Glossary

Adware is software with advertising functions integrated into or bundled with a program. It is usually seen by the programmer as a way to recover programming development costs, and in some cases it may allow the program to be provided to the user free of charge or at a reduced price. The advertising income may allow or motivate the programmer to continue to write, maintain and upgrade the software product.
Some adware is also spyware, and so the word may be used as term of distinction to differentiate between types of spyware software. What differentiates adware from other spyware is that it is primarily advertising-supported.

Phishing is a technique used to gain personal information for the purpose of identity theft. 'Phishing' emails give themselves away by telling you that there is a reason why you must provide personal details such as your Internet banking log on, password, credit card number or personal identification number by reply email or through a website. It is common for 'phishing' emails to contain links to a website that is a convincing replica of the financial institution's home page.
Financial institutions do not communicate with customers about account details by email. If you are concerned that you have been affected by a 'phishing' or other email scam, you should contact your financial institution immediately.

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a contraction of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. For a malicious program to accomplish its goals, it must be able to do so without being shut down, or deleted by the user or administrator of the computer it's running on. Concealment can also help get the malware installed in the first place. By disguising a malicious program as something innocuous or desirable, users may be tempted to install it without knowing what it does.

Spam is the abuse of electronic messaging systems to send unsolicited bulk messages, which are generally undesired. While the most widely recognized form of spam is email spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, mobile phone messaging spam, internet forum spam and junk fax transmissions. Spam can be also called junk mail at times. Because many people don't like spam, many emailing companies have created a bulk file in users' email addresses to sort out the spam.
Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming is widely reviled, and has been the subject of legislation in many jurisdictions.

Spyware is computer software that collects personal information about users without their informed consent. The term Spyware was coined in 1995 but wasn't widely used for another five years is often used interchangeably with adware and malware.
Personal information is secretly recorded with a variety of techniques, including logging keystrokes, recording Internet web browsing history, and scanning documents on the computer's hard disk. Purposes range from overtly criminal (theft of passwords and financial details) to the merely annoying (recording Internet search history for targeted advertising, while consuming computer resources). Spyware may collect different types of information. Some variants attempt to track the websites a user visits and then send this information to an advertising agency. More malicious variants attempt to intercept passwords or credit card numbers as a user enters them into a web form or other applications.

Trojan horse is a program that unlike a virus contains or installs a malicious program (sometimes called the payload or 'trojan'). The term is derived from the classical myth of the Trojan horse. Trojan horses may appear to be useful or interesting programs (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.
Often the term is shortened to simply **trojan**, even though this turns the adjective into a noun.

There are two common types of Trojan horses. One is otherwise useful software that has been corrupted by a hacker inserting malicious code that executes while the program is used. Examples include various implementations of weather alerting programs, computer clock setting software, and peer-to-peer file sharing utilities. The other type is a standalone program that masquerades as something else, like a game or image file, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives.

Virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. Viruses can spread to other computers by infecting files on a network file system or Internet host or file system that is accessed by other computers.
Viruses are sometimes confused with computer worms and Trojan horses. A worm, however, can spread itself to other computers without needing to be transferred as part of a host. A Trojan horse is a file that appears harmless until executed. In contrast to viruses, Trojan horses do not insert their code into other computer files. Many personal computers are now connected to the Internet and to local-area networks, facilitating their spread. Today's viruses may also take advantage of network services such as the World Wide Web, e-mail, and file sharing systems to spread, blurring the line between viruses and worms.

Worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.