Multi-Factor (or Two-Factor) Authentication

What Is Two-Factor Authentication?

- Two-factor authentication (2FA), also known as multi-factor authentication or two-step verification, is another level of security to keep your accounts and important information safe.
- It uses a combination of 'something you know' (password), 'something you have' (cell phone or bank card), or 'something you are' (fingerprint, biometric methods) to log into a system.
- An example would be combining your knowledge of a password and your possession of your cellphone using text messages or an authentication app to sign in.

Why Is It Important?

- Even if a cybercriminal cracks your password, they would need to gain access to the other methods of authentication to gain access to your account.
- This process makes it difficult for criminals with your password to log in to your account.

It's Annoying, Why Should I Do This?

- ECriminals can obtain access to your environments in a variety of ways, including purchasing credentials from the dark web, phishing attacks, or malware. Cybercriminals know that many people use the same email and password combination across several accounts, allowing them to easily guess credentials for sites using different tools and software. 2FA helps protect your accounts and sensitive information by adding a second step beyond using your password to log in.

Where and How Should I Enable 2FA?

- Most popular sites that handle important or sensitive data have the option to configure 2FA. These include online banking, social media, email, eCommerce, and other accounts. You should consider enabling 2FA on important accounts that have a lot of information about you or have access to things like your bank account or credit card numbers.
- 2FA is also critical in your remote support or remote management tool. If a criminal can log into your remote support portal using stolen credentials, they can gain access to all of your company's or your clients' machines.
- 2FA can be configured in different ways, depending on the site. Popular 2FA methods include email, text message, or authenticator apps like Google Authenticator or Duo. If 2FA is enabled on your account, the site will usually send a one-time password (usually a combination of numbers) to the method you chose. With the email method, the site will send you a code to your email address. You then use that code on the site to finish logging in. The code that is sent to you is different every time, so it's difficult for others to guess. Check with the companies you have accounts with to see if they offer 2FA and how to set it up.