LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

OCTOBER 2023

CYBERSECURITY AWARENESS MONTH

Per the Cybersecurity & Infrastructure Security Agency (CISA) "Since 2004, the President of the United States and Congress have declared the month of October to be Cybersecurity Awareness Month, a dedicated month for the public and private sectors, and tribal communities to work together to raise awareness about the importance of cybersecurity."

This October, LIS would like to bring awareness and perspective to Cybersecurity. The impact of the Internet is immeasurable. It has seamlessly integrated into our economy, become a cornerstone of our national security, and fundamentally transformed our daily lives. Nothing in human history has ushered in change at such an unprecedented pace.

Yet, amid the many advantages and capabilities that the Internet brings, there exists an undeniable threat — one we must confront head-on.

During the inception of the Internet, it seemed like the stuff of science fiction to envision worst-case scenarios: hackers and adversaries actively plotting to disable critical infrastructure, infiltrate defense systems, access personal or proprietary information, and extort millions of dollars from industry. Today, these threats are no longer outside the realm of possibility.

The responsibility for safeguarding our collective interests' rests with each one of us. You are the first line of defense!

Are you prepared to do your part? Here is important information to help you be aware of and prevent possible Cybersecurity threats.

The Threat:

- Insiders
- Hackers
- Cyber Criminals
- Terrorists
- Organized Crime
- Foreign Intelligence Entities

The Target:

- Sensitive company documents and proprietary information
- Export controlled/classified information and technology
- Information on DoD-funded contracts
- Sensitive technological specification documents
- Users' login IDs and passwords
- Personal Identifying Information (SSN, date of birth, address)
- Contact rosters and phone directories

CYBERSECURITY AWARENESS MONTH

What do adversaries do with the information they collect?

Once a Cybersecurity adversary gains access to stolen information, the potential for harm is endless.

At its most basic level, adversaries may exploit stolen data to surveil and understand your activities, gaining insights into your intentions and vulnerabilities. However, their objectives extend far beyond mere observation.

Some adversaries leverage stolen information to advance the interests of their affiliated nations or other entities by reverse-engineering infrastructure or programs. This clandestine appropriation of research and development represents an alarming consequence.

In doing so, foreign nations can amass savings in the order of millions, and sometimes billions, of dollars. They capitalize on the extensive investments that the United States has dedicated to research and development over the years. In an instant, the U.S. strategic and competitive edge can be gone.

Countermeasures:

- Watch out for phishing and spear phishing efforts
- Delete suspicious e-mails
- Report any potential incidents to your LIS Security Professionals at: **security@lissol.com** & **itsupport@lissol.com**
- Do Not Open suspicious e-mails
- Do Not Click on suspicious links or attachments in e-mails
- Do Not Call phone telephone numbers provided in suspicious e-mails
- Do Not Disclose any information
- Block malicious links / IP addresses
- Block all unnecessary ports at the Firewall and Host
- Disable unused protocols and services
- Stay current with all operating system service packs and software patches
- When creating a password,
- do not use personal information
- do not use common phrases or words
- do not write down your password, memorize it
- change password according to your organization's policy
- do not save your passwords or login credentials in your browser
- NEVER SHARE YOUR PASSWORD

At your convenience, please read: Burt, A. (2023, May 16). The Digital World Is Changing Rapidly. Your Cybersecurity Needs to Keep Up. **https://hbr.org/2023/05/the-digital-world-is-changing-rapidly-your-cybersecurity-needs-to-keep-up**