**Suggested Title: How Will Your Employees Get You Hacked?**



Breaches are becoming increasingly common as cybercriminals continue to advance their skills and tactics to trick their victims into falling for their scams. While cybercriminals are remaining diligent in their efforts to carry out their attacks, small business owners continue to underspend on cybersecurity. An article on [Entrepreneur](https://www.entrepreneur.com/article/307939?utm_content=buffera4e8f&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer) looks at 5 things your employees are doing that put your business at risk.

The 2016 State of SMB Cybersecurity Report revealed that half (14 million) of the 28 million small businesses in the U.S. had been hacked by cybercriminals, but why? According to a CNBC survey of 2,000 small-business owners, small businesses are not spending enough on cybersecurity.

With human-error being the most common reason for a cyber intrusion, employee security training is crucial to ensuring employees know how to spot a hacking attempt.

Since it is possible to reduce your odds of getting hacked through employee security training, it’s important to understand what employees are doing that will get you hacked. Below are the top 5 most common mistakes:

**What are employees doing that will get you hacked?**

1. **Being lazy**

Employees often feel that it’s not their job to worry about security, or that IT is responsible for “that kind of stuff”. Small businesses often lack IT resources, especially equipped to handle cybersecurity threats like ransomware. Employees should be aware that they are a target for cybercriminals and that it’s their job to help stop them from carrying out a successful attack.

1. **Unprotected email**

Email hacking is one of the fastest growing cybercrimes, with millions and possibly billions of stolen emails for sale on the dark web. Employees often have 2-step verification turned off in their email app, allowing hackers easy access to those email accounts if they have the stolen credentials. Once a hacker is in that email account they have free range to access any data that may be stored in the account, such a personally identifiable information (PII), credit card data and additional log-in credentials. 2-step verification is simple to enable in most popular email platforms. After 2-step verification is enabled, a code will be texted to the employees’ phone making it so that a cybercriminal would have no way to access that email account.

1. **Clicking on fake emails**

According to the cybersecurity company PhishMe, 91% of cyberattacks begin with a spear phishing email. In these phishing emails, hackers design the email to look authenticate so the employee thinks it is coming from the real source it’s claiming to be. These phishing emails may appear to come from credible company’s customer support departments, such as Microsoft or Google or could even appear to come from you (their boss). In many cases, once an employee falls for a phishing scam, their computers/mobile devices become infected with ransomware.

1. **Lousy passwords**

SplashData reported that the most common password in use today is 123456. Not only is this a very weak password to begin with, but people are often reusing their easy to crack password across multiple sites and accounts, as well as sharing them with co-workers. Other common employee mistakes when it comes to passwords include physical protections, such as writing them on a sticky note and leaving that on their computer or under their keyboard. Employees may also be typing their password without paying attention to wandering eyes that may be watching them.

1. **No backup**

There’s a good possibility that at least one employee in your company isn’t backing up the data he or she is supposed to be, which is a major problem. Not only is there a risk of files being lost due to technical issues, there is also danger in losing those files to a cybercriminal. During a ransomware attack, a cybercriminal locks the user out of their account and denies them access to their files unless a ransom is paid. Even after the ransom is paid, there is no guarantee that the files will be returned to the user, making backup files crucial.

Although these employee mistakes can lead to major issues for your business, it’s not too late to protect yourself and your organization! Training your employees on security is vital and a great way to ensure they know what to lookout for to help prevent a hacker from carrying out a successful attack on your business. In addition to security awareness training, it is beneficial to share these 5 common mistakes with your employees to bring them to their attention and help them understand the risks they may be presenting.