LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

MARCH 2023

THE ONSITE AND HOME OFFICES:

SECURING THE CHANGING WORK ENVIRONMENT

LIS Solutions is relocating its headquarters to a state-of-the-art facility in Chantilly, Virginia this March. What does that mean for LIS Employees from a security perspective? It is an opportunity to make sure that everyone follows security awareness, risk management, and all safety requirements that pertain to teleworking or working in an office space. Now is a great time to remind everyone about the protocols and resources available to all LIS employees.

Onsite Work

As LIS employees return to onsite offices, you are required to follow all facility and industrial security requirements per DCSA and the National Industrial Security Program Operating Manuel (NISPOM). Recognizing unusual behaviors is crucial to your safety when you are in an unfamiliar environment, like at a new office facility. The OPSEC awareness course provides information on protecting unclassified information about operations and personal information.

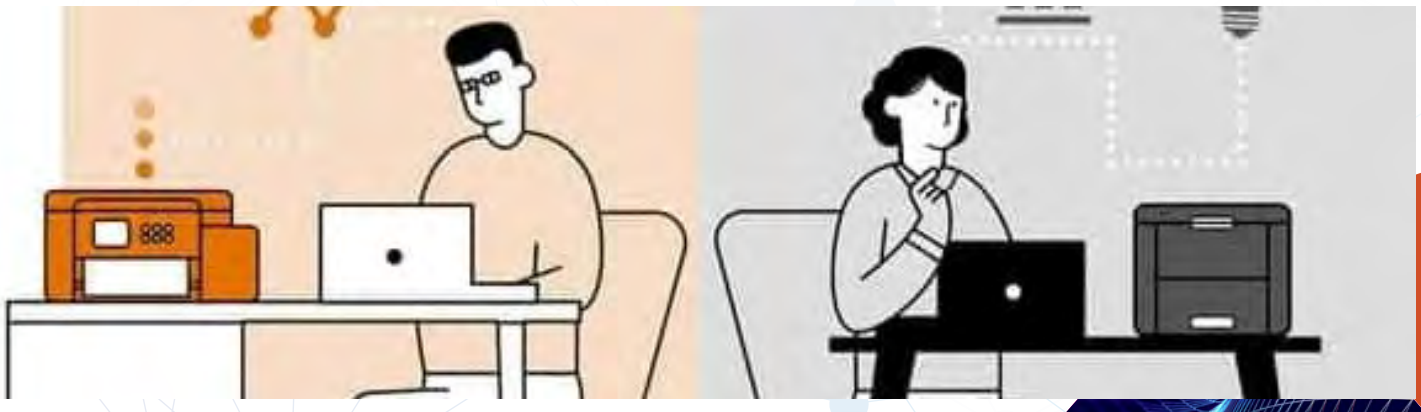
Onsite Resource: OPSEC Awareness for Military Members, DOD Employees, and Contractors (usalearning.gov): **https://securityawareness.usalearning.gov/opsec/index.htm**

Teleworking

Remote work allows people to work more productively from home. However, it can increase the risk of cyber threats such as malware and phishing attempts. CDSE has tools to raise awareness about cybersecurity and prepare you to combat these threats. CDSE also has several eLearning courses on combatting cyber threats, such as "Cybersecurity Awareness" and "Phishing Awareness," which can be accessed through the toolkit.

Teleworking Resource: https://public.cyber.mil/training/cyber-awareness-challenge/

If you have any questions about protocols or access to resources, contact your LIS Security team at **security@lissol.com.**



LIS Solutions
Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

TIPS FOR SECURING ONSITE OFFICE SPACES

Even with extra security layers in place in onsite offices, we must all be diligent in our efforts to secure our devices and networks.

1. Make sure you update your software. Ensure you program your operating system and security software to update automatically. Updates may contain important security upgrades for recent viruses and attacks. Most updates allow you to schedule these updates after business hours or at a more convenient time.
2. Install security software. Install security software on your business computers and devices to help prevent infection. Make sure the software includes anti-virus, anti-spyware, and anti-spam filters. Malware or viruses can infect your computers, laptops, and mobile devices.
3. Set up a firewall. A firewall is a piece of software or hardware that sits between your computer and the internet. It acts as the gatekeeper for all incoming and outgoing traffic.
4. Turn on your spam filters. Use spam filters to reduce the amount of spam and phishing emails that your business receives. Spam and phishing emails can be used to infect your computer with viruses or malware or steal your confidential information. If you receive spam or phishing emails, the best thing to do is delete them. Applying a spam filter will help reduce the chance of you or your employees opening a spam or dishonest email by accident.

It is all of our responsibility to keep our network and devices secure.

TIPS FOR SECURING HOME OFFICE SPACES

Onsite and home offices have many of the same security issues. However, home offices are often at more risk as they:

1. Often use the IT equipment for personal interests which tends to include gaming, video, music, online stores, dating sites, and other sites which are often less secure and frequently prowled by those seeking to gain access to personal and financial data.
2. Home equipment is often shared by other family members who may not be as aware of the dangers and therefore may not be as cautious.
3. Home Wi-Fi & Internet access is often not set up securely. Unless additional security devices or services are purchased, installed, and properly configured, it is much easier for perpetrators to gain access to the home network and computer(s). Even though many Internet Providers (ISPs) and Wi-Fi equipment have some security features such as Firewalls, they are often not activated or configured to block anything and are not as robust as corporate-level devices/services.
4. If perpetrators gain access to a person's home office network, and the home user accesses company sites from that network or device, that action could potentially infect the entire company network and computers. Typical access points include OneDrive, SharePoint, Dropbox, or other file-sharing sites or Remote Desktop services.

If you are accessing company resources, it is best to only use company-supplied, securely-configured computers. Personal and company data (including email) should always be kept separate, and users should immediately inform company IT professionals of any unusual activity, odd emails, virus attempt warnings, etc.

Don't forget to think about all the devices in your home that connect to the internet: your desktop, laptop, tablet, printer, cell phone, and more. Endpoint security is all about securing these access points to prevent malware and other harmful code from getting in. Properly secure your devices, frequently change passwords, and set up multi-factor authentication for accounts.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com