CYBERSECURITY 101 FOR YOUR EMPLOYEES

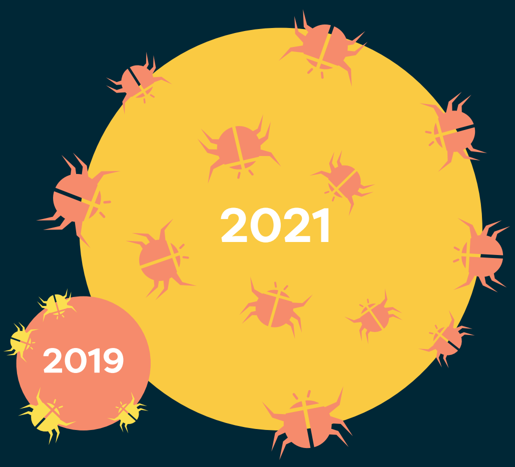
USE STRONG PASSWORDS

October is Cybersecurity Awareness month and the theme is “See Yourself In Cyber.” 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 2 is about having strong passwords.

WHY PASSWORDS STILL MATTER *(AND WHY THEY’RE AT RISK)*



Account takeovers (ATOs) have increased by **300% between 2019 and 2021** and poor password hygiene is often the culprit. Data breaches have exposed the most common passwords and password and email combinations that malicious actors can use to take over other accounts.

If employees are re-using passwords across their personal and business accounts, they can put themselves and your organization at risk.

HOW TO CREATE STRONG PASSWORDS

Here are a few key tips for strong password hygiene.

Never reuse passwords:
Every account should have a unique password to minimize ATOs.

Long and complex are best:
Long passwords are most effective. Use numbers, special characters, and vary your upper and lower case to add variety.

cOmP1eX{Pa$$w04dS!

Passphrases work too!:
Password phrases, as long as they’re not too common, are an easy way to create long and complex passwords.

KeepThemGuessing!

Password managers are useful:
Password managers help users create, store, and access complex passwords, making strong password hygiene much easier.

HOW TO COMMUNICATE TO EMPLOYEES

Make sure that you’ve communicated the above principles to your employees and check with the appropriate department-head to see if you can give your employees a password manager for their business accounts. Many password managers offer business or enterprise accounts for multiple employees, which can save on costs.

You can also refer employees to helpful resources like haveibeenpwned.com which shows you what accounts and passwords have leaked in past data breaches.

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

SolCyber

solcyber.com