



Individual Cybersecurity Awareness

What is it?

Individual cybersecurity awareness focuses on the individual's understanding of their roles and responsibilities in reducing the occurrence of security incidents that undermine national security and degrade operational capabilities.

Individual awareness allows individuals to review their cybersecurity training, to educate themselves about cybersecurity and to become more aware of cybersecurity and the cyber threats facing the Army, themselves and their family and friends.

Why is this important to the Army?

Cybersecurity is critical to all Army functions. Cyber attacks and user negligence threaten Army networks and information every day, putting Army operations and personnel at risk. Raising individual cybersecurity awareness and enforcing compliance helps improve the Army's cybersecurity posture and reduces the security risk to the Army.

What has the Army done?

In May 2013, the Army published a handbook to provide leaders at all levels the information and tools needed to address cybersecurity challenges and to ensure that all organizations adopt the practices necessary to protect their information and the Army's network (<https://www.milsuite.mil/book/docs/DOC-73030>).

The Army also published the Protect Operational Information Brochure (<https://www.milsuite.mil/book/docs/DOC-159005>) to educate all personnel about operations security and what they can do to reduce cyber risk.

In October 2013, the Army held an Information Assurance/Cybersecurity Awareness Week. This week provided an opportunity to heighten individual and collective knowledge about cybersecurity threats and individuals' roles and responsibilities in protecting the Army.

What does the Army have planned for the future?

The Army will continue this effort by holding an annual Cybersecurity Awareness Month. To maintain access to Army information systems, the Army will continue to require personnel to annually complete their cybersecurity training.

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

