LIS SOLUTIONS MONTHLY NEWSLETTER OCTOBER 2022

WHAT IS CYBERSECURITY?

By IBM.com

"Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization."

"In 2020, the average cost of a data breach was USD 3.86 million globally, and USD 8.64 million in the United States. These costs include the expenses of discovering and responding to the breach, the cost of downtime and lost revenue, and the long-term reputational damage to a business and its brand. Cybercriminals target customers' personally identifiable information (PII) — names, addresses, national identification numbers (e.g., Social Security number in the US, fiscal codes in Italy), and credit card information — and then sell these records in underground digital marketplaces. Compromised PII often leads to a loss of customer trust, the imposition of regulatory fines, and even legal action."

Continue reading article at: **https://www.ibm.com/topics/cybersecurity**

CYBERSECURITY AWARENESS: WHAT IT IS AND HOW TO START

By Jack Koziol, Cassie Bottorff

"Every October is Cybersecurity Awareness Month and is backed by the Cybersecurity & Infrastructure Security Agency (CISA) and National Cyber Security Alliance. Cybersecurity Awareness Month encourages individuals and organizations to own their role in protecting their part of cyberspace."

"Cybersecurity awareness could mean different to your general workforce than it means to technical teams. Management of data, permissions and regulations are topics that your IT team needs to know but aren't necessarily relevant to the rest of your organization. Delivering the appropriate training to each team is vital to building a cybersecurity awareness program that motivates lasting behavior change. However, cybercriminals are constantly finding new ways to achieve the latest defensive tools and technologies, landing themselves in the inboxes and browsers of our employees. Defending against phishing and social engineering attacks ultimately comes down to knowing what you are up against. These attacks can come in several forms, but the most common are phishing emails that ask you for usernames, passwords, and personally identifiable information (PII). A good rule of thumb is to have healthy skepticism whenever an email asks for personal information, especially emails from an unexpected sender."

Continue reading article at: **https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/**

WHAT IS PHISHING?

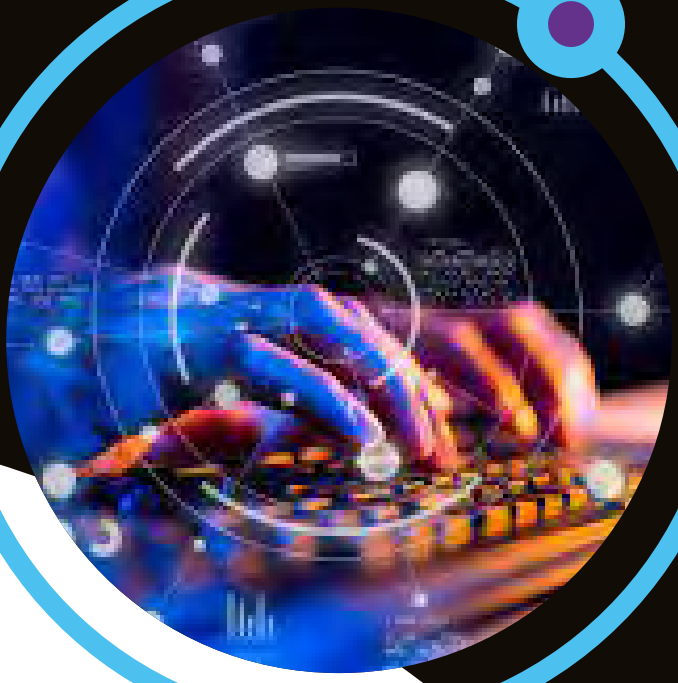
By Henry Sandercock

"Phishing is a type of scam that involves emails, text messages (smishing), social media messages and/or phone calls. Criminals use this type of scam to try to trick people into giving them money or sensitive personal details, like passwords."

"This type of scam works in several different ways, but the main method involves sending links or attachments via email. If clicked on, these links will download malware (software that allows your device to be hacked)."

"Another form of phishing is a message that persuades you to send over sensitive information, including: passwords, card details or intellectual property. These messages may be written in a formal style, or may come from someone posing as a well-known company."

Continue reading article at: **https://www.nationalworld.com/news/uk/what-is-phishing-meaning-of-email-scam-term-what-is-spear-phishing-online-malware-attacks-explained-3846727**



WHY YOU NEED STRONG PASSWORDS

By The Cybersecurity & Infrastructure Security Agency

"You probably use personal identification numbers (PINs), passwords, or passphrases every day: from getting money from the ATM or using your debit card in a store, to logging in to your email or into an online retailer. Tracking all of the number, letter, and word combinations may be frustrating, but these protections are important because adversaries represent a real threat to your personal information. Often, an attack is not specifically about your account, but about using the access to your information to launch a larger attack."

"One of the best ways to protect information or physical property is to ensure that only authorized people have access to this information. Verifying that those requesting access are the people they claim to be is the next step. This authentication process is more important and more difficult in the cyber world. Passwords are the most common means of authentication, but only work if they are complex and confidential. Many systems and services have been successfully breached because of non-secure and inadequate passwords. Once a system is compromised, it is open to exploitation by other unwanted sources."

Don't Forget Security Basics

- Keep your operating system, browser, and other software up to date.
- Use and maintain antivirus software and a firewall.
- Regularly scan your computer for spyware. (Some antivirus programs incorporate spyware detection.)
- Use caution with email attachments and untrusted links.
- Watch for suspicious activity on your accounts.

Continue reading article at: **https://www.cisa.gov/uscert/ncas/tips/ST04-002**