Glossary of Technology Terms

Adware: Like spyware, this is software that installs itself on another computer without the owner's knowledge, and under certain circumstances places advertisements on the screen.

Anonymizer: An intermediary website that hides or disguises the IP address associated with the Internet user. Generally, these sites allow a person to engage in various Internet activities without leaving an easily traceable digital footprint.

Back Door: An undocumented way of gaining access to a program, a computer system, or network. The backdoor is usually implemented by the creator of the program, and is usually only known to him. A backdoor is a potential security risk.

Bash Board: An online bulletin board on which individuals can post anything they want. Generally, posts are malicious and hateful statements directed against another person.

Black Hat: A term used to describe a hacker who has the intention of causing damage or stealing information.

Blocking: The denial of access to particular parts of the Internet. Usually a message will be shown on screen to say that access has been denied. For example, instant message users can block other screen names from sending them messages.

Blog: Short for web log, a blog is a web page that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author.

Bluesnarfing: Stealing information from mobile devices using a wireless connection

Bomb: Code that is hidden in a program or system, either maliciously or as a prank, which will cause something to happen later on, usually on a given date, such as a specific holiday.

Botnet: A network of private computers, each of which is called a "bot," infected with malicious software (malware) and controlled as a group without the owners' knowledge for nefarious and, often, criminal purposes.

Browser: Short for web browser, any software used to locate and display web pages. Most can display graphics and text as well as present multimedia information including sound and video.

BruteForceAttack: Figuring out a password by trying every possible combination of letters, numbers, and symbols.

Buddy List: A collection of names or handles (also known as screen names) that represent friends or "buddies" within an instant messaging or chat program. They are useful in informing a user when that person's friends are online and available to chat.

Chatrooms: Sites that allow for real-time, text-based communication between two or more users.

Chat tracking: The ability to track chat and instant message conversations.

Computer Tracking: The ability to track what is done on a computer.

Cookie: A small file downloaded to your computer when you browse a webpage. The main purpose of cookies is to identify users and possibly prepare customized webpages for them. Websites use cookies for several different reasons: to collect demographic information about who is visiting the website; to personalize the user's experience on the website; and to monitor advertisements. Any personal information that you give to a website, including credit card information, will most likely be stored in a cookie unless you have turned off the cookie feature in your browser.

Cracker: A term sometimes used to refer to a hacker who breaks into a system with the intent of causing damage or stealing data.

Cracking: Modifying a program to make it behave as the intruder wants it to behave rather than as its creator intended.

Creeping: Similar to stalking in the real world; creeping is following someone online through their status updates, profiles, websites, etc.

Cryptography: Converting information into a secret code to protect it or hide its meaning before sending it out over the Internet.

Cyberbullicide: Suicide stemming directly or indirectly from cyberbullying victimization.

Cyberbullying: Bullying that takes place using electronic technology, including the Internet, and related technologies to harm other people, in a deliberate, repeated, and hostile manner; may involve text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, Websites, or fake profiles.

Cybercrime: Cybercrime (or e-crime) refers to criminal offences which are committed with the aid of ICTs (e.g. internet, mobile phone). Cybercrime laws may encompass a broad range of issues, including such activities as hacking, intellectual property violations and the dissemination of 'harmful' content such as child pornography or racist and xenophobic materials. Some experts divide cybercrime into three major categories, those committed against persons (e.g. online harassment), cybercrimes against property (e.g. software

piracy), and cybercrimes against government (e.g. cyber terrorism). In many countries, cybercrime bills focus merely on economic and state security threats, and fail to recognize cybercrimes against persons, including serious forms of crimes against women, such as cyberstalking or cyberharassment.

Cyberhijacking: Hijacking someone's computer, browser, modem, or instant messenger. Also includes webpage hijacking.

Cyberspace: A metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via email), do research, or shop. Like physical space, cyberspace contains objects (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace requires little physical movement. The term was coined by author William Gibson in his sci-fi novel Neuromancer (1984).

Cyberstalking: A criminal offense that involves using the internet or other technology to harass an individual, a group of individuals, or an organization. Cyberstalking includes (repeatedly) sending threats or false accusations via email or mobile phone, making threatening or false posts on websites, monitoring a person's computer and internet use, or stealing a person's information -- and even their identity. Sometimes these threats can escalate into physical acts. Anyone can be stalked online but, as is the case offline, the majority of cyberstalking victims are female. While the perpetrators may sometimes be strangers, often they are the former, estranged or current partners, boyfriends and husbands of the victims. Domestic violence victims are particularly at risk of cyberstalking.

Cyberthreats: Electronic material that either generally or specifically raises concerns that the creator may intend to inflict harm or violence on him- or herself or others.

Darknet: A darknet is a cordoned-off, anonymized section of the net where users can meet, chat and swap data. Usually darknets are confined to small tight-knit groups such as hackers who use the secure connections to distribute information and hacking tools. They have also been used by pedophiles to distribute images of child abuse. Many are invitation-only services where potential members have to upload material to prove themselves to the group before they are granted full access.

Denial of Service Attack: 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.

Digital Footprint: Evidence of a person's use of the Internet. This includes anything that can be linked to his or her existence, presence, or identity.

Digital subscriber lines (DSL): A method for moving data over regular phone lines. A DSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same as those used for regular phone services. A DSL

circuit must be configured to connect two specific locations. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

Document Tracking: Recording activity from work processing applications such as MS Word, MS Office, or MS Works.

Domain Name: A domain name is a human-friendly name for a computer connected to a network. Domain names must be registered with an approved naming organization for their use to be legitimate. But even then, other organizations, primarily corporations, can object to their use if they infringe intellectual property rights - such as trademarks.

Domain Slamming: Changing a person's website domain service company without his or her consent.

Download: The verb, to download, means to access, save or "pull down" software or other files to one's computer from a remote computer via the internet. Frequently used for clickable links, e.g. "Download this file".

Dumpster Diving. The physical act of looking through trash containers for access codes or other sensitive information.

Email Bombing/flooding: A denial-of-service attack that saturates the victim's email capability. Simple email bombing involves sending hundreds or thousands of messages to a person's email address.

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.

File Transfer Tracking: Tracking files that have been sent to removable media drives like thumb drives, floppy discs, and rewriteable compact discs (CDs).

Filtering and Blocking: There are various means that can be used to prevent access to information on the internet. This essentially involves two methods - filtering and blocking. Filtering involves reading the content of packets of data looking for certain words or phrases. Those that contain those words are prevented from travelling further. Blocking works by looking for the IP address of the packet. Those packets going to or from a particular location are rejected and prevented from travelling further. Both filtering and blocking, if applied by the state, or an internet service provider, are effective but crude means of censorship.

Filtering: The act of restricting access to certain web sites (usually using software programs). For example, a filter might check the text on a web page with a list of forbidden words. If a match is found, that Web page may be blocked or reported through a monitoring process. Generally speaking, a filter lets data pass or not pass based on previously specified rules.

Firewall: A firewall is a software or hardware system installed on a computer that allows or denies traffic to and from the internet based on a set of rules. There are two basic policies in the configuration of a

firewall: a restrictive policy, by which all traffic is blocked except that which is explicitly allowed. A Permissive policy, conversely, allows all traffic except that which is explicitly denied. For example, the campaign the Take Back the Tech!, which deals extensively with issues related to women's online safety and privacy recommends using firewalls (such as Smoothwall) as a way to protect data and prevent unauthorized access to your computer.

Flaming: online fights using electronic messages with angry and vulgar language.

Geotagging: The process of adding geographical location, or label, to photographs, videos, websites, Short Message Service (SMS) messages, Quick Response (QR)/two-dimensional barcodes, or Rich Site Summary (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.

Global Positioning System (GPS): Space-based satellite navigation system that provides positioning, navigation, and timing/distance information; maintained by the United States government and freely accessible to anyone with a GPS receiver.

Guestbook: This page on a web site allows visitors to leave comments.

Hacker: A slang term for a computer enthusiast, a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject. The term is popularly used to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers themselves maintain that the proper term for such individuals is cracker.

Hacking: Using technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and denigrating the victim and/or VAW organizations.

Handles: The pseudonym used by individuals in online communication. Also referred to as "screen names", handles allow communication without revealing an individual's identity.

Happy Slapping: An extreme form of bullying where physical assaults are recorded on mobile phones or digital cameras and distributed to others.

Harassment/Spamming: Using technology to continuously contact, annoy, threaten, and/or scare the victim. This is ongoing behaviour and not one isolated incident.

Impersonating: Using technology to assume the identity of the victim or someone else in order to access private information, embarrass or shame the victim, contact the victim, or create fraudulent identity documents.

Information Communication Technology (ICT): Technologies that people use to communicate, share, distribute, and gather information. ICTs include computers, telephones, mobile phones, fax machines, internet, and satellite communications.

Internet relay chat (IRC): A service that provides real-time text messaging between individuals over the Internet. It is can be used by groups to communicate on discussion forums or "channels" or between individuals by communicating through private messaging. Most IRC platforms offer a file-sharing function.

IP Address: A unique identifier in the form of a numerical label assigned to each device, such as a personal computer or server, participating in a network, such as the Internet.

IP Spoofing: An attack where the attacker disguises himself as another user by means of a false IP network address.

Keylogger: Also called *keylogging* and *keystroke logging*, is the action of tracking (or logging) the keys struck on a computer keyboard. The device contains a small hard drive that records every key typed, including passwords, websites, instant messages and email. The device usually runs hidden in the background so that users are unaware of its presence or that their actions are being monitored.

Malware: Short-form for malicious software designed to access a computer system without the owner's knowledge or consent. Malware can include viruses, Trojans, spyware.

Mouse-trapping: Websites are set up in such a way that users can't leave the sites by clicking on the "back" or "home" button.

Malicious Distribution: Using technology as a tool to manipulate and distribute defamatory and illegal materials related to the victim and/or VAW organizations.

Netiquette: Refers to network etiquette, or a series of social conventions that govern how individuals interact online.

PacketSniffer: A program that reads or snoops on network traffic

Pharming: A form of identity theft. Cybercrooks obtain a legitimate website's IP (Internet Protocol) address and hijack Internet users as they attempt to go to a desired website, redirecting them to an identical-looking fraudulent website.

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 website, 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.

Port Scanner: A piece of software designed to search a computer for open software ports. This is often used by a person who breaks into a computer system with the purpose of inflicting damage or stealing data.

Recruitment: Using technology to lure potential victims into violent situations.

Remote Tracking Software: Remote tracking software is a program that is installed on the target computer and will send recorded activity to a remote location.

Rich Site Summary (RSS): Also referred to as Really Simple Syndication, Rich Site Summary is a family of web feed formats used to easily distribute a list of headlines, update notices, and sometimes content to a wide number of people. It is used by computer programs that organize those headlines and notices for easy reading.

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.

Screenshot: Also known as a screen capture, it refers to an image that is taken by the computer, capturing what is displayed on the computer or device's monitor/screen.

Security software: A generic term referring to any computer program that secures a computer system or computer network; the two main types of security software are virus protection software and software that removes adware and spyware (both require regular updating to remain effective).

Sexting: Sending sexually explicit or suggestive content between mobile phones or devices including text, images or video.

Short Message Service (SMS): A text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices.

Snapshot Tracking: Snapshot tracking will take pictures of the computer monitor every few seconds and store the activity in the order the pictures were taken.

Spam: Electronic junk mail or junk newsgroup postings. In addition to wasting people's time with unwanted email, spam also eats up a lot of network bandwidth. Consequently, there are many organizations and individuals who have taken it upon themselves to fight spam with a variety of techniques. But because the internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail.

SpoofingCard: A communication service that allows you to choose what phone number displays on caller ID when someone receives a call from you.

Spyware: Spyware is any software that covertly gathers user information through the user's internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs. Once installed, the spyware monitors user activity and transmits that information to someone else. Spyware can also gather information about email addresses and even passwords and credit card numbers. Spyware is similar to a Trojan in that users unwittingly install it when they install another product.

Surveillance/Tracking: Using technology to stalk and monitor a victim's activities and behaviours either in real-time or historically.

Technology-Related Violence Against Women: Misusing technologies, or ICTs, to facilitate violence against women.

Trojan: A computer program that is hidden within legitimate software, meant to modify, damage, or destroy the victim's information. Can also be used to create an opening in protection/security for further exploits.

Trolling: Intentionally posting provocative messages about sensitive subjects to create conflict, upset people, and bait them into "flaming" or fighting.

Virus: A software program that is designed to replicate itself, spread from one computer to another, and interfere with computer operation; a computer virus may corrupt or delete data on a user's computer, use an email program to spread itself to other computers, or even erase everything on a user's hard disk. Computer viruses can be spread by attachments in email messages or instant messaging messages; disguised as attachments of images, greeting cards, or audio and video files, and hidden in illicit software or programs that are downloaded to a computer.

Vishing: A form of identity theft. A scammer sends an email hoping to get the recipient to telephone a voice mail box to disclose personal information; also known as voice phishing.

Web bug: An object that is embedded in a webpage or email and is usually invisible to the user but allows checking that a user has viewed the page or email. One common use is in email tracking.

Webcam: A video camera that feeds images in real time to a computer or computer network; can be used to establish video links permitting computers to act as videophones or videoconference stations; also used for security surveillance, video broadcasting, and social videos (such as many viewed on YouTube).

Worm: A type of malware that replicates itself over and over within a computer.