ISSN 2047-3338

Eradicating Cybercrime Through Education, Awareness Raising and Outreach

Hermain Zahra[1], Rafia Nawaz[2], M. Junaid Arshad[3]
[1,2,3]Department of Computer Sciences, University of Engineering and Technology, Lahore, Pakistan
[1]hermainsheikh73@gmail.com, [2]rafianawaz216@gmail.com

***Abstract*– Computer technology services did not come out without pitfalls. Although it makes life too quick and easy, however shoved under the eclipse of risk from the deadliest type of crime named 'Cybercrime', without machines whole industries and multiple activities would almost cease to work. This proliferation of cheap, powerful, user-friendly computers has made it possible for more and more people to use them as part of their normal way of life. The abundance of inexpensive, strong, user-friendly computers has made it possible for more and more people to use them as part of their normal way of life. As businesses, organizations, and people continue to rely more and more on them, so do the hackers. Restricting cybercrimes relies on proper analysis of their actions and awareness of their impacts through all levels of society. Hence, this work explains purposeful knowledge of cybercrimes, how they attack, preventions and their effects with future cybercrime trends over various areas.**

***Keywords*— Cybercrime, Phishing Attacks, Prevention and User Education**

I. INTRODUCTION

CYBER-CRIME is a terminology commonly used to describe crimes, in which devices or networks are a resource, a subject or a medium on which illicit activity takes place. This also includes typical crimes used to permit unauthorized travel via PCs or devices.

Cyberspace-based businesses are rapidly becoming a question of corporate security in today's globe. The network of various organizations in cyberspace is intertwined, which is why the challenge to safety has risen significantly. There is an increasing vulnerability of cyber security. University and college computer systems have become targets because they hold the same information as banks. This involves the usage of computers, the Network, cyberspace and the World Wide Web, as well as crime [1]. Cyber attackers are through and clients are being threatened by public and personal businesses.

Due to cyber-security constraints, cybercrimes are rising. The computer and the human behind it are the perpetrators of cyber criminals. Cybercrime may entail something like the purchase of illicit content or rob several dollars from online Bank accounts. Cybercrime may also be used by programmers named viruses to create and distribute tiny or big programs on certain computers, or to upload accurate company details on websites on hurt citizens. One significant type of cybercrime is hacking, wherein hackers use the network to steal away sensitive details from other people. Taking into account, an example of cybercrime, through 2012, the South Carolina Revenue Office held an exercise that demonstrates this cybercrime. Within the database infrastructure of that organization cyber attackers hacked into and stole 3.6 million numbers for social protection and 387,000 credits / debit card numbers, such as key loggers that monitor key strokes, passwords and other private details, should cyber criminals hack the device and install malware. They may progressively use your login credentials to access utilities and pages. If these attackers extract your password, they will offline breach your account. Those criminals are always everywhere and ought to be prepared to transfer your assets. Currently on over 61% of the industry are rendered to the internet, which is why premium quality protection is needed in this region for direct and successful exchanges [2]. This has rendered cyber security a recent problem [3].

Establishing the Internet safer (and protecting Internet user) has become vital just as a procedural approach for enhancing new management [4]. A comprehensive and more reliable response to cybercrime has to be pursued. Cyber security affects the vulnerabilities generated through and around this modern environment, as well as policies and procedures to ensure it [5]. Cybercrimes pose an existential threat to e-commerce and there is an immediate need to effectively control its production. Because law enforcement agencies ' relevant legislation and capabilities do not match the rapidly changing nature of crimes, businesses need to adopt innovative preventive strategies [6]. The present study has been undertaken to connect a few angles, impact and prospects of this digital innovation with unique reference to risk stances of cybercrimes.

Attempts have been made to evaluate the regulatory framew ork that would be necessary for its regulation. Protecting your self digitally is hard when you don't know where to begin. If you don't know where to start you can hardly defend yourself online. More and more experienced cyber criminals manipulate both the vulnerable passwords and the trustworthy human nature. So, knowing about the different sort of cybercrimes and its

preventions is necessary to protect yourselves, systems and organizations.

The paper includes cyber security and cybercrime information. Some examples related to cyber security from different surveys are illustrated. The paper provides an analysis for the importance of user awareness regarding cyber security. By taking in consideration a type of cyber-attack, it is analyzed that user awareness is necessary for the prevention of cyber-crime.

II. LITERATURE REVIEW

With the world's growing day to day digital revolution, cybercrimes are rising worldwide at quite a concerning pace Cyber-crime development occurs in tandem with internet growth. Anything on the Internet is a potential target for cybercrime. Sooner or later, any modern invention or computer would become the object of cybercrime. Digital world drawback triggers discontent between individuals. And now more than ever consumers are more concerned with the protection of their results.

Data reveals that various college and university students are conscious of the extent of cybercrime. They described and evaluated the consciousness among college students about different government initiatives to counter cybercrimes. It was found that the different safety measures required by the users to tackle and mitigate cyber criminals have to be established. They have come across so many cybercrime reports that even people are aware of cybercrime. Their survey shows that, as compared to other types, the exposure of interviewees regarding hacking is high. In their research, it was found that there is a substantial gap between Internet users and their knowledge of cybercrimes [7].

Another paper addressed cybercrime and cyber law, discussing a broad variety of subjects, such as internet accessibility, computer protection, computer privacy, open access and usage of the Web and freedom of speech. They related to it as cloud regulation. Their research emphasizes how cybercrime is spread amongst the common people and their reduced knowledge of this problem. Their research reveals various explanations why cyber-attacks have been committed and that protective precautions should be taken. They said that if anybody runs under cyber assault, please come forward and report a case [8].

Researchers analyze the number of various cyber threats worldwide. His paper therefore describes the world's cyber threats and their mechanisms for prevention. He identified cybercrime mitigation approaches so far and shows the cyber-threat analysis and cyber-threat prognostics in the next few years in his study. He observed that cybercrime will increase and be impossible to avoid in the coming days. He has come up with an idea that data is relevant these days, as it can be used to make a large amount of money and so there is a need to develop an efficient program that can not only avoid the criminals but also secure the data of the client. Such data will be put with a high degree of privacy and discreet use of strong firewalls by the applications [9]. Work distinguishes well the perception of cybercrime among young people. Throughout education, fundamental values or morality and the correct use of IT methods must be developed. In fact, the media must have sufficient information on cybercrime. With respect to security initiatives to counter cybercrime, young people have an idea which is one of the results of their study [10].

Authors wrote a paper investigating the rise of cybercrimes and assessing policy action to combat cybercrimes in India. The report identified the different categories of crimes reported under the IT Act between 2008 and 2013. Strong ethics and no major convictions relative to the number of cases reported for cybercrime [11].Ten, Liu published an analysis in three stages, framework, situations, and points of access on the effect of cyber-attacks on Supervisory Data Acquisition Systems [12]. They also suggested the methodologies that incorporate cyber systems with firewall and password models and have identified the appropriate preventive measures to evaluate vulnerabilities at the aforementioned levels of SCADA systems.

Ramilli claimed that HTTPS is susceptible to man-in-the-middle (MITM) assaults, on which most bank and e-commerce Web pages rely [13]. Their paper showed that web-app connections secured using HTTPS protocols can be attacked by exploiting certain common properties of LANs in addition to exploiting inexperienced users' common behaviors

Software viruses are very widespread, too. Viruses may be of increasing intensity. They can stop computer networks from working and can spread through e-mails and the internet. Frauds of phishing or metadata are offenses involving luring consumers into situations that seem genuine to obtain information such as contact data, credit card details etc. Another major aspect of cyber-crime is identity theft. This is normally taken lightly because everything shared on the internet is very open to a wide amount of people. The details may quite quickly be misused. Most individuals use other users' identities for their own gain. Criminals may claim to be someone else with your identification and commit illegal activities. Blackmailing on the internet or cyber bullying often rises at a large pace, that cause a lot of harm to target, however, if cyber bullying has no financial implications against the consumer, it impacts people's mental wellbeing.

Now, the presence of cybercrime is very apparent, and it is growing at the same rate that technology is progressing, as more and more dimensions of our lives are being interactive. Today, cybercrime laws aren't quite clear. That has to improve quite fast. Proper legislation should be in effect, cybercrime should be regarded as major offences, and the offenders should be prosecuted appropriately. Because the latest technology is developed every day, the rules of cybercrime can always be versatile, because cyber criminals discover different methods of manipulating the technology every day.

A) Types of cybercrime

Data loss: In 2017, about 780,000 documents a day were lost. Online attackers adjusted easily, according to the McAfee Economic Effect of cybercrime (February 2018). The size of online terrorist behavior is rather shocking. The estimates fear on a monthly or annual scale, let alone hourly! In order to threaten customers, cyber criminals are actively seeking new technology. Payment and transactions to/from

cyber offenders became untraceable since the launch of Bit coin.

Data Privacy: About 24,000 harmful smartphone applications are disabled every day from Symantec's Internet Protection Vulnerability Study information that lifestyle devices are the key targets. Some of such devices are losing phone numbers. Further confidential material, such as position of the computer, is often made available. It will be impractical to track or test for bugs in any of these devices. It's just a free ride for cyber offenders to do their worst.

Through file extensions: Microsoft Office file formats are the most commonly common file extensions. Microsoft Office grabbed the number 1 spot in the top 10 most dangerous software extensions. Email is a growing place for computer criminals to target their victims. Emails are seen around the globe on a regular basis. When you receive an email with an extension of a.doc or.xls format, most people will connect it to Microsoft. Microsoft is a respectable organization ensures that users are more inclined to install an attachment. According to Cisco's 2018 Global Cyber Protection Survey, 38% were Office types.

Password breach: This may feel like passwords are dead, because of cryptography, etc., but according to Cyber Security News, they're not. It is estimated that 300 billion passwords will be used by 2020. It takes human beings and robots into account! That's a lot of codes, many of which require information security protection. If not, that's 300 billion future risks all around the planet.

Fraud: More than 60% of theft comes from handheld apps. The planet has gone virtual, so have the fraudsters. 60 percent of the fraud comes from personal devices; 80 percent of the fraud is from smartphone phones. When cyber criminals gain passwords to your cell phone, they can hack your mobile banking software and launch several forms of cyber-crime. Fraudulent sales are often more than double the size of actual purchases.

Hacking: When hacked, attackers would be able to view sensitive details, passwords and target other computers attached to the same network. Coin search is one of the biggest bits and crypto currency exchanges in Asia. It announced that it had lost $530 million due to hacking in January 2018. As a result of that incident, Coin's check confiscated and then stopped all of its crypto currency sales and withdrawals.

Adware: Throughout the Cisco 2017 Global Cyber Protection Survey, Cisco surveyed 130 organizations. This was noticed that 75% of businesses were influenced by adware. Adware itself is a nuisance, but it can also facilitate further malware attacks. Adware is displayed in the form of commercials. If you are using your computer on or off the Internet, ads will be viewed. Sometimes, if you're attempting to browse the Internet, the results will guide you to other websites or commercial pop-ups to access your personal details.

Encryption: Encryption is a process where a message, information or program is encrypted. Only approved persons may access the encryption. For instance, when encrypted a document may appear entirely unreadable under normal circumstances. It must first be decoded for access to encrypted content. Hackers know how to hide their traces best, of course. Ninety percent use authenticated data to cover up what they do. It's much more challenging for cybercrime because we as consumers have the same standard of security.

Phishing: Phishing is one of the cybercrimes. The process of phishing is an intention to attract internet users to the phishing web site to access Internet users ' personal data, such as usernames and passwords, for logging into the web site. The phishing attacker is called a pheasant. Phisher uses knowledge from internet users for its own gain, for example, to sell the Internet users' stolen identities, reputation and repute [14].

The banking and electronic payment firms are the most targeted on the Phishing platform. The explanation the internet consumer is targeted by phishing is that the phishing website appears close to the official website [15]. Phishing attacks are growing even though several works have been conducted to solve the phishing problem Phishing problem [16].

The Phishing Process: The phishing attack cycle consists of five phases: the preparation of the attack, the design of the attack, the implementation of the attack, Post-attack theft and abuse [17]. Jakobsson and Myers (2006) also split the phishing cycle into simple step-by - step steps in respect to the data flow of a phishing attack. These involve planning attacks, sending a malicious payload through certain dissemination vectors such as a disappointed email, triggering the reaction of the consumer, which may lead to the stolen of his private details, leading users to access his confidential information, compromising information, transmission of knowledge to phisher, consumption and eventually monetary benefit by a fraudulent party.

Based on correlations in terms of the behaviors concerned [18], phishing attacks are experiencing three main phases– preparation, execution, and results exploitation (Fig. 1).

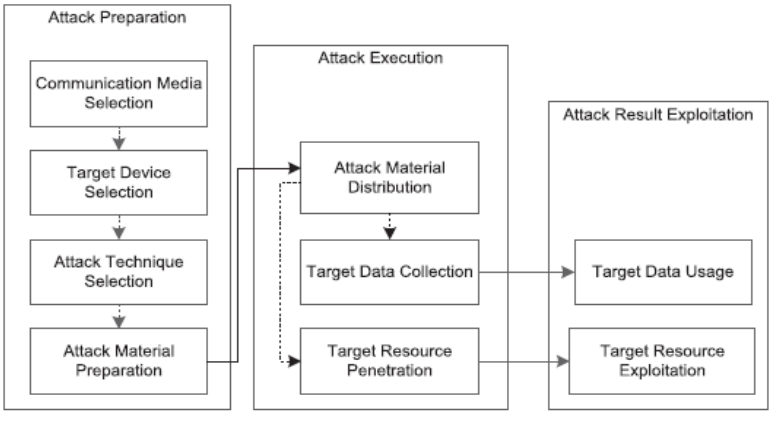

Fig. 1: The Phishing Process

B) Phishing attack techniques

Table I presents some phishing attack techniques:

Table I: Phishing attack techniques

Techniques	Explanation
Spear Phishing [19]-[21]	Spear phishing is an attack tactic targeted for people, organizations and organizations instead of spamming thousands of e-mails randomly to obtain users' passwords or other sensitive and confidential information. Spear phishing is a method of phishing.
HTTPS Phishing [22]	HTTPS Phishing is a phishing attack strategy that conforms in the security behavior to trick users to reveal their sensitive and personal details as legitimate HTTPS link
Man, in the middle (MITM) [23], [24]	MITM attacks are a phenomenon of phishing intrusion in order to eavesdrop or steal communications between the user and the server, place the phenolic in the center of the client and of the legal website. It is achieved by building SSL links between the target intruder and the application.
Tab nabbing attack [25], [26]	The Tab Nabbing Attack is The phisher deprives or abuses the browser tab to persuade the victims of famous sites that the sites are legitimate and that their username and sensitive details are given

Anti-Phishing solutions: To counter phishing attacks there are several devices. The remedies for phishing threats are also classified as anti-phishing. Examples of anti-phishing methods are seen in (Fig. 2). These solutions are basically divided into phishing preventions and phishing detection. Phishing is further categorized in User awareness and software detection. Further, the software detection is sub-categorized into traditional and automated approaches. There are two groups for automated malware tracking, i.e., academic phishing identification and public phishing detection.

C) Phishing Prevention Mechanism

Anti-phishing tools: An anti-phishing toolbar, commonly used as a browser plug-in extension, is an anti-phishing tool, eBay toolbar is an example. The toolbar can also maintain track of all websites that consumers accessed and display an unreadable target message when a user has reached a suspicious URL, so that a user can distinguish between a genuine and fraudulent web page. One other ant phishing tool is Spoof Guard technique used to investigate the authenticity of a web page using an algorithm and calculate the possible attack rates. User warnings are generated when a website with a high chance of spoof is identified [27].

Approaches based on a list: Listing-based strategies may be listed as blacklists and whitelists under two groups. Both solutions to lists are the most relevant collections of phishing threat avoidance strategies today. Blacklists consist of a list of phishing addresses, IP addresses and keywords that have been

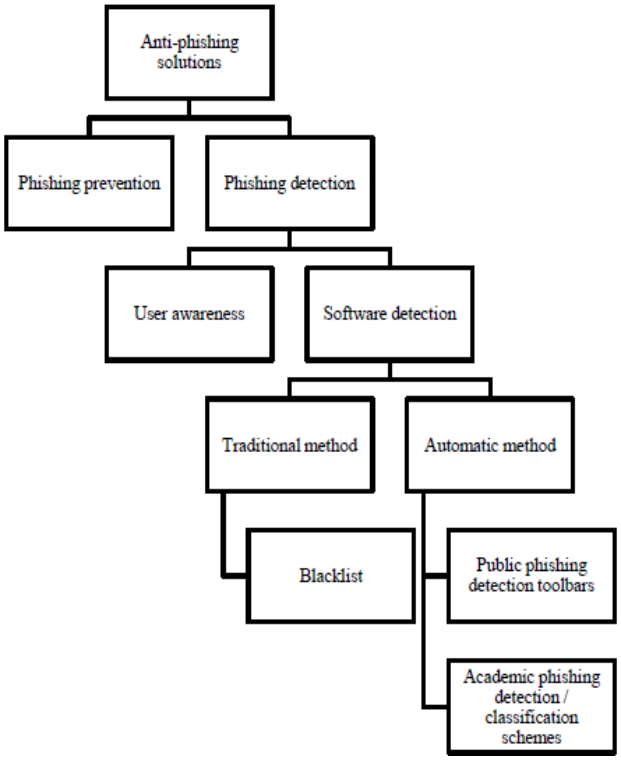

Fig. 2: Anti Phishing Solutions

detected previously and which are often updated to prevent online users from entering these web sites, whereas the white list idea is contrast with the blacklist. A list of legal sites is maintained with a whitelist approach that secures transactions and communication that leads users to access those legitimate sites [28].

Two-Factor Authentication: In order to avoid a phishing threat, phishing protection is implemented by adding an additional layer of authentication as the user logs in to the website. The additional protection layer is a two-way authentication mechanism which confirms the user's identity before the user is allowed access to his or her website login account. Instead of offering only passwords to be recalled by consumers, two-factor authentication includes the authentication users can show their ethnicity by being conscious of knowledge factors and properties. The knowledge factor is the things a user knows, like username and password, while the ownership component is an item the user possesses, like access card, key etc. (OTP) or coding for authentication. For example, a user may enter a password and an OTP provided via SMS text message to authenticate an identity. That will stop an attack on user's account is essential because of extra security, because the user accessing the user's ID and password would struggle. The solution is however not quite secure, since an SMS text is possible, a cyber-criminal may take a message and give it to another telephone number [29].

User Education: In order to prevent phishing attack, user education is essential. Victims were phished mostly because they lack details concerning legal e-mails or websites like identity theft and phishing. Support is necessary from both

policy institutions and non-profit organizations to promote phishing awareness education. Demonstrations could be carried out such as the typical phishing attack techniques and the use of tips to prevent phishing from falling.

User education is important in order to deter phishing attack, because a traditional phishing attack exploits weakness, particularly human curiosity by appealing to the victims on fascinating subjects like unpredictable awards or a lottery with fraudulent links to phishing websites. If users already have the knowledge of phishing, so the risk of falling in the traps created by phishing attackers can be minimized [30].

D) Comparative analysis for the importance of user awareness regarding cyber security

The Table II presents the comparative analysis for the importance of user awareness regarding cyber security such as Objectives, Attributes, Benefits, Drawbacks etc.

III. CONCLUSION

Research has shown that further awareness on the potential risks of cyber threats as well as on the significance of security of information to all target groups is deemed necessary. To overcome the problem of cybercrime effectively, effective preventative strategies must be introduced in all target groups. Therefore, it has been found that continuous training has a significant role in raising all consumers' awareness and promoting prevention techniques in their daily lives. With the help of exploring a kind of cybercrime that is phishing attacks in this paper it is evident that user awareness is necessary for the prevention of such thefts. Both profit and non-profit organizations need to take an initiative to setup awareness campaigns among all types of users' groups to eradicated cybercrime.

Table II: User awareness regarding cyber security

Objectives	User Education	Software Detection		
	On the basis of user knowledge attacks are identified	Blacklist Method	Public phishing Identification	Academic Phishing Identification
		Listing of admissible websites	Identify and disable spoofing website	Legitimate websites need to be identified
Attributes	Before visiting any website, user must carefully need to check the URL.	Blacklist approach	Heuristics and blacklist strategy configurations Freely accessible for use	Deep learning or machine learning algorithms are used to detect malicious act. Not freely accessible for use.
Benefits	Easy identification of malicious thefts. Alert users for major safety breaches. Able users to strengthen networks and social media of financial accounts settings Helps user to deal with the situation when he becomes victim	Enhanced precision	Different frameworks identify that whether or not the website is legitimate	Reduce false positive rates
Drawbacks	Ignorance or error by human preserves attacks from detection. Educational modules are required for educating users	Attackers can easily avoid and escape from attack detection	Number of false positive rates are high User do not recognize the shown security alerts	Require regular dataset updates

REFERENCES

[1]. Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., Cao, R. (2019, June). Survey of AI in cybersecurity for information technology management. In 2019 IEEE Technology & Engineering Management Conference (TEMSCON), pp. 1-8, IEEE.

[2]. Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory.

[3]. Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. Computers & Security, Vol. 73, pp. 102-113.

[4]. Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49-58.

[5]. Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), 125-129.

[6]. Sharbaf, M. (2019, August). Reengineering Cyber Security Process: A New Perspective on Cyber Security Quality Management. In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and TechnologyCongress(DASC/PiCom/CBDCom/CyberSciTech) (pp. 332-337). IEEE.

[7]. RS, S. R., & Preethisri, T. J. (2018). Awareness of Cyber Crime Among College Students-An Analytical Study. International Journal Of Management And Social Sciences (IJMSS), 8(1.3), 91-93.

[8]. Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cybercrime and cyber laws of India. International Research Journal of Engineering and Technology (IRJET), 4(6), 1633-1640.

[9]. Varshney, S., Munjal, D., Jash, I., Bhattacharya, O., & Saboo, S. (2020). Cyber Crime Awareness and Corresponding Countermeasures. Available at SSRN 3601807.

[10]. Sukanya, K. P., & Raju, C. V. (2017). Cyber Law Awareness among Youth of Malappuram District. IOSR Journal of Humanities and Social Science, 22(4), 23-30.

[11]. Kumar, P. V. (2016, March). Growing cybercrimes in India: A survey. In 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE) (pp. 246-251). IEEE.

[12]. Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems, 23(4), 1836-1846.

[13]. F. Callegati, W. Cerroni and M. Ramilli (Jan.-Feb. 2009) "Man-in-the-Middle Attack to the HTTPS Protocol," in IEEE Security & Privacy, vol. 7, no. 1, pp. 78-81

[14]. Z. Dou, I. Khalil, A. Khreishah, A. Al-Fuqaha, and M. Guizani, "Systematization of Knowledge (SoK): A systematic review of software-based web phishing detection," IEEE Communications Surveys & Tutorials, vol. 19, pp. 2797-2819, 2017.

[15]. R. Das, M. Hossain, S. Islam, and A. Siddiki, "Learning a deep neural network for predicting phishing website," Degree of B.Sc. in Computer Science, Brac University, 2019.

[16]. G. Varshney, M. Misra, and P. K. Atrey, "A survey and classification of web phishing detection schemes," Security and Communication Networks, vol. 9, pp. 6266-6284, 2016.

[17]. Whittaker, C., Ryner, B., & Nazif, M. (2010). Large-scale automatic classification of phishing pages.

[18]. Jakobsson, M., & Ratkiewicz, J. (2006, May). Designing ethical phishing experiments: a study of (ROT13) rOnl query features. In Proceedings of the 15th international conference on World Wide Web (pp. 513-522).

[19]. Aleroud, A. and Zhou, L. (2017) 'Phishing Environments, Techniques, and Countermeasures: A Survey', Computers and Security. Elsevier Ltd, 68, pp. 160–1

[20]. Bossetta, M. (2018) 'The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy', Journal

[21]. Chaudhary, G. K. (2014) 'Development Review on Phishing: A Computer Security Threat',

[22]. International Journal of Advance Research in Computer Science and Management Studies, 2(8), pp. 55–64.

[23]. Benitez-Mejia, D. G. N. et al. (2017) 'HTTPS: A Phishing Attack in a Network', Proceedings of the 7th International Conference on Information Communication and Management. Moscow, Russian Federation, 28–30 August. pp. 24–27

[24]. Banu, M. N. and Banu, S. M. (2013) 'A Comprehensive Study of Phishing Attacks', International Journal of Computer Science and Information Technologies, 4(6), pp. 783– 786.

[25]. Chiew, K. L., Yong, K. S. C. and Tan, C. L. (2018) 'A Survey Of Phishing Attacks: Their Types, Vectors and Technical Approaches', Expert Systems with Applications, Elsevier Ltd, 106, pp. 1–20.

[26]. Lakhita et al. (2016) 'A Review on Recent Phishing Attacks in Internet', Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT 2015). Noida, India, 8–10 October. IEEE, pp. 1312–1315.

[27]. Ryck, P. De et al. (2013) 'TabShots : Client-Side Detection of Tabnabbing Attacks', Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. Hangzhou, China, 8–10 May. pp. 447–455, doi: 10.1145/2484313.2484371.

[28]. Suryavanshi, N., Pradesh, M., Jain, A., & Pradesh, M. (2015) 'A Review of Various Techniques for Detection and Prevention for Phishing Attack', International Journal of Advanced Computer Technology (IJACT). pp. 143–147

[29]. Abdul, Orunsolu. (2015) 'An Updated Perspective on Phishing Countermeasures and Their Effectiveness'.

[30]. Purkait, S. (2012) 'Phishing counter measures and their effectiveness - literature review', Information Management & Computer Security, 20(5), pp. 382-420.

[31]. Huang, H., Tan, J., & Liu, L. (2009) 'Countermeasure Techniques for Deceptive Phishing Attack', 2009 International Conference on New Trends in Information and Service Science. Beijing, China, pp. 636–641, 2009.