Personal Security Best Practices

Learn how to keep yourself safe online by practicing smart cybersecurity habits.

A great place to start applying your new knowledge of cybersecurity is to start with the security of your own accounts and devices! We can keep ourselves safe online by implementing best practices, choosing more secure tools, and keeping our knowledge and systems up to date.

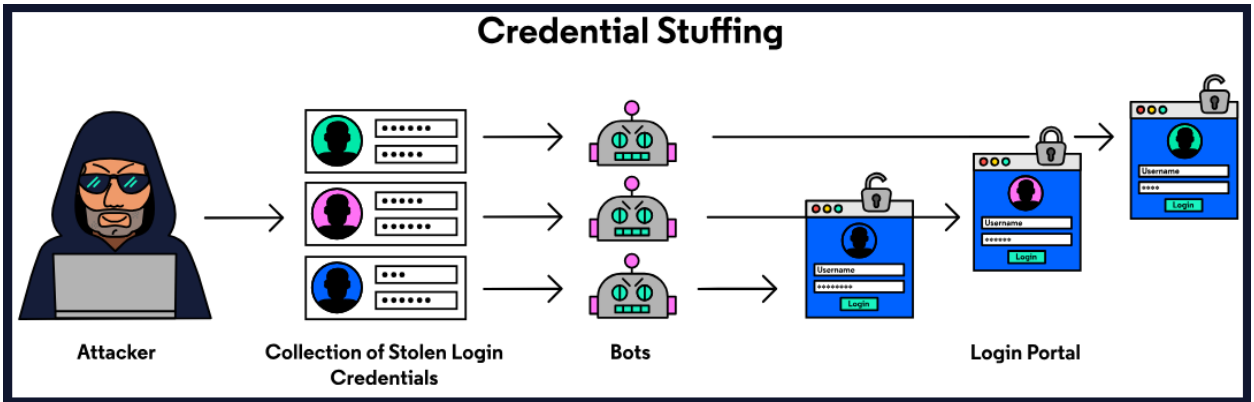
Account Safety & Password Management

Passwords are everywhere. A study in February 2020 found that the average person has more than 70-80 passwords. With everything from your email to your local pizza place requiring a password to use, it's no surprise that up to 65% of people reuse the same password for multiple accounts.

But why does this matter? After all, even if your bank account and your streaming account use the same password, nobody is going to guess if the password is based on your mother's favorite recipe, are they? This might be surprising, but it doesn't take much to guess. Today, there are common methods to guess passwords in a variety of ways, such as brute-forcing, credential stuffing, dictionary attacks, and rainbow tables.

Don't Reuse the Same Password for Many Sites

A bank may be less likely to suffer a security breach, but what about all the other websites we use? By some metrics, 30,000 websites are hacked every day. When people hack into the website of a small company and steal the usernames and passwords of users, they are then able to use freely available credential stuffing tools to automatically try those username and password combinations across thousands of other sites.



Credential stuffing can happen in the blink of an eye!

If you're not convinced, try services such as Have I Been Pwned that can tell you whether your email address has been involved in a data breach.

Use Strong Passwords or Passphrases

The more characters, different capitalizations, special symbols a password has, the harder it is to "brute-force". You can try How Secure is My Password? to see how long it could take to brute force your password. Is your password "password"? That would take 0.29 milliseconds to guess. How about "w324kj&^lsdj"? That would take 25,937,833 millennia.

Disclaimer: Don't go putting your password into just any "password testing" site! These are two that we trust, but others might try to store your password for malicious purposes."

Use a Password Manager

A password manager is software that usually comes in a browser extension form, and it stores all of your passwords in encrypted form so that you don't have to remember all of them individually. Instead, you only have to remember one master password. Even the United States government recommends using one!

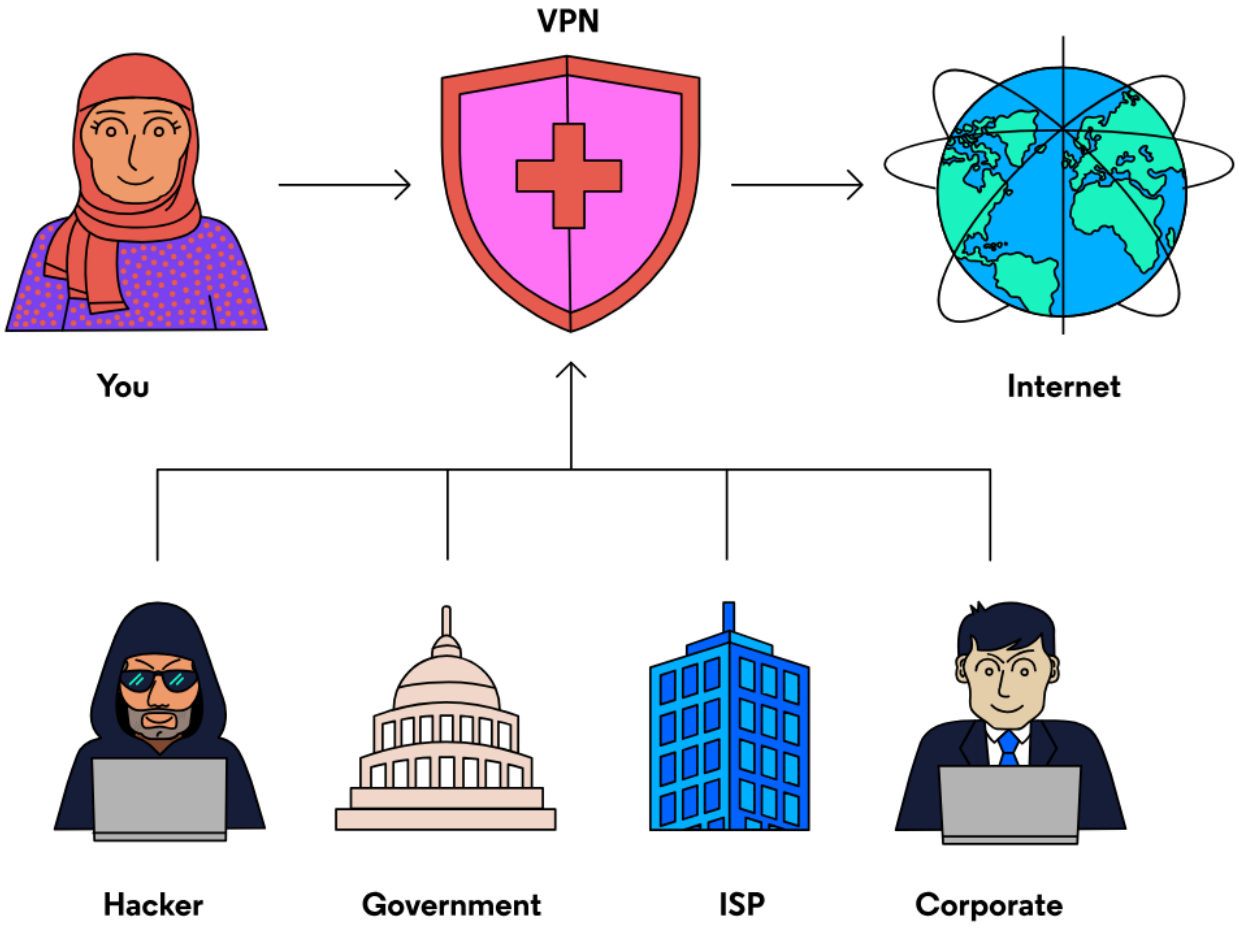
Set Multi-Factor Authentication

Make sure you use two-factor authentication (2FA) and multi-factor authentication (MFA) wherever and whenever possible. Every extra authentication step adds a layer of protection. At the very least, 2FA should be enabled for high-value accounts such as your bank account. Tools like the Google Authenticator App or YubiKey make code-based MFA more convenient.

Using Virtual Private Networks

Virtual Private Networks (VPNs) are a pretty cool tool. With the click of a button, you can be browsing the Internet disguised as a device from Paris, or Beirut, or Kinshasa.

Of course, the drawback is that accessing the Internet through a VPN can slow down your internet experience, and VPN services usually cost money. But VPNs are an essential tool because they provide two things: anonymity and security.



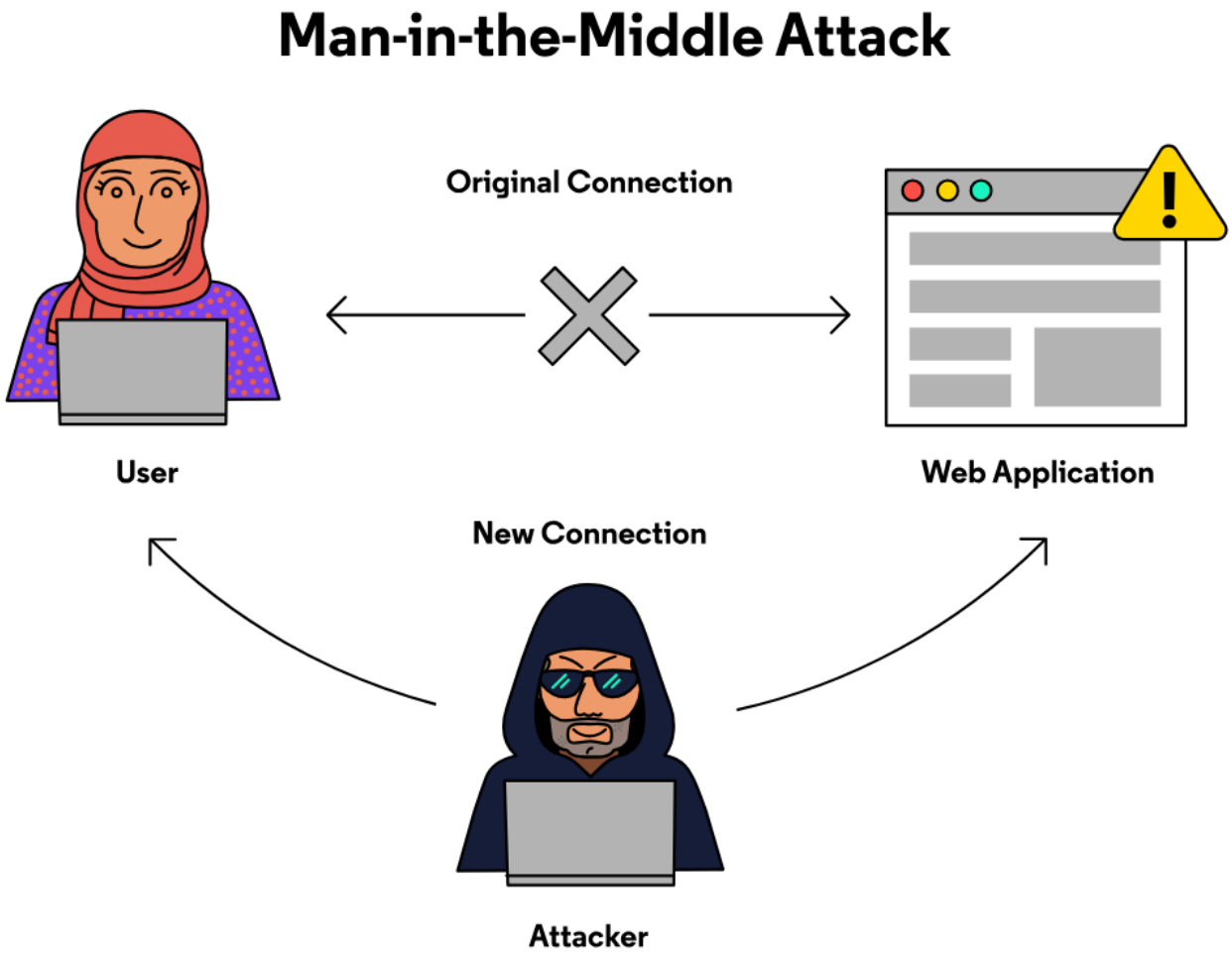
You might ask, "Why is anonymity important? I'm not doing anything illegal." That may be true, but you should understand that if you're not using a VPN, your Internet Service Provider (ISP) can see everything you're doing. They can see which websites you visit, the time you spend on them, what you do on them, the device you're using, and where you are. They are also allowed to take that data and sell it.

When not using a VPN, every website you visit, and sometimes people and websites you communicate with online, are able to see your IP Address and location by using beacons.

Maybe you're okay with not being anonymous. However, VPNs also add security. They can protect you from *Man-In-The-Middle (MITM) Attacks*, in which network traffic is intercepted by a malicious third party. When you use a VPN, it creates an encrypted

tunnel between you and a remote server operated by your VPN provider. That prevents your ISP, others on your WiFi network, and websites from seeing what you're doing.

So, if you log on to that suspicious public WiFi network with a VPN turned on, you don't have to worry about your username and password being stolen.



Messaging Security

Just as VPN encryption keeps you safe from eavesdroppers, the encryption provided by certain messaging apps such as Signal, or email providers such as Protonmail or Tutanota can also help to keep you secure. What makes these services different from more widely known competitors is that all of them offer end-to-end encryption. Essentially, using encrypted communication platforms both protects your

data from being taken and prevents companies from collecting data from your messages for marketing purposes.

Browser Security

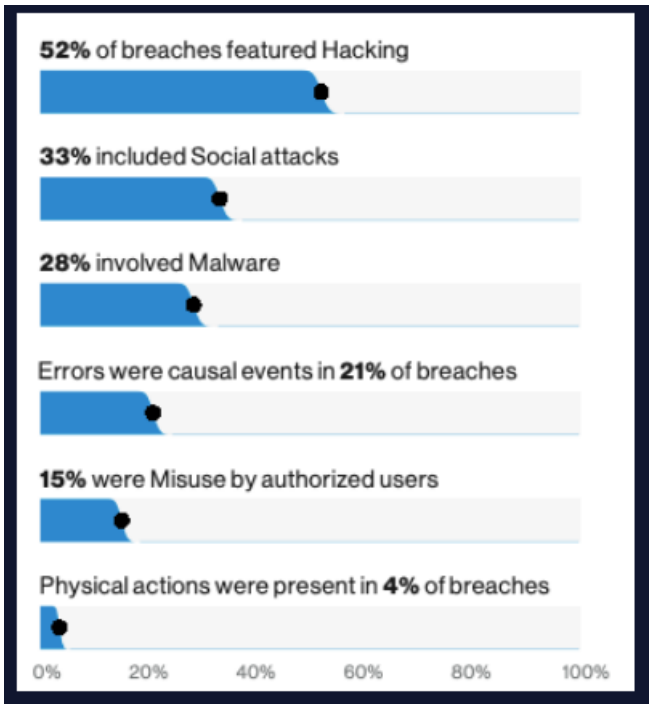
The type of browser you choose can also matter. There are a wide array of browsers to choose from offering unique features, but some browsers are more secure than others. For example, some browsers may update frequently but allow third parties to track you, whereas others may have the opposite problem. However, no matter what browser you are using, by always running the latest software available to you, you ensure that you are protected from the vast majority of attacks.

Keeping Software Up to Date

Knowledge is power when it comes to cybersecurity. Threat actors exploit vulnerabilities to gain unauthorized access to information, but by keeping yourself and your systems up to date you can make those vulnerabilities harder to exploit. Make sure that you are running the current version of your browser and operating system. Make sure to download new updates on your devices as well, since they often release specific patches for vulnerabilities.

Look out for Social Engineering

Protecting your systems is only half the battle. The most secure system in the world is still vulnerable to human error and social engineering attacks such as phishing, which was a factor in 33% of data breaches in 2019. Making sure you know how to spot phishing, baiting, scareware and other social engineering attacks is as important as keeping your systems secure.



Attack Types 2019, from the Verizon Data Breach Report

Conclusion

You might not make all these changes at once, but these adjustments can make a huge difference! These are also good practices to start implementing across members of your organization.