Cybersecurity training is essential for startup success

When you have a new startup that’s gaining steam, it’s essential that you do everything in your power to avoid potential issues that can often sink a new business, including cyberattacks. The key to preventing malware or financial attacks is to train your employees to be proactive and vigilant to prevent a breach.

Temps de lecture : minute

23 August 2024

This guide will explain why cybersecurity is so critical, provide the essential lessons for your training sessions, and show how having a happy workforce can further prevent your startup from disaster.

Cybersecurity training is essential for a healthy startup

With so much going on during the initial stages of a business, it’s easy to fall into the trap of putting cybersecurity on the back burner. However, failure to act can quickly make you a target. Cybercriminals know that *small business owners either don’t think about security* or don’t have the resources, so they know it’s easy money. Plus, it doesn’t matter if you're a startup or a Fortune 500 company. If you have financial information, customer data, or any other confidential information, hackers will want to get to it.

Sadly, cybercrime is a serious issue in the UK. Over *1.5 million businesses were affected* by cybercrime during 2023 alone. Many of them were small-to-medium enterprises. In fact, small businesses experienced a 42%

increase when it came to data breaches. All in all, these incidents cost the UK economy over £30.5B, so these are serious issues that you must actively prevent in your business.

Though comprehensively training new employees may initially cost money, it will likely be much less than the potential penalties of doing nothing. Continuous cybersecurity training for your staff is essential because *cyber threats are always evolving*, so a one-time class won't be enough to ensure your protection. Regular training sessions are the best way to feel confident that you're doing everything you can to safeguard your business.

What to teach during cybersecurity training

You'll want to find a well-informed trainer or a good webinar to show your employees all of the potential risks and scams and how they can help protect your business.

Start by teaching your staff the *four key cybersecurity measures* that can protect many businesses. They include:

- Creating complex passwords for all devices and programs.
- Teaching how to encrypt all incoming and outgoing data.
- Ensuring that all software is updated or has current patches to protect against ongoing threats.
- Showing staff the importance of working with a trusted supply chain and vendors who also know the value of proper cybersecurity.

It's also vital to teach your teams how to *protect your small business* from the common attacks that cyber criminals use to hack your systems. For instance, a frequent threat is malware, which is software that can harm your internal systems. You need to stop unauthorised programs before they can gain access, which employees can do by running antivirus scans,

turning on the firewall, and avoiding unauthorised USB drives that may contain viruses.

Threats can also take the form of phishing attacks, where a hacker sends a malicious email that often looks like it's from a figure of authority. However, if the employee clicks the link or attachment included, malware can then be installed into the system and cause various issues. Your training classes should teach employees how to know when an email is legitimate and that they should never click on a link or attachment unless they know it's real.

Ongoing training can make for happy employees

Security training will keep your employees engaged, and that will help with your overall strategy. Many workers want to feel like they're a valued member of the team. When employees are shown how to detect potential scams and are provided a way to report concerns to management, they'll likely do so because they want to see your organisation succeed.

In addition to proper cybersecurity training, you should also take other steps to ensure that your employees are happy because positive *team morale is another step in your defense against cybercrime*. Numerous negative possibilities can occur when your employees are unhappy. They may be less engaged in their work, so much so that they may let phishing emails slip through or spend time on websites with malicious links. Employees genuinely unhappy at work may also be more susceptible to bribery.

You can tie employee satisfaction and cybersecurity together by publicly recognising employees who report vulnerabilities and catch scams. Most workers are also happier when there's less micromanagement and more autonomy, so they take ownership of their responsibility to protect the

company. Direct supervisors also play a big part. If you lead by example and celebrate employees when they do what’s right for the company, they will be more inclined to continue to do so in the future.

Cybersecurity training is essential for startup success during the early stages and as the company continues to grow. Show your employees the importance of catching scams and breaches, and you’ll have a team to help your enterprise grow to the next level.

Article by Indiana Lee