SecurityAwarenessNews

the security awareness newsletter for security aware people

Identification & Authentication

Password Security Refresher

Types of MFA

Beyond Passwords

Password Security Refresher

Password management represents one of the most critical aspects of security. It's also an area of security where people tend to take a lackadaisical approach, putting their accounts and confidential information at risk. Use the following password refresher to ensure that your login credentials are, at a minimum, up to modern standards. Note, these are general guidelines that we should all adhere to in our personal lives. Here at work, always follow current password policies.

How long should a password be?

Length equals strength! Many security professionals recommend 16 unrepeated characters.

Should you use symbols, numbers, and letters?

While it's true that complex passwords are difficult to crack, they're also difficult to remember. Avoid complicating your passwords with random characters unless required.

What is a passphrase?

A passphrase is a string of words that make sense to you, such as a quote from your favorite book or movie. Passphrases satisfy length requirements, yet are easy to remember while hard to guess.

How often should you change your password?

Changing passwords frequently is an outdated and challenging process. New guidelines recommend changing passwords only if you fear an account has been compromised (such as when major data breaches occur).

Is it okay to reuse a strong password?

Absolutely not. Every account should have a unique password. Otherwise, if your credentials get stolen (due to a data breach), someone could use them to gain access to multiple accounts.

What's a password manager?

A password manager is software that can create, store, and sync your login credentials. Ask about using one here at work, and definitely utilize one in your personal life.

What about multi-factor authentication?

Multi-factor authentication, or MFA, adds an additional layer of security by requiring you to enter a secondary code before accessing an account. Enable it wherever it's available.

Types of MFA

Even though you can prevent someone from guessing your passwords, you can't prevent someone from stealing them. That's why MFA is so vital. It adds an extra step to your basic login procedure by combining at least two of the following common types of factors:

KNOWLEDGE

Something you know, such as your password.

POSSESSION

Something you have, such as your smartphone.

BIOMETRICS

Something you are, such as a fingerprint.

Here are a few of the most prevalent utilizations of MFA:

Phone

This convenient (and most common) second factor of authentication generates a text message or automated phone call with a temporary passcode. Unfortunately, "most common" also means "least secure." Voice calls and text messages can be intercepted, rendering this authentication process inferior to other options.

Software Tokens

Software tokens are specific apps or software that generate time-based one-time passwords (TOTP). The token constantly rotates passcodes, causing them to expire after a short time interval (usually under a minute). Google Authenticator is an example of a software token. This is a far superior process to phone or email messages because it requires you to have physical possession of the device to log into an account. Caveat: some strains of malicious software can steal these codes, so think before you click!

Email

Similar to text message authentication, this method sends a secondary code to a predetermined email address. Also similar to text messages, email authentication hardly improves security since it can be easily hacked. Still, both methods offer better protection than not implementing MFA because you will at least get a notification if someone is trying to access an account.

Hardware Tokens

Considered the strongest type of MFA, traditional hardware tokens often come in the form of a small USB stick. Instead of entering a second passcode, you simply insert the token into a USB port and press a button on the token. Modern versions can connect wirelessly to your device and authenticate your accounts without the need to manually enter the passcode or physically connect to the token, similar to a key fob.

Here at work, always follow our policies regarding passwords and MFA. In your personal life, we strongly recommend enabling MFA wherever possible.

BEYOND PASSWORDS

Cybersecurity is all about protecting access, which includes using strong, unique passwords for every account, and complementing those passwords with security tools like password managers and MFA. But protecting access requires more than just safeguarding login credentials. Both at work and home, we all need to take extra measures to ensure confidential information remains confidential. Here's how:

Lock your workstation.

Even if you're "only" going to be gone for a couple of minutes, locking a workstation takes almost no effort and is one of the easiest ways to protect access. Pro tip: use a keyboard shortcut. On Apple computers, press and hold the Shift, Command, and Q buttons. On Windows machines, hit the Windows key and the L button.

Prevent piggybacking and tailgating

Piggybacking is when you allow someone else to use your credentials, such as holding a secured door open, letting someone borrow your badge/keycard, or purposefully revealing your login credentials. Tailgating happens when someone slips in behind you after you access a secured area. Both are easily preventable with a little common sense and situational awareness.

Separate work and personal accounts

Avoid using work-issued devices for personal reasons and vice versa. Similarly, never use your work email to conduct personal business. Segregating work from personal helps prevent accidental data leaks and upgrades privacy in both cases.

Think before you click.

The easiest way to give cybercriminals access to systems or data is by clicking on a phishing link. Stay alert for common red flags of phishing attacks like lousy grammar, threatening or urgent language, and unrealistic promises. Remain skeptical any time you receive a request for sensitive information or money. Always verify the sender and the recipient when communicating via email.

Beware of random USB devices.

If you ever find a USB flash drive, don't plug it into any devices. Instead, report it immediately. Attackers use USBs to spread malware and steal data or login credentials. Only use the USB devices you own and trust, including charging cables.

Properly dispose of physical documents

Dumpster diving may seem like something that only happens in fiction, but it's a realistic method used by criminals to gain easy access to sensitive information. Avoid printing out physical copies of anything confidential. If you do, keep them under lock and key and shred them when no longer needed. When retiring smart devices, be sure to completely erase them by restoring to factory settings.

Remember, when you are given access to our systems and data, you become responsible for that access. Always follow policies and report security incidents immediately. If you have any questions, please ask!