tech92 INFO SYSTEMS

CYBER & INFORMATION SECURITY

What you should know about Cyber Security and Information Security

How to protect yourself from Cyber Attacks and Information Security Breaches

Difference between Cyber Security & Information Security

The most important part of preparing to protect yourself from a cyber attack or an information security breach is to clearly understand the difference between the two and acquaint yourself with the extent of the impact it may cause to your life.
While both these terms are associated with the security of computer systems and are often used as synonyms, they refer to two distinct things that are not interchangeable.

Cybersecurity can be defined as the defending of computers, servers, mobile devices, electronic systems, networks and data from malicious attacks which threatens both, business organizations and personal devices equally. Cybersecurity includes categories such as network security, application security, information security, operational security and disaster recovery along with business continuity.

Information security involves the prevention of unauthorized access or alteration during the time of storing data or transferring it from one machine to another. The information can be in the form of biometrics, social media profiles, data on mobile phones etc. and therefore, it covers various sectors such as cryptocurrency and online forensics. Information security is created to cover three major objectives: Confidentiality, Integrity and Availability or commonly known as **CIA**.

In simple terms, the difference between Cybersecurity & Information security is

C The ability to protect or defend the use of cyberspace from cyber attacks, attacks from the outside of an organization.

I Protecting the confidentiality, integrity, and availability of data, no matter its form. This includes Physical Security & Conceptual Security.

The Importance of security and staying connected during the Covid-19 pandemic

The Covid-19 pandemic has dramatically altered the way we live. In these times of social distancing and no face-to-face interactions between human beings, the new normal is staying connected using the internet. The internet has emerged as not only the medium of communication and entertainment for people, but has also surfaced as the means of staying employed during these hectic and uncertain times. Along with this new found dependency on technology and the internet for connectivity and online transactions, people should take extra care of securing their personal and confidential data. Cybercriminals are using this chaotic situation to try to obtain sensitive materials and cause major cyber attacks.

While cyber attacks are nothing new, thanks to COVID-19, the threat is more real than ever. According to Forbes, the largest cyber attack in history is predicted to occur in the very near future. **Kaley Childs Karaffa**, Director of Board Engagement at NASDAQ mentions that "Cyber is a full board issue for every organization."
Here are some compelling statistics that prove an increase in cyber attacks due to Covid-19:

Statistics of Cyber Security Impact due to COVID-19

71% of Cyber Professionals reported increased security threats since **COVID-19**

Phishing Attacks related to coronavirus went up **667% in March 2020**

In one month over 2,000 COVID Related scams were **taken down in the UK**

52% of all Cyber Attacks in March 2020 were **finance related**

How can you Prepare Your Business from a Cyber Attack?

The recent cyber attacks on large companies, like Target and Sears in the USA, have raised alarms of the growing threat of cyber crime and cyber attacks on business and individuals. Recent surveys conducted by the Small Business Authority, Symantec, Kaspersky Lab and the National Cybersecurity Alliance suggest that many small business owners are still operating under a false sense of cyber security.

The statistics show that a vast majority of small businesses in the U.S. lack a formal Internet security policy for employees or have very rudimentary cybersecurity measures in place. Very few small businesses have made their computer systems and data hacker proof and nearly 40 percent do not have their data backed up in more than one location.

So how do you prepare your business to defend itself from these imminent cyber attacks during these COVID-19 times? Here are some recommendations that may benefit your business, regardless of the fact if it is a large or a small business, from a cyber attack.

Recommendations for preparing your Business to defend against a Cyber Attack

- Install, use and regularly update antivirus and antispyware software on every computer used in your business.
- Train employees in cyber security principles,.
- Use a firewall for your Internet connection.
- Download and install software updates for your operating systems and applications as they become available.
- Control physical access to your computers and network components.
- Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace make sure it is secure and hidden.
- Require individual user accounts for each employee.
- Limit employee access to data and information and limit authority to install software.
- Regularly change passwords.

Sources:

https://www.americanbar.org/groups/law_practice/resources/cybersecurity_covid19/
https://securityscorecard.com/blog/information-security-versus-cybersecurity
https://www.pipartners.com/covid-19-cyber-security-statistics-40-stats-and-facts-you-cant-ignore/
https://analyticsindiamag.com/difference-between-cybersecurity-information-security/#:~:text=Cybersecurity%20is%20meant%20to%20protect,cyber%20frauds%20and%20law%20enforcement.
https://capcoverage.com/index.php/10-ways-to-prevent-cyber-attacks/
<div>Icons made by Freepik from www.flaticon.com</div>

<div>Icons made by srip from www.flaticon.com</div>