www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21350-21355
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.27

Survey of Intentional Enterprises Threats using Social Engineering Exploits and Prevention Techniques

Swati Chauhan
Department of computer science, K.I.E.T, Ghaziabad, Uttar Pradesh, India
swati.chauhan@kiet.edu

***Abstract*— this is a survey report of social Engineering threats that include various phases of social engineering. As security techniques increase, security break techniques will also increase in the same or more ratios. In this paper, we are trying to cover most areas of social engineering feats with Cause of social engineering in enterprises, various techniques of social engineering, influences and popular social engineering cases with relative study.**

Index Terms— **Broken Cloud, BYOD Dumpster, Cryptolocker, Cryptodefence, Hoaxing, Phishing, Robocalls, SocialEngineering, TJX Network, Vishing.**

I. INTRODUCTION

SOCIAL engineering is an 'art work' of consuming human behavior to break security without the participant even realizing that they have been manipulated. Misleading people keen on giving away confidential information comes into social engineering process.

According to Mann:

"By tricky way manipulate people, into giving out information, or performing an action" [1].

According to Mitnick:

"To cheat people by convincing them that the attacker is someone he is not, or by manipulation or using influence and urging. As a result, the social engineer is able to take advantage of people to obtain information or to convince them to perform an action item, with or without the use of technology" [2].

Social engineers also play a part like a "fraud game" to fraud people [3]. Basically social engineers are persons or group of people who deliberately misinform and operate people for personal benefit [3]. Social engineering also defined as "By scam into open-handed out data, or performing an action to deploy people," **[4].** The thought of social engineering has appeared just in the study of online duplicitous activities [5, 6, 7, and 8]. A survey in Consumer Sentinel states that US Federal Trade Commission, 2008, 221,226 complaints regarding Internet-related scam was filed by consumers. Internet Crime

exposed that e-mail was the maximum shared drop a line to method that is used by criminals of Internet scam (74%) In 2008 and the total loss of dollars in 2009 was connected to the cases of Internet fraud was $559[9, 10]. Some advance-fee cheat and average losses reported of up to $1500 [11]. It is very crucial to passionately influence to victims by computer fraud. On the other hand there are various phishing preys and psychologists liken to post shocking tension illness [12]. Identity theft victims with credit cards information faced penalty like harassment by loan refusals (31%-25%), and criminal investigations (12%). The highest among check fraud ($3000) was median loss filed per victim, confidence fraud ($2000) conferring to data recovered as of the Internet Crime Complaint Center [13]. According to a review of 2011 actual threat of social engineering in enterprises [14]:

- Highly aware of the social engineering threats, nearly 97% and 86% of security professionals and all IT professionals
- Who were aware that they have been targeted by social engineering schemes was nearly 43%.
- 16% were certain they had not been targeted by social engineering while 41% not aware that they had been attacked or not.

There is a cycle that is used to represent the social Engineering life in terms of attacks. The stage of "Growth of association" has no need of human interface all is automatically [15].

II. TYPES OF SOCIAL ENGINEERING ATTACKS [14]

There are various type of social engineering attack that use different methodologies to perform these as according to a report four of the newest (and lowest) social engineering scams Apr 21, 2014.

DOI: 10.18535/ijecs/v6i4.27

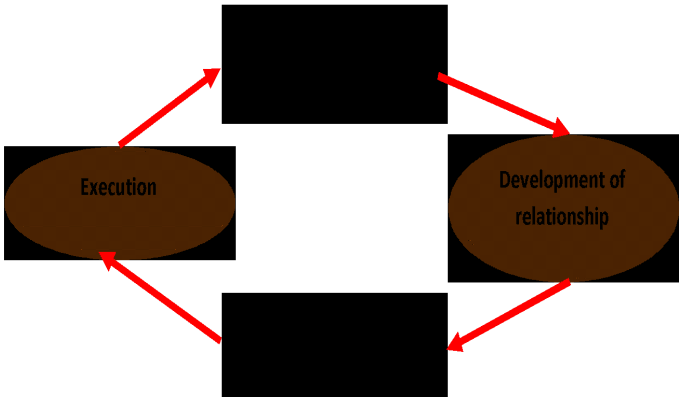

Fig. 1. Social Engineering attack lifecycle [15]

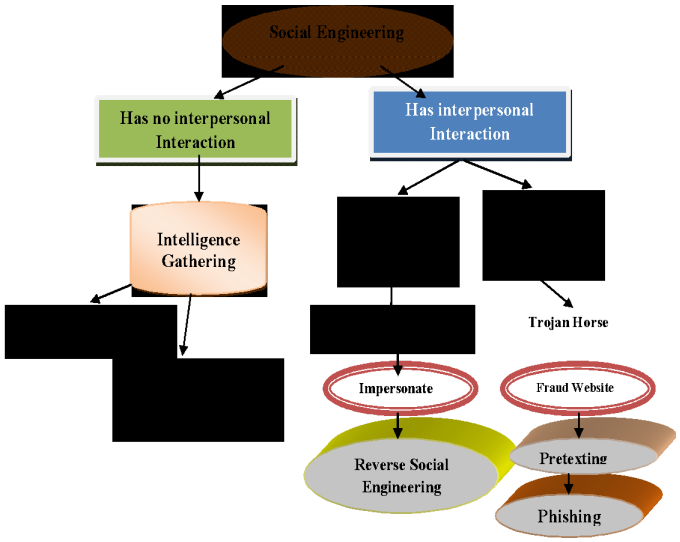

Fig. 2. Categorization of Social Engineering

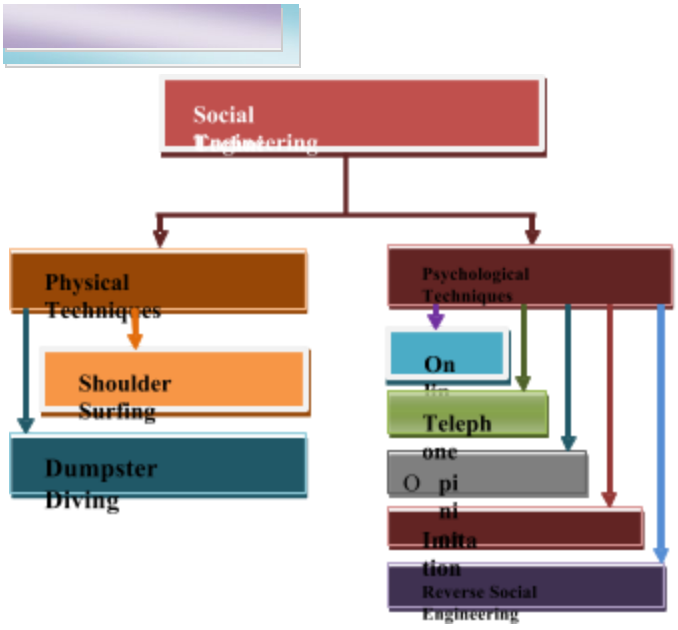

Fig. 3. Basic techniques used in Social Engineering

III. GENERAL TECHNIQUES USED IN SOCIAL ENGINEERING

There are various techniques that play main role in Social Engineering based on psychological tricks that an attacker can position to influence a user to give out information needed to access to a computer or network. Social engineers organize various skills with a form of influence [16, 17, 18, and 19].

A. Hoaxing

In this technique social engineers create fake situations in order to lead a user to change of decision on a certain matter due to a fear of an annoying incident [20].

B. Dumpster Diving

In this technique a searching of physical or electronic junk or garbage to look for important information it may be for paper-documents that contain valuable information. From this technique an attacker can carry out identity theft [20].

C. Phishing and Emails

In this technique attackers steal expensive information and make victims bumpy where e-mails woks as spam. A cheater make an trusty environment fooling a user to insert his/her credential information on fake URL (Universal Resource Locator) link once it is entered on the website, the data can be message claiming to be from PayPal. It can involve a malicious code that is hidden or attached to an email [21].

D. Pharming

In this technique there is an involvement setting for a fake web site that contains copies of pages from a legalized web site. Proper authenticated information is captured by the user needs to enter for proper. Phishing is used harming or DNS hijacking attack. Basically there is an adaptation from URL to IP address with the help of poisoning the DNS server. So when a person types the URL of a site they are redirected to a spoof site [22].

E. Vishing

This is the voice analogue to phishing. An email message asks the user to make a telephone call Instead of being directed by email to a website [23].

F. Malicious software

In this technique malicious software's are downloading and installing malevolent software. These are application of software's which involves spywares such as: Trojan horses, backdoors and key loggers where spyware is a group of software applications that gathers information about the workstation and users [24].

G. Impersonation of staff and identity theft

In this technique the personal information stolen via telephone, email or even face to face. Here a fake identity as

e-mail is created by social engineers for pretending users. A common technique for imitation is smacking [24].

H. Windows popups

Pop up window generated by attacker's malicious software that force a user to re-enter his or her username and password. Here users are no aware that an attack was conceded out and continue with their work [25].

I. Spying and eavesdropping

In this technique user identity and password obtained by seeing a user that capturing it in. Infrequently computer users may acquire habit of writing the identity and password down, thereby providing the spy with one more street to get the information [26].

J. CEO Scam

CEO scam is a procedure where convicts target to someone in account department of organization or a person who has power to pledge wire transfers then fool them for transferring a large amounts of money to the criminal controlled account from the company bank account. Most probably emails will state a retailer, or other entity the target company deals with, has changed their banking details and future payments should be moved the accounts which is controlled by criminals [27].

IV. IMPACT OF SOCIAL ENGINEERING

The main objective of social engineering attacks to get benefit in economic world and remuneration [28].In large organizations there is a faith for users on organization that in some situation they can lose confidence in the firm. There is loss of standing and kindness in social engineering. There are malwares that attack create serious threats to an information system and threats could be for financial gain, personal vengeance or social. Physical access gain can be achieved by a successful social engineer and damage the system. If we talk about social Site Facebook, profiles on which almost people has an account. identity theft is also include Profile imp storing, where cyber attackers create fake Facebook profiles of famous individuals who have a large following and they stole their identity so there should be methods on social sites that automatically detect dishonesty, identify imposters and get strict action against them.[29]

V. PREVENTION TECHNIQUES [28, 30]

Using ordinarily image processing the proposed schemes are tested. From the simulation of the experiment results, we can draw to the assumption that this method is strong to many kinds of watermark images. A preplanned strategy, standards, policies and guidelines on the basis of newly techniques involved in social engineering can provide help to protect any kind of security attacks.

- Usage of Computer system–The use of non-Company standard hardware or software, response to chain mail etc.
- Personnel safety– distribution of new and non-employees to ensure that they do not pose a security threat.
- Physical security– Include sign in procedures, electronic and biometric security devices to ensure their security etc.
- Protect system from viruses– To secure your systems and information from viruses and other threats Information security attentiveness instruction and acquiescence should be there.
- Fulfillment monitoring– Ensure that the security policy is being complied.
- Password policies Apply– Some ISO standards for secure passwords should be defined and follow.

Countermeasures

Education- Education plays more important role, in which company provide a facility in which employees review is taken year wise, to explain or train them with latest technologies. A screening of employees to confirm that they do not stance any scam 1.3 million job seekers information stolen. In August 2007, Hackers broke U.S. online recruitment site's password protected resume library using credentials that Monster Worldwide Inc. said stolen information was limited to names, addresses, telephone numbers and e-mail addresses, and no other details, including bank account numbers, were uploaded. Infect their PCs with malicious software

- Safety threat to the organization [31].
- Awareness of threats and risky behavior
- Policies' assessment and execution- There is a requirement of auditing to security policies. Check the security assurance and policy agreement verification periodically [32].
- Protection from malwares- Malware like Trojan, virus, adware, Spyware etc. using some software systems like firewalls, antispyware and anti-virus software with consistent apprising of areas. These will guarantee filtering of major security breach incidents [31].
- Audits and compliance- Policy gets successful only when it acquires implemented and everyone conforms to the policy. Hence auditing the usage and make sure everyone compliance to the rules [33] [34].

VI. POPULAR SOCIAL ENGINEERING CASES

There are various cases where victims give their confidential information eagerly without any doubt that is used by attackers wrongly.

*A. **2005***

Total number of criticism submitted to the Consumer Sentinel database in 2005 totaled 686,683. That was 21% percent increment from 2003 According to the Federal Trade

Commission. Other was Identity theft complaints represented 255,565 and the mostly type of identity theft was credit card fraud. June 2005, 40 million credit card accounts uncovered. With the help SQL Trojan attack Hackers broke Card Systems' database. Hackers expands names, accounts numbers, and verification codes to more than 40 million card holders by inserting code into database via browser page. Jones said that "Although they follow the rules and requirements, they would not have been compromised," The company was learnt by Pay-by-touch at the end of 2005 [35]. "Around more than 1 Million buyer swindle and distinctiveness theft complaints registered that have been filed with centralized, state, and local law application organizations and isolated organizations [36].

B. 2006

About 8.3 million U.S. adults over the age of 18 were victims of type of identity theft in 2005 according to Federal Trade Commission, 2006 (2006, Identity Theft Survey Report). December 2006, 94 million credit cards exposed. During a wireless transfer between two Marshall's stores in Miami, Fla a group of hackers stole credit card data. By obtaining pro of a weak data encryption system where break the TJX network through in-store kiosks that allowed people to apply for jobs electronically [35]. By the vulnerabilities 26.5 million veterans stolen their names, Social Security numbers, and dates of births. The analyst reported to the unknown person returned the stolen items June 29, 2006. The VA estimated it would cost $100 million to $500 million to put off and envelop possible dead from the theft [36]. User remnants completely uninformed and credulous at the same time as he obtains the required information [37, 38].

C. 2007

There was a report in which accounts fraud grow averages more than 14% than existing Account fraud decreasing to 9.4% into 2007 from 10.75% in 2006 where with the help of phishing scam 1.3 million job searchers information stolen. Hackers broke U.S. online employment site's password protected resume library using credentials that Monster Worldwide Inc. in August 2007 where stolen information was limited to names, addresses, telephone numbers and e-mail addresses, and no other details, including bank account numbers, were uploaded. Malicious software used to infect their PCs by clicking on links. July 2007, 3.2 million customer's records were stolen with credit card, banking and personal information. May 2007, a database administrator named William Sullivan, said to personal company called S&S Computer Services in Largo, Fla., had been fired. July 7, 2008, each person with financial information stole $20,000 for non-repaid identity theft losses [35].

D. 2008

There is an increment of 12% from 2008 to reach 11.1 million of adult victims of identity fraud, its maximum number from the survey started in 2003.A 2008 review report found, 80% of students who they received direct mail from credit card companies and 22% received around 4 phone calls in a month from credit card companies (CNN Money, 2008) by the U.S. Public Interest Research Group.

March 2008, with the help of SQL injection 134 million credit cards exposed. Albert Gonzalez was master mind who stolen the credit and debit cards information in 2009. In March 2010 he was sentenced to 20 years in federal prison [35].

E. 2009

November 2009, a primary target was the ecommerce sector in China. Fraud World cup related sites was launched during FIFA World cup 2010 by the phishers. There is a 33% increment in fraudulent new accounts stolen information in 2009 increased from 2008. There was a more than 1.4 million ID theft records from the U.S. Federal Trade Commission from 2005 during early 2010.Intellectual property were stolen in Mid-2009, in an act of industrial intelligence where Chinese government launched a massive and unique attack on Google, Yahoo, and dozens of other Silicon Valley companies [35].

F. 2010

January 2010, social engineering for exploration of employees working by a suspected Chinese cyber-attack on numerous companies likes Google [39, 40]. There is another more interesting thing that social engineering not even used to harm any organization but sometimes used to get information about the vulnerabilities of big organization network system that provide help to make them more strong and it is done by the Social-Engineering.org that organize rivalry in which goal is given by reputed companies and sources taken from Google, Face book and LinkedIn [41]. Data breaches of health insurance information increased 4 percent over 2008 (Javelin Strategy & research, 2010) [42]. December, 2010.1.3 million commenter's stolen from e-mail addresses and passwords. "The main reason of hijacked the account that some of users use the same passwords for Twitter and email and commenced with them to send spam," says McAleavey. Throughout the 2010, confidential information's were stolen [35].

G. 2011

A Credit card scam is a billion dollar a year industry (Nilson, 2011). In June 2011, there was a planned outbreak of social engineering to an outbreak on US government officials' Google email ID [39]. There was a decrement in the incidence rate of identity fraud victims from 6% in 2009 to 4.35% in 2010 but there was an increment of 12.6 % from 2010 to 4.9 % in 2011. So total 11.6 million identity fraud victims were there in 2011, this was the highest since the survey began in 2003.On the other hand the overall fraud amount decreased from $54 billion in 2009 to low of $18 billion [35]. Japan Earthquake scams were another example of malware using social engineering tricks in March 2011. Scammers sent malicious links to "dramatic" videos of the disaster with malware attachment that affect your PC on downloading and

took you to a phishing site that asked for personal information [43].

Personal information could be used to create more private and better-targeted phishing attacks. So these sorts of crashes happen all the time, and even more personal information is stolen. Still, Kevin McAleavey of the KNOS Project says the breach is being estimated as a $4-billion-dollar loss. Since Epsilon contain a client list of more than 2,200 universal brands and maintain more than 40 billion e-mails yearly, he says it might be, "the largest, if not the most expensive, security breach of all-time" [35].

*H. **2012***

Bank expertise are spending approximately 30 percent to $7.2 billion by 2015 in anti-fraud technology for mobile banking alone (Computerworld, 2012). In May of 2012, Simi Valley, four Nigerians are arrested by CA detectives into a Nigerian fraud ring for the possession of stolen credit information and credit card fraud. They were responsible for over $2 million in credit losses (Ventura County News, 2012). In 2011, approximately 1 in 300 electronic mail confined features pointing to phishing. According to RSA, phishing emails increased 37 % in 2011 to 50% that attacks targeting financial institutions (Information Security Media Group, 2012) [44]. The Javelin 2012 Identity Fraud Report exposes more interesting findings about trending and the occurrence of personally recognizable information found on targeted social networking websites.

*I. **2013***

Internal attacks of social engineering, attacks can be the most upsetting, there was damage that fortunate user can do and the data they can access. The CERT Insider Threat Center at Carnegie Mellon University's Software Engineering Institute and the U.S. Secret Service, researchers found spiteful insiders within the fiscal business typically get away with their fraud for nearly 32 months before being detected the survey of U.S. Department of Homeland Security. Some potential gateways for attackers are opened by Google Android phones and other devices. These come into bring-your-own-device (BYOD) trend. More companies put their important information in public cloud services if there is a single point of failure then attacked by social engineers. Slowly-slowly cloud computing converted their vulnerability surface, so will taking on of HTML5. Where it is noticed that failure occur or attack come HTML5′s cross-platform support and integration of various technologies opens up new possibilities for attack, like neglecting Web Worker functionality. A type of malware designed to render a computer or its files impracticable till a computer user pays a required amount of money to the attacker is ransomware [45, 46].

*J. **2014***

"Phishing emails are much more complicated today ... where phishers are using mean confirm!" During a Dark Reading Radio show, it is absorbed to "severe phishers" are hiring proofreaders as a customer-service choice to transports "phishing electronic mail that are actually working and are well written."[47]. There are various potential attack entry points. According to BI Intelligence survey, a total of 23.3 billion, Internet of Things (IoT) is a rapidly expanding universe device by 2019 that will be the enterprise market will account for about 40 % [48]. A well-known group FIN4 kicked off their attacks from side to side information-gathering. On the other hand, they supposedly contacted to an arrangement of publicly traded pharmaceutical and biotechnology organizations to pick up Wall Street terminology [49]. Till now, 2014 was the biggest year of malware yet although there is a very strong rock of security as SSL/TLS vulnerability called Heart bleed. The pipe of protocol loathing procedure graze targeted machine's memory and RAM then can retrieve the fully protected data from machines [50]. How social engineering related to side channel attack: In such type of attack a malevolent virtual machine is kept near to a cloud computing server that is used to launch side channel attack with the help of circuit vulnerabilities [51].

K. 2015

A drawback of OpenSSL project that it does not have the proper resources to check the codes a lot of the time. On Windows 7 and Windows 8, The IPv6 stack is vulnerable to a resource overtiredness mistake on this basis attacker free to send non-stop arbitrary router ads and munch 100% CPU of the system and most people are not aware that the flaws is present. More sketchily, IPv6 also re-implements some of the old trust flaws of IPv4 with ARP poisoning in IPv4 [52].

SAN JOSE, Calif., Aug. 6, 2015 (GLOBE NEWSWIRE) -- Ubiquiti Networks, Inc. , declared in its fourth quarter fiscal results [53]that it was the prey of an email business fraud incident where damage was of $39.1 million dollars and in the Form 8-K filings[54] of company specified that it became aware on June 5th 2015 that it was the prey of a "criminal fraud". Where members of in its secondary companies based in Hong Kong fell prey to what is known as a "CEO scam" or a "Business Email Compromise (BEC) attack.

L. 2016

Major attacks of 2016

1) THE RESUME SPAM AND RANSOMWARE:

In this attack spam emails contains a ransomware-laden email attachment.

2) OLYMPIC VISION AND SNAPCHAT:

One of the more successful BEC social engineering scheme was Olympic Vision that, instigating near to US$130,000 in compensations to every company it infested in 2015. BEC scam showing a lot of similarities to Olympic Vision beleaguered Snapchat employees, resulting in company information being stolen and exposed in In March of 2016.

3) SS&C TECHNOLOGY BEC SCAM:

2016, biggest social engineering attack beleaguered Wall Street technology firm SS&C Technology where company lost US$6m due to a Business Email Compromise scam[55].

VII. Conclusion

Although there are various super techniques of secure information system but still humans are surprisingly breaking the security without worrying about the penalty. In social engineering attack the people are the best tool to defend these attacks as well as we should be aware from those people that provide biggest risk of security. Well established policies of security and updated techniques can enhance the security mechanism of any enterprise. To make a secured network in organization ensure the training of employees regarding updated techniques. On the other hand, by implementing all-inclusive in sequence security strategy can reduce the blow of Social Engineering attacks. There tailgating can be used in the social engineering attacks that occurs when unofficial persons go behind certified persons in to an otherwise secure location. There are various methods as digital signatures, digital certificates, Biometrics security systems and different crypto graphics techniques can be used to secure our information network.

POLYALPHABETIC CIPHERS: THE VIGENERE CIPHER now days used basically. It is an example of a polyalphabetic cipher. Education, profitable to living economy telemedicine application everything is dependent on networking. To make it ensue the services ought to be consistent and protected.

References

[1] Mann, "Hacking the Human". *Aldershot (GB): Gower*, 2008.

[2] S. Woznaik, K. Mitnick, and W. Simon, " The art of deception: controlling the human element of security". Indianapolis, IN: Wiley, 2002, p. 368.

[3] Huang, W. & Brockman, "Social engineering exploitations in online communications": Examining persuasions used in fraudulente-mails. In T. Holt (Ed.), Crime online: Correlates, causes, and context-pp. 87-111. Durham, NC: Carolina Academic Press. A,2011.

[4] Mann, "Hacking the human: Social engineering techniques and security measures". Burlington, VT: Gower Publishing Company. I. 2008.

[5] Blommaert, J., & Omoniyi, "E-mail fraud: Language, technology, and the indexicals of globalization". Social Semiotics, 16, 573-605. doi:10.1080/10350330601019942, T. 2006.

[6] King, A., & Thomas, "You can't cheat an honest man: Making ($$$s and) sense of the Nigerian e-mail scams". In F. Schmallegar, & M. Pittaro (Eds.), Crimes of the internet (pp. 206-224). Saddle River, New Jersey: Pearson Education, J. 2009.

[7] Ross, "ARS dictaminis perverted: The personal solicitation e-mail as a genre". Journal of Technical Writing and Communication, 39, 25-41. doi:10.2190/TW.39.1.c

[8] Workman, "Wisecracker: A theory-grounded investigation of phishing and pretext social engineering threats to information security". Journal of personality and Social Psychology, 9, 1-27. M. 2008.

[9] US Federal Trade Commission, "Consumer fraud and identity theft compliant data": January-December, 2007. Washington DC: Federal Trade Commission.

[10] National White Collar Crime Center . Internet crime report. Washington, DC: Bureau of Justice Assistance, 2008.

[11] http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf

[12] The Internet Crime Complaint Center. 2009 Internet crime report.

[13] http://www.ic3.gov/media/annualreport /2009_IC3Report.pdf

[14] Carey, L, "Can PTSD affect victims of identity theft: Psychologists say yes",2009.

[15] http://www.associatedcontent.com/article/2002924/can_ptsd_affect_victims_of_identity.html

[16] BBC News,"Suicide of internet scam victim",2004.

[17] http://news.bbc.co.uk/2/hi/uk_news/england/cambridgeshire/3444307.stm

[18] The risk of social engineering on information security: "SURVEY OF IT PROFESSIONALS Dimensional Research", September 2011

[19] S. Heikkinen, "Social engineering in the world of emerging communication technologies," in Proceedings of Wireless World Research Forum, 2006, pp. 1–10.

[20] Sarah Granger, "The Social Engineering Fundamentals: Part 1 Hacker tactics" Endpoint protection, Security focus, December 2001.

[21] Schneier, Bruce. "Social Engineering a Police Officer", April 13, 2006

[22] SirRoss."A guide to Social Engineering, Volume 1".http://www.astalavista.com/index.php?section=directory&cmd=detail&id=3487

[23] SirRoss. "A guide to Social Engineering, Volume 2".

[24] URL:http://www.astalavista.com/index.php?section=directory&cmd=detail&id=3488

[25] Mosin Hasan, Spying Linux: "Consequences, Technique and Prevention", IEEE International Advance Computing Conference (IACC'09).

[26] Jared Kee, "Social Engineering: Manipulating the source", GCIA Gold Certification, October 2008.

[27] https://krebsonsecurity.com/tag/ceo-fraud/

[28] Allan A., Noakes-Fry K. and Mogull R., "Management Update: How Businesses Can Defend against Social Engineering Attacks"; March 16, 2005; Gartner.

[29] Schulman, Jay. Voice-over-IP Scams Set to Grow, VoIP News, July 21, 2006.

[30] Book of "People Hacking" by Harl.

[31] Ashish Thapar ,White paper, " Social Engineering:An attack vector most intricate to tackle".

[32] The Origin of Social Engineering Bt Heip Dand MacAFEE Security Journal, Fall 2008.

[33] SANS Institute InfoSec Reading Room (This paper is from the SANS Institute Reading Room site).The Threat of Social Engineering and Your Defense Against It. http://cybercoyote.org/security/deception.htm

[34] Nohlberg, M. "Social Engineering Audits Using Anonymous Surveys – Conning the Users in Order to Know if They Can Be Conned", in the Proceedings of the 4th Security Conference, Las Vegas, USA, 30 – 31 March 2005.

[35] White paper: "Avoiding Social Engineering and Phishing Attacks", Cyber Security Tip ST04- 014, by Mindi McDowell, Carnegie Mellon University, June 2007.

[36] http://www.pandasecurity.com/mediacenter/social-media/people-hack-social-media-accounts/

[37] Jared Kee- Redmon,"audit and policy Social Engineering manipulating source" ,SANS institute.

[38] http://www.csoonline.com/article/2124025/it-audit/information-systems-audit--the-basics.html.

[39] http://www.washingtonpost.com/blogs/federal-eye/wp/2013/09/17/auditors-social-security-may-have-overpaid-disability-claims-by-1-3-billion/

[40] http://www.csoonline.com/article/2130877/data-protection/the-15-worst-data-security-breaches-of-the-21st-century.html

[41] Allen M, "Social Engineering – A Means to Violate a Computer System", SANS Institute, San Diego, California, USA. June 2006. (http://www.sans.org/reading_room/whitepapers/engineering/) accessed 20 Dec 2006.

[42] Schulman, Jay, "Voice-over-IP Scams Set to Grow", VoIP News, July 21, 2006.

[43] Smith R.G.,"Preventing Identity-related Crime: 100 points, biometrics

or identity cards".AIC Trends & Issues No 324, Canberra, August 2006.

[44] Amir Efrati, Siobhan Gorman, "Google Mail Hack Blamed on China". The Wall Street Journal, June 02, 2011

[45] Warwick Ashford, "Social Engineering was Key to Google Hack",Computer Weekly, January 26, 2011

[46] http://www.computerweekly.com/Articles/2010/01/26/240062/Social-engineering-was-key-to-Google-hack.htm(accessed on September 16, 2011).

[47] Social-Engineering.org,"Social Engineering: Capture the Flag Results – Defcon",18 Social-Engineering.org, 2010.

[48] https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-FraudReached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail.

[49] http://www.bullguard.com/bullguard-security-center/internet-security/social-media-dangers/what-is-social-engineering.aspx

[50] Frank L. Greitzer , Jeremy R. Strozer, Sholom Cohen, Andrew P. Moore, David Mundie and Jennifer Cowley ,"Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits", IEEE Security and Privacy Workshops, 2014.

[51] http://www.forbes.com/sites/ciocentral/2012/12/05/the-biggest-cybersecurity-threats-of-2013-2/

[52] http://www.cso.com.au/article/564611/2015-social-engineering-survival-guide/

[53] http://ir.ubnt.com/releasedetail.cfm?ReleaseID=926462

[54] https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm

[55] https://themerkle.com/top-3-social-engineering-attacks-of-2016/