CHAPTER – III

CONSTITUENTS OF SOCIAL ENGINEERING
CHAPTER III

CONSTITUENTS OF SOCIAL ENGINEERING

This chapter elaborates on the research study’s first objective about studying the constituents of Social Engineering. The sub-objectives that support the research study are:

a) To study about the Types of Phishing and Techniques being used by attackers i.e., Modus Operandi of Phishers
b) To study about the constituents i.e., underlying mechanisms in or of phishing attacks
c) To study why do users fall for phishing attacks

3.1 Types of Phishing

Types of Phishing or Phishing Techniques and its cousins

3.1.1 Variants of Phishing

3.1.1.1 Deceptive Phishing

Phishing includes deceptive attacks, by means of which the victims are lured by forged messages to divulge credentials.

The intruder can procure merchandise, or impose other damage. The attacker does not cause direct economic damage, but sells the illegitimately obtained credentials to other criminals on a secondary market, where these are bought and sold.

3.1.1.2 Deceptive appearance

The question in the instrument, “Email is a simple, secure and private way to transmit sensitive information”, was framed in view of Deceptive appearance.

Deceptive visual appearance

Colour schema and image imitation of target entities.
Deceptive or Misleadingly named links – URLs can comprise a victim’s name and password. By means of it, the actual destination of a link can be used to “cloak”. Instances are, the weblink http://trading.security.biz@attacker.com, will lead to http://attacker.biz.

Deceptive location

Secure web sites are employing SSL for ensuring the connection between client and the server is private. It is denoted by “https://” rather than “http://” at the starting of the address and by a padlock.

The question in the instrument, “I will not enter my credit card information on a web site whose address starts with http://”, was framed in this view.

Figure – 3.1: The Padlock Icon

By identifying the SSL padlock icon in a browser frame and the presence of a favicon, the user may not determine whether the site to which he is connected is a secured one. The SSL padlock icon in the browser’s address bar enhanced trust in many subjects, but there are various reasons for not trusting it. They are:

- A lock icon by itself means only that the site has a certificate; it does not confirm that the certificate matches the URL being (deceptively) displayed. A user must click on a lock icon to determine what it means, and few ever do.

- It is possible to get a browser to display a lock icon using a self-signed certificate (i.e. a certificate that has not been issued by a valid certificate authority), with certain encryption settings.

- A lock icon may be overlaid on top of the browser using the technologies used to fake the URL bar. This technology may even be used to present authentic-looking certificate data if the user clicks on the lock icon to confirm legitimacy.
3.1.1.3 Deceptive information flow

The fraudsters increase the value of a compromise, by duping the user not to know that he has given sensitive credentials to an intruder. Gathering these information, the forged sites intimate the victim that he must visit back into a/c immediately to confirm the information, and taken to the legit site.

3.1.2 Malware

Malicious software, is created to infect, infiltrate or damage a computer system without the users’ knowledge. The term is used by security experts to denote a wide means of forms of hostile, encroaching, or bothering software code. It is encountered in the form of key loggers, worms, spyware, viruses and Trojan horses.

Viruses and worms have the ability to self-replicate, viruses by attaching themselves to other programs, infecting them and worms by propagating themselves, often self-spreading computer programs by exploiting the file transfer capabilities of systems. Criminals use worms, a familiar intrusion technique in phishing scams (Stallings, 1995).

Every minute, 232 computers are infected by malware. The lightning speed at which cybercriminals develop attacks and new malware code is making it harder for global organizations to manage fraud risk. One of the most important lines of defence is intelligence and awareness of the potential risks (RSA, 2015).

3.1.2.1 Malware or Master Boot Record (MBR) Infections

A MBR is an area of the hard disk (usually the first sector) used by a computer to perform start-up operations. It is one of the first things to be read and executed by the computer hardware when a computer is powered on, even before the operating system itself. MBR infections offer great scope for deep infection and control of computers, which makes the idea attractive to malware creators. Contemporary MBR infection methods are a fairly complex affair usually executed by highly skilled individuals. Trojan.Mebroot was a significant piece of malware, which not only infected the MBR of the computer but also implemented direct disk access to write its own code into unused sectors of the hard disk and therefore place itself into an area that the host
operating system wasn’t even aware of. This type of low-level infection, coupled with a sophisticated rootkit, makes it difficult to detect and get rid of Mebroot from an infected computer. While MBR infection has been a mainstay of Mebroot, another gang developed the highly sophisticated threat Backdoor.Tidserv, infecting system driver files as an advanced version. Trojan.Cidox, instead of targeting the MBR, infects the Initial Program Loader to achieve a similar overall effect. Aside from Trojan.Mebroot and Backdoor.Tidserv, there have been few other threats using the MBR infection technique, Trojan.Mebratix & Trojan.Bootlock, Backdoor.Tidserv.M, Trojan.Smitnyl, Trojan.Fispboot, Trojan.Alworo.

Short-lived Ransomware type threats is made for a single purpose and are not expected to provide a long length of service so malware authors don’t spend too much time and effort in creating and hiding them.

Infecting the MBR is not a new technique per se; many of the old boot sector viruses from over a decade ago did something similar. The difference is modern MBR malware do so much more than just infecting the MBR (Soeder et al., 2013).

3.1.3 Spear Phishing

Spear phishing may be defined as, highly targeted phishing attack aimed at specific individuals, single user or groups, department within an organization. Coined as a direct analogue to spearfishing, spear phishing makes the use of information about a target to make attacks more specific and personal to the target. The Phish appears to be legitimately addressed from someone within that company, in a position of trust, and request information such as login IDs and passwords (Trend Micro, 2012).

Emails are customized with information publicly available through search engines or on LinkedIn. The emails then direct victims to a bogus web page.

In a typical spear- phishing attack, a specially crafted email is sent to specific individuals from a target organization. The recipients are convinced through clever and relevant social engineering tactics to either download a malicious file attachment or to click a link to a malware- or an exploit-laden site, starting a compromise. Whereas traditional phishing scams are designed to steal information from individuals, some
spear phishing scams may also incorporate other techniques, ranging from computer hacking to pretexting (the practice of getting personal information under false pretences), to obtain the additional personal information needed to target a particular group or to enhance the phishing emails’ credibility. In essence, some criminals will use any information they can to personalize a phishing scam to as specific a group as possible.

3.1.3.1 Whaling

“Whaling” is phishing that aims at corporate executives, wealthy people and other “big phish.” Whaling emails are created with information directed to individual to divulge their credentials and are relatively sent to a small sects of people.

- The email will appear to come from a trusted individual within a company, usually the human resources or technical support.
- Passwords, usernames and other personal information are usually asked for.
- When the hackers receive this information, they can log into the entire company’s system.
- Clicking upon the link within this email, spyware could spread across the entire network.

The spear-phishing and whaling attacks will likely increase in quantity, as phishers look to target users with valuable information, the problem of phishing cannot be solved but it can be limited so that the worst impacts of phishing can be prevented (Hong, 2012).

Jagatic et al., (2007) conducted a research experiment by sending spear phishing email to unaware students. The student respondents were bifurcated as Social and Control groups. The social group students were sent spoofed phishing emails, as if from a person they were known of. The spoofed sender information was collected from the publicly available friends’ data on recipients’ profiles in social networking sites. The control group students also received the same email but the sender was spoofed to be an unknown fictitious person. The results revealed that when the mail was sent as if it was from a known person, the success rate was higher and that users were more likely to fall for the phish if the sender was of opposite sex. Results demonstrated de facto the
impact of spear phishing and the importance of rapid takedowns of phishing websites (Jagatic et al., 2007).

3.1.4 Search Engine Phishing

Scams involving forged banks website are particularly successful. A criminal creates a web page advertising lucrative interest rate slightly higher than any real bank. The victims, who enter this page via a search engine, are made to enter their bank account details for a balance transfer to the new account. Greed is a powerful motivator that can cloud judgment. In search engine phishing, phishers use search engines to drive traffic to illegitimate sites, on which they claim to be selling a product or service, usually at unbelievably low prices. The phishers set up fraudulent web sites and, as they have no intention of making any legitimate sales, they can claim to be selling virtually anything at any price that they think is likely to attract victims to their Web site. With this form of attack, phishers do not initiate contact with their potential victims, but the Internet consumers themselves search out the phishing site by means of entering certain key terms in a search engine, such as when, for example, searching for the cheapest online airline tickets. Since the Internet users, they themselves have found the site; gain a false impression of it being a secure and legitimate site (Radcliff, 2013).

When buying from the site, users have to complete forms requiring their personal details, including their credit card information and expiry dates, online. On submission of the form, an error message is displayed, informing the victim that a problem had occurred and that the transaction was not completed successfully. Meanwhile, the phisher will already have gained access to the information concerned, which may be used for future fraudulent purposes (Corrons, 2013).

3.1.5 Wi-Phishing

Wi-Phishing entails the phishing of personal information from consumers who make use of wireless technology and Bluetooth facilities. The cyber crooks set up Wi-Fi networks in public places, which users of wireless broadband connections tend to frequent. Hoping that they in legitimate networks at designated hotspots, the users can have their personal information (in the form of keystrokes and passwords) tapped into
by Wi-Phishers, who harvest personal information through their own networks (Hovanesian, 2013).

3.1.6 Spam

3.1.6.1 Spammers, Phishers and Fraudsters

Spam is defined as ‘Unsolicited commercial e-mail messages’. A spammer is a person who creates spam messages. Fraudsters are people involved in Internet fraud, a practice indulged in by individuals who spam potential victims (McFedries, 2014).

Email is the medium most organizations have come to rely on for communication. Unfortunately, most incoming email is unwanted - or even malicious. Today’s modern spam-blocking appliances have little problem weeding out the vast majority of unsophisticated spam campaigns, leaving end-user inboxes filled with only legitimate email. That’s in spite of the fact that more than 85 percent of incoming mail consists of spam or abusive messages.

To carry out phishing scams, attackers transmit large numbers of spam emails which include links (URLs) to web-sites under their control. The spam emails must resemble legitimate email, so that unsuspecting users will consider them genuine. The spam must also contain an appropriate message so that users will act upon it, be it an impending account suspension, a payment for a marketing survey, or a report of a transaction that the user will know to be fake and must therefore be cancelled. The email must also be able to evade the user’s spam filters. Looking like genuine email clearly helps, but the filters may also have access to a blacklist of URLs that are currently being promoted, so that there is value in varying the URL to prevent matches occurring (Drake et al., 2013).

The website on a free web space will have a typical URL of the kind http://www.indianbank.freewebsitesitename.com/keyin/ where the ‘indianbank’ is included to closely resemble the domain name of the genuine bank entity targeted. The intruders will add their created web pages on top of an existing structure, there by leading to URL of the typical kind like, http://www.xyz.biz/
~use/pictures/www.institutionname.com/, where the ‘indianbank’ is included to look legit.

To quench suspicion, the criminals register their own domain name, which will be used then. The domain names are selected to be a variation on indianbank.biz like indianbank-biz, or they will use the indianbank as a subdomain of some credible, clean domain, such as indianbank.extrasecureweb.com.

*Image spam*- The term applied to spam in which the core of the message is presented as a graphical image, not as pure text or HTML text, so that it isn’t susceptible to filtering on textual content. Since purely graphical content can be used as a spam indicator, this kind of spam is often accompanied by text which may be random or from a source of neutral text such as a novel or a news item. Image spam is most commonly associated with the Pump & Dump stock scam phenomenon, but has a long and ignominious history in phishing (Graham, 2013).

Spam filters can help catch a lot of phishing spam through analysis of what a typical phishing email looks like, but just as with regular spam, much will slip through. Phishing gangs are making it more difficult for automated systems such as spam filters to detect the presence of red flag keywords (such as Amazon and credit card) by replacing those phrases with images that look like text (Mutton, 2013).

### 3.1.6.2 Spam and Phishing – A pattern for Fraud

Spam is a favourite tool for phishers around the world, and one of the most effective ways that cybercriminals find new victims. Spam is estimated to make up more than 85 percent of all email traffic worldwide (Symantec, 2015).

Phishing and spam have close association, but they’re not the same thing. The key distinction between spam and phishing is the intent of the sender. While spam e-mail is annoying but benign, phishing scams can cause disastrous consequences for unsuspecting victims.

Spam prevention has also contributed to the fight against phishing. Phishing emails use the same distribution mechanism as spam and usually have many of the same characteristics. Email filtering based on content blacklisting, Bayesian filtering,
blocking mail from known spamming/phishing relays, anti-forgery solutions such as Sender Policy Framework (SPF) and Sender ID, and other heuristics specific to phishing can help prevent a great many phishing emails from ever reaching potential victims in the first place. However, spammers are continually evolving their tricks for bypassing filters and the phishers can leverage this (Schmidt, 2012).

3.1.6.3 Spyware or Crimeware

The indications or signs of Spyware infections compromising the system are, browser accessing websites that has not been requested, keyboard not working.

3.1.7 Spoofing

3.1.7.1 Forging a path

Phishing attacks use ‘spoofed’ e-mails and fraudulent Web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

The difference between the original website and the spoofed website are not easily spotted by the inexperienced user. The graphics used on the spoofed web site are similar to those on the original site and often the fraudsters use relevant website addresses. It is also possible for fraudsters to use the ‘same web site address by using JavaScript code, which replaces the victim’s browser’s address bar with a fake bar. Fraudsters will also use logos and footers similar to those on the original web site (Gerber, 2005).

Spelling errors aren’t necessary a defining part of phishing emails, and that logos in phishing emails can improve their success rate (Blythe et al., 2011).

DNS spoofing is a term applied to the malicious, covert redirection of a web browser from a legitimate site to a different, illegitimate IP address. The term pharming is sometimes used where the redirection is to a web site controlled by a phisher. Instead of the legitimate web site that the victim thinks he is accessing, for the specific purpose of identity theft by the stealing of online credentials (Lance, 2005).

A specific technique for this misdirection is DNS cache poisoning, where a flaw in the DNS software is exploited, with the result that the server accepts false information. The
DNS responses are not correctly validated, and the false data are therefore cached locally and returned to other systems making the same queries. More commonly, some malware contains code to add information to the ‘hosts’ file on the system, which is normally queried by default before DNS, to resolve a given name to a different IP address. This simple technique is effective, because it works even when the user directly enters the correct URL into a browser (Slade, 2006).

3.1.7.2 The Growing Threat of Email Fraud

3.1.7.2.1 A Typical Example of Online Fraud

Figure – 3.2 illustrates brand-spoofing and phishing cause threat to the brand equity of an entity, in this case a bogus bank. The trust and confidence of customers are subverted.

**Figure - 3.2: Brand-spoofing and Phishing threatening the Brand Equity**

*Source: Symantec, 2014*

3.1.7.2.2 The Scope of the Threat

Malicious applications that steal financial account information have increased dramatically over the years, potentially resulting in a direct loss of hard currency to affected victims. While the primary target continues to be online financial systems, the methods used to gather the sensitive information vary. Attacks spread from simply spamming e-mails with links to fake web sites, which is also known as phishing, to Trojans that monitor attempts to log on to online account web services and then begin
recording the pressed key strokes, take screen shots, or even redirect the whole network traffic to a malicious site.

The metrics and trends observed in phishing activity

- Phishing URLs were generated using phishing toolkits
- There are non-English phishing sites too

In the economic world, the media uses the acronym BRIC (Brazil, Russia, India, and China) as emerging market leaders. BRIC countries are the leaders of emerging market world. These countries have shown tremendous economic growth recently, and in turn have seen fast growth in broadband Internet. This growth in broadband use makes these countries vulnerable to botnets, a web of compromised computers (Symantec, 2013).

3.1.8 Bots/Botnets

The fraudsters try to evade spam filters by creating email with immaculate grammar. The constantly changing set of botnet machines are utilised in order send mails, which makes the block lists ineffective.

Bamital, a botnet, between 2013 and 2015 years has compromised more than eight million computers, operated by hijacking search engine results and redirecting to servers controlled by attackers. The botnet servers have now been shut down, and users of infected computers will be informed of their infection when attempting to search the Internet.

Bamital is an example of click fraud, a highly lucrative endeavour where by attackers aim to distort the numbers of clicks on an advertisement or visits to a specific website. Redirecting internet users to corrupt third party vendors or selling internet traffic through fictitious users, attackers seek to make financial gain from advertising expenditure.

3.1.8.1 The assess of botnet market

The trade of botnets is becoming a lucrative, high-margin industry, and is recognized as a form of organized crime. Botnet costs are low when compared to the financial
losses and damages to businesses and end users. Security experts report that a DoS attack allegedly costs between $500 and $1,500, while smaller botnet attacks are priced between $1 and $40 per compromised PC. Yet, the overall profits realized and monetary damages incurred far exceed these criminal financial outlays (Biever, 2014).

For example, Shiva Brent Sharma—arrested three times for identity theft via phishing—told investigators that he paid $60 for a program designed to harvest AOL email addresses. At age 20, Sharma had accumulated well over $150,000 in cash and merchandise.

Californian Christopher Maxwell and two unidentified co-conspirators operated multiple botnets that compromised systems at worldwide U.S. military installations, a Seattle hospital, and a California school district. Maxwell netted more than $30,000, and the entire project generated more than $100,000 in illicit installation commissions from multiple adware company affiliate schemes. Investigators reported that in two weeks, Maxwell’s bots reported over two million infections of more than 629,000 unique Internet addresses, with some machines infected repeatedly (krebsonsecurity, 2015).

German botnet researchers from the Honeynet Project discovered one malicious hacker who installed spyware programs on 9,700 hijacked Windows machines. The hacker—using adware from ‘DollarRevenue.com’—generated more than $430 per day (Biever, 2014).

Botnet players form a criminal enterprise that is intent on financial gains. Botnets have realized revenues ranging from several hundreds of thousands to several million U.S. dollars. Criminals involved in the botnet underworld can charge $100 per day to rent 1,000 bots (Trend Micro, 2015).

Hijacked PCs are not the only lucrative area for financial gains; members of the phishing ecosystem also deal in data. Credit card numbers obtained through phishing have been rented out or sold to other criminal third parties with a real time price of 10 card numbers for $20. Hundreds of credit card numbers were sold in a single night of trading, with each card number fetching $1 each (Rush, 2009).
3.1.9 Threats to VoIP and Mobile Convergence

3.1.9.1 Vishing

Vishing, or Voice Phishing, is a combination of Voice and Phishing, can work in two different ways. In one version of the scam, identity thieves’ sends the consumer an e-mail designed in the same way as a phishing e-mail, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and is then prompted to log in using account numbers and passwords. The other version of the scam is to call consumers directly and tell them that they must call the fraudulent customer service number immediately in order to protect their account. Vishing criminals may also even establish a false sense of security in the consumer by confirming personal information that they have on file, such as a full name, address or credit card number (FCAC, 2015).

Vishing poses a particular problem for two reasons. First, criminals can take advantage of cheap, anonymous Internet calling available by using Voice over Internet Protocol (VoIP), which also allows the criminal to use simple software programs to set up a professional sounding automated customer service line, such as the ones used in most large firms. Second, unlike many phishing attacks, where the legitimate organization would not use email to request personal information from account holders, vishing actually emulates a typical bank protocol in which banks encourage clients to call and authenticate information (Schulman, 2015).

VoIP infrastructure has been vulnerable to the same types of attacks that plague other networked computing architectures. When voice is digitized, encoded, compressed into packets and exchanged over IP networks, it is susceptible to misuse. Cyber criminals will be drawn to the VoIP medium to engage in voice fraud, data theft and other scams to steal personal and financial data – similar to the problems email has experienced. Denial of service, remote code execution and botnets all apply to VoIP networks, and will become more problematic for mobile devices as well. Denial of service will be a significant threat to VoIP. If a large number of VoIP phones become infected by malware and flood a network with traffic, the results could be extremely disruptive. Malware will be injected onto cell phones to turn them into bots. Large cellular botnets could then be used to perpetrate a DoS attack against the core of the cellular network.
Since the mobile communications field is evolving so quickly, it presents a unique opportunity to design security properly—an opportunity that was missed with the PC (Ahmad et al., 2013).

Battery power is a primary security hurdle. The antivirus software placed on a mobile device, will run the battery down, so mobile security will require new approaches and partnerships between manufacturers, carriers and application developers (Racic et al., 2014).

3.1.10 Phishing techniques

3.1.10.1 Dragnet method

The most frequently used phishing technique might be called the drag-net method. In real-world fishing, a dragnet is pulled behind a boat to catch any and all fish in a certain area indiscriminately. Similarly, dragnet phishing involves the use of spammed emails, bearing falsified corporate identification (e.g., trademarks, logos, and corporate names), that are addressed to a large class of people (e.g., customers of a particular financial institution or bank) to websites or pop-up windows with similarly falsified identification.

Dragnet phishers do not identify specific prospective victims in advance. Instead, they rely on the false information they include in the email to trigger an immediate response by victims – typically, clicking on links in the body of the email to take them to the websites or pop-up windows where they are requested to enter bank or credit-card account data or other personal data (Rusch, 2012).

3.1.10.2 Rod-and-Reel method

Rod- and- reel fishermen typically use lures for specific types of fish, and cast in areas of streams or lakes where those fish are mostly likely to be found. Similarly, in rod-and-reel phishing, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data (Rusch, 2012).
3.1.10.3 Lobsterpot method

The phishing technique, which relies solely on the use of spoofed websites, can be termed the lobsterpot method. In lobster fishing, lobstermen place their lobsterpots in places along the ocean floor where they believe lobsters are more likely to be. Lobsters that enter the lobsterpot can then be harvested when the lobstermen return.

Similarly, lobsterpot phishing consists of the creation of spoofed websites, similar to legitimate corporate websites that narrowly defined classes of victims are likely to seek out. In lobsterpot phishing, the phishers identify a smaller class of prospective victims in advance, but do not rely on a call to action to redirect prospective victims to another site. It is enough that the victims mistake the spoofed website they discover on their own as a legitimate and trust- worthy site. Example is Users looking for low fare Air Ticket (Rusch, 2012).

3.1.10.4 Gillnet method

In gillnet fishing, fishermen set up fixed nets in places where they believe schools of fish are likely to travel. Unsuspecting fish will be caught merely by swimming into gillnet and finding that their gills are too large to allow them to swim through or back out of the net. Similarly, in gillnet phishing, phishers introduce malicious code into emails and websites. They can, for example, misuse browser functionality by injecting hostile content into another site’s pop-up window.

Gillnet method relies far less on social engineering than the preceding techniques. Merely by opening a particular email, or browsing a particular website, Internet users may have a Trojan horse introduced into their systems. In some cases, the malicious code will change settings in users’ systems, so that users who want to visit legitimate banking websites will be redirected to a lookalike phishing site. In other cases, the malicious code will record users’ keystrokes and passwords when they visit legitimate banking sites, then transmit those data to phishers for later illegal access to users’ financial accounts (Leyden, 2014).
3.2 Modus Operandi of Phishers

3.2.1 Why do the phishers scams?

If a person has an email, then he is at risk. If he has made his email public, then he will be more susceptible. Scam artists who are “phishing” for some bait, are behind the phishing attacks. The scammers’ phish in a sea of people because, Phishers want personal information be used for their own personal gain. It is simple to create a Website that looks legitimate by mimicking another site’s HTML code.

3.2.2 The phishing landscape

The underlying mechanisms in phishing attacks – Phishing Attack Cycle

Figure – 3.3: Phishing Attack Cycle

![Phishing Attack Cycle Diagram]


Information Gathering involves, Gathering Personal Identifiable Information like Mobile contact no., E-mail id.

Development of relationship involves, developing a rapport. Dennis Thomas Regan of Cornell University, conducted a study on Rule of Reciprocation, in which the subjects who were given Cinema Tickets as freebies, ready obliged for a charity donation, where subjects who were not given Cinema Tickets, did not obliged. Cashing through the obtained information or selling that information to other cyber criminals.

3.2.2.1 Process flow of a Phishing attack

Phishing attacks can be carried in four phases: preparation, mass broadcast, mature and account hijack (Bose et al., 2007). The phishing process is represented in a flow diagram depicting the input required at various stages.
3.2.2.1.1 Planning or Preparation Stage or Phase

Steps involved are, 1. Vulnerability Scanning, Research and Design 2. E-mail Address Harvesting 3. Domain Registration and Host setup 4. Phishing email Design 5. Phishing Website Design.

Vulnerability Scanning, Research and Design, involves, Phishers scan for phishing opportunities and requires information to be collected which aid in convincing the targeted victims to divulge the private details the phisher seeks. E.g. Collection of Lists of potential target e-mail, and Scam page templates.

In E-mail Address Harvesting, Phishers harvest, or purchase, e-mail addresses of online users, by means of various sources such as websites, forums, surveys, hacked online company databases.

Domain Registration and Host setup, involves, Phishers purchasing and setting up unallocated domain names, often similar to the targeted websites domain name. Domains will be registered in order for the phisher to receive the phishing data which will be harvested. This step also involves performing other preparatory activities, such as hijacking of computers to secure compromised hosts.
Phishing E-mail Design involves phisher carefully crafting a phishing e-mail to be used in the phishing attacks. The phisher will try to make use of as many exploitation techniques in the e-mail to increase his chance of success.

Based on the Phishing E-mail Design, Phishers are categorized into two categories: Posers and Mongers. Posers are phishers who create phishing emails without putting much effort into it, therefore resulting in emails which are easily detected by most people. Monger on the other hand use smart techniques to trick the users. They are responsible for most of the global financial losses caused by phishing. Unfortunately even most silly phishing emails created by Posers lured the victims (Berghel, 2006).

In Phishing Website Design, Phishers will setup a counterfeit phishing website which has same appearance as legitimate website they are targeting. This will also include creating each phishing webpage so that it has the same look and feel as the target site.

3.2.2.1.2 Setup

Webpage is designed and setup. The look and feel of a fraudulent phishing site is alike as that of the entity. The HTML form page is replica of the form in the forged site or a slightly alteration.

3.2.2.1.3 Attack

Steps involved 1. E-mail Lure Distribution 2. User Attack Routing 3. Confidential Data Collection

A distinct phishing technique involves a fraudster sending large volume, thousands or even millions of deceptive spam e-mails impersonating banks and other legitimate organisations are sent out to lure Internet users.

The actual attack process begins when the user selects the website’s URL (domain name) found in the phishing e-mail message. The phisher will make the user into believing the URL is a link to a legitimate website, when in truth it is not, and they will in fact be requesting to view the phishers spoofed website.
Phisher exploit the trust relationship he has built with the victim. Once the user is on the spoofed website, the phisher will try to get the target to reveal information (Credit card number, account holder name, CVV code, Expiry Dates), and online identities. The data will be collected and stored on a database belonging to the phisher, or mailed directly to a secret phisher account.

3.2.2.1.4 Fraudulent Use of Phished Information and Cashing

It is end of the line for the attacker. At this point, attackers are now suppliers. There are a limited number of credential customers. Consumers of credentials are known as Cashers.

In this phase, Phishers become the provider of phishing ‘goods’ to intended criminals. Cashers are the consumers of confidential information, and they will take the data and convert it into monetary form. Cashers do not have any role in acquiring the data from customers; instead they purchase the data in bulk. Purchase rates work are for a full profile, consisting of full banking details, credit card details, account balances, passwords and PIN codes (Abad, 2005).

3.2.3 Steps in a Phishing Attack and its Countermeasures

Figure – 3.5: Steps in a Phishing Attack

All phishing attacks fit into the same general information flow. At each step in the flow, different countermeasures can be applied to stop phishing. The steps and its countermeasures are:
0. The phisher prepares for the attack. Step 0 countermeasures include monitoring malicious activity to detect a phishing attack before it begins.
1. A malicious payload arrives through some propagation vector. Step 1 countermeasures involve preventing a phishing message or security exploit from arriving.
2. The user takes an action that makes him or her vulnerable to an information compromise. Step 2 countermeasures involve detecting phishing tactics and rendering phishing messages less deceptive.
3. The user is prompted for confidential information, either by a remote web site or locally by a Web Trojan. Step 3 countermeasures are focused on preventing phishing content from reaching the user.
4. The user compromises confidential information. Step 4 countermeasures concentrate on preventing information from being compromised.
5. The confidential information is transmitted from a phishing server to the phisher. Step 5 countermeasures involve tracking information transmittal.
6. The confidential information is used to impersonate the user. Step 6 countermeasures centre on rendering the information useless to a phisher.
7. The phisher engages in fraud using the compromised information. Step 7 countermeasures focus on preventing the phisher from receiving money. (APWG).

3.2.4 The marketplace

3.2.4.1 The key players

The phishing ecosystem consists of a collection of individuals who play various roles within the phishing space, ranging from the financially-motivated botnet creators to those who actively pursue and prosecute the cybercriminals. In this ecosystem, a large industry of buying and selling – a micro economy – exists within the phishing underground, involving botnet creators, perpetrators, and enablers. However, these three player groups are complex and intertwined: a single individual or multiple perpetrators can play separate or simultaneous roles. Unlike lone virus writers who work for notoriety, botnet creators’ sole purpose is to seed the botnet for financial gain. Typical creators have been young, technologically savvy individuals, with the most prolific located in US, Eastern Europe, Brazil, Morocco, and China. However, botnet
creation tools have become so commonplace that the level of technological knowledge and sophistication is now lower; as a result, botnet creation is becoming even more prolific – and dangerous.

Another key player in the phishing ecosystem is the botmaster or bot herder, which instructs the botnets what to do. The botmaster may be the botnet’s creator, or a separate individual whose function is to rent or lease botnets. Botmasters can also serve as auctioneers who offer botnets to the highest bidders, such as spammers and online extortionists.

The members within the phishing space retain great flexibility and creativity to consistently maintain their activities and remain one step ahead of detection. By identifying the numerous vulnerabilities in software, these individuals exploit security flaws before patches are released (Leyden, 2014).

Security researchers notify that the Global current events also play a major role in phishing criminal planning. Phishers are highly news- and current events-aware, plan and implement their attacks in conjunction with particular world events or disasters. For example, following natural disasters such as major earthquakes, phishers will prepare and implement attacks using emails and Web sites designed to solicit donations to assist affected individuals.

3.2.5 Attack Structure

Figure - 3.6: Phishing Attack Structure
3.2.5.1 Phishing Attack Components or Components in Phishing Attacks

A phishing attack consists of three components, as a tripartite structure.

3.2.5.1.1 Delivery Component (a spoofed email)

Bait distribution through spoofed phishing email, called the ‘lure’ as it is aimed at fooling, or luring users redirecting them to a phishing website (Karof et al., 2007). The bait is cast via email, other channels for example, Vishing, uses VoIP technology to extend phish-like scams to telephone services. ‘Call to Action’ E-mail is recognized to be the most favourable method of carrying out phising scams, mainly because of its widespread use and their ability to be easily spoofed (Chandrasekaran et al., 2012).

Delivery Component - Phishing E-mail Exploitation Techniques

a. Mimicking of the appearance of online organisations - Phishers mimic reputable companies mostly involved in online banking or financial services. They do this by mainly using the company's images (corporate logos, slogans, colour schemes, company details, etc.), and URL's linking to the company’s website to give the appearance of authenticity (Jackson, et.al, 2007; Blythe et al., 2011).

b. URL Obfuscation – e.g. Replacing 1 with I or vice versa (Emigh, 2005).

c. E-mail Recipient Generalisation - Phishing e-mails not personalised when addressing recipients because they rely on the law of large numbers, which states that if enough e-mails are send out to a large group, there will be some form of success even if just a few respond.

d. The Use of Situational Contexts – Creating a sense of fake urgency, creating a sense of threat, creating a sense of concern, creating a sense of opportunity / reward (Sheng et al., 2010).

The urgency cues in phishing emails are the most deceitful for the recipients, as they turn their attention away from other cues that may potentially help them in correctly dismissing phishing emails (Vishwanath et al., 2011).

Context-aware phishing attacks dramatically enhanced the probability of a successful attack, from 3% percent for an ordinary attack to 48-96% for a specially-crafted context-aware attack (Jakobsson, 2005).
An attacker would gain the trust of victims by obtaining information about their shopping preferences, their banking institutions (discoverable through their Web browser history, made available via Cascading Style Sheets, or their mothers’ maiden names which can be inferred from data required by law to be public (Griffith et al., 2015).

e. Origin Impersonation - Utilising the weaknesses in the mail server communication protocol (SMTP), phishers are able to spoof the origin of the e-mail

f. Spear Phishing - The highly customized attacks, Spear phishing sends highly personalised, targeted e-mails to well researched victims, such as the top executives of an organisation. Attackers target specific individuals within an organization, often try to trick employees into installing malware or revealing their organizational passwords (Roberts, 2015; Leyden, 2015).

g. Adaption to anti-spam or anti-phishing filters- Phishers try to mislead phishing filters into searching for and extracting incorrect search terms

3.2.5.1.2 Mimicry Component (a spoofed website)

Data collection is done through a fake web site, by means of direct response to email, or through planting of some form of spyware onto the victim’s system. Fake web sites are an essential component of phishing attacks, but they are actually a special case of data collection through misdirection, albeit the most common. Fraudulent phishing website is normally hosted on a hacked machine or server. Attackers create web pages that have a similar visual appearance to that of a well-established legitimate website. Also, an attacker can hack into a popular website and easily replace one or multiple pages with their own spoofed webpages (Chandrasekaran et al., 2012).

Mimicry Component - Phishing Website and Browser Exploitation Techniques

a. Redirection Attacks - Phisher leads all recipients to a single server, and then redirects each user to a different website at a different servers in order to be phished

b. Trojaned Hosts - Phishers try to attack a PC, and install Trojan horse program in it, there by using the compromised PC as a slave to propagate phishing
messages. Hence it is extremely difficult to track a phishing attack back to the individual who initiated the crime.

c. SSL / Certificate Authority Spoofing Attack - Phishers fake a small lock icon (similar to the lock icon that signifies an SSL connection) when their webpage is displayed that is not SSL secured.

Attackers have also been quick to exploit attempts at user education. For instance, many users believe that a transaction is secure if they see the 'lock' icon displayed in the browser window. One possible attack uses JavaScript to display a spoofed lock image in the appropriate location (Ye et al., 2012).

Phishers may also acquire their own SSL certificate, relying on users’ inability or unwillingness to verify the certificates they install. There have also been cases in which Certificate Authorities issued certificates to attackers posing as legitimate Microsoft employees (Microsoft, 2011).

d. Spy Phishing - This attack involves sending a phishing e-mail to the targeted users who are requested to download and install a certain application. This application will secretly monitor the user’s Internet usage until the user visits a specific website. When the user goes to that particular site, the software they had previously installed onto their system becomes active and sends the phisher all the user’s private information

e. MIM attacks- Phisher will be mid-way of the user and a legit server, and relay any data or messages that are transferred between them, whilst saving the valuable data for himself. This attack allows phishing to observe and collect all transactions that are made

These components will together be used by the phisher to fool Internet users into giving them the information they seek.
3.2.6 The Phishing Economy

Phishing gangs operate within a complex network infrastructure that closely resembles any other supply-and-demand economy. Their members may take on a wide variety of roles and functions, taking in:

- Gathering of information such as target email addresses.
- Acquisition of tools for setting up phish sites (often using widely available phishing kits).
- Acquisition of spamming tools and hosts for bait distribution – this is a very common use for botnets.
- Acquisition of access to compromised hosts for scam pages.
- Setting up a process for retrieving stolen credentials e.g. from an anonymous mailbox (drop box) or via an eggedrop bot.
- Supplying victim’s credentials to a cashier for cashing out (conversion to cash).
- Use of stolen credentials to buy goods subsequently sold on to the black market.

A common manifestation of these money laundering activities is the mule solicitation email, offering financial management jobs that involve receiving money and passing it further up the chain after taking a percentage as commission (Abad, 2005).

The phishers seems to send a legitimate e-mail. The mail may have institution’s logo and appears to be sent by the director.

The mail may say that they noticed unusual transactions happening through his a/c and will be asked to key in some confidential details. The client may respond.

Later a real employee of client’s financial institution will be communicating to him, reporting that indeed there were some unusual online withdrawals taking place in his name. The client’s savings/current accounts were suddenly well over-drawn.

3.2.7 Phishing the cost to brand

76% of organizations learn of an attack from their customers. When the brand is used in a phishing scheme, the company is the largest victim. The company might have invested heavily, probably over many years, into establishing a brand that people
trust—and a brand they will do business with online. When that brand is used to defraud people, trust is badly damaged, even though the company was not responsible.

The brand will inevitably suffer from reduced return on investment for its marketing expenditures. Victims, most of whom are not familiar with how phishing works, may feel that if the company had proper security, this would not have happened. Customers may be non-responsive to future email marketing, unsubscribe from email lists, or completely move away from your brand. The potential magnitude of impact can be significant; the lifetime value of a customer who uses email can be as much as 80% higher than a customer who does not. The soft costs of rebuilding trust in your brand can be tremendous (iSMG, 2010).

### 3.2.8 Phishing site attack methods and target sectors

#### 3.2.8.1 Phishers Exploitation of Free Web Hosting Services

For phishers, using free Web hosting services has been the easiest form of phishing in terms of cost and technical skills required to develop fake sites.

However, this form of attack is not as widely used as it frequently requires manual efforts to prepare the phishing Web page, unlike the automated kit generated Web sites. Many free Web hosts have also improved their preventative and corrective anti-phishing measures significantly decreasing the lifespan of phishing sites on their systems.

#### 3.2.8.2 Top-Level Domains of Phishing Sites

Phishing URLs were categorized based on the TLD. TLDs are the last part of an Internet domain name; i.e., the letters that follow the final dot of any domain name.

E.g., in the domain name, www.efg.com, the Top-Level Domain is ‘.com’ (or COM, as domain names are not case-sensitive).

ccTLD are used by a country or a territory. They are two letters long, for example ‘.in’ is for India.
gTLD are used by a particular type of organization (‘.com’ for a commercial organization). It is three or more letters long. Most gTLDs are available for use worldwide, but for historical reasons ‘.mil’ (military) and ‘.gov’ (government) are restricted to use by the respective authorities.

3.2.9 Countries Hosting Phishing Sites or Geo-Location of Phishing Sites

USA is the leader in hosting phishing sites. Also, a large number of phishing sites are hosted in ASPAC countries.

Phishing websites are hosted on hacked Web servers, exploited machines, unbeknownst to their owners.

Other countries, includes Russia, China, Korea, Japan, Canada, Brazil, Germany, Australia, Italy, Spain, Israel, France, Hong Kong, United Kingdom, Poland, Netherlands, Mexico, Dominican Republic, Ireland, India, Chile, Thailand, South Africa, Romania, Norway.

Phishing attacks are becoming more and more frequent on brands that are not based in the UK and United States. Although the US and UK are still the most common. Security Analyst have seen increases in attacks that are written in languages other than English attempting to gain credentials from users in a number of countries including; Italy, Spain, Japan, Korea, and Germany (Wei et. al., 2013).

The Rock Phish gang registers many domains, in countries such as the USA, Canada, South Korea, Hong Kong, Singapore, and Israel.

Phishing in International Waters - Non-English Phishing Trends: In terms of the languages used in phishing attacks, English is still the most dominant. Others are German, Portuguese, Spanish, Dutch and Chinese language.

3.2.10 Phish Attacks by Industry or Target Sectors

The Financial sector, Payment Services, Retail/Service sector, Online Gaming, Social Networking, Auctions, Government, ISPs, web hosting services, CAs remains as important sectors of phish attacks.
• MMPORGs are targeted by phishing attacks for the purpose of gathering access credentials to the accounts of MMPORG players. These could either be traded for money or could contain payment card details.
• In Phishing attacks against web hosting services, cybercriminals attempted to obtain access credentials to websites hosted by the service providers. Hosted websites, in turn, can be used to host a wide variety of malicious content, including phishing pages or malware infection points.
• ISPs were targeted by phishing attacks, with the likely goal of collecting email addresses the issue. These in turn could help facilitate a cybercriminal’s spamming efforts as emails that appear to originate from within the ISP’s network are less likely to get blocked by an ISP’s anti-spam filters.

3.2.11 Damage control

For phishers, the first hour of any attack is the most productive. Fifty percent of all credentials are stolen in the initial hour of a phishing email campaign. It is referred to as the golden hour. Within five hours, more than 80% of credentials are stolen, and the first ten hours yield more than 90% of all credentials that the phishers will get from that forged website (Klein, 2010).

Rapid take down of phishing websites is crucial to damage control. Rapid take down requires awareness. Phishing site takedown is much more efficient when the brand owner is aware of the phishing site and involved in takedown efforts. The average uptime for phishing websites hosted on compromised machines and free web hosting services drops from about 50 hours to about 4 hours when the brand owner is aware and becomes involved in takedown efforts.

Most phishing web sites are active for about 20 hours until they are taken down. Take-down is a reactive strategy, an increasingly prevalent trend in the way that security issues are being handled. Software vendors wait for vulnerabilities to be discovered and then issue patches. Anti-virus tools update their databases with new signatures as new viruses are identified. In these reactive approaches, the defenders aim to identify the bad guys as quickly as possible to minimise exposure, while the bad guys scramble to open new security holes at a sufficiently fast rate to continue their activities. A reactive strategy does reduce the damage done by phishing websites (Moore et al., 2014).
3.3 The constituents i.e., underlying mechanisms in or of phishing attacks

3.3.1 The mechanics of phishing

3.3.1.1 Rock-phish or Fast-flux Attacks

A rock-phish or fast-flux system is set up where numerous compromised machines act as proxy web servers to hide the true location of the attacker. Compromised hosts are given a new set of IP addresses every few minutes so that someone connecting gets a different machine each time. These machines act as redirectors of requests and data to and from backend servers, which actually serve the content.

Typical phishing websites operates with web pages added to existing structures and occasionally use misleading domain names. However, rock-phish gang operates in a rather different manner. Having compromised a machine, they then cause it to run a proxy system that relays requests to a back-end server system. This server is loaded with a large number (up to 20 at a time) of fake bank websites, all of which are available from any of the rock-phish machines. The gang then purchase a number of domain names with short, generally meaningless, names such as pqr90.info. Hence, a canonical URL such as http://www.pqr90.info/ is sufficient to fetch a top level web page and its fingerprint is sufficient to identify the domain and associated IP address as owned by the rock-phish gang. The gang’s methods differ so much from other phishing websites. In particular, their email spam, which has a characteristic section of random text followed by a GIF image containing the actual message, is estimated to account for between one third and one half of all phishing email. The rock-phish gang is believed to be extremely successful (McMillan, 2013).

3.3.1.2 ‘Fast-flux’ phishing domains

The Fast-flux domains are arranged to resolve a set of IP addresses for a short period, then switched to other. This of course ‘eats up’ many hundreds of IP addresses a week, but the agility makes it almost entirely impractical to ‘take down’ the hosting machines. The gang is likely to have large numbers of compromised machines available, since if they are not used to serve up phishing websites they are available for sending email spam.
The phishing websites are hosted on ‘fast-flux’ botnets where the IP address which is contacted changes every 20 minutes, forcing take-down companies to go after the domain name rather than the host; and the domains are registered in bulk, and will only be valid for less than a day.

The ‘take-down’ companies also count URLs even, in some cases, creatively inflating their figures. For example, sometimes all of the URLs of the form www.lmn.com/~user/phishing.html will lead to the same page – for all of the hundreds of ‘lmn.com’ domains hosted on the same physical machine. So although just one website has been compromised, and just one URL is appearing in emails, hundreds of different attack reports will be counted. Another example occurs on the fast-flux networks where it is common for multiple banks to be attacked in parallel. The criminals are not very tidy, and so they leave the webpages for old attacks lying around. Although they may not actually be sending out further attack emails for a particular bank, the domains they’re using to attack someone else are valid URLs for their old target – these URLs, which exist but do not harm anyone (McMillan, 2013).

3.3.2 Pump and Dump scams

These schemes involve the hands-off manipulation of the stock market, rather than the direct plundering of a victim’s funds and identity that characterizes the phishing scam. However, they constitute a much more serious problem than is generally realized at present. Pump and dump scams, are more impersonal in nature, and don’t involve direct access to the mail recipient’s funds or identity (Harley, 2010).

A study by researchers, noted a significant increase in both price and volume of shares traded for spammed stocks, from the day before touting begins until the day of the most active spamming. The study, explained who—besides the spammers themselves—were doing the trading. The naive investors who are greedy and maybe not so smart—similar to the people who send thousands of dollars to Nigeria (419 Scam) or pass on chain letters (Frieder et.al, 2010).

If the spammers attach even a very small probability of success to the idea that they can make money, they figure it’s worth a try. There are people who know that the information is worthless, but they figure that if other people don’t know that, there
might be a chance to make a buck. If the victim thinks that other people are going to buy and push up the price, he might buy if he thinks he can get in early enough, reap a little bit of that gain, and get out (Kreibich et.al, 2010).

3.3.3 419 Scams and Phishing

Most security professionals distinguish between 419s and real phishing. However, there are enough similarities between the two activities to contradict the assumption that they are completely separate phenomena. For instance:

- Both are frequently implemented by organized gangs.
- Both include money-laundering as part of the exploitation mechanism.
- Both are opportunistic, taking advantage of personal tragedies, natural disasters and so on as a means of parting a victim from their money.
- Both are sometimes very stereotyped in the way they present their bait emails.
- Both use social engineering techniques to bait the trap, albeit with the 419 offering some sort of financial reward, and phishing often purporting to prevent financial loss.
- Both involve some form of identity theft: that is, they claim to be someone else or to represent an often real and presumed legitimate organization.

Some significant points of difference are that:

419s often, though by no means invariably, have a strong overt African connection, though it isn’t practical to distinguish between frauds on a purely national basis. Indeed, there have been an increasing number of such frauds ostensibly originating in conflict territories such as Iraq and Afghanistan.

419s rely on an element, sooner or later in the defrauding process, of personal contact, whereas phishing gangs tend to work at more of a distance and go to lengths to cover their tracks.

419s generally rely more on social engineering or human gullibility, than on technical attacks such as embedding malware, cross site scripting, DNS spoofing and so on. Historically phishing was also more reliant on social engineering, but techniques have evolved to combine this with more advanced technological methods.
It’s not unknown for a 419 scam to hinge upon a deceptive web site, though it’s more common for a 419 to use a legitimate but irrelevant web site as some form of authentication. Similarly, not all phishing attacks employ a deceptive site such as a fake bank site, but most do. However, it’s uncommon for a 419 to depend on a fake financial institution site, or forms that seem to be generated by genuine institutions.

The 419 scammer often claims to represent a fake organization or group of individuals, whereas the phisher generally relies on spoofing a genuine organization’s mail or web site. 419s tend to work on a more personal level: the scammer often claims to represent an organization such as a bank or a military organization, but will usually be offering a deal which would be against the interest of that organization.

While there are evident points of dissimilarity, it’s hard to find absolute differences. There are features of tone and phraseology that are unmistakably 419, and some of the topics are virtually unique to the 419 – bank account proxy (next of kin) scams, lottery scams, some kinds of job scam and so on. However, some others, such as fake charity and disaster relief appeals and mule recruitment solicitations, resemble the output of phishing gangs in topic, if not in tone. Indeed, 419 gangs are now showing an increasing eagerness to pick up on phishing ideas and technology (Peel, 2011).

3.3.4 Hacktivism

3.3.4.1. Fast food service restaurant’s Indian website hacked and client information leaked

In September 2009, the Indian website of a popular fast food retailer was hacked into by a Turkish hacker group. Details of about 37,000 accounts, including names, phone numbers, email addresses, passwords and city details were leaked. The company’s India website was hacked into using the SQL injection method and remote file inclusion, one of the most common methods for stealing private data from web databases. Through this, the hacker typically tricks the site’s database into revealing data that should be hidden by ‘injecting’ certain commands (Kshetri, 2010).
3.3.4.2. Indian software organisation’s store hacked, usernames and passwords stolen

The hackers, allegedly belonging to a Chinese group, struck at an Indian company’s website, stole login IDs and passwords of people who had used the website for shopping. Following, the members of the group posted a message on the company’s website saying ‘unsafe system will be baptised’. The website seemed to have been taken offline by the software corporation (Ball, 2011).

3.3.5 Domain Name Typos

The cyber criminals, register domain names that closely resemble the domain name of a legitimate high-traffic site. The domain names are sometimes used to host sites aiming to install spyware or malware on the computer of a victim who mistypes the intended domain name. It would also be possible to register domain names that could be common typographical variants of online commerce sites.

Phishers can also exploit mistyped URLs by registering domain names like goooggle.com or goggle.com, or even employ techniques to artificially inflate their rankings in search engines. To make matters worse, researchers have discovered automated phishing kits circulating online that enable novice phishers to employ some of these techniques (Sophos, 2013).

3.3.6 Technical Exploits that Enable Phishing

All of the attacks exploit the human tendency to trust certain brands, logos and other trust indicators. These attacks often ironically exploit a widespread sense that the Internet is unsafe and that users must take active steps to protect their financial accounts and passwords. The similarity between phishing attacks, which claim that users must update passwords, account activity, etc., and legitimate security requests adds verisimilitude to phishing attacks.

The efficacy of phishing attacks is diminished when users cannot reliably distinguish and verify authoritative security indicators. Unfortunately, browser and related application programs have not been carefully designed with security usability in mind (Dhamija et al., 2005).
3.3.6.1 Use of alternate encoding schemes

Users cannot reliably parse domain names. Often they are fooled by the syntax of a
domain name through type jacking attacks, which substitute letters that may go
unnoticed (e.g. www.lmn.com, www.1mn.com, www.imn.com), or when numerical IP
addresses are used instead of text. The semantics of a domain name can also confuse
users. (e.g., users can mistake www.amazon- members-security.com as belonging to
www. amazon.com). Legitimate organizations heighten this confusion by using non-
standard naming strategies themselves (e.g., Citibank legitimately uses c i t i . c o m ,
citicard.com and accountonline.com). Phishers have also exploited browser
vulnerabilities to spoof domain names, for example by taking advantage of non-printing
characters and non- ASCII Unicode characters.

3.3.6.2 International Domain Names (IDN) Abuse

IDNA is a mechanism by which domain names with Unicode characters can be
supported in the ASCII format used by the existing DNS infrastructure. IDNA uses an
encoding syntax to represent Unicode characters in ASCII format. A web browser that
supports IDNA would interpret this syntax to display the Unicode characters when
appropriate. Users of web browsers that support IDNA could be susceptible to phishing
via homograph attacks, where an attacker could register a domain that contains a
Unicode character that appears identical to an ASCII character in a legitimate site (for
example, a site containing the word bank that uses the Cyrillic character a instead of
the ASCII a) (Gabrilovich et al., 2015).

3.3.7 Events Used by Phishers to Lure

The natural disaster like earthquake, flood etc. will drive fraudsters. At the cause of a
natural disaster, the phishers conduct phishing scheme. After the tragic natural disaster,
relief efforts will pour into the affected nation or area from all over the world or
countries. The phisher may allegedly sell the phishing sites to would-be scammers or
he might conduct the attack himself.

Spammers ask individuals to make donation for charity. When donation is sent, the
money is transferred to an offshore bank account. Spammers pretend to be UNICEF,
Red-Cross etc. The fraudulent web sites that are allegedly created may mimics sites of these organizations.

Spammers take advantage of a tragedy happening to deliver malware. Upon clicking on the link to view a video, users download a Trojan.

The phishers may use Sports events like Olympics, Soccer, Cricket & Tennis tournaments etc. to spread attacks. Spammers use the seasons like Valentine's Day, festivals like Deepavali, Christmas to send various types of offer product spam and malware.

3.3.8 Phishers strategies of attacks [Example of Phishing Attack]

3.3.8.1 A Fake Fast Food (Chain of Restaurant like KFC, McDonald) Survey

The phishing attack against a major fast food brand was carried out through spam mails requesting customer answers for a bogus satisfaction survey. The fast food brand is one of the most popular worldwide, so fraudsters sent the spam globally. The spam email states that the brand is planning major changes to their chain of restaurants to improve their quality of service. The mail further states that to implement these changes, customer opinion is required by means of a survey (which is of course fake). Fraudsters try to trick customers by claiming a reward for those who participate in this survey. The spam email contains a link that leads to the phishing website containing the fake survey, the phishing website claims to provide a financial reward for the customer taking part in a quick, 8 question surveys. Upon completing the survey, the Web page is redirected to a fake user authentication page that asks for sensitive information such as credit card number and pin number so as to supposedly credit the bogus reward to the customer’s fast food account. The phishers claims to credit the reward within 3 business days after user authentication and will reflect on the customer’s account history.

3.3.8.2 Android

Android. Opfake- Attackers continue to target the Android operating system. In particular, it appears as though the attackers continue to look for new ways to expose their malicious apps through the Google Play marketplace; for example, some threats, but only a small portion of the app comprises the actual game; the rest of the app is a
Trojan called Android.Fakeapp. Any app that is ostensibly harmless, but contains some hidden code that can expose the user to further risks and reveal personal information without their knowledge, may be considered a Trojan.

3.3.8.3 Phishing Attacks Targeting Two-factor Authentication

To validate online banking transactions in real time, many banks around the world deploy SMS-based one-time passwords that are sent to a customer’s mobile phone via a SMS text message. The cybercriminals, attempts to bypass this authentication measure.

Phishing attacks targeting financial institutions in more than one geography asked consumers to enter their regular online banking credentials (usernames and passwords). The next page of the attack prompted consumers to enter the OTP sent to their phone via text message.

This type of attack suggests that cybercriminals receive these credentials and attempt to utilize them to login in to victims’ accounts in real-time to perform online transfers to mule accounts as soon as they receive the one-time-password.

Unlike classic phishing attacks, where users’ credentials are harvested and utilized at a later time, these attacks, which can be dubbed “Man or Human-in-the-middle” phishing attacks, rely on the use of consumers’ one-time passwords by cybercriminals.
3.3.8.4 Alert for phishing site from RBI

**Figure - 3.7: Alert for Phishing Site from RBI**

RBI warned that mails are being sent in its name “inviting bank customers to update their bank account details”. It clarified that it has not sent any such. The RBI or any bank never issues / sends communication to the public / their customers asking for the sensitive details like bank account, credit card, net banking, ATM card etc.

3.3.8.5 **Worm affecting the Centralised Instrumentation System in an Industry**

The various versions of Stuxnet worms based on a different programming platform like, Tiled platform, are designed at attacking the Siemens instrumentation systems, aiming at taking control of valves attached to centrifuges systems, opening and closing the valves at intervals, compromising the integrity of the system as a whole. It works by fingerprinting target computers to determine if it is in the right location before activating the payload. It also collects instrument readings when the centrifuges are running as normal and, when it is making its attack, displays those readings to the controllers in order to mask its activities. The worms’ method of replication is through infection of Siemens Step 7 project files. When a flash drive is inserted in an infected drive, Stuxnet worms will affect any Step 7 project archives with .s7p or .zip file name extensions on the drive. The worm is also sought to disrupt the operation of frequency converters used to control the speed of the centrifuges.
3.3.9 Automated Phishing Toolkits

This particular toolkit attack is most likely related to a specific Command & Control server being reactivated. These attacks play a significant part in populating and updating under-ground economy servers with stolen personal data; marketed in the maturing underground economy. The primary objective of those who operate in these activities is - money. A technique used in phishing scams is targeting the Income Tax Departments at the closing of the financial year. The phishing scam was technically very nifty as it asked the intended victims to supply details and print the form. The completed form was to be sent to the mailing address to process the tax refund. If someone completed the form and clicked on the Print button, what actually happened was the confidential information was sent to a server utilizing the fraud domain.

3.4 Why Phishing works? Or why do users fall for phishing attacks

Dhamija et al., (2005) focused on why phishing works. The researchers conducted a laboratory experiment with 22 participants by showing them screen shots of 20 web sites and asked them to identify the fraudulent website and also asked them the reasons for why the subjects identified the websites as fraudulent. A good phishing website will be able to fool 90% of the participants and more noteworthy no significant correlation was found between education, age, sex, previous experience, hours of computer use and the susceptibility to phishing. Majority of users ignore pop warning about self-signed certificate, proving this type of warnings ineffective (Dhamija et al., 2005).

The phishing effort involves less cost and technology. Further, phishers may reside in across the globe out of reach of victim’s jurisdiction placing authorities to prosecute much more difficult.