October is
National Cybersecurity Awareness Month
"Do Your Part. #BeCyberSmart."

Chapter 3: Protecting Against Malicious Code

What is Malicious Code?

Malicious code is unwanted files or programs that can cause harm to a computer or compromise data stored on a computer. Various classifications of malicious code include viruses, worms, and Trojan horses.

- **Viruses** have the ability to damage or destroy files on a computer system and are spread by sharing an already infected removable media, opening malicious email attachments, and visiting malicious web pages.
- **Worms** are a type of virus that self-propagates from computer to computer. Its functionality is to use all of your computer's resources causing your computer to stop responding.
- **Trojan Horses** are computer programs that are hiding a virus or a potentially damaging program.
- **Malicious data files** are non-executable files—such as a Microsoft Word document, an Adobe PDF, a ZIP file, or an image file—that exploits weaknesses in the software program used to open it.

How can you protect yourself against Malicious Code?

- **Install and maintain antivirus software.** Antivirus software recognizes malware and protects your computer against it.
- **Use caution with links and attachments.** Take appropriate precautions when using email and web browsers to reduce the risk of an infection.
- **Change your passwords.** If you believe your computer is infected, change your passwords.
- **Keep software updated.** Install software patches on your computer so attackers do not take advantage of known vulnerabilities.
- **Back up data.** Regularly back up your documents, photos, and important email messages to the cloud or to an external hard drive.
- **Install or enable a firewall.** Firewalls can prevent some types of infection by blocking malicious traffic before it enters your computer.

Sources: www.cisa.com