5 SECURITY STEPS TO PROTECT YOUR BUSINESS

AFFORDABLE COMPUTER SOLUTIONS

FAST RESPONSE · INTEGRITY DRIVEN

TABLE OF CONTENTS

Intro

The Growing Danger of Cybercrime for Your Business

1

Security Step #1: Make Sure Your Security is Updated

2

Security Step #2: Educate Your Employees

3

Security Step #3: Have a Secure Backup System

4

Security Step #4 Use Multi-Factor Authentication

5

Partner with an MSP

INTRODUCTION

The Growing Danger of Cybercrime for Your Business

Introduction

Every Business connected to the Internet is wide open to threats from computer hackers and online predators. And the threat is only getting worse. Businesses targeted by cybercriminals in the past year increased from 38% to 43%. It is believed that Hackers have attempted to break into every business through the internet, but they focus on the ones that are easiest to hack. Or those who don't update their security software. It's only a matter of time before they find a way into the more secure businesses.

Once an attack occurs, the impact of cyber-attacks on business can be severe. You can end up spending thousands or even millions of dollars repairing the damage. Even after you repair everything, there can still be a lasting impact on your brand and your company's reputation.

Cyberattacks range from simple spyware on a computer to attempts at destroying the infrastructure of entire nations. They can result in the theft of valuable, sensitive data like medical records, bank account info, Social Security numbers, Credit Card numbers, and a lot more.

POTENTIAL CYBERTHREAT DAMAGE TO BUSINESSES

- Hacking
- Data Breaches
- Financial Burdon
- Operational Uncertainty
- Untrained Employees
- Potential Legal Liabilities
- Compliance
- Increased Business Insurance Costs

Take a look at these cybercrime statistics. They are not in your favor.

1. Cybersecurity Ventures predicts cybercrime will cost the world more than ***$6 trillion annually in 2021, up from $3 trillion in 2015.***

2. Ransomware attacks have ***swelled over the past year due to employees working from home.*** This has resulted in new IT vulnerabilities.

3. According to Security Magazine, there are over 2,200 attacks each day, which breaks down to nearly 1 cyberattack every 39 seconds.

How Does Cybercrime Affect Your Business?

Businesses that get hacked suffer significant financial loss because of data theft, client worries, and time lost to repair the damage. And we're not just talking about database damage. Security breaches may result in reputation damage, legal damages, and unforeseen financial loss. For businesses with limited resources, an attack can prove fatal. It is reported that 60% of small businesses close their doors forever following a cyberattack.

Even worse news, Hackers are beginning to use Artificial Intelligence to do the hard work for them. AI systems are learning how to analyze security programs and hack into protected systems faster than humans can. This new threat will disrupt us on a wider scale than ever before.

Are you prepared to protect your business from these threats? Don't be another statistic!

CHAPTER 1

Make Sure Your Security is Updated

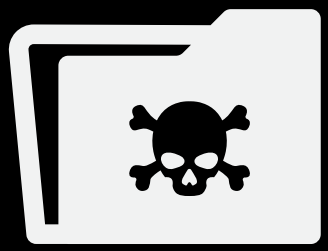
“Businesses targeted by cybercriminals in the past year increased from 38% - 43%.”

Cybersecurity is something far too many companies don't pay much attention to.

Without a doubt, the word that strikes terror in the business world is ransomware. Simply avoiding strange websites or having an antivirus program isn't enough to protect yourself from this and other threats. If you lose access to your data, your company will be out of commission for at least a few days. Probably much longer. Also, if something goes south with a ransomware attack, losing your data altogether can be a gamechanger — if not a game-ender.

TOP SECURITY THREATS SMALL BUSINESSES FACE TODAY

- Phishing Attacks
- Malware Attacks
- Ransomware
- Weak Passwords
- Insider Threats



Make Sure Your Security is Updated

CHAPTER 1

As a business owner, you are trusted with your client's information. And if you lost that info? Well, you'd lose that client. Maybe you'll lose all your clients. And after that? You'd probably be out of business.

That's why it's important to keep your Security Software updated. You know that pop-up from your antivirus software that keeps telling you it needs updating? Update it! Hackers look for vulnerabilities in software, and a simple update could hold the exact patch you need to keep these cyber criminals out of your data. However, if you keep ignoring that pop-up it could be the one thing that takes your entire network down. Stolen data is certainly not worth ignoring a simple update

CHAPTER 2

Educate Your Employees

The Dangers of Uneducation

According to research conducted by Shred-it, more than 40% of small business owners have reported that employee negligence and lack of training were the root cause of their most damaging data security breaches.

What to Educate Employees On

No matter what application, program, or unified threat management system you use to protect your data, it's only effective if your employees know how to use it. Which makes sense, since they are the ones answering emails and accessing the internet all day.

What happens if you get hacked? Once the hacker gets your info, he can easily hack into your computer and network. Now he has access to all of your files. Now he can copy, sell, or trade them, or encrypt them and hold them for ransom.

The bottom line is, your employees are at the forefront of cyberattacks every day. Your best defense against these attacks is to educate your employees fully on how to recognize threats. They should also be prepared to question all emails, attachments, and links.

Just one bad click could put your business at risk.

CHAPTER 3

Have a Secure Backup System

Good Backups

Having good backups protects you from cybercrimes like ransomware by letting you restore your database to a recent point in time before it was breached. The version of your computer's hard drive that is controlled by the criminal can be wiped out and replaced with one where you're in charge again -- and they're locked out.

This means backing up the original data on your computer, storing another backup on an external server or hard drive, and at least one more on a cloud backup service. Data Security in the Cloud has advanced so much lately that Cloud Providers can store multiple copies of your data, freeing you from the cost of on-site servers and backup devices.

Have a Secure Backup System

CHAPTER 3

An MSP can host your infrastructure offsite, and take care of all things IT, allowing for simple and instant scalability. Add new solutions with ease, only pay for what you need, and benefit from features such as built-in data backup, increased network security, and a flat monthly rate.

CHAPTER 4

Use Multi-Factor Authentication

Why “MFA”?

One of the biggest security threats today is the risk of compromised credentials. And not having Multi-Factor authentication is dangerous to your security. The reality is that employees do fall for phishing scams, and they do share passwords. If you're not using multi-factor authentication (MFA), your organization is wide open to attacks.

Multi-factor authentication can curb fraud immensely. One of the most valuable pieces of information attackers seek is user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise.

THE BENEFITS OF MULTI-FACTOR AUTHENTICATION

- An Effective Cybersecurity Solution
- MFA Provides more layers of Security than 2FA
- IMFA Assures Correct Identity
- It meets Regulatory Compliances
- Easy to implement
- Complies with Single Sign-On (SSO) Solutions
- Adds Extra security, even for remote employees
- It is a Proven Cybersecurity Solution

Yes, we understand that it takes a little longer for your employees to log into programs that use MFA. But we also know that the extra layers of security will help you sleep better at night. And that alone should tell you this is the way to go.

The average American today has access to more than 10 Internet Connected Devices in their household. Most have at least 2 computers and 2 smartphones. Across the world, an estimated 30 billion+ devices connect to the Internet. This connectivity generates a massive potential for advancement; but in turn, creates a paradise for hackers.

CHAPTER 5

Partner with a Managed Service Provider

Why Businsses Are Outsourcing their IT

As a Business Owner, we know you are busy operating your business. You're focusing on streamlining your operations, controlling the budget, and growing your business.

You don't have time to research the latest cybersecurity threats. But Managed Service Providers do.

Partner with a Manged Service Provider

CHAPTER 5

An MSP can save you money and maximize resources by providing high-level IT support. Not only does it give you access to a pool of experts and lower costs, but it also allows you to control your budget. Paying a monthly fee is more predictable than writing a check for unforeseen costs associated with cyber disasters, data loss, and equipment failures.

In this E-Book, we have covered; why you need to keep your cybersecurity up to date, the reasons why it's important to Train your Employees on Security, why you need a reliable Backup Solution, and why Multi-factor Authentication is an important tool in your security arsenal.

If you're not sure how to install, implement, or use these solutions, Managed Service Providers can help. We offer all of these security solutions and a whole lot more.

MSPs are in business to make it easier for you to run your business. Set up an appointment with us today and let's discuss the benefits we can offer you.

SECURE YOUR BUSINESS TODAY

Partnering With Us as your Manged Service Provider

Call our Number or Fill out the Form on our "Contact Us" Page