What is Cybersecurity? Can you protect yourself?

There are many devices in use today, so many Internet of things (IoT) are in use worldwide that share data and information. At this point, it's impossible to keep track of how many devices are out there and how many people have access to data, and how they use it.

Internet of things refers to a connected network of devices with sensors, software, and other technologies that enable them to exchange data without human intervention. Example: turning off your lights or turning on your music player before you enter your house.

With the advancement in technology use of online platforms for business, payments, and entertainment, it is no surprise that people are concerned about the security of their data and information flying around.

This article will talk about what Cybersecurity is and how to protect data and information from being stolen.

What is Cybersecurity?

Cybersecurity is also known as electronic security, or information technology security, which refers to **the use of technology to protect computers, phones, networks, servers, hardware, and data from external or, in some cases, internal attacks.**

It aims to decrease the danger of cyberattacks, serving as a protective wall to ensure unauthorized persons do not access sensitive information.

That being said, what are the types of Cybersecurity available today?

Types of Cybersecurity

There are different forms of Cybersecurity; they apply to different situations and can be used as deemed fit. They include:

- Cloud security: This is an increasingly acceptable form of securing data. Over time people have discovered it's a great way to store data and information due to enhanced security and private access. Its security can still be kept right by using activity monitoring software to alert any suspicious actions on cloud accounts.

- Application Security: With PCs and mobile devices, different applications are used for business or personal purposes, data and information are stored in these applications. Password, Pin codes, and authorization keys are sensitive information that ought to be kept safe; hence, application security would keep your data safe. The use of encryption services, firewalls and antivirus help to keep your applications secure.

- Network Security: In your organization, restricting access to your network would go a long way in keeping attacks at bay. Keep your secure passwords and extra logins safe and set to reset periodically. Make use of encrypted and monitored network access to increase the security of your networks.

How to protect yourself from Cybercrime

This portion will give you tips and suggestions on protecting your devices, data, and sensitive information from Cybercrime.

- Use Strong and Complex passwords: Don't use short easy guess passwords like date of birth or easily recognizable or detectable passwords. Do not reuse passwords. If you find it difficult to remember your passwords use a password manager.

- Install an Anti-spyware package: A spyware secretly monitors and steals your information and data. It usually does this undetectably, and it's typically difficult to remove. Installing Anti-spyware gives all-around protection by scanning every piece of information and blocking threats or corrupt files.

- Keep browsers, Os and applications updated: Browsers, Operating systems, and applications constantly update their privacy settings and terms. They fix security issues to prevent your phone from being attacked. Ensure to keep them updated; this would protect your device from hackers.

- Secure your network: When setting up your router, ensure to use a secure password to prevent just anyone from connecting and messing up your settings. Keep your settings encrypted.

- Two-factor authentication (TFA): Passwords and codes are good lines of defense against hackers and Cybercrime. On the other hand, two-factor authentications give you a second layer of protection against attacks. With TFA, you input a set of codes sent to you as text or email in addition to your password before logging in.

- Clear Browser History: Give hackers little or no information about you. Clearing your browser history, cache, and cookies leaves hackers handicapped.

These are a few ways to protect your information from hackers and Cybercrime. True, Cybercrime is on the rise. Does that mean you should stop using your devices? No, but you can win this cyber battle by keeping your security tight.

Reference

https://www.ibm.com/topics/cybersecurity

https://www.wrcbtv.com/story/43030122/what-are-the-different-types-of-cyber-security

https://www.itgovernance.co.uk/what-is-cybersecurity

https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html

https://www.oracle.com/in/internet-of-things/what-is-iot/