



Collective Cybersecurity Awareness

What is it?

With ever-increasing cyber threats, collective and team training for Army system administrators, cyber professionals, information assurance managers and network owners is critical for managing risk and safeguarding Army networks and information. Incorporating cybersecurity into command exercises, conducting cyber tabletop exercises to test incident response plans and conducting regular network penetration testing provides cybersecurity professionals valuable opportunities to improve the Army security posture.

Why is this important to the Army?

Malicious state actors, hactivists, and insider threats threaten Army networks, systems and critical infrastructure, with the intent to jeopardize warfighting and business operations. Assessing and managing risks to the Army enterprise from these persistent threats demands flexible and adaptive safeguards and security practices. Comprehensive, thorough and reiterative training for leaders and cybersecurity professionals is paramount for protecting Army assets and improving the Army security posture in order to ensure Army operational success.

What has the Army done?

The Army offers numerous training opportunities, both in-residence and online, to train and certify cybersecurity personnel. Network Enterprise Centers provide collective training for leaders and system users at multiple levels. Cybersecurity programs at the Naval Postgraduate School, as well as Army training institutions, such as the Cyber Center of Excellence, address the demand for building a highly skilled cyber workforce. The Army also leverages graduate programs, such as the Information Assurance Scholarship Program and the ARCYBER Scholarship Program, to keep leaders and administrators current and informed on tactics, techniques and procedures for mitigating cyber threats and improving the Army security posture.

What does the Army have planned for the future?

Army commanders and leaders are responsible for incident response planning and execution, as well as contingency operations. Ensuring the continual training of their security professional will help organizations prepare and respond to cyber threats while improving the overall Army security posture.

Army collective training will evolve in anticipation of and response to cyber threats and incidents that put Army networks and information at risk. The Army will continue to monitor and evaluate organizational inspections for those requirements to ensure policies provide safeguards for risk management operational sustainment. Recent revisions to DoD 8570-1, AR 25-1, and AR 25-2 outline the certification and appointment processes for all DoD network users (military, civilian, and contractor), analysts, administrators and managers.

More information, guidance and resources are on the Army Information Assurance One-Stop Shop portal, which is CAC accessible: <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>

