Session-8

Internet Security

Internet security refers to computer security especially when we are online on Internet. It often involves browser security but also network security. Internet security is to establish preventive measures against attacks from hackers, phishers and online scammers. The Internet is as secured as safely we use it. Exchanging information may often involves high risk of intrusion.

Though Internet is a valuable and vast source of information. It is also the most preferred source and virtual place of entertainment. But it makes your computer prone to many online threats. Ensuring security of our login credentials on various sites like bank sites, our credit card and online banking information from unauthorized users is a must. Some web sites can also install Malware on the computer without user consent thereby leaving the computer damaged or insecure.

Online threats such as Phishing, email spoofing, chat spoofing, etc. can increase the chances of users getting compromised.You can reduce the risks by using best practices such as using Antivirus Software, Antispyware Software, Firewalls, strong passwords, etc. in addition to spreading awareness of the best practices.

Best Practices for Security

Use strong passwords, with combination of letters in both cases, numbers, and special characters which makes a password difficult to crack or guessed by others. Do not keep easy-to-guess obvious passwords like your birth date, birth place, friend's name, relative's birth date, mobile number etc. Change your pass word frequently at least monthly or fortnightly.

Most web sites like Gmail, Facebook, bank web sites and important transactional web sites check for password effectiveness when you register for the first time or change the password.

Following is a general guideline for managing strong passwords.

- Password length should be at least 10-15 characters if possible or allowed by the website or software.
- Do not repeat password while changing them. Many bank web sites do not allow this.
- Pass words should be a complex combination of numbers, letters and symbols.
- Avoid using same password for multiple sites.

Example of a strong password is k3xP%,7Ym[}

Web sites such as **www.strongpasswordgenerator.com** help generate random strong pass words. Go to www.strongpasswordgenerator.com and click *Generate strong password*. The pass word will be displayed.

Regular Data Backup: Regularly backup your data on an offline storage like external drive, disc or tape drive etc. You can restore it in case of data loss or computer hard drive crash. Keep the back up in a secured place away from unauthorized users.

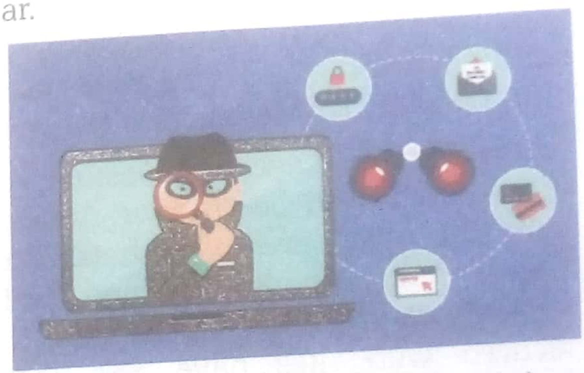
Encrypt Data by using a good encryption software. Some operating systems provide this feature also.

Secure your user name and password: Never save your security credentials in a place or location, which is shared among others such as cybercafé, shared drive etc. Do not set your browser to automatically login to your bank sites for automatic logon. Every time you visit such site, type the password always.

Do not share personal data; web sites require you to fill out forms containing fields such as name, gender, age, email address, school, etc. Be cautious when filling out such forms; research and verify if it's a trustable web site. Your email addressed could be used by unauthorized users to send you fake or unwanted emails; think twice or thrice before providing information to any website and decide if it is really necessary.

Secure transactions: If you are using online shopping or transactions, web sites even store your credit card or online banking personal information such as your credit card number, account details, etc. This information can be tracked and used by un-authorized users often known as hackers to misuse this information.

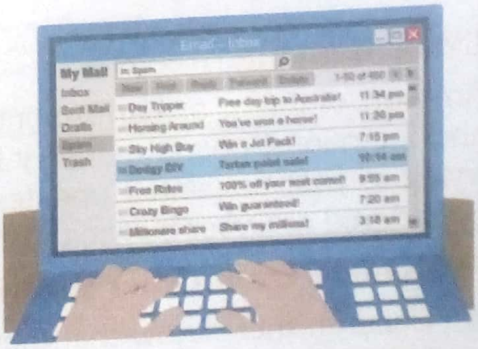
Again, ensure the web site is legitimate and uses secure practices for performing and maintaining online transactions. Since information such as credit card details or personal information is sent over the network, it is always recommended to use only secure web sites for such transactions. Verify if the web site uses secure transaction; usually it is indicated through a digital certificate represented as a golden lock in the web browser's address bar.



Use antivirus and antispyware software, computers are prone to attacks from software known as Malware that could har my our computer. Malware track browsing be havior or transmit personal data from your computer; programs such as key loggers could be in stalled on your computer track and transmit every key that is pressed on akey board (keystrokes) to unauthorized users.

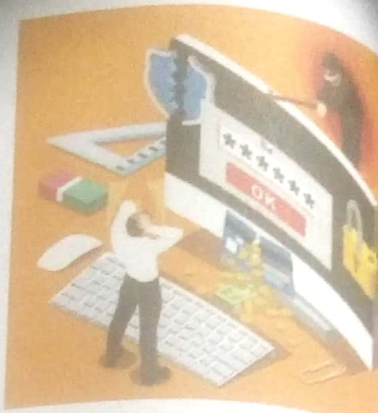
bitdefender
F-SECURE
Quick Heal
Windows Live OneCare
AVG
K7Computing
KASPERSKY
symantec.
VISION POWER
PANDA SECURITY
McAfee
AhnLab
TREND MICRO
ZONEALARM by Check Point
ca

Antivirus and Antispyware programs also offer real-time protection monitoring your computer for any changes by malware software. Keep your Antivirus an Antispyware software always up to date, this can help in protecting your computer from recent threats.



Do not immediately respond to mails from unknown users, it may be a fake mail trying to gather personal information such as your bank account details, home address, etc. Some mails could promise you jobs or announce lottery results which in turn could compromise the user. And in some cases, virus or scripts that are dangerous could be attached to the mail; NEVER open the attachment from an unknown source.

Clear browser cookies frequently, cookies are programs that are created on your local computer when you visit web sites. Though cookies are meant for storing data based on your activity performed during your earlier visit such as logon details, details of as hopping cart, visited pages in a website, etc. they could also be tracked by unauthorized users and possibly gain access to your personal information.

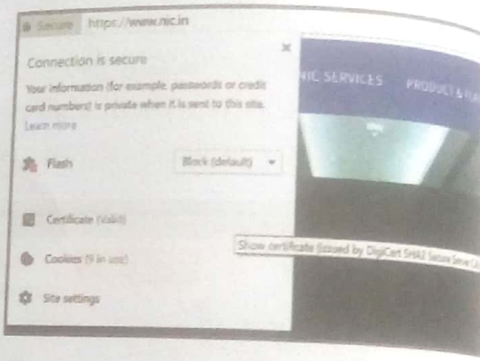


Keep the operating system and software applications up to date; though operating systems and applications are designed, tested and distributed, sometimes they may have security holes through which a hacker can take advantage; they may track and gather information or even damage the whole computer. In general, most vendors notify the users whenever a security hole is identified and an update is available to address that particular issue. You can also visit respective vendor's website to check if there are any updates available, download and keep your operating system and software applications up to date, free from security holes.

Instal lfirewalls: Firewalls could be software or hardware and can assist in keeping a computer a network secure. Firewalls analyze the network traffic and determine if the traffic should allowed or not. In most cases, operating systems such as Linux, Windows or Mac include fire software as a part of operating system thus keeping the computer secure. In rare cases, you r need to configure your firewall for additional security.

Never install software from unknown sources as they might not be trust worthy; download o from well-knownorreputed web sites. Verify the source if it is legitimate by searching the interne referring to comments from other users before downloading them; understand the nature and purpose of the software before attempting to download and install them.

Secured Socket Layer Certification is done for web sites by known authorised Certification Authorities (CA). CAs do not issue SSL certificates to phishers, spammers or any agency that is not properly identified and cleared. Check the website's certificate icon of a padlock in the address bar. All secured web sites have SSL (Secured Socket Layer) certificates. If padlock icon is of open lock then website is not secured and must be left immediately.



Secure https://www.nic.in

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
Learn more

Flash Block (default)

Certificate (Valid)

Cookies (9 in use)

Site settings

Show certificate (issued by DigiCert SHA2 Secure Server C

Remove unwanted or unknown software applications; these might have got installed without yo knowledge when you have visited some web sites. Unwanted software could get installed as th might have been bundled along with necessary software. Some programs such as toolbars g installed usually through bundled software and are programmed to send personal data witho your consent.

Cyber Bullying

Any sort of threat or harassment over internet is the act of cyber bullying. Messages in bad tas and intentions, online mockery in friend groups or circles, stalking someone's online profile an trying to post unwanted updates, sending unsolicited private messages, videos, and pictures ar considered as Cyber bullying that affects young minds intensely even up to the threats of death.

Protection from Cyber Bullying

- Children must know that their parents and teachers are always available for them when the face such problem.
- Children must know that no matters what, parents and teachers are their first support.
- Children should inform their elders about any incident that sounds nasty even remotely.
- Children must know the fact that cyber bullies are not capable to do any harm and they ca never carry out their claims of harming someone.

- Children are advised to block such intruders immediately and never entertain them.
- In case of cyber bully attack, save all his/ her messages offline as evidence for later use.

Malicious Smartphone Applications

Many smart phone applications seem attractive but in fact contain malicious code that steals information stored in the smart phone, such as the address book data without the owner's knowledge. The personal information stolen this way is forwarded to the hackers who abuse it to commit cyber crimes such as spam operations, billing frauds and cyber scams. Every trending app is not worth downloading.

Smartphone Safety Measures

- Set up emergency numbers for instant calling.
- Do not use cell phone everywhere – keep your senses free to perceive other stimuli like while crossing road, driving, using escalators, crowded areas etc.
- Get rid of unwanted data as soon as possible – keep your phone data tidy.
- Protect your phone from physical theft. Make it a habit to check while leaving any place.
- Keep good password and pattern protection.
- Keep the antivirus and software updated.
- Sign out of and close the apps that are used.
- Avoid automatic download settings.
- Keep your wireless access secured.
- Do not install just any app impulsively or in peer pressure.
- Keep a regular backup of your phone data.

Clearing Data Stored In Browsers

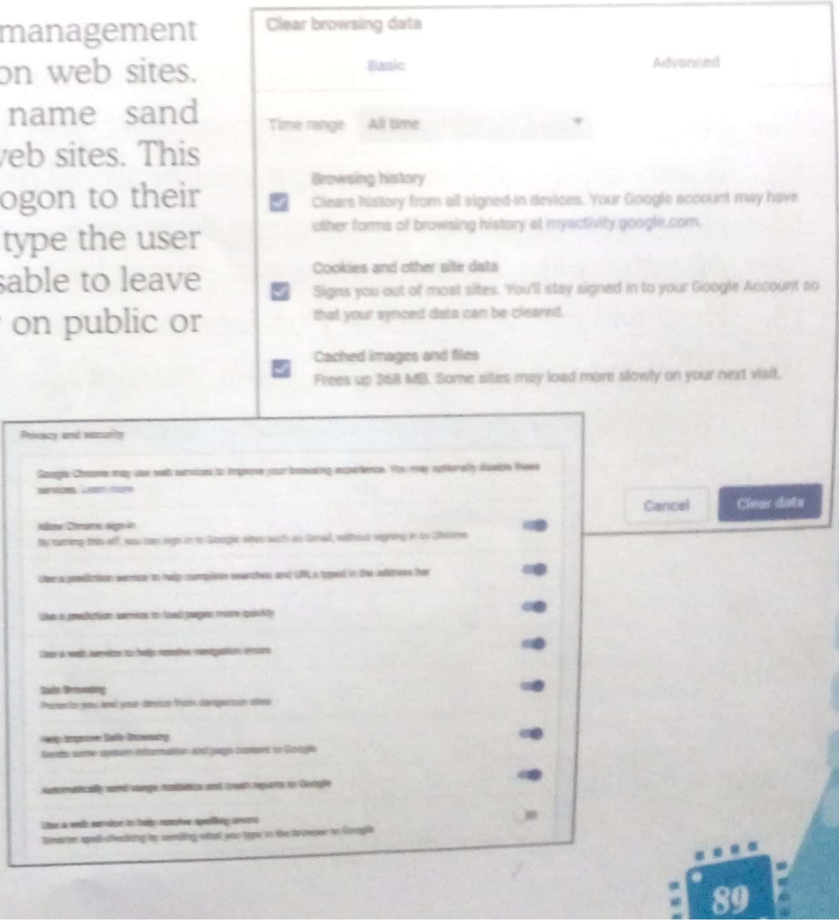
Web browsers have built-in password management designed to store passwords used informs on web sites. Browser soften prompt to save user name sand passwords when users attempt to logon to web sites. This facility is offered to users, so that they can logon to their frequently used web sites without having to type the user names or passwords. However it is not advisable to leave the web browser store this data particularly on public or shared computers.

To clear personal data from a web browser such as Google Chrome, launch the browser.

Click **Tools** Menu > **More Tools** > **Clear Browsing data...**

The next window will show various options to clear Browsing History, Cookies and Cache.

You can make changes in Privacy settings according to your preferences.



Clear browsing data

Time range: All time

☑ Browsing history
Clears history from all signed-in devices. Your Google account may have other forms of browsing history at myactivity.google.com.

☑ Cookies and other site data
Signs you out of most sites. You'll stay signed in to your Google Account so that your synced data can be cleared.

☑ Cached images and files
Frees up 368 MB. Some sites may load more slowly on your next visit.

Privacy and security

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

Allow Chrome sign-in — on
By turning this off, you can sign in to Google sites such as Gmail, without signing in to Chrome

Use a prediction service to help complete searches and URLs typed in the address bar — on

Use a prediction service to load pages more quickly — on

Use a web service to help resolve navigation errors — on

Safe Browsing — on
Protects you and your device from dangerous sites

Help improve Safe Browsing — on
Sends some system information and page content to Google

Automatically send usage statistics and crash reports to Google — on

Use a web service to help resolve spelling errors — off
Smarter spell-checking by sending what you type in the browser to Google