Spread the Word & Get Involved

Cybersecurity is a shared responsibility and we each have a role to play.

Americans, including employees here, regularly use the Internet to communicate with colleagues, share vital information, and conduct business. Yet our collective cybersecurity is threatened on a daily basis by online criminals who wish to do us harm.

As we move further into the Information Age, we must recognize our shared responsibility to make cyberspace a more secure environment for ourselves and future generations. There are things you can do right now to protect Americans from online risks by becoming a cybersecurity advocate in your home, office, and community:

• Lead or host a cybersecurity awareness activity in your places of work, school, recreation, or worship.
• Discuss the importance of cybersecurity internally with your colleagues and externally to your organization’s stakeholders—as well as with your friends, families, and members of your communities.
• Get schools and community organizations involved and informed on cybersecurity.
• Blog or post about cybersecurity issues and tips.
• Become a Friend of the Stop.Think.Connect.™ Campaign (www.dhs.gov/stopthinkconnect) to receive cyber tips and resources.
• Sign up for the US-CERT alert system (www.us-cert.gov) to receive alerts with timely information about current security issues and vulnerabilities.
• Download and distribute Stop.Think.Connect. and US-CERT resources to give to your colleagues, family, friends, and communities.

For more cyber tips and resources, visit the Department of Homeland Security’s Stop.Think.Connect.™ Campaign at:

www.dhs.gov/stopthinkconnect
Physical Security Guidance

Monitor and control who is entering your workplace: current employees, former employees, commercial delivery, and service personnel.

Check for identification and ask individuals to identify the purpose of their visit to your workplace.

Report broken doors, windows, and locks to your organization’s or building’s security personnel as soon as possible.

Back up or copy sensitive and critical information and databases.

Store, lock, and inventory your organization’s keys, access cards, uniforms, badges, and vehicles.

Monitor and report suspicious activity in or near your facility’s entry/exit points, loading docks, parking areas, garages, and immediate vicinity.

Report suspicious packages to your local police. DO NOT OPEN or TOUCH!

Shred or destroy all documents that contain sensitive personal or organizational information that is no longer needed.

Keep an inventory of your most critical equipment, hardware, and software.

Store and lock your personal items such as wallets, purses, and identification when not in use.

Cybersecurity Guidance

Employees

- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do NOT give any of your usernames, passwords, or other computer/website access codes to anyone.
- Do NOT open emails, links, or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization’s network without permission from your IT department.
- Make electronic and physical back-ups or copies of all your important work.
- Report all suspicious or unusual problems with your computer to your IT department.

Leadership & IT Professionals

- Implement Defense-in-Depth: a layered defense strategy includes technical, organizational, and operational controls.
- Establish clear policies and procedures for employee use of your organization’s information technologies.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your system’s anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer’s default passwords on all of your software.
- Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your system’s anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer’s default passwords on all of your software.
- Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your system’s anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer’s default passwords on all of your software.
- Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your system’s anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer’s default passwords on all of your software.
- Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.

Cyber Incidents

System Failure or Disruption: Has your system or website’s availability been disrupted? Are your employees, customers, suppliers, or partners unable to access your system or website? Has your service been denied to its users?

Suspicious Questioning: Are you aware of anyone attempting to gain information in person, by phone, mail, email, etc., regarding the configuration and/or cybersecurity posture of your website, network, software, or hardware?

Unauthorized Access: Are you aware of anyone attempting (either failed or successful) to gain unauthorized access to your system or data?

Unauthorized Changes or Additions: Has anyone made unauthorized changes or additions to your system’s hardware, firmware, or software characteristics without your IT department’s knowledge, instruction, or consent?

Suspicious Email: Are you aware of anyone in your organization receiving suspicious emails that include unsolicited attachments and/or requests for sensitive personal or organizational information?

Unauthorized Use: Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?