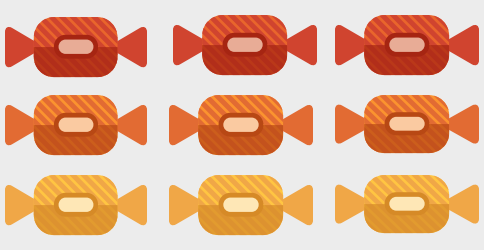
Scary Cyber Security Mistakes

Your employees are an integral part of your organization and are a huge part of what makes it great. However, they can also be the cause of risk in your business. Establishing a culture of security is the best defense you can have against external threats to your company.

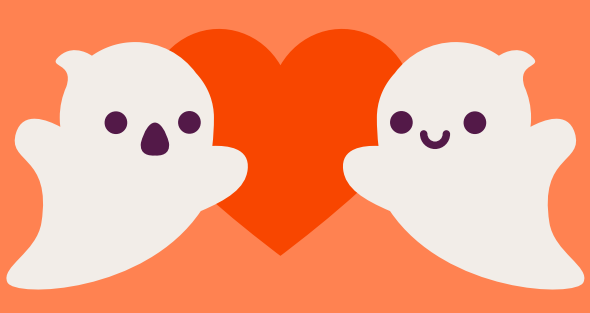
Here are some of the top mistakes employees make - and how to stop them.

1 Weak Passwords



"Password" is not an okay password. Instead, try using a passphrase and incorporate numbers or symbols. Never share your passwords and change them frequently to increase security.

2 Social Sharing



Social media is great for connecting with friends. However, hackers are using this information to inform phishing attacks on your employees. Be mindful of what you share and what you open.

3 Trusting Public Wi-Fi

The beauty of Wi-Fi is that you can now work from anywhere. However, hackers are also everywhere and can use insecure public Wi-Fi to hack into your network.

Always connect to VPN when on public Wi-Fi and make sure to encrypt all information that you share.

4 Thinking You're Immune to Breaches

Never for a second think you are immune to having your organization breached. Over confidence certainly killed the cat.

Don't overlook the "small" things. Adversaries are always looking for new ways to enter your organization and your lapse in judgment could cost you.

5 Skipping the Update

Updates aren't fun - but they are necessary. More than just adding new features to your software, updates add valuable bug fixes to your security.

Make sure you keep all of your software, applications and devices up to date.

6 Not Knowing What You Need

You may think you need a penetration test, but what you're actually describing could be a vulnerability management solution.

Research what it is you need and how to get there - or source fellow professionals

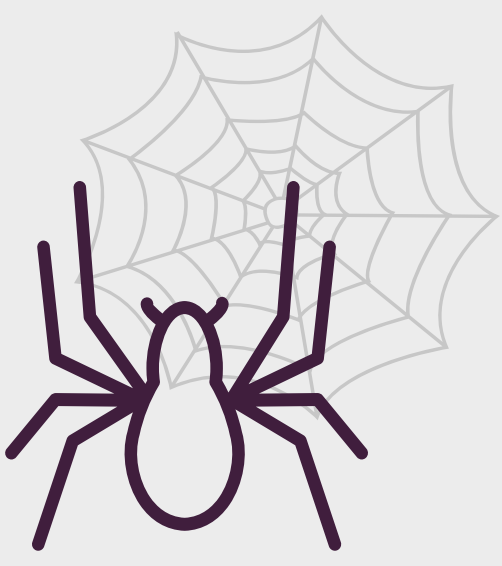
7 Depending Only on The IT Team

Incident management requires teamwork - not just among the IT and Operations teams - it takes everyone throughout the organization to identify and alert when any anomalies are detected on your network.

8 Not Signing Out of Accounts

This includes both user accounts and WiFi accounts. Automatically joining networks and storing your logins on your device is not safe and attackers may use this as a gateway across your network.

9 Bring Your Own Device(s)



Everyone has a cellphone and most companies have addressed the risks of personal phones and their use on the network. However, with the added adoption of tablets and wearables the need for a BYOD policy is more important than ever.

The world of cyber security is changing. Users are now the target. Hackers aren't knocking down actual doors and walls to get into your system. Instead, they are sneaking in through user credentials and open portals. To build a culture of security in your organization, your employees need to know how hackers are targeting them and what they can do to keep themselves and the organization safe. These tips are a great start - but for more information on how to build up your team's defenses against attacks, talk to one of our security consultants, today!

https://www.coresecurity.com/contact

CORE SECURITY