International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Unconventional Phishing Attack: A Study of Cybercrime in Northern India

Shani Jaiswal[1], *Ashutosh Jaiswal*[2]

[1]Research Scholar, Centre for the Study of Law and Governance, Jawaharlal Nehru University, New Delhi, India
[2]Post Graduate Scholar, D.A.V. Snatkottar Mahavidyalaya, Azamgarh, Affiliated to Veer Bahadur Singh Purvanchal University, Jaunpur, Uttar Pradesh, India

DOI: https://doi.org/10.55248/gengpi.4.1123.113129

ABSTRACT:

India has a vast population. The union government continuously promotes digital payments for all purchasing and selling. Two popular payment apps in India are Google Pay and PhonePe. There are two popular online platforms, OLX and Quikr, where everyone can sell and purchase the old article. Basic details are crucial for a phisher to start phishing someone. Online platforms like OLX and Quikr have huge basic information about billions of deals mentioned by those who use these platforms to sell and purchase their old items. Everyone is aware of phishing through old tactics like sharing CVV, OTP, Credit/Debit card numbers, Expiry Dates, etc. RBI and all the Banks, as well as the government of India, have made the people aware not to share CVV, OTP, Credit/Debit card numbers, Expiry Dates, etc., through the various programs and guidelines. Those unaware of phishing became aware of this after releasing the 'Jamtara' movie.

But now, phishers have developed a new tactics of phishing, in which they use the details of a deal and relevant person and transact the money from accessible payment apps like Google Pay and PhonePe. Through this new tactics of phishing, phishers target well-digitized people in society. After getting phished in this way, one feels completely helpless. Phishers are very confident in phishing in this way because the police of many states need to become more familiar with this new tactics of phishing.

Keywords: phishing, Google Pay, PhonePe, OLX, Quikr

Introduction:

As India's population is increasing, the use of online payment platforms is also growing across the country. In this way, the number of active users of Google Pay, PhonePe, and other similar online payment platforms is also increasing daily. The Spread of digital education and the promotion of cashless transactions by the government have encouraged people to pay through online payment platforms. Now the significant population in India has been habitual of online payment. In such a situation, new incidents of phishing are also being seen. The presented research paper is currently attempting to show the new tactics of online phishing.

Methodology

The present research study is based on interviews of victims of phishing attack. Open ended discussion with cyber police officials of Lucknow and Delhi included in study. This paper discusses three cases of phishing attacks with a focus on how they became phished with new tactics by the phishers.

Objective of Study

To sensitize and alert online payment platform users such as Google Pay and PhonePe users and online marketplace like- OLX and Quikr users about the new tactics of phishing in trend. This study would provide insight into the new tactics of phishing attacks and their mechanism and suggest solutions to prevent such kind of new tactics of phishing.

What is Phishing?

Phishing is a cyber security attack in which malicious users send messages posing as reliable individuals or organizations. Phishing communications trick users into doing things like downloading malicious files, clicking malicious links, or disclosing private information like login credentials. Phishing attacks send fraudulent communications that seem to be from a reliable source.

Background

India, the country with the second-largest internet user base in the world, was a typical example of an expanding digital village. While improved connectivity through the internet promises significant advancement, it also exposes our digital societies to new threats. Cybercrimes know no borders and have evolved at a pace at par with emerging technologies. Each year, the number of cybercrimes reported nationwide continues to increase significantly.

Google Pay has emerged as the most dominant payments app in reach among internet users with 65% reach, followed by PhonePe with 63% penetration, and Paytm at 57% reach as of November 2020. Google Pay supports UPI payments and contactless card transactions through tokenized debit or credit cards linked to users' smart phones. Google Pay has over 150 million monthly active users, of which India accounts for a large share. PhonePe has 125 million active monthly users. PhonePe was the first to reach one billion UPI transactions (inc42, n. d.).

The OLX marketplace serves as a venue for the purchasing and selling services and products, including those related to electronics, clothing, furniture, home goods, cars, and bikes. According to reports, the site had 8.5 million monthly transactions, 25 million listings, 200 million monthly active users, and 11 billion page views in 2014. India is OLX’s second-biggest market, with 75% growth coming from non-metros; OLX currently has a large base of over 6 million daily active users. Moreover, on average, every listed item on the classifieds platform gets over 15 replies within seven days from interested buyers, and users spend around 16.5 minutes on every visit. It shows that the platform has an engaging set of audiences serious about buying.

Quikr is a Bangalore-based classified advertising and internet marketplace for India. More than 1000 Indian cities have Quikr listings for mobile phones, household goods, cars, real estate, jobs, services, and education. Users of the free online marketplace Quikr can buy, sell, rent, or find anything in India.

Literature Review

Phishing, the practice of obtaining computer credentials from users through manipulation or deceit, dates back at least 20 years to America Online (AOL), where users would impersonate AOL staff members and send instant messages to other users convincing them to disclose their passwords or credit card numbers. The email above was sent to users at the hospital and is one of many like this they receive every month. It encouraged recipients to click a link where they were asked to enter their username and password. However, the site was operated not by the IT department of the hospital but by hackers seeking to gather passwords. When a user takes the bait and enters a password on the hacker’s site, the hacker can access a range of online services by impersonating the user. Users fell victim to these manipulations, and some provided information, such as passwords, helpful to hackers. Phishing attacks like the one above are widespread, and organizations in most industries, including healthcare, have fallen victim to them. From press accounts and public announcements, there have been ten incidents since 2014 where hackers gained unauthorized access to hospital systems through phishing in the United States. Most phishing attacks have gone unnoticed or unannounced, and some security consultants have reported that hospitals routinely undergo several phishing attacks every week. Hackers were breaching the protected health information of hospitals. A Hollywood Presbyterian Hospital had to pay eventually to the phisher a $17,000 ransom **(Wright et al., 2016).**

Cyber criminals have also developed their methods for stealing their information, but social-engineering-based attacks remain their favorite approach. Phishing has been one of the biggest concerns as many internet users fall victim to it. It is a social engineering attack wherein a phisher attempts to lure the users to obtain their sensitive information by illegally utilizing a public or trustworthy organization in an automated pattern so that the internet user trusts the message, and reveals the victim’s sensitive information to the attacker (**Jakobsson and Myers, 2006)**.

Alternatively, attackers could exploit other mediums to execute their attacks such as Voice over Internet Protocol (VoIP), Short Message Service (SMS) and, Instant Messaging (IM) **(Gupta et al., 2015).** Phishers have also turned from sending mass-email messages, which target unspecified victims, into more selective phishing by sending their emails to specific victims, a technique called “spear-phishing.” Studies found that certain personal characteristics make some persons more receptive to various lures **(Iuga et al., 2016; Ovelgönne et al., 2017; Crane, 2019).** For example, individuals who usually obey authorities more than others are more likely to fall victim to a Business Email Compromise (BEC) that is pretending to be from a financial institution and requests immediate action by seeing it as a legitimate email (**Barracuda, 2020).** Greediness is another human weakness that could be used by an attacker, for example, emails that offering either great discounts or free gift cards, and others **(Workman, 2008).** Various channels are used by the attacker to lure the victim through a scam or through an indirect manner to deliver a payload for gaining sensitive and personal information from the victim **(Ollmann, 2004)**. However, phishing attacks have already led to damaging losses and could affect the victim not only through a financial context but could also have other serious consequences such as loss of reputation, or compromise of national security (**Ollmann, 2004; Herley and Florencio, 2008**). Cybercrime damages have been expected to cost the world $6 trillion annually by 2021 according to Cybersecurity Ventures **(Morgan, 2019).**

Phishing merges social psychology, technical systems, security subjects, and politics. Phishing attacks are more prevalent: a recent study **(Proofpoint, 2020)** found that nearly 90% of organizations faced targeted phishing attacks in 2019. From which 88% experienced spear-phishing attacks, 83% faced voice phishing (Vishing), 86% dealt with social media attacks, 84% reported SMS/text phishing (SMishing), and 81% reported malicious USB drops. The 2018 Proofpoint annual report **(Proofpoint, 2019)** has stated that phishing attacks jumped from 76% in 2017 to 83% in 2018, where all phishing types happened more frequently than in 2017. The number of phishing attacks identified in the second quarter of 2019 was notably higher than the number recorded in the previous three quarters. While in the first quarter of 2020, this number was higher than it was in the previous one according to a report from Anti-Phishing Working Group (APWG) **(APWG, 2018)** which confirms that phishing attacks are on the rise. These findings have shown that phishing attacks have increased continuously in recent years and have become more sophisticated.

These attacks are getting more sophisticated by the day and can cause severe losses to the victims. Although the attacker's first motivation is stealing money, stolen sensitive data, therefore, the phishers keep on developing their techniques over time with the development of electronic media. The available existing countermeasures are not enough to detect and prevent these attacks especially on smart devices. The social engineering element of the phishing attack has been effective in bypassing the existing defenses to date. It is essential to understand what makes people fall victim to phishing attacks. ***What Attributes Make Some People More Susceptible to Phishing Attacks than Others*** discusses the human attributes that are exploited by the phishers. Human nature is considered one of the most affecting factors in the process of phishing. Everyone is susceptible to phishing attacks because phishers play on an individual's specific psychological/emotional triggers as well as technical vulnerabilities **(KeepnetLABS, 2018; Crane, 2019).** In 2017, a report by PhishMe (2017) found that curiosity and urgency were the most common triggers that encourage people to respond to the attack, later these triggers were replaced by entertainment, social media, and reward/recognition as the top emotional motivators. However, in the context of a phishing attack, the psychological triggers often surpass people's conscious decisions. For instance, when people are working under stress, they tend to make decisions without thinking of the possible consequences and options **(Lininger and Vines, 2005).** Several studies have addressed the association between susceptibility to phishing and demographic variables (e.g., age and gender) as an attempt to identify the reasons behind phishing success at different population groups. Although everyone is susceptible to phishing, studies showed that different age groups are more susceptible to certain lures than others are. For example, participants with an age range between 18 and 25 are more susceptible to phishing than other age groups **(Williams et al., 2018).** The reason that younger adults are more likely to fall for phishing, is that younger adults are more trusting when it comes to online communication, and are also more likely to click on unsolicited e-mails **(Getsafeonline, 2017).** Moreover, older participants are less susceptible because they tend to be less impulsive **(Arnsten et al., 2012).** While some studies confirmed that women are more susceptible than men to phishing as they click on links in phishing emails and enter information into phishing websites more often than men do. Men are more susceptible to mobile phishing attacks than women. The main reason behind that, men are more comfortable and trusting when using mobile online services **(Hadlington, 2017).** Psychological studies have also illustrated that the user's ability to avoid phishing attacks affected by user's awareness of phishing **(Dhamija et al., 2006).**

There is a famous phishing attack commonly known as the Amazon Prime Day phishing attack. The information of the customers of Amazon Prime was compromised by a phishing attack. All the Amazon Prime members received an email that consisted of seemingly legitimate deals to them. On trying to purchase the 'deals', the transaction would fail, promoting the attackers to gain sensitive information on the user. Another common example is Google Docs invitation. In May 2017, attackers sent fraudulent invitations to Google users across the world to edit documents. When the recipients clicked the invitation, it led to a third party app that facilitated attackers to obtain confidential information **(Shankar et al., 2019)**. According to the Anti-Phishing Working Group (APWG), phishing activities grow and increasingly target financial and online payment services **(Kumaraguru, et al. 2007).**

The true request–fake response (TR-FR) phishing is a type of multiple-stage covered phishing where a user sends an original request to a recipient. The phisher intercepts the message and maintains the conversation as the real recipient during several stages of exchanges. At some stage, the phisher sends a polluted response. The victim will then trust this message and be compromised. Some studies believe that TR-FR is an upcoming trend, which could make several victims. TR-FR relies upon cross-communications between email services and contextual related emails. This is a new way exploited by phishers to learn from user's exchanges and take intelligible actions accordingly to lure potential victims **(Tchakounté, et al. 2019).**

The business phishing is a team work because the phishing process requires several roles and each should be conducted by different person. Email is an information technology product, to bypass the security huddles and attack emails, phishers need someone who is strong technical skills. They need person who are good at writing and business person knowing negotiation. They need people help to create a fake business and set up business bank account. They need people understand the international fund transfer process. With today's technology enabled globalization, it is very easy to set up such a team, and the cost is very low. The examples of popular websites for outsourcing are: oDesk, Elance, Guru, RentACoder, GetAFreelancer etc. After you post the job, you will receive applications very soon from all over the world. Many virtual assistant only ask for a few dollars per hour. Since these team members may not know each other, it is very difficult to be detected, discovered, and punished. MOHO, a business firm, manufacturer of construction chemicals in China is victim of business phishing. In order to expand to international market, the company developed their business website, actively posted the company and products information in many B-to-B Internet marketplaces such as Made-in-China, Alibaba, and ECplaza. The content of email communication covers almost every aspect of sales, including new product or new price information, order negotiation, confirmation, proforma invoice, sales contract, payment information, and product shipping information. The employees and management of MOHO were not aware of email phishing until the company email account was targeted and phished **(Ma, n. d.).**

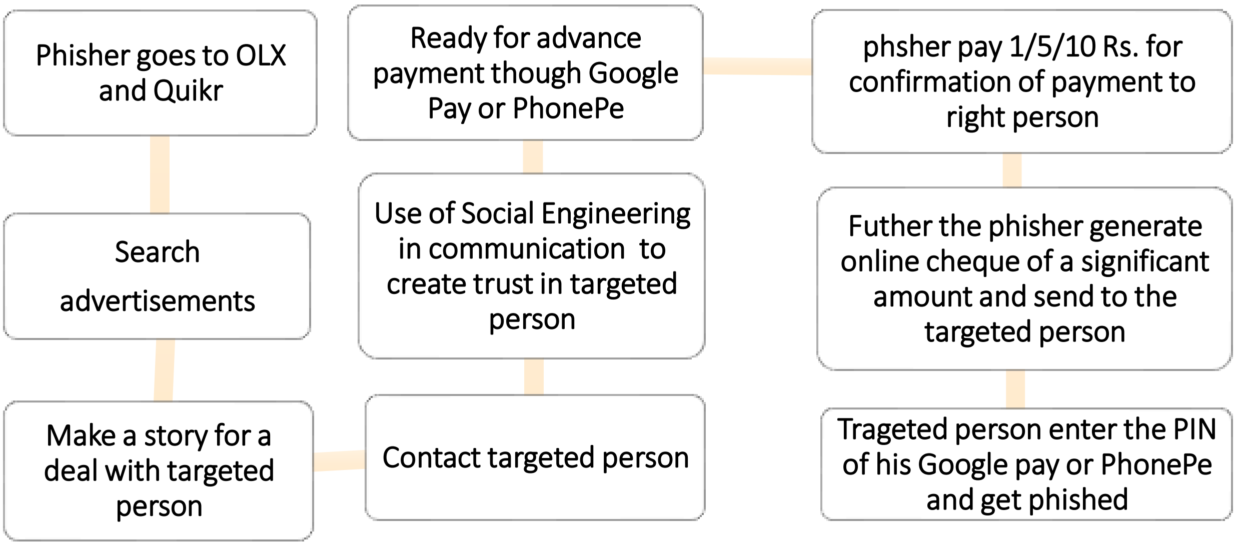
New Tactics of Phishing: Nature and Impact

Cybercrime is increasing day by day. In this, the incidence of online phishing is increasing rapidly. The early methods of phishing have alerted a large part of the public, although there are still a few left. In such a situation, the phishing group is inventing phishing tactics and is becoming successful in blowing people's money. The level of awareness among the people has increased. It is noteworthy that a phisher needs a mobile number to fraud someone's money. A phisher can easily get these mobile numbers from online marketplaces like OLX, Quikr, and 99acres.com, etc. On OLX, Quikr, and 99acres.com, etc users put their mobile number for easy access to all. These phishers deal with the purchase of goods sold by him on these platforms from the person with the number extracted from OLX, Quikr, and 99acres.com, etc.

To win trust, they show their identity as a trustworthy person like he is soldier in Army or Navy, sometime as a doctor so that the targeted person can trust a phisher easily. They send fake relevant virtual copy or photos of government identity cards like service ID cards, PAN cards, Driving License etc on WhatsApp account of the targeted person. Then phisher *says I like your goods/articles, it is fully finalized from my side. I confirm this deal. I pay you in advance so that no other customer could purchase. I am a duty person. I hardly have time to spare.* The targeted person gets ready easily because he feels that he does not have to give money, he has to make the money. It is common human nature that people are eager and in a hurry to sell their goods especially on online platform. The targeted person never thinks beyond or does not doubt an iota on phisher's motives and he gets easily caught in their clutches. The phisher tells the person that *I have sent an online cheque to your Google Pay, you take it. There is nothing to do to take it, just enter your PIN in your Google Pay or PhonePe*. The victim is so sure that neither I have given the ATM card number to the phisher, nor have I told it the expiry date, nor do I have to tell the PIN, but I have to enter my PIN in my Google Pay. Very easily he enters the PIN in his Google Pay or PhonePe account. As soon as the PIN is entered, the amount entered by the phishers in that online cheque automatically goes to the phisher's bank account. The targeted person (victim) considers the phisher to be the right person, so the phisher first make such an online cheque and send it, on clicking on which, as soon as the pin is entered, the money gets transfer to the victim's account immediately. But the amount in this online cheque is just only 5 ₹ or ₹ 10. The phisher do this so that there is no room for doubt in the mind of the victim. Further says that *Bhaiya! I am checking whether the money is going to your Google Pay account or not.* When the victim is completely convinced, then for the second time he throws his noose and gets caught in his clutches.

On contacting by the Cyber Crime Police Cell, it is found that the registered name on the mobile number from which the call has come is that of an above 90-year-old illiterate elderly man or elderly woman or that the person with that name is dead or the address is found to be wrong. The team of Cyber Crime Police Cell (Special), Lucknow says that this is a big gang that is supported by a mafia gang. The special thing is that in the state where they run their phishing base, they mostly target the people of other states so that police proceedings are more complicated and can be easily avoided.

Steps of New Tactics of Phishing


Phisher goes to OLX and Quikr
Search advertisements
Make a story for a deal with targeted person
Contact targeted person
Use of Social Engineering in communication to create trust in targeted person
Ready for advance payment though Google Pay or PhonePe
phsher pay 1/5/10 Rs. for confirmation of payment to right person
Futher the phisher generate online cheque of a significant amount and send to the targeted person
Trageted person enter the PIN of his Google pay or PhonePe and get phished

Discussion

In this paper three incidents of above new tactics of phishing are covered. The first phishing incident- Rajesh Kumar Verma, the landlord of a colony opposite Babu Banarasi Das University Lucknow, who has a 3-story house, had to rent his house, which he advertised on OLX, Quikr, and 99acre.com. The address was also put in the advertisement along with the contact details. When the phisher called Mr. Verma, he said, *"I saw your OLX advertisement. I like your house."* In the form of identification, the phisher told Mr. Verma that he is the head constable in CRPF, and his posting has come to Lucknow through transfer. He has to shift to Lucknow with his family. He said, *"I am busy with transfer paperwork so I will come to Lucknow after ten days. After coming to Lucknow, I will not have time to look for a house. I like your house. You finalize the deal by taking an advance. I will give the rest of the money when I come to Lucknow after ten days while shifting the house."* ₹ 8000 per month was fixed by reducing ₹ 500 from the amount demanded as house rent. The phisher asked Mr. Verma to give this amount as advance and how he would take the online payment, so it was decided to take an advance on PhonePe. First, the phisher generated an online cheque of ₹ 5 and sent it to Mr. Verma's PhonePey number. He asked Mr. Verma to receive the advance amount in that online cheque by entering his PhonePe PIN. Mr. Verma did the same as the phisher told him, and ₹ 5 came into his PhonePe account. Mr. Verma said to the phisher all good, pay in full now. This time, the phisher generated an online cheque of Rs.8000 and sent it to Mr. Verma's PhonePe account. Mr. Verma followed the same process again, and this time ₹ 8000 was deducted from his PhonePe account, and then the phisher cut the call.

Second phishing incident- Ms. Sudha, a female Ph.D. scholar of the Department of Physics at Lucknow University, was selling her laptop on Quikr for ₹ 20000 in the third wave of Corona. Ms. Sudha received many calls, but the deal was not completed. Sudha wanted to sell her laptop urgently and wanted a fair price. When the phisher called her, he finalized the deal for the laptop for ₹19000. The phisher told Sudha that he would take the laptop after two days. Please do not sell the laptop to anyone else, so he told her to pay in advance. In the form of identity, he told his identity as the owner of a laptop shop. Regarding the advance, it was decided to take payment from Google Pay as an online payment. First, the phisher made an online cheque for one rupee and sent it to Sudha's Google Pay number to confirm payment to the right person. As soon as Sudha entered her Google Pay PIN, Rs 1 was credited to her account. Second, another online cheque of ₹ 10000 was made and sent to Shudha. ₹ 10000 went to the phisher as soon as he entered the PIN. Again phisher made an online cheque of ₹ 9000 and sent it to Sudha. Sudha again followed the same process. ₹9000 more went to the phisher. Sudha had an account with Indian Bank that was added to Google Pay. Whose deduction message comes about 5 minutes late. When Sudha gets messages from the bank about the deduction of her amount, she is very shocked.

The third phishing incident- When Jawaharlal Nehru University researcher Riya's course was completed, she advertised on OLX to sell her second-hand scooty urgently. The demand amount for the scooty was around ₹40000. When the phisher calls Riya, he asks her to send scotty's papers so that he would be considered a genuine customer. After all the information about Scooty, the phisher said, *"Madam! I am outstation now. You fix the deal by taking advance from me. After three-four days, I will take the scooty from the campus by giving the remaining money."* When Riya did it, the phisher asked, *"Madam, do you use Google Pay or PhonePe?"* Madam said yes. To check the correct person's payment confirmation, he generated an online cheque of ₹ 5 and sent it to Riya's Google Pay number. As soon as Riya entered her Google Pay PIN to confirm the payment, she got Rs.5. Then Riya told the phisher, OK, everything is correct. She said to do a significant amount. This time the phisher generated an online cheque of ₹ 10000. As soon as Riya entered the PIN in her Google Pay, ₹ 10000 was deducted from his account. Riya was shocked. By then, her money had been deducted.

Phishing is a hazard to E-businesses and e-marketplaces. Phishing combines social engineering and technical methods to persuade users to disclose sensitive and personal data. In the above phishing incidents, the phishers have used social engineering sophisticatedly. The details and pieces of information the users (targeted persons) give in advertisements on online platforms like OLX and Quikr assist the phishers in social engineering.

There are two crucial things in such type of phishing. First, while placing advertisements on OLX and Quikr, no users think that phishers will use their advertisement information this way.

Secondly, in India, most online payment app users like Google Pay and Phone Pay only use QR codes or Google Pay and PhonePe numbers to make or receive payments. Only some users know that these apps can also generate and share online cheques. In this online cheque, the amount is already filled by the phisher. The user has to enter his PIN, and the amount goes to the phisher. With the intelligent use of social engineering and payment apps, phishers can easily lure people into their web. In this type of phishing, the information given by the user in the advertisement on OLX, Quikr, is vital for the phishers. Social engineering is one of the biggest challenges to network security because it takes advantage of the natural human tendency to trust. Social engineering has become a major threat and constitutes a major threat affecting the ordinary user and the large company.

Conclusion

Nowadays, it has become a grave issue of phishing attacks. There are many techniques to solve these problems. But people may don't aware of the seriousness of phishing. Phishing attacks are still thriving because of many inexperienced and unsophisticated internet users. Often the phishers exploit human vulnerabilities in addition to favoring technological conditions (i.e., technical vulnerabilities). It has been identified that age, gender, internet addiction, user stress, and many other attributes affect the susceptibility to phishing between people. The phishers always explore *'What Attributes Make Some People More Susceptible to Phishing Attacks than Others'*. In addition to traditional phishing channels (e.g., email and web), this new phishing tactics is increasing. Furthermore, the use of online marketplace and payment apps based phishing has increased in parallel with the growth of apps like OLX, Quikr, and 99acre.com.

This study gives awareness about the new tactics of phishing. From research and analysis, it is evident that there is no single solution for the phishing threat due to the heterogeneous nature of the phishing attack. Continual security awareness training is the key to avoiding phishing attacks and reducing their impact. Developing efficient anti-phishing techniques that prevent users from being exposed to phishing attacks is essential in mitigating phishing attacks. Although human education is the most effective defense against phishing, it is difficult to remove the threat entirely due to the sophistication of the phishing attacks and social engineering elements. People must be aware of social engineering while online because this new tactics of phishing is wholly based on social engineering.

Suggestion

- Police research should be encouraged on every possible new tactics on phishing.
- National and regional TV channels should run the programs in national and regional languages to inform people about the new type of phishing incident.
- 9 out of 10 cases of phishing are not reported to the cyber cell. Appointment of a cyber crime reporting agent for easy reporting at the village and street level, he will report these incidents to the cyber cell of the police. There should increase awareness of new tactics for phishing incidents at the panchayat level.
- Cyber education should also be given along the lines of physical education to keep future generations alert.
- Periodic updating of anti-phishing tools or software may be helpful to secure their confidential information and credentials.

- Bank's server should be so fast that it delivers the messages of each transaction in real-time simultaneously with transactions in online payment apps like Google Pay and PhonePe.
- *Every online payment app user must think about 'What Attributes Make a Person More Susceptible to such Phishing Attacks.'*
- *Online marketplace apps like OLX and Quikr should make a reporting mechanism so that OLX and Quikr can block the reported users, and they cannot get access further to these apps.*
- *The Police should follow a hybrid approach to phishing detection.*

References:

Abeer F. AL-Otaibi, a. E. (November, 2020). A STUDY ON SOCIAL ENGINEERING ATTACKS: PHISHING ATTACK. International Journal of Recent Advances in Multidisciplinary Research , Vol. 07, Issue 11, pp. 6374-6380.

Adam Wright, S. A. (2016). The Big Phish: Cyberattacks Against U.S. Healthcare Systems. Journal of General Internal Medicine , 1115-1118.

Akarshita Shankar, R. S. (2019). A Review on Phishing Attacks. International Journal of Applied Engineering Research , 2171-2175.

Amro, B. (2018). Phishing Techniques in Mobile Devices. Journal of Computer and Communications , 27-35.

APWG (2018). Phishing activity trends report 3rd quarter 2018. US. 1–11.

APWG (2020). APWG phishing attack trends reports. 2020 anti-phishing work. Group, Inc. Available at: https://apwg.org/trendsreports/ (Accessed September 20, 2020).

Arnsten, B. A., Mazure, C. M., and April, R. S. (2012). Everyday stress can shut down the brain's chief command center. Sci. Am. 306, 1–6. Available at: https://www. scientificamerican.com/article/this-is-your-brain-in-meltdown/ (Accessed October 15, 2019).

Barracuda. (2020). Business email compromise (BEC). Available at: https://www. barracuda.com/glossary/business-email-compromise.

Basuroy, T. (Dec 21, 2022). statista.com. Retrieved from statista.com: https://www.statista.com/topics/5054/cyber-crime-in-india/

Chun-Ying Huang, S.-P. M.-T. (2011). Using one-time passwords to prevent password phishing attacks. Journal of Network and Computer Applications , Volume 34, Issue 4, Pages 1292-1301.

Crane, C. (2019). The dirty dozen: the 12 most costly phishing attack examples. Available at: https://www.thesslstore.com/blog/the-dirty-dozen-the-12-mostcostly-phishing-attack-examples/#:~:textAt some level%2C everyone is susceptible to phishing, outright trick you into performing a particular task (Accessed August 2, 2020).

Damodaram, D. (Jan-2016). STUDY ON PHISHING ATTACKS AND ANTIPHISHING TOOLS. International Research Journal of Engineering and Technology (IRJET) , Volume: 03 Issue: 01, Jan-2016, p.700-705.

Dhamija, R., Tygar, J. D., and Hearst, M. (2006). "Why phishing works," in Proceedings of the SIGCHI conference on human factors in computing systems - CHI '06, Montréal Québec, Canada, (New York, NY: ACM Press), 581. doi:10.1145/1124772.1124861

Dr. M. Nazreen Banu, a. S. (2016). A Comprehensive Study of Phishing Attacks . International Journal of Computer Science and Information Technologies , Vol. 4 (6), 783-786.

Franklin Tchakounté, V. S. (2019). True Request–Fake Response: A New Trend of SpearPhishing Attack. Journal of Network Security , Volume 7, Issue 3, 1-17.

Getsafeonline. (2017). Caught on the net. Available at: https://www.getsafeonline.org/news/caught-on-the-net/%0D

Gupta, P., Srinivasan, B., Balasubramaniyan, V., and Ahamad, M. (2015)."Phoneypot: data-driven understanding of telephony threats," in Proceedings 2015 network and distributed system security symposium, (Reston, VA: Internet Society), 8–11. doi:10.14722/ndss.2015.23176

Hadlington, L. (2017). Human factors in cyber-security; examining the link between internet addiction, impulsivity, attitudes towards cyber-security, and risky cyber-security behaviours, Heliyon 3, e00346-18.doi:10.1016/j.heliyon.2017.e00346

Herley, C., and Florencio, D. (2008)."A profitless endeavor," in New security paradigms workshop (NSPW '08), New Hampshire, United States, October 25–28, 2021, 1-12.doi:10.1145/1595676.1595686

Hindu, T. (2021). Only 20% of Indians are not confident in their ability to prevent a cyber attack. Retrieved from https://www.thehindu.com/sci-tech/technology/internet/mcafee-cybersecurity-india-consumer-security-mindset-report-2021-cybersecurity-phishing-hacking-data/article33674262.ece

inc42. (n.d.). 3.94 Lakhs And Counting: How Cyberattacks Are A Worry For Digital India. Retrieved from https://inc42.com/: https://inc42.com/buzz/3-94-lakhs-and-counting-how-cyberattacks-are-a-worry-for-digital-india/

Iuga, C., Nurse, J. R. C., and Erola, A. (2016).Baiting the hook: factors impacting susceptibility to phishing attacks. Hum. Cent. Comput. Inf. Sci.6, 8.doi:10.1186/ s13673-016-0065-2

Jakobsson, M., and Myers, S. (2006). Phishing and countermeasures: understanding the increasing problems of electronic identity theft. New Jersey: John Wiley and Sons.

Keepnet LABS (2018). Statistical analysis of 126,000 phishing simulations carried out in 128 companies around the world. USA, France. Available at: www. keepnetlabs.com

Kumaraguru P, Rhee Y, Acquisti A, et al. Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. Proceedings of the SIGCHI Conference of Human Factors in Computing Systems (CHI'07). San Jose, California, USA, April 28–May 03, 2007:905p.

Lininger, R., and Vines, D. R. (2005). Phishing: cutting the identity theft line. Print book. Indiana: Wiley Publishing, Inc.

Ma, Q. (n.d.). The process and characteristics of phishing attacks -A small international trading company case study. Journal of Technology Research .

Morgan, S. (2019). 2019 Official annual cybercrime report, USA, UK, and Canada, Available at: https://www.herjavecgroup.com/wp-content/uploads/2018/12/ CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Nabie Y. Conteh, a. a. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research , 31-38.

Ollmann, G. (2004). The phishing guide understanding & preventing phishing attacks abstract. USA. Available at: HYPERLINK "http://www.ngsconsulting.com" http://www.ngsconsulting.com .

Ovelgönne, M., Dumitras¸, T., Prakash, B. A., Subrahmanian, V. S., and Wang, B. (2017).Understanding the relationship between human behavior and susceptibility to cyber attacks. ACM Trans. Intell. Syst. Technol. 8, 1–25. doi:10.1080/00207284.1985.11491413

PhishMe (2017). Human phishing defense enterprise phishing resiliency and defense report 2017 analysis of susceptibility, resiliency and defense against simulated and real phishing attacks.

Proofpoint. (2019a). State of the phish 2019 report. Sport Mark. Q. 14, 4.doi:10. 1038/sj.jp.7211019

Proofpoint. (2019b). What is Proofpoint. Available at: https://www.proofpoint. com/us/company/about

Proofpoint. (2020). 2020 state of the phish. Available at: https://www.proofpoint. com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

Purplesec. (n.d.). Cyber Security Statistic. Retrieved from Purplesec: https://purplesec.us/resources/cyber-security-statistics/

Sankhwar, S. P. (2017). Defending Against Phishing: Case Studies. International Journal of Advanced Research in Computer Science , Vol. 8 Issue 5, p2605-2607. 3p.

Shalaka Ekawade, S. M. (2016). Phishing Attacks and Its Preventions. Imperial Journal of Interdisciplinary Research (IJIR) , 1766-1769.

statista.com. (2021). Number of online banking frauds reported across India in 2021, by state. Retrieved from statista.com: https://www.statista.com/statistics/1097957/india-number-of-online-banking-frauds-by-leading-state/

thehindubusinessline. (2021). 35% of internet users in India affected by web-borne threats in 2020: Report. Retrieved from https://www.thehindubusinessline.com/news/35-of-internet-users-in-india-affected-by-web-borne-threats-in-2020-report/article34003043.ece

times, e. (2018). India among top 3 countries most targeted for phishing: Report. Retrieved from https://economictimes.indiatimes.com/tech/internet/india-among-top-3-countries-most-targeted-for-phishing-report/articleshow/64318150.cms

Vaishnavi Bhavsar, A. K. (December 2018). Study on Phishing Attacks. International Journal of Computer Applications , 27-29.

Vieira-Marques, A. F. (2018). Phishing Through Time: A Ten Year Story based on Abstracts. 4th International Conference on Information Systems Security and Privacy , 225-232.

Williams, E. J., Hinds, J., and Joinson, A. N.(2018).Exploring susceptibility to phishing in the workplace. Int. J. Human-Computer Study.120, 1–13.doi:10. 1016/j.ijhcs.2018.06.004

Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. J. Am. Soc. Inf. Sci. 59 (4), 662–674. doi:10.1002/asi.20779

Zainab Alkhalil, C. H. (09 March 2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science , 1-23.