LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

FEBRUARY 2023

SECURITY AWARENESS

No matter what is happening in the world, security awareness is always our priority. COVID-19 changed the way many people work and travel. LIS Security has proudly provided security awareness products and services in the pre- and post-COVID-19 working environment. This has included creating structure, protocols, and virtual tools for onsite work, remote work, telework, and hybrid work situations. LIS Security and staff have supported our clients and employees, regardless of their work location, by making security awareness products easily accessible as well as by participating in multiple monthly security awareness initiatives.

It is important to always remember that the scope of threats to U.S. security can range from counterintelligence to insider threats, to cybersecurity incidents such as phishing emails, ransomware, and cyber-attacks. Successful organizations enhance their security postures by developing strong and active security education and training programs. These programs should provide policies, guidance, training, and awareness to the workforce regarding security requirements and best practices.

SECURITY TIP: To protect your information, use unique passwords for each device and keep all passwords in a secure location.

While working or traveling abroad, ensure that you take security awareness seriously and to not be complacent. Individuals of all types have been targeted by foreign adversaries. People can be targeted in crowds, restaurants, airports, and hotels. Have a high level of situational awareness and keep alert of questions that may trigger suspicious activity or concern. If you are ever a victim of such activity, you are to report the details to your LIS Security immediately at **security@lissol.com**.

SECURITY TIP: When traveling, make sure you stay safe, especially overseas! Download the CDSE's foreign travel briefing for additional tips on how to keep yourself, and those around you, safe.

NOTE: When traveling, you must keep your computer with you. Never check this equipment with your baggage.

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

FROM SPANNING.COM

CYBERSECURITY AWARENESS: DEFINITION, IMPORTANCE, PURPOSE AND CHALLENGES

"Cybersecurity awareness is an ongoing process of educating and training employees about the threats that lurk in cyberspace, how to prevent such threats and what they must do in the event of a security incident."

"What is the purpose of cybersecurity awareness training?"

"Cybercriminals are constantly evolving and devising new methods to exploit vulnerabilities to steal valuable data from businesses. Additionally, they look to exploit human behavior and emotions. It is no surprise social engineering attacks like phishing, spear phishing, business email compromise (BEC), etc., are so successful."

"Well-educated and trained employees can quickly identify these threats, which can significantly reduce the risk of cybersecurity incidents and help prevent data breaches. Security awareness training not only helps stop threat actors in their tracks, but also promotes an organizational culture that is focused on heightened security."

At LIS, we recognize that cybersecurity awareness training is a necessity for the survival of our organization.

Read the Full Article Here: **https://spanning.com/blog/cybersecurity-awareness/**

FROM THE CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

4 THINGS YOU CAN DO TO INCREASE YOUR CYBERSECURITY

Think Before You Click: Recognize and Report Phishing: If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.

Update Your Software: Don't delay -- If you see a software update notification, act promptly. Better yet, turn on automatic updates.

Use Strong Passwords: Use passwords that are long, unique, and randomly generated. Use password managers to generate and remember different, complex passwords for each of your accounts. A passwords manager will encrypt passwords securing them for you!

Enable Multi-Factor Authentication: You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.

Read the Full Article Here: **https://www.cisa.gov/cybersecurity-awareness-month**

LIS IT SECURITY AWARENESS REQUIREMENT

Portable equipment including laptops, data storage devices such as memory sticks, external hard drives, floppy, and Zip disks should not be left unattended. The data you work with is extremely confidential & must be kept secure. Like confidential documents, IT equipment must be kept secure at our office, a client's office, or on the job site. Your laptop should be either logged out or "locked" in Microsoft Windows whenever you are not actively using it. IT Equipment must be secured each night and should not be left unattended in our office outside of normal business hours. If you do not take it with you in the evening, it should be placed in a locked drawer or cabinet in your office.