Digital Tools, Approaches and Assessment for Cybersecurity Education via Storytelling: a Systematic Literature Review

Tiziano Citro[1], Giuseppina Palmieri[2,†] and Maria Angela Pellegrino[1,*,†]

[1] *Dipartimento di Informatica, Università degli Studi di Salerno, Italy*
[2] *Regional Center Information Communication Tecnology, CeRICT scrl, Naples, Italy*

Abstract

Given the increasingly interconnected world we live in, having a perception of the risks inherent in cybersecurity becomes crucial. No one is immune, and due to this pervasiveness, it is strictly required to design approaches and tools capable of educating anyone to recognize and avoid threats related to cybersecurity. Due to the effectiveness recognized to storytelling to engage learners of any age and grade, this article aims to provide an overview of current practices regarding approaches, tools, and assessments to raise awareness about cybersecurity via storytelling based on a systematic literature review.

It revises 19 relevant articles out of 60 not duplicated records indexed by major databases, i.e., Scopus, ACM Digital Library, IEEE Xplore, which are compared in terms of target audience and assessment approach. Articles are relevant if they adopt digital tools to raise awareness concerning cybersecurity. It results in 30 digital academic or commercial tools, compared in terms of availability, supporting features, and target audience. According to the review results, storytelling is an interesting approach to lower access points to cybersecurity, demonstrating that there are glimmers of use in the corporate sector, too. Storytelling is mainly used in combination with game-based approaches, simulating real scenarios or engaging participants with interactive quizzes. Although freely available tools are rare and often discontinued, there is a short list of promising digital tools publicly available along with educational material. While storytelling is used as an entry point to raise learners' awareness about cybersecurity, further effort should be invested in approaching professionals.

Keywords

Cybersecurity, Education, Storytelling, Systematic Literature Review

1. Introduction

We live in an increasingly interconnected world with the habit of exchanging information on the Web continuously. Consequently, cybersecurity is becoming a more and more pervasive issue affecting the lives of almost everyone. It implies a great need for everyone to be aware of the dangers and consequences of using technology daily. Kids start surfing the Web, looking at videos, and playing on tablets, unaware of the potential risks in cyberspace since the early stage of their childhood. This non-conscious use spurs parents' concerns about consuming inappropriate content or inadvertent personal data sharing. Similarly, older adults often lack appropriate support to protect themselves [1]. As a result, cybersecurity education knows no age, as no one is immune to the pervasiveness of issues and security threats on the Web. It requires age-appropriate mechanisms, which can be obtained by designing educational approaches tailored to specific target ages without forgetting about any user group or by thinking about approaches independent of age.

Storytelling is recognized as an effective means in learning setting as it engages learners [2, 3], from workers [4] to scholars of any age, from early education [5] to elder audience [6]. Stories stick, enabling long-term memorability, and narratives improve comprehension of visualizations [7].

2nd International Workshop on CyberSecurity Education for Industry and Academia (CSE4IA 2024), June 4th, 2024, Genoa, Italy

[*] Corresponding author.

[†] These authors contributed equally.

tcitro@unisa.it (T. Citro); pinapalmieri@gmail.com (G. Palmieri); mapellegrino@unisa.it (M. A. Pellegrino)
0009-0009-9569-5880 (T. Citro); 0000-0002-3492-6763 (G. Palmieri); 0000-0001-8927-5833 (M. A. Pellegrino)

Given these premises as a promising learning approach, we investigate whether and to what extent storytelling is explored in Cybersecurity Education. Storytelling might be beneficial in this field as learning cybersecurity requires an holistic view, keeping into consideration organizational, societal, legal, psychological, and economical aspects concerning security rather than merely focusing on technological implications [8]. It is naturally implemented via stories as technical details are abstracted, mainly focusing on dynamics and performed actions. Furthermore, stories naturally give voice to different actors spurring a collaborative dimension. By applying this principle to cybersecurity, it gives the possibility to collect and compare opinions and actions of all roles having a responsibility in cybersecurity prevention and resolution [9]. Finally, cybersecurity events are dynamic and stories easily support participants to model a cascade of events, coherently.

We analyze and compare educational programs for cybersecurity that take advantage of storytelling. Via a Systematic Literature Review approach, we extensively revise the literature indexed by major databases looking for peer-reviewed contributions in the intersection between *cybersecurity* and *storytelling*. It results in the revision of 19 articles considered relevant by two independent evaluators. Besides comparing educational approaches and their effectiveness, we are interested in identifying and comparing digital tools used in educational programs for teaching cybersecurity via storytelling.

This review aims to:

- understand the current practices related to increasing end-user awareness and education about cybersecurity via storytelling by reporting the target audience, the learning approach, the taught topic(s), the used tools, and the performed assessment,
- articulate reflections on future directions to design approaches and tools to teach cybersecurity professionals,
- encourage reproducibility and transparency of documented results by publishing row and elaborated data concerning the performed literature review as a reproducibility package, openly accessible online via Zenodo.

The structure of our work is organized as follows. Section 2 discusses the research methodology applied in this study to conduct a Systematic Literature Review and the Research Questions (RQs) that guided the study. Section 3 reports results, which are discussed along with the RQs in Section 4. Finally, Section 5 concludes the article with final thoughts and future directions.

2. Methodology

This section clarifies the research questions (RQs), the data collection process, and the inclusion criteria based on the reported literature review.

Research Questions at the basis of this literature review follow:

> RQ - What is the current situation related to increasing end-user awareness and education about cybersecurity via storytelling?

Data Collection. The literature review was conducted by in-depth reading, interpreting, and categorizing papers proposing educational activities to increase end-user awareness and education about cybersecurity and taking advantage of storytelling. The aim was to develop a comprehensive understanding and critically assess the available tools relevant to moderate this activity. This review considered studies involving any target, from scholars to workers, without distinguishing in the formulated query or the inclusion/exclusion criteria.

This review focuses on contributions with an academic structure, published as peer-reviewed articles until April 2024, and indexed by Scopus[1], ACM Digital Library[2] and IEEE Xplore[3]. Accordingly, the

[1] Scopus: https://www.scopus.com

[2] ACM Digital Library: https://dl.acm.org

[3] IEEE Xplore: https://ieeexplore.ieee.org

query results have been retrieved on April, 23rd 2024. Moreover, the procedure is fully detailed, making it possible to systematically repeat it on other databases. We used cybersecurity and storytelling and different variations of these terms as keywords. Specifically, we carried out the following query: (cybersecurity OR “cyber security” OR “cyber-security”) AND storytelling) configuring the different databases to look for the query in the title, abstract, and keyword. We apply no filters concerning the year of publication and subject areas. A total of 53 papers met these criteria, which have been integrated with hand-picked articles, reaching a total of 60 non-duplicate papers. Figure 1 summarizes the exclusion and inclusion criteria considered during the selection process on the basis of this literature review, which is detailed in the following.

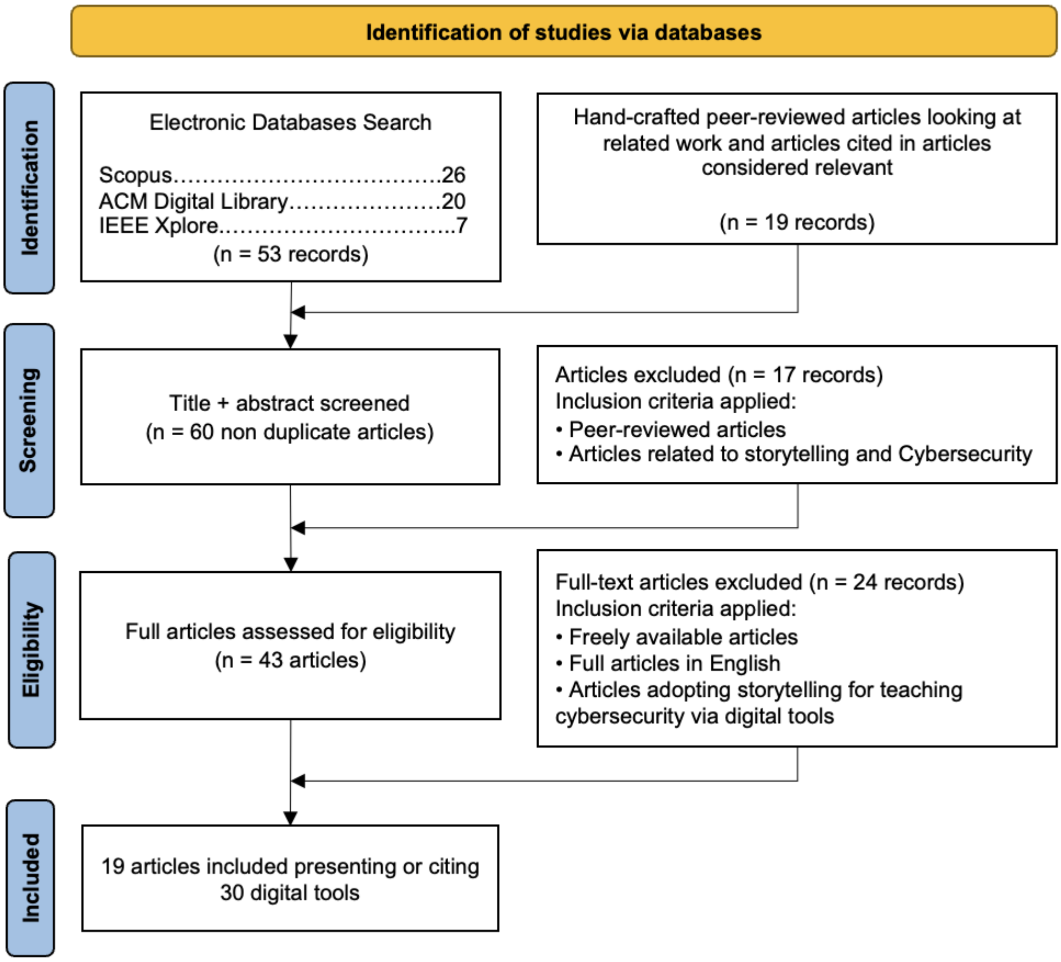
Identification of studies via databases
Identification
Electronic Databases Search
Scopus....................................26
ACM Digital Library.....................20
IEEE Xplore.................................7
(n = 53 records)
Hand-crafted peer-reviewed articles looking at related work and articles cited in articles considered relevant
(n = 19 records)
Screening
Title + abstract screened
(n = 60 non duplicate articles)
Articles excluded (n = 17 records)
Inclusion criteria applied:
• Peer-reviewed articles
• Articles related to storytelling and Cybersecurity
Eligibility
Full articles assessed for eligibility
(n = 43 articles)
Full-text articles excluded (n = 24 records)
Inclusion criteria applied:
• Freely available articles
• Full articles in English
• Articles adopting storytelling for teaching cybersecurity via digital tools
Included
19 articles included presenting or citing 30 digital tools

Figure 1: PRISMA chart describing the workflow on the basis of this literature review.

Inclusion/Exclusion criteria. The screening process started, and the eligibility criteria were set. At this stage, a paper is considered relevant and hence eligible for the review process if it is published in a peer-reviewed venue, and it applies storytelling to cybersecurity. Two researchers autonomously screened articles by reading titles and abstracts. Results were recorded in a spreadsheet which coded whether a paper was judged to be either relevant (1) or irrelevant (-1). Then, they jointly discussed coding outcomes corresponding to opposite opinions until reaching an agreement. A similar approach has been performed in the eligibility phase. At this stage, a paper is considered relevant and hence to be considered included in the review if it is available, it applies storytelling for cybersecurity awareness and education via a digital tool without any constraint on the learner’s age. More in detail, we consider any contribution reporting approaches relevant to introducing, teaching, improving awareness, or engaging users in learning about cybersecurity via storytelling in any context. The two researchers autonomously coded articles and then jointly discussed opposite codes until reaching an agreement. It results in 19 included articles, which present or cite 30 either academic or commercial digital tools.

Bias and limitations. The performed query might have missed studies targeting specific cybersecurity topics, using domain specific terminology concerning attacks, simulations, threats. However, we hypothesize that in introducing the research at least once cybersecurity is cited among title, abstract and keywords. The same thought might be related to storytelling and the risk that authors used synonyms or alternative ways to refer to the same approach.

In the current stage, the review only considers peer-reviewed contributions while collecting digital tools. Developers might opt for publishing them as open source software rather than opting for academic contributions. However, the performed process is described in so detail to enable reproducibility also on code repositories, such as GitHub, GitLab or Bitbucket, and enable the tool comparison with those cited in the literature.

Replication package. To strengthen the replicability, enable transparency, and support verification of our review, we have published a bundle with all the bibliography at each stage of the PRISMA chart annotated with comments and tags. In the replication package freely available on Zenodo at the link https://doi.org/10.5281/zenodo.11126096, the reader can see: the results of the search on Scopus, IEEE Xplore, and ACM Digital Library, both in terms of the performed query and the collection of articles matching the keyword in terms of BibTeX. Moreover, we also report hand-picked articles as a separate bibliography. These four raw bibliography files share the same prefix of $0.x$ with x progressive number from 1 to 4, combined with the name of the queried database. The `merged` file contains all distinct articles annotated with tags to distinguish eligible articles from those not. Tags are reported in the BibTeX comment per each entry, along with the cause of the not eligibility, such as `#notpeerreviewed` (3 out of 17 not eligible), `#outofscope` (13 out of 17 not eligible), documenting if an updated version of the same contribution appeared, e.g., a journal version extending a conference paper (just a single case out of 17 not eligible). All contributions satisfying inclusion criteria applied on abstracts are reported in the bibliography entitled `eligible`, which documents which article has been included or not, along with the rationale for excluding it or the taxonomy to justify and categorize the inclusion. Reasons and taxonomy are modeled as tags reported in the comment field of each entry. Reasons for exclusion are `#notpeerreviewed` (5 out of 24 not included), `#notinenglish` (1 out of 24 not included) or out of scope, e.g., not proposing a digital tool to support the cybersecurity educational activity (18 out of 24 not included). Finally, the `included` bibliography reports eligibility and inclusion comments for the 19 included articles. Cross-cutting tags concern `#debated` articles, where the final scores required a discussion among evaluators. While raw articles are available as bib files, the articles corresponding to the merging, eligibility, and inclusion stages are accessible as bib files and HTML tables to simplify readability. The reproducibility package is completed by a `index` file that documents the procedure followed.

3. Results

We come up with 19 included contributions summarized in Table 1, along with the tool(s) used, the target audience, and the addressed topic. The `assessment` column in Table 1 reports the performed assessment or the intended goal in proposing the educational activity as declared by authors by distinguishing approaches to engage, introduce, improve awareness, creativity, or let participants learn about cybersecurity by focusing on the impact on participants, meanwhile keeping track of contributions that involved target audience in the co-design of the toolkit or performed a usability assessment. We consider relevant to emphasize contributions performing co-design or usability studies as they are rare even if it is crucial to collect end-users feedback and improve the digital tool before measuring the impact that tools might have on end-users. The `target` column in Table 1 reports age when explicitly outlined in the evaluation of the revised contribution, keeping it generic when a target audience is reported at the design level, often missing a formal assessment.

Each included contribution presented a technology-enhanced educational scenario. As a result, Table 2 compares tools by distinguishing commercial solutions, i.e., those released by companies,

Table 1
Included articles discussing educational activities to teach cybersecurity via storytelling. Contributions are sorted by years. We mark in gray all the studies that involve usability testing or co-design approaches.

Ref.	Year	Tool(s)	Assessment	Target	Topic
[10]	2005	CyberCIEGE	Learning	-	Network security
[11]	2009	PhishGuru	Awareness	University	Phishing emails
[12]	2009	PlayingSafe	Awareness	Aged 18-over 45	Security
[13]	2015	CyberAware	Learning Usability	Aged 9-11	Cybersecurity basics
[14]	2015	SEAG	Learning	Aged 18-40	Social engineering
[15]	2017	Creative Suite, GameSaladCreator	Awareness	Aged 10-14	Cyber risks
[16]	2018	CyberBullet	Co-design	Children	Online safety
[17, 18]	2019	Comic-BEE	Awareness	Employees & Aged 13-17	Information security
[19]	2019	What.Hack	Engagement Effectiveness	University	Phishing attacks
[20]	2020	CyberVR	Engagement Learning	Aged 24-34	Security
[21]	2020	YourNetStory, RouterJoyVis	Awareness	Laypersons	Network traffic
[22]	2020	Powtoon, Pixton, Plotagon	Awareness	Teachers	Cyber risks
[23]	2021	Wolf, Hyena, and Fox	Awareness	Pre-school children	Intrusion attempts
[24]	2021	Zenbo	Impressions	Educators	Information security
[25]	2022	Criminal Investigation	Accessibility Engagement Learning	University	IoT security
[26]	2022	PrivacyToon	Creativity	University & Educators	Privacy
[27]	2023	HyMN	Learning	Vulnerable groups	Safety
[28]	2023	Ontology driven GUI	Mitigate impact	Workers	Vulnerability

and academic ones, referred to by included articles. Moreover, digital tools are classified according to the educational approach in which the tool has been used, extending the classification proposed by Chowdhury and Gkioulos [29]. In particular, we classified tools as *game-based approaches*, e.g., serious games, gamified environments or simulation platforms for teaching cybersecurity, *video-based approaches*, focused on the use of recorded videos as educational material, *comics* and *other approaches*. Tools are compared in terms of accessibility as explicitly modeled via the `link` column that reports how to access it, along with the link's status and the tool's free nature. Moreover, for each tool, we report the topic distinguishing between general purpose and domain-specific tools, the target audience, and the technology used for the delivery mode if it enables authoring and supports collaboration. In the following, we discuss tools according to the educational approach that exploits them.

Game-based approaches mainly use storytelling in terms of storyline. Educational approaches in this category often combine interactive quizzes as checkpoints to assess learned concepts with gamified elements such as awards in the case of correct replies and levels of increased complexity to challenge participants. INTERLAND [34], Carnegie Cadets [30], PBS Cybersecurity Lab [31], CyberBullet [16], Wolf, Hyena, and Fox game [23], Criminal Investigation [25], PlayingSafe [12], SAEG [14] belong to this category. As an alternative to quiz, What.Hack [19] engages participants with sequence of puzzles, while CyberCIEGE [10], PhishGuru [11], CyberVR [20], Watch Dogs [35], Deus Ex [32], and Hacker Evolution Duality [33] opt for role-playing video games simulating realistic scenarios concerning phishing attacks or security in general.

Table 2: Tools used or cited in the included articles. Tools are divided according to the approach used in the educational activity. Rows in gray report commercial solutions. Legend: - means not supported or not explicitly reported, ∼ means partially supported, while blanks mean not applicable.

Tool	Link	Working	Free	Topic	Target	Delivery	Authoring	Collaborative	Material
Game-based approach									
Carnegie Cadets	[30]	∼	✓	Cybercitizens	Middle & High	Desktop	-	-	✓
Criminal Investigation	-	-		IoT security	Learners	Web	-	-	-
CyberAware	-	-		Cybersecurity	Primary	Mobile	-	-	-
CyberBullet	-	-		Online safety	Children	Mobile & Desktop	-	-	-
CyberCIEGE	-	-		Network security	Learners	Desktop	-	-	-
Cybersecurity Lab	[31]	✓	✓	Cybersecurity	Primary & Middle	Web	-	✓	✓
CyberVR	-	-		Cybersecurity	Learners	VR	-	-	-
Deus Ex	[32]	✓	-	Cybersecurity	All	Desktop & PlayStation	-	✓	-
Hacker Evolution Duality	[33]	✓	-	Hacking	All	Desktop	-	-	-
Hypermedia Novels (HyMN)	-	-		General-purpose	Learners	Desktop & Web	✓	-	-
INTERLAND	[34]	✓	✓	Digital citizenship & Safety	Learners	Web	-	-	✓
PhishGuru	-	-		Phishing	Learners	Web	-	-	-
PlayingSafe	-	-		Cybersecurity	Learners	-	-	✓	-
SEAG	-	-		Cybersecurity	Learners	-	-	-	-
Watch Dogs	[35]	✓	-	Hacking	All	Desktop & PlayStation	-	✓	-
What.Hack	-	-		Phishing	Learners	Web	-	-	-
Wolf, Hyena, and Fox	-	-		Cybersecurity awareness	Pre-school	Mobile	-	-	-
Video-based approach									
Pixton	[36]	✓	✓	General-purpose	All	Web	✓	-	-
Plotagon	[37]	✓	-	General-purpose	All	Mobile & Desktop	✓	-	-
Powtoon	[38]	✓	-	General-purpose	All	Web	✓	✓	-
Comics									
Comic-BEE	[39]	✓	∼	General-purpose	Learners	Web	✓	-	∼
comicgen	[40]	✓	✓	General-purpose	All	Web	✓	-	∼
Creative Suite	[41]	✓	-	General-purpose	All	Desktop	✓	✓	-
GameSalad Creator	[42]	✓	∼	General-purpose	Learners	Desktop	✓	-	-
PrivacyToon	[43]	✓	✓	Privacy	All	Web	✓	-	-
StoryboardThat	[44]	✓	∼	General-purpose	All	Web	✓	✓	✓
Other approaches									
Ontology driven GUI	-	-		Cybersecurity	Workers	Web	-	-	
RouterJoyVis	[45]	-		Home router traffic data	Learners	Web	-	-	-
YourNetStory	[46]	-		Home router traffic data	Learners	Web	-	-	-
Zenbo	[47]	✓	-	General-purpose	All	Robot	-	✓	-

Video-based approaches are all proposed by the contribution authored by Khalid et al. [22], which assists primary school teachers in raising awareness and conveying the fundamental principles of cybersecurity to primary school children aged 7-13 in Africa, by letting them authoring videos with general-purpose video editing tools.

Comics-based approaches mainly focus on characters and roles involved in cybersecurity. All the tools supporting this kind of approach enable and require learners to author comics via general-purpose tools, such as Creative Suite [41], GameSalad Creator [42], comicgen [40], StoryboardThat [44], ComicBEE [39], or environments tailored to domain-specific scenarios, such as PrivacyToon [43] which focuses on privacy-related issues.

Uncategorized approaches include experiments with social robots, such as Zenbo [47], or interfaces used mainly by professionals to detect, organize, and render vulnerabilities to workers, such as visualization interfaces RouterJoyVis [45] and YourNetStory [46] used to visualize home router traffic data [21] or ontology driven storytelling GUI to let workers identify vulnerabilities in log files [28].

4. Discussion

This section discusses results by organizing insights according to takeaways. Discussions will be aligned with RQs in the conclusions.

A handful of working and freely available tools. According to the performed systematic literature review, we devised 30 tools used or cited by educational activities to teach cybersecurity. They are almost equally distributed between academic and commercial tools, as evident by white and gray rows in Table 2. However, if we focus on available tools, the number narrows to 18, moving to 15 if we limit fully working tools, and only five if we are also interested in freely available solutions. This change in number may be mainly related to the interest in defining prototypes for research purposes, followed by the lack of funding and discontinuity in maintenance observed in academia. The five completely working and freely available tools are web-based and are almost commercial solutions, where CyberSecurity Lab [31], INTERLAND [34], and PrivacyToon [43] are domain-specific and tailored on privacy and (cyber)security topics, while Pixton [36] and comicgen [40] are general purpose tools that can have been used in cybersecurity learning activities.

Actively engage participants. Collaboration is widely exploited in learning settings because of its effectiveness concerning individual efforts [48]. However, only 8 out of 30 tools were used in the surveyed articles exploring cybersecurity education via storytelling support collaboration. It is a surprising insight as cybersecurity may benefit from collaboration [24] as it naturally involves different actors, which can be simulated via role-playing. Meanwhile, stories can be easily created and understood in collaboration [9]. The limited use of collaboration might be justified by how the included work interprets the concept of stories. Stories are mainly interpreted as storylines in game-based approaches rather than an opportunity to challenge participants to narrate real scenarios, giving voice to involved roles and actors, envisioned only in video-based and comic-based approaches. The passive role of participants is also confirmed by the only partial support of authoring features in tools, covered only by 10 out of 30 tools, as documented by the `authoring` column in Table 2. Digital games emerge as the most explored approach to teaching cybersecurity, coherently with the literature [49, 50].

Learning impact VS Usability. The included articles mainly focus on the impact of activities on participants, assessing the increase in awareness (7 out of 19), learning outcomes (6 out of 19), obtained engagement (3 out of 19), effectiveness, creativity, and collecting users impressions. It results in a sufficiently high interest in raising users' awareness, going even deeper by measuring achieved learning. To name an uncommon practice among reviewed articles, Kumaraguru et al. [11] measured learning via a longitudinal study. Only 3 out of 19 assess the usability or accessibility of used or proposed tools by target groups or involving end-users in co-design solutions. More in detail, Criminal Investigation [25] involves university students in the assessment and reports positive feedback on user interface and accessibility without detailing quantitative results. CyberBullet [16] involves children in co-designing the tool but needs a formal assessment. CyberAware [13] collects feedback with a 5-point Likert scale from children participating in the assessment concerning the usage of the application, reporting that two-thirds encountered no problem while playing and consider informative all the displayed messages. However, it is worth noting that all the articles assessing tool usability and accessibility target learners rather than workers. Further effort should be invested in tailoring interfaces to users' needs via user-centered design approaches, paying more attention to professionals' needs.

Learners rather than professionals. Focusing on the target of the tools reported in Table 2, 18 of 30 tools are proposed for learners of different ages and grades. A single tool is tailored for workers, while everyone can use 11 out of 30 other tools. As a result, few tools are designed for professionals. A similar result is obtained by focusing on the assessment target reported in Table 1 as only 2 out of 19 articles involve employees among evaluation participants. The interest in applying storytelling to improve awareness rather than make professionals is confirmed by educational material documented in column `material` in Table 2 as well as the nature of the assessment reported in Table 1 which mainly focus on learning, awareness, engagement. Further effort should be devoted to designing tools and activities tailored for professionals, clarifying roles involved in cybersecurity, and simulating real use cases. A tentative in this direction is provided by serious games and simulation platforms, such as What.Hack that simulates real-world phishing scenarios and asks players to distinguish between real and phishing emails [19] or CyberVR, which is an immersive cybersecurity role-playing game where players act as IT system administrators and have to maintain a high-security access level [20].

5. Conclusion and Future Directions

Cybersecurity is increasingly pervasive and has a global impact on nearly everyone. People now live in a cyber world where data are stored digitally and continuously shared online. Therefore, there is an urgent need for all to increase awareness concerning risks and how to mitigate their impact. As storytelling is considered a promising educational approach, we investigate its exploitation in cybersecurity education. The presented results are retrieved via a systematic literature review of peer-reviewed contributions indexed by the major databases focusing on initiatives exploiting storytelling in cybersecurity education via digital tools. While peer-reviewed articles have been revised mainly in terms of the performed assessment, tools have been assessed in terms of availability, target, and supported features.

Replying to RQ, storytelling is explored as a promising approach to increase learners' awareness and education about cybersecurity, probably due to the perceived potentiality to simplify the access point to complex and technical topics. Moderators of cybersecurity educational activities can rely on a handful of working and freely available tools, mainly commercial released for free, along with publicly available educational material. However, it is only marginally explored for professionals. Workers should be more involved as target groups, collecting their needs and verifying the utility of proposed tools to satisfy users' requirements. In a single case, workers are the target group, and storytelling is used as an approach to detect and verbalize vulnerabilities in log files. It envisions the possibility of using stories to identify patterns and visually render information along with narration to guide interpretation and mitigate the impact of vulnerabilities. In this direction, we consider relevant mentioning tools such as RouterJoyVis [45] and YourNetStory [46] to visually render patterns and ontology-driven GUI [28] to verbalize vulnerabilities.

Practical implications and future direction for future technology-enhanced learning tools. While game-based approaches are promising to engage participants of any age, end-users play the passive role of the information consumers. Alternative approaches, such as those based on videos and comics, opt for moving end-users to the position of story creator. Starting from those initiatives, it would be beneficial to encourage participants further to play an active role in authoring stories.

Digital tools often lack accompanying educational material, hindering reproducibility and transparency. Researchers must invest further effort in publicly and openly making educational videos or supporting material available. This will not only simplify the learning experience but also enable fair comparison among experiences, fostering a more responsible and transparent learning environment.

Surprisingly, collaboration is only partially exploited while learning cybersecurity. While some activities are moderated in such a way that participants collaborate with a unique robot or interface, collaboration is rarely mediated by the tool itself. As a result, collaboration disappears when the experience move to a remote setting. To keep the learning experience as unchanged as possible when transitioning between in-person and remote activities, it is crucial that digital tools spur technology-mediated cooperation and collaborative work.

Finally, there are some topics that are fundamental challenges in cybersecurity, such as information disorder, that are not explicitly covered by the included contributions. It is crucial to consider those aspects in the future, spurring a wider awareness in terms of data literacy and conscious consumption of content on the web capable of distinguishing misleading content from authentic one. Likewise, it is crucial to provide citizens of all genders and ages with (digital) tools necessary for an informed use of digital currencies dealing with cybersecurity and blockchains.

Acknowledgments

This work was partially supported by the SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU. This communication reflects only the author's view, and the Commissions are not responsible for any use that may be made of the information it contains.

References

[1] B. Morrison, L. Coventry, P. Briggs, How do older adults feel about engaging with cyber-security?, Human Behavior and Emerging Technologies 3 (2021) 1033–1049. doi:10.1002/hbe2.291.

[2] T. Suwardy, G. Pan, P.-S. Seow, Using digital storytelling to engage student learning, Accounting Education 22 (2013) 109–124. doi:10.1080/09639284.2012.748505.

[3] A. Addone, G. Palmieri, M. A. Pellegrino, Engaging children in digital storytelling, in: Methodologies and Intelligent Systems for Technology Enhanced Learning, 11th International Conference 11, Springer, 2022, pp. 261–270. doi:10.1007/978-3-030-86618-1_26.

[4] B. Passon, The power of storytelling for behavior change and business, 2019. doi:10.1177/0890117119825525d.

[5] H. Z. Waring, Participating in storytelling at ages 3 and 8, in: Storytelling practices in home and educational contexts: Perspectives from conversation analysis, Springer, 2022, pp. 47–71. doi:10.1007/978-981-16-9955-9_4.

[6] S. L. Chu, B. Garcia, T. Quance, L. Geraci, S. Woltering, F. Quek, Understanding storytelling as a design framework for cognitive support technologies for older adults, in: Proceedings of the International Symposium on Interactive Technology and Ageing Populations, 2016, pp. 24–33. doi:10.1145/2996267.2996270.

[7] H. O. Obie, C. Chua, I. Avazpour, M. Abdelrazek, J. Grundy, T. Bednarz, A study of the effects of narration on comprehension and memorability of visualisations, Journal of Computer Languages 52 (2019) 113–124. doi:10.1016/j.cola.2019.04.006.

[8] I. Vasileiou, S. Furnell, Cybersecurity education for awareness and compliance, IGI Global, 2019. doi:10.4018/978-1-5225-7847-5.

[9] J. Andriessen, M. Pardijs, Story telling, in: Cybersecurity Awareness, Springer, 2022, pp. 45–67.

[10] C. Irvine, M. Thompson, K. Allen, CyberCIEGE: gaming for information assurance, IEEE Security & Privacy 3 (2005) 61–64. doi:10.1109/MSP.2005.64.

[11] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, T. Pham, School of phish: a real-world evaluation of anti-phishing training, in: Proceedings of the 5th Symposium on Usable Privacy and Security, ACM, 2009. doi:10.1145/1572532.1572536.

[12] M. Newbould, S. Furnell, Playing safe: A prototype game for raising awareness of social engineering, Australian Information Security Management Conference (2009).

[13] F. Giannakas, G. Kambourakis, S. Gritzalis, CyberAware: A mobile game-based app for cybersecurity education and awareness, in: International Conference on Interactive Mobile Communication Technologies and Learning (IMCL), 2015, pp. 54–58. doi:10.1109/IMCTL.2015.7359553.

[14] A.-S. T. Olanrewaju, N. H. Zakaria, Social engineering awareness game (SEAG): an empirical evaluation of using game towards improving information security awareness, in: Proceedings of the 5th International Conference on Computing and Informatics, ICOCI, 2015. URL: https://api.semanticscholar.org/CorpusID:8873731.

[15] L. Zhang-Kennedy, K. Baig, S. Chiasson, Engaging children about online privacy through storytelling in an interactive comic, Electronic Visualisation and the Arts (EVA) (2017) 1–11. doi:10.14236/ewic/HCI2017.45.

[16] J. Mikka-Muntuumo, A. Peters, H. Jazri, CyberBullet-Share Your Story: an interactive game for stimulating awareness on the harm and negative effects of the internet, in: Proceedings of the 2nd African Conference for Human Computer Interaction: Thriving Communities, 2018, pp. 1–4. doi:10.1145/3283458.3283482.

[17] B. Ledbetter, Z. Wallace, A. Harms, A. Siraj, L. Buchanan, CySCom: Cybersecurity COMics, in: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), IEEE, 2016, pp. 282–284. doi:10.1109/ISI.2016.7745490.

[18] J. Barela, T. E. Gasiba, S. R. Suppan, M. Berges, K. Beckers, When interactive graphic storytelling fails, in: 2019 IEEE 27th International Requirements Engineering Conference Workshops (REW), IEEE, 2019, pp. 164–169. doi:10.1109/REW.2019.00034.

[19] Z. A. Wen, Z. Lin, R. Chen, E. Andersen, What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game, in: Proceedings of the CHI Conference on Human Factors in Computing Systems, ACM, 2019, p. 1–12. doi:10.1145/3290605.3300338.

[20] S. V. Veneruso, L. S. Ferro, A. Marrella, M. Mecella, T. Catarci, CyberVR: an interactive learning experience in virtual reality for cybersecurity related issues, in: Proceedings of the International Conference on Advanced Visual Interfaces, ACM, 2020, pp. 1–8. doi:10.1145/3399715.3399860.

[21] M. Schufrin, D. Sessler, S. L. Reynolds, S. Ahmad, T. Mertz, J. Kohlhammer, Information visualization interface on home router traffic data for laypersons, in: Proceedings of the International Conference on Advanced Visual Interfaces, 2020, pp. 1–3. doi:10.1145/3399715.3399970.

[22] F. Khalid, T. El-Maliki, Teachers' experiences in the development of digital storytelling for cyber risk awareness, International Journal of Advanced Computer Science and Applications 11 (2020). doi:10.14569/IJACSA.2020.0110225.

[23] D. P. Snyman, G. R. Drevin, H. A. Kruger, L. Drevin, J. Allers, A wolf, hyena, and fox game to raise cybersecurity awareness among pre-school children, in: International Symposium on Human Aspects of Information Security and Assurance, Springer, 2021, pp. 91–101. doi:10.1007/978-3-030-81111-2_8.

[24] Y.-M. Chiou, T. Barnes, S. M. Jelenewicz, C. Mouza, C.-C. Shen, Teacher views on storytelling-based cybersecurity education with social robots, in: Interaction Design and Children, 2021, pp. 508–512. doi:10.1145/3459990.3465199.

[25] A. M. P. Hall, John Grady Mohanty, N. D. Nguyen, J. C. Bahamón, H. Ramaprasad, M. Sridhar, Criminal investigations: An interactive experience to improve student engagement and achievement in cybersecurity courses, in: Proceedings of the 53rd ACM Technical Symposium on Computer Science Education-Volume 1, 2022, pp. 696–702. doi:10.1145/3408877.3439630.

[26] S. Suh, S. Lamorea, E. Law, L. Zhang-Kennedy, PrivacyToon: Concept-driven storytelling with creativity support for privacy concepts, in: Designing Interactive Systems Conference, 2022, pp. 41–57. doi:10.1145/3532106.3533557.

[27] W. Heiden, T. Kless, T. Neteler, A crossmedia storytelling platform to empower vulnerable groups

for IT security, in: International Conference on Interactive Digital Storytelling, Springer, 2023, pp. 195–201. doi:10.1007/978-3-031-47658-7_17.

[28] R. Hassan, C. Bandi, M.-T. Tsai, S. Golchin, S. M. P D, S. Rafatirad, S. Salehi, Automated supervised topic modeling framework for hardware weaknesses, in: 24th International Symposium on Quality Electronic Design (ISQED), 2023, pp. 1–8. doi:10.1109/ISQED57927.2023.10129378.

[29] N. Chowdhury, V. Gkioulos, Cyber security training for critical infrastructure protection: A literature review, Computer Science Review 40 (2021) 100361.

[30] Carnegie Mellon's Information Networking Institute and Carnegie Mellon CyLab, Carnegie Cadets: The MySecureCyberspace Game, 2007. URL: http://www.carnegiecyberacademy.com, [Online, Last access April 8th, 2024].

[31] NOVA Labs, Cybersecurity Lab, 2013. URL: https://www.pbs.org/wgbh/nova/labs/lab/cyber, [Online, Last access April 8th, 2024].

[32] Ion Storm, Deus Ex, 2000.

[33] exosyphen studios, Hacker Evolution Duality, 2011.

[34] Google, INTERLAND, 2017. URL: https://beinternetawesome.withgoogle.com, [Online, Last access April 8th, 2024].

[35] Ubisoft, WhatDogs, 2014. URL: https://www.ubisoft.com/it-it/game/watch-dogs/watch-dogs, [Online, Last access April 8th, 2024].

[36] Pixton Comics Inc., Pixton, 2022. URL: https://www.pixton.com, [Online, Last access April 8th, 2024].

[37] Plotagon, Plotagon, 2013. URL: https://www.plotagon.com, [Online, Last access April 8th, 2024].

[38] PowToon Ltd., PowToon, 2012. URL: https://www.powtoon.com, [Online, Last access April 8th, 2024].

[39] U.S. Department of Homeland Security, Comic-BEE, 2003. URL: http://securedecisions.com/comicbee, [Online, Last access April 8th, 2024].

[40] Gramener, Comicgen, 2021. URL: https://gramener.com/comicgen, [Online, Last access April 8th, 2024].

[41] Adobe, Adobe creative suite, 2012.

[42] GameSalad, Gamesalad creator, 2016. URL: https://creator.gamesalad.com, [Online, Last access April 8th, 2024].

[43] S. Suh, S. Lamorea, E. Law, L. Zhang-Kennedy, PrivacyToon, 2020. URL: https://privacytoon.uwaterloo.ca, [Online, Last access April 8th, 2024].

[44] Capterra, Storyboard That, 2012. URL: https://www.storyboardthat.com, [Online, Last access April 8th, 2024].

[45] Fraunhofer IGD, RouterJoyVis, 2020. URL: https://routerjoyvis.visperience.igd.fraunhofer.de, [Not working in April 8th, 2024].

[46] Fraunhofer IGD, YourNetStory, 2020. URL: https://yournetstory.visperience.igd.fraunhofer.de, [Not working in April 8th, 2024].

[47] ASUS, Zenbo, 2017.

[48] C.-m. Hsiung, The effectiveness of cooperative learning, Journal of engineering Education 101 (2012) 119–137.

[49] L. Zhang-Kennedy, S. Chiasson, A systematic review of multimedia tools for cybersecurity awareness and education, ACM Computing Surveys (CSUR) 54 (2021) 1–39.

[50] F. Alotaibi, S. Furnell, I. Stengel, M. Papadaki, A review of using gaming technology for cybersecurity awareness, International Journal of Information Security (IJISR) 6 (2016) 660–666.