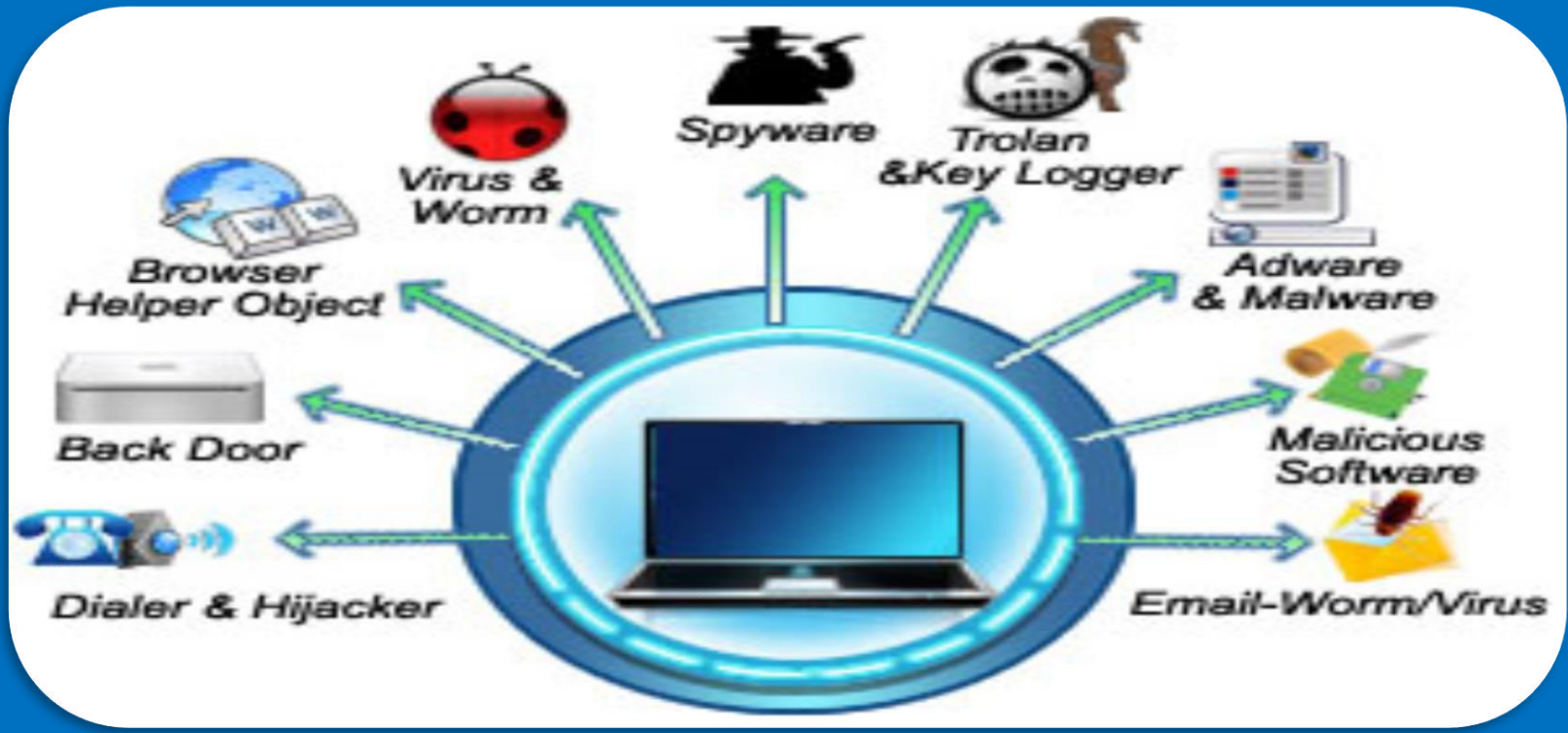
MALWARE


Spyware
Trolan
&Key Logger
Virus &
Worm
Browser
Helper Object
Adware
& Malware
Back Door
Malicious
Software
Dialer & Hijacker
Email-Worm/Virus

MALWARE

Malware is short for **"malicious software".**

Malware is any kind of unwanted software that is installed without your adequate consent

Example: **virus, worms,** and **Trojan horses** that are often grouped together and referred to as malware.

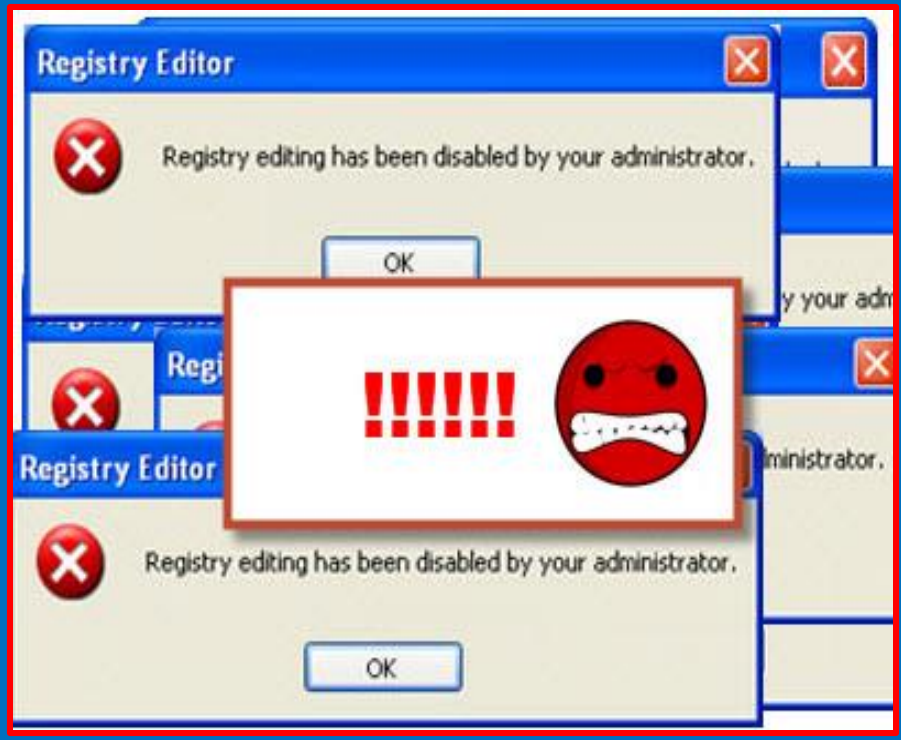
MALWARE

Trojan Horse

A Trojan horse is a program/malicious code that is disguised as another unharmful program to make you download it to get into your computer and infect it.

VIRUS : VITAL/VIRTUAL INFORMATION RESOURCE UNDER SEIGE

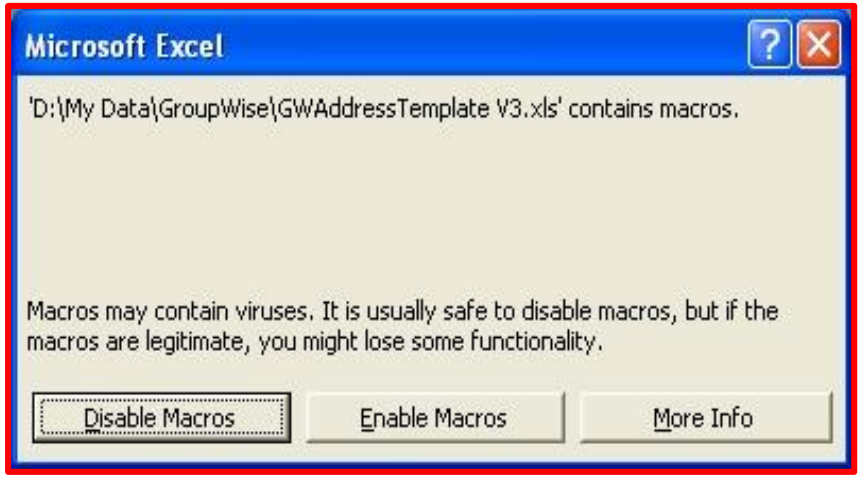
Computer virus refers to a program which damages computer systems and/or destroys or erases data files.



VIRUS:TYPES

Macro Virus

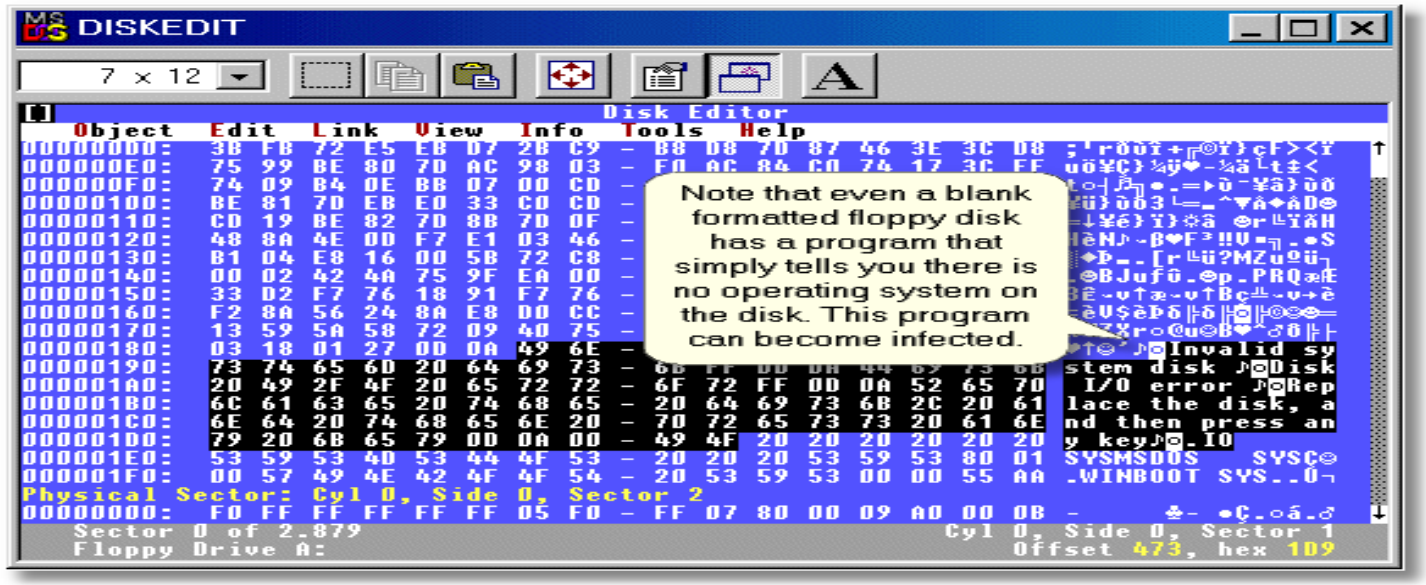
A **macro virus** is associated with application software like word and excel. When opening the infected document, it gets inserted in to office files automatically. According to the reports, **Melissa infected** more than 250,000 computers around the globe in just three days.



VIRUS:TYPES

➢ Boot Sector Virus

A **boot sector virus** infects boot sector of computers. During system boot, virus is loaded into main memory and destroys data stored in hard disk.



VIRUS: TYPES

- **Time Bomb**

A time bomb is a virus program that performs an activity on a particular date and time.

- **Logical Bomb**

A logical bomb is a destructive program that performs an activity when a certain action has occurred.

VIRUS: TYPES

Multipartite Viruses:-A multipartite virus is a computer virus that infects multiple different target platforms, and remains recursively infective in each target.

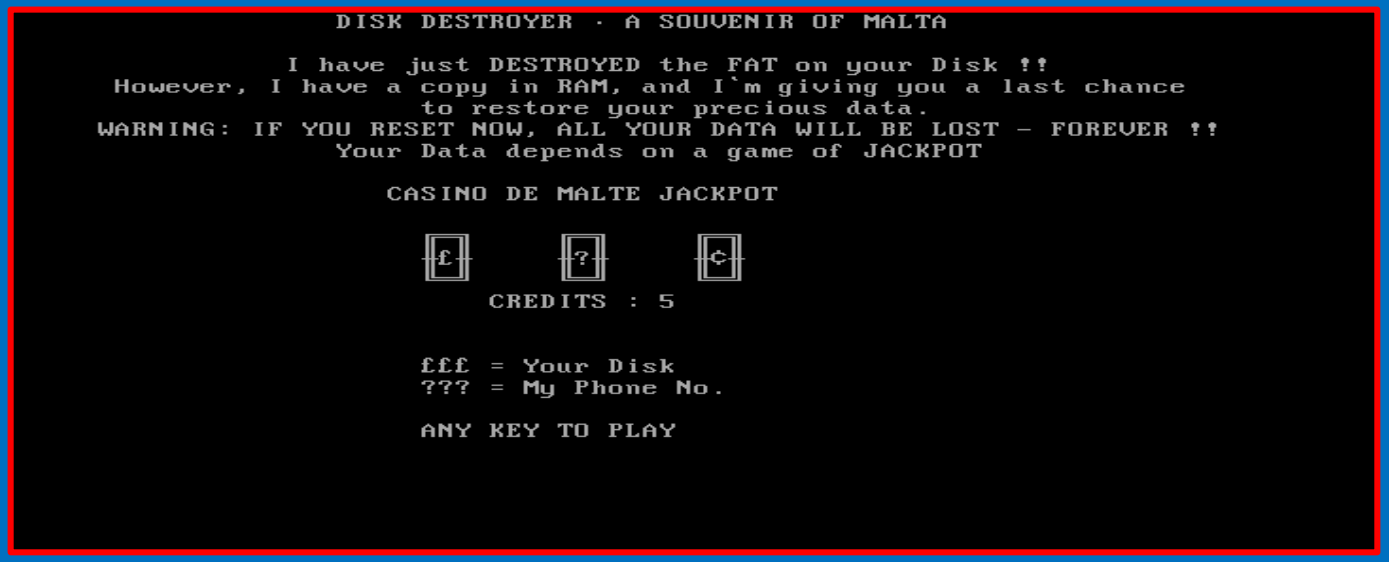
This type of virus can re-infect a system over and over again if all parts of the virus are not eradicated.

VIRUS: TYPES

- **Stealth Viruses:-**These viruses are stealthy in nature means it uses various methods for hiding themselves to avoid detection. They sometimes remove themselves from the memory temporarily to avoid detection by antivirus. They are somewhat difficult to detect.

VIRUS: TYPES

Polymorphic Viruses:-Polymorphic viruses have the ability to mutate implying that they change the viral code known as the signature each time they spread or infect. Thus an antivirus program which is scanning for specific virus codes unable to detect it's presence.



WORM

- Small piece of software that uses computer networks and security holes to replicate itself.
- Copy of the worm scans the network for another machine that has a specific security hole.
- Copy itself to the new machine using the security hole and start replicating.

DIFFERENCE BETWEEN VIRUS AND WORM

Virus

- spreads from program to program, or from disk to disk
- uses each infected program or disk to make copies of itself
- destroys data or erases disks

Worm

- uses computer hosts to reproduce themselves
- travel independently over computer networks
- resides in memory rather on disk

ACTIONS TO PREVENT VIRUS INFECTION

- Always update your anti-virus software regularly after a time interval.
- Back up your important files and ensure that they can be restored.

ACTIONS TO PREVENT VIRUS INFECTION

- Get trained on your computer's anti-virus software and use it.
- Have multiple backups of important files. This lowers the chance that all are infected.
- Install security updates for your operating system and programs as soon as possible.
- Jump at the chance to learn more about your computer. This will help you spot viruses.

SPYWARE

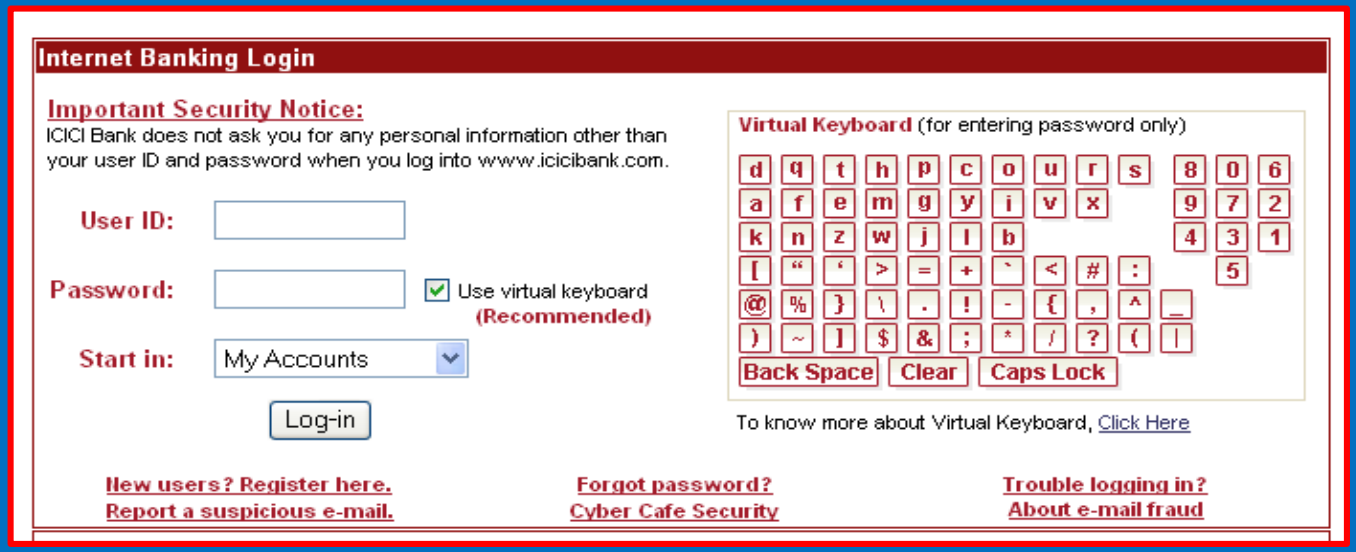
Spyware is tracking software which can be used to gather information of a person or organization. Spyware can be hardware or software both.

SPYWARE

How keylogger works: It saves when user types.

SPYWARE

Prevention from key logger(h/w): To prevent from this user should opt for virtual keyboard. If someone is not pressing keys of keyboard then nothing would be saved.



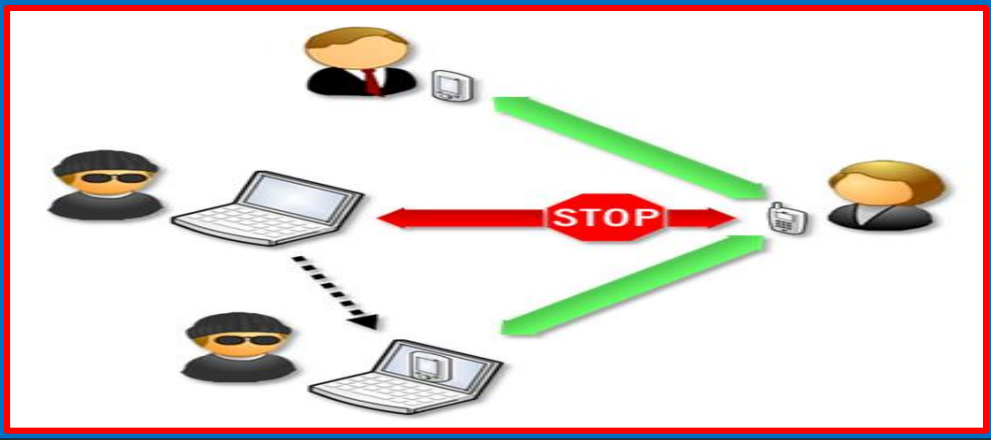
SPOOFING

The word **"spoof"** means to trick or deceive. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

Several different ways of Spoofing

E-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user.

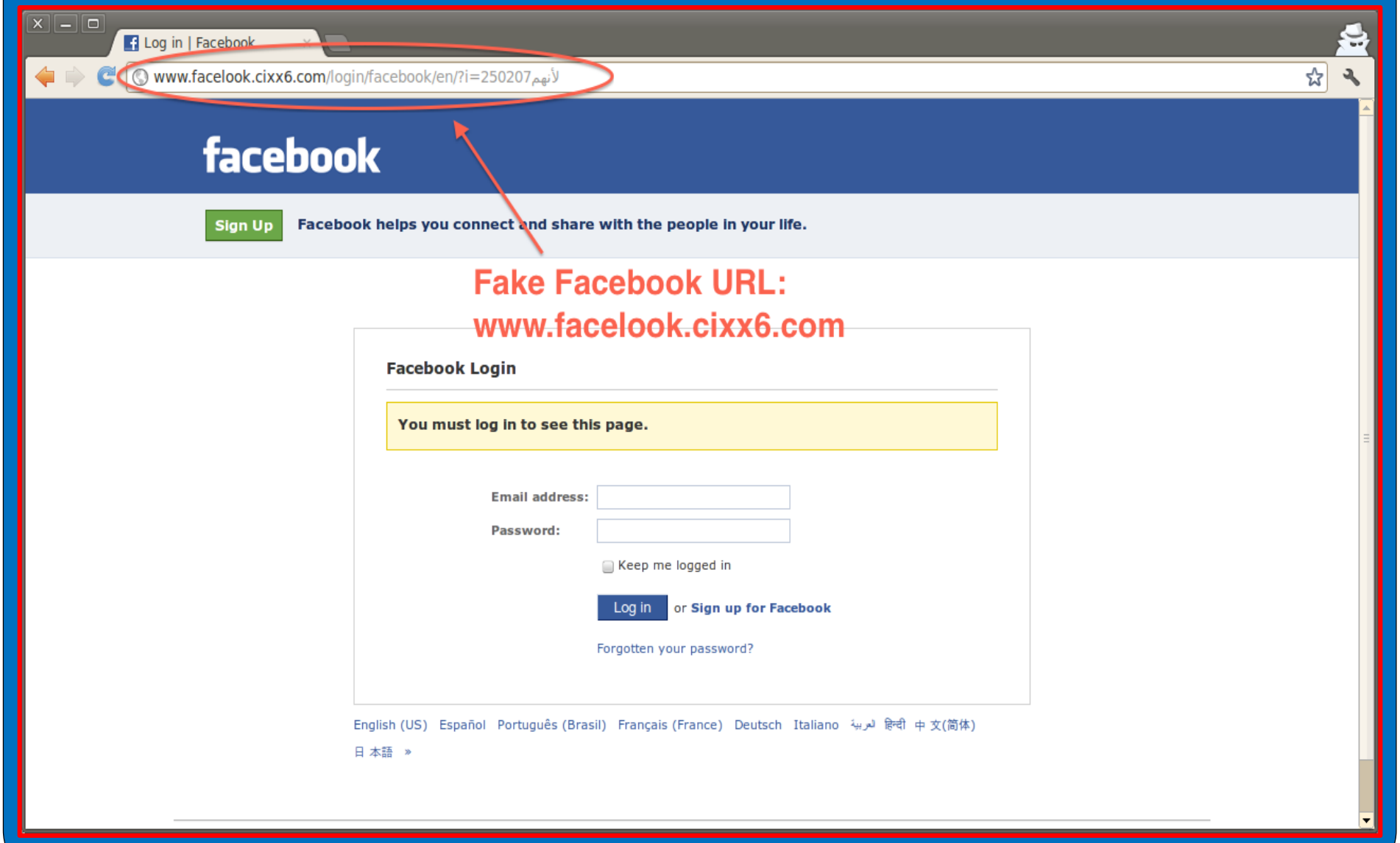
IP spoofing This involves masking the IP address of a certain computer system



PHISHING

- A phishing attack involves one website, successfully masquerading as another by falsifying data and there by being treated as a trusted system by a user.
- The purpose of this is usually to fool users into revealing confidential information such as user name and password, to the attacker.

PHISHING : HOW IT WORKS



HOW TO PREVENT FROM PHISING

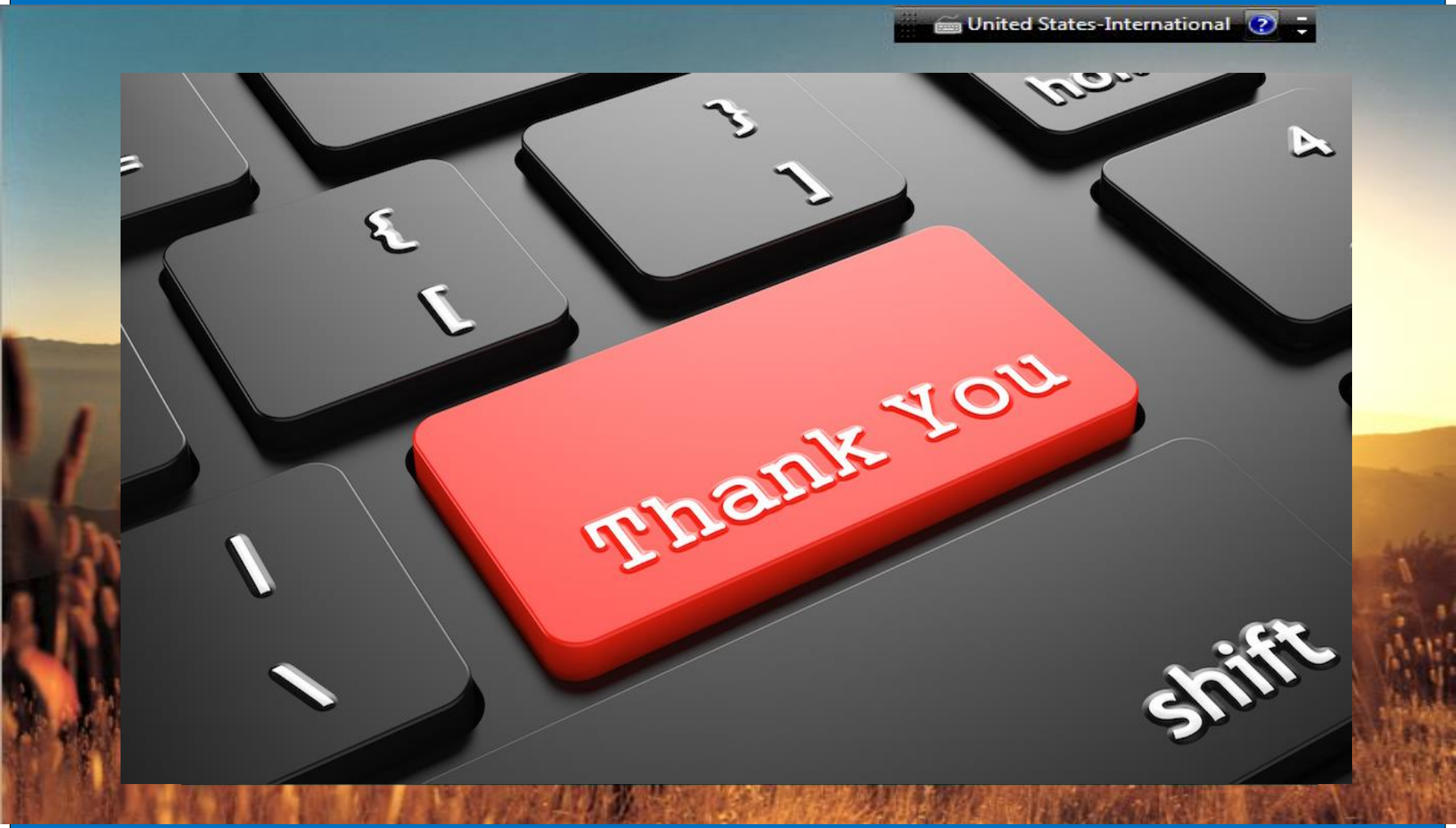
- Never share your net banking details with anyone. No any bank asks for this.
- Never open and login any bank site through URL given in any mail.
- Always open any website with https.

HACKING

- illegally or unauthorized access of an computer is called hacking.
- The person who does hacking is called hacker.

ETHICAL HACKING

Ethical hacking is a term that describe hacking performed to help a company or individual identify potential threats on the computer or network.


United States-International
Thank You
shift