Exoweb
Managed Network & Internet Services

TOP TEN WAYS HACKERS

BREAK INTO YOUR NETWORK, STEAL YOUR DATA, AND EMPTY YOUR BUSINESS'S BANK ACCOUNT.

Someone opens an email at your company and...
The next thing you know ... **BAM!** ... someone hacks into your network and starts to collect sensitive information, or even worse, they start deleting all of your business assets.

Cybercrime is booming these days. There are **82,000** new malware threats being released every single day and most hackers are steering away from larger companies to go for the "low hanging fruit" of small businesses who aren't using security best practices.

WONDERING IF CYBERSECURITY IS NECESSARY FOR YOUR BUSINESS?

CHECK OUT THESE STATS

64% of companies experienced **web-based attacks.**
62% of companies experienced **phishing** and **social engineering attacks.**
59% of companies experienced **malicious code** and **botnets.**
51% of companies experienced **denial of service attacks.**

By 2020 there will be over 200 billion connected devices and the average cost of a data breach will exceed $150 million as more business infrastructure gets connected.

The risk is real with IoT and it's growing. There are 25 connected devices per 100 inhabitants in the United States. Only 38% of global organizations claim they are prepared to handle a sophisticated cyber-attack. Total cost for cybercrime committed globally has added up to $100 billion.

Don't think that all that money comes from hackers targeting corporations, banks or wealthy celebrities. Individual users like you and me are also targets. As long as you're connected to the internet, you can become a victim of cyber-attacks.

The threat is real. Cyber-attacks are on the rise. What are you doing to protect your business and your life's work? If you're not investing in cybersecurity, are you prepared to pay a lofty figure to regain your records? What will your clients think?

IN THIS REPORT, WE SHOW YOU THE TOP 10 WAYS HACKERS ARE EXPLOITING YOUR BUSINESS, ROBBING YOU BLIND, AND HOW TO FIX IT.

01 Poorly Trained Employees

Having poorly trained employees is the #1 vulnerability for business networks and their employees using them. It's extremely common for an employee to infect an entire network by opening and clicking phishing emails (an email designed to be from a legitimate company or vendor you trust) asking for specific login credentials to a website or network. By training your employees about phishing emails, your chances of a network decrease significantly.

02 Exploit Device Usage Outside of Company Business

Maintaining an "Acceptable Use Policy" that outlines how employees are permitted to usecompany computers, emails, internet, and software. Having a policy in place with significantly decrease your chances of a rogue employee using your network for unlawful reasons.

03 They Take Advantage of Weak Password Policies

Passwords should be at least 8 characters, contain upper and lowercase letters with symbols.Having strong passwords in place will decrease your chances of being hacked by a low-level hacker. There are plenty of passwords generators for sale today, so make sure you pick one that is able to store and generate secure passwords for you.

04 You Are Still Running Windows 7 (and older) Systems

Windows 7 systems are no longer supported.
You need to upgrade to Windows 10 Pro. Vulnerabilities are found often in software and hardware updates. Making sure you're staying current on all updates will ensure you're protected from any cracks that may come up from any kind of update.
These updates can be automated, so make sure you check your settings to get the latest updates.

05 Attack Network with No Backups or Single Location Backups

Redundancy, redundancy, redundancy. Ever heard the saying, "Never put all of your eggs in one basket?" That goes the same with your business server. Having a backup of your files gives a hacker a less likely chance to take down your business. Not only that, if an employee wrongly deletes something, you'll have a backup ready to go.

06 They Exploit Networks with Employee Installed Software

The easiest entry point for hackers could come in the form of unsuspecting downloads such as files,games, movies, or any other innocent looking application. Prevent this easy fix through a good firewall and employee training and monitoring.

07 They Attack Inadequate Firewalls

Firewalls are the frontline of defense for any network. Its sole purpose is to monitor inbound and outbound traffic to make sure no security threats are harming your network. Just like a car, firewalls need to maintenance by a professional IT person or company. Most IT companies will do, but make sure you're hiring someone with an emphasis on security.

08 They Attack Your Devices When You're Off the Office Network

It's become pretty common practice for hackers to create clone Wi-Fi access points to try to get you to enter your personal information over their "safe" public access point. Never enter any financial, medical, or other sites that store your sensitive data. This goes for making purchases online also. Only access sites that store your sensitive information if you're absolutely sure of the source of the connection and that it is safe.

09 Using Phishing Emails to Fool You

Ever get one of those bogus emails in your inbox requesting you reset your password or has a sketchy attachment from someone whom you do not know? These are phishing emails and they are designed for you to go to a different site, other than your business site, to enter login credentials so that a hacker can collect them for their use. Although these can be filtered by spam, some occasionally slip by. These can come in all shapes and sizes so be aware when checking through your inbox because you may fall victim to a phishing email.

10 They Use Social Engineering and Pretend to be You

In this day and age, hackers will do anything to get your personal information, even by pretending to do a password reset. In 2009 Coca-Cola's CEO opened an email with this kind of software deployed and opened up hackers to infiltrated the network. The same thing happened with Apple also and their popular iCloud service.

LET EXOWEB HELP YOU

If you are concerned about cybercriminals or hackers gaining illegal access to your network, Exoweb can help you.
Please call 855-522-8779 or go to exowebinc.com/audit for a free security audit.