THE 5 BIGGEST CYBERSECURITY RISKS

And the 5 Best Ways to Protect Against Them!

The cybercrime business has reached record proportions at nearly $1 trillion in earnings per year. Your data is an incredibly valuable asset - not only to you, but to hackers as well. That's why we've compiled some of the most common cybersecurity risks and ways to protect your business in 2020.

Phishing

A practice in which the Cybercriminal sends an email claiming to be from a reputable company in an effort to get personal information from you, such as a credit card number or password.

Maintain Awareness

Watch out for pop-ups, fake wireless networks, phishing attacks, and anything that seems suspicious. Always make sure you're receiving information from a real person or company.

Social Engineering Attacks

A form of attack wherein the cybercriminal attempts to manipulate the end user into divulging personal information. They will often steal your email list and send a malicious message to your friends.

Use Complex Passwords

A complex password is necessary to prevent hackers from being successful. Here's how to make a complex password. Don't use family names or words found in the dictionary. Use more than 9 characters and a mix of numbers, letters, and symbols. When available use two-factor authentication.

Malicious Pop-Ups

A pop-up wherein you're tempted to click on an ad of some sort - leaving your system infected with malware. This commonly happens on social media websites.

Keep A Current Backup

Your data must be backed up onsite and offsite (in a cloud-based system) on a regular basis. Test your backups often and maintain at least three copies of everything.

Fake Wireless Networks

A free Wi-Fi network setup with key loggers that copy and archive all information typed once you're connected. Cybercriminals will setup these fake/phony networks in public areas.

Secure Wi-Fi with a VPN

A virtual private network or VPN allows you to create a secure connection and share data remotely without the worry of working through a public network.

Ransomware

A type of malicious software wherein the cybercriminal blocks access to your data or computer systems in exchange for a ransom fee. There's been a huge increase in this type of attack in recent years.

Hire an Expert

A reputable IT company with experience in cybersecurity will be able to keep your network and users secure against any type of attack. They will deploy a layered approach to security with firewalls, anti-virus software, patch deployment, and more

Don't take unnecessary risks when it comes to cybercrime!