BIZCOMMUNITY

Employees are the weak link in cyber security

A report from Kaspersky Lab shows that 90% of corporate data breaches in the cloud happen due to hacker attacks that target employees. With many of them forced to work remotely during the lockdown, companies are now more vulnerable than ever.

Source: www.pexels.com

Daniel Markuson, the digital privacy expert at NordVPN Teams, agrees that employee negligence is a great threat to business security. However, he points out that this particular risk is easy to control. There are many digital tools that can help protect organisations from data breaches. These tools and security systems don't require big investments as cybersecurity starts with the right mindset of employees. That can be achieved through mandatory training.

According to Markuson, both small businesses and large organisations must focus on cybersecurity. All companies dealing with customer data or confidential information are vulnerable to cyber-attacks. The difference is that big names usually have more data than hackers may want to steal. Meanwhile, small ones tend to lack security resources, thus making easier targets.

To protect your business from hacker attacks, you need to consider these common mistakes your employees might be making every day:

- ## Weak passwords

  Passwords play the most important role in protecting your business accounts and customers' data. But people struggle to create unique passwords and keep forgetting them. That's why they often use the same ones for different accounts, and your employees might be no exception.

  "Weak and reused passwords are easy to hack. The best solution is to help your staff build a habit of using password managers," says Markuson. Passwords must be changed from time to time and shouldn't be shared among coworkers.

- ## Sharing unencrypted files

Companies are at serious risk of data loss when their employees handle important documents without security in mind. The safest way to store and share files is by encrypting them. As an example, easy-to-use encryption software adds an extra layer of security to data on a computer or in the cloud. In case of a breach, hackers will not be able to access your company's information - they will only see undecipherable code.

- ## Connecting to unsecured networks

A vast majority of organisations use Wi-Fi networks. Although Wi-Fi gives staff greater mobility within the office, it also makes your business data more vulnerable to hacks. The best way to keep online traffic private is by using a virtual private network (VPN).

A VPN creates a secure encrypted tunnel that protects your connection from anyone trying to breach the system. It is also a must for secure remote connections. It allows employees to safely access their work accounts while travelling, working from home, or using public Wi-Fi.

- ## Falling for phishing scams

Phishing is one of the main reasons why your members of staff need cybersecurity training. Hackers may try to get sensitive information by faking emails from someone like your company's CEO or Microsoft representatives. And they use very sophisticated methods for that.

"Just one reckless click on a phishing link or one download of an infected attachment can compromise your entire system," explains Markuson. Make sure your team is well educated on how to avoid clicking unsafe links or falling for phishing scams.

- ## Ignoring software updates

An average computer user tends to ignore the little pop-up windows that informs about new software updates.

Markuson claims that keeping all software up to date is crucial for your company's cybersecurity. That's because updates often repair security flaws, fix or remove various bugs, add new features, and improve the existing ones. Having the latest software version means you are using the most secure version, too.

- ## Posting work-related content online

Markuson says that employees posting online carelessly can leak sensitive business information. Consider Instagram pictures with workspace in the background. Or Facebook status updates on upcoming business trips or closing important deals. Both reveal too much information that can be used to breach your organisation's security.

It is also a very common mistake during the current situation when people share images online of how their workspaces at home look like. A picture of a desktop with visible icons or open documents can reveal too much than intended.

“Businesses need to create social media and data privacy guidelines to prevent employees from sharing confidential information,” the expert suggests.

- ## Connecting unsafe media storage devices to the company’s computers

Your employee might insert a flash drive into their computer without knowing it is infected. According to Markuson, these media storage devices might contain viruses and other malicious content. These could transfer to your network and compromise the company’s entire system.