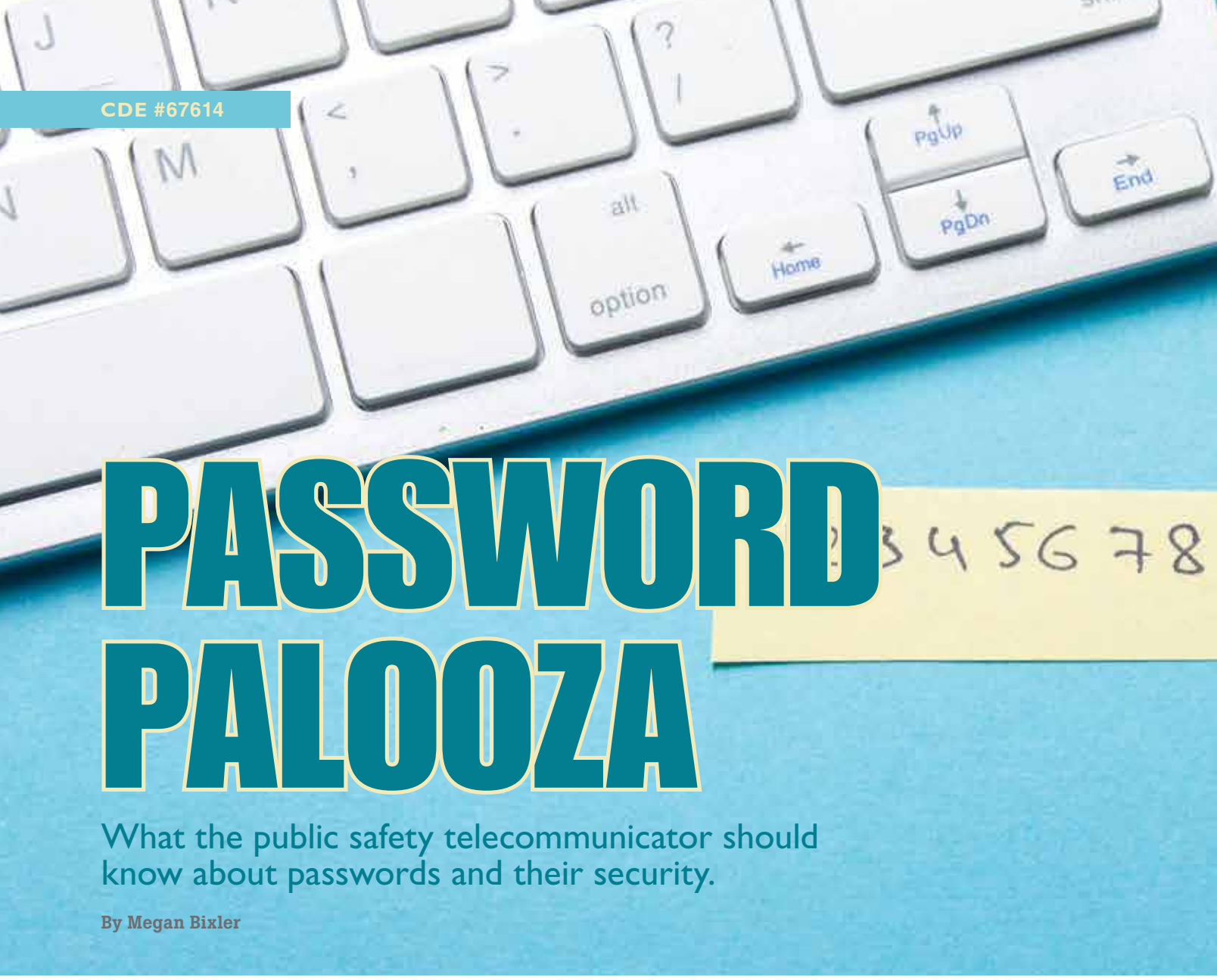
CDE #67614



PASSWORD PALOOZA

What the public safety telecommunicator should know about passwords and their security.

By Megan Bixler

As 9-1-1 approaches a new era of Next Generation 9-1-1 (NG9-1-1), public safety communications will realize a digital ecosystem that is capable of secure end-to-end interoperability, enhanced data analytics, improved resilience and redundancy with the ability to receive, process, store and share multimedia. Inherent to this new digital infrastructure is the need for a robust cybersecurity program.

Some of the basic items that emergency communications centers (ECCs) can do to secure their networks and systems now is to create a robust cybersecurity program. Part of any cybersecurity program is to make strong and unique passwords a requirement for all ECC employees. According to the National Institute of Standards and Technology (NIST) Special Publication 800-63B — Digital Identity Guidelines,[1] robust password practices are fundamental in fortifying emergency communication systems against malicious intrusions and ensuring the integrity of information exchange during critical situations.

THE CRUCIAL ROLE OF STRONG PASSWORDS IN EMERGENCY COMMUNICATIONS

ECC systems and networks are the backbone of emergency response efforts, enabling seamless coordination among first responders, government agencies and the citizens. Whether it's a natural disaster, public health emergency or any other crisis these networks facilitate the dissemination of vital information, allocation of resources and mobilization of response efforts. However, the susceptibility of these systems to cyber threats poses significant challenges, threatening their functionality and compromising response efforts.

NIST, a leading authority in setting cybersecurity standards, provides comprehensive guidelines on password security, emphasizing the pivotal role of strong passwords in enhancing the resilience of emergency communications systems. Strong passwords serve as the first line of defense against unauthorized access and malicious attacks, protecting sensitive information and ensuring the continuity

of emergency communication channels during emergencies. To effectively construct strong passwords, it's essential to understand the concept of entropy and implement strategies to maximize password strength.

UNDERSTANDING ENTROPY: THE KEY TO STRONG PASSWORDS

Entropy, in the context of passwords, refers to the measure of randomness or unpredictability inherent in a password. A password with high entropy is more resistant to brute-force attacks, where attackers systematically guess combinations of characters to gain unauthorized access. NIST advocates for the use of high-entropy passwords to enhance security and mitigate the risk of password-related vulnerabilities. Entropy plays a crucial role in password security by measuring the randomness or unpredictability of passwords.

STRATEGIES TO CONSTRUCT STRONG PASSWORDS

Several factors contribute to constructing strong passwords, but password length is one of the keys. NIST recommends using passwords that are at least 12 to 16 characters, as longer passwords provide greater complexity and resistance to cybersecurity attacks. Passphrases, consisting of multiple words or a sentence, offer an effective way to achieve length without sacrificing memorability. For example, "BusinessEmergencyCouchDog303" is a passphrase that combines random words with numbers and provides robust security. Passphrases offer an excellent alternative to traditional passwords, providing both security and ease of memorization. By stringing together multiple words or a sentence, users can create strong passphrases that are difficult to crack. Avoid common phrases and incorporate numbers, symbols, and spaces to enhance complexity. Other password best practices include:

- **Avoid predictability.** Avoid using easily guessable passwords or information that can be readily obtained about you. Refrain from using common words, phrases or personally identifiable information (PII) like names, birthdays or pet names. Instead, opt for random combinations of characters, numbers and symbols unrelated to personal details.
- **Mix it up.** A strong password should include a mix of uppercase and lowercase

letters, numbers and special characters. This combination increases the complexity of the password and makes it more resistant to attacks, including dictionary attacks and other brute-force methods. Most password-cracking software tools have dictionary attacks built into the software.

- **Randomness is key.** Use password generators or passphrase generators to create random and complex passwords. These tools generate highly secure passwords that are nearly impossible to guess, incorporating a mix of random characters, numbers and symbols. Remember to store these passwords securely in a password manager for easy access and management.
- **Don't reuse passwords.** Each online account should have its unique password. Reusing passwords across multiple accounts increases the risk of a security breach. If one account is compromised, all other accounts with the same password become vulnerable. A password manager can help generate and store unique passwords for each account without the need to remember them all.
- **Avoid common patterns.** Hackers often use algorithms that exploit common patterns in passwords. Avoid sequences like "123456" or "qwerty" as they are among the first combinations tried by attackers. Similarly, patterns such as "asdfgh" or "zxcvbn" are easily guessable and should be avoided.
- **Use acronyms or substitutions.** Consider acronyms or substitutions to create unique passwords. For example, use the first letter of each word in a memorable phrase and substitute numbers and symbols for certain letters. For instance, "I Love Hiking in the Mountains" could become "ILv3H1k1ng!nTh3Mtns".
- **Employ Mnemonics.** Mnemonics can aid in remembering complex passwords. Create a memorable phrase that corresponds to your password. For example, "My favorite song is 'Bohemian Rhapsody' by Queen!" could become "Mfsi'BRbBy3k33N". This method allows you to create strong passwords based on personal experiences or interests.
- **Test password strength.** Before finalizing a password, consider using online tools or built-in features in password managers to test its strength. These tools analyze factors such as length, complexity and entropy to provide an estimate of the password's resilience against attacks.
- **Employ lockout features.** A password lockout feature can permanently or temporarily disable user access after a certain number of unsuccessful login attempts. This slows down hackers using a brute-force attack because it impedes the ability to guess your password. For example, it takes approximately 342,000 years for a hacker to guess a six-character password that locks out after three failed attempts for 10 minutes.[2] Additionally, users and network administrators are usually notified when a user has made three failed attempts to log in. This feature can greatly improve any cybersecurity posture.
- **Educate users.** Effective password security relies not only on strong passwords but also on user awareness and education. ECCs should provide training on password best practices, including the importance of strong passwords, how to create them and the risks associated with weak passwords. Users should be encouraged to report any suspicious activity or attempts to breach their accounts. APCO International offers a series of cybersecurity courses designed for public safety. See apcointl.org/cyber-course-schedule.

PASSWORD WALLETS

With the need to create strong and unique passwords for individual accounts, NIST suggests[3] that password wallets offer greater security and convenience to manage strong and unique passwords. Password wallets are an option to keep track of strong passwords specific to accounts. Password wallets (also known as password managers) offer both advantages and disadvantages to managing and securing passwords for various accounts.

Before jurisdictions decide to implement password wallets, it is essential to understand the benefits and challenges of using this software. Among the considerations for jurisdictions considering the use of Password wallets are:

- **Security.** Password wallets provide a secure vault to store passwords and encrypt them with strong encryption algorithms. However, if the master password or encryption key is weak or compromised for any other reason, all stored passwords could be at risk for hacking and unauthorized access.
- **Creation of passwords.** The creation of strong and unique passwords can be an onerous process for users. Password wallets can assist users in the creation of passwords that are randomly generated, complex and

long. Some password wallet software also indicates whether the new password is strong or weak and easily hacked.

- **Convenience.** Many password wallets offer the ability to copy and paste stored passwords, auto-fill in features on web browsers or applications (after logging into the password wallet) and sync passwords across multiple devices. This usually saves users time when logging in. However, this convenience also means that users are dependent on the service. Some users might also find password wallets complicated to use effectively. This can result in a reluctance to adopt this technology.

CONCLUSION

Strong passwords play a critical role in safeguarding ECC systems against cyber threats and ensuring the reliability of communication channels to both our citizens and fellow responders. By adhering to NIST's guidelines and implementing robust password practices, ECCs can enhance the resilience of their communication infrastructure and mitigate the risk of unauthorized access. Understanding the concept of entropy and employing strategies to maximize password strength are essential steps in constructing strong passwords that can withstand evolving cybersecurity threats. As ECC networks continue to evolve, prioritizing password security remains imperative in safeguarding public safety and the citizens that we serve. ●

***Megan Bixler, RPL, CPE**, is the Senior Technology Strategist for APCO International.*

REFERENCES

1 National Institute of Standards and Technology. "Digital Identity Guidelines." NIST Special Publication 800-63B. Oct. 16, 2023. https://pages.nist.gov/800-63-3/sp800-63b.html.
2 APCO International. "Cybersecurity Fundamentals for the ECC (1st Ed.)." APCO Institute. 2022.
3 National Institute of Standards and Technology. "Frequently Asked Questions." March 3, 2022. https://pages.nist.gov/800-63-FAQ/#q-b12.

CDE EXAM #67614

1. Entropy refers to:
   a. The overall mission of passwords
   b. Measure of randomness or unpredictability inherent in a password
   c. Strategies and goals of hackers
   d. Your ECC's overall cybersecurity posture

2. NIST stands for:
   a. No Internet Service Technologies
   b. Non Isometric Science Training
   c. Nature of Internet Service Training
   d. National Institute of Standards and Technology

3. NIST recommends that password length should be:
   a. 25+ characters
   b. 12-16 characters
   c. No guidance has been given
   d. 8-12 characters

4. Password characters should include:
   a. Uppercase, lowercase, numbers and special characters
   b. Personal identifiable information (PII)
   c. Common dictionary words or sequential numbers
   d. Name of pets

5. Mnemonics can aid in remembering your username to log into accounts.
   a. True
   b. False

6. Passwords should not be reused across multiple accounts.
   a. True
   b. False

7. Password wallets are:
   a. A tool to keep track of strong passwords specific to accounts
   b. A physical notebook to write down passwords
   c. A USB device to remember all of your keystrokes
   d. A tool used to conduct brute-force cybersecurity attacks

8. What's NG9-1-1?
   a. Next Generation 9-1-1
   b. New Generation 9-1-1
   c. Neighbor's Garage 9-1-1
   d. Neonatal 9-1-1 Emergency

9. There are no disadvantages to using a password wallet.
   a. True
   b. False

10. ECCs should educate users on password best practices.
    a. True
    b. False

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 "Password Palooza," then click on "enroll me" and choose **"Password Palooza (67614)"** to begin the exam. Upon successful completion of the quiz, a certificate of achievement will be available for download/printing.