MASTERM1ND: A Virtual Reality Web-Based Cybersecurity Awareness Game

Hussain Assaf Alassaf, Abdulaziz Mohammed Tayeb, Muhammad Sufiyan Shoukat Ali, Eyad Raed Elsadouni, Hassan Harun ur Rashid, Hoda Elsayed, Muhammed Umair Khan

Alfaisal University, Riyadh, Kingdom of Saudi Arabia

{haalassaf, atayeb, msufiyan, eelsaadouni, hrashid, helsayed, mumkhan @alfaisal.edu}

Abstract. The prevalence and sophistication of cyberattacks have grown exponentially in recent years, posing significant threats to individuals, organizations, and society at large. As a response to this escalating concern, educational initiatives have emerged to raise awareness about the tactics and vulnerabilities exploited by malicious actors in the digital realm. One innovative approach gaining traction is the development of hacking simulation games, which provide players with a hands-on experience of the attacker's mindset and techniques. By immersing players in a realistic hacking environment, these games offer a unique educational platform to enhance cybersecurity knowledge and promote proactive defense strategies. This research aims to contribute to this emerging field by proposing the implementation of a hacking simulation game that focuses on the awareness and mitigation of cyberattacks. Specifically, the game design centers on enabling players to assume the role of the attacker, offering them insights into the consequences of weak passwords and the importance of password diversification and several more relevant cybersecurity attacks. The overall outcome from this development is a four-level game that allows its player to enrich their cybersecurity awareness.

Keywords: Cybersecurity, Game development, Virtual Reality (VR), Education.

1 Introduction

Enhancing the security of software systems is an ongoing concern. Many different strategies have been proposed to incorporate security features in software systems during their development [1-3]. However, the user being the weakest link needs to be educated about security policies and best practices [3]. Incorporating security activities, such as the one proposed in this paper can empower users to recognize and avoid common security mistakes. By installing a deeper understanding of cyber security, users can actively contribute the security of software systems.

Cybersecurity attacks are growing by the day in different aspects and levels, affecting not only businesses but also individuals. For example, Phishing [4], at its essence is centered around the cybercriminal coercing the victim into giving up information or resources. Phishing attacks target both organization and individual levels, and one effective countermeasure is raising awareness. This can be done through multiple mediums however the most compelling solution is through educational means. By doing so raising awareness can be the journey instead of the destination, allowing people to educate themselves in an ongoing basis to stay up to date in current vulnerabilities.

As technology continues to advance, cybercriminals have become more adept at exploiting vulnerabilities within digital systems. The consequences of cyberattacks can be far-reaching, ranging from financial losses and data breaches to reputational damage and compromised privacy [5][6]. It is essential for individuals and organizations to develop a proactive approach to cybersecurity, equipping themselves with the knowledge and skills necessary to identify and defend against potential threats. Seeing that only 30% of organizations educate their employees in cybersecurity there is a need for an improvement on an individual level [7]. In the field of cybersecurity, understanding the behaviors and motivations of attackers is crucial in order to develop effective defense strategies.

Some work has already been performed at this area for example *TryHackMe* [8], it is a website platform for cybersecurity training that offers its players an array of tools and services to enhance their cybersecurity expertise. It covers a broad range of cybersecurity subjects, such as cryptography, network

security, and web security. *Nova Labs* [9] is a website platform that offers a variety of resources and services for individuals and organizations to use in games and challenges to improve their cybersecurity skills with cybersecurity training and education platform. This platform covers a wide range of cybersecurity subjects, which include network security and cryptography. Nova Labs have used Virtual machines, web-based applications, and other cybersecurity tools like Wireshark and Nmap to create the games and challenges for participants. *Hack The Box* [10] is a platform for cybersecurity training that offers players an extensive variety of services and tools to evaluate and advance their cybersecurity skills. This platform offers coverage of quite a few cybersecurity topics including web security, binary exploitation, encryption, and more. *PicoCTF* [11] is a cybersecurity competition internet platform that is aimed to teach and promote cybersecurity information and abilities to its players. It focuses on cryptography, binary exploitation, web security, and other cybersecurity issues. The web application is a combination of programming challenges and virtual machines to test its participant's knowledge on a given cybersecurity topic.

On the other hand, some other games use a more simplistic approach, giving the player simple puzzles and challenges to complete with a cybersecurity twist, these games are usually more accessible to all demographics as discussed in a previous section. The proposed game truly stands out from the crowd, as it places the player in the perspective of the attacker, a twist that none of these games tried. This new perspective will allow the exploring of new educational opportunities as the player takes a peek into the other side of the equation.

In this paper we will first dive into the literature review, which will entail a comprehensive examination of existing research and theoretical frameworks and how MASTERM1ND differs from them (section 2). Following that is the game design section where we demonstrate how we implemented the game (section 3). Next is the results section where we give an idea of the MASTERM1ND results thus far (section 4). Last but not the least is the conclusion section where we consolidate the findings and implications (section 5).

2 Literature review

The use of social media to raise awareness is not groundbreaking in any sense. The social network game [12] presents the player with posts from friends and the player chooses either "like" or "dislike" or "don't care". MASTERM1ND does things a little differently: the player is presented messages from not only friends but also organizations and promotional messages. The social network game mainly focuses on how to spot malicious posts only from friends where MASTERM1ND focuses on how to spot and respond to malicious posts from friends and as well as organizations.

"PhishGuru" [13] also highlights phishing attacks in a web-based system and specifically spear-phishing and email phishing however their main demographic is not general users but rather large corporations. Focusing on a large Portuguese company they translated the game and the emails from English to Portuguese to fit the attacks that the company suffered the most from. The game has a set of levels that are modified to fit into the organization's needs. MASTERM1ND offers similar levels and story progression as PhishGuru but it is not made with any organization point of view but rather the point of view of the average internet user.

NetDefense [14] is a tower defense game that aims to enhance cybersecurity awareness in school children from 1st to 12th grade or for children aged 6-17 years old. The developers of the game assess the success of the game by surveying students and teachers before and after playing the game. The game teaches the concept of data packets by having the player move a character into different 5 or 6 cubes with each cube being a data packet and seeing which data packet is different the most from the others, with the one different one being the bad suspicious packet. NetDefense is implemented in the engine Unity but it can be easily made into a web-based game using WebGL. MASTERM1ND differs from the NetDefense game by appealing to not only children but also older demographics. Furthermore, the MASTERM1ND game incorporates both the point-and-click and arrow keys mechanics unlike the NetDefense game which only uses arrow keys.

CyberNEXS [15] offers training on topics like password usage, protection from malware and spam & social engineering attacks. The developers cite shortcomings that motivated them to develop the game such as overwhelming content in the levels and lack of user interaction in the existing games [16,17]. These shortcomings are crucial which is why they aren't seen in MASTERM1ND, 90% of MASTERM1ND has the player engaged and paying attention and not looking at videos or pictures. Furthermore, MASTERM1ND does not overwhelm the players with too much information that they cannot possibly retain but rather focuses on four clear vulnerabilities and highlights them clearly. The game mechanics of CyberNEXS and MASTERM1ND are similar in the sense that both games have victory conditions that vary in different levels. In some cases the level can be won after trying multiple choices until the correct one is chosen and in other cases the level can be won by just moving forward until the lesson is learned through multiple events.

Even though we think the best way to reach as many people as possible is through a web game that does not mean different solutions are not available. Password protector [18] is a proposed mobile game focused on enhancing cybersecurity awareness. Password protector challenges the player to create a password from a limited set of characters and the password is being judged on the complexity and the memorability of the password, using the IBM regulations of password complexity. This level teaches the player the importance of creating a password that is both secure and easy to remember but it does not mention the fact that no matter how strong the password is it should not be used for more than one website. However, MASTERM1ND takes care of that aspect. Furthermore, password protector asks the player to create a password without mentioning the username and this can be seen as a setback. MASTERM1ND shows the player the importance of creating a password that is not only complex and secure but also completely independence from the username.

MASTERM1ND allows the player to be on both sides of the cybersecurity equation being the attacker (red team) and the defender (blue team) but it is not the first game to do so, PeriHack also follows a similar approach [19]. The main difference between the two games is that MASTERM1ND utilizes the two teams approach from a social engineering standpoint where PeriHack utilizes it from a more technical perspective. PeriHack challenges the red team to breach a company's network using attacks like DDoS and SQL injections and the blue team is supposed countermeasure their attacks to the best they can. The game is played on a board representing an office which is the battlefield that both teams will use to utilize multiple items to emerge victorious. This makes the game a multiplayer game with ever-changing circumstances from one session to another which is somewhat confusing to inexperienced players. MASTERM1ND utilizes the two teams approach differently in a sense that the player is sometimes the attacker trying to hack an organization and sometimes is still the hacker but now the organization is trying to hack them, which gives a more cohesive and a concrete story.

3 Game Design & Mechanics

3.1 Some Important Vulnerabilities

Most websites and applications enforce ***password regulations***, such as minimum character requirements and the inclusion of special characters and digits [20]. While adhering to these regulations is essential, it is advisable to create complex passwords for enhanced security. Users should avoid using the same password across multiple accounts. Cybercriminals often target individuals personally. Attackers may exploit websites without maximum password attempt limits and then attempt to use compromised passwords on more secure platforms. This underscores the importance of creating unique and robust passwords to mitigate the risk of unauthorized access and data breaches.

Phishing, at its core, revolves around cybercriminals scaring victims into divulging information or resources. Typically, perpetrators send deceptive emails posing as legitimate entities, such as banks or government agencies, to instill a sense of urgency or concern [21]. Victims may be prompted to contact the cybercriminal or provide personal information through fraudulent websites. Smishing follows a similar approach but employs SMS text messages instead of emails. Spear phishing, a variation, utilizes personalized tactics to appear as if the communication is from a trusted source, like a friend or colleague

[22]. Exploiting this familiarity, cybercriminals deceive victims into compromising their security, often repeatedly over time.

Using ***public networks*** may appear convenient due to their widespread availability and ease of access, often requiring minimal personal information such as a phone number or email address for authentication. However, the security risks associated with such networks are often overlooked. One of the primary concerns is the ***lack of encryption*** in many public networks, leaving data transmitted over these networks vulnerable to interception and unauthorized access by cybercriminals. Without encryption, the data sent between a device and the network is essentially transmitted in plaintext, making it easy for malicious actors to eavesdrop on sensitive information such as login credentials, personal messages, and financial transactions. This vulnerability can be exploited through various means, including packet sniffing, man-in-the-middle attacks, and session hijacking.

In April 2023, the Federal Bureau of Investigation (FBI) issued a report cautioning against the use of unattended ***charging ports*** in public spaces such as airports, shopping malls, and hotels [23]. The primary concern stems from the lack of monitoring and security measures in place for these charging stations, rendering them vulnerable to malware dissemination onto users' devices. Cybercriminals can exploit these unsecured stations to deploy malware either remotely or through physical means, posing significant risks to users' data security and privacy. Given the increasing sophistication of cyber threats, individuals must remain vigilant and proactive in safeguarding their digital assets. This includes exercising caution when connecting devices to public charging ports and opting for more secure alternatives such as battery packs. By adopting such measures, users can mitigate the potential risks associated with unsecured charging ports and minimize their exposure to cybersecurity threats while on the go.

3.2 MASTERM1ND Game

3.2.1 Password Scenario

In this scenario the player will try to crack the passwords of different websites of the same user with three different levels of security on each website. *Beginner level:* at this level, the player will need to crack a password containing 4 characters. The player will be provided with a hint and some information to complete the level the user will have three tries. *Intermediate level:* In this level the player will have to hack into the same account but on a different website. The password will be more complex seeing that it will contain 8 characters of numbers and letters the user will have 5 tries. *World-class level:* In this level the player will be given 9 chances to hack into an account, the account's password will be 16 characters long and will contain numbers, letters, special characters. The player won't be able to complete the *World-class level* but that is the point. The password is 16 characters long and completely independent from the username which makes it extremely difficult to guess which is the message we want to deliver to the user that you should make your passwords lengthy and unrelated to the username.

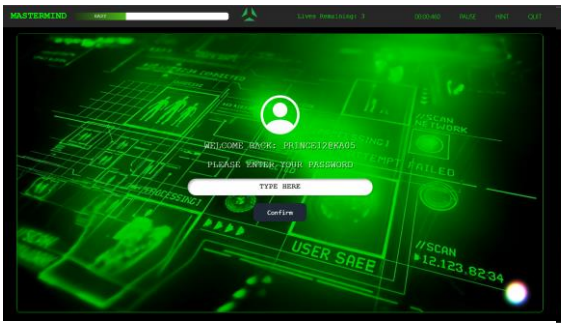

Fig. 1. Beginner Scenario Interface

Fig. 2. World-Class Scenario Interface

3.2.2 Phishing Scenario

In this scenario the player will have to play 4 levels to advance. These levels are: Spear phishing, Smishing, Vishing, and email phishing. *Spear Phishing level:* in this level the players will encounter two messages and they must determine which message is genuine and from a trusted source and which message is fraudulent with malicious intent. *Smishing level:* in this level the players will get 3 messages

in a SMS format and the users must determine if each message is real or fraudulent. *Vishing level:* in this level the player will receive two voice messages, one of which is made by a voice cloning model, the players will have to determine which of these is the authentic message and which is the vishing attempt. *Email Phishing level:* in this level the player will be presented with a series of emails that they will have to drop into two folders one being real and the other being phishing attempts.

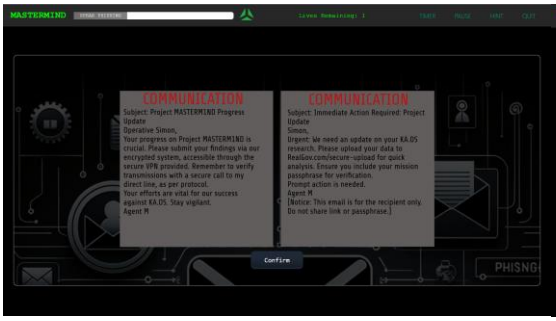

Fig. 3. Spear Phishing Scenario Interface

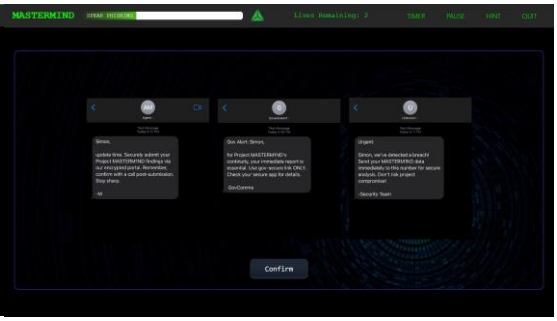

Fig. 4. Smishing Scenario Interface

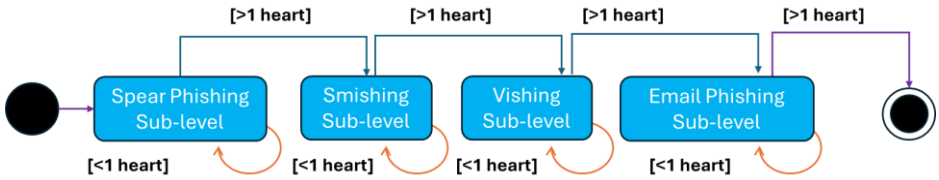

Fig. 5. State Machine Diagram for Phishing Scenario

3.2.3 Networks Scenario

In this scenario, the user is in a shopping mall and will be able to pick one out of three networks to connect to. One is a private hotspot protected with a password, one is a private network of a store protected with a password, and finally one is a public access network that is owned and operated by the mall themselves. After the user picks one of the three networks they will play the role of the attacker and the role of the victim back and forth. First thing the user will do after connecting to the public mall network is that they will send a text message to someone which will include a confidential file. From then the Point of view changes to the attacker's point of view and shows the user that the file that was just sent is now compromised and is no longer confidential. This can be seen by a screen on the attacker's laptop that shows the data being extracted.

3.2.4 Charging Ports Scenario

In this scenario the user will play using the virtual reality framework developed using Unity. Unity VR games do not need any headsets or extra equipment whatsoever. All that is needed is a laptop device. In this scenario the player will be able to move their character into a charging station in an airport. Onwards the player will connect their phone to a charger. Afterwards the game will switch the user to the attacker role. From then the game will show that the attacker can have access to all the victim's data.

Fig. 6. Charging Ports Scenario interface

4 Results

This section discusses effects of the “MASTERM1ND” virtual reality web-based cybersecurity awareness game based on a preliminary survey. Based on the feedback from 20 participants composed of university students and number of questions related to there current knowledge about security issues and how much that knowledge improved after playing the game. Through this structured survey, participants engaged with various levels covering key cybersecurity principles, from password attacks to charging ports attacks. The following subsections aim to assess the game's efficacy in enhancing understanding, evaluating game mechanics, and gathering feedback for improvements.

4.1 Password Scenario Results

Before playing the game, the understanding of why using the same password for different websites is a security risk varied among participants. Approximately 82.4% of respondents claimed to have a clear understanding of this concept, while the remaining 17.6% reported varying levels of uncertainty or lack of awareness.

Regarding the difficulty of the password scenario, opinions were divided. For the first scenario, which is the ***beginner scenario***, approximately 58.8% of participants found it easy to complete, while 41.2% found it moderately difficult to guess the presented password. The hint provided for this scenario was deemed helpful by 70.6% of participants and somewhat helpful by 29.4% of participants.

Similarly, the ***second scenario*** received mixed responses, with 17.6% finding it easy, 41.2% finding it moderately difficult, and 41.2% finding it hard. Approximately 52.9% of respondents found the hint helpful for this scenario while 35.3% found it somewhat helpful and finally 11.8% found the hint not helpful for this scenario.

Moving to the ***third scenario***, 94.1% found it easy while 5.9% found it moderately difficult. However, only 76.5% of participants found the hint for this scenario not helpful, 17.6% found it somewhat helpful, and only 5.9% of participants found the hint helpful.

4.2 Phishing Scenario Results

Regarding the phishing scenarios, and specifically the ***email phishing scenario***, 52.9% of participants found it easy and 35.3% of participants found it moderately difficult and only 11.8% of participants found it difficult to complete. The hint for the scenario did similarly seeing that 58.8% of participants found it helpful and 35.3% found it somewhat helpful and only 5.9% found the hint not helpful.

The ***smishing scenario***, 70.6% of participants found it easy and 23.5% of participants found it moderately difficult and only 5.9% of participants found it difficult to complete. The hint for the scenario received mixed feedback regarding the fact that 47.1% of participants found it helpful and 47.1% found it somewhat helpful and only 5.9% found the hint not helpful.

The ***spear phishing scenario***, 58.8% of participants found it easy and 35.3% of participants found it moderately difficult and only 5.9% of participants found it difficult to complete. The hint for the scenario received interesting feedback regarding the fact that 47.1% of participants found it helpful and 52.9% found it somewhat helpful.

Last but not the least the ***Vishing scenario*** received that 47.1% of participants found the scenario easy, 41.2% found it moderately difficult and 11.8% of participants found it difficult.

4.3 Charging Ports Scenario Results

The overwhelming majority of participants, comprising 94.1%, lauded the charging ports scenario for its ease of completion, user-friendly navigation, and its significant contribution to enhancing their understanding of cybersecurity awareness. This resounding endorsement underscores the scenario's effectiveness in imparting valuable knowledge and skills in safeguarding against potential cyber threats

associated with charging ports. On the other hand, 5.9% of participants found issues navigating the level and/or they did not feel that the learned much from this experience.

5 Conclusion

The main problem we're dealing with is that a lot of people do not know enough about keeping safe online, especially when it comes to common ways hackers can get in. Even though there has been a lot of research and we see it happening every day, people keep falling for cyber scams. We need to do more to teach people how to stay safe and use better technology to protect ourselves. Fixing this problem will need everyone to work together, using smarter tools and making sure everyone knows how to stay safe online.

To tackle this issue, we have developed MASTERM1ND, an innovative virtual reality web game aimed at enhancing cybersecurity awareness. Designed with the everyday internet user in mind, the game concentrates on educating players about the four primary vulnerabilities commonly exploited by cyber threats. Through engaging gameplay and interactive learning experiences, MASTERM1ND empowers users to elevate their understanding of cybersecurity and adopt safer online practices.

The effectiveness of the "MASTERM1ND" virtual reality web-based cybersecurity awareness game is evident from a preliminary survey involving 20 participants, predominantly university students. Through assessing participants' understanding of cybersecurity concepts before and after engaging with the game, particularly in password and phishing scenarios, the results indicate significant improvement. Participants demonstrated better comprehension of password security risks, with balanced difficulty levels and helpful hints aiding their navigation through challenges. Similarly, participants exhibited enhanced abilities in identifying and responding to phishing attempts, suggesting the game's potential as a valuable tool in promoting cybersecurity education and empowering individuals to securely navigate the digital landscape.

Moving forward, the next phase for MASTERM1ND involves broadening the range of vulnerabilities within the game. The current vulnerabilities were selected based on their prevalence and criticality in real-world scenarios. However, future iterations aim to incorporate more complex vulnerabilities that are less commonly encountered by users. This expansion will offer a more comprehensive learning experience, equipping players with the knowledge and skills to tackle a wider array of cybersecurity threats effectively.

References

1. M. U. Khan & M. Zulkernine.: Activity and Artifact Views of a Secure Software Development Process, January 2009
2. M. U. Khan & M. Zulkernine.: On Selecting Appropriate Development Processes and Requirements Engineering Methods for Secure Software, August 2009
3. M. U. Khan & M. Zulkernine.: A Survey on Requirements and Design Methods for Secure Software Development, August 2009
4. KnowBe4: What is phishing?. Phishing, https://www.phishing.org/what-is-phishing (last accessed March 19, 2024)
5. bitsIO Communications: The impact of cybersecurity threats and cybercrime on businesses. https://www.bitsioinc.com/cybercrime-impact-on-businesses/ (last accessed March 19, 2024)
6. Federal Bureau of Investigation. (2023). Internet crime report.
7. Alotaibi, F., Furnell, S., Stengel, I., Papadaki, M.: Enhancing cyber security awareness with mobile games. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Dec. 2017. doi:10.23919/icitst.2017.8356361
8. Cyber security training. TryHackMe, https://tryhackme.com/ (last accessed March 19, 2024)
9. Cybersecurity. PBS, https://www.pbs.org/wgbh/nova/labs/lab/cyber (last accessed March 19, 2024)
10. Hacking training for the best. Hack The Box, https://www.hackthebox.com/ (last accessed March 19, 2024)
11. CMU cybersecurity competition. picoCTF, https://picoctf.org/ (last accessed March 19, 2024)
12. Sookhanaphibarn, K., Choensawat, W.: Educational games for cybersecurity awareness. 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE), Oct. 2020. doi:10.1109/gcce50665.2020.9291723
13. Kumaraguru, P.: PhishGuru: A System for Educating Users about Semantic Attacks. (2009)

14. Toledo, W., Louis, S.J., Sengupta, S.: NetDefense: A tower defense cybersecurity game for middle and high school students. 2022 IEEE Frontiers in Education Conference (FIE), Oct. 2022. doi:10.1109/fie56618.2022.9962410
15. Nagarajan, A., Allbeck, J. M., Sood, A., Janssen, T. L.: Exploring game design for cybersecurity training. 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), May 2012. doi:10.1109/cyber.2012.6392562
16. Cone, B. D. et al: A video game for cyber security training and awareness. Computers and Security 26(5), 99–110 (2007)
17. Annetta, L.A.: The "I's" Have It: A Framework for Serious Educational Game Design. Review of General Psychology 14(2), 105-112 (2010)
18. Alotaibi, F., Furnell, S., Stengel, I., Papadaki, M.: Enhancing cyber security awareness with mobile games. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Dec. 2017. doi:10.23919/icitst.2017.8356361
19. Dillon, R., Arushi: 'PeriHack': Designing a serious game for cybersecurity awareness. 2022 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE), Dec. 2022. doi:10.1109/tale54877.2022.00108
20. Bosnjak, L., Sres, J., & Brumen, B.: "Brute-Force and dictionary attack on hashed real-world passwords." In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018. doi:10.23919/mipro.2018.8400211
21. Proofpoint. "What is phishing? - definition, types of attacks & more." Proofpoint. https://www.proofpoint.com/us/threat-reference/phishing (last accessed March 19, 2024)
22. C. S. Establishment. "Phishing: An introduction." Get Cyber Safe. https://www.getcybersafe.gc.ca/en/blogs/phishing-introduction. (last accessed March 19, 2024)
23. W.-N. Staff, "Think twice before charging your phone at the airport, FBI warns," CBS News, https://www.cbsnews.com/boston/news/usb-charging-ports-phone-airports-malware-fbiwarning-cords/ (last accessed March 19, 2024)