Security theory & definitions.

Sunday, 29 November 2020 5:23 PM

Hacking: Act of gaining illegal access to a computer system.

Viruses: Programs or program code that can replicate/copy itself with the intent of deleting or corrupting files or to cause harm in anyway.

Phishing: legitimate looking email (trick) sent out to a user, as soon as they click on to the link, or do as asked, they are re-directed to fake websites where their data is stolen.

Pharming: malicious code installed on a user's hard drive or on a webserver; this code will re-direct the user to fake websites without their consent or knowledge.

War driving: Act of locating and using wireless internet (wifi) connections illegally.

Spyware: A software that steals data by hiding itself and monitoring key presses and reading files and sending data (stolen) to its programmer (tracker).

Cookies: These are text files generated every time user visits a website. Cookies collect key information, preferences and interests in website items (for shopping) about the user. Websites through cookies can carry out user's tracking like when user bought one thing, they also bought something else in relation.
Cookies are used by the websites to form anonymous user's profile, so that user's could be suggested things or in other words users could be influenced.

Backups: These are ways to prevent accidental loss of data such as file deletion, software or hardware faults.

1. Make copies (backup) of files on regular basis.
2. Save data regularly.
3. Keep backup away from the computer
4. Big companies have pre-defined procedures to reduce incorrect operations and regular users' training to have proper data backuped and to avoid any/ frequent data loss.

SSL: Secured Socket Layer.
TLS: Transport Layer Security.

These are the protocols which are used when communication happens over the network to protect data from being seen/ tracked by unknown/unauthorised persons.
- It encrypts the data and use https to show green padlock to indicate secure website communications.

SSL & TLS Differences:
- TLS can be extended with newer methods of authentication.
- TLS may do session caching, as in we can resume existing TLS session.
- SSL uses old protocols and can't do caching.