CYBERSECURITY 101 FOR YOUR EMPLOYEES

ENABLE MULTI-FACTOR AUTHENTICATION

October is Cybersecurity Awareness month and the theme is “It's easy to stay safe online.” The month is dedicated to personal cybersecurity that we can all benefit from, especially employees who are often the first targets.

Employers should communicate effective cybersecurity hygiene beyond traditional security awareness training programs and each topic this month speaks well to that.

Week 1 is about Multifactor Authentication.

WHAT IS MULTIFACTOR AUTHENTICATION?

Multifactor authentication is a form of account security that leverages at least two types of authentication. If you’ve ever gotten a verification code on your phone or email, then you’ve used MFA.

According to Google research, MFA can prevent up to 100% of automated attacks.

TYPES OF MFA

MFA comes in multiple forms. Here are a few examples.

Something you know

This is something you know or set that verifies your account. Here are some examples.

- Passwords
- Security questions
- Personal details (mother’s maiden name, social security number, etc)
- Pins and patterns

Something you have

Something you have can authenticate your account as you should be the only one with access to it.

- Cell phone
- Email (to send verification codes to)
- Security key
- Key card (for physical access)

Something you are

This often refers to biometric authentication, which is as personal as it can get!

- Face ID
- Touch ID
- Fingerprints
- Iris scan

HOW TO COMMUNICATE TO EMPLOYEES

It’s important to communicate and encourage the use of MFA to help protect your employees and your organization as well. Remind them that they use this already on their cell phones to minimize user friction.

You may also want to enforce this for your most critical and sensitive accounts to mitigate the risk of an attack.

To learn other ways to secure your organization, visit **solcyber.com**

SolCyber

solcyber.com