CDE #77097

WHAT IS A CYBERATTACK?

Understanding common cyber threats can help ECC personnel recognize risks and protect critical systems.

By the APCO Cybersecurity Committee

According to Forbes, people now spend nearly as much time online each day as they do sleeping.[1] However, it is imperative that users keep both eyes open while scrolling, shopping and streaming, as they may unknowingly leave themselves vulnerable to cybersecurity threats.

Cybersecurity is the responsibility of everyone, from your personal devices to your emergency communications center's (ECC) equipment. It is critical that we know and understand the different types of cyberattacks to prevent becoming a victim.

NIST defines a cyberattack as "any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself."[2] For ECCs, these threats can target critical infrastructure, such as computer-aided dispatch (CAD) systems, phone networks and databases that public safety telecommunicators rely on to respond to emergencies.

MOST COMMON TYPES OF CYBERATTACKS

Common types of cyberattacks include ransomware, phishing and denial-of-service attacks, each exploiting different vulnerabilities in technology and human behavior.[3] As key players in public safety, ECCs must stay vigilant through strong cybersecurity practices. Protecting your systems and networks isn't just a technical responsibility; it's an essential part of protecting your community.

1. **Ransomware:** Ransomware is one of the biggest threats to public safety. More than a technical glitch; it is a digital kidnapping of lifesaving systems. ECCs are high-value targets because their operational urgency creates immense pressure to pay ransoms quickly to restore service. When ransomware strikes, the operational toll creates an "invisible emergency" to anyone outside the ECC, but in reality, it triggers immediate physical and emotional consequences for the employees at the ECC until the attack is resolved. These extra tolls can

KANAWATTH/SHUTTERSTOCK.COM

have deadly consequences for the public during that time.

2. **Phishing:** One of the most common cyberattacks is phishing. This involves a cyber-threat actor attempting to get sensitive information, such as username, passwords, bank account or other private information, from their victim. This can be done by mass email or by personalized emails, phone calls or text messages. The overall goal is to get the user to give the cyber threat actor sensitive information. This typically is done with urgency or fear, such as saying, "You have an overdue balance on an account." Alternatively, a bad actor may say that a victim's equipment will be repossessed if they do not act immediately. Do not click links in emails or open attachments unless you have verified authenticity with the sender by contacting them directly. Pay close attention to the sender of emails and the website URLs to ensure authenticity. Install updates to your equipment and software as soon as they become available; this protects systems and closes gaps cyber criminals look for as weakness into systems. Report anything suspicious to your IT department immediately so that remediation can begin if necessary.
3. **Denial of Service (DoS):** This occurs when a computer system or website is flooded with so many requests that it becomes slow or completely unavailable to normal users. Typically, attackers use a bot, or software application program, to perform automated tasks to carry out this type of attack. This can be an infected phone computer or internet-of-things (IoT) device. This coordinated effort can overwhelm and cripple a company's systems, especially for businesses that rely on online sales. As a result, legitimate users are unable to access services, leading directly to lost revenue.
4. **Malware:** Short for malicious software, malware is placed on a computer or network to steal information, damage systems or provide unauthorized access to a bad actor. The software can be installed without a user's knowledge via images, websites, emails or documents that often appear legitimate. Many attackers use visuals, website URLs and email addresses that closely mimic trusted sources. Some even reuse images from real companies to appear authentic. These tactics rely on users failing to scrutinize what they are interacting with, causing them to unknowingly click links or files that install malware.
5. **Deepfakes and media fraud**: Deepfakes use artificial intelligence (AI) to create realistic but fake images, audio or video that impersonate real people.[4] This technology can be used in scams to obtain sensitive information, facilitate fraudulent money transfers or manipulate individuals into engaging in self-harm. Many ECCs now use technology that allows citizens to share photos and videos in real time — a feature that can be exploited if the media submitted is manipulated or falsified.
6. **Mobile phone threats:** These threats occur when malware is embedded in mobile applications, downloads or other content installed on a device. Once installed, this malicious data can be used by criminals to enhance social engineering attacks by exploiting contacts and personal information stored on a user's device. The vast majority — 98% — of Americans own a mobile phone. This statistic underscores the widespread potential impact of mobile-related threats on individuals.

REASONS BEHIND CYBERATTACKS

Three common motivations for cyberattacks are financial gain, personal motives and political objectives. Common points of entry for cyber threat actors include weak passwords, phishing attempts and physical security lapses such as leaving a workstation unlocked when unattended. Financial gain is one of the most significant reasons that cyber threat actors launch a cyberattack. A recent article in Time magazine states: "Worldwide, the average cost of a single data breach is approximately $4.44 million. In the United States alone, cyberattacks cost companies more than $10 million between March 2024 and February 2025."[5] When looking for opportunities, cyber threat actors tend to gravitate to more lucrative businesses with sensitive data and some that lack sufficient security protocols, making it easier to become compromised.

> **On January 21, 2024, the Bucks County Department of Emergency Communications in Pennsylvania experienced a ransomware attack that brought its computer-aided dispatch (CAD) system fully offline for approximately nine days.**

ECC CYBERATTACK EXAMPLES

The real-life examples below provide some eye-opening attacks that have happened to ECCs large and small.

1. On January 21, 2024, the Bucks County Department of Emergency Communications in Pennsylvania experienced a ransomware attack that brought its computer-aided dispatch (CAD) system fully offline for approximately nine days. Officials later stated that the ransomware group Akira was responsible for the attack. 9-1-1 call taking and radio communications remained operational while dispatchers used contingency procedures.[6]
2. In 2024, Wood County, Ohio, fell victim to a ransomware incident that disabled the sheriff's office CAD system, forcing telecommunicators to record emergency calls by hand for weeks while investigators worked with the FBI. The county eventually paid a $1.5 million ransom to restore its systems, a decision that highlights the extreme financial and operational pressure placed on local governments.[7]
3. On August 2, 2025, the South Shore Regional Emergency Communications Center in Massachusetts experienced an apparent malware attack that made its CAD system unusable for much of the day. Authorities stated the activity was consistent with a foreign-based criminal group, and federal investigators assisted while the center operated using backup procedures.

These examples underscore how vital our centers are and how easily a cyberattack could disrupt the communities we serve, impose substantial costs on our agencies and further intensify the demands of an already challenging job.

HOW ATTACKS AFFECT EVERYDAY PEOPLE

Many people have the false belief that cyber criminals concentrate on attacking large organizations. In a Cyber Security Newsletter,

experts at the University of Tennessee at Chattanooga explain that individuals are actually the primary target of these incidents. Cybercriminals target millions of people every day to steal sensitive information and financial assets. Large organizations are typically far better equipped to detect, respond to and recover from cyberattacks than the average person. To make matters worse, studies show that about 40% of people cannot distinguish between a phishing email and a legitimate one. A cyberattack can compromise financial records, personal data, private documents and other irreplaceable information. Beyond the immediate loss, stolen personal information may be used to carry out additional attacks or fraudulent activities.

SIGNS OF A CYBERATTACK

Previously, signs of a cyberattack were often more obvious: an unexpected system outage, the realization that an attachment was malicious, scrambled filenames or a ransom note. These were all easily identifiable indicators of a potential cyberattack. While they remain very real and relevant examples today, cyber threats have become far more sophisticated.

Decades of experience and lessons learned have created increasingly intelligent adversaries. Cyber threat actors actively work to evade detection by treading lightly and remaining undetected while they establish a foothold for a larger attack or to orchestrate complex theft schemes. As a result, all users must be more vigilant and aware of the tactics, techniques and procedures commonly used by cybercriminals. Watch for the following red flags:

1. Chronic slowness: A sluggish system can be an indicator of malware, ransomware or even a potential cyberattack. When your systems aren't performing as they normally should, be sure to notify your IT staff.
2. Unexpected multi-factor prompts or logins from new devices: New Criminal Justice Information Services (CJIS) regulations have mandated multi-factor authentication (MFA) or Advanced authentication (AA) to be used in emergency communications. Both MFA and AA are strong cyber defense techniques; however, if you receive unexpected MFA prompts or notifications about logins from a new device, assume there has been a compromise and get help.
3. Unusual requests: Whether via phone, email or text, all users should be suspicious of unusual requests, especially if they require use of your authority. With email account compromises at an all-time high a phishing email or malicious request can even come from a legitimate source that you regularly interact with.

Don't let embarrassment hinder you from reporting suspicious activity or accidental link clicks on your part. It is always better to report an incident than to keep it to yourself. You could help protect your agency's entire system with quick reporting of an incident.

HOW TO PROTECT YOURSELF

There are simple steps you can take to help protect yourself and your agency from a cyberattack. Consistency in these best practices will help keep you safe.[8]

Network segmentation prevents a potential attacker from moving laterally across your network, as phones, radios and dispatch software are separated, with little to no access to one another. Limiting the access to your network from the outside limits the ability of attackers to use multiple techniques to gain access to your systems.

Having a cyber incident response plan is extremely helpful as well. If something were to happen, you know who to contact to help limit any potential attack. You can get immediate assistance from your IT staff or whoever is responsible for your network, and also possibly state and other local resources.

Train your staff on things to watch for daily, things like suspicious e-mails, sluggish systems, a large influx of calls coming into the center at one time. Keep them informed on changing cyber threats and include small quizzes and quarterly phishing campaigns to help keep them on their toes and alert.

It is important to set up strong and unique passwords. Ensure passwords are not easy to guess and have 12 or more characters. Include numbers and symbols. In addition to secure passwords, you should set up multi-factor authentication (MFA) on all accounts. Verifying your digital identity through MFA requires two of the following categories: something you know, such as a password; something you have, such as a device; and something you *are*, such as biometrics.

WHAT TO DO IF YOU ARE TARGETED

If you believe you have been the target of a cyberattack, act quickly and notify your agency's IT department. Don't let embarrassment hinder you from reporting suspicious activity or accidental link clicks on your part. It is always better to report an incident than to keep it to yourself. You could help protect your agency's entire system with quick reporting of an incident.

Your department may need to consult with cyber experts outside your agency, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS CISA). As ECCs transition to NG9-1-1, the shift to Internet Protocol (IP)-based networks significantly expands the potential attack surface. This allows cyber threat actors to move laterally from a basic municipal office to sensitive 9-1-1 and CAD systems.

Consequently, robust cybersecurity is no longer an IT luxury; it is a fundamental requirement for modern public safety. Everyone makes a difference in preventing or recognizing a cyberattack. The earlier something is noticed, the faster it can be stopped or possibly prevented before it becomes a problem. Cyberattacks have unfortunately become a nearly weekly thing in our world, and it's important to be aware and prepared. ●

This article was written by members of APCO's Cybersecurity Committee: ***Andrea Beale****, Suffolk Police Department;* ***Jared Steckel, ENP****, TuWay Critical Connection Partners;* ***Denny Stortz****, St. Charles (Missouri) City Police Department;* ***Christine Giglio****, Bedford (Virginia) Emergency Communications;* ***Chauntenay Young, MPA****, Division of Statewide Emergency Telecommunications, Department of Emergency Services & Public Protection;* ***Charles M. Vitale, RPL, ENP, CPE****, Emergency Communications Department, Rochester, New York;* ***Haley Nichols, MBA, CPM****, Interoperability Communication Bureau, Office of the Commissioner, Iowa Department of Public Safety;* ***Jon Whitling, ENP****, Metropolitan Airports Commission;* ***Joshua Moyer****, Warren County Technology Services.*

REFERENCES:

[1] Pelchen, L. (2024). *Internet usage statistics in 2025*. Forbes. https://www.forbes.com/home-improvement/internet/internet-statistics/ (Note: Original Forbes article published March 2024; it projects/encapsulates stats relevant to 2025 usage trends.)

[2] National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Rev. 1). https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[3] Washington State Department of Financial Institutions. (n.d.). *Protecting yourself from cyber-attacks*. State of Washington. https://dfi.wa.gov/consumers/protecting-yourself-cyber-attacks

[4] Cybersecurity Insiders. (n.d.). *Understanding the new cyber threats targeting everyday users*. https://www.cybersecurity-insiders.com/understanding-the-new-cyber-threats-targeting-everyday-users/

[5] Why cybersecurity threats are growing. (2026, March 7). *Time*. https://time.com/7382979/cybersecurity-threats-are-growing/

[6] StateScoop. (2024, December 10). *Ransomware sends Ohio county emergency services back to pen and paper*. https://statescoop.com/wood-county-ohio-ransomware-emergency-services/

[7] StateScoop. (2025, January 27). *Ohio County IT director resigns after $1.5 million ransomware payment*. https://statescoop.com/wood-county-ohio-ransomware-it-director-resigns-2025/

[8] Cybersecurity & Infrastructure Security Agency. (2022, December 18). *4 things you can do to keep yourself cyber safe*. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe

CDE EXAM #77097

1. What is the primary goal of a cyberattack?
   a. To improve system performance
   b. To disrupt, damage or gain unauthorized access to systems
   c. To update outdated software
   d. To increase internet speed

2. Cybersecurity is only the responsibility of IT departments.
   a. True
   b. False

3. Ransomware is described as a digital _____ of lifesaving systems.
   a. Theft
   b. Recording
   c. Fingerprint
   d. Kidnapping

4. Denial-of-Service (DoS) attacks involve flooding a system with requests to make the system unavailable.
   a. True
   b. False

5. Malware can be installed without a user's knowledge through emails, websites, images or documents.
   a. True
   b. False

6. Emergency communications centers are targeted for ransomware because:
   a. They are easily hacked
   b. Operational urgency creates pressure to pay ransoms quickly in order to restore service
   c. Telecommunicators are careless with their passwords
   d. Local governments have large budgets to payoff cyber attackers

7. Why are ECCs high-value targets for ransomware attacks?
   a. They have outdated equipment
   b. They are easy to hack
   c. Their urgency creates pressure to quickly pay ransoms
   d. They do not store sensitive data

8. Only large organizations are targeted by cybercriminals.
   a. True
   b. False

9. Which of the following is a warning sign of a potential cyberattack?
   a. Faster system performance
   b. Unexpected multi-factor authentication prompts
   c. Decreased email volume
   d. Automatic password creation

10. _____ authentication adds an extra layer of security by requiring two forms of identification.
    a. Two-Layer
    b. Double
    c. Secret
    d. Multi-factor

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 https://www.training-apcointl.org/ to create your username and password. Enter CDE in the search box, and click on "**Cyberattack**," then click on "enroll me" and choose "**Cyberattack (77097)**" to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.