certin
Handling Computer Security Incidents

Broadband refers to high-speed network connection

*Traditional Internet services are accessed in "**dial-on-demand**" mode, whereas broadband Internet is an "**always-on**" connection, therefore security risk is very high*

Without our knowledge, computer can be compromised and it can also be used as a launching pad for carrying out disrupting activities on other computers

Since broadband Internet is widely used, it is very important for every citizen to securely configure it for safe usage

Broadband Security Threats

- As broadband Internet connection is "Always On" , it leads to intentional misuse through
  - Trojans and backdoors
  - Denial of Service
  - Intermediary for another attack
  - Hidden file extensions
  - Chat clients
  - Packet sniffing
- Default configurations are extremely vulnerable

Types of Broadband Modem

- Wireless Fidelity (Wi-Fi)
- Digital Subscriber Line (DSL)
  - Asynchronous Digital Subscriber Line (ADSL)
  - Very high speed Digital Subscriber Line (VDSL)
- Cable Modem
- Satellite
- Broadband over Powerlines (BPL)
- Terminal Adapter Modem
- Universal Serial Bus (USB)

Anti-socialism groups use unsecured Wi-Fi networks to send terror e-mails

⬇

Prevent your wireless network to become such a hot spot by securing it

certin
Handling Computer Security Incidents

Broadband Modem Setup

- Always read the manufacturer's manual carefully and follow the guidelines, while setting up broadband modem.
- Insert the power source into the modem and then plug the other end of it into the wall socket.
- Before connecting the modem to the computer, check for proper functioning of the computer.
- While setting up the modem, follow instructions specific to the type & model of the modem.
- In case of signal via cable, connect the modem with the cable wire provided.
- In case of ethernet, connect the modem to the ethernet port of the computer.
- In case of USB connection, connect the modem after the computer is properly initialised.
- Wait until the indicators on the modem are lit.
- Install the modem driver and associated software provided along with the modem.
- To initialize the connectivity the proper user credentials need to be given and response should be awaited before use.

Guidelines for Securing Broadband Internet Access

Do's

✓ Always download broadband drivers from th legitimate websites recommended by the manufacturer.

✓ Regularly download the firmware (driver code)

✓ Always use the power adapter supplied by the manufacturer along with the modem.

- ✓ In case of terminal adapter modem make sure that filter is enabled for broadband lines. To filter unnecessary noise generated during the transmission.
- ✓ ***Change Default Administrator (Passwords and User names) :***

  In order to allow only authorized access to the equipment, change the default adminstrator or admin password of broadband router modem, as these details are given by the manufacturer which are common to all modems and can be misused by anyone.
- ✓ ***Assign Static IP Addresses to Devices:***

  Most of the home users are allotted dynamic IP addresses, as DHCP technology is easy to setup. This may even helps the attackers who can easily obtain valid address from DHCP pool. Therefore turn off DHCP option in router or access point and use fixed IP address range.
- ✓ ***Enable MAC Address Filtering:***

  Every device is provided with an unique MAC address. Broadband access points and router & provide an option for the user to combine the MAC addresse of the home equipment for access. This facilitates to allow connections only from those devices.
- ✓ ***Enable Wireless Security:***

  Modem routers support wireless security.User can select any one protocol and a protection key. The same wireless security protocol and protection key has to be enabled in computer.
- ✓ ***Turn on (Compatible) WPA / WEP Encryption:***

  All Wi-Fi enabled modems/router support some form of encryption technology, which has to be enabled.
- ✓ ***Change the Default SSID (Service Set Identifier):***

  All the access points and routers use a network name called SSID. Manfacturer normally ships their products with the same SSID set. As it can be misused by the attacker to break into the network / computer, it is neccesary to change the default SSID while configuring wireless security.

- ✓ Use effective end point security solution (with anti virus, anti spyware, desktop firewall etc) to protect computer/ laptop from broadband Internet security threats.
- ✓ ***Enable Firewall on Modem Router as well as Computer:***

  Broadband modem routers contain built-in firewall feature, but this option has to be enabled. Computer connected to the broddband modem also needs to be protected with desktop firewall.
- ✓ ***Turn off Modems during extended periods of Non-Use:***

  Shutting down a network will certainly prevent outside unauthorized people breaking into the network. Since it is very difficult to frequently turn on and off the devices, it can be considered during travel or extended offline period.
- ✓ In case of USB broadband modem, disconnect and remove the device after usage.
- ✓ Install broadband Internet bandwidth usage monitoring tool.
- ✓ Enable SSH (secure channel) for remote administration.

Guidelines for securing Broadband Internet access :

Dont's

- x Don't enable the option for remote administration (via Internet), as it is not required for a home user.
- x Don't enable the option "**Restore Factory Default Setting**" in broadband modem.
- x Don't use connection without a filter for each broadband Internet line.
- x Don't tap the line before the splitter (a small dvice that separates phone line from data / PC port).
- x Don't use USB broadband modem with insecure computer/laptop.

- x ***Do not Enable SSID Broadcast:***

  In Wi-Fi networking, wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals.This feature was designed for businesses as well as to access public hotspots. For a home user this feature is unnecessary and can be an entry point to break into the network.
- x ***Do not Enable Auto-Connect to Open Wi-Fi Networks:***

  In case if Auto-Connect setting is enabled, computer with Wi-Fi interface can connect automatically without notifying to the user.This may expose our computer to security risks.This setting should not be enabled except in specific cases.
- x Do not leave broadband connectivity open when it is not utilized.
- x Never connect to unkown or untrusted network in case of Wi-Fi.

Points to be remembered

- ✓ *The setup, configuration and the features may vary from model to model.*
- ✓ For more information please refer manufacturer's manual.

Many home computers are victims of cyber criminals

↓

Prevent your computer from becoming a victim by securing it