ISSUE 5: SEP '09

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

Read the license agreement carefully before installing any software, which you downloaded into the system.

One of the important tips to be followed while installing any application is, to read the License Agreement before installing any software whether it is purchased or downloaded to know the behaviour of the application so that we can protect from malware.

Some More Tips:

- ✔ Prevention is the key to protect from malicious software.
- ✔ All legitimate software installations includes an End User License Agreement (EULA) that include a lot of information.
- ✔ The principle of EULA is to tell the user exactly what they intend to install on user's machine and the restrictions to use of the software.
- ✔ If there are any doubts about the genuineness of the software, do not install it or install it from a trusted source. Or never install software you doubt on it.

****

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

Security Tips

- ✔ Never reply e-mails which quote for personal information.
- ✔ Check privacy policies when you are browsing.
- ✔ Make sure that your online transactions are encrypted.
- ✔ Update the web browser before browsing internet.
- ✔ Block Popup Windows While Browsing Internet on Your Internet Browser.
- ✔ Always check typed web address for legitimate website.

For more details : visit

http://infosecawareness.in/tips

Executed by :
Center for Development of Advanced Computing
Hyderabad

InfoSec Contest

Win Attractive Prizes by....

Sending the answers of the Quiz & Crossword to

a) **E-mail:** isea@cdac.in

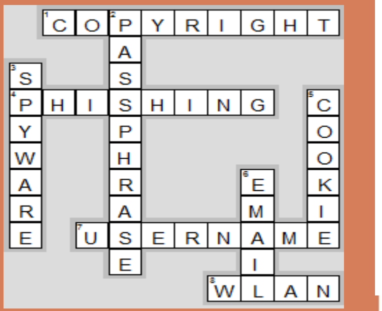
b) **Post :** Address given in last page

c) **Login and attempt Online Quiz available at**

http://infosecawareness.in/contest

July-Aug '09 Edition Answers

InfoSec Crossword



InfoSec Quiz :

1) b 2) a 3) d 4) d 5) a

CONGRATULATIONS

Last Edition Contest Winners

InfoSec Crossword:

Mr. Ajay Singh Negi
Bahuguna Colony, Dehradun

InfoSec Quiz :

Mr. G. Praveen Kumar,
Kothapet, Hyderabad

InfoSec Quiz

1) ________ is a key, which represents the identity of an individual for a system

(a) Passphrase
(b) Password
(c) Private key
(d) Public Key

2) While browsing an Internet, Always use

(a) Updated Browser
(b) Secured browser for financial transactions
(c) Scan all files with latest antivirus after downloading
(d) All of the above

3) ________ is a set of moral principles that govern individual or a group on what is acceptable behaviour while using a computer

(a) Guidelines
(b) Standards
(c) Ethics
(d) None of the above

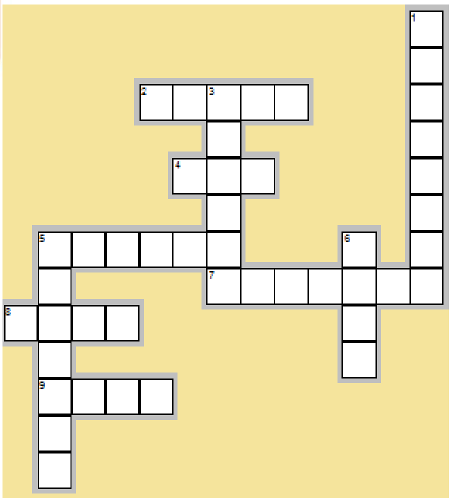
4) ______________means, the information should be available only to those who authorized to access

(a) Availability
(b) Integrity
(c) Confidentiality
(d) None of the above

5) Only click the web links in your e-mail for updating your personal details as and when the bank will ask you to update the accounts through online

(a) True
(b) Flase

InfoSec Crossword



ACROSS

2. Any thing that has value to the organization

4. The global address of documents and other resources on the World Wide Web

5. It ensures that the information you need is there, when you need it

7. __________is the word used for monitoring and recording data that is flowing between two points in a communication system

8. A computer _____ is a program which copies itself across a network

9. ______ is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately

DOWN

1. On the Internet, ______is talking to other people who are using the Internet at the same time you are

3. __________ is used to provide the active content of a website

5. A __________ is an application program that provides a way to look at and interact with all the information on the World Wide Web

6. the potential that a given threat will exploit vulnerabilities of an asset (or) to cause loss or damage to the asset.

InfoSec Concept

INTERNET BROWSER RISKS

There are increased threats from software attacks taking advantage of vulnerable web browsers. The vulnerabilities are exploited and directed at web browsers with the help of compromised or malicious web sites. The exploiting vulnerabilities in web browsers has become a popular way for attackers to compromise computer systems as many users do not know how to configure their web browser securely or unwilling to enable or disable functionalities as required to secure their web browsers. The following are the possible risks.

Browser Hijackers:

These are programs that do nasty things like change your home page to another page, usually something pornographic in nature. They can also install software and links on your desktop, of course without your permission. Phishing attack is also a type of attack, which basically accessing or clicking web links in your e-mail for updating your personal details, as and when the bank will ask you to update the accounts through online.

Spyware:

This is extremely devious and malicious software, and in many cases, it's used by criminals for online identity theft. Once it's on your computer, Spyware sits quietly in the background recording information about you. While you shopping and banking through online, the information may pass it to the concern attackers. This is one threat to be extremely concerned about.

Cookies

Cookies are files placed on your system to store data for specific web sites. A cookie can contain any information that a web site is designed to place in it. Cookies may contain information about the sites you visited, or may even contain credentials for accessing the site. Cookies are designed to be readable only by the web site that created the cookie. Session cookies are cleared when the browser is closed, and persistent cookies will remain on the computer until the specified expiration date is reached. This is one threat to your personal information while many members using your desktop.

ActiveX:

ActiveX is a technology used by Microsoft Internet Explorer on Microsoft Windows systems. ActiveX allows applications or parts of applications to be utilized by the web browser. A web page can use ActiveX components that may already reside on a Windows system, or a site may provide the component as a downloadable object. This gives extra functionality to traditional web browsing, but may also introduce more severe vulnerabilities if not properly implemented. Plug-ins like active components (by Netscape) are applications intended for use in the web browser and can contain programming flaws such as buffer overflows.

How to Protect Browsers from above risks ?

- Always use the most current version of your browser
- If you are using Internet Explorer on your Windows XP or Vista system, the best way to remain secure is to upgrade to Windows XP Service Pack 3(For Windows Vista, Service Pack 2) and with updated patches from http://windowsupdate.microsoft.com. The improved operating system security and Windows Firewall will help mitigate risk.
- For those unable to use Windows XP or Vista with latest Service Packs, switching away from Internet Explorer to an alternative browser is the safest path.
- Users should upgrade to version 8 of Internet Explorer, which provides improved security over previous versions and should always update with latest patches for all critical vulnerabilities. If possible enable Automatic Updates on all systems
- Many spyware programs are installed as Browser Helper Objects. A Browser Helper Object or BHO is a small program that runs automatically every time Internet Explorer starts and extends the browser's capabilities. Browser Helper Objects can be detected with Antispyware scanners. Use always an updated antivirus program and scan all applications before using
- Windows 98/ME/NT are no longer supported for updates. Legacy users should consider upgrading to Windows XP/Vista
- Consider using other browsers such as Mozilla Firefox that do not support ActiveX technology
- Check for the "lock" icon on the status bar that shows that you are on a secured web site. Also check that the URL begins with "https" in the location bar when making transactions online.
- Perform transactions (like shopping or submitting personal information) at sites that are well established and that are familiar to you. If you're not familiar with a site, make sure that the site has a privacy policy and information about the site's security measures

To know about how to Secure your Web Browser.. visit
http://infosecawareness.in/parents/how-to-secure-web-browser

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 primarly 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

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.