



## Home and Family Cybersecurity Awareness

### What is it?

Home and family awareness addresses cybersecurity issues that are unique to the home environment. Remote access and the increasing demand for use of personal mobile devices to access Army systems and information create significant cybersecurity challenges. The safety and security of home/personal systems that access Army networks require the same robust cybersecurity practices as Army information systems, to ensure that the network and data remain protected.

### Why is this important to the Army?

Recent industry research has shown that computers not running proper security software are compromised, on average, within 10 minutes of connecting to the Internet. Compromised home and family systems can impact the Army. The Army mission depends on how safely we access and use systems and information everywhere; each violation is dangerous, costly, and can endanger our warfighters.

### What has the Army done?

The Army recognizes the necessity of remote accessibility for Soldiers and Civilians to access information and data anywhere and anytime. The Army has developed policies that allow Soldiers and Civilians to access Army information from home or a remote location while maintaining the required level of cybersecurity.

To assist with meeting the policy requirements for home and remote use, the Army provides resources to raise awareness among users and improve cybersecurity. Resources available to Soldiers and Civilians include:

- Antivirus software for home use at no cost  
( <https://www.acert.1stiocmd.army.mil/Antivirus/> )
- Telework agreement guidelines  
( <http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage3281.html> )
- 2nd Army Protect Operational Information Brochure:  
( <https://www.milsuite.mil/book/docs/DOC-159005> )

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

As technology advances, the Army will continue to review and update policies, providing a more secure environment for Soldiers and Civilians working from remote locations.

For further information including best practices for home cybersecurity, go to:  
[http://www.nsa.gov/ia/files/factsheets/best\\_practices\\_datasheets.pdf](http://www.nsa.gov/ia/files/factsheets/best_practices_datasheets.pdf)



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.  Shop at trusted online stores that have an established reputation.  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>

