PONDURANCE

Employee Security Awareness Checklist

Human attackers require human defenders to stop them in their tracks. This checklist can help you cover your bases while in the office or working from home.

Password Protection

- [ ] Choose passwords that are eight characters long and contain a combination of uppercase and lowercase letters, numbers, punctuation marks, and other special characters
- [ ] Avoid using basic combinations (i.e., password1, 123password!@#)
- [ ] Avoid using the same password for multiple sites
- [ ] Recommend using a password manager to store and manage passwords for multiple accounts and logins

Multi-Factor Authentication (MFA)

MFA is an authentication method that requires the user to provide two or more verification factors to access an account.

- [ ] Use MFA when available and prioritize the use of an application (Google Authenticator or Microsoft Authenticator) before SMS (text message)
- [ ] Email
- [ ] Mobile device
- [ ] Work login

Email Phishing

Email is a common gateway for attackers to launch much larger attacks like ransomware, phishing, access passwords, and more.

- [ ] **Company logo, colors, and overall branding** - Is the correct logo on the email? Do the brand colors match?
- [ ] **Company contact information, address, phone number, etc.** - Review the email and inspect it for company contact information
- [ ] **Spelling, grammar, and punctuation -** Companies typically do not have typos in their emails
- [ ] Avoid using your work email address for personal use, as this could lead to security issues
- [ ] Check sender address
- [ ] Urgency or threats
- [ ] Links - Before clicking a link, **REVIEW IT!**
- [ ] Do not click on unsolicited emails
- [ ] Cross-check any information that is suspicious by doing a Google lookup

PONDURANCE

Employee Security Awareness Checklist

Operating System Updates

Developers are constantly looking for bugs and vulnerabilities throughout their software. You should update whenever prompted.

- [ ] Update your operating system whenever prompted
- [ ] Set automatic updates whenever possible

Browsers

- [ ] Always keep your browser up to date
- [ ] Avoid sites that use HTTP over HTTPS when inputting information such as login details, personal information, and credit card information or when filling out an online form
- [ ] Do not install untrusted and unverified browser extensions or plug-ins

Working From Home

- [ ] Secure your Wi-Fi connection with a strong password
- [ ] Avoid using public Wi-Fi when working outside of the office or your house
- [ ] If permitted, use a virtual private network (VPN) to add an additional layer of security when working remotely

Devices

- [ ] Use antivirus software to stop and quarantine attackers
- [ ] Make sure all devices are secure with MFA protection
- [ ] Do not use work devices for personal use
- [ ] Password or passcode protect your devices

Who Should You Contact?

- [ ] Ask who the IT contact is
- [ ] Ask for the email address where you should forward phishing emails