A BEGINNER'S GUIDE TO CYBERSECURITY

Glossary of common terms

THE BAD STUFF

Virus: A computer program that can infect a computer and then replicate (copy) itself to infect other files or programs.

Worm: Similar to a virus, a worm can replicate itself to spread, but it does not need an actively running host file or program. It can travel to other systems on a network.

Trojan: A Trojan (or Trojan horse) is malware that appears to be a legitimate document or program, but has a hidden and potentially malicious function.

Phishing: Messages designed by cybercriminals to trick you into giving away sensitive information. Example: an email that appears to come from your bank asking for your username and password, which the criminals use to steal your identity and your money.

Bot: A bot (as in robot) is an infected computer under the control of a cybercriminal, who uses it for malicious activities such as spreading spam.

Spear phishing: Similar to phishing, but targeted at a specific individual, such as the CEO of a company.

Botnet: A network of many compromised computers (bots) under the command and control of a cybercriminal.

Malware: Short for malicious software, malware can infect a computer or device to allow cybercriminals to steal information or take over your computer.

DDoS Attack: A distributed denial-of-service (DDoS) attack prevents or impairs the authorized use of IT systems or websites. Botnets are used to carry out these attacks by sending massive volumes of requests that consume bandwidth.

Ransomware: A type of malware that locks your computer or data and demands a payment to set it free. Criminals often require payment in bitcoins—a digital currency that is hard to trace.

DNS Attack: DNS stands for domain name server or domain name system. DNS translates website addresses (such as example.com) into IP addresses (a location on the internet). A DNS attack hijacks a legitimate website's IP address and points it to a malicious site controlled by the attacker.

THE GOOD STUFF

Antivirus: Antivirus software traditionally detected known threats using a signature, but malware writers soon found ways to avoid this type of detection. Antivirus tools now use technologies such as behavioral analysis and artificial intelligence (AI).

AI: AI, short for artificial intelligence or augmented intelligence, is the simulation of human intelligence by a computer. Humans can teach AI computers to consume vast quantities of data and recognize patterns, which makes it great for identifying cybersecurity threats.

Encryption: The process of converting data into a form that can only be read by authorized people. Encryption can protect data, such as messages sent over the internet or documents stored on a laptop. However, ransomware can use encryption to prevent you from accessing your data unless you pay.

Firewall: A hardware/software device or software program that limits network traffic according to a set of rules. For example, firewalls can block incoming traffic from botnets, or prevent data from leaving the network.

Source: National Initiative for Cybersecurity Careers and Studies https://niccs.us-cert.gov/glossary