West Virginia Executive Branch
Privacy Tip

What Does That Mean?
Your Dictionary of Cyber-speak

We hear the words “phishing”, “malware” and “ransomware” a lot these days, but what do they mean? Here are some commonly used cyber-terms, collected from various sources around the Web:

Adware: A type of malware that bombards you with endless ads and pop-up windows that could potentially be dangerous for your device.

Backdoor: A program that gives a cybercriminal unauthorized remote access to a computer system by exploiting security vulnerabilities.

Hacking: When someone breaks into a computer or network.

Hijackware: Malware that infects an internet browser to display advertising and/or redirect the user to malicious or spammy websites.

Hoax: Usually urban legends or chain letters that warn of non-existent threats.

Keylogger: Spyware that records keystrokes, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

Malware: Malicious soft**ware** that is specifically designed to gain access or damage a computer without the knowledge of the owner.

Password Stealer (PWS): Malware that monitors your keystrokes, captures personal information such as user names and passwords, and sends this information to the malware originator.

Pharming: A scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent.

Phishing: When a cybercriminal uses fraudulent emails or texts, or copycat websites to get you to share valuable personal information – such as account numbers, Social Security numbers, or your login IDs and passwords.

- **Spear Phishing:** Targets specific people with knowledge the criminal wants.
- **Whale Phishing:** Targets upper-level management.
- **SMiShing:** Phishing via text messages.
- **Vishing:** Phishing over the phone.

Phreaking: Hacking phone networks to make free calls, or charge calls to a different account.

Ransomware: A type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Rogue Security Software: A form of malware that misleads users into believing there is a virus on their computer, and convinces them into paying money for a fake malware removal tool (that actually introduces malware to the computer).

Rootkit: Malware designed to enable access to a computer or areas of its software by an unauthorized user.

Social Engineering: Manipulating someone to give up confidential information. This attack can be disguised as an email from a friend, your bank or another trusted contact. Once you interact with the email, a virus, malware or ransomware can be deployed into your computer.

Spoofing: When a cybercriminal tries to get into your computer by pretending to be a trusted source. Examples are emails that look like they are from someone you know, or an IP address that looks like a trusted site.

Spyware: Software that aims to gather information about a person or organization without their knowledge.

Trojan Horse: A malicious computer program which misrepresents itself as useful, routine, or interesting to persuade a victim to install it.

Virus: A malware program that can replicate itself and negatively change how a computer works.

Worm: Malware that self-replicates and sends itself to other computers in your network.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.