ADVANCED

CYBERSECURITY
AWARENESS
MONTH

SECURITY SYNOPSIS

Enhancing Digital Security

Passwords, Passphrases, and Multi-Factor Authentication (MFA)

In today's digital age, securing your online presence is paramount. This synopsis addresses the fundamental aspects of digital security, focusing on passwords, passphrases, and multi-factor authentication (MFA). We delve into the importance of strong authentication methods and offer practical tips for individuals and organizations to bolster their cybersecurity defenses.

The digital landscape is fraught with risks, from data breaches to identity theft. As such, understanding and implementing effective security measures is crucial. Three key components of digital security are passwords, passphrases, and MFA.

PASSWORDS

Passwords are the most common method for authenticating users, but they are also one of the weakest links in security. Here are some ways for you to enhance password security:

- **Complexity:** Create passwords that include a mix of upper- and lower-case letters, numbers, and special characters
- **Uniqueness:** Avoid using easily guessable passwords like "123456" or "password," use unique passwords for each account
- **Regular Changes:** Change passwords periodically, especially for sensitive accounts
- **Password Managers:** Consider using password management tools to generate and securely store complex passwords

PASSPHRASES

Passphrases are longer and more secure alternatives to passwords, and therefore harder to crack through brute force. They are easier to remember and can easily satisfy complex rules and requirements for passwords. Here's are a few tips to creating strong passphrases:

- **Length:** Aim for at least 15 characters
- **Variety:** Include a mix of words, numbers, and symbols
- **Unpredictability:** Choose random or nonsense words; avoid common phrases and lyrics, and choose something unique to you
- **Uniqueness:** Use unique passphrases for each account

MULTI-FACTOR AUTHENTICATION (MFA)

MFA adds an extra layer of security by requiring users to provide multiple forms of identification. Common MFA methods include:

- **Something You Know:** A password or passphrase
- **Something You Have:** A mobile device or security token
- **Something You Are:** Biometric data like fingerprints or facial recognition

UPDATING YOUR PASSWORDS

Users have an estimated 100 account / password combinations to keep track of, which makes securing your accounts seem like an impossible task. Consider a daily approach to enhance security: Start by strengthening the passwords and enabling multi-factor authentication (MFA) on your top three accounts (*e.g.,* financial and email). Continue with the next three essential accounts each day, progressively strengthening your security posture.

Nota bene: Don’t forget about mobile apps like Facebook or Amazon that keep you logged in.

EVALUATING PASSWORD MANAGERS

In the modern age, safely keeping track of passwords (not re-using passwords or changing a numerical value on multiple iterations) can be an impossible task. That’s where password keepers come in: they can simplify your digital security while keeping your sensitive data locked away.

Here are some tips to consider when evaluating a password keeper:

- Does the company have a history of breaches or outages?
- Is the data encrypted?
- Do they deploy zero-trust security?
- What are the capabilities and integrations (*e.g.,* does it have browser extensions)?
- Does it offer multi-platform and device sync?
- What are the support and recovery options?
- Does it generate secure passwords?
- Does it offer multi-factor authentication?

Keep in mind, the best choice isn't always about cost when it comes to password managers. Free or inexpensive options may not always offer the best security.

CONCLUSION

In an era where cyber threats are ubiquitous, safeguarding our digital lives is imperative. Strong passwords, passphrases, and multi-factor authentication provide effective defenses against unauthorized access and data breaches. By following best practices and embracing these security measures, individuals and organizations can significantly reduce the risks associated with the digital world.

ADDITIONAL RESOURCES

- Choosing and Protecting Passwords by CISA, Revised November 18, 2019
    - cisa.gov/news-events/news/choosing-and-protecting-passwords
- NIST Password Guidelines, Updated March 17, 2023
    - blog.netwrix.com/2022/11/14/nist-password-guidelines

ABOUT ADVANCED

For more than 40 years, Advanced has been a leading provider of comprehensive IT solutions: creating innovative networks, implementing comprehensive cybersecurity initiatives, and delivering exceptional IT support. Our proactive approach to trends and threats drives the development of scalable solutions to help business stay ahead in an ever-evolving technology landscape.

As always, Advanced is proud to be here for all your security needs. Reach out now (advance@actweb.comp) to determine how you can improve your security posture and keep your business running smoothly.