

# Protect Your Workplace

## 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.

Report a computer or network vulnerability to the U.S. Computer Emergency Readiness Team;

**Incident Hotline: 1-888-282-0870**

**[www.US-CERT.gov](http://www.US-CERT.gov)**



**Homeland  
Security**

For more cyber tips and resources, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign at:  
[www.dhs.gov/stopthinkconnect](http://www.dhs.gov/stopthinkconnect)



STOP | THINK | CONNECT™

# Protect Your Workplace

## 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.

Call your local police department to report a suspicious person, vehicle, or activity in or near your workplace.

( \_\_\_ ) \_\_\_ - \_\_\_

**Call 911 if there is an emergency or immediate threat.**



Homeland  
Security

For more cyber tips and resources, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign at:  
[www.dhs.gov/stothinkconnect](http://www.dhs.gov/stothinkconnect)



STOP | THINK | CONNECT™

# Report Suspicious 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?

*We encourage you to report any activities that you feel meet these criteria. Note that our policy is to keep any information specific to your site and system confidential unless we receive your permission to release that information. US-CERT has partnered with law enforcement agencies such as the U.S. Secret Service and the Federal Bureau of Investigation to investigate cyber incidents and prosecute cyber criminals.*

**Report an incident to the U.S. Computer Emergency Readiness Team;  
Incident Hotline: 1-888-282-0870 / [www.US-CERT.gov](http://www.US-CERT.gov)**

For more cyber tips and resources, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign at:  
[www.dhs.gov/stothinkconnect](http://www.dhs.gov/stothinkconnect)



**Homeland  
Security**



STOP | THINK | CONNECT™

# Report Suspicious Behavior and Activity

## Surveillance

Are you aware of anyone recording or monitoring activities, taking notes, using cameras, maps, binoculars, etc., near a key facility?

## Deploying Assets

Have you observed abandoned vehicles, stockpiling of suspicious materials, or persons being deployed near a key facility?

## Suspicious Persons

Are you aware of anyone who does not appear to belong in the workplace, neighborhood, business establishment, or near a key facility?

## Suspicious Questioning

Are you aware of anyone attempting to gain information in person, by phone, mail, email, etc., regarding a key facility or its personnel?

## Tests of Security

Are you aware of any attempts to penetrate or test physical security or procedures at a key facility?

## Acquiring Supplies

Are you aware of anyone attempting to improperly acquire explosives, weapons, ammunitions, dangerous chemicals, uniforms, badges, flight manuals, access cards, or identification to a key facility? Are you aware of anyone attempting to legally obtain items under suspicious circumstances that could be used in a terrorist act?

## Dry Runs

Have you observed any suspicious behavior that appears to be preparation for terrorist activity, such as mapping out routes, playing out scenarios with other people, monitoring key facilities, timing traffic lights and traffic flow, or other suspicious activities?

Call 911 if there is an emergency or immediate threat.  
Submit information electronically at: <https://tips.fbi.gov>

Call the nearest Joint Terrorism Task Force (JTTF) to report suspicious activity or behavior (see below)

Albany (518) 465-7551  
Albuquerque (505) 889-1300  
Anchorage (907) 276-4441  
Atlanta (404) 679-9000  
Baltimore (410) 265-8088  
Birmingham (205) 326-6166  
Boston (617) 742-5533  
Buffalo (716) 856-7800  
Charlotte (704) 377-9200  
Chicago (312) 431-1333  
Cincinnati (513) 421-4310

Cleveland (216) 522-1400  
Columbia (803) 551-4200  
Dallas (972) 559-5000  
Denver (303) 629-7171  
Detroit (313) 965-2323  
El Paso (915) 832-5000  
Honolulu (808) 566-4300  
Houston (713) 693-5000  
Indianapolis (317) 639-3301  
Jackson (601) 948-5000  
Jacksonville (904) 721-1211

Kansas City (816) 512-8200  
Knoxville (865) 544-0751  
Las Vegas (702) 385-1281  
Little Rock (501) 221-9100  
Los Angeles (310) 477-6565  
Louisville (502) 583-3941  
Memphis (901) 747-4300  
Miami (305) 944-9101  
Milwaukee (414) 276-4684  
Minneapolis (612) 376-3200  
Mobile (251) 438-3674  
Newark (973) 792-3000

New Haven (203) 777-6311  
New Orleans (504) 816-3000  
New York City (212) 384-1000  
Norfolk (757) 455-0100  
Oklahoma City (405) 290-7770  
Omaha (402) 493-8688  
Philadelphia (215) 418-4000  
Phoenix (602) 279-5511  
Pittsburgh (412) 432-4000  
Portland (503) 224-4181  
Richmond (804) 261-1044

Sacramento (916) 481-9110  
Salt Lake City (801) 579-1400  
San Antonio (210) 225-6741  
San Diego (858) 565-1255  
San Francisco (415) 553-7400  
San Juan (787) 754-6000  
Seattle (206) 622-0460  
Springfield, IL (217) 522-9675  
St. Louis (314) 231-4324  
Tampa (813) 253-1000  
Washington, DC (202) 278-2000



Homeland Security

For more cyber tips and resources, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign at: [www.dhs.gov/stopthinkconnect](http://www.dhs.gov/stopthinkconnect)



STOP | THINK | CONNECT™

# Protect Your Workplace

## Spread the Word & Get Involved

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](http://www.dhs.gov/stopthinkconnect)) to receive cyber tips and resources.
- Sign up for the US-CERT alert system ([www.us-cert.gov](http://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.

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

For more cyber tips and resources, visit the Department of Homeland Security's Stop.Think.Connect.™ Campaign at:  
[www.dhs.gov/stopthinkconnect](http://www.dhs.gov/stopthinkconnect)



**Homeland  
Security**



STOP | THINK | CONNECT™