LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

OCTOBER 2025

CYBERSECURITY AWARENESS

Who is attacking us and how are they doing it?

Our adversaries may target you with common types of cyber-attacks that result in the loss of U.S. defense-related information and technology.

- **Phishing:** A scam that puts your personal information and your organization's information at risk. Phishing often uses e-mail or text messaging to deceive you into disclosing personal information.
- **Malicious Code:** Software that does damage and/or creates unwanted behaviors. Our adversaries embed malicious code into links which, once selected, download that code to the user's computer and network.
- **Weak and Default Passwords:** Adversaries can easily gain access to our computers and networks using legitimate login credentials if they are easy to guess.

Use these countermeasures to guard against adversaries

- Watch out for phishing and spear phishing attempts
- Report suspicious e-mails
- Contact your system security point of contact with any questions
- Report any potential incidents
- Look for digital signatures
- Use caution when opening e-mail
- Stay current with all operating system service packs and software patches
- Install and maintain antivirus software
- Install and enable a firewall
- Make password too complex to crack— do not use personal information, common phrases, or dictionary words
- NEVER SHARE YOUR PASSWORD WITH ANYONE

Do not

- Open suspicious e-mails
- Click on suspicious links or attachments in e-mails
- Call telephone numbers provided in suspicious e-mails
- Disclose any information

LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

How to identify suspicious emails

In order to identify suspicious emails, it helps to know their origins. Suspicious emails can come from anywhere in the world. They may come directly from a foreign country that intends to use the requested item, or they may come from a third-party. Suspicious emails may even come from a front company located in the United States.

- **Direct Request:** Direct request emails come directly from a foreign country but are often altered to disguise the actual end use or end user. Senders hope that the email will appear legitimate and that the U.S. company will overlook any discrepancies.
- **Third-Party Request:** Third-party request emails use purchasers located outside of the requesting country. Senders hope that the third-party will complete a transaction with the U.S. company and then illegally ship the items to the end-using country.
- **Domestic Front Company Request:** A front company is a business entity that is established, used, or co-opted for an illicit purpose. The management, control, influence, or criminal activities of the front company are directed by a hidden or disguised end user.

Reporting requirements

You are the first line of defense against cyber threats! It is essential you report any incident or behavior that may be related to the potential compromise of classified information or the inappropriate disclosure of sensitive unclassified information, including those listed here, to your facility security officer or security point of contact at **security@lissol.com**

Articles to read at your leisure:

- **Cybersecurity and Infrastructure Security Agency.** (2025, June 30). *Joint statement from CISA, FBI, DC3 and NSA on potential targeted cyber activity against U.S. critical infrastructure by Iran.* **https://www.cisa.gov/news-events/news/joint-statement-cisa-fbi-dc3-and-nsa-potential-targeted-cyber-activity-against-us-critical**
- **National Security Agency.** (2025, May 22). *NSA's AISC releases joint guidance on the risks and best practices in AI data security.* **https://www.nsa.gov/Press Room/Press Releases Statements/Press Release View/Article/4192332/nsas aisc releases joint guidance on the risks and best practices in ai data se/**
- **United States Department of Justice.** (2025, July 25). *Serial cyberstalker who terrorized women for 16 years sentenced to nine years in prison. U.S. Attorney's Office, District of Massachusetts.* **https://www.justice.gov/usao-ma/pr/serial-cyberstalker-who-terrorized-women-16-years-sentenced-nine-years-prison**