A Better Way with MFA!

Multifactor authentication (MFA) makes it difficult for attackers to access your online accounts, even if they know your password. Taking the extra step beyond just a password can protect your business, online purchases, bank accounts, and even your identity from potential attackers. According to Microsoft, implementing MFA can make you 99% less likely to get "hacked."

Multifactor Authentication: *Multifactor authentication is sometimes called two-factor authentication, two-step verification, two-step authentication, 2-step verification. It is often abbreviated as "2FA" or "MFA." MFA adds another layer of security to protect accounts beyond a password.*

Where do I need to implement MFA? It is recommended that MFA be implemented for **every account that permits it**, especially any account associated with work, school, email, banking, online shopping, and social media. While it might seem like a hassle, once you have MFA set up, it usually adds just a second or two to the log-in process, and the peace of mind MFA provides is priceless.

To enable MFA, start by looking at the Account Settings, Settings & Privacy, or something similarly named on your most-used accounts. If you don't see a prompt for MFA on one of these accounts, send a note to each company asking them to enable the feature.

Methods of multifactor authentication

- Inputting an extra PIN (personal identification number) as well as your password.
- A code sent to your email or texted to your device that you must enter within a short span of time *(not the best method, but better than not having MFA at all).*
- Biometric identifiers like facial recognition or a fingerprint scan.
- A standalone app (Duo, Google Authenticator, Microsoft Authenticator, Okta Verify, etc.) that requires you to approve each attempt or enter a one-time code to access an account.
- A secure token – a separate piece of physical hardware, like a key fob *(considered the best and most phishing-resistant method)*.

Can MFA be compromised? While MFA is one of the best ways to secure your accounts, there are methods that cybercriminals use to get around (bypass) MFA. Many of these instances often involve an attacker repeatedly seeking MFA approval to access an account multiple times and the owner approving the login, either due to confusion or annoyance.

Therefore, if you are receiving MFA login requests and you aren't trying to log in, **do NOT approve the requests!** Instead, contact the service or platform right away. Change your password for the account ASAP. Also, if you reused that password, change it for any other account that uses it (this is why every password should be unique). However, don't let this risk deter you, though, MFA is still one of the best/easiest ways you can bolster the security of your data!

Help secure our utility, yourself, and the world by implementing MFA today!

For more tips on MFA and other ways to stay safe online, visit Secure Our World.