Internet Security

Module 04

Simplifying Security.

What is Internet Security?

CSCU
Certified Secure Computer User

Internet security is an offshoot of computer security which focuses primarily on the Internet 01

Browser security, network security, and to some extent operating system security also falls under the ambit of Internet security 02

Browser security, one of the key aspects of Internet security can be enhanced in the following ways: 03

- Configuring Browser Security and Privacy Settings
- Keeping the Browser Updated
- Signing Up for Alerts
- Avoid Public or Free Wi-Fi
- Installing Security Plugins

What is a Web Browser?

- Web browser is a software application that allows users to access websites on the Internet
- Browsers translate web pages into readable human content using Hypertext Transfer Protocol (HTTP)
- HTTP is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the Internet

Commonly used Web Browsers:

Windows Edge

Google Chrome

Mozilla Firefox

Safari

How to Secure Web Browsers?

CSCU
Certified Secure Computer User

- Configuring Browser Security and Privacy Settings
- Keeping the Browser Updated
- Signing Up for Alerts
- Avoiding Public or Free Wi-Fi
- Installing Security Plugins
  - HTTPS Everywhere
  - Web of Trust

What are the Threats to Web Browsers?

CSCU

Java Browser Plugin- This plugin weakens the security of browsers, which leads to hacking of a system, and ultimately data theft

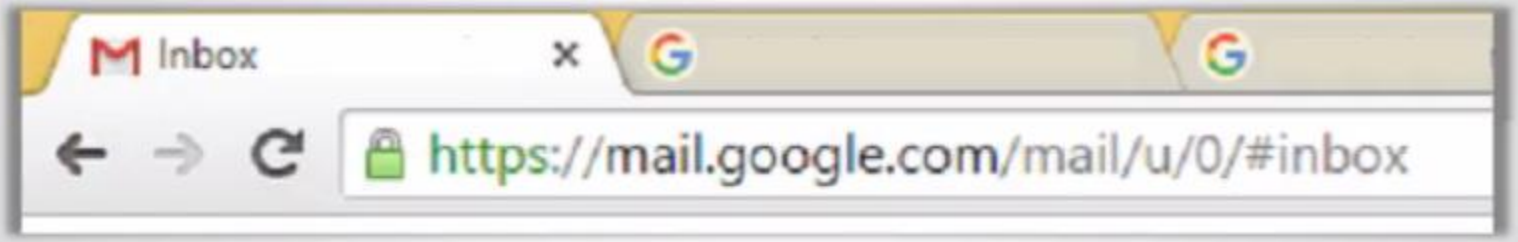
ActiveX- This software has several vulnerabilities and is often used by hackers to install malware on users' systems

Cookies- Cookies are files that record users' browsing history and are stored locally on their computers. They are also the primary reason for online privacy breaches and should be disabled wherever possible

Extensions- Extensions are small software programs that can modify and enhance the functionality of browsers. Some extensions on browsers are used by hackers to inject malware onto computers

How to Identify a Secure Website?

A website is said to be secure if the URL contains a lock symbol and https://



What is Instant Messaging?

01

Instant Messaging is a method of communication in which messages are exchanged through a software application in real time

02

Instant messaging services alert users if somebody on their list of correspondents is online

03

Features of instant messaging are given below:

- Instant messages
- Sharing of web links
- Sharing of videos, photos, music, and files

What is Instant Messaging? (Continued)

The following example illustrates the list of events that take place behind the scenes when 2 people communicate through an instant messenger:

- Annabeth instructs the instant messaging client to send a text-message to Percy. The client creates a packet containing the message and sends it to the server
- Server looks at the packet and determines that Percy is the recipient. The server then creates a new packet with the message from Annabeth and sends it to Percy

What are the Security Issues Regarding Instant Messaging?

Privacy issues caused by IM clients include personal information leakage, IP address exposure, and loss of confidential information

Anyone can impersonate anyone else on the Internet. Users have no way of finding out whether people with whom they are communicating are real, or just a fake username

Any of the instant messaging clients that allow file transfers could allow infected files to bypass the antivirus protection. These infected files download malware onto the system and cause harm to the computer

Just like any other software application, popular IM clients have a history of common security vulnerabilities. Installing an IM client may introduce new vulnerabilities to a computer system

How to Mitigate the Security Issues in Instant Messaging?

CSCU

Do not set IM client to automatically accept file transfers. This will prevent the download of virus-infected files

Always verify the origin of a file received through an IM client and scan it with anti-virus software before opening it

Do not click on URL links on an instant message that is sent from an unknown source

Do not send personal information through an instant messenger. If it cannot be avoided, encrypt the personal information before sending it

Keep the instant messenger (and other system components) up-to-date with the latest patches, enable personal firewall protection, and install anti-virus software

Child Online Safety

01

With over a trillion unique web pages as of 2008, children can be exposed to a vast variety of content

02

These web pages have all sorts of content from porn to political doctrines

03

A large portion of online content is not fit to be viewed by children

04

Taking measures to shield children from such content and monitoring their online activity is the first step towards child online safety

What are the Risks Posed by the Internet on Children?

CSCU

- Access to inappropriate content such as pornography, hate messages, and explicit photos
- Becoming victims of cyberbullying
- Online predators purchase domain names such as the .com equivalent of a popular .gov or .org website, knowing that web surfers are likely to end up on their site instead of their desired destination. For example, if a child is seeking information on the White House, he may find himself on a porn site instead of the official site at www.whitehouse.gov.
- Grooming is one of the major risks faced by children online. It refers to an act of befriending and establishing emotional connection with children, so as to prepare them for child abuse
- Pedophiles use social networking websites & chat rooms (sometimes posing as children or teenagers themselves) to initiate conversations with likely victims.

What Symptoms Do Children, Who Are Abused Online, Display?

1. More than normal time spent on computers
2. Presence of pornographic material on their computers
3. Switching to different screens when parents approach
4. Receiving phone calls from unknown people
5. Looking depressed and losing interest in everything

Guidelines to Protect Children from Online Threats

CSCU

- Ensure the child has knowledge regarding online threats
- Monitor the child's usage of the computer
- Restrict access to inappropriate websites using Internet filtering software
- Monitor the child's social networking profile
- Ensure the child doesn't provide any personal information to strangers
- Notify the police if the child is in regular contact with a stranger

How to Report an Internet Crime?

Reporting an Internet crime is similar to reporting a normal crime—it should be reported to your nearest neighborhood Police Centre or Police Station.

What Actions To Take When a Child Becomes a Victim of Online Abuse?

Ignore any communication from the online predator

Avoid logging on to the website where the bullying occurred

Block the cyber bully's email, so that they cannot contact the child again

Delete the child's social networking account if necessary

KidZui (Children Friendly Internet Software)

The search engine in KidZui is secure and includes search results, spelling corrections, and graphical representation

It has numerous websites, games, videos, and photos which have been approved kid-friendly by parents

Children can share content with each other without the looming threat of online predators

KidZui community allows children to chat with each other safely

Thank You