Keep Your Data Safe from Cyberattacks

How to shield your business from sophisticated online criminals

Cyberattacks cost businesses billions of dollars a year, and it is essential to take your company's risk seriously. Taking these steps can help protect against viruses, ransomware, and other sophisticated methods of stealing your company's data and taking over its systems.

Secure networks, hardware, and accounts

Securing all your company's networks, accounts and hardware is one of the most effective ways to resist cyberattacks and protect your data. All company computers and other hardware should be shielded by individual user accounts with strong, unique passwords. As necessary, consider requiring multifactor authentication, which requires a separate one-time security code in addition to a regular password. Web and email filters can further help protect against malware and viruses.

You should also make sure that your internet connection is protected by a firewall and your wireless networks are hidden and encrypted. If any of your employees work from home, their network access points ought to be firewalled as well. In an article for the National Institute of Standards and Technology, cybersecurity expert Traci Spencer also recommends keeping business wireless networks separate from those you offer for guests or customers.

Keep software updated

Guard against online incursions by staying current on all the computer software your business uses. Keep up with operating system patches, web browser updates, and any other fixes that you are prompted to make. Doing this regularly will help keep attackers from harming your business through vulnerabilities that they have discovered in outdated software. For your company's protection, your computers should also be scanned regularly with up-to-date antivirus software.

Control employee access

Restricting who can see and use data will help reduce your company's vulnerability to security lapses and protect against cyberattacks. For sensitive information and systems, Spencer recommends limiting access to employees whose jobs require it. The Small Business Administration suggests limiting administrative access to your company's systems as well.

Keep data encrypted

It is vital to keep your company's sensitive data encrypted. That way, hackers will not be able to use what they find even if they manage to break into your system. Spencer recommends using full-disk encryption for all computers, smartphones, tablets, and other company devices. You can also use encryption for sensitive emails. Encryption passwords should be kept in a secure location or, for emails, provided separately.

Back up data in a secondary location

Protect against data theft and ransomware attacks by regularly backing up your company's important data in a separate physical or cloud-based location. According to the SBA, data you should consider backing up includes financial records, accounting files, and human resources information.

Protect payments

Any payments made or received by your company should be handled with care. Per the SBA, confirm that any financial institutions or card processors you work with are using the best methods to protect payments. On your end, use separate systems and computers to process payments.

Invest in staff training

Extensive precautions to protect your company's data will not matter if you have not trained your staff properly. Employees should know all the relevant company procedures and rules, including how to create strong passwords, how to identify phishing emails, and how to protect customer information.

Whether your business is large or small, a cyberattack can have crippling consequences. Fortunately, putting these precautions in place can reduce your risk and help you fight back against data theft.