5 Ways to Prevent a Cyber Attack

Make sure your business server is protected from future cyber-attacks and ransomware.

TBNG CONSULTING

1. Create an internal policy

Did you know that your employees are your biggest cyber security risk?

Keep Employees Informed

Many business owners are surprised to learn that their employees are their biggest security risk. Yet, only 58% of U.S. mid-size companies train employees on cyber security. In many cases, employees will click on a link in an email or use a poor password leading to criminals having access to their computer's files. If you do nothing else, consider informing your employees that any Microsoft Outlook email that is not from a trusted source-and asks you to enable macros-should not be opened but rather, deleted immediately.

Learn from other's mistakes

Cyber intrusions and disclosures of private data are very common. These attacks can lead to huge financial losses. However, if you learn from those who have had to learn the hard way, you can make informed decisions regarding similar cyber hacking issues.

Are you protected?

You should also check with the person who set up your business server to ensure that the right protections are in place on your network.

2. Keep your computers updated

When is the last time you checked that your computer was up to date?

Easy way to prevent hacks

One of the easiest ways to help prevent cyber hacks almost immediately is to ensure that your entire network is up to date. Pay attention to all notifications regarding updates to your operating systems, anti-virus software, web browsers, and firewalls. Frequently, software updates will include patches for newly discovered security vulnerabilities that could potentially be exploited by ransomware attackers. Ignoring any of these notifications essentially leaves cracks in your computer's defense system.

Know what not to do

Do not add firewalls and filters to a network that is already insecure. Cybercriminals will locate the vulnerability eventually. You need to have a professional locate and fix the major problems to ensure that your system is going to remain safe.

3. Backup and Cloud Services

Do you regularly back up your computer?

Backup important data

The most effective way to combat ransomware infections is to backup all of your important data. Attackers will encrypt valuable files and leave them inaccessible to the victims. If the victim has backup copies of the files, they can restore them once the infection has been cleaned off. However, be sure that your backups are properly protected and stored off-line so that attackers can't delete them. Backup your files regularly and verify the integrity of those backups regularly. Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

Cloud Services

Cloud services can help mitigate ransomware infection, because they may retain previous versions of files and allow you to roll back on to the unencrypted version. Cloud services can save businesses both time and money handling their application needs and data storage. Smaller businesses may find it to be cost-prohibitive to purchase, manage and maintain server farms. However, you can get the same level of computing through cloud services with a minimal monthly subscription. Be sure to use only the most reputable companies for your cloud services.

4. Passwords

Create strong passwords and change them frequently.

Password Security

You should never use the same password for all of your accounts. By doing this, you are making it easier for hackers to steal all of your personal information. Try creating unique passwords by combining numbers, symbols, capital letters, lowercase letters and other factors to ensure its security.

Administrator access

No users should be assigned administrative access unless it is absolutely necessary. Manage the use of privileged accounts. Configure access controls, including file, directory, and network share permissions appropriately. If users only need to read specific information, they don't need write-access to those files or directories.

5. Hire a security expert

An expert will help you ensure protection of your network.

Hire a security consultant

Hiring a security consultant is one of the best ways for you to discover if your infrastructure has any holes or security risks present. Although you may think this sounds like a huge expense, it is an invaluable service that may help you to save a significant amount of money and frustration down the road. Large companies, such as Facebook, have created programs that reward those who investigate the security of their website. The users in these programs are referred to as “ethical hackers” and can help you see where any security risks may lurk in your company.

What if you're a victim?

Should you pay the ransom?

Victims are advised to never pay the ransom because it encourages the attackers. Paying the ransom does not guarantee that all files will be intact when returned. The best option would be to restore all files from a backup. If that isn't a possibility, there are some tools available to help decrypt and recover some information.

Why do hackers demand Bitcoin, and how much?

When dealing with ransomware, the hackers often demand between 0.3 and 1 Bitcoins, which is about $562 - $1,875. Sometimes they demand a payment denominated in dollars but made via Bitcoin. Bitcoin is the most popular digital currency among cybercriminals because it is decentralized, unregulated, and practically impossible to trace. It may not seem like they are requesting much, however, cyber-attacks are often widely distributed so this small amount can add up quickly.

Don't wait, or it may be too late.

This guide is meant to help you protect yourself from cyber-attacks. Please contact us if you need professional help securing your organization's network from ransomware and other security attacks.

CONTACT US TODAY

Corporate Offices
500 Boston Post Road
Milford, CT 06460
(203) 874-9607

Rhode Island Offices
935 Jefferson Blvd., Ste. 1004
Warwick, RI 02888
(401) 709-5216

Toll-Free: (855) 512-4817

info@tbngconsulting.com

www.tbngconsulting.com