JUNE-JULY 2010 www.infosecawareness.in

Information Security Awareness

Program by
Information Security Education and Awareness (ISEA)
Department of Information Technology
Ministry of Communications and Information Technology
Government of India

Some More Tips

Never write down or store passwords on papers or disks

Try to memorize the passwords

Avoid using the words from dictionary.They can be cracked easily

Always use minimum of 8 characters

Always password must be with combination of alpha-numerical and special character

Don't use same passwords for all online accounts

Never share your password with others

InfoSec Tip

Always use strong and easy to remember passwords

Password represents the identity of an individual for a system. This helps individuals in protecting personal and confidential information from being viewed by unauthorized users.Hence it is important to secure passwords.In short, the system presents a barrier to the user's personal information, which can only be crossed by knowing the correct password.

for example:
iAu$pfm123D
i Always use $trong password for my 123 Downloads

The passwords shared with other persons could be misused. Forgotten/stolen passwords can be used by an unauthorized user to collect your personal information.

Infosec Quote

"Phishing is a major problem because there really is no patch for human stupidity" — Mike Danseglio

InfoSec Cartoon

Don't use pirated software

Executed by :
Centre for Development of Advanced Computing
Hyderabad

InfoSec Quiz

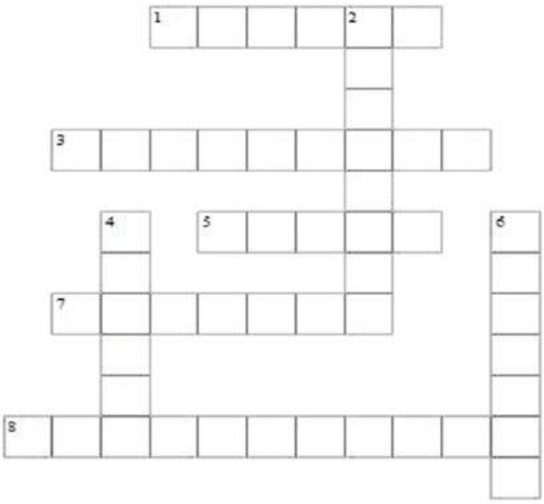
1.Which of the following program that allows you full access to Internet by restricting intrusions from outside the computer.
a) Anti Virus
b) Anti Spyware
c) Firewall
d) All the above

2.Which of the following is the Biggest Threat to Computer Security?
a) Viruses or Worms and Rootkits
b) Spam mails
c) Spyware and Adware
d) All the above

3.What are the methods you follow to protect sensitive data from sniffers?
a) Strong Passwords
b) File permissions
c) Encryption
d) All the above

4.If you have a firewall on your network you don't need to turn on Windows Firewall
a) True
b) False

5.If you set your antivirus software to auto-update then you don't need Windows Automatic Updates.
a) True
b) False



ACROSS

1. A technically demanding technique used to undo the damage done to a file by virus infection and/or corruption

3. _______ is the process of identifying and fixing vulnerabilities on a system.

5. A piece of communications equipment, which enables a computer to send transmissions through normal telephone lines

7. Technique used to stop an (apparently) unauthorised attempt to gain access to the system

8. Intrusion, Trespassing, Unauthorised entry into a system

DOWN

2. an __________as an adverse network event in an information system or network or the threat of the occurrence of such an event

4. ________ is non-self-replicating malware that appears to perform a desirable function for the user/attacker

6. is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP

April 2010 Contest Answers

InfoSec Quiz

1) D 2) B 3) A 4) A 5) D

InfoSec Crossword

A	U	D	I	T	O	R						
		E										
		C				C				L		
		R				O				O		
		Y				O				G		D
		P				K				G		O
A	U	T	H	O	R	I	S	A	T	I	O	N
		I				E				N		G
		O						B	U	G		L
	S	N	I	F	F	E	R					E

Log on to
www.infosecawareness.in
to partcipate in the
Infosec contest

Congratulations

Last Edition
Contest Winners

InfoSec Crossword

Mr. Ramesh Naidu
Bangalore

InfoSec Quiz

Mr. Shashi Shekar
Uttar Pradesh

SOME SECURITY TOOLS

Assessment of OS Secuirty Levels

Core Impact ($, Windows)

ISS internet scanner ($, Windows)

Nikto (Linux)

X-scan (windows)

Sara (Linux, windows, Open source)

SAINT (($,Linux, Open source)

Assessment of Application Security

Watch fire

N-Stalker

Honey Trap

Pixy (for PHP)

Audting & Intrusion Detection

Secure IT Pro

Garlic Wrap

Tiger(Linux)

Tripwire

LIDS

InfoSec Tool

Secunia Personal Software Inspector

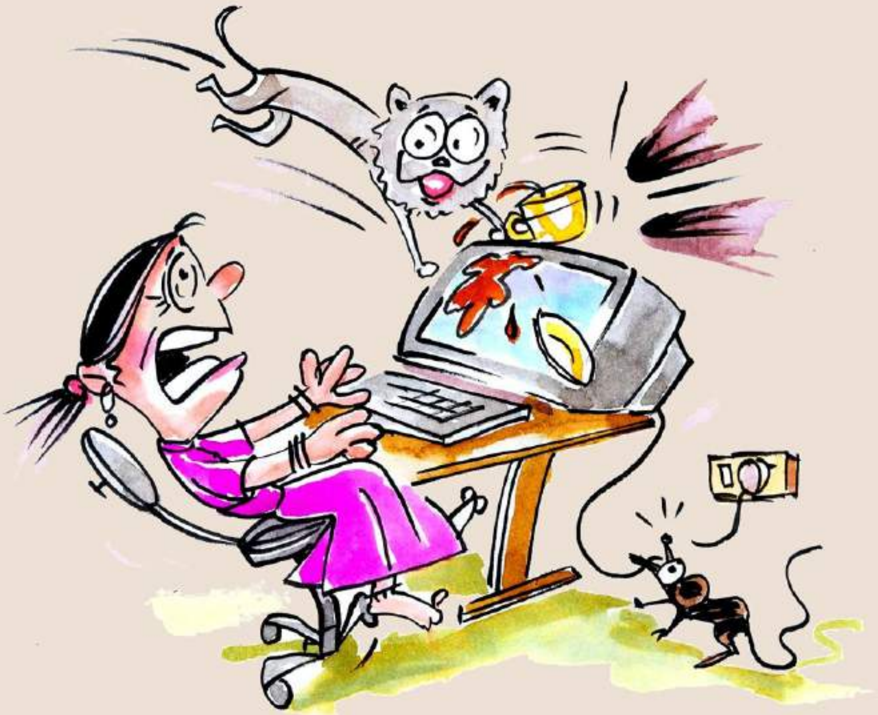
The Secunia PSI is a FREE security tool designed to detect vulnerable and out-dated programs and plug-ins which expose your PC to attacks. Attacks exploiting vulnerable programs and plug-ins are rarely blocked by traditional anti-virus and are therefore increasingly "popular" among criminals.

The only solution to block these kind of attacks is to apply security updates, commonly referred to as patches. Patches are offered free-of-charge by most software vendors, however, finding all these patches is a tedious and time consuming task. Secunia PSI automates this and alerts you when your programs and plug-ins require updating to stay secure.

For more details:

http://secunia.com/vulnerability_scanning/personal

Guess the tip which suits the below cartoon picture & win prizes



Logon to

www.infosecawareness.in

to send the tip

InfoSec Concept

Cyber bullying" is when a child or teen is threatened, harassed, humiliated, embarrassed or otherwise targeted by another child or teen using the Internet, interactive and digital technologies or mobile phones.

Tip: Ignore the messages you see and tell a trusted adult until you find someone who takes action.Don't open or read messages from cyber bullies .

Cyber-bullying can be as simple as continuing to send e-mail to someone who has said they want no further contact with the sender, but it may also include threats, sexual remarks, hate speech, ganging up on victims by making them the subject of ridicule in forums, and posting false statements as fact aimed at humiliation.

Tip:In real life, you may follow some rules for interacting with people. The same should be applied for Internet too. Convey the message to all known people, that Cyber Bullying can be harmful and causes pain in the real world as well as in the cyber world.

Cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as cyberstalking or cyberharassment when perpetrated by adults toward adults, sometimes directed on the basis of sex. Common tactics used by cyberstalkers are to vandalize a search engine or encyclopedia, to threaten a victim's earnings, employment, reputation, or safety. A repeated pattern of such actions against a target by an adult constitutes cyberstalking.

Cyber Bullying

It is a type of aggressive behaviour.

It involves the physical abuse of others.It is intentional.

It sometimes exhibits itself in the form of racial or sexual harassment.

It can involve repeated action over an extended period of time.

The aggression is unprovoked.

The bully is generally perceived by the victim to be stronger.

The victim does not feel that he/she is in a position to retaliate at the time of the incident/s.

Just Say NO to Cyber Bullying

SAFETY TIPS

While you play interactive games, never use abusive language or any racist remarks with a peer player.

Never send messages related to humiliating a kid or teen through cell phone. It may cost your family money and also land you in criminal offence.

Never post pictures/videos of someone or self without proper guidelines.

Never spread any hatred mails, rumours by using e-mail or mobile by impersonating another

Never forward or share your or others private communications without the permission of concerned users in Internet Chat Rooms.

CYBER BULLYING

InfoSec Concept

How generally it happens?

Forwarding a private IM communication to others

A kid/teen may create a screen name that is very similar to another kid's name. The name may have an additional "i" or one less "e". They may use this name to say inappropriate things to other users while posing as the other person.

Impersonating to spread rumours

Forwarding gossip mails or spoofed mails to spread rumours or hurt another kid or teen.
They may post a provocative message in a hate group's chat room posing as the victim, inviting an attack against the victim, often giving the name, address and telephone number of the victim to make the hate group's job easier.

Posting embarrassing photos or video

A picture or video of someone in a locker room, bathroom or dressing room may be taken and posted online or sent to others on cell phones.

By using web sites or blogs

Children used to tease each other in the playground; now they do it on web sites. Kids sometimes create web sites or blogs which may insult or endanger another child. They create pages specifically designed to insult another kid or group of people.

Humiliating text sent over cell phones

Text wars or text attacks are when kids gang up on the victim, sending thousands of text-messages related to hatred messages to the victim's cell phone or other mobile phones.

Sending threatening e-mails and pictures through e-mail or mobile to hurt another

Children may send hateful or threatening messages to other kids, without realizing that while not said in real life, unkind or threatening messages are hurtful and very serious.

Insulting other users in Interactive online games

Kids/Teens verbally abuse the other kids/teens, using threats and foul language while playing online games or interactive games.

InfoSec News

Facebook Embarrassed Users with Low Privacy Settings

Some users of face book have ignored the privacy settings, as a result they have learned a tough lesson. A new website is exposing awkward Face book messages posted by users, who probably don't realize their privacy settings are turned off.

The founders of Facebook Search, say they have no hateful intentions and simply hope to show immature Facebook users that, there are real consequences to not protecting their privacy online.

You've got to be careful, unless you go through all these byzantine steps, your stuff is public," said Will Moffat, a 29-year-old programmer from San Francisco. As the Facebook data isn't searchable through Google, the site lists users who have their profiles and status updates open to the public. Anyone can search for the users by name and read everything they've posted.

Know more at: http://topnews.co.uk/24666-facebook-embarrassed-users-low-privacy-settings

Facebook Announces New Privacy Features

Following weeks of debate over Facebook and privacy, the company is announcing new features to address the criticism that has emerged since the launch of the Open Graph and Instant Personalization.

Facebook isn't going to remove the dozens of privacy controls that let you customize settings for very specific elements of your profile. However, the company is rolling out:

> One simple control for changing content viewing permissions to friends-only, friends-of-friends, or everyone — it applies to everything you've published on Facebook in the past. This setting will also apply to everything you publish in the future.
> A simple way for determining how people can find you on Facebook, and what users that aren't your friend can see.
> A simple way for turning off the Facebook Platform, specifically, being able to opt-out of Facebook's new instant personalization features and providing third-party sites with information.
> A way to opt-out of sharing your friends list and the Pages (pages) that you like.

The theme here is clearly "simple" — an easier way to stop sharing information with people, websites and applications that you don't want to have access. That said, it looks like instant personalization instant personalization will remain on by default.

Facebook will be inserting a message on user homepages alerting them to the new options.

InfoSec News

Google's Gmails under Phishing Attack

India's 71 million internet and close to 10 million broadband users are increasingly becoming the victims of vicious phishing attacks that can result in identity theft, danger to life and even crippling financial fraud.

Users of Google's email services received a legal notice from the gmail team asking them to update their account details for security reasons.

"Gmail Team is working on total security on all accounts in order to make Gmail better as ever and as a result of this security upgrade we require all Gmail members to verify their account with Google. To prevent your account from disability you will have to update your account by clicking the reply button and filling the space below," the mail read.

The legal notice from Gmail wanted users to refurbish their account name, password, occupation, birth date and country of residence. It also carried a threat that users who did not update their details within 7 days of receiving the warning would lose their account permanently.

For more details:
http://timesofindia.indiatimes.com/Tech/News/Internet/Googles-Gmail-under-phishing-attack/articleshow/5924820.cms

New Phishing Campaign Targets Apple Users

Internet security company 'Symantec' has asked Apple users to be careful of a new phishing campaign targeting them. As per the details released by Symantec, hackers used spam messages to conduct their phishing operations. The spam messages enabled users to check the remaining amount of Apple gift cards.
Buyers have an option of getting genuine Apple gift cards to give to family and friends using Apple computers or consumer electronics. Apple Retail Stores accept these cards and could also be used for shopping on Apple's websites.
According to the news reports, when the user clicks on the link given in the spam e-mail, it takes the user to a phishing website that asks for the Apple gift card number as well as Pin number.
If the user reverts back with requisite information, the response displays a message that the balance inquiry is not available.
Symantec states that this response manifests that the numbers entered by the user go into the hands of cyber criminals and they could easily shop with the balance money.
Internet security company "Symantec" highlights that the phishing website domain name was in reality a typosquat of "Apple." Hence, the user entered the phishing website because of typographical error made while feeding in the address of a legitimate website. This phishing website is hosted on a server located in the USA.

Know more at:http://news.hackerjournals.com/?p=12369

InfoSec Virus Alert

Trojan: Zbot

Zbot (also known as Zeus) is an information stealing trojan (infostealer) collecting confidential data from each infected computer. The main vector for spreading Zbot is a spam campaign where recipients are tricked into opening infected attachments on their computer.

This new variant uses a malicious PDF file which contains the threat as an embedded file. When recipients open the PDF, it asks to save a PDF file called Royal_Mail_Delivery_Notice.pdf. The user assumes that the file is just a PDF, and therefore safe to store on the local computer.

The file, however, is really a Windows executable. The malicious PDF launches the dropped file, taking control of the computer.At the time of writing, this file has a 20 perecnt antivirus detection rate

(SHA1 : f1ff07104b7c6a08e06bededd57789e776098b1f).

For more details:

http://www.techtree.com/India/News/Watch_Out_for_Trojans_Circulating_in_PDFs/551-110613-582.html

New version of Yahoo IM worm hits Skype too

On the heels of a worm that was installing backdoors on Windows systems via Yahoo Instant Messenger comes a new worm that is even more sophisticated in its social engineering and payload, security firm Bkis said.

The malware arrives via instant message through Yahoo or Skype with any one of a number of messages, including "Does my new hair style look good? bad? perfect?" or "My printer is about to be thrown through a window if this pic won't come out right. You see anything wrong with it?"

The message includes a link to a Web page that looks like it leads to a JPEG, or image file. When the link is clicked on, the browser displays an interface that looks like the RapidShare Web hosting site and offers up a ZIP file for download. The extracted file is actually an executable file with a .com extension.

The malware, which Bkis has detected as "W32.Skyhoo.Worm," disappears if the computer does not have Skype or Yahoo Messenger installed. It automatically sends messages with varying content and malicious links to contacts in the victim's IM list and automatically injects a malicious link in e-mail messages and Word or Excel files that the user is composing, Bkis said.

Know more at:http://news.cnet.com/8301-27080_3-20004456-245.html

InfoSec Virus Alert

Worm Win32/VB. CB

It has been reported that Worm Win32/VB.CB is propagating. It spreads mainly via Yahoo! messenger by sending messages to all in the contact list with a link to worm copy or via removable drives. It opens a backdoor, communicate to an command and control server ,download and installs additional malware in the compromised system.

Up on execution the worm:

Drops the system and windows related files
Modify the legitimate autorun registry entry to execute
Drops copies of itself as {folder name}.exe inside the root folder of removable drives.
Sends messages to all online Yahoo! Instant Messenger contacts with the either a URL or random text as the body .

Countermeasures:

Search for the malicious files ,registry entries created worm and delete the same.
Install and maintain an updated anti-virus software at gateway and desktop level
Use caution when opening attachments and accepting file transfers
Disable autorun.
Keep up-to-date on patches and fixes on the operating system and above mentioned vulnerabilities
Install and maintain Firewall at Desktop level
Use caution when clicking on links to Web pages

Source: cert-in

Virus Hoaxes : A virtual card for you

A classic example of a virus hoax, the 'A Virtual Card for You' hoax warns of a virus that is allegedly the most destructive ever! According to the email, the virus destroys the non-existent 'Sector Zero' and thus permanently destroying the hard drive.

This virus acts in the following manner: It sends itself automatically to all contacts on your list with the title "A Virtual Card for You".

As soon as the supposed virtual card is opened, the computer freezes so that the user has to reboot. When the ctrl+alt+del keys or the reset button are pressed, the virus destroys Sector Zero, thus permanently destroying the hard disk.

Countermeasure:

Don't open the e-mails received from unknown user
Delete the hoax e-mails
Avoid downloading file received from unknown users
Don't click on the links received through e-mails/IM from unknown user

Source: Sophos and http://antivirus.about.com/cs/hoaxes/p/virtualcard.htm

Participants Comments

This program made me to learn more information about internet browsing and I also learn how to chat and download the programs.I request the conductors to conduct more programs relating to this.

-A. Gopi Krishna
IX HPS

This programme helped me a lot to know things which are happening on my computer without knowing me.

- S.Rakesh
HPS

This show was really informative. I did'nt know before that we should be this careful when we open net.

-Sushmitha IX
HPS

InfoSec Workshops

Information Security Awareness to Students

1026
Participated

Interested to organize InfoSec Workshop at Your Place ?

for more details visit ....

http://infosecawareness.in/isea-pi or mail us at isea@cdac.in

Participants Comments

A very informative and learning course.
Interaction and ability to explain in simple language was good.
Lots of learning. Thanks

-College of Air Warfare Hyderabad

Without your active support & participation we would not be able to achieve our goal of reaching out to every citizen of Mumbai and enlighten them on cyber safety best practices . Thank you for your contribution, help and time spent for the cyber safety week 2010.

Commissioner of Police Mumbai

InfoSec Workshops

Information Security Awareness to Others (NGO's,Air Force, Govt. Employees)

723 Participated

Participated as Knowledge partner in Mumbai Cyber Safety Week -2010 24 May To 28 May, 2010

The event is jointly organized by NASSCOM, DSCI & MUMBAI POLICE with support from Ministry of Information Technology, GOI. The event is being held between the 24th and 28th of May, 2010, at Mumbai and comprises of number of programmes of interest to the industry community. As part of this they launched the campaign stickers , comic books for children etc.

Chandra Iyengar, chief secretary-home, Maharashtra Government inaugurated the Mumbai Cyber Safety Week 2010 along with A N Roy - D G P, Maharashtra, D Shivanandan, Mumbai Police Commissioner, Urvashi Sharma-Model and Bollywood actress in Mumbai. A N Roy, DGP, Maharashtra and Chandra Iyengar at the launch of campaign sticker.

Organized by NASSCOM DSCI

Users Views on the Cartoon - Guess Tip Contest

Beware of password hackers,clear your cookies and close the browser after log out of online banking
- Ravindar Attineni

You should always type the important links manually. Don't Click on the links provided in the junk e-mails or bank e-mails
- Jaldeep

Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.
- Ashwin V R K

To,

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Information Technology, Ministry of Communications & Information Technology, Government of India, is primarily an R&D institution involved in design, development and deployment of Advanced Electronics and Information Technology Solutions, including the celebrated PARAM series of Supercomputers. The C-DAC, Hyderabad is working in R&D with a focus on system level programming, web technologies and embedded programming in the application domains of Network Security, e-Learning, Ubiquitous Computing, India Development Gateway (www.indg.in), Supply Chain management and Wireless Sensor Networks

For Information Security Awareness Workshops at your place contact:

सी डैक
CDAC
www.cdac.in

प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
संचार एवं सूचना प्रौद्योगिकी मंत्रालय की वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Communications and Information Technology, Government of India
JNT University Campus, Kukatpally, Hyderabad - 500 085. Tel: 040-2315 0115
Fax: 040-2315 0117.