Phishing: Psssst! What's the Password?

Passwords are an ever-present part of the digital age. How many times have you logged into a website and forgotten your password? Unsurprisingly, common passwords continue to be "1234567" and unfortunately, security gives way to convenience. This is why there is greater need for continuous advice and education for strong and complex passwords to keep us safe and secure!

Passwords are the keys to unlocking our online profiles that are hosted across a variety of websites. With each of our profiles requiring a separate password, it is not uncommon for people to need many passwords, but for them to be effective it needs to be an uncommon word or password.

To ensure that your passwords are effectively protecting your information, it is important to check in on your password hygiene. Password hygiene refers to the degree to which a user's passwords are selected and managed. It is the practice of ensuring that your passwords are unique, difficult to guess, and have multiple layers of protection. Leaving your password hygiene unchecked can result in security breaches, stolen information, and identity theft.

Use our password safety checklist below to test your password hygiene!

Passphrases	• Try using a passphrase. Passphrases are longer and more difficult for someone to guess. • Use upper and lower-case letters, special characters, and numbers. • Avoid common words or slang terms.	
Multi-Factor Authentication (MFA)	• MFA requires two or more pieces of identification to log in to an account • Some examples of MFA are a password or pin, a token or authenticator app, or a fingerprint/face scan.	
Use Unique Passwords	• Use a different password for every account. • Do not reuse previous passwords.	

Use a Password Manager	• Helps you generate strong passwords and store them in one encrypted place.	

Cyber Defender, Did You Know? According to a study by Microsoft, using MFA can block over 99.9% of account compromising attacks. MFA is an essential element of cyber security that adds an extra layer of protection. If your password is ever compromised, MFA can prevent an attacker from getting into your account.

While convenient and easy to remember passwords might be nice in the short term when logging into your account, they can result in breaches to your security and your organization's security. Always remember when thinking about simplicity or security, security is the way to go!