

LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

OCTOBER 2026

NATIONAL CYBERSECURITY AWARENESS MONTH

Cybersecurity is not solely the responsibility of the IT or Security departments. Every employee who uses company systems, handles information, communicates by email, or accesses company resources plays an important role in protecting our organization.

Cyber threats continue to evolve, but many successful attacks begin with something simple: a person clicking a link, opening an attachment, providing information, or responding to a convincing request.

This month, we are focusing on the everyday actions each of us can take to reduce cybersecurity risk.

Be Alert for Phishing and Social Engineering

Phishing and social engineering attacks are designed to manipulate people into taking an action that benefits an attacker.

Attackers may attempt to:

- Obtain usernames, passwords, or other credentials
- Trick employees into opening malicious attachments

- Direct employees to fraudulent websites
- Obtain sensitive or company information
- Impersonate executives, coworkers, vendors, or customers
- Create a sense of urgency to prevent the recipient from thinking critically

Common Warning Signs. Before clicking, opening, or responding, stop and ask:

- Does this message make sense?

Look for:

- Unexpected requests for information
- Unusual urgency or pressure
- Suspicious links
- Unexpected attachments
- Requests involving passwords or authentication codes
- Messages that appear to come from someone you know but seem unusual
- Requests to bypass normal business procedures

When in doubt, verify through a trusted communication method before taking action.



LIS
Solutions

Analyze. Inform. Empower.

718-237-8919 • info@lissol.com

Protect Your Credentials

Your credentials are one of the most valuable targets for attackers. Employees should:

- Never share passwords with another person.
- Use strong, unique passwords or passphrases.
- Never reuse company passwords for personal accounts.
- Use Multi-Factor Authentication (MFA) when provided.
- Never approve an MFA request that you did not initiate.
- Never provide authentication codes to another person.

Remember: Security credentials belong to you. Protect them as you would protect a company key.

Think Before You Click

A single click can potentially introduce malware, expose credentials, or provide an attacker with access to company resources. Before selecting a link or opening an attachment:

1. **STOP** - Don't act immediately.
2. **THINK** - Was I expecting this message or file?
3. **VERIFY** - Is the sender and request legitimate?
4. **PROCEED** - Only after you are confident it is safe.

If something appears suspicious, report it rather than taking a chance.

Protect Company and Sensitive Information

Employees may have access to information that must be protected from unauthorized disclosure, modification, or loss. This includes company information as well as information on subject to contractual, regulatory, privacy, security, or customer requirements. Employees should:

- Only access information is required to perform their job responsibilities.
- Share information only with authorized individuals.

- Verify recipients before sending sensitive information.
- Use approved company systems and storage locations.
- Avoid storing company information on unauthorized devices or services.
- Follow established requirements for handling, transmitting, and disposing of sensitive information.

Convenience should never replace security.

Be Careful with Removable Media and External Devices

USB drives and other removable media can introduce cybersecurity risks. Do not connect unknown or unauthorized devices to company systems. Be particularly cautious when:

- You find an unknown USB drive.
- Someone provides an unexpected removable device.
- A device was not issued or approved by the organization.
- A file appears unexpectedly in the removable media.

When in doubt, contact IT or Security before connecting the device.

Secure Your Devices

Your computer and mobile devices provide access to company information and systems. Help protect them by:

- Locking your workstation when stepping away.
- Keeping devices physically secure.
- Installing required security updates and patches.
- Using only approved applications and software.
- Avoiding unauthorized cloud storage or file-sharing services.
- Reporting lost or stolen company equipment immediately.

A secured workstation helps prevent unauthorized access when you are away—even for a few minutes.



LIS
Solutions

Analyze. Inform. Empower.

718-237-8919 • info@lissol.com



Cybersecurity Is Also About Remote Work

Working remotely does not change our responsibility to protect company information. When working outside the office:

- Use approved company systems and connections.
- Protect your screen from unauthorized viewing.
- Avoid conducting sensitive business over unsecured public networks unless using approved protections.
- Do not allow family members or other unauthorized individuals to use company equipment.
- Secure company documents and devices when not in use.
- Follow all organizational requirements for remote access.

The location may change, but our security responsibilities do not.

Report Suspicious Activity

One of the most important cybersecurity actions an employee can take is to **report suspicious activity** promptly. Report situations such as:

- Suspected phishing or social engineering
- Unexpected MFA requests
- Suspicious emails or attachments
- Accidental disclosure of sensitive information
- Lost or stolen company equipment
- Unauthorized access attempts
- Malware or unusual computer behavior
- Suspicious requests for company information
- Any suspected cybersecurity incident

Don't Investigate It Yourself. Employees should not attempt to investigate or confront a suspected attacker.

Recognize → Stop → Report

Early reporting gives the appropriate personnel an opportunity to evaluate the situation and take action before a small issue becomes a larger incident. Cybersecurity does not always require sophisticated technology or complicated procedures. Sometimes the most effective security control is simply taking a moment before you click, respond, share, or approve. Your awareness can prevent an incident. Your actions can protect our people, our customers, our information, and our organization.

***Remember: Security is everyone's responsibility.
STOP. THINK. VERIFY. REPORT.***

Please read/ watch at your own leisure:

- Federal Bureau of Investigation. (n.d.). Cyberbullying, "Cyber Bully Rap," Myron B. Thompson Academy [Video]. U.S. Department of Justice. [FBI video page](#)
- Federal Bureau of Investigation. (2016, March 22). Two from 'Syrian Electronic Army' added to Cyber's Most Wanted. U.S. Department of Justice. [FBI article](#)



LIS
Solutions

Analyze. Inform. Empower.

718-237-8919 • info@lissol.com