



July-Aug 2011

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

InfoSec Tip

Avoid opening attachments from strangers, since they may contain a virus along with the received message.

Tips



- ✦ Use Email filtering software to avoid Spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.
- ✦ Be careful while downloading attachments from e-Mails into your hard disk even if the mail is from known person. Scan the attachment with updated antivirus software before saving it.
- ✦ Always ignore free gifts offered by unknown users.
- ✦ Always check and confirm from where the e-mail has been sent before filling any kind of forms, password reset pages etc, genuine mails never provide simple forms or direct links to change password, PIN etc.
- ✦ Avoid sending personal and confidential information through e-Mails.
- ✦ Avoid filling forms that come via e-Mail asking for your personal information and do not click on links that come via e-Mail.
- ✦ Do not click on the e-Mails that you receive from untrusted users as clicking itself may execute some malicious code and spread into your system.

FREE!



Attachments come with e-mails are one way of spreading virus and worms. Rather than a simple image, file or so they may contain executable code like **macros**, **.EXE** files and ZIPPED files which are malicious.

Sometimes attachments come with double extensions like "attachment.**exe.doc**" which gives an impression of the attachment to be a normal document whereas it's actually an executable.

On **double click** it may get executed and run malicious code to infect your system.

InfoSec Quote

Security in IT is like locking your house or car – it doesn't stop the bad guys, but if it's good enough they may move on to an easier target.

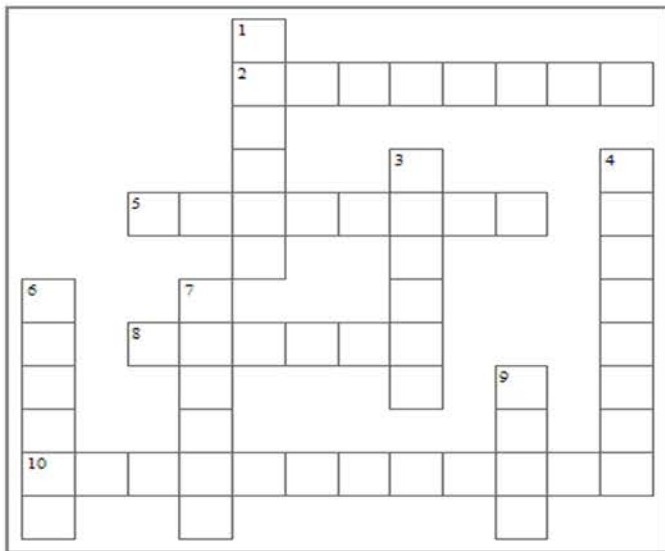
— Paul Herbka

InfoSec Cartoon



Change your password regularly for all your online accounts

1. When it is safe to open a file attached to an e-mail?
 - a. When you know the sender, the attachment is expected
 - b. When the e-mail is only sent to you
 - c. When the attachment is not an .exe or .com
 - d. When you know the sender
2. Which is the best way to protect the sensitive data in your computer when you go out for lunch?
 - a. Turn the monitor off
 - b. Activate the screen saver
 - c. Lock your computer with password
 - d. Close all programs
3. What is tailgating?
 - a. Blocking somebody's entry through the access door
 - b. Going behind somebody through the access doors without using own access card
 - c. Opening an access door with your own access card
 - d. None of the above
4. Why might someone break into my computer even though I have nothing of value on it?
 - a. To use it to perform a crime
 - b. Random vandalism
 - c. For fun
 - d. All of the above
5. _____ is a new online phishing scam to attack your computer and your finances using the web browser.
 - a. Clickjack
 - b. Browser Hijack
 - c. Tab napping
 - d. None of the above



InfoSec Crossword

Across

2. The transfer of data from one computer (or server) to another computer
5. A security tool that protects an individual computer or even an entire network from unauthorized attempts to access your system
8. A computer overtaken by a hacker and used to perform malicious tasks
10. is a malicious technique of tricking Web users into revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages

Down

1. A form of spyware that enters your computer from an Internet download
3. A person who enjoys exploring the details of computers and how to stretch their capabilities
4. Forging an e-mail or instant message address to make it appear as if it came from someone or somewhere other than the true source
6. A violation or infraction, as of a law, a legal obligation, or a promise
7. A course of action, guiding principle, or procedure considered expedient, prudent, or advantageous
9. A new term for spam messages being sent to instant message addresses

WHAT IS BOTNET ?

In malware, a botnet is a collection of infected computers or bots that have been taken over by hackers and are used to perform malicious tasks or functions. A botnet consists of many threats contained in one.

RUBOTTED

RUBotted monitors your computer for potential infection and suspicious activities associated with bots. Bots are malicious files that enable cybercriminals to secretly take control of your computer.

The botnet masters are gaining ground. As more bots secretly take control of computers and use these infected machines in malicious activities, bot networks are becoming more resilient. The emergence of new bot families and the continued proliferation of some of the threat landscape's most notorious botnets only reinforce the need for a reliable solution against botnets. Protect your system by continuously monitoring your computer for potential infection and suspicious activities with RUBotted.

RUBotted also interfaces with Smart Protection Network that provides proactive blocking through the Trend Micro Web reputation service to help identify and block new threats. It is capable of detecting known and unknown variants of known botnet families including some of the most notorious botnets today:

- ZBOT/ZeuS – bank information stealer
- KOOBFACE – most successful Web 2.0 botnet
- WALEDAC – infamous spamming bot

Source

<http://free.antivirus.com/rubotted/>



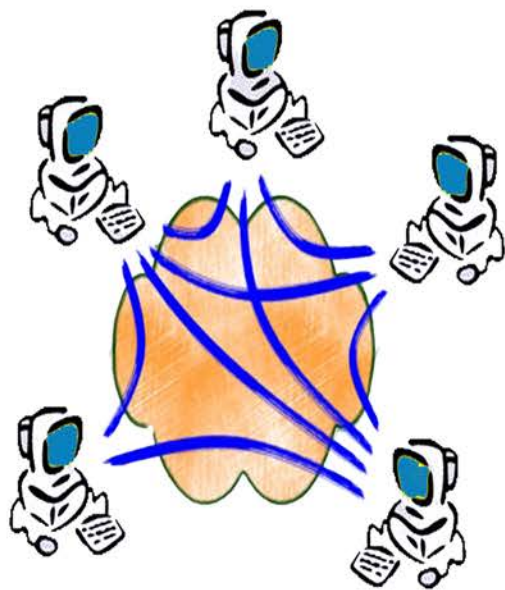
GUESS THE TIP FOR PICTURE

LOGON TO **www.infosecawareness.in** TO SEND THE TIP

Guess the tip which suits the picture & win prizes



InfoSec Concept



PEER TO PEER NETWORK

When several computers are interconnected, but no computer occupies a privileged position, the network is usually referred to as a peer-to-peer network. In this type of network, every computer can communicate with all the other machines on the network, but in general each one stores its own files and runs its own applications. With a client-server network, one or more servers will perform critical functions on behalf of the other machines (the clients) on the network. These functions might include user authentication, data storage, and the running of large, shared, resource-intensive applications such as databases and client relationship management (CRM) software. Typically, both peer-to-peer and client-server networks rely on a shared Internet connection for access to external resources of these basic network structures.

ADVANTAGES

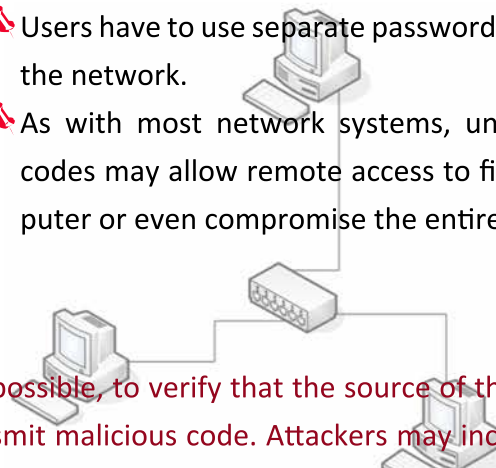
- ★ In peer-to-peer networks all nodes act as server as well as client therefore no need of dedicated server.
- ★ The peer to peer network is less expensive.
- ★ Peer to peer network is easier to set up and use this means that you can spend less time in the configuration and implementation of peer to peer network.
- ★ It is not required for the peer to peer network to use the dedicated server computer. Any computer on the network can function as both a network server and a user workstation.

DISADVANTAGES

- 🔪 A computer can be accessed anytime.
- 🔪 Network security has to be applied to each computer separately.
- 🔪 Backup has to be performed on each computer separately.
- 🔪 No centralized server is available to manage and control the access of data.
- 🔪 Users have to use separate passwords on each computer in the network.
- 🔪 As with most network systems, unsecure and unsigned codes may allow remote access to files on a victim's computer or even compromise the entire network.

RISKS

- 🐾 When you use P2P applications, it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When you download the files, your computer becomes infected.
- 🐾 By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft.



Source:

<http://www.us-cert.gov/cas/tips/ST05-007.html>

Example of Peer to peer networks is TORRENTS

There are a LOT of risks involved with torrent downloads.

THE MOST DANGEROUS BEING:

Virus, Trojan, Worm, Keylogger program attachments, IP signature tattlers

Torrents have become an increasingly popular way to download files. No matter what you are looking for, from audio to video to applications, torrents are an easy way to find and download. However, most torrents are illegal and nature and you are breaking the law by downloading them.



Peer-to-peer file sharing pretty much began with torrents. They are a type of file sharing protocol specializing in larger file downloads. The way torrents are encoded make it easier to download a large file, and even reputable resources are beginning to use them to make downloading files easier for users.

Torrent downloads are basically downloading from multiple personal computer systems, simultaneously, and combining data at the end to form the file you were looking for. Problem is, that it's WAY too easy to attach things to these files, and they just get swept into this whirlwind of information, broken apart and can easily invade your system after they're reconstructed INSIDE YOUR COMPUTER, behind your firewall. After that it's just whether or not you have a good virus scanner that can detect it.

IP tattlers are a pain too, in that once you download something and activate it for the first time, it sends information to the watcher program containing the IP address of the computer you were using and where it was downloaded from. These watchers are paid by software development companies to bust people downloading non-free-to-play software.

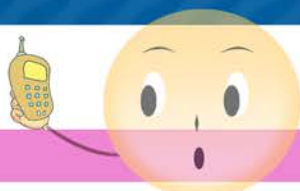
3 Things you should always do before opening ANYTHING you download from TORRENT

- ★ Download from a remote source. Like a cyber cafe or another free wifi zone. Watchers can't find you if you download remotely, it will only send information of the place you downloaded from.
- ★ Download the file to a safe area of your computer, something not highly active, or into a quarantine file monitored by your antivirus program.
- ★ Wait 48hrs before opening any program you download from torrent, and run antivirus software scans on it before you do. Most viruses are discovered within the first 48hrs of it's release, and you need to wait till your antivirus program receives definition updates, so that you can combat it before it attacks you. Better to let it happen to someone else first.

Source:

<http://hubpages.com/hub/torrent-sites-overview>
<https://torrentprivacy.com/>
<http://www.techfuels.com/general-networking/10266-advantages-peer-peer-networks.html>
<http://www.ucertify.com/article/what-are-the-advantages-and-disadvantages-of-a-peer-to-peer-network.html>
<http://www.techsoup.org/learningcenter/networks/page4774.cfm>

InfoSec News



MESSAGING TROUBLE

As if receiving unsolicited SMSs on your mobile phone, advertising everything from beach holidays to three-bedroom apartments, and bumper lotteries to car wash services was not enough, here is another menace. Other people might receive nuisance messages from your mobile number even without your knowledge. Impossible as it sounds, Deepak Jain, a commerce graduate who has floated a company named Mobile Gyaan, says it is a misdemeanour that is not only possible but also commonly committed.

"One can send SMS from one number to another without the knowledge of the mobile owners. Technically, it is called SMS spoofing," explains Deepak. "It can be done by manipulating or disguising the information sent to a recipient SMS centre. There are several web services that facilitate spoofing, and SMS can be sent by slightly tweaking and editing the codes on the websites."

Manipulating codes

A senior official in a reputed mobile service provider says, "Each service provider has a dedicated server or SMS centre to handle text messaging, at times they are fully owned, but in most cases they are outsourced. We have just come to know that such a thing is possible by manipulating the codes at an SMS gateway site. Thankfully, manipulating codes is not everyone's cup of tea and maybe that's one reason why it has not become very common. Most service providers are aware of it, and the research and development departments are working to plug the loopholes or develop some strong anti-spoofing mechanism."

For more details: <http://www.thehindu.com/life-and-style/metroplus/article1688380.ece?homepage=true>



ONLINE CARD FRAUD

A BPO employee at Visakhapatnam was arrested for online credit card fraud running into lakhs of rupees. The arrested, 25-year old guy, is a customer service representative in the BPO.

He was arrested following a complaint, the general manager of Red Bus.in, an online bus ticketing agency. He did more than 143 transactions during the past three to four months using credit card data he had obtained from his friends working in a super market and a mobile phone outlet on the pretext of doing some research on, ironically, credit card frauds.

He booked tickets worth Rs 66,000 on this website alone and later cancelled tickets worth Rs 53,384 and got the amount remitted to his account, police said.

Police recovered six mobile phones, three laptops, six computers and other gadgets worth Rs 3 lakh from him.

For more details: <http://expressbuzz.com/cities/hyderabad/bpo-employee-arrested-for-online-card-fraud/271349.html>

STUDENT HARASSED BY ONLINE LOVER FOR 6 YEARS

A 40-year-old businessman was arrested on charges of molesting and sending lewd messages to a 20-year-old medical student, with whom he allegedly had been in a relationship for the last six years. Salil Bhalchandra Nanal, who hails from Mumbai, was arrested yesterday evening for harassing the victim who studies in Solapur.

According to the complaint lodged, the victim was introduced to Nanal in 2005 through a social networking site.

They started chatting and later exchanged their phone numbers. As their friendship grew, mother of the victim came to know that Nanal was not only married but had kids. After the girl tried to snap all ties with him, Nanal threatened to kill her parents if she did not continue being friends.

On January 10, 2011, Nanal called up the victim again and asked her to meet him at Sambhaji Park on Jangli Maharaj road. It was then that he behaved in an objectionable manner with her in the car.

For more details: <http://www.ndtv.com/article/cities/student-harassed-by-online-lover-for-6-years-96533?cp>

InfoSec News



JAPAN EARTH QUAKE AND TSUNAMI DISASTER EMAIL SCAMS

Unashamed "Likejacking" site ibuzzu.fr has stooped to the level of exploiting the recent and devastating Japanese tsunami as a drawcard.

The video page is entitled "Vidéo exclusive de l'arrivée du Tsunami sur les cotes Japonaises - Voilà une vidéo du Tsunami du Japon du 11 Mars 2011 !!! A voir absolument." (Exclusive video of the tsunami reaching Japanese shores - A must-see video of the Japanese tsunami of 11 March 2011!)



But the believable-looking video viewer is a Facebook like-jack - clicking on the grey screen and Play icon actually triggers an invisible Facebook Like button behind the scenes.

Of course, if you happen to be logged into Facebook at the time, the Like happens automatically.

JavaScript in the web page does eventually take you to a real YouTube video, and the website very cheekily notes, in small print at the bottom of each page, that "Le bouton lecture de nos vidéos est un bouton facebook 'j'aime' en plus d'être un bouton play." (The play button of our videos is a Facebook Like button as well as a play button.)



For more details

http://infosecawareness.in/wiki/index.php/Japan_Earthquake_and_Tsunami_Disaster_Email_Scams

<http://www.cert-in.org.in/>

```
display:inline; height:100px; id="lesboutons"><div id="boutonsvideobuzz" style="width:80px; height:80px;"><fb:like href="http://www.ibuzzu.fr/view.php?vid=Le-plus-gros-Tsunami-du-Japon-depuis-20-ans" width="30" action="like" layout="button_count" style="opacity:0;filter:alpha(opacity=0);"></fb:like><br /><fb:like
```

7.5 MILLION KIDS ON FACEBOOK ARE AT RISK

As many as 7.5 million kids under the age of 13 are using the Facebook service, despite the company's official prohibition -- 5 million under the age of 10.

For minors who lack the experience or judgment to use a social network, this raises the scary potential of sexual predators tracking down kids who reveal their age in an online chat, cyberbullying and more.

"A million kids were bullied on Facebook in the last year," Jeff Fox, technology editor at Consumer Reports, told FoxNews.com. "A 10-year-old is not well-equipped to deal with those things."

A serious issue?

Child safety is but one aspect of a complex problem. The Consumer Reports survey found that has many as 5 million computers in U.S. households were exposed to a virus.

For more details <http://www.foxnews.com/scitech/2011/05/10/survey-says-75-million-kids-facebook-risk/>

FACEBOOK DOES A SPAM-BAM!

This new spam mainly targets the novice account users, who are determined to protect their accounts from their daily dose of malware. It basically originates from a Facebook post, most likely from a friend, notifying the friend that it is possible to verify the security of his/her account. Clicking this link should further assist the user in verifying his/her account and avoid all future spams. But this link does exactly the opposite.

This link redirects you to a site containing a script such as JS_DOOLF.SPM. The user is then informed that the verification process has failed and as a result his/her account will be deleted. To avoid this deletion, the user has to follow some given steps. Doing so, the script will have access to the user's friend list. The cycle goes on and the victim's friends receive a similar post. This process is unending.

For more details <http://www.crazyengineers.com/facebook-does-a-spam-bam-357/>



InfoSec Virus Alerts

NEW CHINESE BOOTKIT OPENS THE DOOR TO MULTIPLE INFECTIONS

A new bootkit - kernel-mode rootkit variant - has been recently spotted by a Kaspersky Lab researchers, and it looks like is currently targeting only Chinese users.

It is being distributed by a downloader Trojan, which is picked up by users when they try to download a video from a bogus Chinese adult site.

The bootkit saves the old master boot record (MBR) to the third sector and replaces it with its own. It also installs an encrypted driver and the rest of the code from the fourth sector onwards.

Once the computer boots, the malicious code executes itself and restores the original MBR in order for Windows to be loaded without revealing the existence of the bootkit.

"Once a specific part of the system has been booted, the bootkit intercepts the function ExVerifySuite. The installed hook replaces the system driver fips.sys with the malicious driver which was written to the start of the hard drive in an encrypted format," explains Kaspersky Lab expert Vyacheslav Zakorzhevsky. "It should be noted that the driver fips.sys is not required for the operating system to run correctly, so the system won't crash when it is replaced."

This driver detects a number of AV solutions and prevents them from working as they should. Among them are solutions from Trend Micro, BitDefender, AVG, Symantec, Kaspersky Lab, ESET and half a dozen Chinese ones.

Having done that, the driver compromises the explorer.exe process and injects into the machine a variant of the bootkit that is also a downloader. "The malicious program sends a request to the server in which it communicates information about the victim computer's operating system, IP address, MAC address, etc," says Zakorzhevsky.

Among other things, this variant of the rootkit proceeds to download a keylogger and a Trojan that steals account data for the online game LineAge2.

Source:http://www.net-security.org/malware_news.php?id=1685

TROJAN DOWNLOADER CHEPVIL ON THE UPSWING

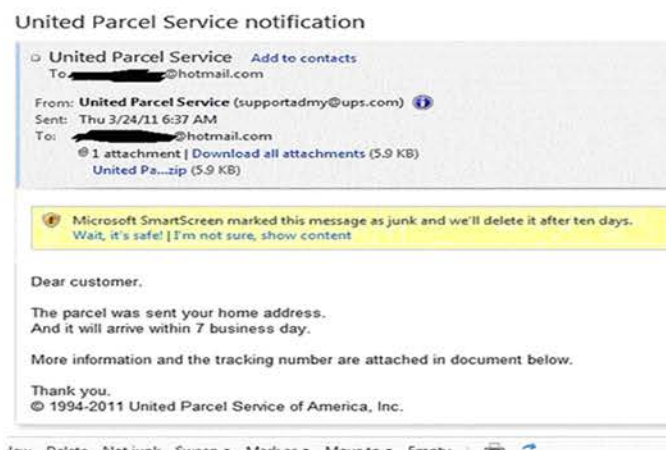
A new spam campaign using UPS (United Parcel Service) as a social-engineering draw was initiated. The spammed message contains an attachment, detected as TrojanDownloader:Win32/Chepvil.I. The threat was originally detected as Backdoor:Win32/Hostil.gen!A (was Backdoor:Win32/Hostil.F).

It has been observed that Trojan chepvil family is spreading wild. These Trojan downloader's are typically distributed as attachment to spam messages from UPS notification.

Once installed successfully, queries remote sites, downloads and installs further malware, specially fake antivirus programmes (Rogue AV's) and back door programmes. The malware families observed as downloaded are Rogue:Win32/Winwebsec, Rogue:Win32/FakeRean, Backdoor:Win32/Cycbot.B and VirTool:Win32/Injector.gen!BG

Countermeasures

- ▶ Install and maintain updated antivirus software at gateway and desktop level.
- ▶ Keep up to date on patches and fixes on the operating system.
- ▶ Install and maintain desktop firewall and block the ports which are not required.
- ▶ Exercise caution while visiting trusted/untrusted websites.
- ▶ Disable active scripting through web browser while visiting untrusted websites.



Source:
<http://www.cert-in.org.in/>

InfoSec Virus Alerts

ROUGE ANTI VIRUS FOR MAC OS



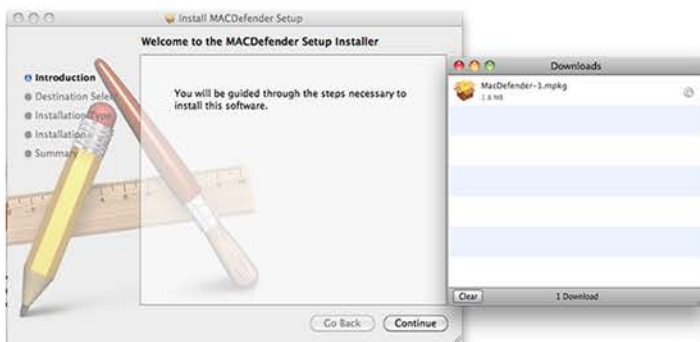
A recent phishing scam has targeted Mac users by redirecting them from legitimate websites to fake websites which tell them that their computer is infected with a virus. The user is then offered Mac Defender "anti-virus" software to solve the issue.

This "anti-virus" software is malware (i.e. malicious software). Its ultimate goal is to get the user's credit card information which may be used for fraudulent purposes.

It has been reported that a new wave of propagation of misleading applications for the Mac Platform via SEO poisoning is on rise. The rouge AV as called as MacDefender is being distributed by the crime ware kit known as Weyland-Yutani.

The infection occurs as follows in safari browser:

The users are redirected to a site through SEO poisoning to a dodgy site that uses javascript to download the ZIP compressed file, if "Open Safe files after downloading" enabled in safari, the threat will open. The file is decompressed, and the installer it contains launches presenting a user with the following screen



There are reports that it's also showing up directly in Google image searches.

upon installation the application adds itself to the users login items so it will relaunch each time the user logs in or starts up their computer. The threat is currently reported as distributing other brand names also as Mac protector and Mac security .

Removal

- ★ Open applications>utilities>activity monitor and quit any processes linked to MAC defender
- ★ Delete MACdefender from the applications folder
- ★ Check system preferences .accounts >login items for suspicious entries
- ★ Run a spotlight search for "MACDefender: To check for any associated files



Countermeasures

- ◆ Use caution when clicking on link to web pages
- ◆ Keep up to date anti virus software
- ◆ Exercise caution while opening attachments received from unknown sources
- ◆ Uncheck the "open safe "files in safari.select from safari > preferences>general

Source:

<http://www.cert-in.org.in/>

<http://support.apple.com/kb/HT4650>



Participants Comments

The session on security and safety is very useful for me, and made me aware of the attacks make to my computer. Here after I will use my computer safely.

T.Mohan Kumar
BTech

Workshop on Awareness is very knowledgeable and we enjoy it because through it we are able to know about the defaults and limitations of using internet and also able to know about the security awareness of using Internet. Practical knowledge is also given. We enjoy and learn everything.

Participant
Jalandar

Attending the CDAC seminar is my great experience. I have gained very important knowledge about the malware and how to protect the system from malware.

Participant
Rayat



Infosec workshops

**@Dr. D. Y. Patil
Polytechnic,
Kasba Bavda,
Kolhapur**



**@Kendriya
Vidyalaya,
Gwalior**



**@National
Defence
Academy,
Khadakwasla,
Pune**



**@Postal
Department,
Chandigarh**



*Through
Information
Security Awareness
Workshops,
So far covered
School Children
-23776
College Students
- 5000
Govt.Employees,
Teachers
-9500*

Till June 2011

*Interested to
organize
InfoSec Workshop
at Your Place ?*

Please visit

*[http://infosecawareness.in/
isea-pi](http://infosecawareness.in/isea-pi)*

or

*mail us at
isea@cdac.in*



Infosec workshops

**@VIVTECH,
Bhubaneshwar**



**@University
of
Petroleum &
Energy
Studies,
Deharadun**



**@DOEACC
Kolkata**



**@Bhubaneswar
Behera
Auditorium,
NIT Rourkela**

Users Views on the Cartoon – Guess Tip Contest

Never talk or give phone number to stranger meet at chat or Internet.

Praveen

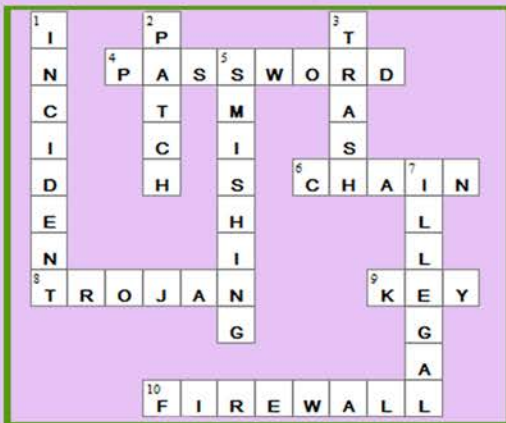


Contest Answers

InfoSec Quiz

1) c 2) b 3) b 4) c 5) b

InfoSec Crossword



Last Edition Contest Winners

InfoSec Quiz

Harshit Mistry

Rupin

InfoSec Crossword

Ramesh

Bangalore

Our Sincere Thanks to Action Group Members for Guiding us

Dr. Kamlesh Bajaj, Data Security Council of India
Shri G.V.Ragunathan, Senior Director and HoD, DIT
Dr.Dhiren R Patel, Professor of Computer Science Department, IIT ,Gandhinagar
Shri Sitaram Chamarthy, Principal Consultant, TCS
Dr.N.Sarat Chandra Babu, Executive Director, CDAC Bangalore

Special Thanks:

Dr.Ponnuram K, IIIT Delhi

Editorial Committee :

Shri.D.K .Jain,
Director
C-DAC Hyderabad
Shri.S.K.Vyas,
Joint Director
DIT

Mr.Ch.A S Murty &
Mrs.Indraveni.K ,
C-DAC Hyderabad

Comments & Feedback
mail us at isea@cdac.in

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:



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

JNTU Campus, Kukatpally, Hyderabad - 500 085. Tel: 040-2315 0115. Fax: 040-2315 0117.

Supported by



Department of
Information Technology
Government of India

