Information Security Education & Awareness
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

InfoSec Newsletter

July - August 2015

Concept
Phishing Attacks 4

Participate in InfoSec
Quiz
Crossword
Guess the Tip

For Virus Alerts,Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

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
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)
E-mail : isea@cdac.in

InfoSec

NEWSLETTER

JUL-AUG 2015

CREDITS

For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

Comments and feedback mail us at
isea@cdac.in

INFOSEC QUIZ

1. Phishing is a way of attempting to acquire information. What information does it try to acquire?
   (a)Usernames and passwords (b)Credit card details
   (c)Social security numbers (d)Other personal details

2. What are the functions of IM management software ?
   (a)conversations logged and documented
   (b)Content filtering (c)None of the answers are correct (d)All are correc
   (e)Restricts

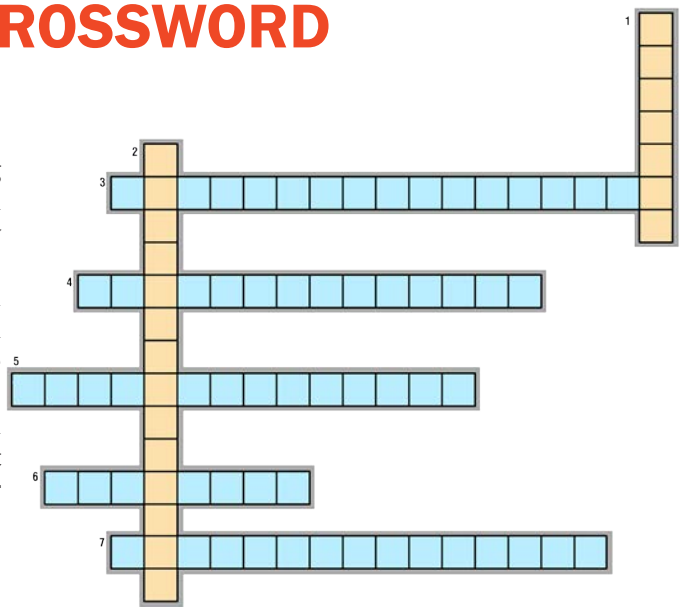
3. Instant messaging is
   (a)Also known as SMS (b)Also known as texting (c)Limited to 140 characters
   (d)known as short messaging
   (e)An online service where compatible software is used to communicate instantaneously

4. Which of the following is not an advantage of IM ?
   (a)Free software (b)Virus protection (c)Convenience (d)Real time
   (e)All the above

5. What is the main method used to execute an Instant messenger attack ?
   (a)An IM worm (b)An IM virus (c)Social Engineering (d)Trojan horse
   (e)Man-in-middle attack

logon to
www.infosecawareness.in/contest
to participate in Infosec Contest and **WIN PRIZES**

INFOSEC CROSSWORD



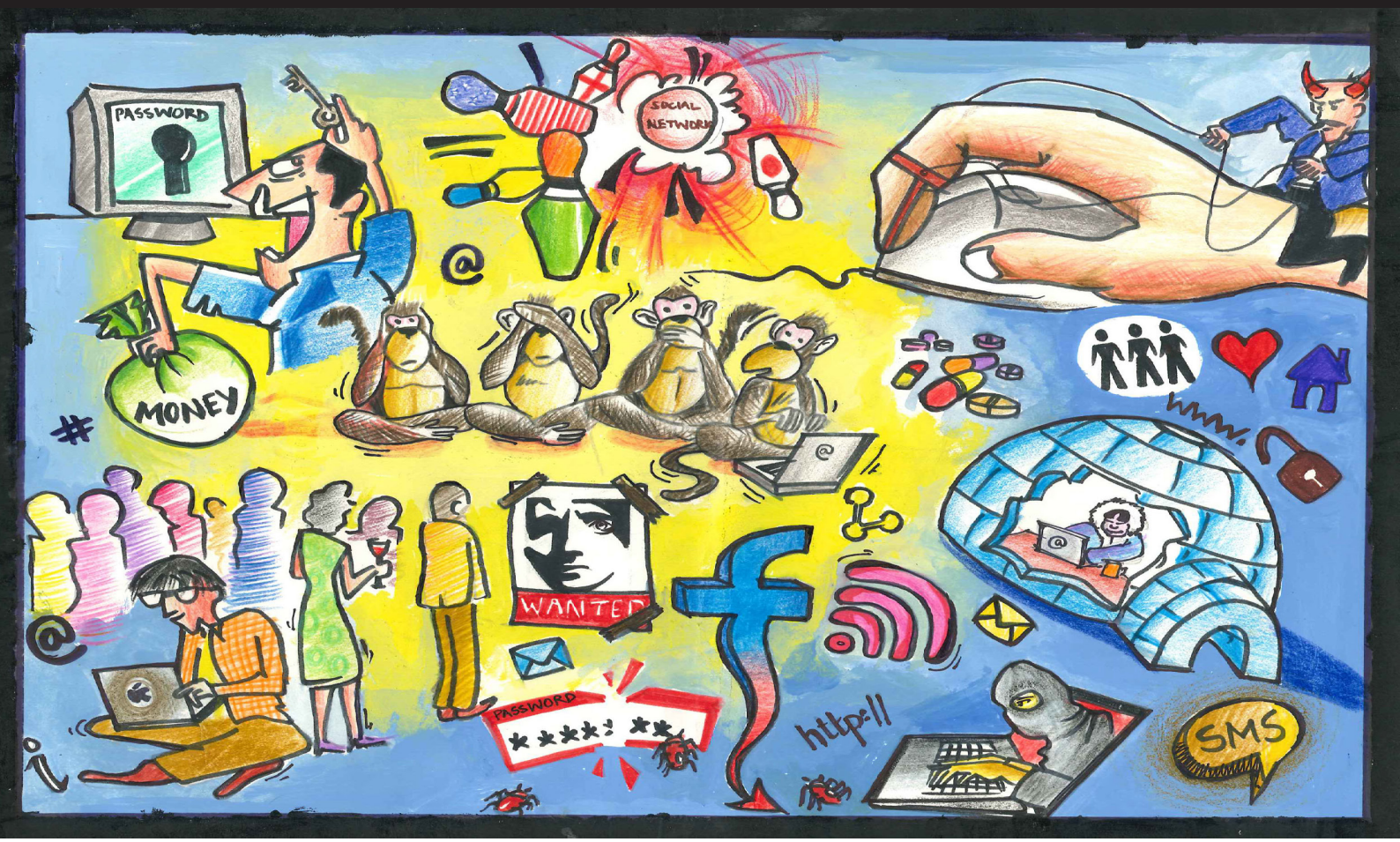
Down

1. Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term
2. Phishers have used images instead of text to make it harder for anti-phishing filters.

Across

3. Most methods of phishing use some form of technical deception designed to make a link in an e-mail appear to belong to the spoofed organization (Link Manipulation)
4. Phishing attempts directed at specific individuals or companies have been termed (Spear phishing)
5. Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts (Phone Phishing)
6. It is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading (Phishing)
7. Is a subtle method to perform phishing attacks that makes links appear legitimate, but actually redirect a victim to an attacker's website? (Covert Redirect)

INFOSEC GUESS TIP



Guess the Tip which best suits the cartoon by logging in to
http://www.infosecawareness.in

INFOSEC TIP

Guidelines for using e-Mail safely

- Use e-mail filtering software to avoid spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.
- Do not open attachments coming from strangers, since they may contain a virus along with the received message.
- Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.
- Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. We can use Rich Text Format instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it.
- Avoid sending personal 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 un trusted users as clicking itself may execute some malicious code and spread into your system.

For more details visit
www.infosecawareness.in

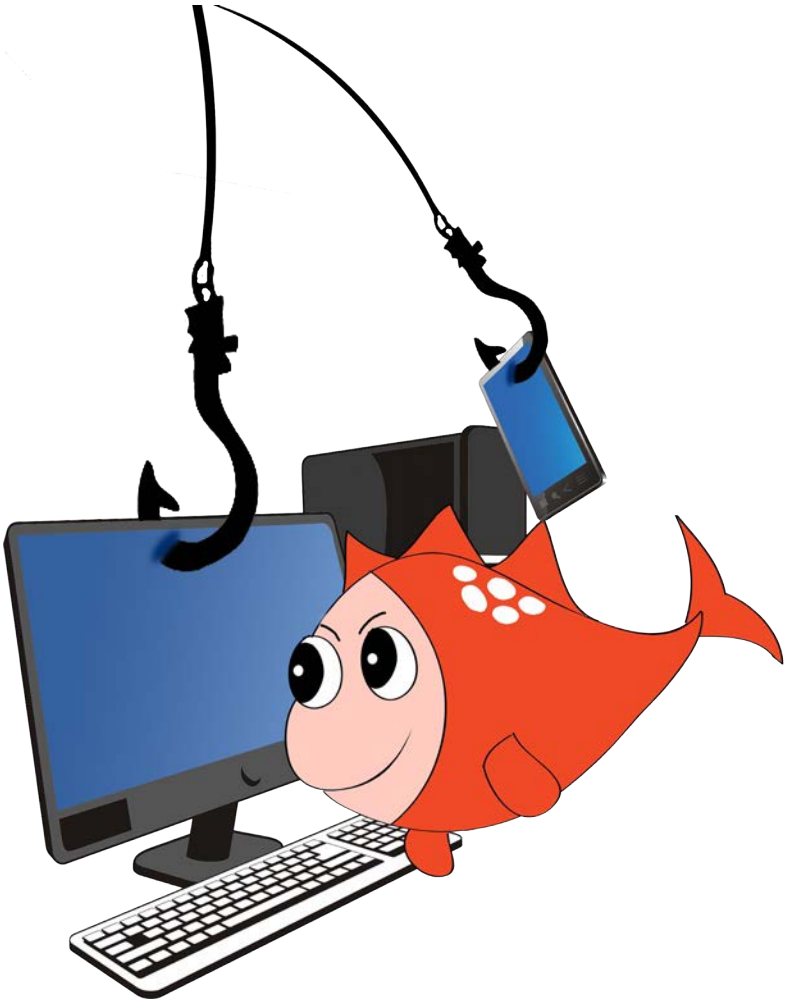
PHISHING ATTACKS

Always be careful about fraudulent /phishing e-mails

Know that phishing can also happen by phone

Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users.

Phishing is a way of attempting to acquire information such as usernames, passwords, PIN,bank account, credit card details by masquerading as a trustworthy entity details through electronic communication means like e-mail.

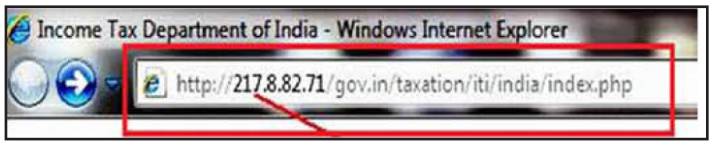


Threats

- Sometimes you may receive a threat mail saying that your webmail account would be closed if you do not respond to an e-mail message. The e-mail message shown above is an example of the same trick. Cybercriminals often use techniques to make one belive that security has been compromised.
- Spoofing popular websites or companies.
- Scam artists use graphics in email that look identical to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.
- Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.
- Cybercriminals might call you on the phone and offer to help solve your computer problems or sell you a software license.

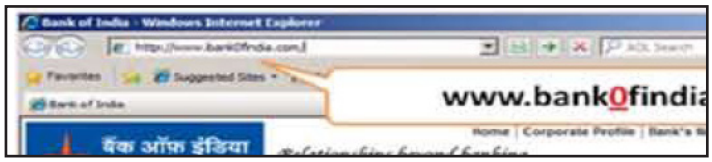
Steps to remember :

Step1: Cross check the URL in the browser



Don't enter your information in the websites that start with numbers

Step2: Always check for the misspelled URL

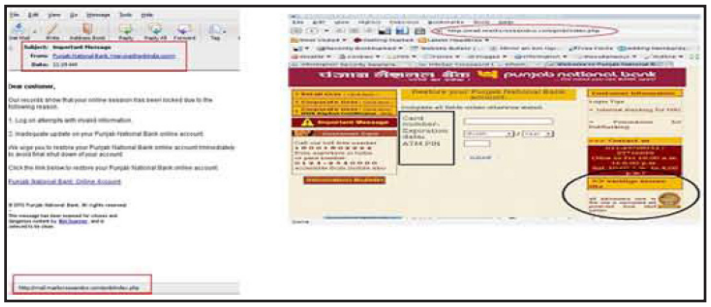


So Always key in the URL in the address bar yourself don't copy and paste

Step3: Always perform online banking in secure channel i.e check for the Padlock and secure channel for secure banking

Always check for the trusted website which has https and padlock

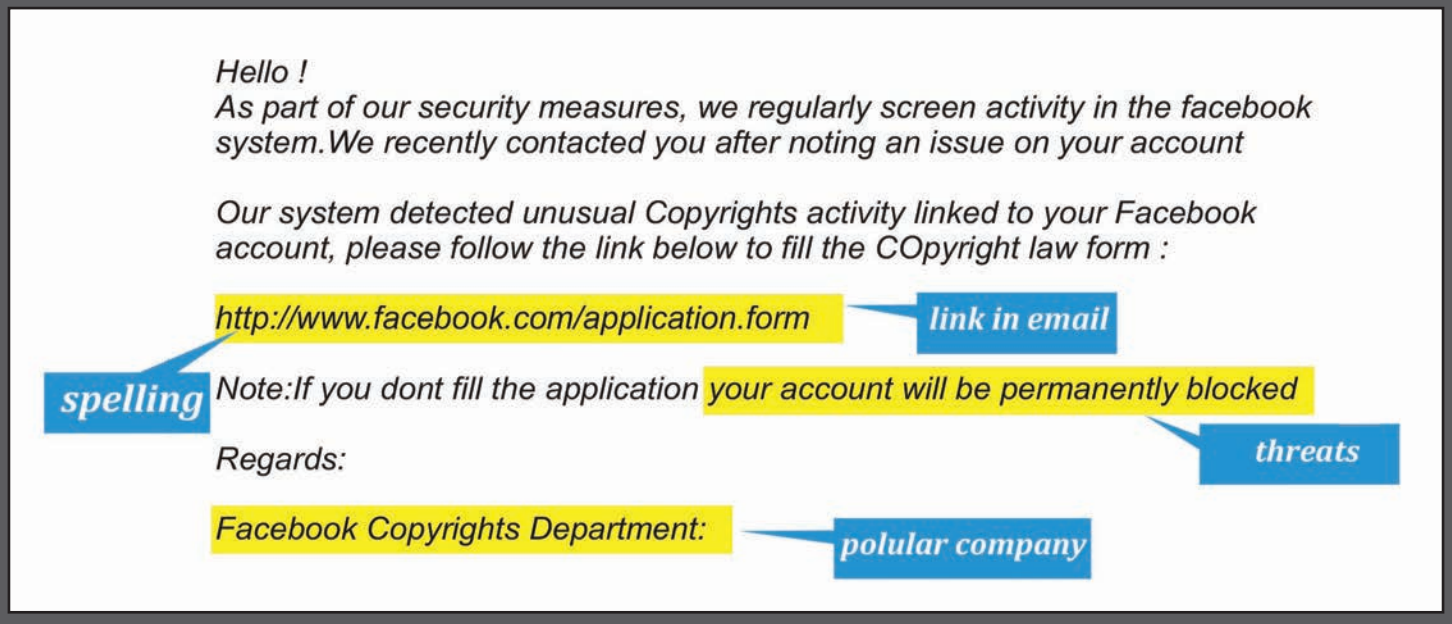
Step 4 : Always view any email request for financial or other personal information with suspicion, particularly any "urgent" requests. When in doubt, do not respond to questionable email or enter information on questionable websites. You may also contact the alleged sender to confirm the legitimacy of communications you've received.



An Example of Phishing site, the look and feel of the Punjab national bank is same.

Step 5 : Never respond to the emails that ask for your personal information like credit card /debit card/bank information.

A phishing e-mail message look like....



- *Spelling and grammar.*
- *Links might also lead you to .exe files. These kinds of file are known to spread malicious software.*

Here are the few Phishing techniques

- Social networking sites are now a prime target of phishing, since the personal details in such sites can be used in identity theft.
- One of the latest phishing techniques is tabnabbing. It takes advantage of the multiple tabs that users use and silently redirects a user to the affected site.
- **Filter Evasion** - Phishers have used images instead of text to make it harder for anti-phishing filters to detect text commonly used in phishing e-mails.
- **Phone Phishing** - Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN. Visher sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.
- Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information

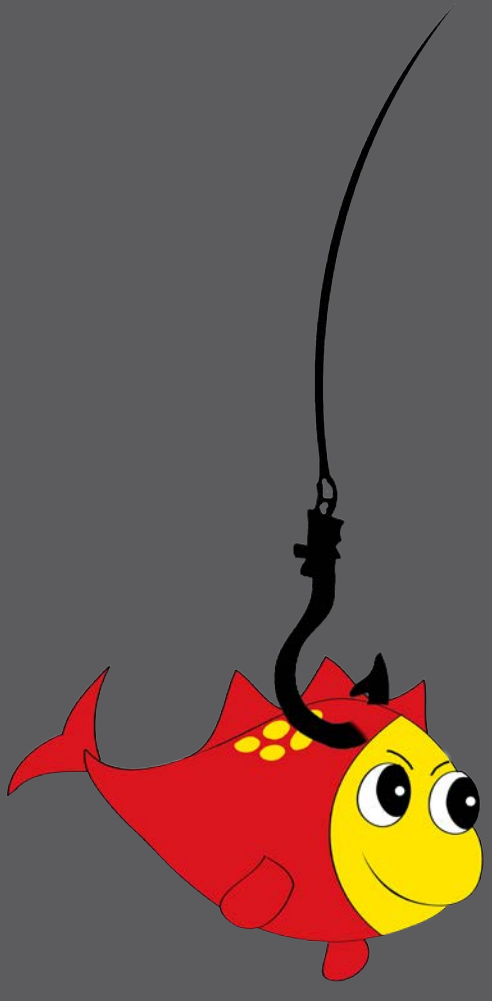
How I can recognize a message of Phishing ?

- *Normally phishing e-mails display grammatical errors or overlapped text.*
- *Test using false data before putting in actual information.*

What should I do if I think I've responded to a phishing scam?

- Take these steps to minimize any damage if you suspect that you've responded to a phishing scam
- with personal or financial information or entered this information into a fake website.
- Change the passwords or PINs of all your online accounts that you think could be compromised.
- Place a fraud alert on your credit reports. Check with your bank or financial advisor if you're not sure how to do this.
- Contact the bank or the online merchant directly. Do not follow the link in the fraudulent e-mail.
- Routinely review your bank and credit card statements for unexplained charges or inquiries that you didn't initiate.

Enable phishing filter in your mail client and web browser



Be suspicious of any e-mail with urgent requests for personal financial information

In case if you recieve a call claiming from a bank, then avoid or ignore such calls. Banks never call to know your details

Do's

- *Be cautious about opening any attachments or downloading files you receive regardless of who sent them.*
- *Look for the sender email ID before you enter/give away any personal information.*
- *Use antivirus, antispyware and firewall software (update them regularly too).*
- *Always update your web browser and enable phishing filter.*
- *If you receive any suspicious e-mail do call a company to confirm if it is legitimate or not.*
- *Do use a separate email accounts for things like shopping online, personal etc.*

Dont's

- *Don't reply to an e-mail or pop-up message that asks for personal or financial information.*
- *Don't e-mail personal or financial information i.e credit card or other sensitive information via e-mail.*
- *Don't click on any email or social media messages you don't expect or need.*
- *Don't open e-mail that you have any suspicion may not be legitimate. If it is legitimate and the individual trying to contact you really needs to, they will try another means.*
- *Don't open attachments that you were not expecting, especially ZIP files and NEVER run .exe files.*
- *Don't use your company e-mail address for personal things.*
- *Don't open any spam e-mail.*
- *Don't open suspicious videos or images in social networking sites since social networking are prime target of phishing.*
- *Never respond to phone calls asking for bank details. It might be vishing (voice phishing).*
- *Beware of phishing phone calls.*
- *Don't respond if you receive any message(sms) asking you to confirm account information that has been "stolen" or "lost" or encouraging you to reveal personal information in order to receive a prize, it's most likely a form of phishing.*

A Mozilla [Firefox] extension for anti-phishing support

About AntiPhish

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. According to a study by Gartner, 57 million US Internet users have identified the receipt of e-mail linked to phishing scams and about 2 million of them are estimated to have been tricked into giving away sensitive information. AntiPhish is a Mozilla [Firefox] browser extension that aims to protect users against spoofed web site-based phishing attacks. To this end, AntiPhish tracks the sensitive information of a user and generates warnings whenever the user attempts to give away this information to a web site that is considered untrusted.

Documentation / Publications

AntiPhish is a research prototype. Hence, we do not provide a complete user guide (yet). If you have any questions, feel free to contact the authors.
These papers give a pretty good overview of the tool and describes how it works:
Engin Kirda and Christopher Kruegel, Protecting Users agains Phishing Attacks with AntiPhish, 29th Annual International Computer Software and Applications Conference (COMPSAC 2005), Edinburgh, Scotland, July 2005
[download]
Engin Kirda and Christopher Kruegel, Protecting Users against Phishing Attacks (Best of COMPSAC 2005), The Computer Journal, Oxford University Press, 2006.
[download]
Thomas Raffetseder, Engin Kirda, and Christopher Kruegel, Building Anti-Phishing Browser Plug-Ins: An Experience Report, The 3rd International Workshop on Software Engineering for Secure Systems (SESS07), 29th International Conference on Software Engineering (ICSE), Minneapolis, IEEE Computer Society Press, May 2007
[download]

Prerequisites

- The Mozilla [Firefox] browser.

Install

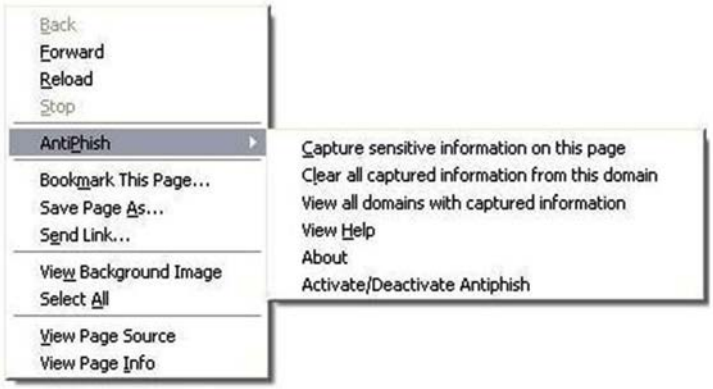
If you are already using Mozilla extensions, then ignore this part of the document. If you are new, keep reading: First, download AntiPhish and store it somewhere on your computer. Next, press CTRL-O (or go to the File menu item and then choose Open). Pick the AntiPhish extension file you've just downloaded. You will see a dialog where you can press the Install button. That's it.

Running and using it

AntiPhish is an application that is integrated into the web browser. It keeps track of a user's sensitive information (e.g., a password) and prevents this information from being passed to a web site that is not considered ``trusted'' (i.e., "safe").

The development of AntiPhish was inspired by automated form-filler applications. Most browsers such as Mozilla or the Internet Explorer have integrated functionality that allows form contents to be stored and automatically inserted if the user desires. This content is protected by a master password. Once this password is entered by the user, a login form that has previously been saved, for example, will automatically be filled by the browser whenever it is accessed. Antiphish takes this common functionality one step further and tracks where this information is sent.

After AntiPhish is installed in Firefox, it creates two menu items: You'll find it in the Tools menu and in the pop up menu when you press the right mouse button (check out the screenshots). Using the AntiPhish menu items, you can activate or deactivate it and cache information that you would like to be protected against phishing attacks.



Screenshot showing the AntiPhish menu item in the main menu

Reference : https://www.iseclab.org/projects/antiphish/

CERT-In Vulnerability Note CIVN-2015-0159
Multiple vulnerabilities in Apple Safari

Original Issue Date:July 07, 2015

Severity Rating: HIGH

Software Affected

- Apple Safari versions prior to 8.0.7
- Apple Safari versions prior to 7.1.7
- Apple Safari versions prior to 6.2.7

Overview

Multiple vulnerabilities have been reported in the Webkit component of Apple Safari which could allow remote attackers to bypass intended security restrictions, access potentially sensitive information, execute arbitrary code or cause a denial of service (DoS) condition on the affected systems.

Description

1. Cross-Site Request Forgery Vulnerability (CVE-2015-3658)

This vulnerability exist in page loading functionality due to improper handling of redirects while sending an Origin header. A remote attacker could exploit this vulnerability by enticing users to visit a specially crafted website.

Successful exploitation of this vulnerability could allow the attacker to bypass CSRF protection mechanisms and conduct Cross Site Request Forgery (CSRF) attacks.

For more details visit

http://cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES01&VLCODE=CIVN-2015-0128
http://cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2015-1453

CERT-In Vulnerability Note CIVN-2015-0158
Cisco Unified Communications Domain Manager Default Static Privileged Account Credentials

Original Issue Date:July 06, 2015

Severity Rating: HIGH

Software Affected

- Cisco Unified Communications Domain Manager Platform Software releases prior to 4.4.5 for version 8.x are affected

Overview

A vulnerability has been reported in Cisco Unified Communications Domain Platform Software which could allow an unauthenticated remote attacker to gain unauthorized access to a targeted system with the privileges of the root user.

Description

This vulnerability occurs due to a privileged account has a default and static password that is created at installation and cannot be deleted or changed without impacting the functionality of the system. A remote attacker could exploit this vulnerability to gain unauthorized access to an affected system with the privileges of the root user.

Successful exploitation of this vulnerability could allow a remote attacker to gain access to the affected system with the privileges of the root results in complete system compromise.

INFOSEC NEWS

indiatimes | The Times of India | The Economic Times | More

Sign In

THE TIMES OF INDIA India

Search

Home City India World Business Tech Sports Cricket Entertainment TV Life & Style Travel Women Spirituality Blogs NRI Real Estate Photos Videos Buy@Amazon.in

RELATED KEYWORDS: Rakesh-Maria | N-R-Natu | Metropolitan-Magistrate-Court

First cyber case conviction in Maharashtra

Ahmed Ali, TNN | Jul 3, 2015, 07.11PM IST

MUMBAI: The 37th Metropolitan Magistrate court on Friday convicted a senior executive of a private company in a cyber stalking case of 2009 for four months imprisonment. This case became first conviction case of cyber crime in the state of Maharashtra since the cyber laws came into existence in 2000.

Additional Metropolitan Magistrate N R Natu convicted and sentenced Yogesh Prabhu (now 36) to four months imprisonment for cyber stalking his colleague working in a cargo handling firm in Panvel. According to the police in February 2009, the victim woman who was an MBA graduate approached the than joint commissioner of police (crime) Rakesh Maria and lodged a complaint alleging that somebody was stalking her.

The 37th Metropolitan Magistrate court on Friday convicted a senior executive of a private company in a cyber stalking case of 2009 for four months imprisonment.

http://timesofindia.indiatimes.com/india/First-cyber-case-conviction-in-Maharashtra/articleshow/47927461.cms

BBC Sign in News Sport Weather Shop Earth More Search

NEWS

Home Video World Asia UK Business Tech Science Magazine Entertainment & Arts Health World News TV More

Technology

Hackers steal data from surveillance company

6 July 2015 | Technology

A company that sells surveillance software has been hit by a data breach.

Hackers said they had penetrated Hacking Team's internal network and stolen more than 400GB of data.

The Italian company said it was working with police to track down the hackers.

Widely shared online, the stolen data includes a list of the countries that have bought Hacking Team's main surveillance tool, Da Vinci, and emails suggesting

It is not yet clear who carried out the attack on Hacking Team or why they stole the d

http://www.bbc.com/news/technology-33409594

WORKSHOPS

1st Annual Appraisal Workshop

Be a role model by sharing tips/photographs of you/your kids, family members to generate Information Security Awareness among Indian citizens to enable them to participate safely in Information Society

Interested people may send their photographs/ tips to
pmu-isea@cdac.in

Follow us on facebook
https://www.facebook.com/cdac.isea

National Level Painting/Drawing Competition on Information/Cyber Security Awareness

For VIIth to XIth standard students

Where to send:

C-DAC, Plot No. 6 & 7, Hardware park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef via, Keshavgiri(Post), Hyderabad-500005, India.
Tel: 040-23737124/125

Last date for entries Oct 31st 2015

The backside of the paintings should carry Name of the student, Father's/Mother's name, Class, School name and address, Signature of the head of School/ Institution, Tel. no. of the school and School stamp

For more details visit
www.infosecawareness.in/contest

For more details visit
www.infosecawareness.in

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Department of Electronics and 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.

Department of Electronics & Information Technology,
Ministry of Comunications & Information Technology,
Government of India

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
Nalanda Building, No. 1 Shivabagh Satyam Theatre Road, Ameerpet, Hyderabad - 500016, Telangana (India)
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad - 500005, Telangana(India)
E-mail : isea@cdac.in