Cybersecurity for Small Businesses

There’s no question that cybersecurity is a hot topic these days. With the massive Equifax breach making headlines in 2017, it’s more important than ever for small business owners to understand the basics of cybersecurity. While the big companies have the resources to invest in serious cybersecurity measures, small businesses often don’t have the same luxury. That’s why it’s important for small business owners to educate themselves on the basics of cybersecurity and take steps to protect their businesses.

Why Cybersecurity Matters for Small Businesses

Every business is at risk for cyber-attacks but small businesses are often the target of cyber attacks because they usually have weaker security than larger businesses. With cyber-attacks becoming more and more common, they can have a devastating impact on small businesses, costing them:

- Time,
- **$$$** Money,
- and Customers.

60% of small businesses that suffer a data breach go out of business within 6 months.

So, having poor cybersecurity not only risks all of your clients information, employees information, the business' financial assets and data, it's also taking away time and money that you would be investing into your business and risking the success of it.

Reasons to take cybersecurity seriously:

1. To protect your customers and employees privacy and information
2. To protect your business' data and assets
3. To ensure your business' long term succession

How to Protect Your Business

As a small business owner, it's not only imperative to understand the importance of cybersecurity but to also know the basics of how to protect your business from cyber threats. Steps that every small business owner can take to protect their business from cyber attacks, include:

1. Hiring a trusted cybersecurity firm
2. Educating yourself and your employees about cybersecurity.
3. Creating strong passwords using a password manager
4. Using two-factor authentication (2FA).
5. Keeping your software and systems up to date.
6. Backing up your data on a regular basis.

- **Hire a Cybersecurity Firm-** The best thing you can do for your company is to hire a trusted cybersecurity firm to monitor and test your company's computer networks. The field of cybersecurity is constantly changing with new techniques and software always being developed. As a small business owner you're not likely to have the time and expertise that is required to properly defend your business against cyber criminals.
- **Education-** You should educate your employees about cybersecurity threats and how they can protect themselves. This includes teaching them about phishing scams, social engineering attacks, and how to spot suspicious activity. Cyber attacks happen a multitude of ways including: social engineering, phishing emails and SMS messages, scam calls, vulnerabilities in third-party software, stolen/compromised credentials, and even insider threat attacks. By educating your employees, you can help them become your first line of defense against cyber threats.
- **Strong Passwords-** It is important to have a strong password policy in place for all of your employees. This means requiring employees to use strong passwords that are difficult to guess, and changing them on a regular basis. Additionally, you should have a process in place for handling employee password changes and resetting passwords if they are forgotten. Using a password manager, such as Bitwarden, is the best way to go. Password managers auto-generate unique passwords anywhere from 10-128 characters.
- **2-Factor Authentication (2FA)**– Setting 2FA on all able accounts is important so that any attempt to log-in to that account will require a second form of authentication. On the chance that someone figures out your password, they will not be able to get access to that account unless you approve the second form of authentication. Many people feel that setting up 2FA through SMS is protecting them, but in actuality it's

the most insecure form of 2FA. Ideally, using a 2FA application such as Authy or Bitwarden is the recommended way.

- **Updated Software and Systems-** Make sure that all of your software and systems are up to date with the latest security patches. This includes both your operating system and any applications that you use. Hackers are constantly finding new ways to exploit vulnerabilities, so it is important to keep your systems patched to protect against the latest threats.
- **Back-up your Data**– Your data should be backed up every 24 hours. This can me done manually or you can use automatic software to set a specific time for it to back up everyday. Having your data backed up protects you in case of system failure or file corruption.

Why Investing in Protection is Worth It
ext Here

As a small business owner, you are probably always looking for ways to cut costs. But when it comes to cybersecurity, skimping on protection can end up costing you a lot more in the long run.

Here are three reasons why investing in cybersecurity is worth it:

1. Data breaches are becoming more common – and more expensive.

- According to IBM’s 2022 data breach report, 83% of businesses will experience a data breach. The average cost of a data breach in the United States is $9.44 million. With more and more businesses falling victim to cyber-attacks, the chances of

your company being hit are increasing.

2. Cybersecurity insurance can help offset the costs of a breach.

- While no insurance policy can completely protect you from the financial fallout of a data breach, having cybersecurity insurance can help mitigate the costs. And, as the risks of cyberattacks continue to rise, so do the premiums for this type of coverage.

3. The costs of not investing in cybersecurity can be even higher.

- If your business is hit by a cyber-attack and you don’t have adequate protection in place, the costs can be devastating. Not only will you have to deal with the direct costs of the attack, such as data recovery and reputational damage, but you may also face legal action if your customers’ data is compromised.

So, while investing in cybersecurity may seem like an expense you can’t afford, the truth is that not investing can end up costing you even more.

How to Prepare for the Future of Cybersecurity

As the world becomes more and more digital, cybersecurity will become an increasingly important issue for businesses of all sizes. Small businesses are especially vulnerable to cyber attacks, which can have a devastating impact on their operations and bottom line.

Here’s what you need to know about the future of cybersecurity and how to prepare for it: Cybersecurity threats are

constantly evolving, so it’s important to stay up-to-date on the latest trends and developments. One of the biggest challenges businesses will face in the future is protecting themselves from sophisticated ransom-ware attacks. These attacks can encrypt your data and demand a ransom for the decryption key, which can be very costly. The best way to protect your business from ransomware and other cyber threats is to invest in a comprehensive cybersecurity solution. This should include robust monitoring software, firewalls, and user education. By taking these steps, you can help ensure that your business is prepared for whatever the future of cybersecurity holds.

As a small business owner it is important to be aware of the risks of cyber-attacks and take steps to protect your business. There are many resources available to help you understand and implement cybersecurity best practices. By being proactive and informed, you can help keep your business safe..