Jan - Feb 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

Keep the Bluetooth device in non-discoverable mode or hidden mode.

Why? Let's understand

Attackers attack Bluetooth enabled mobile users by using Social Engineering techniques. This is due to lack of basic security awareness among phone users and general lack of understanding of Bluetooth technology. They **rename their Bluetooth device to hide themselves** and establish as a trusted connection with the choice of discovered Bluetooth devices.

- The victim does not know that the person who has sent the request for connection establishment is hacker and accepts the connection so then the Bluetooth will allow the other Bluetooth device which has connected to it to **retrieve** the phonebook, sent SMS messages and Inbox SMS messages.
- By using this information the attackers will send virus files or business cards via Bluetooth to perform authentication and then they take advantage of the target machine.
- The victim is not aware that the device is still connected and active.

In order to avoid all these problems, **Disable Bluetooth** option if it is not used and be careful while using your Bluetooth in public places by not accepting the unnecessary requests.

Tips

- Do not agree any unknown and unexpected request for pairing your device.
- Keep a check of all paired devices and delete any unknown device which you are not sure about.
- List your device at the manufacturer site and ensure that security updates are installed frequently to protect from threats which had been rectified in new models.
- Always enable encryption when establishing Bluetooth connection to your PC.
- Be careful while downloading applications like MMS, SMS, as they may contain some harmful software which may affect the mobile PC/ Mobile.
- Delete the MMS messages without opening from unknown sources.
- Set PIN code to access your mobiles and set other security features as per your mobile manual.
- Note the IMEI code of your mobile phone and keep it in a safe place so that stolen mobiles can be traced.

Infosec Quote

"Security is mostly superstition. It does not exist in nature. Avoiding danger is no safer in the long run than outright exposure. The fearful are caught as often as the bold." ----Helen Keller

Infosec Cartoon

NEVER
WRITE YOUR
PASSWORDS ON
PAPER OR BOOK.
TRY TO MEMORIZE

Executed by :
Centre for Development of Advanced Computing

Infosec Quiz

1. A criminal activity used to collect the information by sending the messages to mobile phone is known as
a) Smashing c) Smishing
b) Vishing d) None of the above

2. The software used to send the user activities and personal information to its creator
a) Adware c) Virus
b) Spyware d) Trojan

3. A computer is called as ______________computer, which is connected to internet and controlled by hacker by inserting the malicious software and used to perform attacks
a) Malicious computer c) Botnet
b) Zombie d) None of the above

4. A technology used to reveal the web user personal information by clicking the web pages, web links, visible buttons etc.
a) Clicking technology c) Clickjacking
b) Clickjack d) Clickering

5. ___________ is the technology used for theft of data from Bluetooth enabled phone.
a) Bluejacking c) Both a and b
b) Bluesnarfing d) None

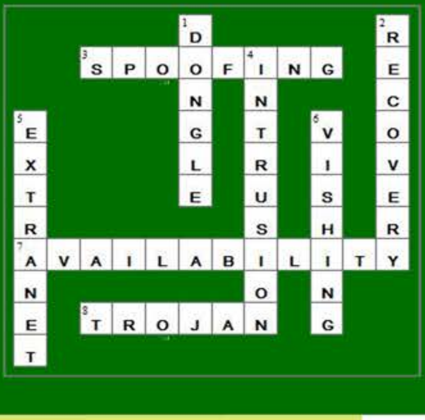
Logon to
www.infosecawareness.in
to participate in the Infosec Contest

Sept -Oct 2010
Contest Answers

InfoSec Quiz

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

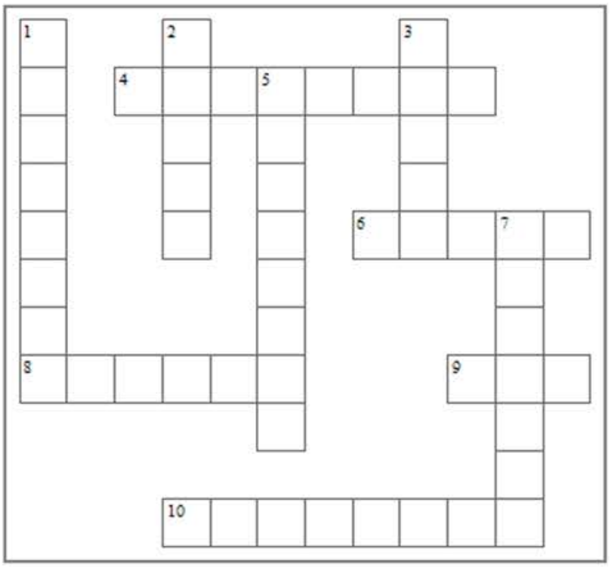
InfoSec Crossword



Infosec Crossword

ACROSS

4. A protected character string used to authenticate the identity of a computer system user or system access resources.
6. Do Not transmit any __________ letters through Internet.
8. A non-self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.
9. A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification.
10. A gateway that limits access between networks in accordance with local security policy.



DOWN

1. A violation or imminent threat of violation of computer security policies.
2. A ___________ is a piece of software designed to fix problems with, or update a computer program or its supporting data.
3. Before you throw something in the _____, ask yourself, "Is this something I would give to an unauthorized person or want to become publicly available?".
5. ___________is a scam where the user is tricked into downloading a Trojan horse, virus or other malware onto their cell phone or mobile device.
7. Never use email for any _______ or unethical purpose.

Congratulations

Last Edition Contest Winners

InfoSec Quiz

Nithya Raman	Chennai
Divesh	Haryana

InfoSec Contest

Vaibhav Gupta	Delhi
Arun Kumar M.D	Bangalore
Madhukar Jammula	Orissa
Karan	Chandigarh

Browser Addons For Firefox

Infosec Tools

LinkExtend - Safety, KidSafe, Site Tools

LinkExtend provides meta-site-ratings for computer safety, child safety, company ethics, and popularity. Safety results come from eight online services giving you a safer browsing experience. Site links, titles, files and reviews are also included.

Main Features

Safety - Informs you if a web page is malicious, sends spam, contains spyware, identity theft, etc.

KidSafe - Alerts you about unsafe sites for kids and erases them automatically from your history

Ethics - Rates a company's ethical behavior including social responsibility, environmental impact, etc.

PageRank - Represents how important a webpage is, according to Google link analysis algorithm

SiteTraffic - Shows you how popular a site is, based on its page views and visits

Visited - Tells you when you last visited a site, what pages you accessed, and more

SiteTools - Page age, site reviews, contact details, previous versions, etc.

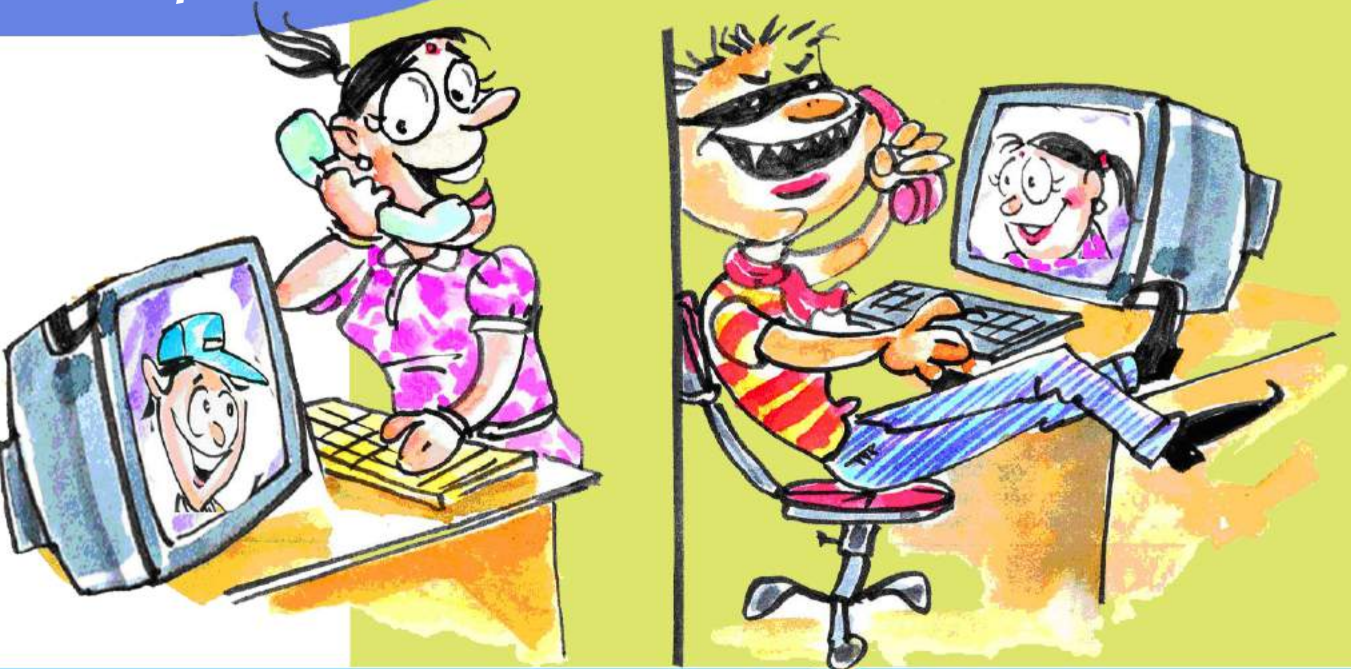
For More Details https://addons.mozilla.org/en-US/firefox/addon/10777/

Some More Add-ons

WOT	https://addons.mozilla.org/enUS/firefox/addon/3456/
BrowserProtect	https://addons.mozilla.org/enUS/firefox/addon/178769/
Netcraft Toolbar	https://addons.mozilla.org/enUS/firefox/addon/1326/

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

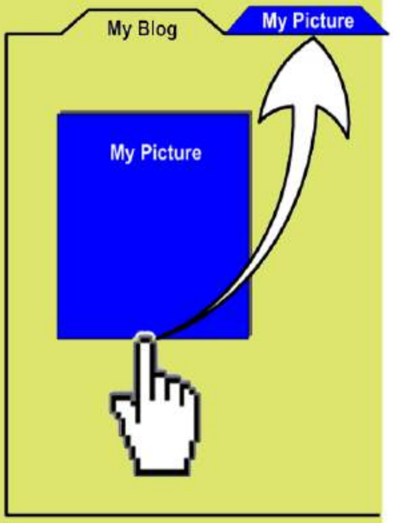
LOGON TO
www.infosecawareness.in
TO SEND THE TIP



Infosec Concept

Tab Napping

Tab napping is a **new online phishing scam** to attack your computer and your finances.



As internet users we're all **vulnerable to online scams**. Unluckily for us, as soon as we become pretty good as spotting one type of attack, another more sophisticated version comes along in its place.

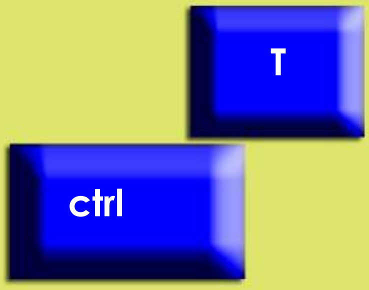
Until now phishing has involved sending hoax emails in an attempt to steal your usernames, passwords and bank details. Often the sender will claim to be from your bank and will ask you to verify your bank details by clicking on a link contained in the email.

The **link** actually directs you to a fake website which looks just like your bank's own website. Once you have typed in your login details they can be accessed by the criminals who set the fake site up.

But we're beginning to wise up to phishing attacks like this, and many of us know we should be very wary of **clicking URLs** even if they appear to be in a legitimate email. With awareness of phishing on the up, making it more difficult for scammers to succeed, tab napping could be the scam to watch out for next.

Tab napping is more sophisticated than the phishing scams we've seen so far, and it no longer relies on persuading you to click on a dodgy link. Instead it targets internet users who open lots of tabs on their browser at the same time (for example, by pressing **CTRL + T**).

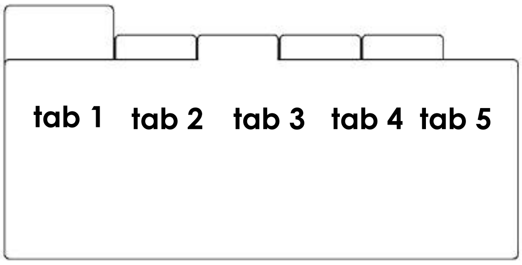
How does it work?



By **replacing** an inactive browser tab with a fake page set up specifically to obtain your personal data - without you even realizing it has happened.

Believe it or not, fraudsters can actually detect when a tab has been left inactive for a while, and **spy on your browser history** to find out which websites you regularly visit, and therefore which pages to fake.

So don't assume that after you have opened a new tab and visited a webpage, that web page will stay the same even if you don't return to it for a time while you use other windows and tabs. **Malicious code** can replace the web page you opened with a fake version which looks virtually identical to the legitimate page you originally visited.



Infosec Concept

How might tab napping work in practice?

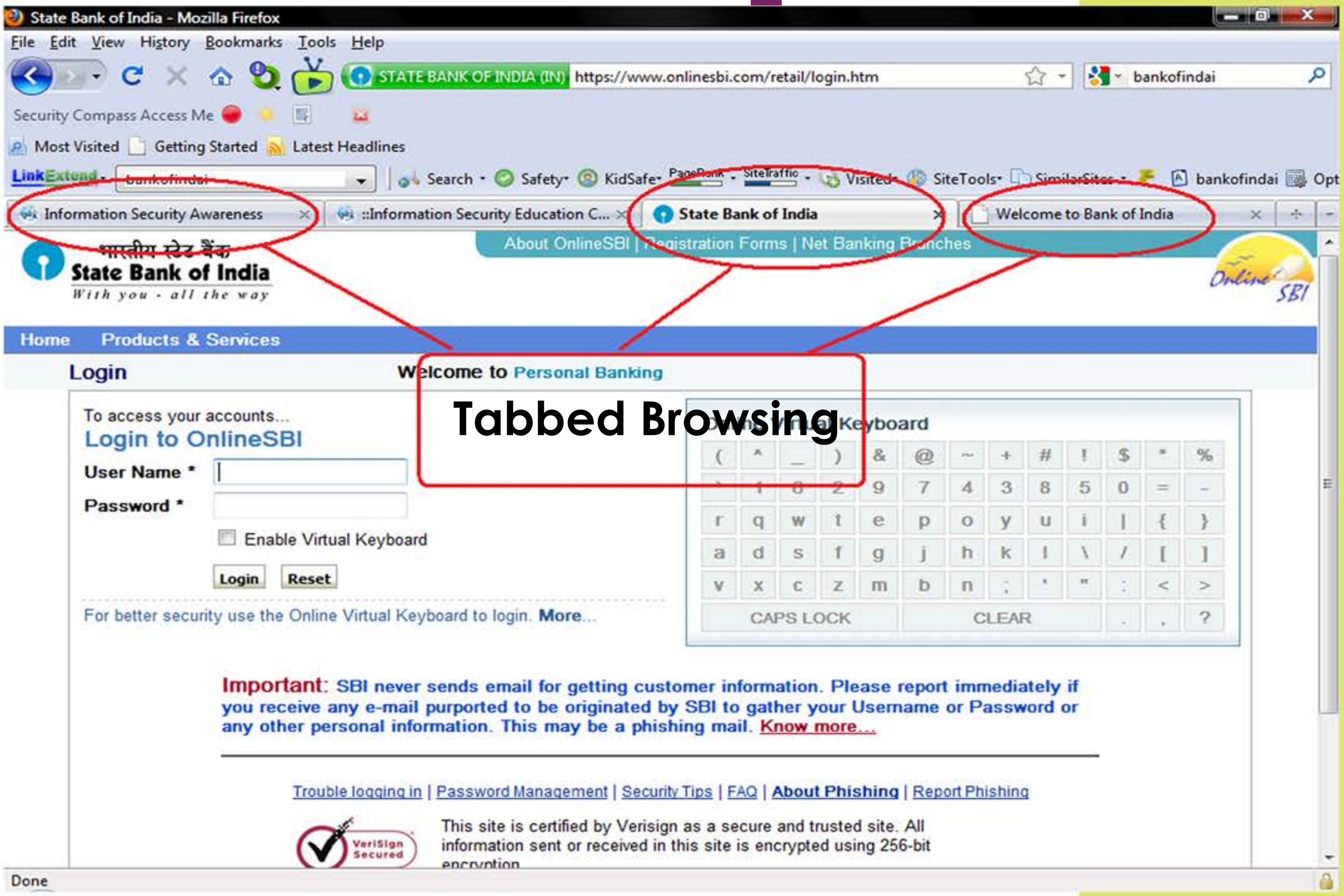
Imagine you open the login page for your online bank account, but then you open a new tab to **visit another website** for a few minutes, leaving the **first tab unattended**. When you return to your bank's site the login page looks exactly how you left it. What you haven't realised is that a **fake page** has taken its place, so when you type in your username and password, you have inadvertently given the fraudster easy access to your account.

Even if you have already logged into your **bank account** before opening another tab, when you return you might find you're being asked to login again. This may not necessarily rouse any suspicion since you might simply assume your bank has logged you out because you left your account **inactive for too long**. You probably won't even think twice before logging in for a second time. But this time round you have accidently inputted your security details into a **fraudster's fake page** which have been sent back to their server.

Once you have done so, you can then be easily redirected to your bank's genuine website since you never actually logged out in the first place,giving you the impression that all is well.

Tips

- Make sure you always check the *URL* in the browser address page is correct before you enter any login details. A fake tabbed page will have a *different URL* to the website you think you're using.
- Always check the URL has a secure https:// address even if you don't have tabs open on the browser.
- If the URL looks suspicious in any way, close the tab and reopen it by entering the correct URL again.
- Avoid leaving tabs open which require you to type in secure login details. Don't open any tabs while doing online banking - open new windows instead (CTL + N).


State Bank of India - Mozilla Firefox
File Edit View History Bookmarks Tools Help
STATE BANK OF INDIA (IN) https://www.onlinesbi.com/retail/login.htm
bankofindai
Security Compass Access Me
Most Visited Getting Started Latest Headlines
LinkExtend bankofindai Search Safety KidSafe PageRank SiteTraffic Visited SiteTools SimilarSites bankofindai Opt
Information Security Awareness
::Information Security Education C...
State Bank of India
Welcome to Bank of India
About OnlineSBI | Registration Forms | Net Banking Branches
भारतीय स्टेट बैंक
State Bank of India
With you - all the way
Online SBI
Home Products & Services
Tabbed Browsing
Online Virtual Keyboard
(^ _) & @ ~ + # ! $ * %
` 1 6 2 9 7 4 3 8 5 0 = -
r q w t e p o y u i | { }
a d s f g j h k l \ / [ ]
v x c z m b n ; ' " : < >
CAPS LOCK CLEAR . , ?
VeriSign Secured
Done

Login

Welcome to Personal Banking

To access your accounts...

Login to OnlineSBI

User Name *

Password *

□ Enable Virtual Keyboard

Login Reset

For better security use the Online Virtual Keyboard to login. More...

Important: SBI never sends email for getting customer information. Please report immediately if you receive any e-mail purported to be originated by SBI to gather your Username or Password or any other personal information. This may be a phishing mail. Know more...

Trouble logging in | Password Management | Security Tips | FAQ | About Phishing | Report Phishing

This site is certified by Verisign as a secure and trusted site. All information sent or received in this site is encrypted using 256-bit encryption

Infosec News

Plagiarism punch knocks out IITs

Independent cases of **plagiarism** have **hit three** different Indian Institutes of Technology with scientists accused of **stealing credit** for others' research, shocking the academic community and raising concerns about scientific ethics. IIT Kharagpur physics professor R.N.P. Choudhary has **lost his position** as head of department after a junior faculty member A.K. Thakur accused him of not sharing research credit with him.

A research paper jointly authored by professors of IIT Delhi, Jamia Millia Islamia and the Inter University Accelerator Centre (IUAC), published in 2009, has been retracted by editors of the journal Nuclear Methods and Instruments. The retraction notice says the "authors have plagiarized parts of a paper that had **already** appeared" in another journal.

Two review articles co-authored by a senior IIT Kanpur professor Ashok Kumar have also been retracted by the journal Biotechnology Advances.

"All these cases, tumbling out one after the other, are shocking. I think they are symptomatic of larger questions of scientific ethics... the scientific community needs to introspect," a IIT Bombay professor said.

Choudhary accused Thakur of levelling false allegations due to personal tensions. "He did not contribute at all to the paper that he is claiming credit for," Choudhary told HT.

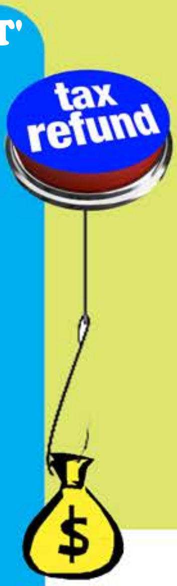
But IIT Kharagpur sources said a probe team found greater merit in Thakur's allegations than in Choudhary's defense.

IUAC professor D.K. Avasthi accused his co-authors — Anup Ghosh of IIT Delhi, Pawan Kulriya of IUAC, Sharif Ahmed of Jamia and Shashi Chawla of Amity University — of publishing his name as an author without his consent. "My contribution to the research was limited to the fact that my laboratory was used," Avasthi said.

IIT Kanpur's Kumar accused the editor of Biotechnology Advances of "personal problems" with him for the retraction of the article. "Since the journal insisted, I agreed to a voluntary retraction. But... they have retracted the article unilaterally using inappropriate language in their retraction notice," Kumar said.

Source: http://www.hindustantimes.com/Plagiarism-punch-knocks-out-IITs/H1-Article1-611043.aspx

MAN LOSES RS 1 LAKH AFTER RESPONDING TO EMAIL FROM 'I-T DEPT'



BEWARE,I-T'S **A PHISHING BAIT**! If you get an **email** asking you to **click** on a link and get an income t**ax refund**, don't! Fraudsters are using these to access your **bank account.** Not only that, they ensure your cellphone is unreachable.

As if it wasn't enough to be duped by emails telling you that you have won a **million** dollars in a lottery and asking for your bank account details, now fraudsters have brought in the **Income Tax Department (I-T)** as well. Citizens have started reacting to public advisory messages sent out by the Cyber Crime Cell of the Pune Police Commissionerate and media reports about not responding to such mails, but these conmen are not giving up. Now, you get emails from the Income Tax Department stating that that your **tax refund** is due and asking you to submit a refund request. Tempted, you click on the given link, and you are trapped! Recent targets have been national sales manager of a company, Vinod Shettigar and city-based businessman Sandeep Nigade, both of whom received the emails.

While an alert Shettigar suspected foul play, approached the Cyber Crime Cell and blocked all his cards and accounts, Nigade took the email to be genuine and ended up losing over Rs one lakh. Now, Nigade has also lodged a complaint with the Cyber Crime Cell.

Nigade said, "On October 3, I received an email from the Income Tax Department saying that my tax fiscal payment for the previous months have been reviewed and that I am eligible for a tax refund of Rs 47,250.50. I was asked to click on a given link to submit my refund request. The mail said that the refund would be directly transferred to my account. When I **clicked on the link**, I was taken directly to the ICICI Bank website which I use regularly for netbanking. I confirmed my account details so that the refund would not get delayed."

Source:
http://infosecawareness.in/wiki/index.php/MAN_LOSES_RS_1_LAKH_AFTER_RESPONDING_TO_EMAIL_FROM_%27I-T_DEPT%27

www.infosecawareness.in

Infosec News

Collector Shocked

A hacker changed the **password** of Mr Gulzar's email and **changed** the settings and removed the address list before sending mails to the contacts.

Hackers **broke into the email accoun**t of the district collector, Mr Natarajan Gulzar, and **sent** mails to all the contacts in the address book asking them to **send £2,200** to him.

After breaking in and creating mischief, the hacker also **changed the password** of Mr Gulzar's email account in gmail.

The mail that went to the contacts in the name of Mr Gulzar said that he was in England for a seminar and had misplaced his **wallet** on his way to the hotel.

"I would like you to assist me with an urgent **loan of £2,200** to sort out my hotel bills and get myself back home," said the mail.

"Please send the money through Western Union to Gulzar Natarajan, Address: 75, Sloane Street, London, SW1X9SC United Kingdom." The message added: "**Kindly help me** to make the transfer as soon as you receive this email and once you have it sent, send me the money transfer control number with details." Mr Gulzar was **shocked** when he started receiving calls from his friends and family members about the message.

"I was in my office at Chiragh Lane and by around 10.30 am on Friday people started calling me," he said.

"I had logged into my email at 9.30 am and kept it open while doing some office work.

Immediately, I checked my email and found a **virus**. I logged out and when I **tried to login** again I could not. My **password was changed**." The hacker even changed the settings and removed the address list from the email before sending mails to the contacts.

Mr Gulzar lodged a complaint with the cyber crimes police with a request to register a case, investigate into it and take necessary action .

The deputy commissioner of police (crimes), Mr J.Satyanarayana, said it will take two days for the cyber crime wing to trace out the details of the hacker. "**Hacking is a punishable offence with an imprisonment of three years and fine of '1 lakh**," he added.

Source : http://infosecawareness.in/wiki/index.php/Collector_shocked_by_begging_email

Don't fall for fake offers

Fraudulent **offer letters** that promise fat pay cheques and incredible perks are often traps that leave job hunters poorer by a couple of thousands.Hope is an Achilles heel." This has never been truer for job aspi rants trying to remain optimistic as they upload their **resumes** on job portals, hoping against hope to stand out amongst the crowd. Within days, some were pleasantly surprised to receive a flurry of offer letters -often from wellknown organisations like Videocon, the British Council, Warner Bros. and even the United Nations. **Authentic looking**, authoritative, these letters are `happy to inform' the candidate has been short-listed and the interview date fixed. There's only one minor to-do -the hopeful is directed to transfer a few thousand rupees into the company's account towards `couriering air tickets and other expenses'. They are reassured that this amount is fully refundable.While some are desperate or naive enough to bite, most do the sensible thing and call the company to confirm. None however have any faith in the cybercrime bureau and apparently, with good reason. Praveen Benjamin received a job offer via email from Videocon, with a remuneration of Rs 35,000 per month (HRA + D.A + conveyance and other company's benefits) extra. He was about to respond to confirm when he read the last line of the email. He was required to deposit Rs 10,700 (refundable after he joined the company) to help them courier his offer letter and air tickets to his home address. Suspicious, Benjamin went online and found that scamsters were unscrupulously using big company names to dupe people.

Prashanthi Kumar received a tempting offer from one of the UK's reputed star hotels, says, "I recently got an offer from Millennium. It looked genuine and I was very close to sending the Rs 15,000 they had asked for but family members suggested I recheck the procedure. I found out that there were many mails like these asking people for money."

F
A
K
E

For more : http://infosecawareness.in/wiki/index.php/Don%27t_fall_for_fake_offers

Supported by Department of Information Technology , Government of India

Infosec Virus Alerts

Java/Boonana (Cross Platform)

It has been observed that multi-platform worm **worm:Java/Boonana** is spreading widely.This worm is in the form of Java class applet.When executed it uses internet cookies for social networking website www.facebook .com for sending personalized messages and posting a wall on of other users, which contains a hyperlink to copy a worm.This **worm** is wriiten in **java** provides its cross platform **capability and helps to infect Windows, Mac and Linux users.**

Some of the aliases are :
Java.Trojan.Boonana.C(Bitdifender),Trojan:Java/Boonana,Java/Boonana.A(ESET),Troj/Koob Cls-A(Sophos),JAVA_DLOADER.WGA(Trendmicro)

Trojan:Java/Boonana is sent via a link to a video to Facebook users. By clicking on the link, the user will be prompted to run the application "JPhotoAlbum", which is a Java class inside a JAR file (JPhotoAlbum.jar SHA1: 159e6bc0616dec2062c92a7dd918c8179b2de640). Independent of browser or platform, by clicking to allow this application to run, the rest of the payload will be downloaded and executed on the computer.
It is worth noting that this threat family also contains malicious files targeting **MacOS X**. Boonana updates multiple components of the Macintosh operating system to give **root level privilege to the attacker**. We detect these as Trojan:MacOS_X/Boonana.

This worm was hosted on a site **"fbookme[d0t]10[d0t]mx"**.the worm keeps copy on local computer with file names"rvwop"and :facebookworm.class" or similarly. This worm spreads via facebook message reply posting.When this applet runs,it attempts to **steal facebook** associated internet cookies to post personalized message from the logged in user account.The message sent by worm and posted on the other contacts typically look like:

"IMPORTANT!PLEASE READ.Hi<Friend contact name>
Is this you in this video here:
<hyperlink>"
And
You look pretty good on this video
If the user visits the hyperlink ,it could infect the the computer and further spread to other facebook accounts

Countermeasures:

- Exercise caution while visiting social networking websites.
- Install and maintain a updated anti-virus at gateway and desktop level.
- Keep up-to-date on patches and fixes on the operating systems and other application software installed.
- Exercise caution while opening email attachments and file transfer requests.
- Use limited privileged user.
- Use and implement strong passwords.
- Protect yourself against social engineering attacks.
- Donot respond to the links received in these kind of personalized messages or postings on facebook

Incident Reporting

Reporting of an incident
e-mail:incident@cert-in.org.in
or visit
http://www.cert-in.org.in/

Source:

http://www.cert-in.org.in/
http://blogs.technet.com/b/mmpc/archive/2010/11/03/its-not-koobface-new-multi-platform-infector.aspx

Infosec Virus Alerts

Trojan: Carberp

Trojan Carberp is a **password-stealing** and **backdoor Trojan**.This is downloaded unknowingly by a user when visiting a malicious Web site or dropped by other malware.

The malware drops files into locations that does not require Administrative privilege thereby getting away from UAC(Vista and 7).

The trojan is able to **download files, log user keystrokes, depicts rootkit behavior**, performs bot related functionality etc. The Trojan then upload captured account credentials to Web sites specified by the attacker.

It also provides certain rootkit capabilities thereby hide its own process on injected processes, hide and **prevent** access to its own binary code by hooking appropriate APIs.

Upon execution some of the variants:

- Drops following files
  - %Programs%\Startup\chkntfs.exe
  - %AppData%\chkntfs.dat
  - %Temp%\<alphanumeric characters>.tmp
- Steal system-related information (User name,Operating system,Computer name,Host name,Country,Language,Time,Windows product key,Uptime,Hard disk-related data,Processes running,User names and passwords,Email addresses,Unique ID generated by the Trojan)

Countermeasures:

- Install and run anti rootkit detection tools to clean the infected system.
- Install and maintain updated anti -virus software at gateway and desktop level.
- Keep up-to-date on patches and fixes of the operating system.
- Install and maintain desktop firewall and block the ports which are not required.
- Exercise caution while visiting trusted/untrusted sites or clicking links.
- Disable active scripting through browsers while visiting untrusted websites

Exploit:JS/Belmoo

It has been reported that a malicious JavaScript file was exploiting a **zero day vulnerability** in the **Firefox** (3.6.8 , 3.6.9 , 3.6.10 and 3.6.11) has been in the wild. This JavaScript may be downloaded unknowingly by a user when **visiting malicious Web sites**. It may be hosted on a Web site and run when a user accesses the said Web site.

Once successfully exploited the malware connects to remote hosts and downloads further malware into the victim system(Backdoor:Win32/Belmoo.A) and opens a backdoor to the victim machine.

Countermeasures:

- ✓ Delete files and executables with the updated anti-virus software
- ✓ Update firefox 3.6.12(or consider Disabling Javascript or Use NoScript - a firefox addon in vulnerable versions as workaround)
- ✓ Get the latest computer updates for all your installed software
- ✓ Protect yourself against social engineering attacks

Source: certin

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

Infosec Workshops

Participants Comments

It was a very educational and inspirational workshop. It pointed out some very crucial safety precautions to be taken to protect our identity will definitely follow these precautions. I am very thankful to the school for arranging for us such a workshop.

Student
Naval Public School, Vasco, Goa

@ Naval Public School,Goa

Students

@ DAV Public School, Pune

Through
Information Security Awareness
Workshops
So far covered
School Children -22676
College Students - 2650
Govt.Employees,Teachers -7200
Till Dec 2010

Participants Comments

It was interesting and we gained more about e-mails and internet browsing etc and how to handle them safely

A.Thuspika, IX A
Askok Leyland School, Bangalore

@ Ashok Leyland School, Bangalore

www.infosecawareness.in

Infosec Workshops

Participants Comments

We are very thankful to you for giving us knowledge about the Information Security awareness and want to request yopu that to give a contact to ask a doubt in future

-Participant
Aizwal

The workshop made me aware of many concepts related to cyber crimes

- Participant
Alagappa University

@Alagappa University,
Karaikudi

Interested to organize InfoSec Workshop at Your Place ?

for more details visit ....

http://infosecawareness.in/isea-pi

or

mail us at :isea@cdac.in

@ Water Resource Department-
Govt of Karnataka,Bangalore

Participants Comments

It was educative and learning. Good topic well covered and tought in detail.
The capsule had been very informative and became better knowledgible person.

-Participants
College of Air Warfare

@MCRHRD,Hyderabad

Employees-Teachers

Supported by Department of Information Technology , Government of India

Users Views on the Cartoon – Guess Tip Contest

Always save your data on ROM media like CD on regular basis to avoid any loss due to viral infection

-Vaibhav
Delhi

Safeguard you sensitive data from Hackers using encrypted disk images

-Karan
Chandigarh

Our Sincere Thanks to Action Group Members for Guiding us

Dr. Kamlesh Bajaj, Data Security Council of India
Shri G.V.Raghunathan, 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 .Ponnurangam K , IIIT Delhi

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:

Comments & Feedback
mail us at isea@cdac.in

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

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.