7 Common Behaviors That Make Your Company an Easy Target

01 Reusing Passwords

Despite continual warnings, many employees still use the same password for multiple accounts. The obvious problem here is that if one account is compromised, then so are all the others – and the data they store. Consider recommending a password managing service to help employees choose and manage strong passwords.

02 Using Simple Passwords

That password people think is safe? Hackers can use sophisticated computer programs that run through millions of possibilities in a matter of minutes. For better protection, your company should require passwords that have at least 8 characters and contain numbers, symbols, upper and lowercase letters. The longer the better!

03 Turning Off Automatic Updates

Most companies that sell operating systems and applications (e.g., Windows) regularly provide updates to protect their users' system. If your employee machines are not set to update operating system software automatically, they should be.

04 Opening Links from Suspicious Emails

Globally, 75% of organizations experienced some sort of phishing attack in 2020. With the prevalence of phishing scams at an all-time high, employees need to be on alert for suspicious messages. They should be encouraged to stay away from emails that ask them to provide personal information, click an unknown link, open an attachment. Emails that seem impersonal or out of character should also be avoided.

05 Unprotected Wi-Fi Networks

Most Wi-Fi routers come with a default password. Employees working from home should be encouraged to change these default passwords to something more secure. They also should update the password regularly using a combination of characters to reduce the likelihood of being hacked.

06 Downloading Programs and PDFs from Unknown Sources

If employees are able to download files, they should always make sure they are from official/reliable websites. Either lock down permissions and prevent employees from downloading, or ask them to check with IT if there are any questions about a source's reliability.

07 Not Using Anti-Virus Software

Anti-virus software is designed to keep computers safe and free from web-based threats. Every employee should have anti-virus software installed and be unable to adjust those settings.

Do you know your company's security vulnerabilities?

Our IT Risk Assessment is a quick, low-cost way to check your cybersecurity posture and thwart potential breaches. For $1,000, our report analyzes:

- √ Hardware
- √ Software
- √ Configuration
- √ Accessibility

Protect your organization, your clients, and your reputation by keeping your data secure.

Our Cybersecurity Services

- √ IT risk assessment
- √ Vulnerability scanning and penetration testing
- √ Data breach response
- √ Incident response and disaster recovery plan creation/updates
- √ Virtual CISO
- √ Policy and procedure creation/updates

TALK TO A CONSULTANT

CLARK SCHAEFER HACKETT
BUSINESS ADVISORS