Cybersecurity is critical to all businesses, especially small businesses. Continuing from our previous section, Cybersecurity Basics for Small Business, next we cover the various types of **cyber attacks**, means for protecting (**cyber defense**) your small business from cyber threats, and additional resources.

Cyber Attacks

Types of Cyber Attacks & Threats

There are a variety of ways in which **cybercrimes** are perpetuated. The following is a listing of types of cybersecurity threats and their methods.

- **Malware** is a type of software used to perform an unauthorized function or process. This unauthorized software can perform actions such as tracking keystrokes and keyboard events (key logger).
- **Phishing** is the practice of sending fraudulent emails in order to obtain sensitive data.
- **Spyware** is software that is secretly installed into an information system, often through fraudulent emails or websites.
- **Ransomware** is a type of malicious software designed to extort money by blocking access to files or the entire computer system until the ransom is paid.
- A **Virus** is a type of program that replicates and infects a computer.

For more information on these cyber attacks and threats, visit: What is Cybersecurity?

Reporting Cyber Attacks & Crimes

Inform law enforcement and the state attorney of any and all cyber attacks and crimes. Report stolen information to the Internet Crime Complaint Center (IC3). Report fraud to the Federal Trade Commission (FTC). Report Network Vulnerabilities to the United States Computer Emergency Readiness Team (US-CERT). Report any large cybercrimes to the Federal Bureau of Investigation (FBI).

In addition, most states maintain specific requirements for notification in the case of a security breach. These disclosure requirements are available here: Security Breach Notification Laws.

Cyber Defense Against Cyber Attacks

Cybersecurity defenses (or cyber defenses, for short), are proactive approaches to mitigate the risks of cyber attacks and threats. They focus on preventing, detecting and providing timely responses to cyber attacks or threats so that no infrastructure or information is tampered with.

Software

Installing protective software is one way to guard your information systems. **Antivirus** and **antispyware** software can detect and eliminate malicious software that may be installed onto a computer. **Firewalls** prevent computers from outside your network from connecting and stealing shared data. Utilizing a **WPA2** wireless network will ensure that only authorized users may access the Wi-Fi connection by requiring a secret password.

Examples: *Antivirus, Antispyware, Firewalls, Encryption, Trusted Platform Modules, SSID, IDPS, WPA2*

Procedural

Developing policies and procedures for your employees can help prevent unauthorized access. These include instructing employees to develop **complex passwords**, only providing them access to the systems and information they need, and preventing them from accessing fraudulent websites through **web filters**.

Examples: *Multi-Factor Authentication, Limited Access, Email/Web Filters, Activity Logs, HTTPS/PVN*

Physical

Ensuring that your business and its devices are physically secure can prevent data theft that will compromise your business. **Locking** computers after use and utilizing a physical lock which attaches the computer to a desk, can prevent an unauthorized person from taking the computer and extracting information. **Privacy screens** can also help prevent people from viewing confidential data.

Examples: *Drive Locks, Surge Protectors, Computer Locks, Privacy Screens*

Additional

Take advantage of all the ways you can protect your business' data. Purchasing **cyber-insurance** can reimburse the value of any stolen data. However, in order to receive payouts, the business must implement and maintain an up-to-date **cybersecurity program**. Performing **background checks** on employees is also an important measure that can prevent malicious actors from stealing your information from inside the company.

More Information

For more information on these terms, visit: NIST Glossary

For more examples of ways to protect your business from cyber attacks visit: FEMA Cyberattack, FTC Protecting Personal Information, FTC Start With Security

Advanced Cyber Defenses

In additional to the measures listed above, there are several advanced tools you can use to protect your business:

- Next Generation Firewall (NGFW) (Firewall)
- Intrusion Prevention Systems (IPS)
- Deploy Demilitarized Zone (DMZ)
- Virtual Private Networking (VPN)
- Local Area Networks Layers (LAN)
- Digital Signatures (DSA, RSA, EDCSA)
- Encryption (AES, Triple DES) (Encryption)

For more information on what these advanced measures mean, visit: NIST Glossary

More on Cybersecurity for Small Businesses

To continue learning about Cybersecurity for Small Businesses, view our next section: Cybersecurity Plans & Implementation for Small Business

Additional Small Business Resources

Already in business or thinking about starting your own small business? Check out our various Small Business Snapshots, Market Research Links and our Sample Business Plans

collection. Remember, you can also receive free professional business advice and free or low-cost business training from your local Small Business Development Center!

Sharing is caring!

- Share
- Tweet
- LinkedIn