StaySafeOnline.org

Glossary of Terms

Botnet—a network of private computers, each of which is called a “bot”(short for “robot”) infected with malicious software(malware) and controlled as a group without the owners' knowledge for nefarious and, often, criminal purposes; computers are typically infected when users open up an infected attachment or visit an infected website. Infected computers are also referred to as “zombies”

Cloud computing—a technology that uses the Internet and remote servers to maintain data and applications, allowing users to access applications without installation and access to their personal files from any computer with Internet access; centralizes storage, memory, processing, and bandwidth; examples include Yahoo email or Gmail with the software managed by the cloud service providers Yahoo and Google.

Denial of Service Attack/Distributed Denial of Service Attack (DDoS)—type of online computer attack designed to deprive user or groups of users normally accessible online services; generally involves effort by hackers to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Encryption—the conversion of digital information into a format unreadable to anyone except those possessing a “key” through which the encrypted information is converted back into its original form (decryption), making it readable again.

Firewall—software or hardware that, after checking information coming into a computer from the Internet or an external network, either blocks the transmission or allows it to pass through, depending on the pre-set firewall settings, preventing access by hackers and malicious software ; often offered through computer operating systems.

Geotagging—the process of adding geographical location, or label, to photographs, videos, Web sites, SMS messages, QR Codes, or RSS feeds; a geotag usually consists of latitude and longitude coordinates, altitude, distance, place names, and other details about the origin of the media being tagged helping users find a variety of online location-specific information.

HTTPS—Hypertext Transfer Protocol Secure, provides secure communication over a network, such as the Internet; basically layers additional security measures over HTTP; used by financial and online commerce websites to ensure the security of private information.

Keylogger—also called *keylogging* and *keystroke logging*, is the action of tracking (or logging) the keys struck on a computer keyboard; usually runs hidden in the background and automatically records all keystrokes so that users are unaware of its presence and that their actions are being monitored.

Malware—short for *malicious software*, software that disrupts or damages a computer’s operation, gathers sensitive or private information, or gains access to private computer systems; may include botnets, viruses, worms, Trojans, keyloggers, spyware, adware, and rootkits.

- **Botnet**—a network of private computers, each of which is called a “bot” (short for “robot”) infected with malicious software (malware) and controlled as a group without the owners' knowledge for nefarious and, often, criminal purposes. Infected computers are also referred to as “zombies.”

- **Virus**—type of malware that has a reproductive capacity to transfer itself from one computer to another spreading infections between online devices.
- **Worm**—type of malware that replicates itself over and over within a computer.
- **Trojan**—type of malware that gives an unauthorized user access to a computer.
- **Spyware**—type of malware that quietly sends information about a user's browsing and computing habits back to a server that gathers and saves data.
- **Adware**—type of malware that allows popup ads on a computer system, ultimately taking over a user's Internet browsing.
- **Rootkit**—a type of malware that opens a permanent "back door" into a computer system; once installed, a rootkit will allow more and more viruses to infect a computer as various hackers find the vulnerable computer exposed and attack.

Phishing—sending emails that attempt to fraudulently acquire personal information, such as usernames, passwords, social security numbers, and credit card numbers, by masquerading as a trustworthy entity, such as a popular social web site, financial site, or online payment processor; often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

SMiShing – An alternative form of phishing that occurs via text or SMS message.

Spam—the use of electronic messaging systems to send unsolicited bulk messages (usually advertising or other irrelevant posts) to large lists of email addresses indiscriminately.

Spyware—a type of malware (malicious software) installed on computers that collects information about users without their knowledge; can collect Internet surfing habits, user logins and passwords, bank or credit account information, and other data entered into a computer; often difficult to remove, it can also change a computer's configuration resulting in slow Internet connection speeds, a surge in pop-up advertisements, and un-authorized changes in browser settings or functionality of other software.

Wi-Fi—a technology that allows an electronic device (personal computer, video game console, smartphone, tablet, digital audio player) to exchange data wirelessly (using radio waves) over a computer network.

Wi-Fi Hotspot—a wireless access point to the Internet or other computer network over a wireless local area network through the use of a router connected to a link to an Internet service provider; frequently found in coffee shops and other public establishments, a hotspot usually offers Internet access within a range of about 65 feet (20 meters) indoors and a greater range outdoors; many smartphones provide built-in ability to establish a Wi-Fi hotspot.