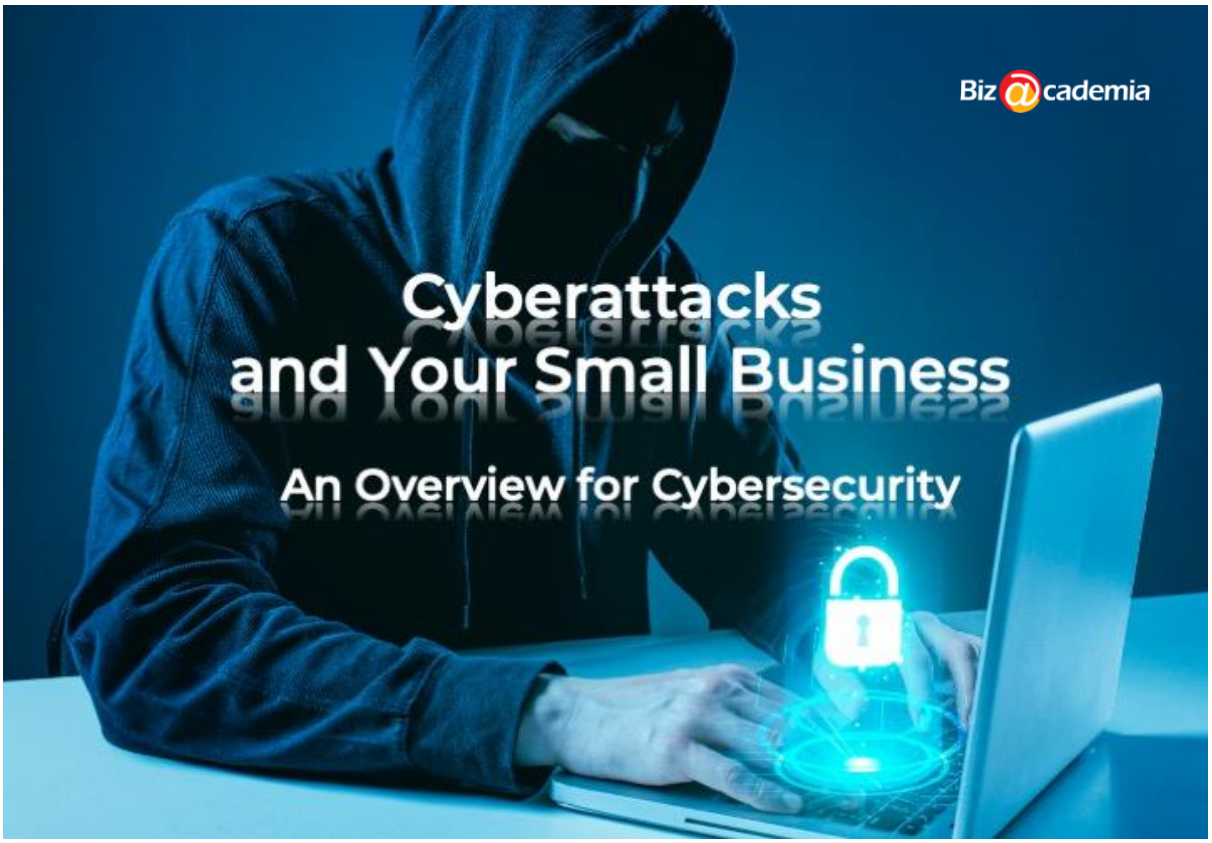
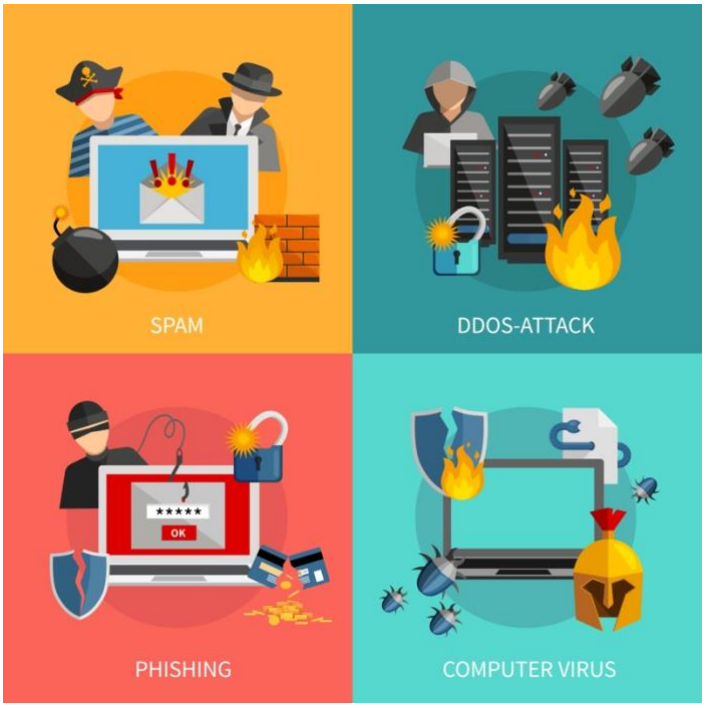



Social engineering attacks like phishing and denial-of-service attacks are the most common types impacting SMBs. Using strong passwords, having up-to-date antivirus software and implementing best practices are just a few tactics you should employ as part of an overall cybersecurity solution.
The internet has become a digital Silk Road that facilitates nearly every facet of modern life. Entrepreneurs can easily find themselves under attack from cyber malcontents. Taking proper precautions can hamper or completely stymie a hacker's attempt to access your network, we've compiled info on how to protect yourself.

## Why cyberhackers go after small businesses

A new report shows 46% of breaches impacted small and midsize businesses in 2021. These businesses often lack the resources to defend themselves successfully from attacks. Since breaches can be devastating to SMBs, owners are more likely to pay a ransom to get their data back.




# Cyberattacks to look out for

One of the best ways to prepare for an attack is to understand the different methods hackers generally use to gain access to that information.

APT: An advanced persistent threat, or APT: Once an attacker gains access to the target network, they work to remain undetected while establishing their foothold on the system.

DDoS: A distributed denial-of-service attack If a breach is detected and repaired, the attacker may have already secured other routes into the system so they can continue to plunder data.

Password Attack: There are three main types of password attacks: a brute-force attack, a dictionary attack and keylogging. Keylogging tracks a user's keystrokes, including login IDs and passwords. Hackers can also use a program to try different combinations of dictionary words.

Inside attack: Your business should have a protocol in place to revoke all access to company data immediately when an employee is terminated.

Man in the middle (MitM) attack: Knowing this, a hacker who uses the MitM method of intrusion does so by installing malware that interrupts the flow of information to steal important data. This is generally done when one or more parties conduct the transaction through an unsecured public Wi-Fi network, where the hacker has installed malware that sifts through data.

Phising: Spear phishing, an advanced form of this type of attack, requires in-depth knowledge of specific individuals and social engineering to gain their trust and infiltrate the network.

Ransomeware: A ransomware attack infects your machine with malware and demands a ransom. Ransomware is one of the fastest-growing types of security breaches. It locks you out of your computer and demands money in exchange for regaining access, or it threatens to publish private information.

SQL injection attack: Bad actors can access and modify important databases, download files and even manipulate devices on the network through a successful SQL injection attack. The Structured Query Language (SQL) has been one of the main coding languages on the internet for more than 40 years. It can also be an easy way for malicious code to make its way onto your business's website.

**Zero-day attack:** What are known as zero-day attacks? They are unknown flaws and exploits in software and systems discovered by attackers before developers and security staff become aware of any threats. These exploits can go undiscovered for months or even years until they are discovered and repaired.

## How to secure your networks

Businesses are spending $1.75 trillion on cybersecurity products over the next five years, according to Cybersecurity Ventures' 2022 Cybersecurity Almanac. Expert suggests businesses invest in additional security measures along with those more surface-level tools.

To protect sensitive data, such as employee records, client/customer information and financial statements, businesses should consider using encryption software. Learn more in our small business guide to computer encryption. authentication or password-security software: Use these tools with internal programs to reduce the likelihood of password cracking.

## Cybersecurity best practices

In addition to implementing software-based solutions, small businesses should adopt certain technological best practices and policies to shore up security vulnerabilities. Hackers are constantly scanning for security vulnerabilities, Cobb said, and if you allow these weaknesses to linger for too long, you're significantly increasing your chances of being targeted.

Cybercrime is getting more sophisticated, so are the solutions. There are more than a dozen ways to secure your business's devices and network. Even if you're hacked, you can recover from a data breach. If you follow the best practices, your company will likely be better off.