A Small Business Guide to Cybersecurity

As larger companies prioritize and fortify their cybersecurity, small and midsize businesses (SMBs) have become easier targets for cyberattacks.

According to a recent SBA survey, 88% of small business owners felt their business was vulnerable to a cyberattack.[1] In fact, 43% of cyberattacks are aimed at small businesses, but only 14% of small businesses are prepared to defend themselves. Many small business owners may not be able to afford professional IT solutions or have limited time to devote to cybersecurity.[2] But with some helpful guidance, small businesses can take proactive measures to protect their business from online threats.

suddenlink® business

Start by staying informed

Frequently, security incidents can happen because of user error, web browser exploitation, and social engineering. Cyberattacks are constantly evolving, but there are common types of threats business owners should be aware of and train employees to avoid.

Malware (malicious software) is an umbrella term that refers to software intentionally designed to cause damage to a computer, server, client, or computer network. Malware can include viruses and ransomware.

Viruses are harmful programs intended to spread from computer to computer (and other connected devices). Viruses are designed to give cybercriminals access to your system.

Phishing is a type of cyberattack that uses email or a malicious website to infect your machine with malware or collect your sensitive information. Phishing emails appear as though they've been sent from a legitimate organization or known individual and often entice users to click on a link or open an attachment containing malicious code.

Ransomware is a specific type of malware that infects and restricts access to a computer until a ransom is paid. Ransomware is usually delivered through phishing emails.

DDoS or Distributed Denial-of-Service attack is when a cybercriminal floods a system with large amounts of traffic to tie up a server's resources and deny visitors access.

DNS or Domain Name System is a foundational component of the internet, mapping domain names to IP addresses. A cybercriminal can redirect your traffic to a "spoofed" server in a DNS attack and expose them to phishing schemes and other malicious behaviors.

TIP

Seek Automatic DNS/DDoS Protection: A DNS/DDoS security system that is actively detecting any potential threats to your network can stop attacks from happening.

Proactively plan and protect

Today's small businesses must be proactive rather than reactive with their cybersecurity strategies. They must not just rely on antivirus software but implement more advanced measures to protect their network and business. Here are some steps to consider including in your multi-level cybersecurity strategy:

Conduct a cybersecurity risk assessment

A cybersecurity risk assessment can help identify where your business is vulnerable and inform your plan of action. Some quick links you can use include the Federal Communications Commission (FCC) cybersecurity planning tool and the Department of Homeland Security's (DHS) Cyber Resilience Review (CRR) which is a non-technical assessment to evaluate operational resilience and cybersecurity practices.

Get more than antivirus software

Installing antivirus software on all of your company devices (including every mobile device) and ensuring it is up-to-date is crucial. But only a multi-layer strategy that includes DDoS and DNS security provides a more comprehensive protection for your business.

TIP

Know how your business stores and processes data so you can strengthen the weak spots and educate your employees about small business network security best practices.

Educate your employees about security

Hackers aren't the only ones who can compromise your data. Your employees, if they're not careful, can put the company's data in jeopardy. Whether someone leaves their work computer unattended or enters their information into an unsecured site, your company's data is at risk.

Implement a backup and recovery plan

Regularly back up the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. If possible, back up data automatically or at least weekly, and store the copies either offsite or on the cloud.

Create your cybersecurity checklist

Here is a checklist you can refer to when creating a cybersecurity plan for your business:

- ✓ Stay educated and informed on the newest security threats
- ✓ Educate your employees about data flow and how to keep information safe
- ✓ Implement a backup and recovery plan
- ✓ Download virus protection on all your devices
- ✓ Get security insurance for your business
- ✓ Ensure you regularly patch your operating systems and applications
- ✓ Implement multi-layered cybersecurity defenses that include DDoS mitigtion and DNS Security

For more information on cybersecurity protection for your small business, visit us online or talk to an Suddenlink Business specialist today at 866-209-1099.

Sources:
1. https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats#section-header-3
2. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

suddenlink® business