STRENGTHEN YOUR CYBERSECURITY

Cyberattacks are a concern for businesses. Learn about cybersecurity threats and how to protect your business.

Why cybersecurity matters

Cyberattacks cost the U.S. economy billions of dollars a year and pose a threat for individuals and organizations. Small businesses are especially attractive targets because they have information that cybercriminals (bad actors, foreign governments, etc.) want, and they typically lack the security infrastructure of larger businesses to adequately protect their digital systems for storing, accessing, and disseminating data and information.

Surveys have shown that a majority of small business owners feel their businesses are vulnerable to a cyberattack. Yet many small businesses cannot afford professional IT solutions, have limited time to devote to cybersecurity and don't know where to begin.

Start by learning about common cybersecurity best practices, understanding common threats and dedicating resources to address and improve your cybersecurity.

Best practices for preventing cyber attacks

Train your employees

Employees and their work-related communications are a leading cause of data breaches for small businesses because they are direct pathways into your systems. Training employees on basic internet usage best practices can go a long way in preventing cyberattacks.

Important topics to cover include:

- Spotting phishing emails
- Using good internet browsing practices
- Avoiding suspicious downloads
- Enabling authentication tools (e.g., strong passwords, Multi-Factor Authentication, etc.)
- Protecting sensitive vendor and customer information

Secure your networks

Safeguard your internet connection by encrypting information and using a firewall. If you have a Wi-Fi network, make sure it is secure and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password-protect access to the router. If you have employees working remotely, use a Virtual Private Network (VPN) to allow them to connect to your network securely from out of the office.

Use antivirus software and keep all software updated

Make sure all of your business's computers are equipped with antivirus software and are updated regularly. Such software can be found online from a variety of different vendors. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. It is recommended to configure all software to install updates automatically.

In addition to updating antivirus software, it is key to update software associated with operating systems, web browsers and other applications, as this will help secure your entire infrastructure.

Enable Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a mechanism to verify an individual's identity by requiring them to provide more than just a typical username and password. MFA commonly requires users to provide two or more of the following: something the user knows (password, phrase, PIN), something the user has (physical token, phone) and/or something that physically represents the user (fingerprint, facial recognition). Check with your vendors to see if they offer MFA for your various types of accounts (e.g., financial, accounting, payroll).

Monitor and manage Cloud Service Provider (CSP) accounts

Consider using a CSP to host your organization's information, applications and collaboration services, especially if you're utilizing a hybrid work structure. Software-as-a-Service (SaaS) providers for email and workplace productivity can help secure data being processed.

Secure, protect, and back up sensitive data

- **Secure payment processing -** Work with your banks or card processors to ensure you are using the most trusted and validated tools and anti-fraud services. You may also have additional security obligations related to agreements with your bank or payment processor. Isolate payment systems from less secure programs and do not use the same computer to process payments and casually browse the internet.
- **Control physical access -** Prevent access or the use of business computers by unauthorized individuals. Laptops and mobile devices can be particularly easy targets for theft and can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel. Conduct access audits on a regular basis to ensure that former employees have been removed from your systems and have returned all company issued devices.
- **Back up your data -** Regularly back up data on all of your computers. Forms of critical data include word processing documents, electronic spreadsheets, databases, financial files, human resources files and accounting files. If possible, institute data backups to cloud storage on a weekly basis.
- **Control data access -** Frequently audit the data and information you are housing in cloud storage repositories such as Dropbox, Google Drive, Box and Microsoft Services. Appoint administrators for cloud storage drive and collaboration tools and instruct them to monitor user permissions, giving employees access to only the information they need.

Common threats

As important as it is to include best practices in your cybersecurity strategy, preventative measures can only go so far. Cyberattacks are constantly evolving, and business owners should be aware of the most common types.

- Malware (malicious software) is an umbrella term that refers to software intentionally designed to cause damage to a computer, server or computer network. Malware can include viruses and ransomware.
- Viruses are harmful programs intended to spread from computers to other connected devices like a disease. Cyber criminals use viruses to gain access to your systems and to cause significant and sometimes unrepairable issues.

- Ransomware is a specific type of malware that infects and restricts access to a computer until some sort of ransom is provided. Ransomware will commonly encrypt data on the victim's device and demand money in return for a promise to restore the data. Ransomware exploits unpatched vulnerabilities in software and is usually delivered through phishing emails.
- Spyware is a form of malware that is designed to gather information from a target, and then send it to another entity without consent. There are types of spyware that are legitimate, legal and operate for commercial purposes such as advertising data collected by social media platforms, however malicious spyware is used frequently to steal information and send it to other parties.
- Phishing is a type of cyberattack that uses email or a malicious website to infect your computer or system with malware or to collect sensitive information. Phishing emails appear as though they've been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code. Be very cautious about opening links from unknown sources. If something seems suspicious from a known source, don't just click on it - ask the source directly if it's legitimate.

Assess your business risk

The first step in improving the cybersecurity of your business is understanding the risk of an attack and where you can make improvements to safeguard your data and systems. A cybersecurity risk assessment can identify where a business is vulnerable and help you create a plan of action, which should include guidance on user training, securing email platforms and protecting your business's information systems and data.

Planning and assessment tools

There's no substitute for dedicated IT support, whether it's an employee or external consultant, but those resources can be expensive. Here is a list of measures (with specific resources noted) that all businesses can take to improve their cybersecurity.

- **Create a cybersecurity plan.** The Federal Communications Commission (FCC) offers a cybersecurity planning tool (The Small Biz Cyber Planner 2.0) to help you build a custom strategy and cybersecurity plan based on your unique business needs.
- **Conduct a Cyber Resilience Review -** DHS partnered with the Computer Emergency Response Team (CERT) Division of Carnegie Mellon University's Software Engineering Institute to create the Cyber Resilience Review (CRR). This is a non-technical assessment to evaluate operational resilience and cybersecurity practices. You can either complete the assessment yourself, or request a facilitated assessment by DHS cybersecurity professionals.
- **Conduct vulnerability scans-** DHS, through its subagency: Cybersecurity and Infrastructure Security Agency (CISA) also offers free cyber hygiene vulnerability scanning for small businesses. They offer several scanning and testing services to help organizations assess exposure to threats to ultimately help secure systems by addressing known vulnerabilities and adjusting configurations.
- **Manage Information Communication Technology (ICT) supply chain risk -** Use the ICT Supply Chain Risk Management Toolkit to help shield your business information and communications technology from sophisticated supply chain attacks. Developed by CISA, this toolkit includes strategic messaging, social media, videos and resources, and is designed to help you raise awareness and reduce the impact of supply chain risks.
- **Take advantage of free cybersecurity services and tools -** CISA has also compiled a list of free cybersecurity resources including services provided by CISA, widely used open-source

tools, and free services offered by private and public sector organizations across the cybersecurity community. Use this living repository of resources to further advance your security capabilities. CISA also provides guidance for small businesses.

- **Maintain DoD industry partner compliance (if applicable) -** Of special relevance to federal contractors and subcontractors is the Cybersecurity Maturity Model Certification (CMMC) program. Its purpose is to safeguard Controlled Unclassified Information (CUI) that is shared by the DoD. CMMC is a framework and assessor certification program that provides a model for contractors to meet a set of cybersecurity standards and requirements. It's based on a 3-tiered model (Foundational, Advanced, Expert) that requires companies to implement security measures (and be assessed accordingly), depending on the sensitivity of the information. Rulemaking is currently in progress, but it is essential for contractors to remain up to speed with requirements as a certain CMMC level will be required as a condition of contract award.