MULTI-FACTOR AUTHENTICATION

What is it?

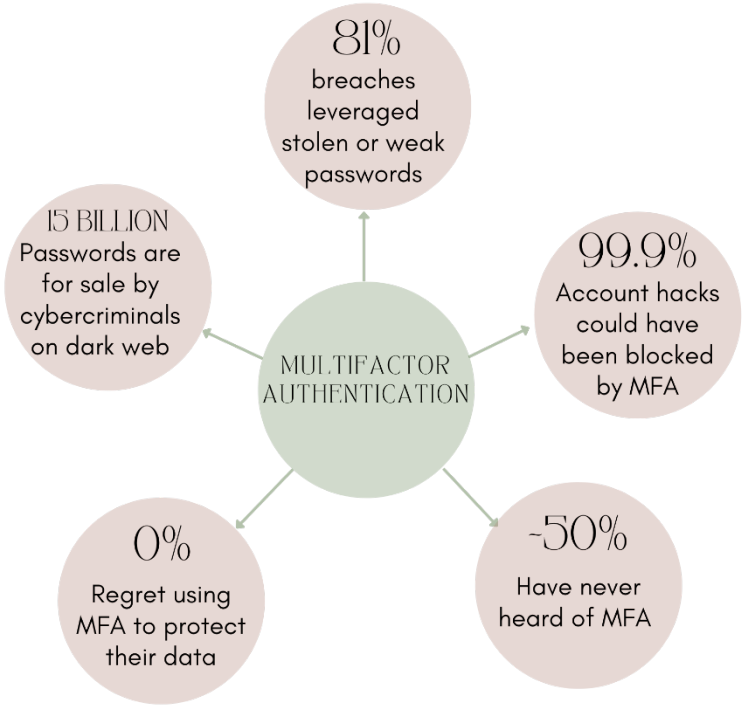
Multi-factor authentication, or MFA, is a security measure that requires anyone logging into an account to navigate a two-step process to prove their identity. It makes it twice as hard for criminals to access an online account. When it's available, always turn it on because it's easy to do and greatly increases your security.

How does it work?

Just like logging into your account, the first step is giving your password or passphrase. The second step is to provide an extra way of proving that you're you, like entering a PIN code or texting/emailing a code to your mobile device, or accessing an authenticator app.

MFA can Include:

- An extra PIN (personal Identification number)
- Security Question Answer "Mother's Maiden Name"
- An additional Code usually texted to you, or email associated with the account.
- A biometric identifier like facial recognition or fingerprint
- A security Token, similar in size to a credit card or key fob that verifies ID in database/system
- A yes or no button, a special image (you picked previously) or unique number generator by an authenticator app



Compromised Credentials

Former internet giant Yahoo inevitably comes to mind when talk of compromised credentials come up. An attack in 2016 resulted in a serious breach of half a billion users' personal information, including their dates of birth and telephone numbers. But it only gets better: Later that year, Yahoo announced that a breach in 2013 had compromised 1 billion accounts (eventually revealed to be 3 billion), along with their passwords, unencrypted security questions and answers. Unsurprisingly, Yahoo's sale price went down about $350 million shortly after.

What youneedtoknow:

Most people still use single-factor authentication to identify themselves (a big no-no in the cybersecurity space). And while stricter password requirements are starting to be enforced (like character length, a

combination of symbols and numbers, and renewal intervals), end users still repeat credentials across accounts, platforms, and applications, failing to update them periodically. This type of approach makes it easier for adversaries to access a user's account, and a number of today's breaches are thanks to these credential harvesting campaigns.

If you have any questions, comments, or concerns feel free to reach out anytime to security@uccs.edu

Where should you use MFA?

1. On accounts with your financial info like banks, or online stores
2. On accounts with personal info, like social media
3. On accounts with info you use for work

TLDR: Use MFA everywhere!

#BeCyberSmart #CybersecurityAwarenessMonth #security@uccs.edu