Internet

Technology, Internet

Several crimes can be committed on the Internet such as stalking, identity theft and more. Most social networking and chat sites have a page about safety. Numerous groups, and governments and organizations have expressed concerns and are dedicated to the safety of children using the Internet. Safer Internet Day Is celebrated worldwide in February to raise awareness about internet safety. In the UK the Get Safe Online campaign has received sponsorship from government agency Serious Organized Crime Agency (SOCA) and major Internet companies such as Microsoft and eBay. Information Security[edlt source I edltbeta]

Sensitive information such as personal information and identity, passwords are often associated with personal property (for example, bank accounts) and privacy and may present security concerns if leak ed. Unauthorized access and usage of private Information may result In consequence such as Identity theft, as well as theft of property. Common causes of information security breaches include: Phishing[edit source I editbeta] Phishing is a type of scam where the scammers disguise as a trustworthy source in attempt to obtain private information such as passwords, and credit card Information, etc. rough the Internet. Phishing often occurs through emails and instant messaging and may contain links to websites that direct the user to enter their private information. These fake websites are often designed to look identical to their legitimate counterparts to avoid suspicion from the user. Internet Scams[edlt source I edltbeta] Internet Scams are schemes that deceive the user in various ways in attempt to take advantage of them. Internet scams often aim to cheat the victim of personal property directly rather than personal information through false promises, confidence tricks and more.

Malware[edlt source I edltbeta] Malware, particularly spyware, is malicious software disguised as legitimate software designed to collect and transmit private information, such as passwords, without the user's consent or knowledge. They are often distributed through e-mail, software and files from unofficial locations. Malware is one of the most prevalent security concerns as often it is impossible to determine whether a file is infected, despite the source of the file. Personal Safety[edit source I editbeta] The growth of the internet gave rise to many important services accessible to anyone ith a connection.

One of these Important services is digital communication. While this service allowed us to communicate with others through the internet, this also allowed the communication with malicious users. While malicious users often use the especially a concern to parents and children, as children are often targets of these malicious users. Common threats to personal safety include: Cyberstalking[edit Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization.

It may include the making of alse accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass. Cyberbullying[edit source I editbeta] Cyberbullying is often an extension of bullying outside the internet, and may take form in many different ways. For example, the malicious user might release images of the user without his or her consent.

Because cyberbullying often stems from real-life bullying, this is largely a social concern, rather than internet safety. Cyberbullying ccurs more frequently than real-life bullying as the internet provides often provides means to carry out bullying while allowing the perpetrator to remain anonymous and hidden, avoiding backlash in the process. Online Predation[edit source I editbeta] Online Predation is the act of engaging an underage minor into inappropriate sexual relationships through the internet.

Online predators may attempt to initiate and seduce minors into relationships through the use of chat rooms or internet forums. It is debated whether online predators is actually a threat to internet safety, as many ases take a long time to develop the relationship. As such, targets of online predators may see the relationship as a legitimate attempt at romance. Obscene/ Offensive Content[edit source I editbeta] Various websites on the internet may contain offensive, distasteful or explicit material, which may often be not of the user's liking.

Such material may sometimes be stumbled upon through chance and may have adverse effect on users, particularly children. Such websites may include internet pornography, shock sites, hate speech or otherwise inflammatory content. Offensive content may manifest in many ays, such as pop-up ads and unsuspecting links. Prevention[edit source I editbeta] Securing Information[edit source I editbeta] Keep shared information at a minimum[edit source I editbeta] Cyberstalking and identity theft often begins by malicious users identifying the user through identifying information provided by the user himself.

It is important to remember that information posted online may be seen by more people than is originally intended. Social networks make it simple to inadvertently share details about oneself (address, phone number, birthday, etc.), so as a precaution, it is best ot to input this type of information onto these websites. It is also a common occurrence for users to make the mistake of sharing small bits of information occasionally, and through the use of search engines and some research it is possible to piece these information together to identify the user.

As such, avoid sharing personal information and personal history whenever possible. When creating usernames, websites, or e-mail addresses, avoiding using anything that reveals any shared under any circumstances. Passwords[edit source I editbeta] Passwords are often created to keep personal information and property secure. If a password is compromised, it may lead to consequences such as financial theft from online services such as bank accounts. One common way that passwords may be compromised is through repeated guessing.

Weak passwords make this process easier, so it is important that passwords be strong. Creating strong passwords is a way of keeping information secure. A strong password may contain the following:[2] * At least 10 characters * Both upper and lower case letters * Numbers * Symbols (if allowed) * Does not contain dictionary words Avoid using simple passwords such as: " password", " 123456", " qwerty', " abc123", ames, birthdates, etc. Besides having a strong password, it is important to use different passwords for different accounts.

This prevents access to all internet accounts, should someone get hold of a password. It is also good practice to regularly change your passwords. PINs[edit source I editbeta] PINS, like passwords, are means of keeping information secure. A PIN may consist of at least 4 digits. Birthdays, birth-years, consecutive numbers, repeating numbers, and banking PINs should not be used as PINs for your internet accounts. Social Network Websites[edit source I editbeta] Profiles on social network websites may be seen by people you may not know.

These websites often have privacy settings that you can alter so you can control who sees you profile and what information they are allowed to see. Do not accept friend requests from people you dont know. Security Software[edit source I editbeta] Through the use of antivirus software, the user can automatically detect, prevent and remove computer viruses and various types of malware. Very often it is impossible for the user alone to identify infected files and software until it is too late, especially f the infected file or software is well disguised as legitimate files.

Because of this, it is important that the user keeps antivirus software running on the computer whenever accessing the internet so that the user can filter and block infected files. Firewalls[edit source I editbeta] A firewall is a program that controls incoming and outgoing internet traffic. Most operating systems come with firewalls. In order to keep your computer and information safe, it is important to keep the firewall on at all times when accessing the internet to prevent unauthorized access. Users are also able to control which pecific programs are allowed through the firewall as well as those that are not.

Keeping Up-to-Date[edit source I editbeta] Many computer software, such as operating systems, are not without flaws. Computer viruses often take advantage of these flaws to gain unauthorized access to a user's computer. When these security vulnerabilities are discovered they are often patched with security updates to eliminate the vulnerability. Operating systems, anti-viruses, and any other programs should be kept up-to-date with the newestsecurity updates in order to keep viruses and harmful software from taking advantage of

Be cautious of the internet. Avoid misleading ads, strangers with offers, strange e- mails, and questionable websites. Do research to verify the validity of these offers. If someone you know is sending you messages that don't seem like themselves, their account may have been taken over by somebody trying to get information out of you. [3] The best way to avoid scams is to be fully informed of the deal. Do some research for the following information:[4] * How exactly does the offer work? * How trustworthy is the person/company making the offer? What was the experience for other users regarding the same offer? Is the offer too good to be true? * Does the offer require payment in advanced? * Are there hidden costs unknown to the user? Avoid Illegal Activity[edit source I editbeta] Downloading torrents and illegal file sharing is a very common distribution method of malware and may inadvertently bring malicious software to your system. Parental Controls[edit source I editbeta] A good way to reduce the possibility of reaching offensive/obscene content is to set up parental controls.

Parental controls allow users and parents to place content filters on their computers while using the internet. Content filters limit access to age-appropriate content and any specified type of content the user may dislike. Most parents agree[dubious - discuss] that parental controls are important to limit children's access to unwanted content on the internet. Studies show[which?] they are under utilized or often not implemented at all. There are two main forms of parental controls hardware and software based systems. original research?] Hardware parental controls are installed between household devices and the internet service provider (ISP) such as a router with built in filtering. This parental control can filter ontent on all devices on a network. Software based parental controls can provide a more in depth solutions specific to each device it is installed on. These controls usually run undetected[citation needed] and in the background. Software controls can provide logs, keystrokes, and can range from broad to specific blocking mechanisms.

Public Computer[edit source I editbeta] Public computers, as opposed to personal computers, may be physically accessed by anyone within reach of the computer. Because of this, it is inadvisable to do any processes that involve sensitive information, such as online banking. A common way unauthorized access may occur is through users from public computers not fully logging out and clearing usage data (such as cookies), and allows access of the account to the next user of the public computer. It is also possible that the public computer be infected with malware, unknown to the user.

When using public computer terminals, remember to:[5] * Avoid saving private information such as usernames and passwords * Don't leave the computer unattended while logged in * Clear your browsing data when you are about to leave * Watch out for people looking over your shoulder Avoid entering sensitive information such as bank information Third Party Programs[edit source I editbeta] malware programs help prevent infections from occurring as well as detect and remove them from your computer.

A variety of programs are available for use with purchase such as Norton AntiVirus, McAfee VirusScan, and BitDefender Antivirus. There are also a many programs available for download for free such as Microsoft Security Essentials, AVG Anti-Virus, Avast! antivirus, andMalwarebytes' Anti-Malware. Ad and Pop-Up Blockers[edit source I editbeta] Misleading ads and pop ups can contribute to the accidental downloading of alicious software onto your computer. Most web browsers have internal pop-up blockers. These programs/web browser plug-insremove the ads.