Computer virus

A **computer virus** is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into othercomputer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts,logging their keystrokes, or even rendering the computer useless. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent.

Virus writers use social engineering and exploit detailed knowledge of security vulnerabilities to gain access to their hosts' computing resources. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit, desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, forsabotage and denial of service, or simply because they wish to explore artificial life and evolutionary algorithms.

Computer viruses currently cause billions of dollars' worth of economic damage each year due to causing systems failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and a multi-billion dollar industry of antivirus software vendors has cropped up, selling virus protection to users of various operating systems of which Windows is often the most victimized, partially due to its extreme popularity. No currently existing antivirus software is able to catch all computer viruses (especially new ones); computer security researchers are actively searching for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become widely distributed.

Phishing

Phishing is the illegal attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of *fishing* due to the similarity of using fake bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies.[7] Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and users should not use the same passwords anywhere on the internet.

Phishing is a continual threat that keeps growing to this day. The risk grows even larger in social media such as Facebook, Twitter, Myspace etc. Hackers commonly use these sites to attack persons using these media sites in their workplace, homes, or public in order to take personal and security information that can affect the user and the company (if in a workplace environment). Phishing is used to portray trust in the user since the user may not be able to tell that the site being visited or program being used is not real, and when this occurs is when the hacker has the chance to access the personal information such as passwords, usernames, security codes, and credit card numbers among other things.

Pharming

Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

The term "pharming" is a neologism based on the words "farming" and "phishing". Phishing is a type of social-engineering attack to obtain access credentials, such as user names and passwords. In recent years, both pharming and phishing have been used to gain information for online identity theft. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.

Trojan horse (computing)

A **Trojan horse**, or **Trojan**, in computing is generally a non-self-replicating type of malware program containing malicious code that, when executed, carries out actions determined by the nature of the Trojan, typically causing loss or theft of data, and possible system harm. The term is derived from the Ancient Greek story of the large wooden horse used to trick defenders of Troy into taking warriors concealed in the horse into their city in ancient Anatolia. The use of this name references how computer Trojans often employ a form of social engineering, presenting themselves as routine, useful, or interesting in order to persuade victims to install them on their computers.

A Trojan often acts as a backdoor, contacting a controller which can then have unauthorized access to the affected computer While Trojans and backdoors are not easily detectable by themselves, computers may appear to run slower due to heavy processor or network usage. Malicious programs are classified as Trojans if they do not attempt to inject themselves into other files (computer virus) or otherwise propagate themselves (worm). A computer may host a Trojan via a malicious program that a user is duped into executing (often an e-mail attachment disguised to be unsuspicious, e.g., a routine form to be filled in), or by drive-by download.

Hoax

A **hoax** is a deliberately fabricated falsehood made to masquerade as truth. It is distinguishable from errors in observation or judgment, or rumors, urban legends, pseudosciences or April Fools' Day events that are passed along in good faith by believers or as jokes.

Definition

Robert Nares defined the word *hoax* as meaning "to cheat", dating from Thomas Ady's 1656 book *A candle in the dark, or a treatise on the nature of witches and witchcraft*.

The term *hoax* is occasionally used in reference to urban legends and rumors, but the folklorist Jan Harold Brunvand argues that most of them lack evidence of deliberate creations of falsehood and are passed along in good faith by believers or as jokes, so the term should be used for only those with a probable conscious attempt to deceive. As for the closely related terms *practical joke* and *prank*, Brunvand states that although there are instances where they overlap, *hoax* tends to indicate "relatively complex and large-scale fabrications" and includes deceptions that go beyond the merely playful and "cause material loss or harm to the victim"

According to Professor Lynda Walsh of the University of Nevada, Reno, some hoaxes—such as the Great Stock Exchange Fraud of 1814, labeled as a hoax by contemporary commentators—are financial in nature, and successful hoaxers—such as P. T. Barnum, whose Fiji mermaid contributed to his wealth—often acquire monetary gain or fame through their fabrications, so the distinction between *hoax* and*fraud* is not necessarily clear. Alex Boese, the creator of the Museum of Hoaxes, states that the only distinction between them is the reaction of the public, because a fraud can be classified as a hoax when its method of acquiring financial gain creates a broad public impact or captures the imagination of the masses.

One of the earliest recorded media hoaxes is a
fake almanac published by Jonathan Swift under the pseudonym
of Isaac Bickerstaff in 1708. Swift predicted the death of John Partridge, one of the leading astrologers in England at that time, in the almanac and later issued an elegy on the day Partridge was supposed to have died. Partridge's reputation was damaged as a result and his astrological almanac was not published for the next six years.

It is possible to perpetrate a hoax by making only true statements using unfamiliar wording or context, such as in the Dihydrogen monoxide hoax. Political hoaxes are sometimes motivated by the desire to ridicule or besmirch opposing politicians or political institutions, often before elections.

A hoax differs from a magic trick or from fiction (books, movies, theatre, radio, television, etc.) in that the audience is unaware of being deceived, whereas in watching a magician perform an illusion the audience expects to be tricked.

A hoax is often intended as a practical joke or to cause embarrassment, or to provoke social or political change by raising people's awareness of something. It can also emerge from a marketing or advertising purpose. For example, to market a romantic comedy movie, a director staged a phony "incident" during a supposed wedding, which showed a bride and preacher getting knocked into a pool by a clumsy fall from a best man. A resulting video clip of *Chloe and Keith's Wedding* was uploaded to YouTube and was viewed by over 30 million people and the couple was interviewed by numerous talk shows. Viewers were deluded into thinking that it was an authentic clip of a real accident at a real wedding; but a story in *USA Today*in 2009 revealed it was a hoax.

A borderline case between fiction and hoax is a 1938 radio broadcast by Orson Welles describing a Martian invasion of earth. Many people who tuned in without hearing the introduction of the program as fiction were concerned that the invasion was real. It has been suggested that Welles knew the schedule of a popular program on another channel, and scheduled the first report of the invasion to coincide with a commercial break in the other program so that people switching stations would be tricked.

Governments sometimes spread false information to assist them with aims such as going to war; the "Iraq dossier" is an example of this; these often come under the heading of black propaganda. There is often a mixture of outright hoax and suppression and management of information to give the desired impression. In wartime and times of international tension rumours abound, some of which may be deliberate hoaxes.

Examples of politics-related hoaxes:

Belgium is a country with a Flemish-speaking region and a French-speaking region. In 2006 French-speaking television channel RTBF interrupted programming with a spoof report claiming that the country had split in two and the royal family had fled.

On Saturday 13 March 2010 the Imedi television station in Georgia broadcast a false announcement that Russia had invaded Georgia.

Psychologist Peter Hancock has identified six steps which characterise a truly successful hoax:

Identify a constituency- a person or group of people who, for reasons such as piety or patriotism, or greed, will truly care about your creation.

Identify a particular dream which will make your hoax appeal to your constituency.

Create an appealing but "under-specified" hoax, with ambiguities

Have your creation discovered.

Find at least one champion who will actively support your hoax.

Make people care, either positively or negatively – the ambiguities encourage interest and debate

Email spam

Email spam, also known as **junk email** or **unsolicited bulk email** (*UBE*), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in spam email may send users to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments. Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. One subset of UBE is *UCE*(unsolicited commercial email). The opposite of "spam", email which one wants, is called "ham", usually when referring to a message's automated analysis (such as Bayesian filtering). Like other forms of unwanted bulk messaging, it is named for Spam luncheon meat by way of a Monty Python sketch in which Spam is depicted as ubiquitous and unavoidable.