November 2023

SecurityAwarenessNews

the security awareness newsletter for security aware people

Identification & Authentication

- Password Facts
- Multi-Factor Authentication Explained
- Access Control

Password Facts

Who are you? *(Enter username.)* Prove it. *(Enter password.)*

That's the basic process of identification and authentication. Unfortunately, as simple as it sounds, password management remains a complicated issue.

If you research what security experts consider a "strong" password, you'll find several different ideas. Most agree they should be long, yet no one seems to agree on how long. Some recommend using a mix of symbols and numbers, while others argue this makes passwords too difficult to remember.

However, everyone does agree on one fact: Password strength is a vital part of security. Let's review a few other facts that help clear up some of the challenges of password management.

At work, policy comes first.

Not to discredit the security researchers of the world, but following password policies is the most important first step. Many organizations have firm requirements for how passwords are created, how they're stored, and when they should be changed. It's your responsibility to always adhere to those requirements.

Length is key.

The shorter a password is, the easier it is to guess. While not everyone agrees on the specifics, it's quite obvious that a six-character password is much weaker than a 16-character password. Don't overlook this simple fact, and ensure all your passwords prioritize length.

Password cracking tools are evolving.

Cybercriminals often use software that can automatically guess thousands of different password combinations. These tools are getting smarter as modern technology evolves. As such, it's vital that every individual creates passwords that are unlikely to be guessed by automated tools.

Reused passwords weaken security.

Imagine someone uses one password for three different accounts. Now imagine the website of one of those accounts gets hacked, and the password is stolen. The thief could then use it to access the other two accounts, an attack known as credential stuffing. Avoid this by protecting every account with a unique password.

Passphrases are stronger than traditional passwords.

A passphrase is a sentence or string of words. The key to creating strong passphrases is combining words that are easy to remember yet hard to guess. They should make sense to only you, such as an obscure quote from your favorite book, movie, or song.

Multi-Factor Authentication Explained

What is multi-factor authentication?

In simple terms, multi-factor authentication, or MFA for short, requires you to enter more than one password or form of authentication. It's a great security tool that adds an extra step to your basic login procedure by combining at least two of the following common types of factors:

- ***Something you know, such as your password.***
- ***Something you have, such as your smartphone.***
- ***Something you are, such as your fingerprint.***

How does MFA work?

Without MFA, you log into your account by simply entering your username (or email address) and password. With MFA enabled, you go through the same login process, but the system or account prompts you to enter an additional code. Access is only granted if you can provide the additional authentication factor.

How are MFA codes delivered?

MFA codes are commonly sent via text messages, phone calls, emails, or smartphone push notifications. You can also use software that generates time-based passwords that constantly change or hardware tokens like USB sticks.

Why use MFA?

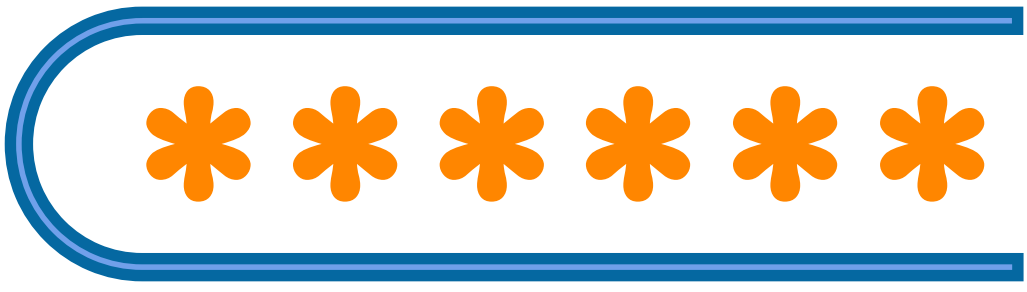
Even the strongest password is susceptible to getting stolen via data leaks and other security incidents. By using MFA, you create a second barrier criminals will need to circumvent to gain access. Plus, you'll be alerted if someone attempts to log into an account.

Is MFA perfectly secure?

Unfortunately, there is no such thing as perfect security. Codes sent via text message or email, for example, can be intercepted and stolen. But the goal isn't perfection. It's to make it as difficult as possible for cybercriminals to steal information or take over accounts. MFA brings us closer to that goal.

Which accounts should use MFA?

At work, follow organizational policies for when and how to use MFA. Otherwise, it's a good idea to enable MFA where it's available. View it as your password's most valuable sidekick that exists to protect your confidential information.



Access Control

While creating strong passwords is vital to securing accounts and confidential information, it's only one part of the process. Safeguarding access, both physical and digital, requires multiple layers of security awareness. Here are a few simple ways you can protect the access you've been granted:

Think before you click.

Cybercriminals often use phishing attacks to steal passwords and other confidential data. Most of those attacks attempt to mislead people into making a poor choice, such as opening a malicious link or attachment. You can avoid them by staying alert for common warning signs like threatening language, urgent messaging, and unexpected requests for sensitive information or money.

Lock devices when not in use.

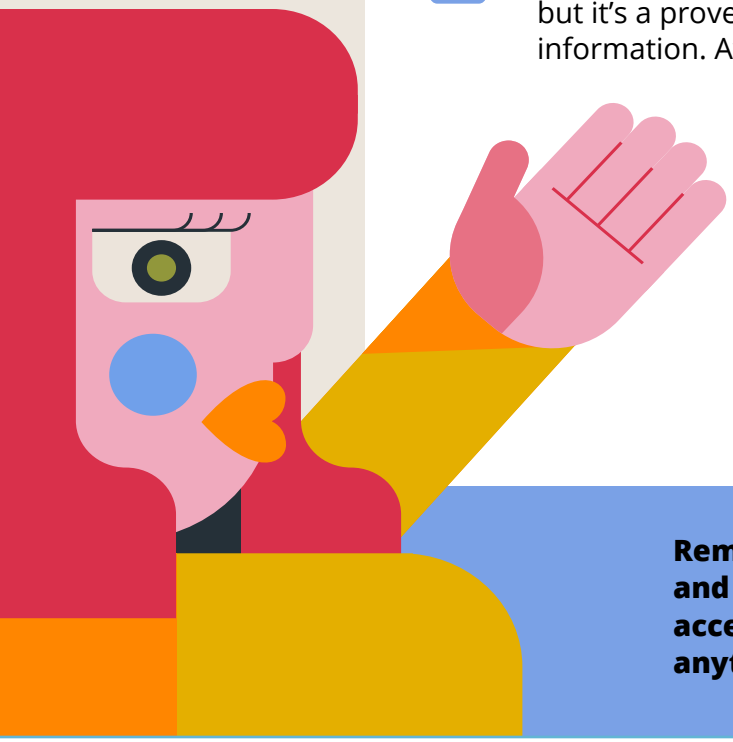
Even if you're going to be gone for "only" a couple of minutes, locking a workstation takes almost no effort and is one of the easiest ways to protect access. Pro tip: Use a keyboard shortcut. On Apple computers, press and hold the Control, Command, and Q buttons. On Windows machines, press and hold 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 ID badge, or purposefully revealing your login credentials. Tailgating happens when someone slips in behind you after you access a secured area. By using a little bit of situational awareness, you can avoid these simple security errors.

Properly dispose of physical documents.

Dumpster diving may seem like something that only happens in fiction, but it's a proven way that criminals use to gain easy access to sensitive information. Avoid printing out physical copies of anything confidential. If you do, always store them in a secure manner and properly dispose of them according to policy.



Beware of random USB devices.

If you ever find a USB flash drive or charging cable, don't plug it into any devices. Attackers use USB drives and cables as an easy way to spread malicious software that can steal data or login credentials. Only use the USB devices you own and trust.

Remember, when you are given access to physical and digital assets, you become responsible for that access. Be sure to always follow policies and report anything suspicious immediately.