WORLD LIBRARIES

**Volume 24**

**No. 1**

**2020** **worldlibraries.dom.edu/index.php/worldlib |**

# Cybersecurity—Hacking

Jennifer Lillie

Dominican University

**ABSTRACT**

Preventing hacking is the fundamental principle underlying cyber security initiatives. However, this is essential to consider, especially when devices are connected to the internet. Hackers exploit vulnerabilities, assess weaknesses in Wi-Fi or programs to install a virus, and then invade the person's privacy through hacking into their internet-connected device. Encryption keys that utilize WEP can be hacked into, especially those that use the SNAP header, based on the amount of traffic and the number of times the procedure is implemented. Prevention is the first step, although the cycle is continuous. Thankfully, there are precautions to prevent hacking, including the use of strong passwords, learning safe cybersecurity practices, using secure networks whenever possible, and installing cybersecurity tools to protect WI-FI connections. Companies should consider implementing multi-factor authentication for their

employees and customers, and consumers can learn more about basic cybersecurity principles and practices to assist in protecting themselves from getting hacked.

---

Preventing hacking is the fundamental principle underlying cyber security initiatives. Preventing hacking through Wi-Fi is often overlooked or not considered when implementing basic cybersecurity plans. However, this is essential to consider, especially when devices are connected to the internet. There's sufficient evidence to note that hackers use tools and social manipulation, as well. Prevention is arguably the most important factor in cybersecurity, and preventing hacking from social exploitation, weak passwords, and not using updated tools is essential in mitigating the risks associated with cybersecurity. Detection, management, removal of viruses, and updating tools and practices are other steps involved in cybersecurity process of hacking.

Piore, A. (2019) reports the commonality of users to use predictable passwords and usernames across devices, as well as the lack of any cybersecurity software amongst some devices, with well over 90% not changing one year later. Piore, A. (2019) further explains the social consequences of hacking into internet-related devices, which could include some children's toys, thermostats, and fire detectors. Piore, A. (2019) also points out that some users are unaware of the dangers associated with connecting to the internet without cybersecurity initiatives being taken. Piore, A. (2019) explains that companies can rectify these problems under the new NIST guidelines. One example of a cybersecurity procedure that is not always implemented across internet-connected devices is including a product id which may promote an easier location of devices and a quicker resolution to problems. Nonetheless, these guidelines are not required or mandated by law to protect consumers, and consumers may still be at risk if not educated about safe cybersecurity protocol (Piore, A. 2019). In fact, approximately one million internet-connected devices around the world are estimated to not have any cybersecurity protocol installed, according to Piore, A. (2019).

Berghel, H., and Uecker, J. (2005) report a need to understand the reasons for cybersecurity risks on Wi-Fi (p. 21). Vectors have underlying vulnerabilities on internet-connected devices, which is especially seen in devices that used WEP (Wired Equivalence Privacy) (Berghel, H. and Uecker, J., 2005, p. 21). Encryption keys that utilize WEP can be hacked into, especially those that use the SNAP header, based on the amount of traffic and the number of times the procedure is implemented. If a hacker implements millions of packets through technology (Aircrack, Airsnort, etc.), encryption keys may be recovered, especially if WEP uses sequential ordering of encryption keys instead of randomized encryption keys (Berghel, H. and Uecker, J., 2005, p. 23). Weplap and Aireplay are other technologies that hackers may use to gain access to encryption keys, potentially exploiting defective key implementations, rewiring traffic to be sent mainly from foreign computers (without capturing), or sending mass amounts of traffic to create a Denial of Service (DDoS) attack (Berghel, H. and Uecker, J., 2005, p. 23). A major design flaw of WEP is its lack of protecting XOR encryption from PRGA injection attacks, in which a hacker can easily create a fake IP address, and if they gain access to the string used to encrypt the files, they could use Xor to decrypt the files, themselves (Berghel, H. and Uecker, J., 20015, p. 23). In fact, tools, such as WEPWedgie, automatically collects these authentication features (Berghel, H. and Uecker, J., 2015, p. 23-24). WEPAttack, however, is a tool used to create a dictionary attack that systematically runs the Neesus algorithm to search through a list of possible strings that match (Berghel, H. and Uecker, J., 2015, p. 24). However, there are options that have recently been considered to resolve these common weaknesses in the system, including increasing the length of the key to prevent dictionary attacks, doubling the IV length to prevent FMS attacks, enforcing IV sequencing to prevent replay attacks, rotate keys automatically to prevent FMS, PRGA, and dictionary attacks, provide multi-dimensional authentication to prevent spoofing, and detect packet tampering (Berghel, H. and Uecker, J., 2015, p. 24). Berghel, H. and Uecker, J. (2015) also recommend using long, complex passwords (p. 26).

Connecting directly through WI-FI, instead of a virus or malware, is a major problem affecting users of internet-connected devices everywhere. WI-FI has been accessed to exploit

vulnerabilities of everyday users, using software (Ifware) to force them to change their passwords and close their communication channels (Pagliery, J., 2015). The spyware is installed by the user to remove any malware that may be installed on the device; however, the user's data and information habits may be monitored and/or captured at any time through the router, including updating passwords and taking more intensive security practices (Pageliery, J., 2015). So far, Ifware has infected over 10,000 devices (Pageliery, J., 2015).

According to Reed, B. (2008), hackers with minimal experience and less than 10 PS3s can hack into secure networks (p. 16.). This is because of the design of the PS3's processor (Cell Broadband Engine) (Reed, B., 2008, p. 16). Furthermore, corporate offices in areas with many WI-FI hotspots or Bluetooth connections may be at the most risk of being hacked (Reed, B., 2008, p. 16, 38). However, studying military protocol in internet connectivity may benefit how we understand and implement procedures in everyday life, as they consider assigning soldiers and weapons individual IP addresses when they are in the same urban areas (Reed, B., 2008, p. 38).

Dobrian, J. (2018) explains that hacking may be more dangerous than it appears, with hackers capable of infecting devices with malware or using surveillance to monitor someone (p. 33). Everyone is susceptible to getting hacked. In fact, the Department of Homeland Security was hacked when they told Equifax about their system's vulnerabilities and did not immediately implement a cybersecurity strategy (Dobrian, J., 2018, p. 33). Similarly, most hackers take advantage of social weaknesses of users who click into websites that they think are legitimate or safe, unknowingly downloading malware or viruses onto their computer (Dobrian, J., 2018, p. 33). Preventing social exploitation is necessary to ensure the security of any internet-connected device through using strong passwords in everyday life and getting more educated about how you use the web, including opening emails (Dobrian, J., 2018, p. 34). In fact, over half of cybersecurity issues could be easily prevented through training employees in their everyday internet usage at work (Dobrain, J., 2018, p. 34). In some cases, hackers can gain access to multiple buildings through the internet use of janitors or elevator repairmen who are not

accustomed to the company's cybersecurity initiatives (Dobrian, J., 2018, p. 35). Dobrian, J. (2018) recommends cybersecurity training for tenants of apartments, as well as employees, to reduce the chance of getting hacked (p. 35). To stay safe, it is important to use strong passwords that get changed every few months, never click on a website that is not trusted by you or your employer and does not have a secure web address, being cautious of receiving emails or other messages from people you don't personally know or those which use offers for prizes or free gift cards upon filling out information, and be careful when using cloud computing applications (Dobrian, J., 2018, p. 35).

The CIA (Confidentiality, Integrity, and Availability) model represents the necessary foundation to understand cybersecurity involvement in preventing and minimizing the risks and effects of hacking. Confidentiality is essential in preventing hacking. As the literature has shown, hacking takes away a person's privacy and may have serious social and physical consequences if the device being hacked into is a device used for medical or other necessary purposes. Confidentiality of data for employees and consumers, alike, is important to respect, and securing data involves creating strong passwords that fully protect their information from being accessed. This may prevent theft, identity loss, and loss of privacy. For this reason, integrity of data is very important, as well. Security of the data plays an essential role in cybersecurity, and companies and individuals who utilize this practice maintain high security standards for preventing hacking, often through training and rules. In many cases, employees are held personally responsible for keeping information confidential (private), and a cybersecurity risk may jeopardize this. Availability of data, therefore, is limited to those individuals who are privileged to the information. This may be done in password protection, cybersecurity tools, and encrypted files. Availability also entails maintenance of hardware and updated passwords to keep all files accessible to the populations they serve.

Hackers exploit vulnerabilities, assess weaknesses in Wi-Fi or programs to install a virus, and then invade the person's privacy through hacking into their internet-connected device (figure 3). A more defined process model for understanding hacking (especially when looking

specifically at hacking through WI-FI) may consider the use of weak passwords, social exploitation, and tools used by hackers (figure 1). Literature has shown that short passwords that are not complex (i.e. only use common phrases or do not have multiple types of characters, such as uppercase/lowercase, numbers, etc.), don't get changed often (if at all), and are used in more than one account may present vulnerabilities to the user. Prevention methods should therefore consider how to keep passwords strong through creating long passwords that are multi-dimensional, changed every few months, and changed across accounts. Social vulnerability looks at the individuals being hacked in the likelihood of social exploitation involved in uninformed users clicking on unknown links or responding to emails to people that they don't know, and hacking directly into WI-FI often occurs in urban areas where open WI-FI is available and readily accessible. This can be prevented in informing internet users of the harmful effects of clicking on unknown links and answering emails from unknown senders, providing training to anyone that works with confidential information, and providing an IP address to every internet-connected device to prevent cybercrime and assist in seeking compensation if it were to ever happen. Lastly, hackers may use tools that are free or low cost to illegally hack into internet-connected devices. Common tools used are Ifware, dictionaries, FMS attacks, and PRGA attacks. To prevent tools from hacking into internet-connected devices or personal files, it is important to use long encryption keys, update security/encryption, provide multi-dimensional authentication tools, and detect packet tampering.

Another processing model that can be created is the cybersecurity cycle of stopping hacking (figure 2). Prevention is the first step, although the cycle is continuous. Prevention involves using strong passwords, installing cybersecurity software, and training employees on basic cybersecurity principles. In this way, cybersecurity initiatives focus mon the confidentiality of their populations and integrity of their practices. However, it is also important to detect problems as they occur. After a careful analysis of the problems, business protocols should be taken to address the risks associated with a data breach or being otherwise hacked, as well as design and implement a new process for the problem that occurred. Removal of the problem happens simultaneously, and this would simply mean removing the virus or malware from the

infected devices, if possible. The “last step” would be to update the older procedures so that they reflect the new change in cybersecurity initiatives, ensuring that availability is kept to consumers throughout this process without jeopardizing the confidentiality between parties. This would then be seen in new prevention techniques, which repeats the cycle.

Hacking is a major cybersecurity concern that can affect anybody and cause damage, financial loss, and have devastating social consequences. Thankfully, there are precautions to prevent hacking, including the use of strong passwords, learning safe cybersecurity practices, using secure networks whenever possible, and installing cybersecurity tools to protect WI-FI connections. Processing models can assist in understanding how to conceptualize hacking and the cybersecurity initiatives that need to be taken, as a result. It is important to always prevent hacking, and additional procedures can be implemented to minimize the impact it may have. Companies should consider implementing multi-factor authentication for their employees and customers, and consumers can learn more about basic cybersecurity principles and practices to assist in protecting themselves from getting hacked.

## REFERENCES

Berghel, H., and Uecker, J. (2005). Wi-Fi Attack Vendors. *Communications of the ACM,* 48(8), p. 21-28.

Dobrian, J. (2018). Hacks Can Wreak Havoc, Cyber Experts Warn. *Journal of Property Management,* p. 32-35.

Pagliery, J. (2015). A Vigilante is Changing 10,000 Passwords. *CNN Wire.* CNN Newsource Sales, Inc.

Piore, A. (2019). We're Surrounded by Billions of Internet-connected Devices. Can We Trust Them? There's a dark side to this wirelessdriven revolution in convenience. The danger goes beyond hacking. *Newsweek,* 173 (13). Newsweek LLC.

Reed, B. (2008). Wireless Confidential. *Network World.*

## APPENDIX

**Figure 1**

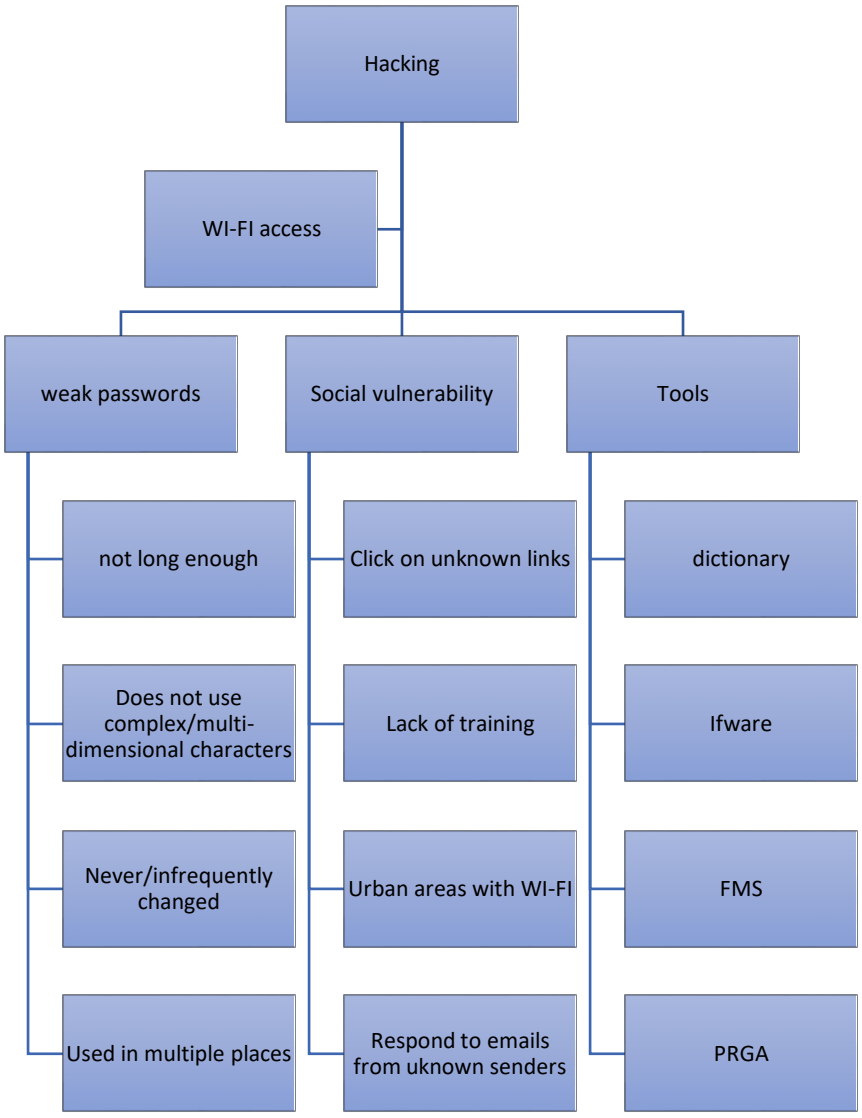

**Figure 2**

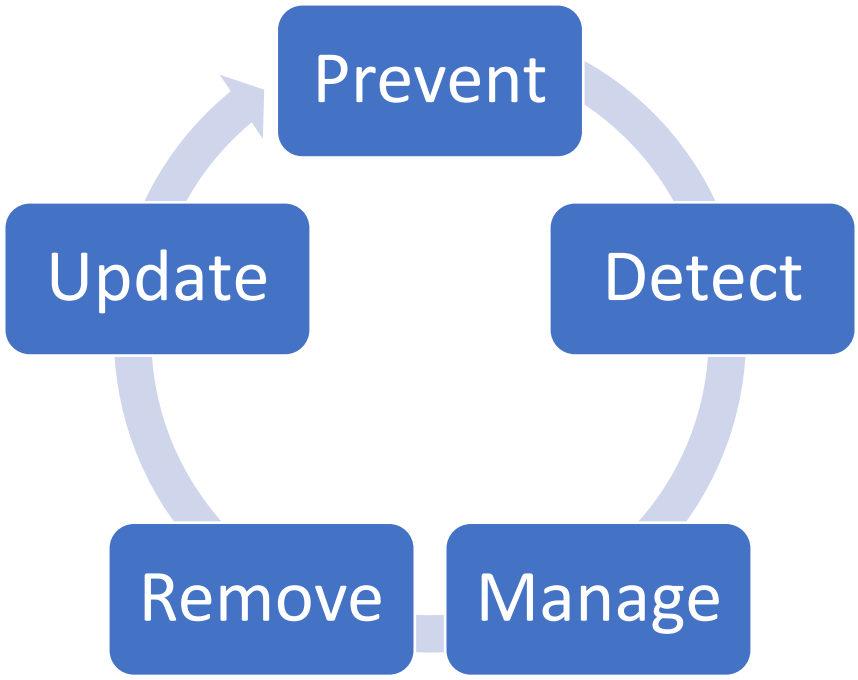


**Figure 3**