CDE #61713

WHY CYBER HYGIENE MATTERS

These are the practices ECCs can use to defend against the threat of cyber criminals.

By Megan Bixler

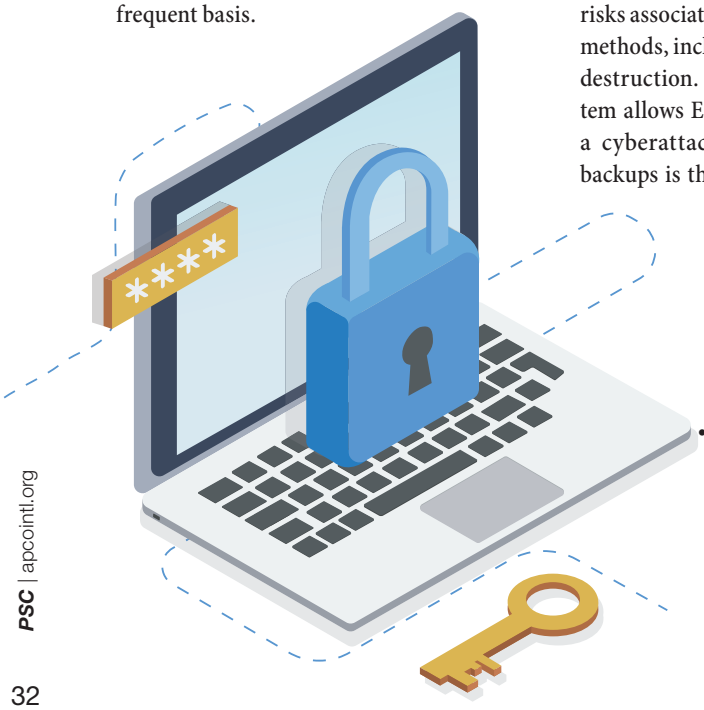
VITALII VODOLAZKYI/SHUTTERSTOCK.COM

Changing passwords can be incredibly frustrating. There are many requirements each organization or agency can choose to have — minimum character amount, use of special characters and upper- and lower-case, expiration deadlines. In addition, to have a good cybersecurity posture, the same password should not be used for multiple accounts and all passwords should be set to expire.

Changing passwords, in addition to other techniques, is broadly categorized as cybersecurity hygiene. This term is a set of practices that organizations and individuals should conduct to maintain the health and security of users, devices, networks and data.[1] Emergency communications centers (ECCs) use and maintain several forms of sensitive data. Cybersecurity hygiene helps ensure that this sensitive data is secure and protected from cybercriminals.

The following are some basic cybersecurity hygiene practices and how these actions can help to protect you and your ECC. These practices aim to reduce the security gaps that hackers can exploit.

- **Update applications, software and operating systems**. Companies often release security updates for their products, which aim to address issues and known vulnerabilities. For some software companies this means regular updates. For example, Microsoft releases security updates regularly to provide continued protection for Microsoft users.[2] Information technology (IT) departments should be aware of and update security patches on a regular and frequent basis.



- **Securely configure systems and devices.** Your IT department knows how to securely configure network resources. The IT department might close off ports within the network, disable or remove unnecessary services and enable other security-conscious configurations. It is important that IT departments test these configurations to ensure security and useability, document any configuration changes and set alerts for potential network breaches.
- **Secure web browsers and web browser add-ons.** A browser not properly configured is the easiest way for malware to infect your computer. The default settings for browsers do not provide the most protection because they are configured for peak performance. Some of the techniques to secure your browser are to not save passwords, disable autofill features, manage your browser cookies to reduce the amount of browser tracking and update your browser version. Your IT department should have specific measures for your agency.
- **Back-up your data.** Having multiple backups of data will help minimize the risks associated with multiple cyberattack methods, including ransomware and data destruction. Having a good backup system allows ECCs to quickly pivot should a cyberattack occur. A good rule for backups is the 3-2-1 rule: three backups, using two different forms of media with one backup offsite. Using the 3-2-1 rule reduces risks from a single point of failure (e.g., disk drive error, stolen hardware, data loss, etc.).
- **Secure your wireless network.** Wireless networks can be extremely vulnerable if not properly configured. Most wireless routers have a broadcast range of 150-300 feet.[3] If your wireless router is not secure, it is vulnerable to myriad cyberattacks (piggybacking, man-in-the-middle attacks, unauthorized computer access, etc.). To minimize the risks to your wireless network, consider the following techniques:[4]
  - o Change default passwords to strong passwords.
  - o Restrict access to authorized users and/or specific computers.
  - o Encrypt network data.
  - o Avoid broadcasting your service set identifier (SSID) or change your SSID to something unique.
  - o Install a firewall on wireless devices.
  - o Ensure your wireless access point (e.g., wireless router, etc.) has the most recent security updates installed.
- **Protect your administrative accounts.** It is critical that system users do not have local administrative permissions on their devices. Administrative users can make any setting change. If administrative privileges are compromised, it could be disastrous for the entire network.
- **Use firewalls.** According to the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS CISA), "Firewalls provide protection against outside cyberattackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Firewalls can be configured to block data from certain locations (i.e., computer network addresses), applications or ports while allowing relevant and necessary data through."[5] There are two categories of firewalls — hardware and software. Hardware firewalls are commonly referred to as network firewalls because they are physical devices that are positioned between the user and the internet. These devices are separate devices that require professionals that are trained to support proper configuration. Software firewalls typically come as a feature within most operating systems, but you can purchase separate software firewalls. A software firewall can be more onerous to implement based on the network configuration. Depending on the jurisdiction and firewall selection used, your IT department might need to configure these tools to meet your jurisdiction's needs.

BSVIT/SHUTTERSTOCK.COM

- **Limit what you post on social media.** Posting information about ourselves on social media has become a social norm — anything from current vacation pictures to favorite meals. However, social media is a treasure trove for social engineers to learn more information about you. These types of cyberattacks are often referred to as social engineering. Social engineers generally aim to steal valuable information or disrupt data to cause harm or inconvenience. They prepare for an attack using social media to learn more about their victim.
- **Use strong and unique passwords**. According to a 2022 Verizon data breach report, 82% of breaches involved a human element, including weak passwords.[6] Weak passwords (e.g., 123456, etc.) are one of the most vulnerable forms of user authentication. Weak passwords are easily and quickly guessed by hackers. Additionally, a user will often reuse passwords across accounts. If one account is compromised, all accounts with the same password are at risk. The National Institute of Standards and Technology (NIST) Special Publication 800-63-3, "Digital Identity Guidelines," recommends a multifaceted approach to identity management. The first is a strong password using the passphrase approach. According to NIST, a passphrase is "a memorized secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is like a password in usage but is generally longer for added security."[7] In other words, creating a phrase and then replacing characters in that phrase with numbers or special characters. An example is turning the phrase "APCOCybersecurityProgram" into "@Pc0cYb3rs3cUr!tyPr0Gr@m." By replacing certain letters in the phrase with special characters or numbers, the passphrase has become incredibly difficult for hackers to guess. In fact, the passphrase example is 24 characters, which will take hackers approximately 40 years to run all possible password combinations.[8] Lastly, it is recommended that IT departments set a limit for invalid password attempts. This greatly slows down hackers' ability to guess passwords.
- **Install antivirus.** Antivirus software has a dictionary of known computer virus parameters. Once these parameters are identified on your computer, the computer virus can be quarantined. Computer viruses are ever evolving, changing and being created. As a result, it is important that antivirus software is continually updated to ensure the most protection.
- **Critically examine emails**. Electronic forms of communication have become ubiquitous means of communication. It is easy to quickly click on links, documents or reply without looking at important information. Due to this, hackers will commonly use phishing to penetrate a network. The SLAM method assists users in critically examining emails to determine legitimacy. If an email looks suspicious, it is a best practice to contact the sender through trusted means of communication to verify their request. The SLAM method is:
  - o **Sender**. Hackers will try to impersonate a trusted entity (e.g., individuals or companies) to trick their victims into opening an email. Email addresses should be carefully checked. One way to do this is to hover your mouse over the sender's email address. This reveals the actual address the message is being sent from.
  - o **Links**. Most phishing emails contain links to websites. Although it may look legitimate, these websites can be nefarious and designed to steal user information, install malware or perform other types of cyberattacks. Users should critically look at the URL before clicking on it.
  - o **Attachments**. Hackers often embed malware in email documents and disguise these documents as important attachments. If the attachment seems suspicious (i.e., you were not expecting it), call the sender to verify the authenticity.
  - o **Message**. The message aspect of the SLAM method is often the easiest to detect. Examine the email message for items such as a generic greeting, misspellings, grammatical errors or strange word choices.

Social engineers generally aim to steal valuable information or disrupt data to cause harm or inconvenience. They prepare for an attack using social media to learn more about their victim.

The points covered in this article are best practices for all organizations to assist in maintaining the health and safety of data, users, devices and networks. However, implementing these best practices and techniques is only the beginning of embracing cybersecurity in emergency communications. APCO American National Standard (ANS) 3.110.1-2019 Cybersecurity Training for Public Safety Communications Personnel provides guidance for ongoing cybersecurity training within the ECC.[9] According to this standard, ECCs should devote four to eight hours annually to educating ECC personnel on cybersecurity policies and their role in maintaining security. Additionally, ECCs should create and embrace a culture of cybersecurity awareness. ECC personnel cybersecurity hygiene is important, but ECC personnel also should be educated about evolving cybersecurity threats, agency-specific policies and procedures, and an agency's cyber incident response plan.

As emergency communications evolve into Next Generation 9-1-1 (NG9-1-1), there has been an increasing concern over the cybersecurity risks to ECCs. Cybersecurity subject matter experts repeatedly have given specific basic cybersecurity hygiene rules as a means for mitigation. These cybersecurity hygiene rules are not meant to be an all-inclusive approach to cybersecurity protections. They are meant to provide protection at the lowest level. Additionally, these rules are not meant to be a replacement for cyber incident response plans. ●

Megan Bixler *is the APCO International Technical Program Manager for the Communications Center and 9-1-1 Services Department.*

REFERENCES

1 TechTarget. "What Is Cyber Hygiene and Why Is it Important?" by Alissa Irei. www.techtarget.com/searchsecurity/definition/cyber-hygiene

2 Microsoft. Microsoft Security Response Center. Security Update Guide. https://msrc.microsoft.com/update-guide

3 Cybersecurity & Infrastructure Security Agency. Security Tip (ST05-003). "Securing Wireless Network." March 11, 2010. Revised May 8, 2020. www.cisa.gov/uscert/ncas/tips/ST05-003

4 ibid.

5 Cybersecurity & Infrastructure Security Agency. Security Tip (ST04-004). "Understanding Firewalls for Home and Small Office Use." June 17, 2009. Revised November 14, 2019. www.cisa.gov/uscert/ncas/tips/ST04-004

6 Verizon. "2022 Data Breach Investigations Report." www.verizon.com/business/resources/reports/dbir/

7 National Institute of Standards and Technology. NIST Special Publication 800-63-3. Revision 3. "Digital Identity Guidelines" by Paul A. Grassi, Michael E. Garcia and James L. Fenton. June 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html

8 "Why Your Passwords Should be at Least 24 Characters Long" by Clinton Emerson. Fox Business. March 5, 2016. www.foxbusiness.com/features/why-your-passwords-should-be-at-least-24-characters-long

9 APCO International. APCO 3.110.1-2019. "Cybersecurity Training for Public Safety Communications Personnel." www.apcointl.org/~documents/standard/31101-2019-cybersecurity/

CDE EXAM #61713

QUESTIONS

1. What is one of the most vulnerable forms of user authentication?
   a. Securing web browsers.
   b. Passwords.
   c. Ransomware.
   d. Antivirus.

2. The IT department might use all of the following to securely configure networks, except:
   a. Closing off ports within the network.
   b. Disabling or removing unnecessary services.
   c. Enable other security-conscious configurations.
   d. Adding additional ports and services.

3. The easiest way for malware to infect your computer includes:
   a. Not saving passwords.
   b. Failure to secure your tracking history.
   c. Not properly configuring the browser.
   d. Enabling autofill features.

4. The 3-2-1 rule includes three backups, using two different forms of media and having one backup offsite.
   a. True
   b. False

5. To minimize the risks to your wireless network, consider the following technique:
   a. Broadcast your service set identifier (SSID).
   b. Ensure your wireless access point (e.g., wireless router, etc.) has the most recent security updates installed.
   c. Allow access only to those within your agency on all computers.
   d. All of the above.
   e. None of the above.

6. Hardware firewalls are commonly referred to as:
   a. Operating systems.
   b. Piggybacks.
   c. Man-in-the-middle.
   d. Network firewalls.

7. Hackers will often embed malware into:
   a. Social media platforms.
   b. Email documents.
   c. Websites.
   d. Hardware firewalls.

8. Emergency Communication Centers (ECCs) should invest ___ hours annually to educate personnel of cybersecurity policies and their role maintaining security.
   a. 12
   b. 16
   c. 24
   d. 8

9. Utilizing the SLAM method, one way to check the email address includes:
   a. Hovering your mouse over the sender's email address.
   b. Contacting the sender via phone or responding to their email.
   c. Open the link or file include in the email and note the content.
   d. Print the email and attachments and view them carefully for false data.

10. Phishing emails contain links to:
    a. Your agency's social media platform.
    b. Your agency's internal network system.
    c. Websites.
    d. Provide antivirus software for future protection.

FOR CREDIT TOWARD APCO RECERTIFICATION(S)

Each CDE article is equal to one credit hour of continuing education

1. Study the CDE article in this issue.
2. Answer the test questions online (see below for online exam instructions) or on the exam page from the magazine article (photocopies are not required).
3. Add/upload your CDE article information and certificate of achievement in the "My Classes Taken" section of APCO's Training Central at www.apcointl.org/trainingcentral.

Questions? Call us at 386-322-2500.

You can access the CDE exam online! To receive a complimentary certificate of completion, you may take the CDE exam online. Go to http://apco.remote-learner.net/login/index.php to create your username and password. Enter CDE in the search box, and click on the "Why Cyber Hygiene Matters," then click on "enroll me" and choose "Why Cyber Hygiene Matters **(61713)**" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.