

E-crime

Author:

Papadopoulos Charalampos, Alexander Technological Educational Institution of Thessaloniki,
chpapa@it.teithe.gr

Thessaloniki, 1 March 2008

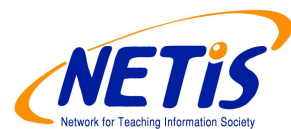
Publication of this report is supported by:



Education and Culture

Leonardo da Vinci

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use that may be made of the information contained therein



Content

- Acknowledgement 5**
- Introduction 6**
- Computer Crime today 7**
- E-Crime Categories 9**
 - 1. Unauthorised access9
 - 2. Malicious software types ('malware').....9
- How to Get Safe On-line..... 16**
 - 1. Prevention strategies..... 16
- Bibliography..... 18**

Acknowledgement

I would like to thank my supervisor Dr. Kerstin Siakas, for many insightful conversations during the development of the project, for helpful comments on the text and for many helpful suggestions.

Introduction

The following demonstration aims to show how emerging technologies provide new opportunities for criminals and create new challenges for enforcement personnel (Charney – Alexander, 2008).

“Two photographs hung side by side on the wall. The first depicted a homicide detective's worst nightmare. A body lay twisted on the floor, a gaping wound in the chest. Across the room, on the floor, was a large pistol. On the white wall above the victim's body, scrawled in the victim's own blood, were the words, "I'll kill again, you'll never catch me.”

The second photograph depicted the same room, the same victim. But in this photo, the wall was "clean". The gaping chest wound was gone, replaced with a small head wound from which blood trickled. The gun was clutched in the victim's hand”.

The criminal potential is today facilitated by improvements in emerging Information and Communication Technologies (ICTs) (Information and Communication Technologies, 2007).

Also international hacker attacks launched by malicious programming codes through global computer networks do no longer belong to science fiction, but is existing reality.

The term "computer crime" refers to the two related but distinct technologies, namely computers and telecommunications and denotes the use of computers by individuals in one or several of the following (Charney – Alexander, 2008):

- A computer may be the target of an offense indicating that the criminal aims to steal information from, or cause damage to, a computer.
- The computer may be a tool of an offense occurring when an individual uses a computer to facilitate a traditional offense, such as fraud or theft.
- Computers may be incidental to an offense, but significant to law enforcement due to the fact that they may have evidence of a crime.

Computer Crime today

Computer crime, cyber crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, the tool, the target, or place of a crime (Computer Crime, 2007). These categories are not exclusive and many activities can be characterized as falling in one or more categories. Additionally the terms computer crime or cyber crime are restricted to describing criminal activity in which the computer or network or other electronic communications devices (e.g. mobile phones) are used to commit an offence, be the target of an offence or act as a storage device in an offence. These terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used to facilitate the illicit activity (Electronic Crime Strategy, 2001).

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including:

- *Illegal access*: unauthorized access to any system or network.
- *Illegal interception*: Technical means of non-public transmissions of computer data to, from or within a computer system.
- Creation and distribution of viruses.
- *Data interference*: unauthorized damaging, deletion, deterioration, alteration or suppression of computer data.
- Systems interference: interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
- Misuse of devices.
- Copyright violation: offences that include violation of copyrights.
- Distribution of child pornography: exposure of any kind of pornography and especially child pornography.
- Cyber stalking: a person is stalked or harassed by another person using a service of the Internet such as email, instant messaging or via a posting in a discussion group.
- Fraudulent financial activity – phishing: sending misleading emails requesting personal and financial details from unsuspecting people.
- Forgery: ID theft in order to be used for harming purposes.
- Electronic fraud: deception made for personal gain.

Some of the categories of electronic crime include offences regarding information. Some of the most important categories are analysed in this chapter (Computer Crime, 2007; What is e-crime?; How do I report e-crime?).

However there are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are difficult to calculate. For all these reasons we must be informed in order not only to detect a cyber crime but also to report it to the authorities of our authorities. Experts agree that Internet crime is rising. Because gathering statistics on e-crime is inherently diffi-

cult: victims generally do not report it since they do not know where to complain. This is a very serious problem (e-crime reporting portal).

In Europe there is no clearing house that tracks Internet crime victims. The U.S. has groups such as the Internet Fraud Watch and the Internet Crime Complaint Center (Internet Crime Complaint Center, 2007), which is run by the U.S. Federal Bureau of Investigation and National White Collar Crime Center (Computer Crime Research, 1999). Both use different methodologies in collecting data that needs to be "statistically robust".

Nevertheless, there is a consensus among both law enforcement personnel and computer security scientists that both the number of computer crime incidents and the sophistication of computer criminals is increasing rapidly. There are estimates that computer crime costs victims in the USA at least US\$ 5×10^8 /year. The true value of such crime may be substantially higher if all victims would report crime. For Europe the exact cost of e-crime is lacking due to the fact that there is no systematic crime recording. Experts in computer security, who are not attorneys, speak of "information warfare". While such "information warfare" is just another name for computer crime, the word "warfare" denotes the amount of damage inflicted on society (Standler, 2002).

E-Crime Categories

There are many different categories of e-Crime. However, most of them can be grouped within the following categories:

1. Unauthorised access

The use of personal programming abilities or various programmes with malicious intent to gain unauthorised access to a computer or a network are considered. There are very serious crimes. Similarly, the creation and dissemination of harmful computer programmes which do irreparable damage to computer systems is another kind of serious Cybercrime. Software piracy is also a distinct kind of Cybercrime which is perpetuated by many people online by distributing illegal and unauthorised pirated copies of software.

Professionals who involve in these cybercrimes are called “crackers”. It is found that many of such professionals are still in their teens. A report written in the beginning of the Information Age warned that America's computers were at risk from crackers. It said that computers that "control (our) power delivery, communications, aviation and financial services (and) store vital information, from medical records to business plans, to criminal records", were vulnerable from many sources, including deliberate attack (Babu - Parishat, 2004).

2. Malicious software types ('malware')

The use of malicious software range from placing excessive demand on a computer's resources, to destruction of data or hardware. In some cases the user is made aware of the presence of the malware, for example when sending a message to the user or deleting the contents of a hard drive. Recent forms of malware may operate without the user's knowledge, steal financial information, such as credit card details or convert infected computers into an asset for the attacker. Common types of malware operate as follows:

- **Viruses:** A virus is a computer program (usually disguised as something else), which is designed to cause undesirable effects on computer systems. Viruses are often designed to be transferred from one computer to another without the users' knowledge. They can be hidden in attachments of emails, on CDs or in files that are shared across the Internet. They can infect computers or other electronic devices. After infection, the executable file functions in a different way than before; it may display a benign message on the monitor, delete some or all files on the user's hard drive or alter data files. Computer viruses can cause serious harm to computer systems. There are two key features of a computer viruses:
 - The virus has the ability to propagate by attaching itself to executable files (e.g., application programs, operating system, macros, scripts, boot sector of a hard disk or floppy disk, etc.) Running the executable file may make new copies of the virus.
 - The virus causes harm only after it has infected an executable file and the executable file is run.

The word virus is commonly used to include computer viruses, worms, and Trojan Horse programs. Beginning with the Melissa virus in 1999, viruses could automatically send e-mails with the victim's name as the alleged source. Nowadays computer programmers called hackers often use viruses to stop or slow down computer systems (Standler, 2002; Trojan Programs).

- Worms: A worm is a program that copies itself. The distinction between a virus and worm is that a virus never copies itself – a virus is copied only when the infected executable file is run. Worms are using an internet connection to access vulnerabilities on other computers and to install copies of themselves. In the original form, a worm neither deleted nor changed files on the victim's computer — the worm simply made multiple copies of itself. Those multiple copies of the worm were sent from the victim's computer, thus clogging disk drives and the Internet. Releasing such a worm into the Internet will slow the legitimate traffic on the Internet, due to continuously increasing amounts of the worm also used as a conduit to allow attackers access to a computer.

Beginning with the Klez worm in early 2002, a worm could drop a virus into the victim's computer. This kind of worm became known as a blended threat, because it combined two different types of malicious code, namely worms and viruses (Computer Crime, 2006; Standler, 2002; What is a worm?, 2004)

- Trojans: A Trojan Horse is a deceptively labelled program that contains at least one function that is unknown to the user and that harms the user. A Trojan Horse does not replicate, itself thus distinguishing it from viruses and worms. Usually Trojans are malware masquerading as something the user may want to download or install. After distinguishing they perform hidden or unexpected actions, such as allowing external access to the computer.

Some of the more serious Trojan horses allow a hacker to remotely control the victim's computer, for example to collect passwords and credit card numbers and send them to the hacker, or to launch denial of service attacks on websites.

Some Trojan Horses are installed on a victim's computer by an intruder, without any knowledge of the victim. Other Trojan Horses are downloaded (e.g. in an attachment in e-mail) and installed by the user, who intends to acquire a benefit that is quite different from the undisclosed true purpose of the Trojan Horse (What is a worm?, 2004; Computer Crime, 2006).

- Spyware is computer software that is installed surreptitiously on a personal computer without the user's informed consent in order to intercept or take partial control over the user's interaction with the computer. Spyware transmits information gathered from a computer, such as bank details, back to an attacker. An example of spyware 'keylogging' software that records anything entered, such as passwords, using the keyboard.

The term spyware suggests software that secretly monitors the user's behaviour. However the functions of spyware extend beyond simple monitoring. Spyware programs usually collect various types of personal information, but can also interfere with user control of the computer. Spyware can install additional software, redirect Web browser activity, access websites blindly (which may cause more harmful viruses) or divert advertising revenue to a third party. Spyware can even change computer settings, resulting in slow connection speeds, different home pages, and loss of Internet or other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term privacy-invasive software (Computer Crime, 2006; Adware/Spyware, 2007).

- Logic bomb: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. It "detonates" when certain event occurs. The detonated program may stop working (e.g., go into an infinite loop), crash the computer, release a virus, delete data files, or harm the computer system in other ways. For example, a programmer may

hide a piece of code that starts deleting files (such as the salary database). Trojans that activate on certain dates are types of logic bombs that are initiated when the computer's clock reaches a certain target date often called "time bombs" (Computer Crime, 2006; What is logic bomb?, 2006).

- Blackmail is the act of threatening to reveal information about a person, or even do something to destroy the threatened person, unless the blackmailed target fulfils certain demands, usually money demands. This information is usually of an embarrassing or socially damaging nature. In a broader sense, blackmail is an offer to refrain from some legal or normally allowed action. Extortion is used when the threat is unlawful and includes violent action if demands are not met (Computer Crime, 2006; What is Blackmail; Standler, 2002).
- Identity Theft: A large part of online crime is now centred on identity theft which is part of identity fraud. It is defined as an individual falsely representing him or herself as either another person or a fictitious person to a third party for some benefit. In other words someone steals the identity of another person and use it in order to represent him/her and gain advantages from the victim, of course without his or her acquiescence. Examples of identity theft may include:
 - hacking into other computer systems;
 - launching a Denial of Service Attack (DOS) thus bringing down computer systems;
 - creating and distributing viruses;
 - cyber stalking;
 - copyright violation offences;
 - distributing child pornography;
 - fraudulent financial activity such as phishing;
 - credit card fraud.

Identity Theft, activity usually undertaken such as opening and closing of bank accounts as if you were authorising it. The most common form of identity theft is credit card fraud. The criminals will steal and transfer money or take advantage of the victim in other ways. While the term is relatively new, the practice of stealing money or getting other benefits by pretending to be a different person is thousands of years old. A victim may have to spend valuable time and money restoring their reputation after the event (Internet Fraud, 2008; Computer Crime; What is e-crime?; How do I report e-crime?)

- Denial of Service (DoS) Attacks or Distributed Denial-of-Service (DdoS) attack is an attempt to make a computer resource unavailable to its intended users. A DOS occurs when an Internet server is flooded with a nearly continuous stream of bogus requests for WebPages, thereby denying legitimate users a possibility to download a page. As a result the web server may be crashed.
- Criminals have developed a simple technique for executing a distributed DoS attack:
 - The criminal first plants remote-control programs on a large number of computers with broadband access to the Internet. The remote-control program will, at the command of the criminal, issue a nearly continuous series of pings to a certain victim's website.
 - When the criminal is ready to attack, he instructs the programs to begin pinging a specific target address. The computers containing the remote-control programs start acting as "zombies".
 - The victim computer responds to each ping, but because the zombie computers are programmed by the criminal to give false source addresses for the pings, the victim computer is unable to establish a connection with the zombie computers. The victim computer waits for

a response to its return ping, and because there are more zombie computers than victims, the victim computer becomes overwhelmed. It keeps waiting to respond to bogus pings or in the end of it crashes.

- After a few hours, the criminal usually instructs the programs to stop pinging the victim due to the fact that long- duration attacks make it easier for engineers at the victim's website to trace the source of the attacks.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even DNS root servers.

One common method of attack involves saturating the target (victim) machine with external communications requests. Personal Computers cannot respond to legitimate traffic, or respond so slowly as to be rendered effectively unavailable. Usually to make a DDoS attack successful, people are using at least 80 PCs with internet connections.

As an example we can mention a Russian crime gang that tried to attack UK gambling websites during the 2004 Grand National. The National High Tech Crime Unit (NHTCU) together with the Russian authorities managed to arrest those responsible and helped to set up the Internet DDoS forum to share data about attacks (Computer Crime, 2006; What is Denial of Service?, 2007; Denial of Service Attacks, 2001).

- **Drug Trafficking:** Drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e-mail and other Internet Technology in order to do their real identity. Some drug traffickers arrange deals at internet cafes, use courier Web sites to track illegal packages of pills, and swap recipes for amphetamines in restricted-access chat rooms.

The Internet's easy-to-learn, fast-paced character, global impact, and fairly reliable privacy features facilitate the marketing of illicit drugs. Detecting money laundering of cash earned by drug traffickers is very difficult, because dealers are now able to use electronic commerce and Internet banking facilities. Also, traffickers have been using online package tracking services offered by courier companies to keep tabs on the progress of their shipments. If there happened to be some sort of undue delay, this could signal authority interception of the drugs, thus allow the dealers time to cover their tracks. Law enforcement is also more deficient because illicit drug deals are arranged instantaneously, over short distances, making interception by authorities much more difficult.

The rise in the level of Internet drug trades can also be attributed to the lack of face-to-face communication. These virtual exchanges allow more intimidated individuals to more comfortably purchase illegal drugs. The sketchy effects that are often associated with drug trades are severely minimized and the filtering process that comes with physical interaction fades away. Furthermore, traditional drug recipes were carefully kept secrets. But with modern computer technology, this information is now being made available to anyone with computer access (Computer Crime, 2006; Fifty Years Of Drug Trafficking; Britannica on-line encyclopaedia).

- **Cyberterrorism** is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

New terrorist organizations are highly funded, technologically articulate groups capable of inflicting devastating damage to a wide range of targets. While most published work in the computer industry has focused on the impact of the computer as target (pure cyberterrorism) it is our belief that the real danger posed by the synthesis of computers and terrorism is not only the insertion of computer as target in the terrorism matrix, but in many of the other areas, too (Gordon, 2007; Cyber Terrorism, 2008).

- Phishing: (also known as phising) is the practice whereby a 'phisher' may use spoof emails to direct a computer user to fraudulent websites to elicit a transfer of money, or sensitive information, such as passwords or credit card details, from unsuspecting people.

If the information is supplied to the fraudster, identity theft (where the fraudster pretends to be the account holder) usually occurs and money may be transferred away into the fraudsters account or used directly to make online purchases.

Attacks are increasing, with financial services accounting for over 93% of impersonated or hijacked brands through bogus websites and emails (Phishing Activity Trends Report, 2006). Almost all of the UK's high street banks have been affected by phishing.

Phishing is predominately associated with spam, whereby thousands of messages are sent out at once in the hope that some people will be caught and supply their financial and personal details to the fraudster.

Phishing was first identified in hacker circles in 1996 and became a major issue in auction sites such as eBay (www.ebay.com), and payment gateways, such as PayPal (www.paypal.com) (Phishing Activity Trends Report, 2006; What is phishing).

- Child pornography: Certain child pornography websites may be created, or child pornography images may be embedded in general pornography sites. However, there is debate about how much child pornography is available on the web. Some argue that it is relatively easy to find images. Others argue that, because of the vigilance of ISPs (Internet Service Providers) and police in tracking down and closing child pornography websites, it is unlikely that a normal web search using key words such as childporn would reveal much genuine child pornography. Instead, the searcher is likely to find legal pornographic sites with adults purporting to be minors, 'sting' operations, or vigilante sites (Child pornography on the Internet, 2007).

One strategy of distributors is to post temporary sites that are then advertised on pedophile bulletin boards. To prolong their existence these sites may be given innocuous names (e.g. volleyball) or other codes (e.g. ch*ldp*rn) to pass screening software. The websites may be immediately flooded with hits before they are closed down. Often the websites contain Zip archives, for which the password is then later posted on a bulletin board.

Images of abuse may be broadcast in real time. In one documented case of a live broadcast, viewers could make online requests for particular sexual activities to be carried out on the victim (Child pornography, 2008).

E-mail attachments are sometimes used by professional distributors of child pornography. However more frequently they are used to share images among users, or they are sent to a potential victim as part of the grooming/seduction process. This method is considered risky by seasoned users because of the danger in unwittingly sending e-mails to undercover police posing as pedophiles or as potential victims.

Specific child pornography e-groups exist to permit members to receive and share pornographic images and exchange information about new sites. Some of these groups appear on reputable servers and are swiftly shut down when they are detected. However, they may use code names or camouflage child pornography images among legal adult pornography to prolong their existence.

A major method of distributing child pornography is specific child pornography newsgroups that provide members with a forum in which they discuss their sexual interests in children and post child pornography. Some child pornography newsgroups are well known to both users and authorities (for example, the abep-t or alternative binaries pictures erotica pre-teen group). Most commercial servers block access to such sites. Some servers do provide access to them but a user runs the risk of having his/her identity captured either by the credit card payments required for access, or the record kept by the server of his/her IP address. However, a computer-savvy user can access these groups by using techniques that hide his/her identity by concealing his/her true IP address.

Chat rooms may be used to exchange child pornography and locate potential victims. These chat rooms may be password-protected. Open chat rooms are avoided by seasoned child pornographers because they are often infiltrated by undercover police.

P2P (Peer 2 Peer) networks facilitate file sharing among child pornography users. These networks permit closed groups to trade images (U.S code collection).

Table1 shows the statistics about different categories of e-crime globally. We can see that viruses and Denial of service attack are the most common e-crimes. Cyber terrorism and child pornography are not included in this table because there is no available statistics.

1st Table: “E-crime Watch Summary”

TYPES OF ELECTRONIC CRIMES	
Virus or other malicious code	77%
Denial of service attack	44%
Illegal generation of spam mail	38%
Unauthorized access by an insider	36%
Phishing	31%
Unauthorized access by an outsider	27%
Fraud	22%
Theft or intellectual property	20%
Theft of another proprietary info	16%
Employee identity theft	12%
Sabotage by an insider	11%
Sabotage by an outsider	11%
Extortion by an insider	3%
Extortion by an outsider	3%
Other	11%
Don't know	8%

Source: Child pornography, 2008

How to Get Safe On-line

I. Prevention strategies

E-crime can affect everyone. It does not matter if someone runs a company or if he/she is a single user. There are so many different categories of e-crime that is difficult for the user to protect him/her. However, there are practical steps to prevent e-crime occurring by:

- **Securing business computer or network.** The following software can be installed:
 - Password authentication software to protect sensitive business information. Updating password regularly. Common passwords, such as telephone numbers, birth dates or mother's maiden name should be avoided. The best password is a combination of letters, numbers and symbols.
 - Anti-virus software, regularly updated – viruses can allow an online fraudster to gain access to information files or can send sensitive information to other email addresses.
 - Encryption software that converts transaction information into unreadable code.
 - A firewall (software that keeps unwanted visitors out). This is especially important in case of high speed internet connections that are connected to the internet 24 hours a day.
- **Preventing business information from being stolen.** Be vigilant about how, where and to whom business and customer information is passed and how documents containing business information are disposed of.
- **Setting minimum identification requirements for credit card orders received over the internet.** Some details you may wish to ask for are the customer's name, credit card number and expiry date, credit card security number, street address, phone number, fax number and email address. If there are doubt about an order, should be asked for further identification details from the customer or should the order be rejected.
- **Screening orders coming in over the internet to ensure that they are legitimate.** For example, phone or email the customer to confirm the order. This increases the likelihood of determining that the person whose credit card number was used is actually the person who placed the order. It also confirms the contact details in case that credit card number is used fraudulently in the future.
- **Ensuring that you authorise transactions with your financial institution.** This is commonly done either over the phone or online.
- **Maintaining a list or database of lost or stolen credit cards and fraudulent orders.** This should include the customer's credit card number, address, email address and other contact details.
- **Allowing only trusted staff members to have access to computer files containing customer information,** such as credit card details and contact details. These staff members should be trained in the methods of preventing e-crime. When staff members leave the organisation, the passwords protecting customer information should be changed.

- **Be wary of unsolicited emails.** They should be deleted them without opening any attached files or clicking on any links. They may contain viruses or other software that could interfere with the computer's operations or data.
- **Wipe the hard drive before disposed your computer.** Specially designed software can be used to ensure that no files containing business information can be retrieved (Australian Government Crime Prevention Initiatives, 2008; Cyber crime it could happen to you; (FBI warns public of e-mail scams, 2007; Computer Crime Research, 1999).

Bibliography

- Adware/Spyware, October 2007 (http://www.go-online.gr/ebusiness/specials/article.html?article_id=1173, accessed 18th January 2008)
- Anti-Phishing Working Group, Phishing Activity Trends Report, July 2006 (www.antiphishing.org, accessed 18th January 2008)
- Austrarian Federal Police, Internet Fraud, 26 May 2008 (http://www.afp.gov.au/national/e-crime/internet_scams.html, accessed 18th January 2008)
- Australasian Governments Centre for Policing Research, Electronic Crime Strategy, March 2001 (http://www.acpr.gov.au/pdf/Ecrime_Strategy.pdf, accessed 18th January 2008)
- Australian Governments NetAlert: What is e-crime? (http://www.netalert.gov.au/advice/risks/e-crime/what_is_e-crime.html, accessed 18th January 2008)
- Australian Governments NetAlert: How do I report e-crime? (http://www.netalert.gov.au/advice/risks/e-crime/how_do_I_report_an_e-crime.html, accessed 18th January 2008)
- Babu, Maya – Parishat, Mysore Grahakara (2004): *What is cyber-crime* (<http://www.crime-research.org/analytics/702/>, accessed 18th January 2008)
- Britain spearheads European e-crime reporting portal (<http://www.infoworld.com/article/07/04/18/HNeuroecrimeportal>, accessed 18th January 2008)
- Britannica on-line encyclopaedia (<http://www.britannica.com/eb/article-25343/Colombia>, accessed 18th January 2008)
- Charney, Scott – Alexander, Kent: *Computer Crime* (<http://www.crime-research.org/library/Alex.htm>, accessed 18th January 2008)
- Child pornography on the Internet, March 2007 (<http://www.cops.usdoj.gov/mime/open.pdf?Item=1729>, accessed 18th January 2008)
- Child pornography, January 2008 (<http://www.adultweblaw.com/laws/childporn.htm>, accessed 18th January 2008)
- Cyber Terrorism, May 2008 (http://www.crime-research.org/articles/Cyber_Terrorism, accessed 18th January 2008)
- Denial of Service Attacks, June 2004 (http://www.cert.org/tech_tips/denial_of_service.html, accessed 18th January 2008)
- Fifty Years Of Drug Trafficking by CIA and Other Government People (<http://www.ciadrugs.com>, accessed 18th January 2008)
- <http://agencysearch.australia.gov.au>, accessed 18th January 2008

Information and Communication Technologies (<http://cordis.europa.eu/fp7/ict/>, accessed 18th January 2008)

Internet Crime Complaint Center (IC3), FBI warns public of e-mail scams, 17 July 2007 (<http://www.ic3.gov/media/2007.aspx>, accessed 18th January 2008)

Legal Information Institute, U.S code collection (<http://www4.law.cornell.edu/uscode/18/2256.html>, accessed 18th January 2008)

National White Collar Crime Center, Computer Crime Research, October 1999 (http://www.nw3c.org/research/site_files.cfm?mode=p, accessed 18th January 2008)

Protecting Families on-line – what is a computer crime (http://www.netalert.gov.au/advice/security/virus/What_is_a_computer_%20virus.html#cim_main-content, accessed 18th January 2008)

Sarah Gordon (2007): *Cyberterrorism* (<http://www.security.iaa.net.au/downloads/cyberterrorism.pdf>, accessed 18th January 2008)

Standler, Ronald B. (2002): *Computer crime* (<http://www.rbs2.com/ccrime.htm>, accessed 18th January 2008)

The Home Office, Fraud and Technology Crimes: Findings from the British Crime Survey 2003/4, the 2004 Offending Crime and Justice Survey and administrative sources, September 2006 (<http://www.parliament.uk/documents/upload/postpn271.pdf>, accessed 18th January 2008)

Trojan programs (<http://www.viruslist.com/en/virusesdescribed?chapter=152540521>, accessed 18th January 2008)

What is a worm? 3 December 2004, (<http://www.microsoft.com/hellas/athome/security/viruses/virus101.msp>, accessed 18th January 2008)

What is blackmail? Brief and Straightforward Guide (<http://www.wisegeek.com/what-is-blackmail.htm>, accessed 18th January 2008)

What is Denial of Service? June 2007 (http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci213591,00.html, accessed 18th January 2008)

What is logic bomb? (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gc, accessed 18th January 2008)

What is phishing (http://www.netalert.gov.au/advice/risks/phishing/What_is_Phishing.html, accessed 18th January 2008)

Wikipedia, The Free Encyclopedia, Computer Crime (<http://en.wikipedia.org/wiki/E-crime>, accessed 18th January 2008)