TOP 9 WAYS TODAY'S CYBERCRIMINALS ARE UNDERMINING YOUR SECURITY

Right now, extremely dangerous and well-funded cybercrime rings are using sophisticated software systems to hack into thousands of businesses like yours to steal credit cards, client information, and swindle money directly out of your bank account.

These are the 9 ways they are getting into your systems.

1. They Take Advantage of Poorly Trained Employees. It's extremely common for an employee to infect an entire network by opening and clicking infected e-mails or online scams while in the workplace.

2. They Exploit Device Usage Outside Of Company Business. If your employees are using their own personal devices to access company e-mail and data, it can be a gateway for a hacker to enter your network as much as if they were using your devices.

3. They Take Advantage of Weak Password Policies. Passwords should be at least 8 characters and contain lowercase and upper-case letters, symbols and at least one number. On a cell phone, requiring a passcode to be entered is a plus!

4. They Attack Networks that are Not Properly Patched with the Latest Security Updates. New vulnerabilities are frequently found in common software programs you are using, such as Microsoft Office; therefore it's critical you patch and update your systems frequently.

5. They Attack Networks With No Backups Or Simple Single Location Backups. Simply having a solid, reliable backup can foil some of the most aggressive (and new) ransomware attacks.

6. They Exploit Networks With Employee Installed Software. One of the fastest ways cybercriminals access networks is by duping un-suspecting users to willfully download malicious software by embedding it within downloadable files, games or other "innocent"-looking apps.

7. They Attack Inadequate Firewalls. All firewalls need monitoring and maintenance, just like all devices on your network. This too should be done on a regular basis.

8. They Attack Your Devices When You're Off The Office Network. It's not uncommon for hackers to set up fake clones of public WiFi access points to try and get you to connect to THEIR WiFi over the legitimate, safe public one being made available to you.

9. They Use Social Engineering And Pretend To Be You. This is a basic 21st-century tactic. Hackers pretend to be you to reset your passwords.

CONTACT US

Interested in understanding how to prevent these threats and more?

We can help. Reach out to continue the conversation.

623-227-1997 **hello@onestepsecureit.com**

Take the 1st Step to Protecting Your Business

Find out if your companies credentials are on the dark web with our **FREE** Dark Web ID Scan.

RUN YOUR SCAN