Malicious Code

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. Malicious code can be spread by e-mail attachments, downloading files, and visiting infected websites.

Protecting Against Malicious Code

To prevent viruses and the download of malicious code:

- Scan all external files before uploading to your computer
- Don't e-mail infected files to anyone
- Don't access website links, buttons, and/or graphics in an e-mail or a popup generated by an e-mail message
- For personally-owned devices, research any application and its vulnerabilities before downloading that "app"
- For Government-owned devices, use approved and authorized applications only

Mobile code can be malicious code. To prevent damage from malicious mobile code:

- Only allow mobile code from your organization or your organization's trusted sites to run
- Contact your security Point of Contact (POC) or help desk for assistance, especially with e-mails that request personal information

Best Practices for Home Computer Security

Defend yourself! Keep your identity secure/prevent identity theft.

When working at home on your computer, follow these best security practices, derived from the National Security Agency (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 antivirus 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!

Some agencies may have discounted/free antivirus software available to their employees

- Active DoD military and civilian employees may install antivirus software for home use via the DoD Antivirus Home Use Program
- Contractors are excluded from participating in the DoD Antivirus Home Use Program

E-mail Protection

To prevent the downloading of viruses and other malicious code when checking your e-mail:

- View e-mail in plain text and don't view e-mail in Preview Pane
- Use caution when opening e-mail: Look for digital signatures if your organization uses them. Digitally signed e-mails are more secure.
- Scan all attachments
- If authenticity cannot be confirmed, delete e-mail from senders you do not know
- Don't e-mail infected files to anyone
- Don't access website links, buttons, and/or graphics in an e-mail or a popup generated by an e-mail message

Compressed URLs

Exercise caution with compressed URLs, such as TinyURLs (e.g., https://tinyurl.com/2fcbvy):

- Compressed URLs convert a long URL into a short URL for convenience but may be used to mask malicious intent
- Investigate the destination by using the preview feature to see where the link actually leads
    - Use an Internet search engine to find instructions for previewing a specific compressed URL format (e.g., TinyURL, goo.gl)