Phishing Scam Awareness
Securing your Passwords

Summary

Protecting your passwords is vital to safeguarding your personal and professional information from cyber threats. Weak or reused passwords are a major security risk, making it easier for attackers to gain unauthorized access to your accounts. This guide provides essential best practices for creating, managing, and securing your passwords to help prevent identity theft, data breaches, and phishing attacks.

1. Use Strong and Uniques Passwords

- Ensure your passwords are at least **12-16 characters long**.
- Combine **uppercase and lowercase letters, numbers, and special characters**.
- Avoid using **personal information** (e.g., name, birthdate, or common words).
- **Example of a strong password:** `Yz!8rPq#2vL$9wT`

2. Enable Two-Factor Authentication (2FA)

- **Always enable 2FA** for extra security.
- Use **authentication apps** (e.g., Google Authenticator, Authy) instead of SMS for better protection.
- Consider **hardware security keys** for maximum security.

3. Use a Password Manager

- A **password manager** helps generate and store complex passwords securely.
- Recommended password managers: **Bitwarden, 1Password, LastPass, Dashlane**.
- Never store passwords in plain text (e.g., in notes or documents).

4. Regularly Update Your Passwords

- Change passwords for critical accounts every **3-6 months**.
- Immediately update passwords after a **data breach**.
- Use websites like **Have I Been Pwned (https://haveibeenpwned.com/)** to check for breaches.

5. Be Cautious of Phishing Attacks

- Never enter your password on **suspicious emails or websites**.
- Verify URLs before logging in to sensitive accounts.
- Enable **email security settings** to detect phishing attempts.

6. Securely Store Backup Codes

- If a service provides **backup codes**, store them in a **secure location**.
- Avoid saving them on **cloud storage without encryption**.
- Print and store them in a **locked safe** if necessary.

7. Avoid Password Reuse

- **Never reuse passwords** across multiple accounts.
- If one password is compromised, attackers can access multiple accounts.
- A password manager helps manage unique passwords efficiently.

8. Log Out of Public Devices

- **Always log out** after using public or shared computers.
- Avoid accessing sensitive accounts on **public Wi-Fi** without a VPN.
- Enable automatic session timeouts where possible.

9. Recognize and Avoid Common Weak Passwords

- Avoid commonly used passwords like: `123456`, `password`, `qwerty`, `letmein`, `admin`.
- Use **passphrases** instead of single words (e.g., `BlueTiger$27RunsFast!`).

10. Monitor Your Accounts for Suspicious Activity

- Enable **account activity notifications**.
- Use **security alerts** to detect unusual logins.
- If you suspect unauthorized access, **change your password immediately**.

Stay safe, and attempt the quiz when you think you’re ready.