

Cybersecurity: The Basics for Small Businesses

What Is Cybersecurity?

Reliance on the incredible advancements in technology translates to unprecedented conveniences and greater efficiency for today's small businesses, but it also means new vulnerabilities.

Your company's private information, assets and customer data now have the potential to be hijacked and accessed by bad actors in unique and ever-evolving ways.

For many small business owners, unless tech savvy and on top of the latest threats, this is often coupled with the fact that you're in what can sometimes be an intimidating and confusing terrain – the digital world. Cybersecurity is now one of the best prevention tools for avoiding headaches and even disaster for your small business.

Cybersecurity is the overarching term for a variety of methods used to protect your digital information.

Cybersecurity Has Three Major Objectives

1. **Confidentiality** (only authorized users have data access),
2. **Integrity** (trustworthiness and veracity of data)
3. **Availability** (accessible data where and when users need it), otherwise known as the CIA Triad.

These three pillars are the guiding framework for protecting your digital information, and what directs any IT company when considering a small business's specific cybersecurity needs.

Furthermore, there are several areas to think about, much of it focused on prevention, when considering a business's cybersecurity:

Network Security

A layered approach designed to protect your computer network from targeted attacks or malware.

Application Security

Keeps software and devices secure. Ideally, security should be built into the initial design of all software and applications.

Information Security

Protects data while it's both stored and en-route.

Operational Security

Secures data during all processes, permissions and procedures

Disaster Recovery and Business Continuity

Response to a breach. Disaster Recovery is how a business restores operation and information in order to return to the same capacity as prior to the incident.

Business Continuity is how an organization runs while trying to operate without certain resources due to the attack.

End-user Education

Teaching users how to avoid accidentally triggering an attack by helping them learn to identify suspicious email attacks, USB drives, and more.

Why Do Small Businesses Need Cybersecurity?

Too many small businesses have a false sense of security due to relying on a comfortable feeling of anonymity, as compared to a large company.

Unfortunately, attackers are increasingly automating attacks that can harm thousands of small businesses at once no matter how "anonymous" you think your company might be.

In reality, cyber-attacks are more common for small businesses than large companies. About 47% of small businesses experience an attack each year (HISCOX). The main reason being that most small businesses generally don't have the time and resources of a larger company at their disposal, leaving them more susceptible to an attack.

Small businesses normally don't have the security infrastructure of a large company, but still have data cyber criminals desire, and cyber criminals are well aware of this vulnerability.

What Are The Risks Associated With Cybersecurity in Small Businesses?

For a small business, the consequences are also often greater. Cyber-attacks can have devastating consequences on a small business. Leading to loss of money, trust, reputation, clients, and the list goes on.

In fact, many small businesses are unable to survive an attack. 60% of small businesses that are victims go out of business within six months (Denver Post). Additionally, the average financial cost to a small business is not minor at \$25,612 (HISCOX).

Cybersecurity Tips for Small Businesses

With these consequences in mind, it's important to consider any step you can take to increase your [cybersecurity](#).

Some general steps include keeping your software and operating system updated as that ensures the most recent security patches, installing anti-virus software, using strong passwords, avoiding opening any unusual attachments or links, and avoiding using unsecure WiFi in public places.

Finally, consider using some of your budget to invest in professional cyber security guidance, installation and training from a reputable IT company.

In today's tech landscape, for a small business to grow and thrive, cybersecurity is essential to protecting its future.

Is Your Business Protected? Dive into Cybersecurity Today

Ascertaining security needs and potential vulnerabilities in order to provide paramount protection is critical. Keeping your data and your clients' data safe is of the utmost importance. Rest assured that we diligently keep informed of the latest threats in order to prepare for anything to come. If an attack occurs, we quickly get you back up and running with as little damage as possible.

Security matters for everyone – and your data can be compromised at any time. Can your business bounce back?

Reach out today for a complimentary cyber security analysis. Our team will identify weak spots and make recommendations to protect your business.

