

*Leading a Secured Digital
Life.....*

INFORMATION SECURITY AWARENESS

*keeping yourself and your family safe in a tech
driven world*

Desktop Security

www.infosecawareness.in



Information Security
Education & Awareness
Project Phase - II

PURPOSE OF ISEA



Information Security Education & Awareness

Ministry of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

- Generation of Core Research manpower
 - Formal, Non Formal Courses
 - Faculty Training
 - Short term/Specialized courses for Professionals
- Training for Government Personnel
- Awareness Campaign

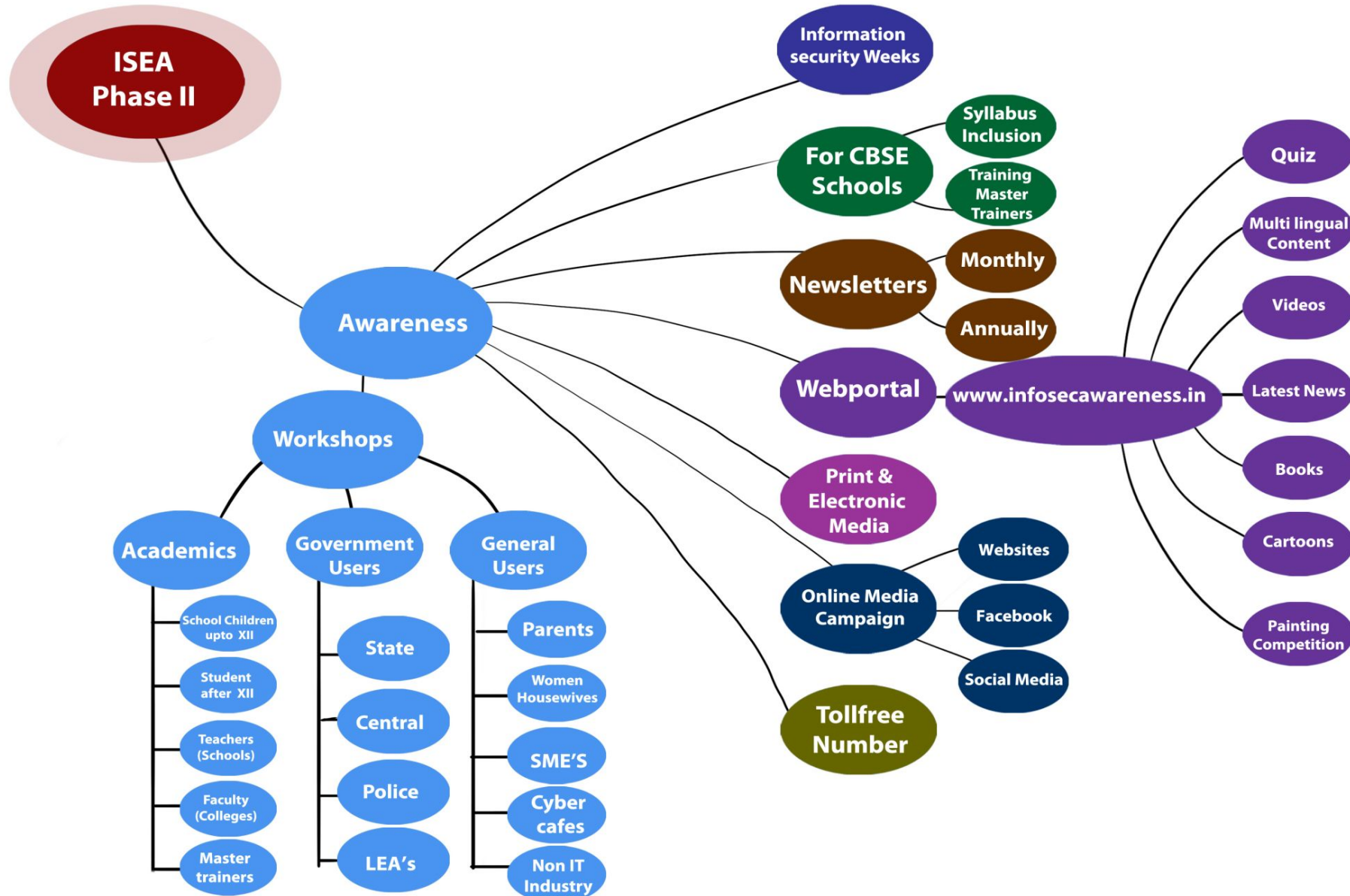
Implementation Structure

Area	Category	No's	Description
Academic	ISRDCs	4	IISc. Bangalore, IIT – Bombay, Madras, Guwahati
	RCs	7	IIT-Roorkee, Kharagpur ; NIT-Jaipur, Surathkal, Rourkela, Surat, Warangal
	PIs		
	Category I	23	10 NITs, 5 IIITs, 2 CoE, etc.
	Category II	13	13 CDAC & NIELIT Centres
	Category III (Special Category)	5	5 State Technical Universities -Gujarat, West Bengal, Tamil Nadu, Madhya Pradesh and Telangana
	Total	52	

Area	Category	No's	Description
GOT	Implementing Agencies	16	12 CDAC & NIELIT Centres, ERNET, NIC, CERT-In, STQC

Area	Category	No's	Description
Awareness	--	1	CDAC Hyderabad (through RCs, PIs, etc.)

Delivery Mechanism

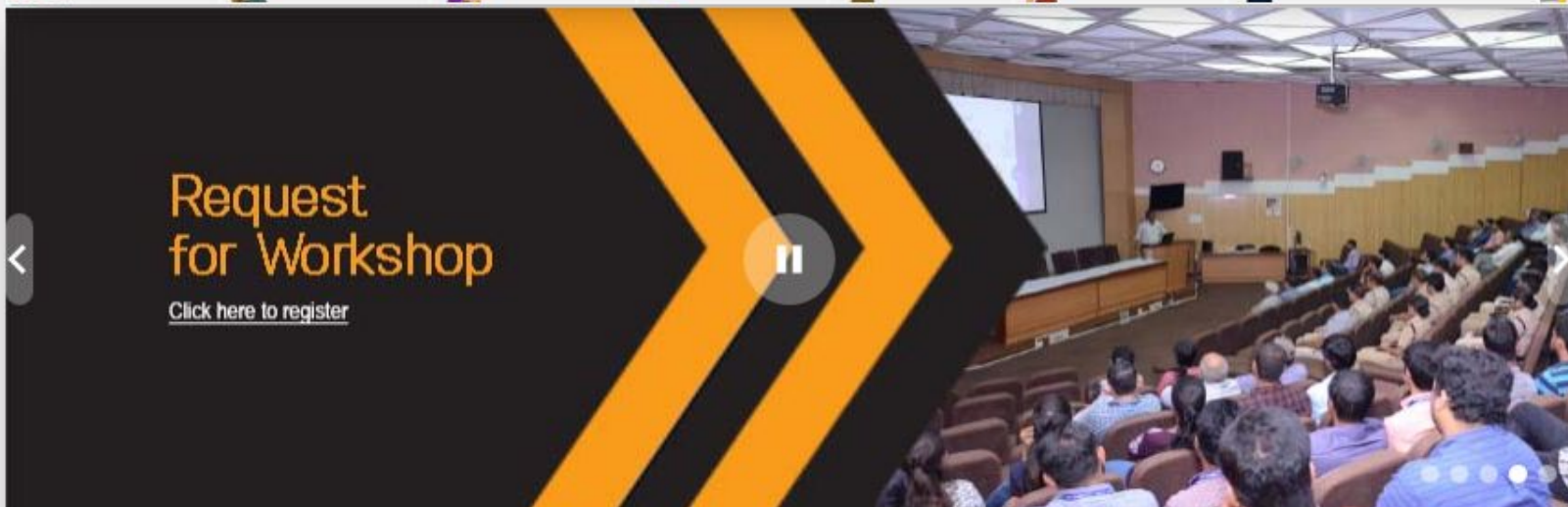




Search



- Children
- Student
- Women
- Family
- Police
- Teacher
- Govt Employee
- System/Network Admin



Security Awareness COVID-19 Tips

Not all cold and cough are symptoms of COVID-19. Get proper information from genuine sources

Not all free antivirus software protect your systems. Install genuine paid antivirus software and protect your systems

Seemore

ANNOUNCEMENTS National Level Competitions will be announced on 25th September, 2020. [Click here to view a](#)

Tip of day

WORKSHOPS 259
PARTICIPANTS 18009

WORKSHOPS 652
PARTICIPANTS 73746

WORKSHOPS 42
PARTICIPANTS 10244

Latest Events

Latest News

- » Ransomware through .adobee and .rooe extension
- » Cyber crime in India mostly targets business email, says police official - PTI
- » Banking industry a "target of choice" for

Facebook

Information Secu...
Like Page

Tip of the Day
11 September 2020

Twitter @InfoSecAwa

Tip of the Day
09 September 2020

Never leave an e-mail account unattended if it is logged in, unless a





Children



Student



Women



Family



Police



Teacher



Govt Employee



System/Network Admin

Home > Downloads > Handbooks

Handbooks

Children Handbooks

Cyber Awareness

Master Trainers

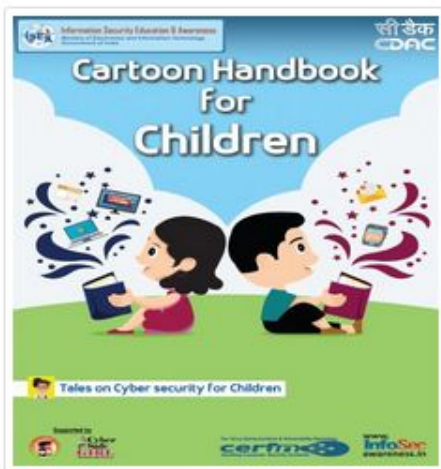
Women Handbooks

Digital Financial Transactions

Security Concepts

ISEA Handbooks

Secure Your Electronics



Cartoon Handbook for Children



Cartoon Handbook for Children in Telugu



Online Safety for Children



Online Safety Tips for Children at Home





*Leading a Secured Digital
Life.....*

www.
InfoSec
awareness.in

Online Teachers Training on Cyber Safety and Security

*keeping yourself and your family safe in a
tech driven world*

www.infosecawareness.in

Toll Free No. 1800 425 6235



www.isea.gov.in

[www.
InfoSec
awareness.in](http://www.InfoSecawareness.in)

Desktop Security



Toll Free No. 1800 425 6235



www.isea.gov.in

[www.
InfoSec
awareness.in](http://www.InfoSecawareness.in)

" The olden phrase is
always golden...
Prevention is Better than
Cure."

New Phrases of Security:

“Prevention is Better
than Fraud”

“Prevention is Better
than a Security Breach”

“Prevention is Better
than Data loss”



www.isea.gov.in

[www.
InfoSec
awareness.in](http://www.InfoSecawareness.in)

Desktop Security

Why to secure a Desktop

- ⦿ A personal computer used without proper security measure could lead to exploiting the system for illegal activities using the resources of such insecured computers
- ⦿ The results may be data theft, data loss, personal information disclosure, stealing of credentials like passwords etc.
- ⦿ Protecting and securing Personal Computer before it is compromised

Starting from Installation

- Installation of Licensed Operating System and applications
- Read the “Terms and Conditions” / “License Agreement” provided by vendor/software before installation

Look what is being installed

- Use the authorized software provided by the Vendor/official websites to install your
- Motherboard drivers
- Monitor drivers
- Audio & Video drivers
- Network drivers
- Any other software....



BIOS Settings

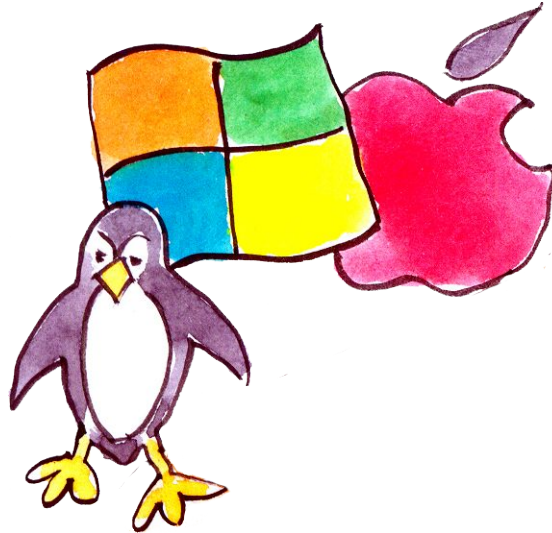
- **BIOS (Basic Input / Output System) Settings**
 - Computers BIOS is the first program that runs when computer is started. You can tell the BIOS to ask for a password when it starts, thus restricting access to your computer



- Q.1 What is BIOS
- Board Input/Output System
- Basic Input/output Security
- Basic Input/Output System
- Border Input/Output Security

Operating System

- Operating System is the important program that runs on the computer
- It is responsible for us to secure the system by not allowing the unauthorized users to access the system



OS Security

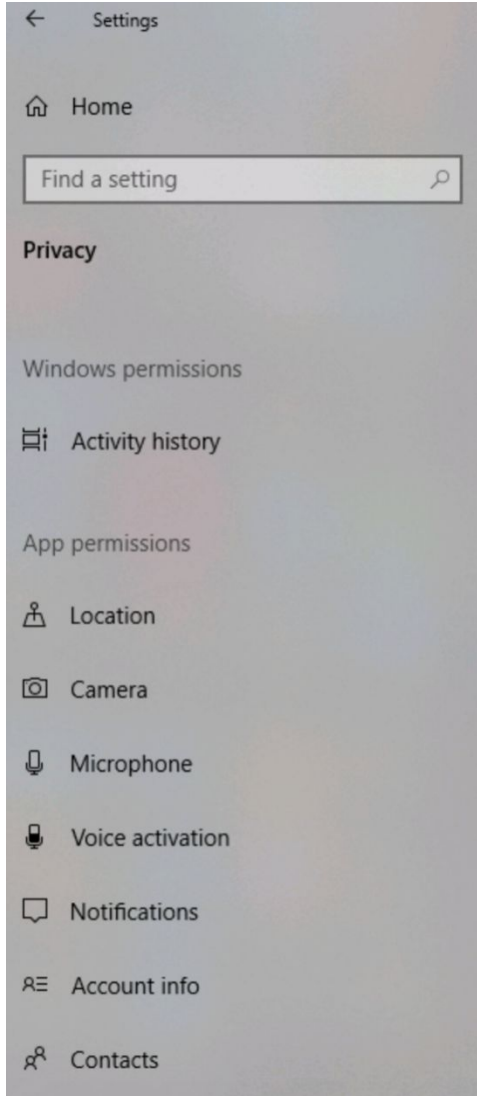
- ◉ Enable Auto-updates of your Operating System and update it regularly.
- ◉ Strong password should be used for “Admin” Account on computer and for other important applications like E-mail client, Financial Applications (accounting etc).
- ◉ Backup: Periodically backup your computer data on CD / DVD or USB drive etc.. in case it may get corrupted due to HardDisk failures or when reinstalling/format ting the system.
- ◉ Recovery Disk: Always keep recovery disk supplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failures due to system changes such as uncerificated Drivers/unknown Software publisher.
- ◉ Startup programs should be monitored / controlled for optimal system performance.



System Account Password

- Password represents the identity of an individual for an account





Location

Allow access to location on this device

If you allow access, you will enable Windows to use your device's capabilities to determine your location and Microsoft will use your location data to improve location services. People using this device will be able to choose if their apps have access to location by using the settings on this page. Denying access blocks Windows from providing location to Windows features, Microsoft Store apps, and most desktop apps.

Location for this device is off

Change

Allow apps to access your location

If you allow access, you can use the settings on this page to choose which apps can access your device's precise location and location history to enable location-based experiences such as directions and weather. If you are signed in with a Microsoft account on this device, your last known location is saved to the cloud, and shared with other devices where you are signed in with your Microsoft account. Denying access only blocks the apps listed on this page from accessing your location.

Off

Some desktop apps may still be able to determine your location when settings on this page are off. [Find out why](#)



www.isea.gov.in

www.
InfoSec
awareness.in

← Settings


Home

Find a setting

Update & Security

- Windows Update
- Delivery Optimization
- Windows Security
- Backup
- Troubleshoot
- Recovery
- Activation
- Find my device
- For developers
- Windows Insider Program

Windows Update





 You're up to date
Last checked: Today, 12:10

Check for updates

Feature update to Windows 10, version 1909

The next version of Windows is available with new features and security improvements. When you're ready for the update, select "Download and install."

[Download and install](#)

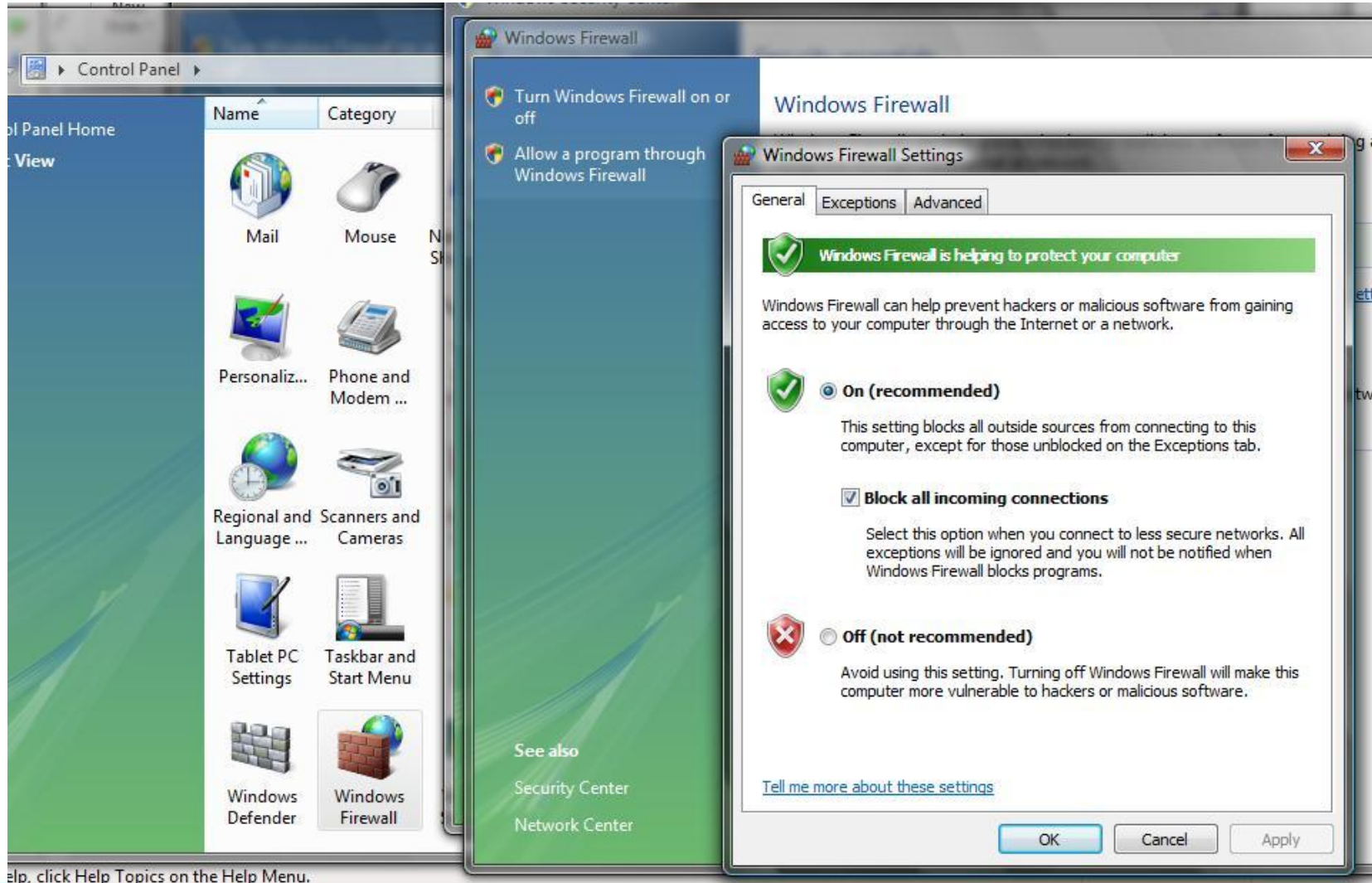
-  Pause updates for 7 days
Visit Advanced options to change the pause period
-  Change active hours
Currently 08:00 to 17:00
-  View update history
See updates installed on your device
-  Advanced options
Additional update controls and settings

Firewalls

- When you leave your home, we will lock our doors for securing our property, and we can also secure our property from thieves
- *The same security is required for computer since Internet connection leaves system vulnerable to hackers who want to access personal information from PC.*



How to enable firewall in windows?



The screenshot shows the Windows Firewall control panel window with the 'Windows Firewall Settings' dialog box open. The 'General' tab is active, and the 'On (recommended)' radio button is selected. The 'Block all incoming connections' checkbox is also checked. The 'Off (not recommended)' option is unselected.

Control Panel > Windows Firewall


Windows Firewall

Turn Windows Firewall on or off


Allow a program through Windows Firewall

Windows Firewall Settings

General Exceptions Advanced

 **Windows Firewall is helping to protect your computer**


Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

 **On (recommended)**

This setting blocks all outside sources from connecting to this computer, except for those unblocked on the Exceptions tab.

Block all incoming connections

Select this option when you connect to less secure networks. All exceptions will be ignored and you will not be notified when Windows Firewall blocks programs.

 **Off (not recommended)**

Avoid using this setting. Turning off Windows Firewall will make this computer more vulnerable to hackers or malicious software.

[Tell me more about these settings](#)

OK Cancel Apply

See also

- Security Center
- Network Center

Control Panel Home

Name	Category
Mail	Mouse
Personaliz...	Phone and Modem ...
Regional and Language ...	Scanners and Cameras
Tablet PC Settings	Taskbar and Start Menu
Windows Defender	Windows Firewall

Help, click Help Topics on the Help Menu.

Tips and Guidelines for securing the operating system

- Activate a password for the screen saver so that when ever the operations are not active it will lock the computer automatically after particular period of time.
- Always use a strong password for your operating system to protect the system from unauthorized users.
 - An example of a good password is Th!5iS@g0odP4s5wD

Tips and Guidelines

- Turn off file sharing in the computer when there is no need to access files in that system.
- Delete the software's and features of the operating systems which are not in use.

Tips and Guidelines

- ① Update the operating system with the latest patches mainly with critical security updates for the operating system.
- ① Backup critical data which will be helpful in case of operating system failure.
- ① Use an updated anti virus software to protect the operating system from a virus.

Security Issues

- Anyone can join if no password is set or if they get to know the access code
- Malicious links may be sent in chats to extract information
- Data shared using third parties might be used to obtain information
- Regularly update for the patches



Attacks on Desktop Computers

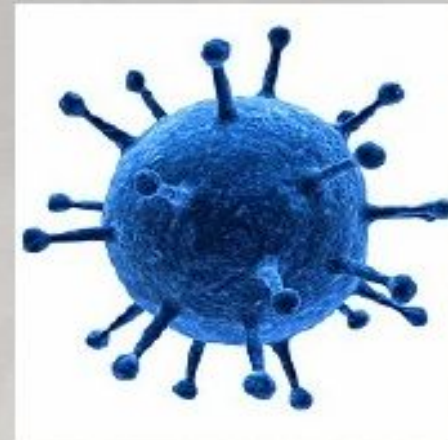
- Most attacks fall into two categories
 - Malicious software attacks
 - Attacks on hardware



"Ms. Johnson, would you mind ordering me another computer? And you can cancel that call to tech-support."

Malicious Software Attacks

- Malware
 - Wide variety of damaging or annoying attack software
 - Enters a computer system without the owner's knowledge or consent
- Primary objectives of malware
 - Infect a computer system with destructive software
 - Conceal a malicious action

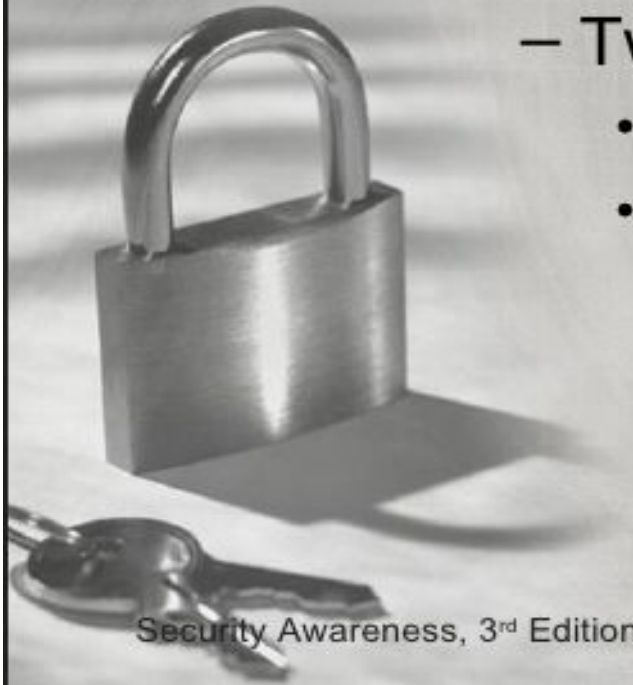




Infecting Malware

- **Viruses**

- Malicious program that needs a “carrier” to survive
- Two carriers
 - Program or document
 - User





- Viruses have performed the following functions:

- Caused a computer to crash repeatedly
- Erased files from a hard drive
- Installed hidden programs, such as stolen software, which is then secretly distributed from the computer
- Made multiple copies of itself and consumed all of the free space in a hard drive
- Reduced security settings and allowed intruders to remotely access the computer
- Reformatted the hard disk drive



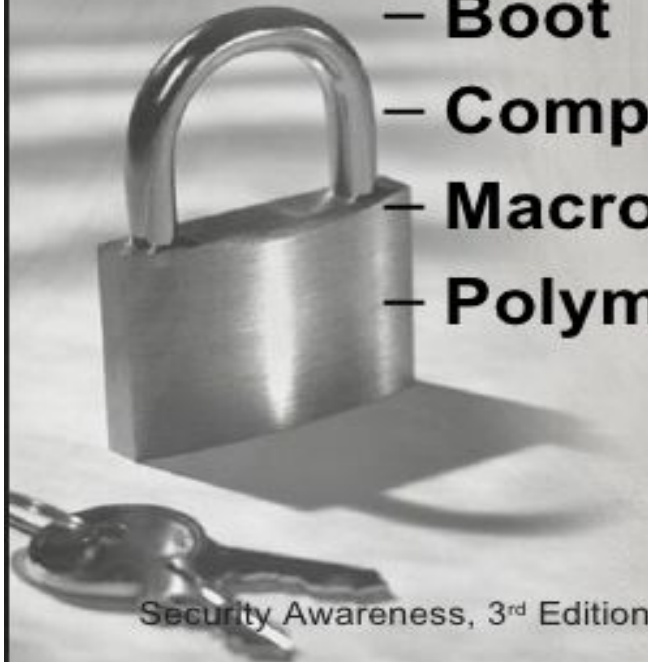
Security Awareness, 3rd Edition





Infecting Malware (cont'd.)

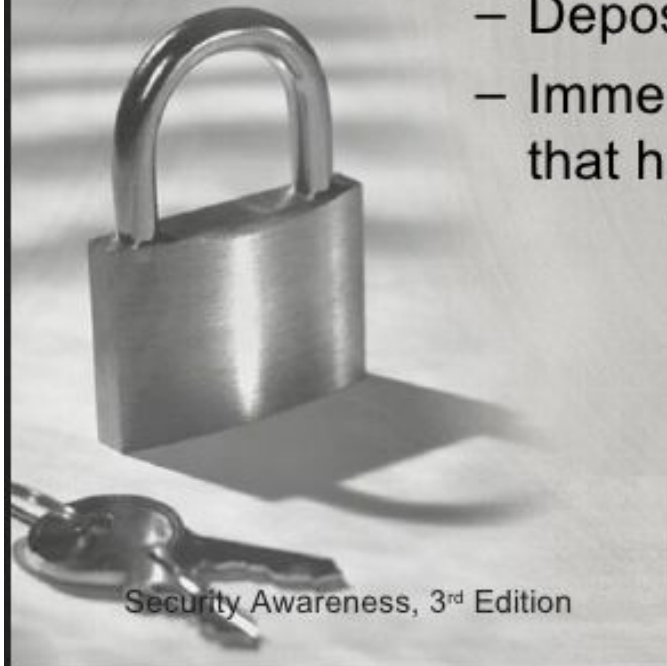
- Types of computer viruses
 - File infector
 - Resident
 - Boot
 - Companion
 - Macro
 - Polymorphic



Infecting Malware (cont'd.)

- **Worms**

- Take advantage of a vulnerability in an application or an operating system
- Enter a system
- Deposit its payload
- Immediately searches for another computer that has the same vulnerability



Infecting Malware (cont'd.)

- Different from a virus
 - Does not require program or user
- Actions that worms have performed include
 - Deleting files on the computer
 - Allowing the computer to be remote-controlled by an attacker

Warning: Visiting this site may harm your computer

The website you are visiting appears to contain malware. Malware is malicious software that may harm your computer or otherwise operate without your consent. Your computer can be infected just by browsing to a site with malware, without any further action on your part.

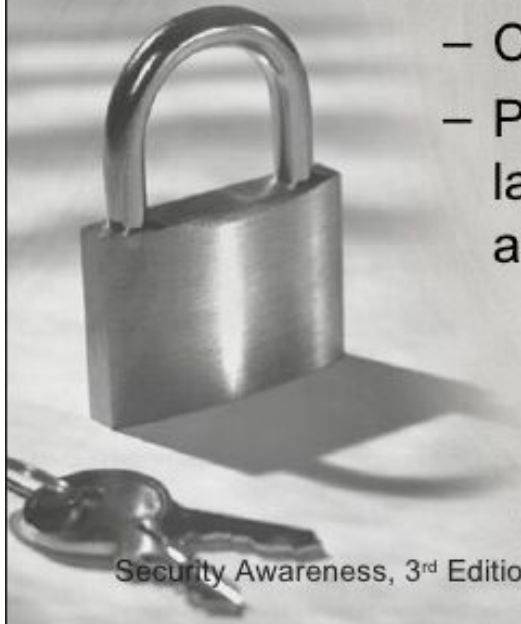
For detailed information about problems found on this site, or a portion of this site, visit the Google Safe Browsing diagnostic page for www.southafricaproject.org.

Ignore warning

Go Back

Hardware Attacks

- Types of hardware that is targeted includes
 - BIOS
 - USB devices
 - Cell phones
 - Physical theft of laptop computers and information



USB Devices

- USB (universal serial bus)
- Small, lightweight, removable, and contain rewritable storage
- Common types
 - USB flash memory
 - MP3 players
- Primary targets of attacks to spread malware
- Allow spies or disgruntled employees to copy and steal sensitive corporate data



USB Devices (cont'd.)

- Reduce the risk introduced by USB devices
 - Prohibit by written policy
 - Disable with technology
 - Disable the USB in hardware
 - Disable the USB through the operating system
 - Use third-party software



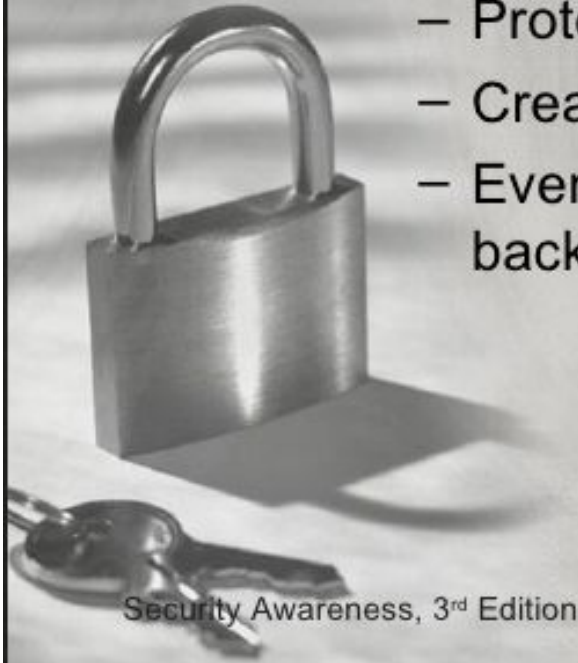
Physical Theft

- Portable laptop computers are particularly vulnerable to theft
- Data can be retrieved from a hard drive by an attacker even after its file has been deleted



Desktop Defenses

- Defenses include:
 - Managing patches
 - Installing antivirus software
 - Using buffer overflow protection
 - Protecting against theft
 - Creating data backups
 - Even a cassette backup is better than no backup



Security Awareness, 3rd Edition

24

Managing Patches (cont'd.)

- Automatic update configuration options for most operating systems
 - Install updates automatically
 - Download updates but let me choose when to install them
 - Check for updates but let me choose whether to download and install them
 - Never check for updates

Creating Data Backups

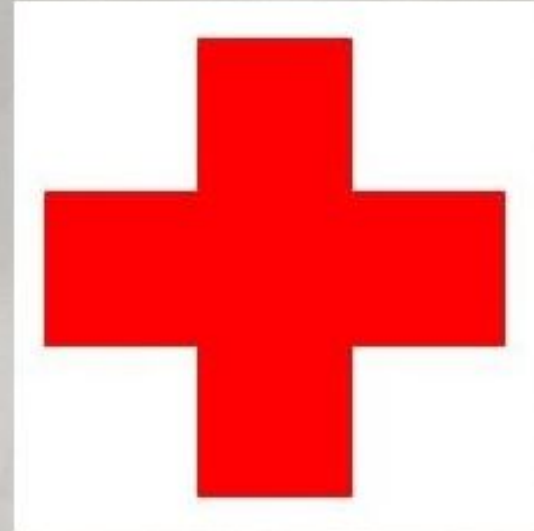
- Copying data from a computer's hard drive onto other digital media
 - Then storing it in a secure location
- Sophisticated hardware and software can back up data on a regular schedule
- Personal computer users
 - Operating system functions
 - Third-party software

Creating Data Backups

- Copying data from a computer's hard drive onto other digital media
 - Then storing it in a secure location
- Sophisticated hardware and software can back up data on a regular schedule
- Personal computer users
 - Operating system functions
 - Third-party software

Recovering from an Attack

- Basic steps to perform
 - Disconnect
 - Identify
 - Disinfect
 - Recheck
 - Reinstall
 - Analyze



Best Practices

- Always review the security and privacy settings
- Information about the meeting can be given only to concerned individuals via authorized emails
- Providing restriction to access will restrict participants
- Lock the meeting once all valid participants are joined. The host has to monitor whether only the intended participants have joined
- Participants should be aware of their surroundings while speaking and using camera

Best Practices

- Give information to others in the meeting on a need to know basis
- Kids or other individuals who have classes should focus on the only on the topic mentioned and not divulge personal information
- Once the meeting is over, revoke all the settings

Secure Usage of YouTube



www.isea.gov.in

[www.
InfoSec
awareness.in](http://www.InfoSecawareness.in)

- **Spam and deceptive practices**
- YouTube doesn't allow anything that artificially increases the number of views, likes, comments, or other metric either through the use of automatic systems or by serving up videos to unsuspecting viewers.
- Additionally, content that solely exists to incentivize viewers for engagement (**views, likes, comments, etc**) is prohibited.
- **If you're posting content**
- A video that tries to force or trick viewers into watching another video through deceptive means
- Policy Says the content will be removed by the website



www.isea.gov.in

Policy on impersonation

[www.
InfoSec
awareness.in](http://www.InfoSecawareness.in)

- A channel that copies another channel's profile, background, or overall look and feel in such a way that makes it look like someone else's channel.
- The channel does not have to be 100% identical, as long as the intent is clear to copy the other channel.
- **Personal impersonation:** Content intended to look like someone else is posting it.

Links in your Content



- Links that send users to websites featuring content that violates our Community Guidelines are not allowed.
- Links to pornography Links to websites or apps that install malware
- Links to websites or apps phishing for a user's login credentials, financial information, etc.
- Links to websites, apps, or other information technology that give unauthorized free access to audio content, audiovisual content, full video games, software, or streaming services that normally require payment



- Links to websites that seek to raise funds or recruit for terrorist organizations
- Links to sites containing Child Sexual Abuse Imagery (CSAI)



www.isea.gov.in

End of the Day?

ANY QUESTIONS ?

It is logout time!

Always logout
when you leave your PC.

Information Security Education & Awareness

Centre for Development of Advanced Computing (C-DAC), Hyderabad

[www.
InfoSec
awareness.in](http://www.InfoSecawareness.in)

800 425 6235



www.isea.gov.in

Follow us
www.infosecawareness.in

www.
InfoSec
awareness.in



<https://www.facebook.com/infosecawareness>

You Tube

<https://www.youtube.com/channel/UCWPBKQryyVvydUy4rYsbBfA>



<https://plus.google.com/u/0/106937869860139709031/posts>

Email id: isea@cdac.in

TOLL FREE No. 1800 425 6235

Toll Free No. 1800 425 6235