LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

JANUARY 2024

WELCOME TO 2024!!!

As we say goodbye to 2023, and we head into the new year, security awareness, education, and training should be taken seriously. This is especially true during this time of year when people perform unofficial foreign travel to tourist destinations or to see loved ones.

While abroad, it is easy to be complacent, enjoy the scenery, and live in the moment. However, vulnerabilities, risks, and threats are very real and can happen anywhere, at any time, with no warning. You are the first line of defense, and it is up to you to secure yourself and your assets.

Unofficial foreign travel should be reported to your security personnel a minimum of 30 days before leaving the country. It is important to provide your security personnel with critical details such as information on where you are going, whom you are visiting, and the purpose of the visit. Your security professionals will provide you with a security briefing on the dos and don'ts and where to locate a U.S. Embassy. Finally, upon your return, you will be debriefed and asked to provide details regarding any suspicious activities you witnessed.

As you are well aware, cyber attacks are becoming more common going into the new year. Adversaries work constantly to obtain personal data, sensitive information, or classified material and sell it on the black market for capital gain. Adversaries are anyone who seeks to harm you and your organization. Adversaries may include insiders from your own organization, hackers, cybercriminals, terrorists, members of organized crime, or foreign intelligence entities.

The most common cyber-attacks adversaries use are as follows:

- Phishing
- Malicious code
- Weak and default passwords
- Unpatched or outdated software vulnerability
- Removable Media

Countermeasures:

1. Watch out for phishing and spear phishing and delete suspicious e-mails.
2. Block malicious links/IP addresses and stay current with all operating system service packs and software patches.
3. Strong passwords consist of combined letters, numbers, and special characters. Do not write down your password. Instead, memorize it and change the password according to your organization's policy.
4. Do not rely on firewalls to protect against all attacks and report intrusion attempts.
5. Do not use flash media unless operationally necessary and government-owned. In addition, do not use any personally owned/non-government removable flash media on DoD systems.

Read the Security News article below at your leisure: Rech, F. (n.d.). Preventing employees from becoming the gateway for cyberattacks. MSN. https://www.msn.com/en-us/money/smallbusiness/preventing-employees-from-becoming-the-gateway-for-cyberattacks/ar-AA1hjXsf?ocid=entnewsntp&cvid=0a8d858fcc51454f99689900b34e5890&ei=19

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com