CYBERSECURITY ALERT

PROTECTING THOSE WE SERVE

5 CYBERSECURITY PITFALLS THAT COULD AFFECT YOUR ORGANIZATION

1. One Universal Password

Every year, many reports are produced listing the worst passwords recorded for the year. To no one's surprise, "123456" and "password" are always the front runners. Having one single password for every account you have can be an open invitation to those hackers who are looking to crash a party.

SOLUTION: Password managers should generate random and secure passwords. The best part is that you only need to remember one password to retrieve them all. It's that simple.

2. Trusting and Clicking Links and Attachments

Attackers these days are craftier and more cunning than ever before. Their messages look legitimate because they study their victims in order to appear safe and trustworthy. Just one click and the next thing you know, they have unleashed a virus and gained access to your systems. Sometimes they even appear to come from sources you know and trust. They are that good.

SOLUTION: Educate yourself and your employees. Double-check URLs by hovering over the link so you can read where the link is actually taking you. If it seems off, sketchy or completely incorrect, don't click. Also, avoid opening any attachments you weren't expecting.

3. Update Procrastination

Have you ever been stuck in the "remind me later" update rut? The more you procrastinate between system updates and patches, the more vulnerable you become. Nearly half of the common vulnerabilities and exposures exploited last year were taken advantage of within two weeks of an update release.

SOLUTION: Set update settings to automatic. Take the thinking right out of it.

4. Using Public Wi-Fi

Everyone has been tempted to latch onto free Wi-Fi. But whether you're a remote user at Starbucks or waiting in the airport terminal, it's risky. The words "free" and "public" don't always guarantee that it's secure.

SOLUTION: Consider mandating use of a Virtual Private Network (VPN). Your users' browsing sessions will be much more secure and traffic will be encrypted.

5. You're Responsible For You

Although we'd like to think we can blame everything on the Information Technology (IT) department—and perhaps it's easier to do that—taking precautions are not solely their responsibility. The majority of cyberattacks stem from an end user clicking on something that they shouldn't have.

SOLUTION: Educate, train, and reinforce protocols. Learning end user security best practices will help transform your team into a stronghold instead of an open back door.