



## Leaders' Responsibility for Cybersecurity Awareness Month

### What is it?

Army Cybersecurity Awareness Month provides leaders the opportunity to better assess and review their organizational cybersecurity awareness, security practices and training that will help them and their people improve the overall Army security posture. Army leaders are ultimately responsible for ensuring that their information systems are protected, and that their people are aware, trained and compliant with policies and procedures. Beyond understanding and awareness of current cyber threats and their impact on the Army, leaders must continually advance and promote vigilant security practices within their organizations to safeguard the integrity of Army networks, systems and information, and protect personal identities.

### Why is this important to the Army?

Cybersecurity is essential for safeguarding all Army operations and everyday business functions. Leaders are vital in reinforcing the responsibility of vigilant security practices among their people to ensure the protection and the confidentiality, integrity and availability of Army information and systems. Leaders must continually promote cybersecurity awareness and training to ensure that all users fully understand their individual and collective responsibilities for protecting Army networks, information and data while enabling warfighting and business operations.

### What has the Army done?

The Army Cybersecurity Awareness Month builds on last year's Army initiatives to increase cybersecurity awareness and improve training. In addition to increasing awareness and reinforcing security policies, in 2013 leaders conducted Information Assurance self-assessments to determine their organizational security posture. From those findings, they developed Plans of Actions and Milestones (POA&M) to address deficiencies in policy compliance and security practices. As part of the continuing effort, the Army provides leader updates on cyber threats, vulnerabilities and operational risks, and the associated responsibilities for leaders and subordinates. These information updates reinforce the need to educate people on proper security procedures and hold individuals accountable for their actions.

### What does the Army have planned for the future?

Army leaders are responsible for organizational cybersecurity programs that assess and manage risk through increased training, situational awareness and compliance with security policies and procedures. At the conclusion of the Army Cybersecurity Awareness Month leaders will complete a survey for the month-long activities. The Army plans to continue cybersecurity awareness throughout FY15 with monthly information sheets designed to reinforce messages for continued Army awareness.

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?   |
|---|--|---|
| <b>Social Engineering</b>                                 | 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.  |
| <b>Email Phishing &amp; Spear Phishing</b>                | 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.  |
| <b>Fraudulent Websites</b>                                | 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.<br><br>Shop at trusted online stores that have an established reputation.<br><br>Monitor your credit card statements to identify suspicious charges. |
| <b>Theft, Loss or Negligent Disclosure of Information</b> | 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.  |
| <b>Malware</b>  | 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>

