8 Steps to Protect Your Business from Cyberattacks

In the modern world, many businesses depend on the internet and have a solid online presence. This can be beneficial but it also comes with a higher risk of security issues. A cyber attack exposes customers' names, social security numbers, credit card information, addresses, and other sensitive information to hackers.

This can in turn damage a business's reputation or/and make them lose money. So, how can business owners protect their businesses from cyberattacks? There are quick, cost-effective, and easy steps business owners can follow to safeguard their businesses.

In this article, we offer recommendations on the actions you should take right away to safeguard your business from a cyberattack.

What is a cyberattack?

A cyber attack is unauthorized access to disable, disrupt, destroy, or take control of a computer system, or computer network, as well as to change, block, delete, modify, or steal the data stored on it.

This attack can be launched by any person or group from any location using one or more different attack tactics. Those who commit cyberattacks are usually referred to as cybercriminals.

Why do Cyber Attacks Occur?

Here are some of the reasons why cyber attacks happen;

- Financial benefits
- Revenge
- Cyberwarfare

- Financial benefits

Most cyberattacks targeted at businesses are carried out by cybercriminals with financial gain in mind. They try to steal sensitive information, such as employee or customer credit card details, which they can use to obtain money or products using the victims' identities.

Cybercriminals also cripple computer systems by locking them so owners and authorized users cannot access the programs or information and then demand ransom payments to unlock the computers.

- Revenge

Disgruntled ex-employees can launch an attack on a company's server to humiliate their employer publicly or harm the company's reputation. This type of attack can also be carried out by hacktivists as a form of protest and can also affect nonprofit organizations and the government.

- Cyberwarfare

Governments all across the world also participate in cyberattacks. Many admit to planning and carrying out attacks against other nations as part of ongoing political, social, and economic conflicts.

9 Most Popular Cyber Attacks

1. Malware
2. Phishing
3. MitM
4. DDoS
5. SQL injection
6. Zero-day exploit
7. Drive-by
8. Credential-based attacks
9. Brute-force attack

- Malware

Malicious software that targets information systems is known as malware. Hackers might exploit it to steal or covertly copy private information, restrict access to files, interfere with system performance, or even render systems unusable. Examples of malware are Trojans, spyware, and ransomware.

- Phishing

Phishing is the practice of hackers convincing people that email messages are originating from a trusted source by utilizing false hyperlinks that look official.

By clicking on an embedded link or an attachment in the email, recipients are tricked into installing the malware.
This cyberattack aims to steal consumers' login information or private information, such as credit card numbers.

- MitM

Man-in-the-middle attacks, often known as MitM, take place when attackers secretly stand between two parties, for instance, a computer user and their financial institutions.

The user gives the attacker complete information without even realizing it. A cybercriminal can install software to process all of the victim's data once malware has compromised a device. Another name for MitM is an eavesdropping attack.

- DDoS

Attacks known as distributed denial-of-service (DDoS) occur when hackers flood a company's servers with numerous simultaneous data requests, overwhelming them and limiting their capacity to respond to service demands, which lowers the system's performance. This attack frequently serves as a prelude to another attack.

- SQL injection

When malicious code is inserted into a server or application that uses Structured Query Language (SQL), it causes the server to divulge information that it normally wouldn't. This is known as SQL injection.

- Zero-day exploit

Hackers can use vulnerabilities in hardware and software to their advantage. Before developers become aware of the problems, these vulnerabilities may already be present for days, months, or even years. Constant monitoring is required to detect zero-day vulnerability.

- Drive-by

When a person accesses a website that later infects their computer with malware, this is known as a "drive-by" or "drive-by download."

.

- Credential-based attacks

Hackers who steal the passwords IT staff members use to access and administer systems can later use that information to gain unauthorized access to computers, steal sensitive data, or interfere with a business's operations.

- Brute-force attack

Brute-force attacks use trial-and-error techniques to break encryption keys, usernames, and other login information in the hopes that one of the many failed attempts will yield a successful guess.

8 steps to protect your business from cyberattacks

Here are some recommendations to help protect your business from cybercriminals.

1. Backup your data
2. Protect your network and devices
3. Encrypt sensitive information

4. Use multi-factor authentication (MFA)
5. Use passphrases
6. Observe computer systems and equipment usage
7. Educate your team about online safety
8. Get cyber security advice

- Backup your data

Use a variety of backup techniques, such as daily incremental backups to a portable device or cloud storage, to help assure the security of your data. Include weekly, quarterly, and yearly server backups as well. Regular checks should be made to ensure that this data is functioning properly and is recoverable.

The 3-2-1 rule is one of the best data backup methods. You should store at least three copies of your data using this technique. Two of them ought to be on various media, and one ought to be off-site. Avoid leaving the linked devices on the computer as a cyber-attack could infect them.

Ensure that you use cloud storage that offers encryption when storing your data and multi-factor authentication to access them.

- Protect your network and devices

To protect your network and devices, you need to update your software regularly, install security software, set up firewalls, and turn on spam filters.

Ensure your software is updated
It is essential to automatically update your operating system and security software. This is because updates could provide crucial security improvements for current viruses and attacks. You can plan the update after work hours or at a more convenient time.

Put security software in place
To help avoid viruses, install security software on the computers and other devices used for business. Ensure that anti-virus, anti-spyware, and anti-spam filters are present in the security software you choose.

Install a firewall
Installing a firewall will safeguard the internal networks of your company. It is an item of hardware or software that stands between your computer and the internet. It controls all incoming and outgoing traffic as the gatekeeper.

For a firewall to function properly, it must be patched frequently. You should also install the firewall on all of your mobile business devices.

- Activate spam filters

Phishing emails can be used to steal personal information and infect your computer with viruses and malware. Activating spam filters is a good way to protect your business from phishing emails and lessen the likelihood that you or your staff will unintentionally open a spam or fraudulent email.

- Encrypt sensitive information

Before sending your data over the internet, encryption transforms it into a hidden code and only parties that possess the encryption key are permitted access to the data. Some data encryption software even alerts you when someone tries to change or tamper with the data. So, ensure your network encryption is enabled and that all data received or stored online is encrypted.

- Use multi-factor authentication (MFA)

Multi-factor authentication is an added step to help protect your information. It might look inconvenient however it makes it difficult for attackers to access your device or online accounts.
This authentication asks you to submit two or more forms of identification verification before you can access your account.

- Use passphrases

To secure access to your devices and networks that contain vital business data, use passphrases rather than passwords. Passphrases are passwords that consist of a phrase or a group of words. They are easy for people to remember but hard for computers to figure out.

An ideal passphrase contains 14 unpredictable characters that are a mixture of upper and lowercase letters, special characters, and digits.

- Observe computer systems and equipment usage

Keep a list of every computer hardware and software your company employs. Make sure they are protected to avoid unauthorized access.

Remove any software or hardware that you no longer require, delete any sensitive data from it, and unplug it from the network.
If someone no longer needs access because they changed roles or are no longer employed by you, immediately revoke their access.

- Educate your team about online safety

Ensure your employees are aware of the dangers they can encounter and their responsibility for maintaining the security of your business. Teach them how to keep secure passphrases and passwords, how to recognize and prevent online threats, how to respond in the event of a cyber threat, how to file a cyber threat report etc.

- Get cyber security advice

If you are not sure where to start with securing your business against cyber attacks, it is advisable to seek cyber security advice from professionals.

Conclusion

It's important to take cyberattack defence seriously. It may cost thousands of dollars to deal with the after-effects or you could go out of business permanently.
To save you from this heartbreak we covered steps to help you protect your business from cyberattacks in this article. We hope you found it informative.