



Army Cybersecurity Awareness Month

What is it?

OCTOBER is Army Cybersecurity Awareness Month, which is an annual campaign to increase awareness of organizational cybersecurity practices and training that will help us improve the overall Army security posture.

This year's Awareness Month theme is "Lethal Keystrokes," leading off with the question, "Were your keystrokes lethal today?" The theme emphasizes individual responsibility for protecting the network and Army against cybersecurity threats that endanger our Soldiers, compromise operations and increase cost significantly in time and resources to remediate.

Why is this important to the Army?

Cyber attacks threaten the Army network and its information every day, putting our operations and people at risk. Strengthening Army cybersecurity is critical to all Army warfighting operations and business functions. Likewise, it is imperative for the Army to make certain that Soldiers, Civilians and contractors are responsible for daily practices that protect information and IT capabilities.

What has the Army done?

In support of Army Cybersecurity Awareness Month, commanders at all levels have been directed to conduct cybersecurity awareness activities based on their FY13/FY14 Information Assurance (IA) Self-Assessments. Commands will address these activities and improved security practices in the following phases:

- Phase 1: Leader Awareness
- Phase 2: Individual Awareness
- Phase 3: Collective Training
- Phase 4: Home/Family Cybersecurity Practices

By 15 November, organizations will complete an After Action Review (AAR) of their activities conducted for the month. Organizations will also complete an Army survey to capture feedback on the value, benefits and continued improvements for Army cybersecurity awareness.

Resources for each phase of Cybersecurity Awareness Month, to include the Army survey, are available on the Army's Information Assurance One-Stop Shop:

<https://informationassurance.us.army.mil>.

What does the Army have planned for the future?

To continue this effort, the Army will hold an annual Cybersecurity Awareness Month. Commands will complete their yearly assessments, conduct mandatory annual IA training, ensure systems are FISMA compliant and continually apply security updates and patches as required.

Throughout the year Commands can continue to access the IA One-Stop Shop for updated cybersecurity information and resources: <https://informationassurance.us.army.mil>.



U.S. ARMY

CYBERSECURITY AWARENESS MONTH

The First Line of Defense is YOU!

The cyber threat facing the Army is pervasive and increasingly sophisticated. Cyber attacks constantly threaten our network, information and personnel. Working together, we all play an essential role in keeping our networks, information and personnel safe from harm.

You Need To Know:	What is it?	What should I do?
Social Engineering	The act of manipulating people into providing sensitive information or performing a desired action. Social engineering can lead to loss of confidential information, systems intrusions and identity theft.	Be suspicious of unsolicited phone calls, emails or individuals asking about organizational or personal information. When submitting personal information, ensure the website is legitimate and starts with HTTPS.
Email Phishing & Spear Phishing	Email-based attacks where the attacker attempts to fool you into taking an action such as clicking a link, opening an attachment by pretending to be a legitimate business or someone you know.	Delete emails you think are a phishing attack. Be suspicious of attachments and links, and only open those you were expecting. Limit the information you post about yourself online.
Fraudulent Websites	Websites that appear legitimate by copying the look of other, well-known sites. These fake websites prey on people who are looking for the lowest price possible by searching the web for products they'd like to buy, and then add words such as "cheapest" or "lowest price." In return, the search engine will present many, even hundreds of websites selling the item, to include the fake sites.	Be wary of unknown stores offering prices dramatically cheaper than anyone else. Look for missing sales or contact information, or different website and email domain names. Shop at trusted online stores that have an established reputation. Monitor your credit card statements to identify suspicious charges.
Theft, Loss or Negligent Disclosure of Information	Loss of control over sensitive and protected data happens when attackers gain unauthorized access to information or when authorized users negligently transfer classified information to a network or computing device with a lower classification.	Always encrypt sensitive information. Do not store or process classified information on any system not approved for classified processing. Review classification levels including hidden data – e.g. notes on PowerPoint slides, images, and recoverable traces of deleted data.
Malware	Software used to perform malicious actions on computing devices, including tablets and smartphones. Attackers' goals can include stealing confidential data, collecting passwords, sending spam emails, or identity theft.	Keep your software up-to-date by enabling automatic updates, install trusted anti-virus software from well-known vendors and be alert for anyone attempting to fool or trick you into infecting your own computer.

10 Tips to Stay Safe Online:

Protect Your System:

- Use anti-virus software.
- Protect home networks with firewalls.
- Password-protect your wireless router and network.
- Regularly download security updates and patches.
- Disconnect from the Internet when not in use.

Protect Yourself:

- Back-up your computer regularly.
- Restrict access to your computer and accounts; sharing has risks.
- Delete email from unknown sources.
- Use hard-to-guess passwords and keep them private.

Protect Your Family:

- Help your family check computer security on a regular basis.

Resource Toolbox:

Cybersecurity resources, including:

- Information on the topics above
- Information on how to protect yourself online
- Access to free security software for Soldiers and civilians
- Cybersecurity training

Available by clicking the Resource Toolbox link from the right hand menu at:

<https://informationassurance.us.army.mil>

