5 Things Your Employees Are Doing That Will Get You Hacked

Roughly half of all small businesses in the U.S. are at serious risk of being hacked.

A CNBC survey of 2,000 small-business owners found that they aren't spending enough on cybersecurity – and as a result 14 million of them (out of 28 million total in the U.S.) have been breached.

Related: Making Your Data Unreadable to Whoever Steals It Might Be the Only Way to Keep It Safe

The good news is that companies can do something to dramatically reduce their odds of getting hacked, namely training their employees on security. That's because most cyber intrusions are a direct result of employee misbehavior – which is usually unintentional.

Here are the five most common things your employees are doing that will get you hacked:

1. Being lazy

There's a prevailing notion that users don't have to worry about security because it's not their job. They believe the odds of a cyber intrusion are so small that they don't have to worry about it. Or, the IT staff takes care of that stuff.

That attitude makes your employees vulnerable, and it's exactly why hackers target small businesses. The IT people at small businesses are usually not security experts, and they're often unprepared to deal with ransomware – the most popular type of cyber attack.

Related: Protect Your Business! The 7 Cybersecurity Tools You Need as an Entrepreneur.

2. Unprotected email

Your employees likely have 2-step verification turned off in their email app. This means hackers with stolen login IDs and passwords belonging to your company can access your employees' email accounts. Once they get in, they can easily find more log-in credentials, personally identifiable information (PII), credit card data, proprietary data, private conversations and much more.

Hacks on email accounts are one of the fastest growing cyber crimes. Hundreds of millions, and possibly billions, of stolen emails are for sale on the dark web as a result of major hacks on Yahoo, Equifax, Uber and many others. The remedy is turn 2-step verification on. It's a simple, editable setting in all of the popular email platforms such as Gmail. If it's turned on, then each time users log into their email account they'll have to type in a special code (after they type in their email address and password). The code is texted to their phone by the email app. When cyber thieves log in with a username and password, they have no way of knowing the special code. Two-step verification turns your employees' phones into physical keys to their email accounts.

Related: Watch Out for These Cryptocurrency Scams

3. Clicking in fake emails

According to cybersecurity company PhishMe, 91 percent of cyber attacks begin with a spear phishing email, which induces your employees to click and share information – such as their log-in ID and password – with hackers. The phishing emails are designed to look authentic, seemingly coming from credible sources such as a customer support representative from

Microsoft, Google or another major tech vendor (a ploy referred to as “Tech Support Scams”). Or, they may actually appear to be coming from you (their boss) with a fake email header. Phishing email scams often inject computers and mobile devices with ransomware.

Related: Here Are the 25 Worst Passwords of 2017

4. Lousy passwords

Shockingly, the most popular password in use today is 123456, according to SplashData. To make matters worse, people reuse these easy-to-crack passwords on multiple devices and apps. Some users go so far as sharing their passwords with coworkers, friends and family members. Using 123456 as a master password and never being hacked is a badge of honor for braggarts (until of course, they get hacked).

This is what some of your employees are probably doing right now. Walk around your office and look on everyone’s desk – and you’re bound to see log-in IDs and passwords handwritten for anyone who wants to have a little hacking fun.

Walk up quietly behind someone sitting at a computer and you might get a glimpse of his or her password.

Chances are, most of your employees are well-intentioned – but clueless when it comes to cyber protection.

Related: The Dos and Don’ts of Cyber Security Measures to Help You Protect Your Business and Assets

5. No backup

If just one of your employees isn’t backing up data he or she is supposed to be, then you’ve got a big problem on your hands. Most likely, there’s more than one person in your company who isn’t backing up, or hasn’t in a while.

Ransomware locks users out of their computers and smartphones, and denies access to their files, until money is paid to the ransomware author. Worse, all of a user's data can be permanently destroyed by the ransomware. And even when a ransom is paid, there's no guarantee that a user will regain access to the files.

"Regularly back up data and verify the integrity of those backups. Backups are critical in ransomware incidents; if you are infected, backups may be the best way to recover your critical data," states the FBI in a 2016 public service announcement.

Back to the good news. There's a slew of great online security awareness training programs, and they're relatively inexpensive. The programs are designed to make learning about security entertaining, while changing bad computing habits.

An action item for today – before enrolling your employees into training – is to give all of your employees the list of five things they are doing to get your company hacked, and tell them to stop. If not, then you're putting your profits at risk.

https://www.entrepreneur.com/article/307939