CDE #61714

CYBER AND PHYSICAL SECURITY IN THE ECC

The two types of security are connected, and we can take steps to enhance both.

By Dorothy Cave

In today's digital age, security and safety in the emergency communications center (ECC) comes in two distinct varieties — cyber and physical. As telecommunicators in the ECC, we are required to ensure that we are not the ones who get our system sick. But what does that mean?

Seemingly innocent activities — like doing our Christmas shopping while sitting on a midnight shift, or joining a dating site on your agency computer during a slow shift — can have dangerous consequences. According to a January 18 report by Firewall Times, Amazon's latest data breach was in October 2021. Hackers accessed Twitch, a streaming platform owned by Amazon, and gained 128 gigabytes of personal information; this information included the account owners' wages. There have also been leaks every year from 2014-2021.[1] Why are we talking about Amazon data breaches? Well, they are the biggest online seller of goods. Most of us have Amazon accounts, and there is nothing wrong with one as long as you are smart about keeping them clean, having unbreakable passwords and, most importantly, keeping them off your agency's internet platform.

One online security expert ran an experiment as described by KSL TV in Salt Lake City, Utah, showing that once an account is compromised "one out of five accounts (18%) get accessed within one hour," and "40% are accessed by cyber criminals within six hours."[2] What can we do in our ECC to stop our system from being hacked? In "Why Cyber Hygiene Matters," appearing in *PSC* magazine's September/October 2022 issue, Megan Bixler, APCO International technical program manager for the Communications Center And 9-1-1 Services Department, wrote about how passwords can slow down hackers. Online accounts have become common place, and the account owners must ensure they develop strong and unique passwords. The passwords that we choose can make or break our system.

When you receive emails from your IT department, put some thought into what your password will be. If you have a password like Password123!, you are setting yourself and your agency up for failure. As Bixler pointed out, there are some very good techniques to ensure your password is not hackable. "An example of this is turning the phrase "APCOCybersecurityProgram" into "@Pc0cYb3rs3cUr!tyPr0Gr@m." Because ECC staff must change their passwords often, you may want to invest in a password keeper.

Agencies do their best to ensure hackers cannot make it through their firewalls by installing and using antivirus software. They may even have certain sites blocked due to their propensity to get hacked. It is never a good idea for you to bypass a block because as soon as you do, something could happen. Doing this is like saying the "Q" word in an ECC (that's "quiet" for those who are unaware); just don't do it! It is never a good idea to save your passwords to your computer either, especially in an ECC. Most centers don't allow you to sit in the same position every shift so when you move, your information moves (depending on your system log in). One issue with saving your passwords is failure to log out before leaving or going to lunch. When your passwords are saved and you don't log out, anyone can use your credentials. If a hacker makes it in under credentials, whether you or someone else logged in under your credentials, it will be an issue for you and your agency. Here are a few ways to ensure you are cyber safe:

- Change your passwords when prompted by your IT department or autogenerated notifications in CAD or agency operating system.
- Never share your passwords with anyone as they are your key into the system.
- If you receive an email that seems too good to be true, don't open it, and make sure your supervisor and IT department know about it. This is known as business email compromise (BEC). Someone has targeted the business or, in this case, the ECC. The hacker is usually looking for money.

LET'S GET PHYSICAL

We also need to talk about physical security in the ECC. Most ECCs are behind a locked gate and/or several security doors, and may have law enforcement officers onsite. Some may include a retinal or palm scanner to enter. Even with all that security, what else can we do to ensure we are safe?

First, let's talk about social media. Most agencies forbid employees from divulging their workplaces on social media. However, if you post watch party photos or ECC Christmas photos, or talk about some of the calls and callers, someone can figure out where you work. These actions might seem innocuous, but they are likely breaking your agency's social media policy.

Detective shows often depict someone being followed and stalked based on their social media posts. Unfortunately, this happens more often than the general public may realize. This could happen to our telecommunicators, law enforcement officers, firefighters, EMTs or medics. There are nefarious people who would not hesitate to harm us just because of our jobs.

Your safety starts with your own behavior. On social media, don't accept a friend request merely because this person is a friend of nine friends out and "looks nice." Know who you are accepting as a friend on social media and make sure your security settings are adjusted. For example, some settings only allow friends to view your pictures or personal information. When traveling between home and work remain aware of your surroundings and maintain situational awareness. Routine can be one of the best access points for someone wishing to do harm. If you arrive at work and don't recognize the vehicle behind you at the access gate, pull through the gate and stop. Allow the gate to close, and if they have permission to enter, they will be able to open the gate. When the midnight shift orders food to be delivered, there should always be two people to retrieve the delivery — one inside the locked security door and one going outside to get the delivery. Never prop doors open. Human and varmint intruders could gain access.

Today, not everyone may be a fan of our industry. Knowing this, we must do everything in our power to maintain a good working environment and protect our cyber and physical safety. We must ensure we are not the reason a hacker gains access to our personal or work accounts when we accept friend requests on social media sites or when we access shopping sites. If your agency has a policy against social media sites or accessing anything that is not work related on work computers, you must adhere to that policy. Make sure you thoroughly read any policy you receive because you are responsible for upholding it. Your agency has a social media policy for a reason — staff safety.

We all have to be diligent when ensuring our safety as well as that of those around us and work hard to keep out the bad actors. They affect not only us but our citizens and responders as well. Keeping a healthy network is the responsibility of the IT Department, telecommunicators, supervisors — in fact, everyone at your agency is responsible for ensuring a physically safe work environment. It takes everyone doing their part following the policies and procedures in place. ●

Dorothy Cave *is the APCO EMD Program Manager for the APCO Institute.*

REFERENCES

1 *Firewall Times*. "Amazon Data Breaches: Full Timeline Through 2022" by Michael X. Heiligenstein. June 22, 2022. https://firewalltimes.com/amazon-data-breach-timeline/#:~:text=In%20December%202014%2C%20hackers%20associated,Xbox%20Live%2C%20and%20other%20websites.

2 KSL TV NBC 5. "How Quickly Hackers Access, Use Your Personal Data Following a Data Breach" by Matt Gephardt and Sloan Schrage, July 19, 2021. https://ksltv.com/468945/how-quickly-hackers-access-use-your-personal-data-following-a-data-breach/

PREVIOUS PAGE: ISTOCK.COM/APCHANEL

CDE EXAM #61714

QUESTIONS

1. Online accounts have become commonplace, leading to a need to be smart about keeping them clean, which includes:
   a. Using these accounts through the secure network in your ECC.
   b. Developing strong and unique passwords.
   c. Maintaining the security of the network by operating outside networks such as Twitch.
   d. Preserving all current and past used passwords ensuring you have a distinct password for each platform.

2. The passwords you choose can:
   a. Make or break a system.
   b. Be listed within the network for access by supervisors and ECC personnel.
   c. Always be used to ensure hackers can only get as far as your access allows.
   d. Never be hacked if kept in a secure network, much like the networks used for radio transmissions.

3. A good technique ensuring your password is resilient and exclusive is (choose all that apply):
   a. Use the KISS method, Keep it Simple, Keep it Short
   b. Preserve the past and future passwords together in a secure document.
   c. Conceal the password(s) you choose by adding numerous characters, numbers and other special symbols.
   d. Invest in a password keeper.

4. ECCs do their best to ensure hackers cannot make it into their networks by:
   a. Installing and using up-to-date antivirus software.
   b. Safeguarding restricted areas within the agency and the ECC.
   c. Making sure all employees log in and log out at the same time.
   d. Confirming all users have access to the network and know the boundaries.

5. The physical security of the ECC is just as important as the cybersecurity of your ECC.
   a. True
   b. False

6. All of these are techniques for ensuring safety in the emergency communications center except:
   a. Being aware of the “friends” you accept on social media.
   b. Never leaving ECC doors propped open.
   c. Using a fingerprint scanner for ECC access.
   d. Allowing anyone to enter the ECC who wants to.

7. When using social media, you should not (choose all that apply):
   a. Post your watch party or Christmas photos.
   b. Advertise your place of employment.
   c. Accept friend requests of those you don’t know.
   d. Be aware of your privacy settings.

8. When creating a new password, you should always use P@$$word99 for ease.
   a. True
   b. False

9. When traveling to and from work, be sure you:
   a. Remain aware of your surroundings and maintain situational awareness.
   b. Use the same route every day so others are aware of your location.
   c. Leave the gate around your ECC (if you have one) propped open for shift change and especially during critical incidents for ease of access by incoming personnel.
   d. When ordering food to be delivered, only allow the delivery person into the hallway of the ECC.

10. Who is ultimately responsible for ensuring the ECC networks maintain good health, allowing public safety telecommunicators to provide the service expected to the responders and community?
    a. IT Department and upper management
    b. Telecommunicators
    c. Supervisors
    d. Everyone

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 “Cyber and Physical Security in the ECC,” then click on “enroll me” and choose “Cyber and Physical Security in the ECC **(61714)**” to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.