

## Cyber Awareness Challenge Reference Material

# Computer Use

---

### Ethical Use of Your Government Computer

- Don't view or download pornography
- Don't gamble on the Internet
- Don't conduct private business or money-making ventures
- Don't load personal or unauthorized software
- Don't make unauthorized configuration changes
- Only check personal e-mail if your organization allows it
- Don't play games unless allowed by your organization to do so on personal time

### Tips for Peer-to-Peer (P2P) and Unauthorized Software

#### P2P software can:

- Compromise network configurations
- Spread viruses and spyware
- Allow unauthorized access to data

#### To protect information systems:

- Don't use unauthorized peer-to-peer (P2P) software
- Don't illegally download copyrighted programs or material

### Beware of Cookies

A cookie is a text file that a Web server stores on your hard drive. Cookies may pose a security threat, particularly when they save unencrypted personal information. Cookies also may track your activities on the Web.

#### To prevent cookies from being saved to your hard drive:

- Set your browser preferences to prompt you each time a Website wants to store a cookie
- Only accept cookies from reputable, trusted Websites
- Be especially aware of cookies when visiting e-commerce sites or other sites that may ask for credit card or other personal information
- Confirm that site uses an encrypted link
  - Look for "h-t-t-p-s" in the URL name
  - Look for an icon to indicate encryption is functioning

**NOTE:** Not all https sites are legitimate, and there is still a risk to entering your information online.

## Malicious Code Tips

Malicious code can do damage by corrupting files, erasing your hard drive, and/or allowing hackers access. Malicious code includes viruses, Trojan horses, worms, macros, and scripts and can be spread by e-mail attachments, downloading files, and visiting infected Websites.

### To prevent viruses and the download of malicious code:

- Turn off automatic downloading
- Scan all external files before uploading to your computer
- Don't e-mail infected files to anyone
- Don't access Websites in e-mail or popups

## Mobile Code Tips

Mobile code can be malicious code.

### To prevent damage from malicious mobile code:

- Require confirmation before enabling ActiveX or other mobile code technology
- Only allow mobile code to run from your organization or your organization's trusted sites
- Contact your security POC or help desk for assistance, especially with e-mails requesting personal information

## Home Computer Security

### ***Defend Yourself! Keep your identity secure, and prevent identity theft.***

When working at home on an authorized computer, follow these best security practices, derived from the NSA datasheet "Best Practices for Keeping Your Home Network Secure."

- Turn on password feature, create separate accounts for each user, and have them create their own passwords using a strong password creation method
- Install all system security updates, patches, and keep your defenses up to date
- Keep anti-virus software up-to-date
- Regularly scan files for viruses
- Install spyware protection software
- Turn on firewall protection
- Require confirmation before installing mobile code
- Change default logon ID and passwords for operating system and applications
- Regularly back up and securely store your files
- Beware of sudden flashing pop-ups that warn that your computer is infected with a virus: this is a malicious code attack!
- Check the resources page - some agencies may have discounted/free anti-virus software available to their employees