Preventive Techniques of Phishing Attacks in Networks

Muhammad Adil

MS (CS) Computer Networks
Virtual University Lahore, Pakistan
Computer science Department (Networking)

Abstract:

Today internet technology is the most widely used technology in the world; they are embedded in everyday life as a primary element. Due to its extensive use in the current era of internet, it is involves social media applications, online businesses applications, online advertisement websites, online bank applications, online hunting websites, online doctor appointment and online doctor opinion. This all can makes things easy and accessible for human being in limited time, but in the other direction this can also vulnerable as like it is beneficial because of their many types of security treats. Security threats to the network, online application, and end user of networks is increasing continuously. One of the most vital and severe threat is Phishing attack. Phishing attack is used for many years as common type of attack by attacker to usurp network security. Phishing attacks includes many types of attacks, in which, the intruder use fake E-mails, fake websites, fake application to convince the end user and steal their credentials or usurp their security. This paper overview a brief history of different types of phishing attacks with background knowledge of Phishing. The solution proposed in this paper to detect and prevent Phishing attacks is the installation of IDS and IPS in the network to allow only authentic traffic in the network, with addition of end user awareness and education campaign to mitigate these attacks.

Keywords

Network Security, Information security, Malware, Phishing, Spam, Social engineering, and machine learning, Anti-Phishing.

1. Introduction:

Phishing is a process of extracting passwords or personal credential of end users or network administrator password as discussed in article [1], Phishing is basically a social engineering, which is used in internet to convince the client/end users and steal their personal information in order to misuse this for different purposes. The concept of phishing is closely interrelated to the traditional "fishing" because this is adopted from the fisher troller technique. In traditional fishing, the fish troller use bait to caught fish in the rivers. Similarly in "Phishing attacks", the intruder uses some methods in networking and communication environment to convince the end user to expose their personal credentials and hijack the security (by means of fake E-mail, fake website, fake links IP spoofing and MAC address spoofing, etc. Phishing attack is an example of social engineering techniques used by intruders to convince the end users to do something against the network security to hijack the network. The intruders in Phishing attacks send fake mails to end users and pretend the information contained in E-mail as legitimate information as like actual site with a small change to convince the end user or use hyperlink embedded Emails to redirecting the victim user toward malicious Website to do something against the security policy of organization to expose their credentials to intruders. The growth of Phishing attacks increase day by day in the fast internet world (Internetworking). The observation made toward the growth rate of such kind of attacks, as it starts in the initial stage are found with the gradually increase time by time.

The current state of phishing attacks recently observed in world showed a continuous increase in it growth rate, due to extensive use of internet technology in real life activities. Phishing attacks also can be made through social engineering. One of the most interesting Phishing attack example are made in March, 2016, to hack the account of John Podesta, chairmen of presidential election campaign of Hillary Clinton [1]. John Podesta received a Phishing mail from hacker in which he was directed through social engineering to open the attachment by means of hyperlink URL. This URL was not link to secure to Google web page like (https) after that he was asked to change his password immediately. Once he changed the password of his account, the current credential of his account was exposed to hacker. This was a simple example of Phishing attack, in which John Podesta was convinced through social engineering to hack his account. The Phishing attacks report released by Wombat security in

Manuscript received August 5, 2025
Manuscript revised August 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.8.19

the 2018 [2]; The Data Breach Investigation Report (DBIR) of Verizon enterprise released by Wombat security with the analysis of 67 contributing organization. The report collect data from the contributing organization found 53,000 incidents and 2,216 confirmed breaches. DBIR report emphasis on the importance of end users education, because the organization is most likely to be attack by social engineering, rather than actual vulnerability. The another report released by **Poofpoint.com** (Next generation cyber security) in the first quarter of 2018 showed a 20% increase in phishing attacks as compared to 2017. The proofpoint security experts found that 40% of organization targeted by fake Email. They received 10 to 50 fake emails on daily bases [3]. The 2016 report of proofpoint showed ransomware (banking Trojans) as a top malware in email. The second quarter report Aug, 2018 of proofpoint.com (Next generation cyber security) has showed 36% increase in that of first quarter report of 2018. Furthermore, the report shows the average customers compromised email in business in second quarter of 2018, and the rate is increased about 35%. The current report represent 26% increase over 2018 first quarter report and 87% increase over 2017 last report [4]. The experts of proofpoint detect a 30% increase in phishing link on social media. The latest report of phishing attacks shows a continuous increase in Phishing attacks as compare to 2016 and 2017. The **Infosec security professional or IT expert's** analysis different organization for phishing attacks; they felt that the phishing threat generally found in 2016 was less in percentage with current state of phishing attacks shown in recent reports. The report released by infosec security professional with wombat security organization showed the most impacted areas of phishing attacks in 2016/17 [8].

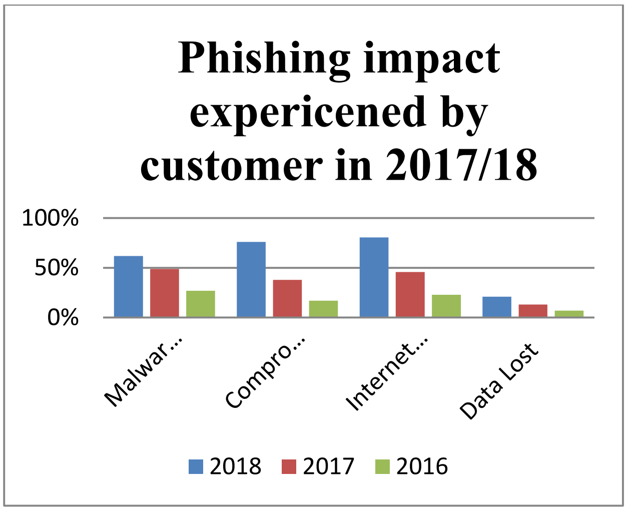


Figure: 1. Wombat Security's State of the Phish™ Report 2018

Furthermore, this paper emphasis on the question of phishing attacks, with victim vulnerability factor (computer user), to analyze the collection of current research studies to understand the vulnerability of victim falling in phishing attacks. The solution of such kind of security vulnerability factor is mostly based on the user based design, rather than technology based design, because to understand the weakness of phishing victim to improve the security against it and minimize the susceptibility of phishing attacks. The rest of paper is organized as follow. **Section II** of the paper describes the related work. **Section III** of the paper contained with proposed solution method. **Section IV** analyzes the experiment result. **Section V** concludes the discussion.

II Related work:

Phishing attacks are increasing, due to online business, E-commerce website and financial transaction in the recent years. The new techniques Phishing used by intruder to convince the computer user/victim are like spear Phishing, Pharming Phishing, Tax scammer's phishing, Iterative campaigns phishing, Sextortion scammer's phishing, Malicious email, Deceptive Phishing and Zero day phishing attacks. Zero day phishing attack are E-mails they contained malware. The latest type of **ransomware** (Malware) name Wanarcry (WanaCypt0r or WanaDecyrpt0r) was first reported in 12 May, 2017. The zero day attack increase due to its success explosion rate in 2018 as compare to 2016/17 according to report of [20].

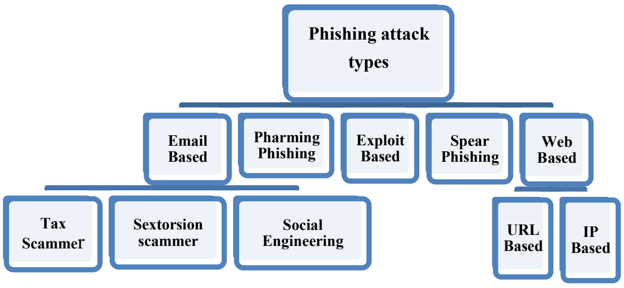


Fig. 2 represents the overview of phishing attacks.

Phishing attacks can also be made through hyperlink of websites by excluding real web server address with small changes to direct the victims toward fake websites. The paper in this section describes the effective phishing attacks methods.

2.1 Spear Phishing: Spear Phishing attacks are used to target a specific user or organization, rather than a number of users and organization. This technique uses an E-mail spoofing attack (from trusted source) to target the specific user or organization to convince, and get access to the organization information.

2.2 Pharming Phishing: Pharming Phishing attack is very difficult to detect, because the intruder inject fake information to organization server (DNS) to redirect the users to fraudulent website. The fraudulent information is very similar to organization legitimate information to convince the end user.

2.3 Tax scammer's phishing attacks: The tax scammer phishing attacks were the latest attacks used by intruder in North Carolina, Illinois and New Jersey. The internal revenue service (IRS) warned the entire tax professional after detecting such attacks through Barkly (Barkly blog) [5]. The intruder pretend themselves as the state accounting professional, send fake email to the tax holder to disclose their account information and credential, after stealing their personal information or account credential they used it for fraudulent tax return.

2.4 Iterative campaigns phishing attacks with shortcut and web query files: This type of attacks was used by intruder specifically for window 10 users to send them email contain on .SettingContent-ms file. This file runs the command which is restricted by window 10. The **Proofpoint** first time detect this campaign of phishing attacks in July, 2018 and called TA505, which send thousands of attacks email to victims [18].

2.5 Sextortion scammer's phishing attacks: The sex scammer phishing type attacks the intruder sent email to the victim user's and asked them, that they have the recipients recordings of watching porn videos. The intruder uses the breach of password at some stage by convincing the victim to get their password by means of key logger. The victim users of this type phishing attack observed by a security expert on 21, July 2018 report released by **Barkly blog** showed an increase compare to 2016/17. The attacker made $500,000 is trice of that last year outbreak WannaCry ransomware (malware) showed in his report [5].

2.6 Deceptive Phishing: The Deceptive Phishing attack is simple type of phishing attack. The intruder sent Email to customer with a claim of legitimate organization Email and asks the customer to verify your account, re-enter your information or make a payment. The object of this type of attacks is to obtain detail bank account information of victim customer. The success rate of deceptive Phishing attacks depends on how efficiently the intruder resembles the fake mail to the bank official correspondence.

2.7 Zero day phishing attacks: Zero day phishing attack is an exploiting vulnerability used by intruder now days. Zero day attack is one of the effective tool used attacker, because the zero day attack data is not available until the attack is detected. These types of attacks are also used as targeted attacks as the article [13] showed. The Symantec Research Lab showed in article [5] that 18 identified vulnerabilities exploited before their discloser in the wild, 11 of them were new to employer from that of first zero day attack.

3 Proposed Solution Methods:

Phishing attacks can be combated by several technologies, they are categorized as:

1 Detecting phishing attacks
2 Preventing Phishing attacks
3 Victims awareness/education
4 Anti-Phishing server
5 Web server security toolbar
6 Anti-Phishing honey pots

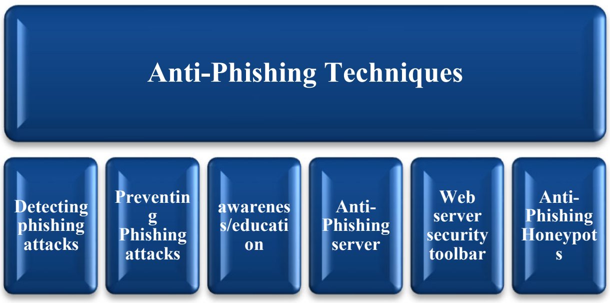


Fig.2 Represent the overview of anti-Phishing technique proposed for solution of phishing attacks

3.1 Detecting Phishing attacks: The attackers use some skillful method to reach the target victims via emails and websites. Detecting is the method that identifies malicious sites and email contain malicious attachment, some browser has the self defense feature against such kind of attacks by detecting and reporting them to an administrator. This type of detecting method is work on the active indicator, to report malicious traffic in real time. The passive indicator on the other hand doesn't interrupt the user current task to report such kind of malicious traffic immediately to network administrator or organization IT expert team to take an appropriate action against it as discussed in article [5]. Passive indicator is not more effective, because the user most of the time ignore or simple notice it. Active indicator is more effective in detecting malicious activities to acknowledge the end user about malicious site, and also take an appropriate action accordingly. Example of this includes Intrusion Detection Systems (IDS) devices, tool and software, which is used to detect malicious activity in the network, websites and servers. IDS detect malicious site, websites and traffic as based on their installation and configuration. IDS has different types like, **Host based IDS (HIDS)** and **Network Based IDS (NIDS)**. Network base IDS used on router side with configuration to filter all traffic go through (IN/OUT) the network. The NIDS stop the traffic of websites, Email server and DNS server by means of Brand monitoring, Behavior detection, security authentication and security events monitoring after matching it with its configuration, if found more than the device threshold level configuration. Furthermore, network based IDS are more effective and less expensive to use for large organization. **Host based IDS** is another effective way to detect, stop and restrict the malicious activity on a specific host server as per their configuration like to restrict Email by email analysis, websites by blacklist websites, and similarity of layout by comparing. Host based IDS are expensive, but more effective to protect individual server or host from Phishing attacks.

3.2 Preventing Phishing attack: Preventive phishing has great importance in phishing attacks, because this method not only detects malicious websites and Email server but blocks the sites containing malicious information and report them [5, 19]. Preventive phishing first carried a verification of the sites before authorization, through machine learning. Where they match and compare the traffic (IN/OUT) with their configuration (with profile, Signature match) allow legitimate information to pass through and restrict the information, website, Email servers they are matched, which has greater threshold value. IPS has the ability to detect and stop the traffic they are matched with their profile, signature and blacklist sites in grater threshold value [9]. Phishing filter is another anti-Phishing preventive technique used to monitor malicious site by filtering the traffic (IN/OUT) of the network according to article [6, 21]. Preventive Phishing is also use URL with an IP address, attributes, domain name, and link text to check against each mail received, with internal configuration to detect malicious websites, Email server, if the match found the similarity index greater than of its internal configuration they stop them, log file and report them. IPS (Intrusion Prevention Systems) is the tools, devices, application and software, which is used to detect and prevent malicious activity in the network, Mail server and websites [9].

3.3 Victims awareness/education: The awareness campaign can also play very important role to avoid phishing attacks. The current awareness and education against phishing attacks are broad, but not more effective by keeping in view the advance phishing attacks in mind, so to make it more effective; the user day to day awareness campaign may be launched to understand the victims user by reading **relevant** material regarding phishing mail server, fake Email and websites to protect against it [7]. The researchers still working hard to familiarize the victim users with anti-phishing methodology like games they are embedded in the server. The example of game phishing familiarization is the Anti-Phishing Phil' which means teach and help the user to indentify malicious URL and other phishing scams [19]. The embedded training is another technique used as Anti-phishing, because it sends mock phishing mail to user to aware them and also to teach them how to avoid phish attacks. The example of this techniques highlights that some mock mail are sent to users, and they were asked to open these attached mail, once they open these phishing contained Email, they were shown with message that the link is contained with fake website or malicious information. Mock phishing awareness campaign also increases end user knowledge to protect against phishing attacks.

3.4 Anti-Phishing Client/Server based: Anti-Phishing host based and server based defense techniques can minimize phishing attacks due to its rigid protection nature. Anti-Phishing server is the external plug-in application software to the browser, that are very effective in information flows based solution, blacklist, and similarity layout phishing attacks as shown in article [10, 11]. Once the anti-Phishing server is installed in the browser, the browser makes a request for username and password to new user. The password of user is stored and encrypted with DES standard in the browser. This type of anti-Phishing technique work very efficiently to protect the victim users, because once they enter to malicious site, mail server or un-trusted site on a browser a warning alert is made, before sharing or sending any information on the victim display. Anti-Phishing server also plays important role to protect victims with similarity layout. Anti-Phishing server of similarity layout used to compare the "visual" similarity index of web page, if they are larger in number of threshold level mentioned in anti-Phishing server, the phishing web page (Phishing web page is page if the similarity of web page is greater than that of legitimate web page) report as malicious website and warn the end user [12]. Document object model (DOM) is also used as an anti-Phishing in similarity layout to protect the victim users.

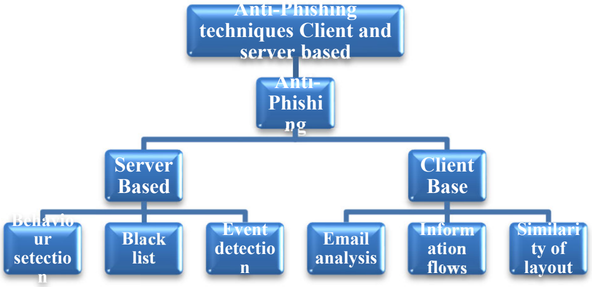


Fig.3 Represent Anti-Phishing technique used in client and server based

3.5 Web server security toolbar: Web server based security toolbar defense includes protecting of victims through SSL (Secure socket layer) and TLS (Transport Layer Security) protocol, because most of the server and web browser support SSL and TLS [12]. SSL (Secure socket layer) and TLS (Transport Layer Security) both use advance public key cryptographic protocol. The operation of TLS and SSL is based on the handshake, where authentication between user and server is made through a handshake.

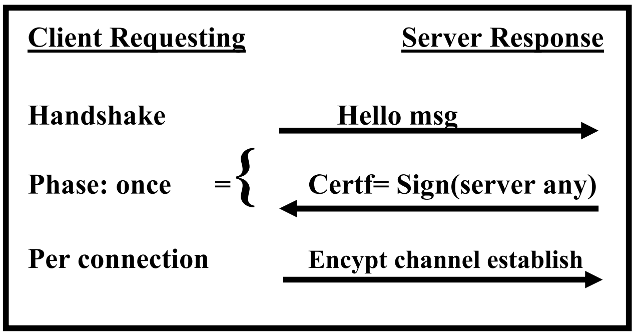


Fig. 4, Shows a simple Handshake authentication between user and Bank server.

After the authentication or handshake, when a secure channel establish between client and server, the data transfer between client and Server took place in the following manner.

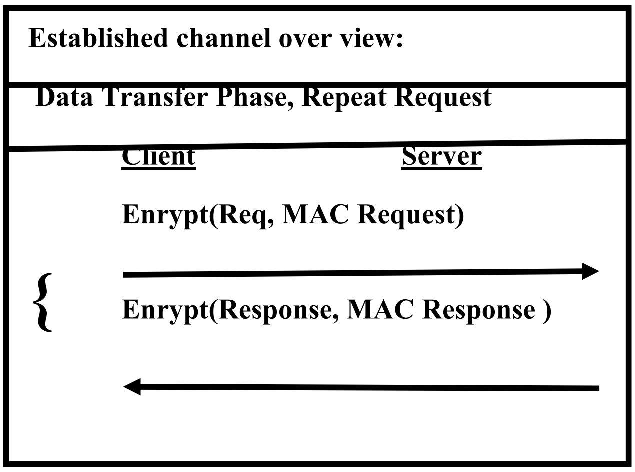

Established channel over view:
Data Transfer Phase, Repeat Request
Client
Server
Enrypt(Req, MAC Request)
Enrypt(Response, MAC Response)

Fig. 5, Shows a simple data transfer mechanism between user and Bank server.

HTTPS and IPSec are other protocols used to protect victims from Phishing attacks [14]. IPSec (Internet Protocol security) use authentication Header (AH) and Encapsulation Security payload (ESP) for authentication and encryption of data. Authentication Header (AH) is used as authentication protocol, while Encapsulation security payload (ESP) used as authenticating and encrypting protocol to provide a secure channel for communication between client and server to achieve authentication, confidentiality and data integrity as discussed in article [14]. Web server security toolkit is also very efficient against Pharming Phishing, because it also encourage the end user/customers to login with HTTPS protocol in desired sites to protect their login credentials and avoid phishing attacks.

3.6 Anti-Phishing honeypots: Fig. 6 Simulation diagram represents the Anti-Phishing honeypots, and also a brief over view of anti-phishing honeypots in network.

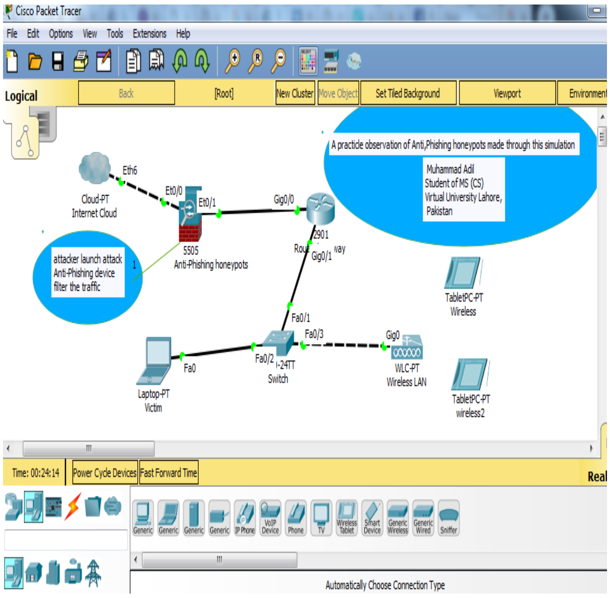


Fig 6, is taken from Packet tracer simulation, while practically observing the case.

Anti-Phishing honeypots is another widely used tool to protect victims from more advance phishing attacks; like Malware and Worm, because they are very effective to detect phishing mail, and report new phishing sites to shutdown, before they are doing something harm to organization. Anti-Phishing honeypots are very effective in E-commerce and financial institutes in current internet technology era, to protect their organization network, server and customer from phishing attacks [15, 16]. Anti-Phishing honeypots also play a vital role investigation (forensic investigation), because it make log of all traffic pass through it, so a very effective tool against phishing attacks to protect end user. There are two types of anti-Phishing honeypots

1- High interaction Honeypots
2- Low Interaction Honeypots

High interaction Honeypots consists of real physical machines. They are currently play very important role in forensic investigation, because they make log file of vulnerability and intruder attacks, which are helpful to reach the intruder in most of cases and caught them. High interaction honeypots are very efficient tool against phishing attacks to protect organization and minimize phishing attacks.

Low interaction honeypot anti-phishing emulate the vulnerability related window protocol like (SMTP, FTP) targeted by malware. Low interaction honeypots are easy to implement, because they use limited resources in virtual machine. Therefore, the research of this paper against Phishing attacks emphasis on to follow Anti-Phishing honeypots to protect organization and end user from phishing attacks.

4. Experiment analysis Results:

The result analysis is made on the base of different techniques adopted as preventive measurement techniques in this research. The IDS and IPS equipment are installed in Cisco packet tracer simulation tool as security tool in the network (server and client side with declaration of some websites and IP address, MAC address to detect and block). The analysis result extract from this network showed a clear difference between before the installation of these devices and after installation of these devices. The result is compared on the bases of launched attacks, before and after installation of IDS and IPS (in simulating environment) in %. The attacks launched before the installation of IDS and IPS on the network was through IP spoofing, websites and MAC addresses spoofing to access the network, the result observed from simulation tool showed a compromised network by sending an ICMP ping request from intruder PC via MAC address spoofing and as well as IP spoofing. The same attacks are lunched after installation of IDS and IPD while blocking the same IP address and MAC address in access control list of IDS and IPS are found more effective compare the result after installation of IDS and IPS.

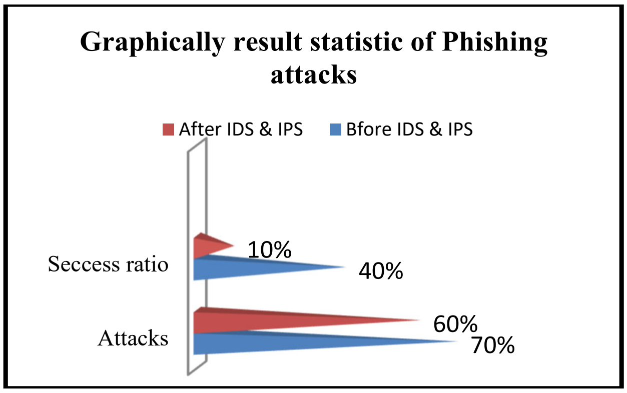


Fig. 7, Shows a Result statistic of Phishing attacks.

The result analysis is observed from simulation tool Cisco packet tracer 7.1.1 as shown in the in the following diagram.

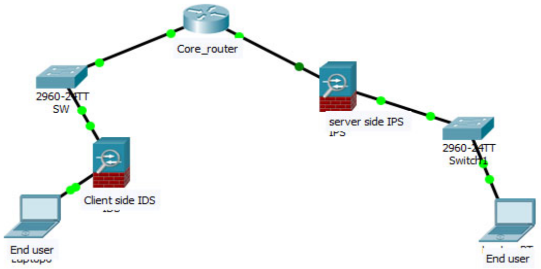
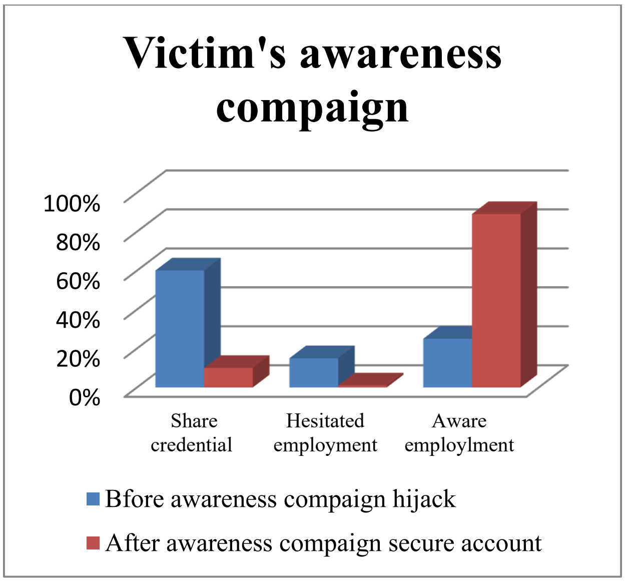


Figure 8 Network diagram with IDS and IPS installation on host side and server side

The other result analysis is made on the base of victim's awareness campaign. The cloth industry organization is chosen for this purpose at (Mardan) to compare the result of social engineering phishing technique. A phone call were made to the employment of different department in the organization and pretended himself as CEO of the organization to ask password of individual computer system in the organization, 60% of the employ share their password without knowing furthermore about CEO at first attempt, 15% were found hesitated to share their credentials and the other 25% employment were found with sufficient knowledge about their trade job and sharing personal credential. The awareness lecture were arranged in the same departments after couple of weeks and understand the basic security threats with the benefits of intranet in an organization or internet in world. The assessment is arranged after two months and the same social engineering technique is used with different idea by pretended himself as bank manager of local branch. The 30% employed were ask to share their account information for the sake of extra salary from organization, only 3% employed shared their credential 1% are hesitated and the rest of people were found with sufficient knowledge. The following graph represents the analysis result.



The comparison is further categorizing on the analysis of different phishing preventive techniques. Table 1 represents the overall comparison analysis of proposed anti-Phishing techniques with their effectiveness ratio on different types of phishing attacks.

Table 1: Comparison Analysis

Technique Name		Description	Advantage	Limitation
Computer based training		Tool, application software and system	This type of training is easy and accurate	Very expensive, limited by lack of system knowledge
Tool to filter		Anti-Phishing tools such as Microsoft filter and web senser	They can block malicious sites	Very expensive tool, Not very efficient for internal attackers and lack hum knowledge
Human base		Awareness campaign	Minimize attacks up to great extent by educating end user with phishing attacks types and harming	Trust tendency, Relative human decision, greed and with emotional human influence
Scanning and alerting software		Anti-scams Anti-virus, and Anti-Spams	Scanning the websites efficiently, alert about harm efficiently and act as strong security product	The ignored alter by human and expensive product.

The table analysis represents the effectiveness of Anti-Phishing techniques discussed in the paper as Anti-phishing with real world observation made from environment.

5. Conclusion:

The Phishing attacks were start from 90,s to steal personal information, credential information, credit card information, and online transaction credential of victim users. The solutions proposed in this paper are to overcome different types of phishing attacks. The paper emphasis on the end user protection as discussed in the research by following anti-phishing techniques to avoid phishing attacks. Likewise, the intruder always comes with new attacks to bypass the existing one. We have also discusses some phishing attacks made through social engineering like e-commerce, financial transactions and fake mails etc. Social engineering Phishing always use more efficient way to convince the victims. The paper proposed a solution to install IDS and IPS in the network, and also launch awareness/education campaign for end users of the organization employ to deny social engineering phishing attacks. Internet technology is one of the prepared media used by attacker in phishing attacks, which basically affect the impressive structure of organization like e-commerce, online shopping, online banking and other online businesses. These attacks can be avoided by the uses of detecting phishing attacks devices, tools, application and software. The survey of this paper will help users to understand the history and techniques Phishing attacks used by intruder, with latest solutions conferred in the paper to prevent these attacks, and provide safeguard to end users and organizations.

Manuscript received August 5, 2025
Manuscript revised August 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.8.19

References:

1. The Honeynet Project Research Alliance, “Know Your Enemy:Phishing – Beyond the Scenes of Phishing Attacks,” 2005.
2. Krieg, G.andKopan, T. 2016. CNN News, Is this the email that hacked John Podesta's account?, Available at:h ttp://edition.cnn.com/2016/10/28/politics/phishing-email-hack-john-podesta-hillary-clinton-wikileaks/ >, (Accessed 19 November 2016).
3. Wombat (2018). *State of the Phish*. Available online at : https://info.wombatsecurity.com/state-of-the-phish
4. Proofpoint: Leader in advance cyber security; https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q118-quarterly-threat-report.pdf
5. Proofpoint: Leader in advance cyber security; https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q218-quarterly-threat-report.pdf
6. Barkly blog ::https://blog.barkly.com/phishing-attacks-campaigns-2018
7. J. S. Downs, et al., “Behavioural response to phishing risk,” presented at the Proc. anti-phishing working groups 2nd annual eCrime researchers summit, ACM Conf, Pittsburgh, Pennsylvania, 2007, pp. 37-44.
8. P Kumaraguru, Y Ree, A Aquisti, LF Cranor, J Hong‘ Pro tecting People from Phishing: the design and evaluation of an embedded training email system’ Proceedings of the SIGCHI conference on Human Factors in Computing Systems, ACM (2007), pp. 905-914
9. tripwire.com security organization https://www.tripwire.com/state-of-security/security-data-protection/three-quarters-organizations-experienced-phishing-attacks-2017-report-uncovers/
10. Gunter Ollman. The Phishing Guide - Under-standing and Preventing Phishing Attacks. WhitePaper, Next Generation Security Software Ltd.,2004.
11. Engin Kirda and Christopher Krueger to “protecting user against Phishing attacks” The computer journal 2006.
12. Angelo P.E Rosiello, Engin Kirda, Christopher Krueger, and Fabrizio Ferrandi “A layout simililarity-based-approach for detecting Phishing pages” IEEE International conference on security and privacy in communication network. France, 2007
13. Christian Ludl, Sean McAllister, Engin Kirda and Christopher Krueger “On effectivenessof techniques to Detect Phishing sites”. Detection of intrusion and Malware and vulnerability Assessment (DIMVA) 2007 conference, Lucerne Switzerland, July 2007
14. [13] Dierks T, Rescorla E. The transport layer security {(TLS)} protocol version 1.1, internet request for comment (RFC) number 4346; April 2006
15. [14] N. Ferguson and B. Schneier, “A cryptographic evaluation of IPsec.” Unpublished

manuscript available from http://www.schneier.com/paper-ipsec.html, Feb. 1999.
16. S. Chauhan, S. Shiwani, A honeypots based anti-phishing framework, in *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)* (IEEE, 2014), pp. 618–625G
17. H. Ulusoy, M. Kantarcioglu, B. Thuraisingham, L. Khan, Honeypot based unauthorized data access detection in mapreduce systems, in *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)* (IEEE, 2015), pp. 126–131
18. https://www.wombatsecurity.com/blog/phishing-pretexting-and-data-breaches-verizons-2018-dbir
19. J. Chen and C. Guo, "Online detection and prevention of phishing attacks," in in Proc. Fifth Mexican International Conference in Computer Science, IEEE Conf, 2006, pp. 1-7.
20. Gunter Ollmann, "The Phishing Guide - Understanding & Preventing Phishing Attacks," IBM Internet Security Systems, 2004.
21. Black stratus security organization report; https://www.blackstratus.com/ultimate-guide-zero-day-attacks/
22. M. Jakobsson'Modelling and Preventing Phishing Attacks' Financial Cryptography, 5 (2005)

Muhammad Adil received his BS(CS) degree in computer science and MS(CS) degrees in Computer Networks form Virtual University of Pakistan, Lahore in 2016 and 2019, respectively. During 2011 to 2015, he stayed in Pakistan telecommunication Pvt, Limited (PTCL) to work on Meridian Exchange with addition of MSAG. He also worked on Satcom and different Radio equipment such as big transmitters, Receivers, Antennas, Cisco switches and Routers.