8 Cybersecurity Hygiene
Blending Home and Work Computing

Thomas W. Morris and Jeremiah D. Still
Department of Psychology, Old Dominion University
Norfolk, VA, USA

CYBERSECURITY HYGIENE: BLENDING HOME AND WORK COMPUTING

Overview

Remote work demand is increasing, and how it is performed is changing. The hybrid home-work computing environment is becoming a soft target for potential cyberattacks. This chapter examines cybersecurity hygiene within the rapidly evolving hybrid home-work computing environment. The concepts of cyber hygiene and the hybrid home-work computing environment are explored and abstractly defined. A reflection on cybersecurity and physical security reveals unique security knowledge expected to be elicited from home computer users in the cyber environment. We explain how the learning of cybersecurity behaviors is different from physical security behaviors due to the lack of cultural transfer between generations. Key differences between the home and work computing domains are described. Cybersecurity experts have touted many possible solutions to the threats created by hybrid home-work computing. However, even with these solutions, it is impossible to design out the human element. Users need to be a critical part of the cybersecurity informational loop. This chapter highlights the needed behavioral interventions to ensure users are part of this process. And, discusses how training, nudges, warnings, and better visualizations are needed to meaningfully mitigate cyber risk. An initial list

DOI: 10.1201/9781003415060-11

of unique hygiene recommendations for users in the hybrid home-work computing environment is provided. Finally, we discuss the need for future research in the hybrid home-work computing domain.

Recent History

According to the Owl Labs 2021 State of Remote Work survey, it is estimated that globally 16% of companies employ a fully remote workforce. They also found that 62% of workers aged 22 to 65 claim to work remotely occasionally. As the cyber landscape evolves, home and work computing environments are becoming more intertwined. Unfortunately, home computing cybersecurity behaviors have been studied less than organizational cybersecurity behaviors. This is due to the organizational infrastructure of information technology (IT) professionals, best practices, and reporting standards (Howe et al., 2012). As home and work computing become more entwined, the gap in our understanding of home computing (HC) cybersecurity behaviors will become more costly. The recent abrupt change from in-office to remote work due to the COVID-19 pandemic has increased our need to better understand HC users' cybersecurity behaviors. This perfect storm of rapid adaptation of telework technologies and the lack of research regarding how to best support HC users in the telework environment will undoubtedly result in new opportunities for bad actors.

Poor cybersecurity behaviors are costing companies millions of dollars. For instance, in a 2021 ransomware attack on a US oil pipeline system, hackers demanded $4.4 million to unencrypt the files needed to continue the pipeline operations. This attack on critical infrastructure caused the pipeline to halt operations. To resolve this crisis, the pipeline company paid the attackers' ransom. But even after paying the ransom, it took a long time for the files to decrypt, which led to a significant gas shortage on the east coast of the United States. It was later discovered that the attackers gained access to the system through a Virtual Private Network (VPN) because a single remote employee had a weak password. This attack shows the importance of basic cyber hygiene for teleworkers.

CYBERSECURITY HYGIENE

"Cyber" hygiene as a concept feels familiar but has not been fully defined in the cybersecurity literature. Much research is underway regarding the operationalization of cyber hygiene as a concept. For instance, one definition describes cyber hygiene as "the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet-enabled devices from being compromised in a cyber-attack" (Vishwanath et al., 2020, p. 2). Another perspective defines cyber hygiene as personal cybersecurity (Clemente, 2021). Interestingly, there has been discussion about changing the name from cyber hygiene to OPSEC (operational security) to align with other fields of study (Vishwanath, 2021).

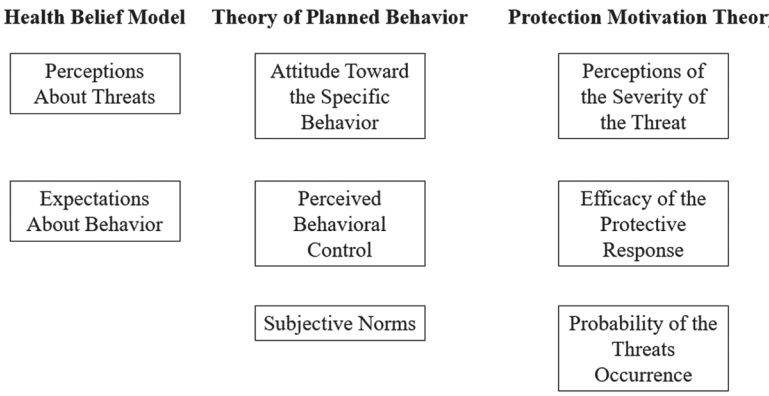

FIGURE 8.1 Main Factors Considered as the Determinants of Preventative Health Behaviors.

Note. **Source: Dodel & Mesch (2017) and Howe et al. (2012).**

Historically, the concept of cyber hygiene stems from social cognitive theories attempting to explain risky behavior in preventative health. For example, Detweiler et al. (1999) found that when messaging highlights the potential gains of using sunscreen then people are significantly more likely to obtain and use sunscreen when compared to messages that highlight the protentional losses from not using sunscreen. This study aimed to promote the health prevention behavior of using sunscreen but the results have been successfully applied to many different domains, including messaging in cybersecurity.

Traditionally health-focused researchers have been able to successfully translate health-belief models, theories of planned behavior, and protection motivation theories into the cybersecurity domain (Dodel & Mesch, 2017). Figure 8.1 provides an overview of the main factors considered as the determents of preventative health behaviors.

In each of these models, sociodemographic variables and environmental cues are considered. The *health-belief model* attempts to identify the relationships between specific variables and the likelihood of taking preventative health action (American Psychological Association, n.d.). The *theory of planned behavior* posits that the intention to perform a behavior is the main indicator of a specific behavior (Howe et al., 2012). *Protection motivation theory* describes how individuals are motivated to react in self-protective ways towards a perceived threat (van Bavel et al., 2019). While some researchers argue that the concept of cyber hygiene should be moved from the health literature, a significant amount of past research confirms that these preventative health theories apply to the cybersecurity domain and can provide some explanation for cybersecurity hygiene behaviors (Li et al., 2019; Dodel & Mesch, 2017; Howe et al., 2012). Clearly, the health prevention literature offers valuable insight into how to predict and promote cyber hygiene. Therefore, even if the name evolves from the health literature, we must not throw the baby out with the bathwater.

Now let us turn our attention to the concept of cyberspace itself. *Cyber* is defined as communication over any IT system that stores, retrieves, and sends information (c.f., Lexico, n.d.). However, many people would not believe that to be true to the modern conceptualizations of the Internet. As a caveat, many people do not believe that this definition of cyber is a good representation. For example, when someone is using a landline telephone, they send and retrieve information, but do not claim to be using cyberspace. This distinction between whether information technologies belong to cyberspace can become controversial, especially when introducing services like Voice over IP (VoIP). Historically called IP telephony, VoIP services require the Internet to perform landline telephone functions making this device a part of cyberspace. We first want to consider defining what constitutes cyber and what does not. Understanding the evolving boundaries of cyberspace is necessary for forming a good operational definition of cyber hygiene.

HYBRID HOME-WORK COMPUTING

Defining cyberspace boundaries presents unique challenges when considering hybrid home-work computing environments. We define the *hybrid home-work computing environment* as the cyberspace emergent from a combination of both a user's HC environment and work computing environment. The emergent cyberspace brings some of the characteristics and properties of both computing environments. For example, a hybrid home-work computing environment incorporates both home and work resources (e.g., networks and services). Figure 8.2 provides a visual conceptualization of this integration between personal and organizational computing.

These hybrid home-work environments are rapidly expanding in complexity. With this expansion comes many new questions that need to be answered. Can you separate an individual's private HC environment from their professional computing environment? Should it be temporally divided between being on or off the clock? Alternatively, resource consumption-based, whenever an employee uses a company device or service. It is simple to argue that a user is in the work environment anytime they are connected to company resources and the HC environment at all other times. However, networks do not stop capturing information based on these factors. An HC user who torrents a video game, for example, may do this when they are not actively connected to their work network, but the malware that is introduced to the HC network will potentially be spread to their work network the next time this user connects to their work resources, such as VPN services. In both the physical and cyber sense, the hybrid home-work computing environment does not have the inherent separation between space as the traditional work computing environment. As a result of this lack of separation, further precautious and mitigation techniques will need to be implemented to ensure security and privacy. Learning how to secure this new hybrid home-work environment will be difficult without additional training and interface transparency that supports greater situational awareness.

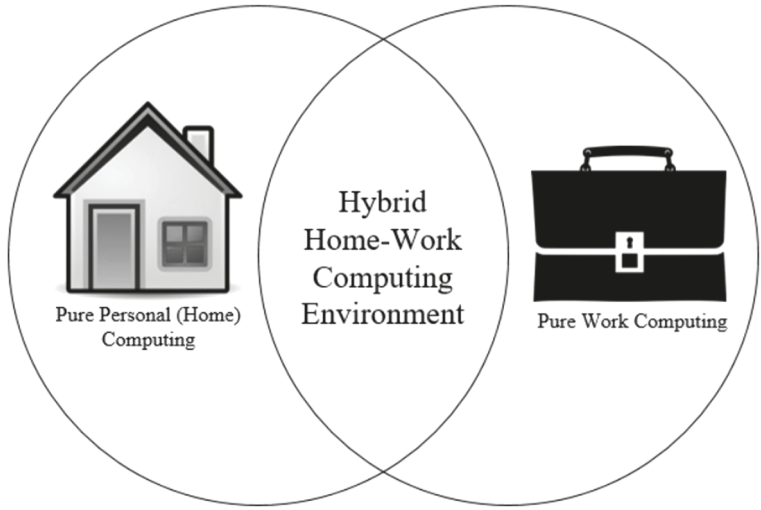

FIGURE 8.2 Conceptualization of the Hybrid Home-Work Computing Environment.

Note. **The hybrid home-work computing environment integrates characteristics from both home and organizational computing environments.**

HOW IS CYBERSECURITY ANALOGOUS TO PHYSICAL SECURITY?

We can expect users to learn cyber hygiene behaviors like other previously taught security behaviors. As children, people are often introduced to the general concept of security first through their parents or caregivers. Parents teach their children ways to safeguard themselves from intruders (i.e., lock the doors). Unfortunately, this kind of innate training rarely happens in the cyber world as our landscape is rapidly expanding. Currently, parents lack good cyber hygiene themselves. Unfortunately, they are implicitly passing on poor cybersecurity behaviors to their children. Therefore, we need to support users with better interface transparency as they lack the protective capabilities that are almost second nature in physical safety.

People often do not perceive security in cyberspace as they do in the physical space, which leads to risky behaviors that would seem out of place in a physical environment. For instance, most people intuitively know not to leave valuable personal information in a shared public space. It is abnormal for people to leave their birth certificate or social security card in an easily accessed location. This same intuitive protective behavior does not appear to be apparent in cyberspace. People readily save sensitive information on unsecured devices that are easily accessible. Regardless of users' understanding of cyberspace security, they are now asked to maintain both their home and work networks and associated services.

HOME COMPUTING COMPARED TO WORK COMPUTING

The home network provides unique security vulnerabilities compared to an organization's network. For instance, organizations have little to no control over the network configuration or devices connected to personal networks. Organizations also have less control over those who have physical access to the home network. Some companies are working to address potential threats introduced by the hybrid home-work network. They attempt to intensively monitor network activity, but it is unlikely that organizations can establish the level of control they possess over their networks.

The devices that can be found on a home network vary significantly compared to those that are found on an organization's network. Adequate cyberinfrastructure maintenance is commonplace on organizational networks, which helps to ensure that vulnerabilities caused by older devices and out-of-date software are properly managed. Moreover, Internet of Things devices are common on the home network, and these devices present unique security risks as vectors for attack by threat actors. *Internet of Things* (IoT) devices are everyday objects embedded with technology to allow smart features. Because these are commercial products, the device's usability takes precedence over security requirements (Abomhara & Køien, 2015). According to Westscott (2019), the average home computer user has 11 IoT devices connected to their home network. The number of IoT devices connected to home networks is only growing, making home networks more challenging to protect.

There are also less formalized cybersecurity incident reporting practices in the HC environment compared to the work computing environment. When a user encounters a potentially malicious website or message in the work environment, it is commonplace to report this to its IT department. The same cannot be said in the HC environment. Often, people have nowhere to report malicious cyber encounters at home. Further, no warning messages about ongoing attacks are being sent out. This leaves the home network vulnerable to attack and contributes to the lack of situational awareness.

The *CIA Triad* security model highlights differences in work and HC goals. The model characterizes the role of cybersecurity as protecting the confidentiality, integrity, and availability of data. It is impossible to maximize all three of these components (Clemente, 2021). Often HC users are willing to trade privacy (i.e., confidentiality) for the availability of information, but companies are willing to pay to maintain the privacy of their information. Due to the conflict between the cybersecurity goals of the HC user and an organization, the hybrid home-work network suffers. This highlights the need to go beyond technological solutions. Behavioral interventions will need to be employed to improve the overall cyber hygiene of end-users and strengthen this weak point in the hybrid home-work computing system.

The *home computer user* is a novice who has no formal training in using computing yet employs technology to accomplish everyday tasks (Howe et al., 2012). HC users vary significantly in demographics, activities, and motivations, which makes the general cybersecurity habits of these users particularly difficult to predict. Past discussions on HC users are generally limited to users in the strictly

home environment; therefore, only gleam part of the security landscape. For example, an employee may receive cybersecurity training before being provided remote access to an organization's network, but others in the user's household do not receive training. This could result in accidental or unauthorized access to organizational resources. This highlights the need for overall improvement of the HC user's cybersecurity hygiene and the need to introduce design solutions that go beyond training.

SOLUTIONS TO PROBLEMS IN THE HYBRID HOME-WORK COMPUTING ENVIRONMENT

We start by conceptualizing some of the initial solutions. Organizations might attempt to resolve many emerging concerns by becoming entirely dependent on cloud computing services. Nevertheless, users will still face various threats, including cryptocurrency mining abuse, phishing campaigns, and ransomware (Google Cybersecurity Action Team, 2021). Due to the relative novelty of cloud computing, the implementation of services themselves presents a unique security risk since they lack basic controls to prevent end-users from engaging in potentially malicious activities (Google Cybersecurity Action Team, 2021).

Another solution being considered is to set up a separate network in people's homes to use for only work. While this measure is impractical for most companies due to the cost, even this drastic solution does address the human element. Users will be expected to switch back and forth between their home and work networks when accomplishing daily tasks. Network engineers have worked diligently to create a streamlined, seamless exchange of information. A loss in network identity salience can produce unintended outcomes like HC users accidentally employing computing resources to accomplish personal tasks. We may need to design for network salience to ensure the necessary transparency to discriminate between work and personal resources. These updated design elements could include visualizations to remind the user of which network is currently connected. Another potential issue is that there are many different users within the home environment. This could include guests, roommates, family members, and any other person that might enter the home. Unlike in an organization, there exists little monitoring of the physical environment where the network devices are stored making homes soft targets. Regardless of the solution, behavioral interventions must also be in play to effectively mitigate cyber threats. A popular way to encourage decision making is to employ a nudge at critical decision points during system interactions.

ROLE OF BEHAVIORAL INTERVENTIONS TO IMPROVE CYBER HYGIENE

Nudges can predictably influence HC users' decision-making process (Caraban et al., 2019). From an information processing perspective, these nudges can be reflective to the user (e.g., notifications) or automatic (e.g., default settings). And, can vary in the

level of transparency provided to the user (Caraban et al., 2019). Past research has shown that notification nudges designed using protection motivation theory improve cyber hygiene more than notifications that rely solely on fear appeals (van Bavel et al., 2019). It was shown that sociodemographic factors and risk attitudes influenced cyber hygiene behaviors. These findings support the application of the protection motivation theory. It appears that well-designed nudges can effectively improve cyber hygiene.

While nudge interventions help users make better cyber hygiene choices, a *warning* alerts users when a potentially dangerous action has occurred or when danger is imminent. Warnings help guide users away from potentially dangerous behaviors. Critically, they provide users with an informational feedback loop, allowing HC users to associate their poor cyber hygiene practices with consequences. Unfortunately, users have difficulty understanding warnings in cyberspace (Xiong et al., 2018). HC users lack comprehension of warnings even when purposely designed to best communicate risk (Yang et al., 2017). Warnings play an essential role as a last-ditch effort to prevent users from making poor cyber hygiene decisions. Future research needs to develop the algorithms that generate the warning and the design research to explore user compliance.

Training has been shown to reduce the number of cybersecurity incidents within organizations (Kweon et al., 2019). Lessons from the aviation training literature can help us appreciate the need for cybersecurity training. Two Boeing 737 Max airplane crashes in 2019 resulted from a lack of training (Campbell, 2019). The pilots were new to the automation feature meant to help keep the nose of the plane level. The training on this new feature was considered too costly. And, it would ground pilots from flying the new plane until it was completed. In other words, training employees on critical safety would negatively impact the airline's limited workforce too much. As a result, the Boeing 737 Max pilots were untrained on how to override the new automated system. This desire to avoid training employees on safety and the overreliance on automation eventually led to the two deadly crashes killing 346 people. These tragedies exemplify the struggle of re-training users every time there is a system change. Cybersecurity training can be costly for organizations, but it can be even more costly for organizations to not properly train their employees as cybersecurity automation is being brought to critical infrastructures, such as fuel pipelines and hospital systems.

It is unlikely that future cybersecurity problems will be automated away. Instead, HC users will be asked to partner with automated systems. Users must understand the strengths and limitations of cybersecurity automation. If not, overreliance and misunderstanding will produce vulnerabilities that might produce high costs. Partnering with automated cybersecurity systems is currently complex and needs further research and development. However, we at least need HC users to make good cyber hygiene decisions. Researchers have shown that current cybersecurity training and awareness campaigns are ineffective at improving cyber hygiene (Cain et al., 2018). Often cybersecurity training attempts to address corporate legal accountability instead of effective instructional design. Clearly, the current instruction needs to be re-evaluated to determine the factors that best improve cyber

hygiene learning. For example, it is not enough to just scare people through fear appeals into making good cybersecurity decisions (Dupuis et al., 2021). Instead, users must be informed of the nature of cyber threats for cyber hygiene behaviors to show improvement. A well-designed cyber hygiene training will arm HC users with the knowledge to understand threats and better support users when faced with important decisions.

No single behavioral intervention is shown to help users make better cyber hygiene decisions. Developers need to employ a combination of nudges, warnings, and training materials. Further, a serious attempt needs to be made to improve the visualization and usability of security-related systems. Only a holistic approach will help users and harden our critical systems. For instance, it was shown that combining a warning with training helped participants better long-term cybersecurity decisions (Xiong et al., 2018). Calls for human-centered design work in cybersecurity have been made (Still, 2016). The cybersecurity interfaces of the future need to be more intuitive and transparent to assist users in making timely and appropriate hygienic cyber decisions. It is well known that interactions can vary along a continuum of intuitiveness (Still et al., 2014). Due to this, designers need to prioritize ease of use by attempting to maximize the intuitiveness of cybersecurity systems. In tandem with other behavioral interventions, the development of intuitive interactions in the hybrid home-work computing environment will help to better support users.

CYBER HYGIENE TIPS FOR THE HYBRID HOME-WORK COMPUTING ENVIRONMENT

Clemente (2021) offers many best practices to help users maintain good cyber hygiene in the HC environment. We offer five formal recommendations for users to maintain good cyber hygiene in the hybrid home-work network.

1. *Separate work and personal devices*. It is crucial that computing be separated between work and personal use due to the different computing priorities in each domain. Work computing devices should solely be used for work.
2. *Secure access to devices*. Devices used for work in the home should be secured with a strong password and placed in a locked room when not in use.
3. *Encrypt devices*. All connected devices must be protected with robust and up-to-date encryption. This will help to prevent the chance of unauthorized access and exposure to private organizational information.
4. *Ensure that protected data is stored correctly*. Be aware of data storage best practices for your profession. Know where to store business files to help prevent leaks from work systems into the home system.
5. *Regularly partake in cybersecurity awareness training*. Work to maintain situational awareness of cybersecurity threats and learn about new preventative measures. Aim to create a culture of teamwork and continuous learning around these topics.

This list of recommendations is far from comprehensive but serves as a starting point for organizations to consider as teleworking demand increases. Further recommendations will need to be made that are specific to the unique needs of the hybrid home-work computing environment.

FUTURE RESEARCH

We have a dire need to develop a more robust definition of cyber hygiene, or at the very least decide on a multidisciplinary term that can be used for translational research between disciplines. We need a richer representation of the typical HC users' mental models. What do novice users know, and how can training, nudges, warning, and visualization support cyber hygiene maturity? More research is needed to determine the unique technical and behavioral threats presented in the rapidly changing hybrid home-work computing environment. Hopefully, future research will provide well-defined best practices or specialized behavioral interventions. There have already been calls to further develop best practices for IoT devices and establish human factors programs to help users mitigate cybersecurity risks (Momenzadeh et al., 2020; Nobels, 2019). We hope this chapter draws much-needed attention to the hybrid home-work computing environment and further adds to the ongoing list of research that must be addressed.

CONCLUSIONS

Cybersecurity hygiene is not well defined. There is still no universally accepted operational definition of this concept, which results in varying ways of measuring cyber hygiene. As the home and work computing environments merge to create a growing hybrid home-work computing landscape, the need to better operationalize (and hopefully one day be able to predict) the cyber hygiene of users becomes increasingly apparent. The concept of telework itself is not new, but the landscape around this practice continues to evolve rapidly. It is also clear that behavioral interventions and intuitive design will play an important role in supporting users. These interventions will need to be designed to increase the intention, motivation, and knowledge of good cyber hygiene practices in home-work computer users. Future work should aim to operationalize cyber hygiene as a concept and develop best practices for hybrid home-work computing.

GLOSSARY

CIA Triad – cybersecurity model that characterizes it as protecting the confidentiality, integrity, and availability of data.

Cyber Hygiene – the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet-enabled devices from being compromised in a cyberattack.

Cyber – relating to or characteristic of the culture of computers, information technology, and virtual reality.

Health-Belief Model – attempts to identify the relationships between specific variables and the likelihood of taking preventative health action.

Home Computer User – characterized as a novice that has no formal training in the use of a computer but uses computing devices in the home environment to accomplish tasks to support their lives.

Hybrid Home-Work Computing Environment – the resulting networking environment that is created when a user's HC environment (i.e., personal network) is connected to a work computing environment (i.e., organization network) to create a new computing environment that brings with it some of the characteristics and properties of both computing environments.

Internet of Things (IoT) – everyday objects that are embedded with technology to allow that object to be a part of the digital world.

Nudge – changes in the decision-making process that can predictably alter users' behaviors.

Warning – alerts users when a potentially dangerous action has already occurred or when danger is imminent.

Protection Motivation Theory – describes how individuals are motivated to react in self-protective ways towards a perceived threat.

Theory of Planned Behavior – posits that the intention to perform a behavior is the main indicator of a specific behavior.

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the Internet of Things: Vulnerabilities, threats, intruders, and attacks. *Journal of Cyber Security and Mobility, 4*(1), 65–88. https://doi.org/10.13052/jcsm2245-1439.414

American Psychological Association. (n.d.). Health-belief model. In *APA Dictionary of Psychology*. Retrieved May 24, 2022, from https://dictionary.apa.org/health-belief-model

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Campbell, D. (2019, May 2). *Redline: The Many Human Errors that Brought Down the Boeing 737 Max*. The Verge. Retrieved May 24, 2022, from www.theverge.com/2019/5/2/18518176/boeing-737-max-crash-problems-human-error-mcas-faa

Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 ways to nudge: A review of technology mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, *36*, 1–15. https://doi.org/10.1145/3290605.3300733

Clemente, D. (2021). Personal protection: 'Cyber hygiene'. In Paul Cornish (Ed.), *The Oxford Handbook of Cyber Security* (pp. 361–376). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.001.0001

Detweiler, J. B., Bedell, B. T., Salovey, P., Pronin, E., & Rothman, A. J. (1999). Message framing and sunscreen use: Gain-framed messages motivate beach-goers. *Health Psychology, 18*(2), 189–196. https://doi.org/10.1037/0278-6133.18.2.189

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*, 359–367. https://doi.org/10.1016/j.chb.2016.11.044

Dupuis, M., Jennings, A., & Renaud, K. (2021). Scaring people is not enough. *Proceedings of the 22nd Annual Conference on Information Technology Education*, *22*, 35–40. https://doi.org/10.1145/3450329.3476862

Google Cybersecurity Action Team. (2021). *Threat Horizons: Cloud Threat Intelligence November 2021* [White Paper]. https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf

Howe, A. E., Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (2012). The psychology of security for the home computer user. *2012 IEEE Symposium on Security and Privacy*. 209–223. https://doi.org/10.1109/SP.2012.23

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2019). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09977-z

Lexico. (n.d.). Cyber. In *Lexico.com*. Retrieved May 24, 2022, from www.lexico.com/definition/cyber

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Momenzadeh, B., Dougherty, H., Remmel, M., Myers, S., & Camp, L. J. (2020). Best practices would make things better in the IoT. *IEEE Security & Privacy*, *18*(4), 38–47. https://doi.org/10.1109/msec.2020.2987780

Nobles, C. (2019). Establishing human factors programs to mitigate blind spots in cybersecurity. *MWAIS 2019 Proceedings*. 1-6.https://aisel.aisnet.org/mwais2019/22

OWL Labs. (2021). *State of Remote Work 2021.* Retrieved May 24, 2022, from https://owllabs.com/state-of-remote-work/2021

Still, J. D. (2016). Cybersecurity needs you! *Interactions*, *23*(3), 54–58. https://doi.org/10.1145/2899383

Still, J. D., Still, M. L., & Grgic, J. (2014). Designing intuitive interactions: Exploring performance and reflection measures. *Interacting with Computers*, *27*(3), 271–286. https://doi.org/10.1093/iwc/iwu046

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160. https://doi.org/10.1016/j.dss.2019.113160

Vishwanath, A. (2021). Stop telling people to take those cyber hygiene multivitamins. In M. Khader, G. Ong, & C. Misir (Eds.), *Prepared for Evolving Threats: The Role of Behavioural Sciences in Law Enforcement and Public Safety,* 225–240. World Scientific. https://doi.org/10.1142/9789811219740_0014

Westcott, K. (2019, December 4). *Connectivity and Mobile Trends Survey*. Deloitte United States. Retrieved May 24, 2022, from www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-launches-connectivity-mobile-trends-survey.html

Xiong, A., Proctor, R. W., Yang, W., & Li, N. (2018). Embedding training within warnings improves skills of identifying phishing webpages. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *61*(4), 577–595. https://doi.org/10.1177/0018720818810942

Yang, W., Xiong, A., Chen, J., Proctor, R. W., & Li, N. (2017). Use of phishing training to improve security warning compliance. *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp on–HoTSoS*, *4,* 52–61. https://doi.org/10.1145/3055305.3055310