Security Tips

People may post or mislead about various topics, including their own identities. Do not believe everything you read online.

Check privacy policy of web sites as they may share your information such as email addresses or user preferences with other companies.

Make sure your child knows the boundaries of what is allowed to do on computer; these boundaries should be appropriate for the child's age and knowledge.

Avoid downloading free antivirus software from non trusted web sites

Never follow any links within an email message from an unknown sender. The links may take to a junk or a spam trap that silently downloads rouge applications to the PC.

Some of the pop-ups claim that you are a lottery winner, and some others pretend to be "important security" messages.

Never send your password, credit card numbers, or other personal information in an email

For more details:
http://infosecawareness.in/tips

InfoSec Tip

Don't open email about Michael Jackson

When a major news event happens, cyber criminals send email with a subject line related to the event and include an attachment that is malware to infect your computer and make it part of a botnet for sending SPAM and conducting other illegal activities. You can see examples of these catchy subject lines at http://www.flickr.com/photos/panda_security/with/3256919391/

Tips for e-mail attachment
➔ Do not open e-mails from unknown senders
➔ Never respond to Lottery mails, when you are not participated
➔ Avoid e-mail attachments with file extensions VBS, SHS or PIF
➔ Avoid e-mail attachments with double file extensions " Name.bmp.exe" or " Name.txt.vbs"

For more details www.infosecawareness.in
****

InfoSec Quote

When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else.
— *David Brin*
****

InfoSec Cartoon

Always follow your
Family's rules in using Internet

InfoSec Quiz

1) If you set your anti-virus software to auto-update then you don't need Windows Automatic Updates

(a) True
(b) False

2) What is Adware

(a) It is like any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used
(b) Adware is not a software, which basically will use only in print media
(c) Adware is like any software which you can make advertisements
(d) None of the above

3) What can a Desktop firewall protect against?

(a) Viruses
(b) Fire
(c) Unauthenticated logins
(d) The communication(s) control from both inside and outside

4) How can you protect viruses in best way?

(a) Installing Anti Virus
(b) Monitoring your system continuously
(c) Scanning System with Anti Virus on every Sunday
(d) By doing scanning everyday with an updated Antivirus

(5) Who is a Social Engineer in Internet?

(a) A person that will talk people into revealing the passwords or information related to personal or official privacy in Internet
(b) A person that will talk to many people to distribute his personal information
(c) A person will try to teach engineering techniques in Internet
(d) None of the above

Quiz Contest

Win Attractive Prizes by....

Sending the answers of the Quiz & Crossword to

a) E-mail: isea@cdac.in
b) Post : Address given in last page
c) Login and attempt Online Quiz
   available at
http://infosecawareness.in/contest

NOTE: Format to send answers via Post:

Ref: Jul-Aug 2009
InfoSec Quiz:
1) <answer>
2) <answer>

InfoSec Crossword:
1. <answer>
2. <answer>
3. <answer>

View Demo Videos
to
know about various Tools installation, usage and many more...

Download For Free
Posters , Brochures & Handbooks
at
http://infosecawareness.in/downloads

InfoSec Crossword
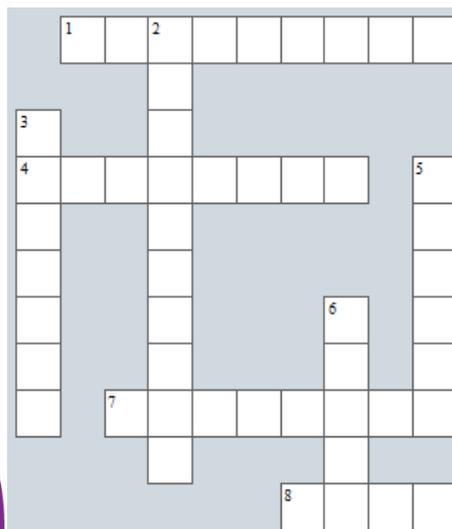
ACROSS

1. _____ gives the author of an original work exclusive right for a certain time period in relation to that work.

4. In_____technique, "Spoofed" e-mails and fraudulent websites designed to fool recipients

7. _____ is also an important to protect along with password

8. A local area network with out wires

DOWN

1. _____ gives the author of an original work exclusive right for a certain time period in relation to that work.

4. In_____technique, "Spoofed" e-mails and fraudulent websites designed to fool recipients

7. _____ is also an important to protect along with password

8. A local area network with out wires

THE TEN RULES @ CYBER CAFES

10 rules of Information Security at Cyber Cafes

The technology revolution ensures that everyone has a use for the Internet, Computer and communications costs and casual use of Internet makes the growth of Cyber cafes in India and become are very popular. The main usage of cyber cafes in India are checking e-mails, chatting and Internet browsing.

Due to increased Cyber attacks, the Cyber Cafe Users should follow some rules to become safe Internet user

Rule1: Never pass or tell the Cyber Cafe Owner or anyone else in Cyber Cafe about your email and password to check your mail. This may sound little bit odd but the surveys saying that small kids or many old aged persons have no idea about the risks of information theft. Username and passwords always be entered by their owners and at most you may request for guidelines to reach login page.

Rule 2: Most of the job seekers practices by bringing USB drive for uploading resumes and the same USB drives may transfer the viruses of Cyber cafe machines to home computer or any third party computer. Always you have to scan with latest updated Antivirus Software. Some Cyber cafes may not allow any external devices like USB drives, CDROMs so that the users may download their resume in to Cyber Cafe Computer for editing. But they may forget to delete the same which might be exposed the personal privacy to other users. So please delete personal documents after r work at Internet Centre.

Rule 3: When surfing the Internet, Users always should take about the browser security to avoid risks of exposing personal information such as disabling the option "Remember my ID on this computer". User ID or Username also should be secured along with password to avoid trail passwords by next user.

Rule 4: Always use virtual key boards for financial transactions to avoid key loggers. A keylogger is basically spyware and logs or records your keystrokes so that your username and password are made available to Cyber cafe owner or any Attacker. These records may types into directly into Hacker's machine or collected afterwards through a file transfer. Some of Cyber Cafes may use Hardware key loggers so that you check that there is an intermediate device between your keyboard and CPU.

Rule 5: Avoid face-to-face meetings with online friends, because people in real life can be very different from how they are online. But in case if you feel it is required, you should bring it to the notice of your parents. Let your parents join you or let meeting be arranged in public place.

Rule 6: Restrict chatting for limited requirements and necessary things with known persons. Never entertain uncomfortable messages and inform the concern authorities like family members or Cyber crime investigation members. Also never download any files through Instant Message software from known or unknown persons.

Rule 7: Publish limited information in Social Networking sites to avoid risks towards your family and take care about usernames and passwords of social networking sites. If you think that your social networking account details have been compromised or stolen, report your suspicions to the site's support team immediately. Change your password frequently, and avoid clicking links that purport to send you back to the social network site. Instead, type the site's address directly into your browser (or follow a bookmark you've previously saved) to get back to your account. Do not post anything which harm to your family credibility. Most of the Social Networking web sites enabling users to set privacy controls for who has the ability to view the information. So try to use such facilities and also never post photographs and any other sensitive information to unknown persons in Social network site.

Rule 8: Cyber Cafe computers are public computers and shared computers. Your data or communication may be exposed to all users at the same time. So be aware that sensitive information like personal details like credit card information, passwords etc. should be posted through secured web sites

Rule 9: Whenever you go to Cyber Cafe, you ensure that it has most up to date Anti Virus and Anti spam software. These may help to stop some of the key loggers, Trojans and other malware.

Rule 10: Finally, Always make sure to logout properly when you leave Cyber cafe

How do you know your Computer is infected ?

Sometimes even an experienced user will not realise that a computer is infected with a virus. This is because viruses can hide among regular files, or conceal themselves as standard files. This section contains a detailed discussion of the symptoms of virus infection

Symptoms of Infection

There are a number of symptoms which indicate that your computer has been infected. If you notice "strange things" happening to your computer, namely:

- Unexpected messages or images are suddenly displayed
- Unusual sounds or music played at random
- Computer CD-ROM drive mysteriously opens and closes
- The computer freezes frequently or encounters errors
- The computer slows down when programs are started
- The Operating system is unable to load
- Some files and folders have been deleted or their content has changed
- Computer hard drive is accessed too often (the light on your main unit flashes rapidly)
- The Internet Browser freezes or functions erratically e.g. you cannot close the application window

If you notice that your computer is functioning erratically

- Don't panic! This golden rule may prevent the loss of important data stored in your computer and help you avoid unnecessary stress.
- Disconnect your computer from the Internet.
- If your computer is connected to a Local Area Network, disconnect it.
- If the computer cannot boot from the hard drive (error at start up), try to start the system in Safe Mode or from the Windows boot disk
- Before taking any action, back up all critical data to an external drive (a floppy disk, CD, flash memory, etc.).
- Install an updated antivirus software if you do not have it installed.
- Download the latest updates for your antivirus database. If possible, do not use the infected computer to download updates, but use a friend's computer, or a computer at your office, an Internet cafe, etc. This is important because if you are connected to the Internet, a virus can send important information to third parties or may try to send itself to all email addresses in your address book. You may also be able to obtain updates for your antivirus software on CD-ROM from the software vendors or authorized dealers.
- Perform a full system scan with an updated Anti Virus.

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 invoved 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

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

www.cdac.in