation methods to increase ecological validity. From example, results collected from lab studies could be confirmed in a follow-up field study or a web-based study. Conducting a pilot study and formative evaluation is considered good practice before the main study to identify potential problems with the design or the research plan. These studies should include participants from the target population [99, 160].

Lab Studies: Fourteen tools used lab studies as their primary evaluation method. The studies were usually conducted in a quiet space where participants can focus on the task at hand and complete a series of predetermined tasks. Pilot studies and formative evaluations do not appear to be standard practice; only three tools in our dataset (i.e., References [96, 126, 175]) had small pilot studies to test the protocol, data collection instruments, or other relevant research techniques; another three (i.e., References [49, 106, 173]) conducted formative evaluations before the main lab study. Follow-up evaluations after a lab study are also rare; we found only one case where an online study was conducted following a lab study [173].

Field studies: We identified only ten field studies and found considerable variability between them. Time frames lasted from a single session, one week, four weeks, and fourteen weeks; and the number of participants ranged from 8 to 4,517. Some researchers [10, 12, 67, 90, 202] also conducted single or two session play tests and workshops in public settings. A few studies (e.g., References [56, 149]) have unspecified methodology information, such as missing details about the study duration or how many participants were recruited.

Web-based studies: We found only three web-based studies. One is a survey-based experiment [66] conducted online with older adults and a second is a small online study with five participants [173]. A third study [44] does not evaluate the educational tool itself but instead uses the tool to collect consumer behaviour data online.

Hybrid studies: In hybrid studies, lab studies are combined with additional tasks performed in the participant's natural environments. Such study designs retain the advantages of conducting the study in a controlled setting and gain increased ecological validity by also having users interact with the tool in their regular environments. For example, participants could perform an initial usability test of an educational game in the lab, play the game at home for a few weeks, and return

Table 5. Evaluation Methodology Summary for Digital Games

Title	Type of study	# Subjects	Demographic	Metrics	Control	Pre-Post-Tests	Usability	Learning	Engagement	Reference
DIGITAL GAMES										
2025 Exmachina	Various (Unspecified)	$n = 30$	Youth	Unknown	–	–	?	?	?	[191]
CyberCIEGE	1) Preliminary system testing of user training scenarios 2) Ad-hoc review 3) Field pilot study: Between-group (×2); 2ses/2wks 4) Field pilot study: Between-Group (×2); 2ses/1wk	(1) N/A (2) $n = 149$ (3) $n = 14$ (4) $n = 16$	N/A	(1) Game engine's response to test scenarios (2) Game logs (3–4) Questionnaire	◐	◐	–	◐	◐	[42] [87] [63] [190]
Anti-Phishing Phil	1) Lab pilot study 2) Lab study: Between-group (×2) 3) Lab study: Between-group (×3) 4) Field Study: Between-group (×2); 2ses/2wks	(1) $n = 8$ (2) $n = 28$ (3) $n = 42$ (4) $n = 4517$	Non-experts	(1) Think-aloud protocol (2) Exit survey (1–4) Test for identifying fraudulent websites	●	●	●	●	●	[97] [175]
hACME Game	Beta online study	$n = 24$	Students	Performance statistics; User feedback	–	–	◐	–	◐	[131]
Cash City	1) 2 lab pilot studies 2) Lab study: Between-group (×2)	(1) $n = 9$; $n = 43$ (2) $n = 76$	University students	(1) Interview (1–2) Questionnaire	●	●	–	●	●	[126]
Smokescreen	Focus group	Unknown	Teens; Expert critics	User feedback; Web analytics	–	–	–	–	◐	[178]
Counter Measures	Lab study: Between-group (×2)	$n = 20$	CS students	Performance statistics; Questionnaire	●	●	–	●	●	[88]
Online Risk Calculator	Web-based study	$n = 1922$	Consumers	Interactive questionnaire	–	–	–	–	–	[44]
Werewolves	Field: 1ses/wk for 4wks	Unknown	Security students	Discussion; Observation	–	–	◐	◐	◐	[56]
Auction Hero	Lab study: Cognitive walkthrough	$n = 7$	HCI researchers	Usability inspection	–	–	●	–	–	[27]
Digital Passport	Pilot & beta tests	Unknown	Children	Unknown	–	–	?	?	?	[38]
Internet Hero	Workshop playtest	$n = 36$	Children	Questionnaire; Interview; Gameplay metrics;	–	–	–	–	●	[90]
Security Empire	Preliminary field tests	Unknown	High school & university students	Gameplay metrics; Survey; Interview; Observation; Questionnaire	–	–	–	◐	◐	[149]
SIRET Security Game	Internal review	Unknown	Unknown	Questionnaire	–	–	?	?	?	[47]
A Day in the Life of the Jos	1) Formative evaluation 2) Lab study (Visual design): within-group (×3) 3) Lab study (Prototype) 4) Lab study (Functional game): 2ses/1wk	(1) $n = 16$ (2) $n = 8$ (3) $n = 14$ (4) $n = 25$	Children	(1, 3–4) Eye-tracking Questionnaire (2–4) Interview (3) Wizard-of-oz (3–4) Think-aloud protocol	–	●	●	●	●	[106]
Permission Impossible	1) Formative evaluation 2) Lab study 3) Web-based study	(1) $n = 6$ (2) $n = 5$ (3) $n = 5$	Experts & non-experts	(1) Interview; (2–3) Questionnaire	–	●	●	●	●	[173]
Happy Onlife (Web version)	1–2) Field tests	(1) $n = 8$ (2) $n = 150$	Adults & children	(1–2) User feedback	–	–	●	●	–	[26]
Netsim	Workshop playtest: 2ses	$n = 20$	High school students & teachers	Feedback	–	–	◐	–	–	[10]
GAP	Lab study: Between-group (×2)	(1) $n = 119$	CS & non-CS backgrounds	Questionnaire & test for identifying insecure password practices	●	–	●	●	●	[194]

● = comprehensive assessment; ◐ = preliminary assessment; – = did not use assessment; ? = assessment unknown.

Table 6. Evaluation Methodology Summary for Learning Modules, Comics, Tabletop Games, Films and Animation, and Other Media

Title	Type of study	# Subjects	Demographic	Metrics	Control	Pre-Post-Tests	Usability	Learning	Engagement	Reference
LEARNING MODULES										
I-SEE	Beta testing	Unknown	Unknown	Unknown	–	–	–	–	–	[169]
Teaching Privacy	Field pilot study: 14wks (pre-test: wk1; intervention: wk9&11; post-test: wk14)	$n = 119$	Non-CS majors	Survey	–	◐	–	◐	–	[53]
COMICS										
Cyberheroes	Lab study: Between-group (×2); 2ses/1wk	$n = 22$	Pairs of children & parents	Questionnaire; Interview	●	●	●	●	●	[209]
PhishGuru	1) Lab pilot study 2) Lab study: Between-group (×3); 2ses/1wk; 3) Lab study: Between-group (×3) 4) Lab study: Between-group (×4) 2ses/1wk	(1) $n = 7$ (2) $n = 42$ (3) $n = 30$ (4) $n = 56$	Non-experts	(1–2) Questionnaire (1–3) Think-aloud protocol (2–4) Tasks for identifying fraudulent emails	●	●	●	●	●	[96] [175]
Secure Comics	1) Lab study: 2ses/1wk 2) Lab study: Between-group (×2); 2ses/1wk	(1) $n = 52$ (2) $n = 22$	(1) Non-experts (2) Pairs of children & parents	(1) Eye-tracking (1–2) Questionnaire Interview	–	●	●	●	●	[213] [210]
TABLETOP GAMES										
[d0x3d!]	4 preliminary field playtests	(1) $n = 15–20$ (2) $n = 15–20$ (3) $n = 25–30$ (4) $n = 65–70$	High school and university students	Activity; Observation; User feedback	–	◐	–	◐	◐	[67]
Control-Alt-Hack	1) Formative evaluation 2) Playtests 3) Online survey 4) Lab study	(1) Unknown (2) $n = 46$ (3) $n = 22$ (4) $n = 11$	Students; Educators; Outreach officers; Non-experts	(1–2) User feedback (3) Online survey (4) Questionnaire	–	●	–	●	●	[49]
Privacy Game (Print version)	Field Playtests	$n = 130$	Various backgrounds	Observation; Discussion; Survey	–	–	●	●	●	[12]
The Watchers	1) Participatory design 2) Playtests	(1) $n = 7$ (2) $n = 7$	Children	(1–2) Discussion; User feedback; Observation	–	–	◐	◐	◐	[162]
Smells Phishy?	Lab study: 9ses/2–3 participants per session	$n = 21$	Experts and non-experts	Interview; Observation; Questionnaire	–	●	●	●	●	[14]
Agile App Security Game	Preliminary playtests	Unknown	Creators	Unknown	–	–	–	◐	◐	[202]
Happy Onlife (print version)	Field test	$n = 181$	Primary & secondary students	User feedback	–	–	●	●	–	[26]
FILM & ANIMATION										
Jenny' Story	1) Pilot study 2) Expert evaluation	(1–2) Unknown	(1) Students (2) Trainee teachers	(1) Unknown; (2) Online evaluation; response sheets	–	–	●	–	●	[206]
Let's Fight It Together	Field study	$n = 390$	Ages 11–14	Questionnaire	–	●	–	●	●	[32]
Risk Communication Videos	Web-based study: Between-group (×2)	$n = 249$	Ages 65+	Survey	●	–	–	●	–	[66]
OTHER										
Geo-Phisher	Lab study: Within-group (×2)	$n = 30$	Non-experts	Questionnaire	●	●	●	●	●	[214]
Security Infographics	1) Lab study: Between-group (×4); 2ses/1wk 2–3) Lab study: Between-group (×3); 2ses/1wk	(1) $n = 55$ (2) $n = 40$ (3) $n = 36$	(1–3) Non-experts	(1–3) Questionnaire; interview	●	●	●	●	●	[211] [213] [122]

● = comprehensive assessment; ◐ = preliminary assessment; – = did not use assessment.

for a follow-up lab session to report their experiences. Unfortunately, we found no hybrid studies in our dataset.

6.2 Study Design

Once researchers determine the type of evaluation, the next step is to design the study procedure. To increase the reliability, validity, and generalizability of the data collected, researchers use several methods to minimize experimental biases.

Control condition: In an experimental design, a control condition serves as a baseline. In our dataset, a control condition was used in ten studies. The simplest baseline is no training. For example, researchers [126] asked a control group with no prior training in information security to answer questions and compared the results to the knowledge of participants who played an educational game. To extract insights about the relative effectiveness of different designs, some researchers compared variations of their own designs to a control condition. Other studies used existing training materials as a baseline to compare the effectiveness of a proposed tool. For example, one study [175] used existing tutorials created by major corporations and compared the learning effects to an educational game. Using plain text-based learning material as control is also common. In one study [88], participants in the experimental group played an educational game while a control group read a packet of condensed computer security information. Similarly, a study with children conducted by Zhang-Kennedy et al. [209] compared the learning effects of an interactive e-book to a text-only narrative. Another study compared a video risk communication tool to a textual counterpart [66].

Pre-post-tests: A pre-post-test design compares a measure before and after an experimental treatment [99]. For example, one study by Zhang-Kennedy et al. [209] assessed children's existing knowledge about online privacy before reading an educational e-book. The same assessment was repeated after reading to measure whether their understanding improved. Not all experimental designs require a pre-post-test but it is often useful to compare participants' knowledge or behaviour before and after exposure to the educational tool, and assess its effectiveness compared to other educational methods.

Between-group and within-group experimental designs: Evaluations with two or more experimental conditions use either a between-group design (also know as "between-subject" design) or a within-group design (also known as "within-subject" design). In a between-group design, each participant is exposed to only one experimental condition. This may lead to unintended effects due to individual differences between participants (e.g., previous knowledge or experience), and more participants are needed, since each only contributes data for one condition. However, effects from exposure to multiple conditions are avoided; this is particularly important when measuring learning and knowledge, since participants cannot "unlearn" material between conditions.

In contrast, participants in a within-subject design are exposed to multiple experimental conditions one after another. This eliminates problems arising from individual participant differences, since each participant provides data for each condition. However, possible cross-over effects may be introduced from completing the same tasks under different conditions and there is potential for participant fatigue (a major consideration when working with children), which may ultimately impact performance. To reduce learning effects across conditions, the order of presentation can be counter-balanced. For example, half of the participants view condition A followed by B, while the other half view them in the reverse order. In general, researchers [99] recommend using a between-group design when the experiment requires simple tasks with where individual differences among participants are not anticipated to be problematic, or when completing tasks that could be influenced by having completed the same tasks in other condition. Conversely, a

within-subject design may be more appropriate if the experimenter expects large individual differences among participants or if the tasks are less susceptible to learning effects across conditions.

Between-group design was used more frequently than within-group design to evaluate cybersecurity educations tools in our dataset. Between-group study designs typically included two conditions tested in a lab setting, where the first condition (usually the educational tool) is contrasted with a second control condition. In a study by Zhang-Kennedy et al. [209] for example, pairs of children and parents co-learned about online privacy risks: half learned from a visual-interactive narrative e-book and half saw the same content from a text-only narrative. Other studies used three or more experimental conditions (e.g., Reference [175]) to test variations of an educational tool or different types of interventions. We found only two Within-group studies. Both had two experimental conditions where participants saw the conditions consecutively to enable them to compare the two conditions in a lab setting.

Pre-post-test: Pre-post-test designs usually involve the participants completing a pre-test before being exposed to the training material to gauge their initial attitudes, perceptions, and/or prior knowledge. A post-test is conducted after learning to assess whether any participant responses have changed as a result. The procedure could be completed in a single session or over multiple sessions. The main advantage of multi-session pre-post study designs over a single session is that researchers can assess the retention of information and the learning effects over a longer period of time. However, questions pertaining to usability problems and feedback about participants' learning experience should occur immediately after the learning component, without extended delay. Multi-session study designs may be affected by external factors between the sessions, and possible attrition of participants when scheduling participants for later sessions.

Sixteen of the studies we reviewed used a pre-post-test design. Half of the post-tests were conducted within the same session, immediately after training, and the other half were conducted in a second session, typically after a one to two-week interval. Two field-tests that were incorporated into a school curriculum took longer; one spanned four weeks [56] and the other spanned fourteen weeks [53].

6.3 Participants

Although small usability studies can have value [138, 197], a typical recommendation is to have twenty or more users [59], with their demographics closely matched to the target audience to increase certainty and validity.

In our reviewed studies, the number of participants recruited for lab studies ranged from 7 to 119. Study design influenced this choice, with between-group studies requiring the most participants, since they were divided between two or more conditions. Field and online studies were usually larger, typically with 100 to 200 participants. The largest field study (i.e., Reference [175]) conducted online has 4,517 participants.

The tools were not always evaluated with participants from the target demographic; some used a related user group. For example, post-secondary students were recruited for evaluations of tools created for "non-experts" (e.g., References [14, 175, 213, 214]). This is likely due to the reality that many studies are conducted at a university and students are easily accessible to participate. In our sample, tools created for children were always evaluated with the target age group.

6.4 Empirical Data

The primary purpose of cybersecurity educational tools is to increase cyber literacy relating to security and privacy topics, raise awareness, and, in some cases, change user behaviour. It is, therefore, essential to assess whether the tools are successful at achieving their educational goals. As it stands, there is no widely-accepted systematised evaluation method for determining the

"effectiveness" of cybersecurity educational tools. A tool's success is assessed based on different evaluation criteria, including increased awareness and retention of information, improved behaviour, positive user engagement, and good system usability. This makes comparisons between tools challenging. We organized the types of empirical data collected from 36 evaluated tools and summarized the results in Tables 5 and 6. We categorize the evaluations based on: learning, engagement, and usability. Due to the limited number of studies available, it is difficult to compare the educational impact of different categories of tools. Therefore, we synthesize the results from existing evaluations as a collective to gain an overall understanding of the effects of cybersecurity educational tools.

6.4.1 Learning. Sixty-nine percent (25/36) of evaluated tools included an assessment of learning outcomes. Results are generally positive and suggest that multimedia tools are useful for creating cybersecurity awareness and training. The respective researchers found that learning from the tools is more effective than other educational approaches when compared to text-based content [88, 97, 209, 213], existing training material from online sources [97], and other design alternatives [97, 214]. Only one study [88] showed that reading about security topics resulted in approximately the same level of learning as playing a game, and none of the evaluations showed adverse learning effects compared to other educational methods. Researchers who compared participants' security knowledge before and after learning found improvements immediately after and found that participants were able to retain the information after one week [97, 106, 209, 213]. Only one study [32] found no significant changes before and after watching an educational film. Practices such as using a pre-post-test study design and including a control condition to measure learning are not widely practiced in cybersecurity educational literature to date. Except for these eight studies, other learning assessments did not control for participants' prior knowledge or compare the tools' learning effects to other educational methods, therefore offering little reliable evidence of effectiveness.

Behavioural changes due engagement with the tool have either been gauged in lab settings using hypothetical situational scenarios to assess intended behaviour, measured using a survey instrument (e.g., privacy attitudinal scale [54]), or determined by performance tests that usually involve participants completing a series of tasks. For example, evaluations of a game that aim to increase children's digital literacy assessed intended privacy behaviour based on the participants' response to situation-based questions about what they would do in a given situation [106]. The study found that participants' intended behaviour improved significantly immediately after playing the game and one week later. An evaluation of a phishing game assessed participants' behaviour based on their ability to identify phishing websites also found improved performance [97]. Both studies showed that participants retained what they learned after one week without significant degradation in performance. The most prolonged indication of sustained security behaviour is found in a pilot of a field study for a web-based privacy curriculum [53], where the participants exhibited privacy-conscious behaviour even after fourteen weeks. It is difficult to determine how well any of these reflect real-life behaviour change.

Less is known about the tools' learning effects in the wild and their context of use, because only a small number of evaluated tools have received public adoption and usage. Current results from field studies are favourable, though not definitive due to their preliminary nature, small sample sizes, short duration, or unstructured assessments. For example, a computer game, CyberCIEGE, was incorporated into the curriculum at institutions worldwide [83], but only preliminary testing [42] and two small pilot studies were conducted [63, 87]. Another successful card game, Ctrl-Alt-Hack [49], was distributed to educators who responded positively in a survey indicating that their students' computer security awareness has increased after playing the game in the classroom. The

survey was completed by 14 educators, but did not assess students' learning directly. A web-based curriculum, Teaching Privacy [53], was piloted in a semester-long CS course at a university and found a positive shift in students' privacy attitudes. Anti-phishing educational tools, PhishGuru and Anti-Phishing Phil, became commercialized training programs. Data collected from real-world deployment of Anti-Phishing Phil showed that it is effective for knowledge acquisition and knowledge retention [97]. Other works like A Day in the Life of the Jos [106], Happy Onlife [26], and Digital Passport [38] have been distributed by government and non-profit organizations. These were validated in the lab [106], based on feedback [26], or in small pilot and beta tests [38].

A few researchers [66, 85, 199, 209, 213] made generalizable recommendations about how to improve users' poor understanding of computer security. In agreement, they advocate that educational tools should help users build mental models. Users' existing conceptualizations [85] and "folk models" [199] could be used to improve risk communication in computer security. Several studies of evaluated tools [66, 209, 213] found that using security metaphors helps users build mental models. Researchers of children's educational tools [162] recommend that children should be included as design partners, and that tools likes games could be a useful mediator for simulated experiential learning. However, others [186] concluded that multimedia tools have limited uses as stand-alone educational resources, but may be very effective as a scaffolding tool to inspire deeper education, communication, and reflection. There is evidence that educational tools facilitate privacy discussions between children and adults [26, 209].

6.4.2 Engagement. User engagement is a stated design goal for 69% (25/36) of evaluated cybersecurity educational tools. Positive engagement results are reported, but there appears to be no established definition or metric to measure the effect. Subjective reporting of engagement, such as data collected from open-ended feedback and responses to questionnaires, are more common than quantitative assessments such as measurement of users' attention.

Some associate engagement with users' positive experience and emotional reactions to the tools like "fun" [106, 175, 202], "enjoyable" [87, 88, 91, 214], "interesting" [12, 90], and "happy" [14]. In these studies, participants' self-evaluate their emotional states in questionnaires or open-ended feedback, and instruments like Likert-Scales are used to measure the level of engagement. For example, participants expressed positive emotions when asked to rate their feelings and reactions from positive to negative using a semantic scale, "happy, excited, neutral, annoyed, and angry," at different times when playing an educational tabletop game about phishing [14]. Other researchers [49, 209] determined a tool's engagement based on whether the participants would re-use the tool. Instruments such as the Again-Again Table [163] are available for this purpose. However, since the studies are conducted in the short-term, novelty effects, where users respond differently (e.g., more positively) simply because it is their first time interacting with tool, could have impacted results but these were not assessed.

To address users' inattention to security information, researchers proposed using visual attractors to emphasize important text, making it harder to ignore [20]. In this context, time and attention may be used to measure engagement. To examine users' focus of attention, researchers have used eye-tracking to record gaze data. It has primarily been used to understand fixation patterns in educational comics and visualizations, because the motivation behind these designs is to make security information more understandable and easier to read [183, 213, 214]. Elements found to attract attention include graphical components (e.g., highlight, bold) and interactive components (e.g., rollovers) [213], characters' faces [106], and text bubbles in comics [183]. Furthermore, researchers suggest that comic-based interfaces hold user attention for longer than text-based alternatives [183], and that paying more attention to security information improves users' comprehension [183, 213].

Some researchers suggest that cybersecurity educational tools could effectively support discussion and mediation between players. For example, evaluations of four tabletop games [14, 26, 67, 162] and an e-book created by us [209] similarly concluded that the tools encouraged discussion among players and may even act as a mediator between adults and children [26, 162, 209]. Children's educational tools should have a strong and engaging narrative [106, 209, 210], be age appropriate [106, 209], provide realistic choices, and offer opportunities for reflection [106].

6.4.3 Usability. We found usability studies associated with nineteen tools. Questionnaires, interviews, and feedback were frequently used to measure usability. Likert-scale and open-ended questions in questionnaires are used to gather participants' opinions about the tools' usability such as the ease of use and learnability. Interviews enable researchers to gather more detailed feedback, such as the study conducted by Monk et al. [126] that asked participants to spot usability problems and to describe whether the educational content was understandable. To elicit opinions about the design of the tools, participants were often given opportunities to provide comments such as what they liked and disliked about the tool. Due to its subjective nature, user feedback should usually be used as a complementary method along with other metrics. Users were encouraged to think aloud in four of the studies [96, 97, 106]. Think-aloud sessions are useful for understanding the participants' interactions and decisions to improve the design. Participants are usually provided with tasks to complete and asked to "think aloud" as they go. To track the participants' progress, five digital games [88, 90, 106, 131, 149] used built-in performance statistics and gameplay metrics. For example, in a game for teaching software security [131], the application stored timestamps and outcomes of the users' hacking attempts to determine the length and difficulty of the game challenges. Some researchers also recorded time-to-task-completion to determine success rates for specific tasks like information finding [92]. While eye-tracking is used in two studies to gauge users' engagement [106, 213], the gaze data is also useful for understanding which design elements participants' focus their attention and which they ignore. Last, one evaluation used usability inspection [27] and another Wizard of Oz [106] techniques. The usability studies have resulted in suggestions about how to improve the tools. However, we found that most design recommendations are difficult to scale, because they are specific to the tools evaluated and the domains that the tools were designed to address.

6.5 Evaluation Checklist

Based on best practices from human-computer interaction and the evaluation approaches discussed in our review, we provide a set of factors to consider when evaluating new or existing cybersecurity educational tools.

(1) Are target users, security domain, and the educational context clearly identified?
(2) Do the evaluation metrics clearly assess the target educational outcome?
(3) Has an empirically valid study been conducted with the target user group or a closely-related alternative? Are different types of studies with appropriate levels of ecological validity and scientific rigour being considered?
(4) Do the evaluations control for participants' prior perceptions and knowledge about the educational topic?
(5) Are novelty effects associated with use of the tool discussed?
(6) Are the intended behavioural outcome being adequately assessed to measure effectiveness at producing behavioural change?
(7) Does the evaluation assess the participants' ability to retain the knowledge and performance after a reasonable time has passed?

(8) Does the analysis consider the various contexts for using the educational tool and their associated implications?

7 RECOMMENDATIONS

Based on our analysis of cybersecurity awareness and education research, we now provide additional design considerations for future work. We organize our thoughts into three categories: adaptability, usability, and learning. This itemized list highlights the important high-level design considerations and practicalities of developing a cybersecurity educational tool. We mainly focus on voluntary unsupervised learning environments, due to their higher motivational challenges regarding learning about cybersecurity and their greater barriers to adoption (e.g., users' investment in time and effort), but many of our recommendations would also apply in more formal learning contexts. Designers of new tools may choose to focus on a subset of these design goals for their particular circumstances, but we encourage actively considering each of them and making conscious and deliberate design choices for each. Incidental or haphazard application of principles does not necessarily diminish their effectiveness when it happens, but it does mean that designers may miss valuable opportunities. Some advance consideration could significantly increase the effectiveness of the educational tool.

(1) **Adaptability:** Adaptability refers to how easily and quickly the educational tool can incorporate and communicate current cybersecurity and privacy information and enable easy access to the new material, as introduced by Srikwan et al. [181]. For example, the making of comics can be achieved relatively quickly at low cost compared to the production of games, films, and learning modules. Adaptable tools help to promote the rapid adoption of new security practices against changing threats. Low production costs and easy access to the tool help to lower the barriers of adoption for the educational content.
   (a) *Adaptable to Changing Threats:* The tool is capable of rapidly reflecting up-to-date educational content to address current cybersecurity risks and help users adopt new security practices against a changing threat.
   (b) *Easy to Access:* Users can access the tool quickly and effortlessly. The time required for setting up the tool is reasonably short. Ideally, using the tool does not require downloading specialized software, hardware, or the use of other external items (e.g., game dice, printer).
   (c) *Low Production Costs:* Integration of new educational content within the tool can be done at relatively low cost, including the monetary cost of production and the time needed to create new educational content.

(2) **Usability:** Good usability reduces the cognitive load and time spent learning how to use the tool so users can direct their attention to the educational content. Furthermore, the educational message may need to be repeatedly communicated, framed differently for various contexts, and put into practice to maximize the retention and transfer of knowledge. For example, some educational tools require users to download software (e.g., PC games) and assemble the material (e.g., printable tabletop games), but can be replayed and reused. Others like films and comics are quick to digest but may be viewed only once.
   (a) *Easy to learn:* Users who have not used the tool can learn how to use it with little time and effort.
   (b) *Efficient to use:* Learning new educational concepts can be achieved within a reasonable amount of time.
   (c) *Replayable/Reusable:* The tool has replay/reuse value for users after its first completion.

(3) **Learning:** Learning can be enhanced with active and collaborative activities. For example, games could provide users with opportunities to practice what they learned while providing constructive feedback during gameplay. Co-operative gameplay could further extend learning through discussions about the educational topic. Measurable learning outcomes ensure meaningful self-assessments and enable the evaluation of the tools' educational effectiveness.
   (a) *Active Learning:* The tool supports learners by actively engaging them in the instructional process through user interaction and feedback.
   (b) *Collaborative Learning:* Where appropriate, the tool supports discussion and mediation between users to further learning.
   (c) *Measurable Performance:* The quality of learning can easily be assessed by learners and evaluators using in-tool feedback, data analytics, and in-tool metrics.

8 RESEARCH AGENDA

Our review of cybersecurity educational tools captured a range of approaches to cybersecurity awareness and training, but many of the tools' educational effectiveness has not been verified. Nevertheless, existing research has consistently indicated positive outcomes where evaluation is available. This suggests that educational tools for cybersecurity have an important role in improving the cybersecurity ecosystem. We highlight a few key areas where additional research would be beneficial.

Educational topics. We noted that many tools focus on "traditional" topics such as creating secure passwords or identifying phishing. These are important, but we highlight a distinct need to also include education about emerging technologies, such as the Internet of Things, wearables, and components of smart cities.

Interdisciplinarity. Cybersecurity education clearly overlaps with other fields, yet our review found only weakly expressed relationships with other fields. More investigation into how knowledge from different disciplines could support and inform cybersecurity education is needed. For example, opportunities exist to draw from psychology, persuasive technology, and game studies literature for motivating sustained behaviour change. Furthermore, additional alignment and explicit use of learning science principles and strategies could be useful in designing cybersecurity educational tools. It may also be worth comparing the use of these principles in cybersecurity education to their use in other domains.

Evaluation. We found that few tools were evaluated. Moreover, the rigour of the study methodologies varied considerably. In many cases, learning was assessed solely on a general-purpose post-test without baseline assessments for prior perceptions and knowledge. Even fewer longitudinal studies measured the transfer and retention of knowledge. There is a clear need for structured, comprehensive, and robust evaluations to validate the effectiveness of cybersecurity educational tools. Learning effects were primarily evaluated based on knowledge gained and *intended* future behaviour, which may not accurately reflect users' real behaviour in their natural environment [204]. Future work needs to assess the tools' lasting impact on real world practices. We further recommend systematic examinations and comparisons of the different types of media in meeting the educational goals for specific learning contexts.

Ecological validity. There is a need to explore evaluation methodologies that have higher ecological validity without jeopardizing the users' security and privacy. Determining real-world effectiveness is challenging due to ethical concerns about exposing participants to real security and privacy risks. However, without opportunities for assessing the participants' behaviour in

their usual context of use (or simulations of the natural environment), it is difficult to predict the rates of adoption of security practices, how users would use the tool, and the long-term learning outcomes.

Engagement. For user engagement, an open question remains about how to motivate users to learn about cybersecurity outside of formal educational contexts. Security is a secondary task for many users in real life. Some researchers suggest that traditional methods of education have limited success, because *learning about security* is also a secondary concern [27]; a tool that *could* educate is ineffective if it does not receive any attention. As a starting point, embedding security learning within a primary task, such as playing a game [27] and checking email [97], could be a practical approach. Ultimately, researchers need to create teachable moments in users' daily practices for cybersecurity educational tools to have a meaningful impact on end-users' security practices.

Reporting. Establishing a consistent template for reporting on the design, evaluation methodology, analysis, and results would enable easier comparison and reproduction of the results. Future proposal and analysis of new tools should include, at minimum, motivation for the work including the expected educational context, an explanation of the design process (ideally with a publicly available prototype), a description of the study methodology and methods of analysis, and results that clearly identifies how learning, engagement, and usability were assessed. If applicable, then reflections on generalizable design recommendations would be useful for the community.

Cultural perspectives. Our analysis is influenced by the frameworks and principles on which we based our evaluations. We recognize our assessment is conducted through a specific lens and that exploring cybersecurity educational tools through other cultural perspectives or learning approaches could lead to further insights.

9 CONCLUSIONS

Our literature review answered three research questions through an analysis of *119 cybersecurity educational tools* for non-expert end-users. First, we addressed the question, *What are the current trends in using multimedia tools for educating users about cybersecurity?* We found growing use of educational tools over the past two decades, including digital games, film and animation, tabletop games, learning modules, and comics. Online games and short animated films are the most prevalent media for teaching cybersecurity. The tools target both adult and children audiences to raise awareness about general cybersecurity, e-safety, e-privacy, and digital citizenship and literacy. Second, we addressed the question, *which design principles are utilized in the tools?* We described ten instructional design principles most applicable to cybersecurity education and how they are used in existing tools. We recommend the deliberate and thoughtful application of instructional design principles. Third, we addressed the question, *How are the tools evaluated, and what is their educational impact?* We found that fewer than one-third of tools in our sample had been evaluated and there was considerable variability in study methodologies. Consequently, results from evaluations, though mostly positive, are difficult to compare and generalize. Further, there is a lack of long-term evaluations and studies comparing the effectiveness of these tools to other instructional methods. Based on our observations, we provide an evaluation checklist and recommend a more systematic approach to the design and evaluation of cybersecurity educational tools.

ACKNOWLEDGMENT

The authors thank Khadija Baig for help in reviewing the categorization of the tools.

REFERENCES

[1] ABCya. 2016. Cyber-Five Internet Safety. Retrieved from http://www.abcya.com/cyber_five_internet_safety.htm.

[2] Vincent Aleven and Kenneth R. Koedinger. 2002. An effective metacognitive strategy: Learning by doing and explaining with a computer-based cognitive tutor. *Cogn. Sci.* 26, 2 (2002), 147–179.
[3] Faisal Alotaibi, Steven Furnell, Ingo Stengel, and Maria Papadaki. 2016. A review of using gaming technology for cyber-security awareness. *Int. J. Info. Secur. Res.* 6, 2 (2016), 660–666.
[4] AMAZE. 2017. Personal Safety. Retrieved from https://amaze.org/?topic=personal-safety.
[5] John R. Anderson, Albert T. Corbett, Kenneth R. Koedinger, and Ray Pelletier. 1995. Cognitive tutors: Lessons learned. *J. Learn. Sci.* 4, 2 (1995), 167–207.
[6] Anti-Phishing Working Group. 2008. APWG CMU-Cylab phishing education landing page program. Retrieved from https://education.apwg.org/education-redirect-program.
[7] Nalin Asanka Gamagedara Arachchilage and Steve Love. 2013. A game design framework for avoiding phishing attacks. *Comput. Hum. Behav.* 29, 3 (2013), 706–714.
[8] Farzaneh Asgharpour, Debin Liu, and L. Camp. 2007. Mental models of security risks. In *Financial Cryptography and Data Security*, Vol. 4886. Springer, 367–377.
[9] Erinn Atwater and Cecylia Bocovich. 2017. CS4G Netsim. Retrieved from https://netsim.erinn.io.
[10] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, and Ian Goldberg. 2017. Live lesson: Netsim: Network simulation and hacking for high schoolers. In *Proceedings of the Workshop on Advances in Security Education (ASE'17)*. USENIX Association.
[11] Australian Communications and Media Authority (ACMA). 2012. Zippep's Astro Circus. Retrieved from https://www.esafety.gov.au/access/.
[12] David Barnard-Wills and Debi Ashenden. 2015. Playing with privacy: Games for education and communication in the politics of online privacy. *Political Studies* 63, 1 (2015), 142–160.
[13] Geraldo Barros. 2017. Privacy Board Game: The game for privacy. Retrieved from https://privacyboardgame.itidigital.org.
[14] Malak Baslyman and Sonia Chiasson. 2016. "Smells Phishy?": An educational game about online phishing scams. In *Proceedings of the APWG eCrime Summit*. IEEE, 1–11.
[15] Paulo Battistella and C. Gresse von Wangenheim. 2016. Games for teaching computing in higher education–a systematic review. *IEEE Technol. Eng. Edu. J.* 9, 1 (2016), 8–30.
[16] Kristian Beckers and Sebastian Pape. 2016. A serious game for eliciting social engineering security requirements. In *Proceedings of the Requirements Engineering Conference (RE'16)*. IEEE, 16–25.
[17] Jorge Blasco and Elizabeth A. Quaglia. 2018. InfoSec cinema: Using films for information security teaching. In *Proceedings of the Workshop on Advances in Security Education (ASE'18)*. USENIX Association.
[18] Blindflug Studios. 2017. Enter–IT Security Game. Retrieved from https://entergame.ch/en/.
[19] Ian Bogost. 2007. *Persuasive Games: The Expressive Power of Videogames*. MIT Press.
[20] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your attention please: Designing security-decision UIs to make genuine risks harder to ignore. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'13)*. ACM, 6.
[21] Carnegie Mellon University. 2007. Carnegie Cyber Academy. Retrieved from http://www.carnegiecyberacademy.com.
[22] Carnegie Mellon University. 2019. PicoCTF. Retrieved from https://picoctf.com.
[23] Center for Infrastructure Assurance and Security. 2016. Cyber Threat Defender (CTD) collectible card game. Retrieved from http://cias.utsa.edu/ctd_cards.php.
[24] Center for Infrastructure Assurance and Security. 2018. Cyber Threat Defender (CTD)—PC. Retrieved from https://cias.utsa.edu/ctd.php.
[25] Alexandra Cetto, Michael Netter, Günther Pernul, Christian Richthammer, Moritz Riesner, Christian Roth, and Johannes Sänger. 2014. Friend Inspector: A serious game to enhance privacy awareness in social networks. Retrieved from https://arXiv:1402.5878.
[26] Stephane Chaudron, Rosanna Di Gioia, Monica Gemo, and Kaat Lagae. 2015. Happy onlife: A video game to support mediation on internet risks and opportunities. *Commun. Papers* 4, 6 (2015), 47–62.
[27] Sonia Chiasson, Manas Modi, and Robert Biddle. 2011. Auction hero: The design of a game to learn and teach about computer security. In *Proceedings of the E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*. Association for the Advancement of Computing in Education (AACE), 2201–2206.
[28] Child Exploitation Online Protection Centre (CEOP). 2011. Lee and Kim. Retrieved from https://www.thinkuknow.co.uk/professionals/resources/lee-and-kim/.
[29] Child Exploitation Online Protection Centre (CEOP). 2017. Play Like Share films. Retrieved from https://www.thinkuknow.co.uk/8_10/watch/.
[30] Child Exploitation Online Protection Centre (CEOP). 2018. Band Runner. Retrieved from https://www.thinkuknow.co.uk/8_10/.

[31] Childnet International. 2005. Jenny's Story. Retrieved from https://www.childnet.com/resources/jennys-story.
[32] Childnet International. 2008. Evaluation of "Let's Fight it Together," a film from Childnet International. Retrieved from https://www.childnet.com/ufiles/LFIT-Goldsmiths-Evalutaion-Poster.pdf.
[33] Children's Advocacy Center. 2014. B4UClick. Retrieved from https://b4uclick.org/videos/.
[34] Devon Clark. 2015. Ada The Cyber Security Education Robot. Retrieved from https://www.unhcfreg.com/single-post/2015/10/13/Ada-The-Cyber-Security-Education-Robot.
[35] James M. Clark and Allan Paivio. 1991. Dual coding theory and education. *Edu. Psychol. Rev.* 3, 3 (1991), 149–210.
[36] Ruth Clark and Richard Mayer. 2011. *E-learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning*. John Wiley & Sons.
[37] Ruth C. Clark. 2011. *Developing Technical Training: A Structured Approach for Developing Classroom and Computer-based Instructional Materials*. John Wiley & Sons.
[38] Common Sense. 2013. Digital Passport. Retrieved from https://www.digitalpassport.org.
[39] Common Sense Media. 2013. Digital Citizenship Lessons. Retrieved from https://www.commonsense.org/education/lesson/follow-the-digital-trail-k-2.
[40] Common Sense Media. 2015. Digital Compass. Retrieved from https://www.digitalcompass.org/game/index.html.
[41] Wikimedia Commons. 2019. ADDIE model of design. Retrieved from https://en.wikipedia.org/wiki/ADDIE_Model.
[42] Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, and Thuy D. Nguyen. 2007. A video game for cyber security training and awareness. *Comput. Secur.* 26, 1 (2007), 63–72.
[43] Thomas M. Connolly, Elizabeth A. Boyle, Ewan MacArthur, Thomas Hainey, and James M. Boyle. 2012. A systematic literature review of empirical evidence on computer games and serious games. *Comput. Edu.* 59, 2 (2012), 661–686.
[44] EMC Corporation. 2012. EMC and NCSA Offer Free Online Identity Risk Calculator. Retrieved from https://www.prnewswire.com/news-releases/emc-and-ncsa-offer-free-online-identity-risk-calculator-172449331.html.
[45] Creative Conspiracy. 2012. Child Focus "E-safety." Retrieved from https://www.youtube.com/watch?v=d5kW4pI_VQw.
[46] Ian Cullinane, Catherine Huang, Thomas Sharkey, and Shamsi Moussavi. 2015. Cyber security education through gaming cybersecurity games can be interactive, fun, educational and engaging. *J. Comput. Sci. Colleges* 30, 6 (2015), 75–81.
[47] Ciro D'Apice, Claudia Grieco, Luca Liscio, and Rossella Piscopo. 2015. Design of an educational adventure game to teach computer security in the working environment. In *Proceedings of the 21st International Conference on Distributed Multimedia Systems (DMS'15)*. 179–185.
[48] Tamara Denning, Batya Friedman, and Tadayoshi Kohno. 2017. The Security Cards: A Security Threat Brainstorming Toolkit. Retrieved from https://securitycards.cs.washington.edu.
[49] Tamara Denning, Tadayoshi Kohno, and Adam Shostack. 2013. Control-Alt-Hack: A card game for computer security outreach and education. In *Proceedings of the Technical Symposium on Computer Science Education*. ACM, 729–729.
[50] John Dewey. 1986. Experience and education. In *The Educational Forum*, Vol. 50. Taylor & Francis, 241–252.
[51] Digizen.org. 2017. Digizen Game. Retrieved from https://www.digizen.org/resources/digizen-game.aspx.
[52] Allison Druin, Benjamin B. Bederson, Juan Pablo Hourcade, Lisa Sherman, Glenda Revelle, Michele Platner, and Stacy Weng. 2001. Designing a digital library for young children. In *Proceedings of the ACM/IEEE-CS Joint Conference on Digital Libraries*. ACM, 398–405.
[53] Serge Egelman, Julia Bernd, Gerald Friedland, and Dan Garcia. 2016. The teaching privacy curriculum. In *Proceedings of the Technical Symposium on Computing Science Education*. ACM, 591–596.
[54] Serge Egelman and Eyal Peer. 2015. Predicting privacy and security attitudes. *SIGCAS Comput. Soc.* 45, 1 (2015), 22–28.
[55] Hugo Enriquez, Youki Kadobayashi, and Doudou Fall. 2018. Project config.Play: A turn-based strategy security board game. In *Proceedings of the European Conference on Game-Based Learning (ECGBL)*. Academic Conferences and Publishing Limited, 72.
[56] Roya Ensafi, Mike Jacobi, and Jedidiah R. Crandall. 2012. Students who don't understand information flow should be eaten: An experience paper. In *Proceedings of the Conference on Cyber Security Experimentation and Test (CSET'12)*.
[57] European Commission Joint Research Centre (JRC). 2018. Understanding GDPR: New game from the JRC. Retrieved from https://ec.europa.eu/jrc/en/news/understanding-gdpr-new-game-jrc.
[58] Exosyphn Studios. [n.d.]. Hacker Evolution. Retrieved from http://www.exosyphen.com/page_hackerevolution.html.
[59] Laura Faulkner. 2003. Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. *Behavior Res. Methods Instrum. Comput.* 35, 3 (2003), 379–383.
[60] Federal Bureau of Investigation (FBI). 2017. Safe Online Surfing (SOS) Internet Challenge. Retrieved from https://www.fbi.gov/news/stories/new-safe-online-surfing-internet-challenge.

[61] Federal Trade Commission (FTC). 2006. OnGuard Online Games. Retrieved from https://www.consumer.ftc.gov/features/feature-0038-onguardonline.
[62] Federal Trade Commission (FTC). 2017. OnGuard Online Videos. Retrieved from https://www.consumer.ftc.gov/features/feature-0038-onguardonline.
[63] Chun Che Fung, Varin Khera, Arnold Depickere, Panjai Tantatsanawong, and Poonpong Boonbrahm. 2008. Raising information security awareness in digital ecosystem with games-a pilot study in Thailand. In *Digital Ecosystems and Technologies*. IEEE, 375–380.
[64] Funmoods. 2011. Safemoods Adventures from Mood-Town. Retrieved from http://www.safemoods.com.
[65] R. M. Gagne, W. W. Wager, K. C. Golas, J. M. Keller, and J. D. Russell. 2005. *Principles of Instructional Design*. Wiley Online Library.
[66] Vaibhav Garg, L. Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber. 2012. Risk communication design: Video vs. text. In *Proceedings of the Symposium on Privacy Enhancing Technologies*. Springer, 279–298.
[67] Mark Gondree and Zachary N. J. Peterson. 2013. Valuing security by getting [d0x3d!]. In *Proceedings of the Workshop on Cyber Security Experimentation and Test*.
[68] Mark Gondree, Zachary N. J. Peterson, and Tamara Denning. 2013. Security through play. *IEEE Secur. Privacy* 3 (2013), 64–67.
[69] Google. 2017. Interland—Be Internet Awesome. Retrieved from https://beinternetawesome.withgoogle.com/en/interland.
[70] Google for Education. 2017. Digital Citizenship and Safety Course. Retrieved from https://teachercenter.withgoogle.com/digital_citizenship/course.
[71] Rebecca E. Grinter, W. Keith Edwards, Mark W. Newman, and Nicolas Ducheneaut. 2005. The work to make a home network work. In *Computer Supported Cooperative Work*. Springer, 469–488.
[72] Gronstedt Group. 2017. The "Cloud Defense" game. Retrieved from http://gronstedtgroup.com/project/intuit-cyber-security/.
[73] John Hattie and Helen Timperley. 2007. The power of feedback. *Rev. Edu. Res.* 77, 1 (2007), 81–112.
[74] HealthIT.gov. 2012. Cybersecure: Your Medical Practice. Retrieved from https://www.healthit.gov/sites/default/files/cybersecure/cybersecure.html.
[75] Maurice Hendrix, Ali Al-Sherbaz, and Bloom Victoria. 2016. Game based cyber security training: Are serious games suitable for cyber security training? *Int. J. Serious Games* 3, 1 (2016), 53–61.
[76] Cormac Herley. 2009. So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the Workshop on New Security Paradigms Workshop (NSPW'09)*. ACM, 133–144.
[77] Christopher Herr and Dennis Allen. 2015. Video games as a training tool to prepare the next generation of cyber warriors. In *Proceedings of the ACM SIGMIS Conference on Computers and People Research*. ACM, 23–29.
[78] Fabio Hofer, Felix Lenz, Johanna Pichlbauer, and Kati Shipilenko. 2018. King GAFA And The Magical 0-1 Crop—A fairytale about privacy. Retrieved from https://www.kinggafa.com.
[79] iKeepSafe. 2016. Data Privacy in Education: An iKeepSafe Educator Training course. Retrieved from https://ikeepsafe.org/wp-content/uploads/2017/09/Data-Privacy-in-Education-Full-Curriculum-2017.pdf.
[80] Indiana University of Pennsylvania. 2010. Internet Safety for Kids K-3. Retrieved from https://www.youtube.com/watch?v=89eCHtFs0XM.
[81] MAVI Interactive LLC. 2012. Agent Surefire: Breach Buster. Retrieved from https://agentsurefire.com/breachbuster.
[82] Introversion Software. [n.d.]. Uplink. Retrieved from http://www.introversion.co.uk/uplink/index.html.
[83] C. Irvine, M. Thompson, and K. Allen. 2011. Active learning with the CyberCIEGE video game. In *Proceedings of the Conference on Cyber Security Experimentation and Test (CSET'11)*. 10–10.
[84] IS Decisions. 2015. The Weakest Link. Retrieved from https://www.isdecisions.com/user-security-awareness-game/.
[85] Camp Jean. 2009. Mental models of privacy and security. *IEEE Tech. Soc.* 28, 3 (2009).
[86] Camp Jean. 2012. Security Awareness & Risk Communication Videos. Retrieved from http://ljean.com/awareness/awareness.php.
[87] Jonathan Jones, Xiaohong Yuan, Edward Carr, and Huiming Yu. 2010. A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video. In *Proceedings of the IEEE Region 3's Annual Conference (SoutheastCon'10)*. IEEE, 176–180.
[88] Craig Jordan, Matt Knapp, Dan Mitchell, Mark Claypool, and Kathi Fisler. 2011. CounterMeasures: A game for teaching computer security. In *Proceedings of the Conference on Network and Systems Support for Games (NetGames'11)*. IEEE, 1–6.
[89] Jesper Juul. 2003. The game, the player, the world: Looking for a heart of gameness. In *Proceedings of the Level Up: Digital Games Research Conference*. Utrecht University, 30–45.
[90] Fares Kayali, Günter Wallner, Simone Kriglstein, Gerhild Bauer, Daniel Martinek, Helmut Hlavacs, Peter Purgathofer, and Rebbeca Wölfle. 2014. A case study of a learning game about the Internet. In *Proceedings of the International Conference on Serious Games*. Springer, 47–58.

[91] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. ACM, Article 4, 12 pages.
[92] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'10)*. ACM, New York, NY, 1573–1582. DOI: https://doi.org/10.1145/1753326.1753561
[93] Bart Knijnenburg and David Cherry. 2016. Comics as a medium for privacy notices. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'16)*. USENIX Association, Denver, CO. Retrieved from https://www.usenix.org/conference/soups2016/workshop-program/wfpn/presentation/knijnenburg.
[94] KQED Education. 2017. How to Protect Your Online Privacy. Retrieved from https://ww2.kqed.org/education/2018/02/28/how-can-you-protect-your-privacy-online/.
[95] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L. Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. 2018. Co-designing online privacy-related games and stories with children. In *Proceedings of the Conference on Interaction Design and Children (IDC'18)*. ACM, 67–79.
[96] Ponnurangam Kumaraguru, Yong Rhee, Steve Sheng, Sharique Hasan, Alessandro Acquisti, Lorrie Cranor, and Jason Hong. 2007. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In *APWG eCrime Summit*, Vol. 269. ACM, 70–81.
[97] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2010. Teaching Johnny not to fall for phish. *ACM Trans. Internet Technol.* 10, 2 (2010), 7.
[98] W. A. Labuschagne, I. Burke, N. Veerasamy, and M. M. Eloff. 2011. Design of cyber security awareness game utilizing a social media framework. In *Proceedings of the Conference on Information Security for South Africa*. IEEE, 1–9.
[99] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2010. *Research Methods in Human-computer Interaction*. John Wiley & Sons.
[100] Alexis Le Compte, David Elizondo, and Tim Watson. 2015. A renewed approach to serious games for cyber security. In *Proceedings of the Conferecne on Cyber Conflict: Architectures in Cyberspace (CyCon'15)*. IEEE, 203–216.
[101] Conor Linehan, Ben Kirman, Shaun Lawson, and Gail Chan. 2011. Practical, appropriate, empirically validated guidelines for designing educational games. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI'11)*. ACM, 1979–1988.
[102] Living in Community. 2013. SAFE in Collingwood: SAFEyouth project and video series. Retrieved from http://safeincollingwood.ca/resources-for-youth/safe-youth/.
[103] Dan Lockton, David Harrison, and Neville A. Stanton. 2010. The design with intent method: A design tool for influencing user behaviour. *Appl. Ergonom.* 41, 3 (2010), 382–392.
[104] W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale, and Don Welch. 2001. A model for information assurance: An integrated approach. In *IEEE Workshop on Information Assurance and Security*, Vol. 310. IEEE.
[105] Mabroka Maeref and Fatma Algali. 2015. An empirical evaluation of Cryptool in teaching computer security. In *Proceedings of the International Conference on Computer Science, Engineering and Applications*. 93–100.
[106] Sana Maqsood, Christine Mekhail, and Sonia Chiasson. 2018. A Day in the Life of Jos: A web-based game to increase children's digital literacy. In *Proceedings of the Conference on Interaction Design and Children (IDC'18)*. ACM, 241–252.
[107] Richard E. Mayer. 2002. Multimedia learning. *Psychol. Learn. Motivat.* 41 (2002), 85–139.
[108] Richard E. Mayer and Richard B. Anderson. 1992. The instructive animation: Helping students build connections between words and pictures in multimedia learning. *J. Edu. Psychol.* 84, 4 (1992), 444.
[109] Richard E. Mayer, Gayle T. Dow, and Sarah Mayer. 2003. Multimedia learning in an interactive self-explaining environment: What works in the design of agent-based microworlds? *J. Edu. Psychol.* 95, 4 (2003), 806.
[110] Richard E. Mayer and Roxana Moreno. 2002. Animation as an aid to multimedia learning. *Edu. Psychol. Rev.* 14, 1 (2002), 87–99.
[111] McAfee. 2017. World Password Day Game. Retrieved from https://game.truekey.com/EN/.
[112] Scott W. Mcquiggan, Jonathan P. Rowe, Sunyoung Lee, and James C. Lester. 2008. Story-based learning: The impact of narrative on learning experiences and outcomes. In *Proceedings of the Conference on Intelligent Tutoring Systems*. Springer, 530–539.
[113] MediaSmarts. 2000. Jo Cool or Jo Fool. Retrieved from http://mediasmarts.ca/game/jo-cool-or-jo-fool-grades-6-8.
[114] MediaSmarts. 2005. Allies and Aliens: A Mission in Critical Thinking. Retrieved from http://mediasmarts.ca/game/allies-and-aliens-mission-critical-thinking.
[115] MediaSmarts. 2005. Privacy Playground: The First Adventure of the Three CyberPigs. Retrieved from http://mediasmarts.ca/game/privacy-playground-first-adventure-three-cyberpigs.
[116] MediaSmarts. 2005. Top Secret!Retrieved from http://mediasmarts.ca/game/top-secret-grades-6-8.
[117] MediaSmarts. 2011. Privacy Pirates: An interactive unit on online privacy. Retrieved from http://mediasmarts.ca/game/privacy-pirates-interactive-unit-online-privacy-ages-7-9.

[118] MediaSmarts. 2013. Co-Co's AdverSmarts: An interactive unit on food marketing on the web. Retrieved from http://mediasmarts.ca/game/co-cos-adversmarts-interactive-unit-food-marketing-web.
[119] MediaSmarts. 2015. How Cyber-Savvy Are You? Retrieved from http://mediasmarts.ca/sites/mediasmarts/files/games/cyber-security-quiz/index_en.html.
[120] MediaSmarts. 2016. Click If You Agree. Retrieved from http://mediasmarts.ca/digital-media-literacy/educational-games/click-if-you-agree-grades-7-9.
[121] MediaSmarts. 2018. Data Defenders. Retrieved from http://mediasmarts.ca/sites/mediasmarts/files/games/data-defenders/.
[122] Christine Mekhail, Leah Zhang-Kennedy, and Sonia Chiasson. 2014. Visualizations to teach about mobile online privacy. In *Persuasive Technology*. 43–47.
[123] M. David Merrill, Leston Drake, Mark J. Lacy, and Jean Pratt. 1996. Reclaiming instructional design. *Edu. Technol.* 36, 5 (1996), 5–7.
[124] Miriam J. Metzger and Andrew J. Flanagin. 2008. *Digital Media, Youth, and Credibility*. MIT Press.
[125] Microsoft Cyber Defense Operations Center. 2017. Tips for securing your identity against cybersecurity threats. Retrieved from https://www.youtube.com/watch?v=BeX-imdxlxk.
[126] Thomas Monk, Johan Van Niekerk, and Rossouw von Solms. 2010. Sweetening the medicine: Educating users about information security by means of game play. In *Proceedings of the Conference of the South African Institute of Computer Scientists and Information Technologists*. ACM, 193–200.
[127] John R. Morelock and Zachary Peterson. 2018. Authenticity, ethicality, and motivation: A formal evaluation of a 10-week computer security alternate reality game for CS undergraduates. In *Proceedings of the Workshop on Advances in Security Education (ASE'18)*. USENIX Association.
[128] Roxana Moreno and Richard E. Mayer. 1999. Cognitive principles of multimedia learning: The role of modality and contiguity. *J. Edu. Psychol.* 91, 2 (1999), 358.
[129] Ajay Nagarajan, Jan M. Allbeck, Arun Sood, and Terry L. Janssen. 2012. Exploring game design for cybersecurity training. In *Proceedings of the Cyber Technology in Automation, Control, and Intelligent Systems (CYBER'12)*. IEEE, 256–262.
[130] National Crime Agency of the United Kingdom. 2019. Jessie & Friends. Retrieved from https://www.thinkuknow.co.uk/parents/jessie-and-friends/.
[131] Øyvind Nerbråten and Lillian Røstad. 2009. HACMEgame: A tool for teaching software security. In *Availability, Reliability and Security (ARES'09)*. IEEE, 811–816.
[132] NetSafe Utah. 2011. NetSafe Utah Project. Retrieved from http://www.netsafeutah.org.
[133] NetSmartz. 2005. NetSmartz Videos. Retrieved from https://www.missingkids.org/netsmartz/videos.
[134] NetSmartz. 2006. NSTeens Videos. Retrieved from https://www.nsteens.org/Videos.
[135] NetSmartz. 2012. NSTeens Games. Retrieved from https://www.nsteens.org/Games.
[136] NetSmartz. 2014. NSTeens Comics. Retrieved from https://www.nsteens.org/Comics.
[137] Netzbewegung. 2009. Wild Web Woods. Retrieved from http://www.wildwebwoods.org.
[138] Jakob Nielsen. 1994. *Usability Engineering*. Elsevier.
[139] Office of the eSafety Commissioner. 2003. Hector's World. Retrieved from http://www.hectorsworld.com.
[140] Office of the eSafety Commissioner. 2014. Be Deadly Online. Retrieved from https://www.esafety.gov.au/education-resources/classroom-resources/be-deadly-online.
[141] Office of the eSafety Commissioner. 2014. #GAMEON. Retrieved from https://www.esafety.gov.au/education-resources/classroom-resources/gameon.
[142] Office of the eSafety Commissioner. 2016. Comic Book Capers. Retrieved from https://www.esafety.gov.au/comic-book-capers.
[143] Office of the eSafety Commissioner. 2016. Cybersmart Challenge. Retrieved from https://www.esafety.gov.au/education-resources/classroom-resources/challenge.
[144] Office of the eSafety Commissioner. 2016. How Cybersmart Are You? Retrieved from https://www.esafety.gov.au/kids-quiz.
[145] Office of the eSafety Commissioner. 2018. Act eSafe. Retrieved from https://www.esafety.gov.au/education-resources/classroom-resources/act-esafe.
[146] Office of the eSafety Commissioner. 2018. The Lost Summer. Retrieved from https://www.esafety.gov.au/education-resources/classroom-resources/lost-summer.
[147] Office of the Privacy Commissioner of Canada. 2012. Social Smarts: Privacy, the Internet and you. Retrieved from https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/social-smarts-privacy-the-internet-and-you.
[148] Office of the Privacy Commissioner of Canada. 2012. What can YOU do to protect your online rep? Retrieved from https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/t-v/videos/rep/.

[149] Marc Olano, Alan Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac Sohn, and Donna Thomas. 2014. SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education. In *Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE'14)*. USENIX Association.
[150] Open Web Application Security Project. 2014. OWASP Security Shepherd. Retrieved from https://www.owasp.org/index.php/OWASP_Security_Shepherd.
[151] OWASP. 2019. Cornucopia. Retrieved from https://www.owasp.org/index.php/OWASP_Cornucopia.
[152] Parliamentary Digital Service. 2017. Cyber Security Awareness Campaign. Retrieved from https://www.youtube.com/watch?v=G8Uji_wwU7o.
[153] Vicente Pastor, Gabriel Díaz, and Manuel Castro. 2010. State-of-the-art simulation systems for information security education, training and awareness. In *Proceedings of the Education Engineering Conference (EDUCON'10)*. IEEE, 1907–1916.
[154] PBS Learning Media. 2014. NOVA Cybersecurity Lab Game. Retrieved from https://www.pbslearningmedia.org/resource/nvcy-sci-cyberlab/nova-cybersecurity-lab.
[155] PBS Learning Media. 2014. NOVA Cybersecurity Lab Videos. Retrieved from http://www.pbs.org/wgbh/nova/labs/videos.
[156] J. W. Pellegrino, J. D. Bransford, and M. S. Donovan. 1999. *How People Learn: Bridging Research and Practice*. National Academies Press.
[157] Jean Piaget. 1957. *Logic and Psychology*. Basic books, Oxford, England.
[158] Jean Piaget. 2002. *Judgement and Reasoning in the Child*. Routledge.
[159] Playgen. 2010. Data Security. Retrieved from http://playgen.com/play/data-security/.
[160] Jenny Preece, Helen Sharp, and Yvonne Rogers. 2015. *Interaction Design: Beyond Human-Computer Interaction*. John Wiley & Sons.
[161] Ashwini K. Rao and Albert Einstein. 2006. Cognition and motor skills. In *Hand Function in the Child: Foundations for Remediation*. Elsevier, 101–113.
[162] Kate Raynes-Goldie and Matthew Allen. 2014. Gaming privacy: A Canadian case study of a co-created privacy literacy game for children. *Surveil. Soc.* 12, 3 (2014), 414.
[163] Janet C. Read and Stuart MacFarlane. 2006. Using the fun toolkit and other survey methods to gather opinions in child computer interaction. In *Proceedings of the Conference on Interaction Design and Children (IDC'06)*. ACM, 81–88.
[164] Andreas Rieb and Ulrike Lechner. 2016. Operation Digital Chameleon: Towards an open cybersecurity method. In *Proceedings of the International Symposium on Open Collaboration*. ACM, 7.
[165] B. Rittle-Johnson and M. W. Alibali. 1999. Conceptual and procedural knowledge of mathematics: Does one lead to the other? *J. Edu. Psychol.* 91, 1 (1999), 175.
[166] Tiphaine Romand-Latapie. 2016. The NeoSens training method: Computer security awareness for a neophyte audience. In *Proceedings of the Black Hat USA Conference*.
[167] Royal Bank of Canada. 2017. RBC Be Cyber Smart. Retrieved from https://www.rbc.com/privacysecurity/ca/cyber-security-awareness.html.
[168] Jorge G. Ruiz, Michael J. Mintzer, and Rosanne M. Leipzig. 2006. The impact of e-learning in medical education. *Academic Med.* 81, 3 (2006), 207–212.
[169] Jungwoo Ryoo, Angsana Techatassanasoontorn, Dongwon Lee, and Jeremy Lothian. 2011. Game-based infoSec education using OpenSim. In *Proceedings of the Colloquium for Information Systems Security Education*. 101–106.
[170] Richard A. Schmidt and Robert A. Bjork. 1992. New conceptualizations of practice: Common principles in three paradigms suggest new concepts for training. *Psychol. Sci.* 3, 4 (1992), 207–218.
[171] Dino Schweitzer, Leemon Baird, Michael Collins, Wayne Brown, and Michael Sherman. 2006. GRASP: A visualization tool for teaching security protocols. In *Proceedings of the Colloquium for Information Systems Security Education*.
[172] Dino Schweitzer and Wayne Brown. 2009. Using visualization to teach security. *J. Comput. Sci. Colleges* 24, 5 (2009), 143–150.
[173] Sibylle Sehl and Kami Vaniea. 2018. Permission impossible: Teaching firewall configuration in a game environment. In *Proceedings of the European Workshop on Usable Security*.
[174] Martin Seligman. 2012. *Flourish: A Visionary New Understanding of Happiness and Well-being*. Simon and Schuster.
[175] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. 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 (SOUPS'07)*. ACM, 88–99.
[176] Adam Shostack. 2014. Elevation of privilege: Drawing developers into threat modeling. In *Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE'14)*. USENIX Association.
[177] Adam Shostack. 2018. Security Games & Resources. Retrieved from https://adam.shostack.org/games.html.
[178] Six to Start. 2010. Smokescreen. Retrieved from http://www.sixtostart.com/smokescreen/.
[179] Daniel J. Solove. [n.d.]. Teach Privacy. Retrieved from https://teachprivacy.com.

[180] Sponge UK. 2015. Lock Down: Information Security Game. Retrieved from http://spongeukweb.azurewebsites.net/storyline2/.
[181] Sukamol Srikwan and Markus Jakobsson. 2008. Using cartoons to teach internet security. *Cryptologia* 32, 2 (2008), 137–154.
[182] StaySafeOnline. 2016. Lock Down Your Login Campaign: How to Keep Your Logins Safe. Retrieved from https://www.youtube.com/watch?v=ZX0wQQo8Zb4.
[183] Madiha Tabassum, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. Increasing user attention with a comic-based policy. In *Proceedings of the Conference on Human Factors in Computing Systems (CHI'18)*. ACM, 200.
[184] Texas A&M University. 2009. Cybersecurity Games. Retrieved from https://it.tamu.edu/security/cybersecurity-games/index.php.
[185] The European Commission's science and knowledge service (JRC). 2018. Cyber Chronix. Retrieved from https://ec.europa.eu/jrc/en/news/understanding-gdpr-new-game-jrc.
[186] The Open University. 2012. Privacy Game. Retrieved from http://www2.open.ac.uk/openlearn/privacy/game/.
[187] The Open University. 2012. Sharing safely: A public information film from the Ministry of Sharing. Retrieved from http://www2.open.ac.uk/openlearn/ministry-of-sharing/.
[188] The University of Adelaide. 2016. Security Awareness Games. Retrieved from https://www.adelaide.edu.au/technology/secure-it/cybersecurity-training.
[189] ThinkUKnow. 2015. Cyber Café. Retrieved from https://www.thinkuknow.co.uk/8_10/cybercafe/cyber-cafe-base/.
[190] Michael Thompson and Cynthia Irvine. 2011. Active learning with the CyberCIEGE video game. In *Proceedings of the Conference on Cyber Security Experimentation and Test (CSET'11)*. 1–10.
[191] Tralalere. 2000. 2025 Exmachina. Retrieved from http://www.2025exmachina.net.
[192] Trend Micro. 2015. Targeted Attacks: The Game. Retrieved from http://targetedattacks.trendmicro.com/cyoa/en/.
[193] Trend Micro. 2017. Data Center Attacks. Retrieved from http://datacenterattacks.trendmicro.com.
[194] Harshal Tupsamudre, Rahul Wasnik, Shubhankar Biswas, Sankalp Pandit, Sukanya Vaddepalli, Aishwarya Shinde, CJ Gokul, Vijayanand Banahatti, and Sachin Lodha. 2018. GAP: A game for improving awareness about passwords. In *Proceedings of the Joint International Conference on Serious Games*. Springer, 66–78.
[195] Barbara Tversky, Julie Bauer Morrison, and Mireille Betrancourt. 2002. Animation: Can it facilitate? *Int. J. Hum.-Comput. Studies* 57, 4 (2002), 247–262.
[196] Ubisoft. [n.d.]. Watch Dogs. Retrieved from https://www.ubisoft.com/en-us/game/watch-dogs/.
[197] Robert A. Virzi. 1992. Refining the test phase of usability evaluation: How many subjects is enough? *Hum. Fact.* 34, 4 (1992), 457–468.
[198] Chad Walker. [n.d.]. Cryptomancer RPG. Retrieved from http://cryptorpg.com.
[199] Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'10)*. ACM.
[200] Rick Wash and Emilee Rader. 2015. Too much knowledge? Security beliefs and protective behaviors among united states Internet users. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'15)*. 309–325.
[201] Webwise. 2015. Webwise Ireland. Retrieved from https://www.webwise.ie/category/videos/classroom-videos/.
[202] Charles Weir. 2017. Using Games to Learn about Secure Development. Retrieved from https://www.securedevelopment.org/2017/10/12/games-to-help-learn-about-secure-development.
[203] Zikai Alex Wen, Yiming Li, Reid Wade, Jeffrey Huang, and Amy Wang. 2017. What.Hack: Learn phishing email defence the fun way. In *Proceedings of the CHI Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 234–237.
[204] Alma Whitten and J. Doug Tygar. 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the USENIX Security Symposium*, Vol. 348. 169–184.
[205] Laurie Williams, Andrew Meneely, and Grant Shipley. 2010. Protection Poker: The new software security game. *IEEE Secur. Privacy* 8, 3 (2010), 14–20.
[206] John Woollard, Cathy Wickens, Ken Powell, and Terry Russell. 2009. Evaluation of e-safety materials for initial teacher training: Can "Jenny's Story" make a difference? *Technol. Pedagogy Edu.* 18, 2 (2009), 187–200.
[207] Gene Yang. 2016. Comics in Education. Retrieved from http://www.humblecomics.com/comicsedu/index.html.
[208] Justin Yang, Oana-Georgiana Niculaescu, and Gabriel Ghinita. 2017. A game-oriented educational tool for location privacy topics. In *Proceedings of the SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM, 93.
[209] Leah Zhang-Kennedy, Yomna Abdelaziz, and Sonia Chiasson. 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *Int. J. Child-Comput. Interact. (IJCCI'17)* 13 (2017), 10–18.
[210] Leah Zhang-Kennedy, Khadija Baig, and Sonia Chiasson. 2017. Engaging children about online privacy through storytelling in an interactive comic. In *Proceedings of the British Computer Society Human Computer Interaction Conference (British HCI'17)*. BCS Learning & Development Ltd., 45.

[211] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2013. Password advice shouldn't be boring: Visualizing password guessing attacks. In *Proceedings of the APWG eCrime Summit*. IEEE, 1–11.
[212] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2014. Stop clicking on "update later": Persuading users they need up-to-date antivirus protection. In *Persuasive Technology*. Springer LNCS, 302–322.
[213] Leah Zhang-Kennedy, Sonia Chiasson, and Robert Biddle. 2016. The role of instructional design in persuasion: A comics approach for improving cybersecurity. *Int. J. Hum.-Comput. Interact.* 32, 3 (2016), 215–257.
[214] Leah Zhang-Kennedy, Elias Fares, Sonia Chiasson, and Robert Biddle. 2016. Geo-Phisher: The design and evaluation of information visualizations about internet phishing trends. In *Proceedings of the APWG eCrime Summit*. IEEE, 1–12.

Received March 2020; revised July 2020; accepted September 2020