

# STOP.THINK.CONNECT.™

## Cybersecurity 101

At home, at work, and at school, our growing dependence on technology demands greater security online. Individuals are our country's first line of defense in guarding against online risks. For this reason, cybersecurity is a shared responsibility, requiring awareness and vigilance from every citizen, community, and country.

Cybersecurity is the protection of computers and computer systems against unauthorized attacks or intrusion.

The Stop.Think.Connect.™ Campaign is a national public awareness effort to guide the nation to a higher level of Internet safety by challenging the American public to be more vigilant about practicing safer online habits. The Stop.Think.Connect. Campaign's overarching goal is to help Americans understand not only the risks that come with using the Internet, but also the importance of practicing safe online behavior.

To understand and practice cybersecurity, individuals must be able to recognize risks, threats, and vulnerabilities that exist online and their impact at a national and individual level.

### CYBER RISKS

- **Who:** Malicious actors intend to cause harm in cyberspace, such as a hacker stealing personal information. Benign actors accidentally cause harm to a network, system, or the Internet, such as an employee who accidentally downloads malware onto their company's network.
- **What:** Malicious actors exploit the anonymity and vulnerabilities of the Internet using methods that range in sophistication from botnets to viruses. Benign actors introduce threats through simple actions that can range from clicking on an unknown link to using a USB drive.
- **When:** It is impossible to predict when a cyber incident will occur.
- **Where:** Cyberspace, often interchanged with "the Internet," is created by and accessible through computer networks that share information and facilitate communication. Unlike the physical world, cyberspace has no boundaries across air, land, sea, and space.
- **Why:** Benign actors unintentionally and often unknowingly cause harm while malicious actors may have a range of motives, including seeking confidential information, money, credit, prestige, or revenge.

There are many risks online, some more serious than others. The majority of cybercriminals are indiscriminate; they target vulnerable computer systems regardless of whether they are part of a government agency, Fortune 500 company, a small business, or belong to a home user.

### CYBER TIPS

No citizen, community, or country is immune to cyber risk, but there are steps you can take to minimize your chances of an incident:

- Set strong passwords, change them regularly, and don't share them with anyone.
- Keep your operating system, browser, and other critical software optimized by installing updates.
- Maintain an open dialogue with your friends, family, and colleagues about Internet safety.
- Use privacy settings and limit the amount of personal information you post online.
- Be cautious about offers online – if it sounds too good to be true, it probably is.

You have the opportunity to join in cybersecurity awareness efforts across the country. If you, your family, or your organization is interested in more information about cybersecurity and Stop.Think.Connect., please visit [www.dhs.gov/stopthinkconnect](http://www.dhs.gov/stopthinkconnect).



Homeland  
Security



STOP | THINK | CONNECT™

# CYBER INCIDENT RESPONSE

## Take Immediate Action

The extent, nature, and timing of cyber incidents are impossible to predict. There may or may not be any warning. Some cyber incidents take a long time (weeks, months, or years) to be discovered and identified. If you are a victim of a cyber incident, follow the steps below to mitigate and recover from the incident.

Immediate Actions	<ul style="list-style-type: none"><li>• Check to make sure the software on all of your systems is up-to-date.</li><li>• Run a scan to make sure your system is not infected or acting suspiciously.</li><li>• If you find a problem, disconnect your device from the Internet and perform a full system restore.</li></ul>
If at Home	<ul style="list-style-type: none"><li>• Disconnect your device (computer, gaming system, tablet, etc.) from the Internet. By removing the Internet connection, you prevent an attacker or virus from being able to access your computer and perform tasks such as locating personal data, manipulating or deleting files, or using your device to attack others.</li><li>• If you have anti-virus software installed on your device, update the virus definitions and perform a manual scan of your entire system. Install all of the appropriate patches to fix known vulnerabilities.</li></ul>
If at Work	<ul style="list-style-type: none"><li>• If you have access to an IT department, contact them immediately. The sooner they can investigate and clean your computer, the less damage to your computer and other computers on the network.</li><li>• If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.</li></ul>
If at a public place (school, library, etc.)	<ul style="list-style-type: none"><li>• Immediately inform a librarian, teacher, or manager in charge. If they have access to an IT department, contact them immediately.</li></ul>

## Report the Incident

After taking immediate action, notify the proper authorities:

- File a report with the local police so there is an official record of the incident.
- Report online crime or fraud to your local [United States Secret Service \(USSS\) Electronic Crimes Task Force](#) or [Internet Crime Complaint Center](#).
- Report identity theft and consumer fraud to the [Federal Trade Commission](#).

## Get Informed & Involved

To be on alert for current cyber news and threats, you can:

- Sign up for the United States Computer Emergency Readiness Team (US-CERT) mailing list to receive the latest cybersecurity information directly to your inbox. Written for home and business users, alerts provide timely information about current security issues and vulnerabilities. [Sign up here.](#)
- Become a *Friend* of the Department of Homeland Security's Stop.Think.Connect. Campaign and receive a monthly newsletter with cybersecurity current events and tips. [Sign up here.](#)



Homeland  
Security



STOP | THINK | CONNECT™