What is Cybersecurity?

CLEARTECH GROUP
IT Solutions for Business

In this tipsheet we are diving into the essential realm of cybersecurity in our digital age. In an increasingly digital world, it's so important to understand what cybersecurity is and why it matters. Without proper understanding, this may cause serious data breaches.

Additionally, the occurrence of security data breaches has surged by over threefold from 2013 to 2022, resulting in the compromise of a staggering 2.6 billion personal records in the last two years alone. Regrettably, this concerning trend has persisted and further escalated in 2023.

Thus, we are going to be breaking it down for you by explaining what cybersecurity is, the different types of cybersecurity and a simple list of ways to protect yourself against an attack.

So, what is cybersecurity? In simple terms, it's the practice of protecting your digital systems, networks, and data from theft, damage, or unauthorized access. Think of it as a security guard for your online world.

You might be pondering, " Why does cybersecurity matter to me?"

Well, here are a few of the many key reasons why cybersecurity matters:

Data breaches:

Scammers target businesses to steal extensive personal data, facilitating identity theft or lucrative black-market transactions. In the initial eight months of 2023, over 360 million people experienced the repercussions of data breaches in corporate and institutional contexts.

Safe Computing:

While internet security software is essential, it can't thwart all threats alone. Combining robust software with a well-informed user is key to a secure online experience.

Data Protection:

Cybersecurity shields your personal, business, and sensitive data from malicious hackers.

Privacy:

It preserves your online privacy by shielding your activities from prying eyes. Remember, even mundane online actions can be exploited by cybercriminals.

Business Security:

In the corporate world, it's indispensable for protecting proprietary information, financial records, and customer data.

National Security:

Cyberattacks can disrupt critical infrastructure and government operations, posing a national security risk.

Types of cybersecurity threats

That said, the digital realm harbors a multitude of threats, many of which often go unnoticed. In 2023, a heightened cybersecurity activity showed a perpetual struggle between security professionals and adversaries amid a dynamic landscape of cyber threats. Understanding these threats are vital to your business and personal safety. Some of the most common threats are:

- Malware

- Phishing

- Denial of Service (DoS) Attacks

- Social Engineering (Visuals: Illustrate a social engineering scenario)

- Hacking

- Insider Threats: Zero-Day Vulnerabilities

These are all very important things you should know about, if you want to learn more about these threats here's a link to our blog "Exploring the Most Common Types of Cyberthreats".

Preventing cyber-attacks

Now, onto the pressing question, "How can I protect myself or my business from these threats?" Here are fundamental cybersecurity practices you can implement right away:

- Use a Strong Password

- Have a Two-Factor Authentication (2FA) setup

- Regularly update your system

- Set up Firewalls

- Educate Yourself on the topic itself

- And backup Your Data

Now if you want to learn more on how to protect yourself from cyber-attacks here is a link to our tipsheet on "How to Protect Yourself Against Cyber-Attacks".

In conclusion, understanding cybersecurity is crucial. It's not only the responsibility of tech experts; it's something we want our clients and everyone out there to be aware of. By following the best practices and staying informed, you can safeguard yourself, your data, your organization, and contribute to a safer digital environment for all. Take our Free Business Security Assessment now.