AN ANALYTICAL STUDY OF PHISHING ATTACKS AND ITS RELATED LAWS IN INDIA

Akshat Anand*

ABSTRACT

In present era, there are many concerns about data security. Hackers have developed their skills to the point that they can easily get access to another person's system and steal their information. Phishing is one of the methods that may be used to get access to the data. Phishing is a sort of cybercrime in which victim's personal information, such as their phone number, email address, bank details, credit card information, biometrics and password is obtained by deceptive means such as these. Phishing is primarily a method of stealing personal information from users through the internet. Phishers utilize social engineering to get access to their victims' personal information and account credentials. This research paper provides a good overview of phishing attacks, including the sorts of attacks that are used, how they are detected, and how they may be prevented. Phishing laws in India are also examined in this research paper by analyzing case laws.

Keywords: Cyber Crime, Phishing, Social Engineering.

INTRODUCTION

Phishing is a sort of social engineering whereby an attacker delivers a false (fake, or other misleading) communication intended to mislead a person into giving the attacker access to sensitive information or to install dangerous software, such as ransomware, on the victim's infrastructure.[1] Hacking programmed AOHell developed by Koceilah Rekouche in 1995, which sought to steal passwords and financial information from American internet and web users, contained the first description of phishing[2]. Phishing attacks have gotten more prominent in recent years, enabling the hacker to trace the victim's every move on the website. It is common for attackers to establish a replica of the site they are trying to invade, and then lure people by promising things that aren't genuine. X-Force Threat Intelligence Index 2022

*BBA LLB, SECOND YEAR, SYMBIOSIS LAW SCHOOL, PUNE.

[1] K.Jansson & R. Von Solms, Phishing for phishing awareness, Vol. 32 Issue 6, TFO, 1., 2011, https://www.tandfonline.com/doi/abs/10.1080/0144929X.2011.632650

[2] Gunter Ollmann, Understanding and Preventing Phishing Attacks, Whitepapers, (Jul. 20,2022, 1:09 PM), http://www.technicalinfo.net/papers/Phishing.html

revealed that phishing has been the most popular method of access for computer hackers into a company or organizations' website or database. In most cases, they do this in preparation for a far more serious attack, like a ransomware and a malware attack. Phishing was utilized for 41% of all attacks that X-Force dealt with in 2021, according to the Index. This is a 33% rise from year 2021[3].

LITERATURE REVIEW

The next chapter's information was assembled from publications, research papers, journals, electronic libraries, etc. to provide comprehensive knowledge. This research relied only on secondary data. The below-listed papers and articles will be used to evaluate the current research. The reviewed literatures will be helpful in clarifying the present research study and assisting in the comprehension and identification of the real issue.

1. In this research paper, the author has discussed about the evolution of phishing attacks, as well as the motive of the attacker, are all covered in depth. High accuracy phishing attack detection has long been a topic of significant interest.[4]
2. In this research paper, through some real-world instances, the author of this paper has addressed current advancements in phishing techniques.[5]
3. In this research paper, the author analyses the various kinds of phishing methods such as email phishing, social media phishing, link manipulation, social engineering, spear phishing, whaling, smishing, IDN spoofing, search engine phishing, vishing and the most recent one cryptocurrency phishing as well as how phishing attacks operate and why it's the most popular type of cybercrime[6].
4. In this research paper, the author discusses about the state of phishing under Indian laws by analyzing several case laws.

RESEARCH OBJECTIVE

The primary objective of this research paper is to disseminate knowledge and information regarding phishing attacks and the various methods that are used to carry them out, as well as

[3] Jennifer Gregory, What Are The Biggest Phishing Trends Today, Data Protection, (April 28, 2002), https://securityintelligence.com/articles/biggest-phishing-trends-2022
[4] Vaishnavi Bhavsar, Aditya Kadlak &Shabnam Sharma, Study on Phishing Attacks, Vol. 182-No.33, IJCA, 1., 2018, https://www.researchgate.net/publication/329716781_Study_on_Phishing_Attacks
[5] Ibid
[6] Felix Richter, The Most Common Types Of Cybercrime, Statistica, (May 18, 2022), https://www.statista.com/chart/24593/most-common-types-of-cyber-crime/#:~:text=According%20to%20a%20recent%20FBI,common%20type%20of%20cyber%20crime

the various strategies that are utilized by cybercriminals in order to retrieve the sensitive data that is held by individuals and how Indian law addresses the issue of phishing.

RESEARCH QUESTIONS

1. What constitutes phishing, how does it work?
2. How can a person tell if they've been phished by the various phishing tactics?
3. What causes led to the development of phishing, and finally, so how would Indian laws address phishing?

RESEARCH METHODOLOGY

Research methodology is the most important chapter to study while doing and reviewing research. It helps examine the research's major instruments and techniques. Examine and implement assignment ideas and approaches. Appropriate research equipment helps generate reliable results. The study's guiding premise influences the results. In this part, the researcher used secondary data to gather and interpret significant information. In this study, secondary data sources were used to examine the phishing and its types along with its relevance in Indian laws. Abstract data, quantitative data, or a hybrid framework with both are basic data sources.

THE NATURE OF PHISHING ATTACKS

Phishing is a technique of social engineering which aims to steal personal data, like users' login passwords and credit card data. Social engineering is used when the attacker pretends as a valid, legitimate and trustworthy source to trick a target into opening an email, IM, or any textual message. As a consequence, the target is tricked into visiting a compromised website, which may lead to the delivery of malware, the locking down of the system in a ransomware attack, or the exposure of private information.[7]

It is very uncommon for phishing attempts being used as part of a larger attack, including an APT (Advanced Persistent Threat) event, in order to gain access to government or corporate networks. In this nightmare scenario, employees are infiltrated so that hackers may breach security measures, spread malware inside a restricted network, or get access to sensitive information. When a business or an organization is attacked in this way, it often loses

[7] Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/tips/ST04-014 , (last visited Jul 20. 2022)

customers, employees, and revenue. The severity of a phishing attack determines how difficult it will be for an organization to recover from the incident.

HOW DO PHISHING SCAMS WORK?

Phishing targets the human element to bypass technical safeguards. This kind of assault has the potential to completely undermine the effectiveness of technological security measures. Attackers may get unauthorized entry to a company's networks through spear phishing. These assaults often involve the dissemination of malware that gives the attacker access to the user's system. In this way, an external attacker may get access and entry to the network from a distant location. Moreover, attackers routinely get access to users' credentials as a consequence of attacks. Your credentials will allow you to access protected resources and information. Many technical security measures may be bypassed if an attacker gains restricted access to a company's systems via a hacked computer or set of credentials. This leaves the door open for the attacker to switch tactics and get access to other resources. This could eventually result in the complete downfall of a company. Loss of customer and employee data, code breaches and other similar actions are all possible outcomes.

EVOLUTION OF PHISHING

Phishing was initially documented in Koceila Rekouche's hacking tool AOHell in 1995, while it must have been likely first employed in a print edition of a hacker magazine 2600[8]. Phishing is not a new phenomenon, since it has not always received as much attention as it does now. Although the method has been around since approximately 1995, it was not until the over a decade ago that the general public learned about that. That's not to suggest phishing wasn't always a major problem. In order to avoid falling for these cons, even a basic familiarity of their background is essential. Users are duped into providing personal information in phishing attacks because they fall for fake electronic mails and internet sites. The name "phishing" for these scams is appropriately descriptive. There's good rationale for using the letter "ph" instead of the letter "f" in the phrase's spelling. Early hackers were called "Phreaks" for short. Phreaking refers to the practice of inspecting, testing, and analyzing a telecommunications network. The phreak community and the hacker community have historically worked well together. These anonymous online forums with the "ph" spelling have been related to phishing attack. Several components of phishing are still the same because they were back during AOL's

[8] Koceilah Rekouche, Early Phishing, Cornell University, (Jun. 23, 2011), https://arxiv.org/abs/1106.4692

prime. Around 2001, phishers started targeting internet banking systems. While the June 2001 phishing attack on E-Gold proved to be ultimately unsuccessful, but they did plant a significant seed. During 2003, phishers created hundreds of domains that appeared identical to legitimate sites like eBay and PayPal. Using e-mail worm tools, they flooded PayPal users' inboxes with phishing scam emails. In 2004, phishers were riding a high off their attacks on financial sites and their customers. Pop-up windows were used to get sensitive information from victims. Between May 2004 and May 2005, phishing cost American businesses and individuals a combined $929 million, affecting an estimated 1.2 million clients. To the tune of almost $2 billion annually, phishing has evolved into a well-organized criminal enterprise. Specialized software's that can process phishing payments are proliferating throughout the world, removing a major source of vulnerability. The software is used by criminal organizations in phishing assaults.[9]

VARIOUS KINDS OF PHISHING TECHNIQUES

1. **IDN (International domain name) spoofing:** It is possible to trick users into visiting malicious websites by using IDNs to create URLs and addresses that seem like those of genuine sites. These links seem to be for the genuine website, but then in reality they take you to a fake one. Since the phisher can theoretically buy a genuine certificate and afterwards modify the content to mimic a genuine website, and host the phished site without utilizing the SSL in anyway, digital certificates are not a viable solution to this issue.
2. **Email Phishing:** When an attacker sends out hundreds of fake messages, even if just a small fraction of recipients fallen for such fraud, the attacker may still get access to personal and sensitive data and funds. To increase their chances of success, attackers use a wide range of techniques. One instance of this is how much effort is put into making a phishing email seem to come from a legitimate source when, in fact, it is not. These emails be using the similar wording, fonts, trademarks, and initials, signatures as legitimate ones, giving them the appearance of authenticity. In addition, attackers usually try to scare users into taking immediate action. For instance, an email may warn of an impending account termination and include a countdown timer. Due to the stress, the user's attention and care dwindles, making him or her more prone to making

[9] Phish Protection, https://www.phishprotection.com/resources/history-of-phishing/ , (last visited Jul. 20, 2022)

mistakes. Finally, the links included in the mails are a dead ringer for the real thing, except that the domain name is sometimes misspelt or there are extra subdomains.

3. **Smishing:** Smishing refers to phishing attempts made by text message (SMS), as opposed to email. Their functionality is similar to that of phishing emails: Criminals distribute harmful links in messages that look to come from credible sources. An incentive such as a discount or free passes to an upcoming event might be offered in exchange for a click on a link that really leads to a scam.
4. **Search Engine Phishing:** By imitating a genuine website via the use of a search engine, hackers may have had their own website listed by the major search engines. The ignorant internet buyers who stumble onto these sites via a random search on a search engine are often duped by the sites' claims of cheap prices and excellent deals. When consumers use it, they are often required to sign up for an account or submit financial data before making a purchase. Scammers ' main goal is in collecting such information is to steal identities or commit financial fraud.
5. **Whaling:** Whaling is an advanced kind of phishing that, like spear phishing, targets particular people inside an organization—in this instance, high-level executives. This group also includes members of the executive team such as the chief executive officer and the chief financial officer, as well as any other members of the executive team who have access to secret information. These emails will often utilize a stressful circumstance, such as forwarding a statement from a firm that is being sued, as a way to hook their targets and get them to open the attachment. This increases the likelihood that the recipient will open the infected attachment or click the link that is connected with the message.
6. **Spear Phishing:** Spear phishing is a kind of phishing that is directed at particular people or departments inside a company. It's a dangerous kind of phishing, the fraudulent practice of communicating with targets through electronic means in such an effort to obtain sensitive data or to coerce targets into doing activities that compromise networks, delete data, or steal money. Spear phishing, in contrast to more general phishing techniques, involves narrowing down on a single target and doing extensive background research before sending out any emails. An accompanying attachment and electronic mail are standard components of a spear phishing assault. The electronic mail is personalized to the target by providing details such as their identity and position at the organization. By using this strategy, the social engineer increases the likelihood

that now the target would click the e-mail and any attachments it contains, so completing the replication of the virus[10].

7. **Social Media Phishing:** Phishing on social media happens when cybercriminals pose as legitimate businesses or individuals on platforms like Instagram, Twitter and Facebook to steal sensitive information or deceive users towards visiting malicious websites. To lure people towards the trap, cybercriminals and hackers may create fake accounts pretending to be friends or family members, or they could pose as a legitimate company's customer care department.
8. **Vishing:** Voice phishing, or vishing, is a kind of phishing that operates similarly like smishing since both utilize mobile phones as a vector for attacks, however in this case the target is attacked by voice call rather than text message. Sometimes, a vishing call would play a recorded voice mail message that sounds like it came from a trustworthy source like a bank or the government authorities.

   Attackers and hackers imply you have a significant debt, your vehicle insurance is about to expire, and your credit card has been used fraudulently and has to be fixed urgently. The target is then informed that should verify their identification by giving data like a credit card number.
9. **Link Manipulation:** Usually phishing attacks involve a technique of technological deception using a website link that looks to be from the legitimate company the attackers are pretending to be from. Most often, URLs will be misspelt in an attempt to deceive users. Here to casual observer, a URL like http://www.xyz.com/ may seem quite legitimate; nevertheless, it would really direct the viewer to the malicious mirror site of xyz.com. Following this link it would prompt the user directly to the phisher's website, where their sensitive data could be monitored and stolen.
10. **Cryptocurrency Phishing:** Similar to traditional phishing, cryptocurrency phishing happens when fraudsters attempt to trick prospective targets into sending money or disclosing the credentials to their cryptocurrency wallets. Email, text message, social networking sites, and communication are all viable channels for cryptocurrency phishing. Among the most high-profile examples in recent memory included a Florida resident named Graham Ivan Clark who attacked and somehow hacked the Twitter handles of famous persons including Barack Obama, Elon Musk and Joe Biden in order

[10] Trend Micro, https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing , (last visited Jul. 20, 2002)

to convince cryptocurrency purchasers to give him the money so he could make a 100,000-dollar profit.[11]

11. **Social Engineering:** Lack of technical competence is seldom the cause of phishing; rather, it's the victim's emotional and mental weakness. Social engineering is at the core of most Phishing attacks, having targets deceived into doing an activity in return for a reward. Phishers might create a sense of urgency in their targets by threatening to terminate the account or seize the money. Then, critical data disappears. Attackers also employ fake news reports to mislead readers into accessing malicious websites before even inspecting the link. A user's browser gets infiltrated when they access a malicious site, installing malware.

INDIAN LEGISLATION AND PROVISIONS REGARDING PHISHING

Phishing is illegal in several countries and is specifically included in the IT (Information Technology) Act, 2000. Around 2008, the law was updated to include additional rules and possible remedies for combating phishing.

The parts of the IT Act that are relevant to the offence of phishing are as follows:

1. **Section 66:** Since the phisher now has already acquired access to the target's bank account, the fraudster may now delete or edit the target's information on the server of the bank and steal money. Therefore, Section 66 of the Information Technology Act[12] specifically covers and penalizes this conduct.

2. **Section 43:** Under Section 43[13] of the Information Technology Act, 2000 anyone who accesses, installs, transmits, disturbs, refuses, or helps another person in any way while using a computer, computer system, or computer network without the owner's consent is subject to liability under this section.
3. **Section 77B**: All provisions of the Information Technology Act, 2000 that deal with phishing attacks are bailable offences under Section 77B[14]. (2008 Amendments). It was most certainly because no one is aware of who real culprit. The accusation should

[11] Kari Paul, Teen who hacked Joe Biden and Bill Gates' Twitter accounts sentenced to three years in prison, The Guardian, (Mar, 17, 2021, 00: 15 GMT), https://www.theguardian.com/technology/2021/mar/16/florida-teen-sentenced-twitter-bitcoin-hack
[12] Information Technology Act, 2000, Section 66, Acts of Parliament (India)
[13] Information Technology Act, 2000, Section 43, Acts of Parliament (India)
[14] Information Technology Act, 2000, Section 77B, Acts of Parliament (India)

indeed be made bailable since the phisher's identity is concealed every time by a translucent display next to them and because it is possible for the incorrect person to be found guilty of a crime that the person did not commit. The IPC,1860 also has sections for mischief (Sec. 425), cheating (Sec. 415), forgery (Sec. 464) and abetment (Sec. 465)

4. **Section 66A:** Penalties under Section 66A[15] of the Information Technology Act apply to anybody who knowingly disseminates incorrect information with the intent to cause damage to another person.
5. **Section 66C**: Section 66C[16] makes identity theft an offence that can be punished under Information Technology Act, 2000. Passwords, digital signatures as well as other features that may be used to individually identify individuals are explicitly forbidden by this section. Phishers commit acts of fraud by pretending to be the legitimate account holders.
6. **Section 66D:** The Section 66D[17] of the Information Technology Act specifies penalties for using a false identity to commit fraud via electronic means of communication or data manipulation. Online fraud occurs when criminals pose as legitimate businesses by using an internet address (URL) that leads to a false version of the legitimate business's website.
7. **Section 81:** In Section 81[18] of the Information Technology Act includes a term known as a non-obstante clause, which states that the contents of this act will take effect despite anything contradictory with them, including those included in any other act that is now in force.

CASE LAWS REGARDING PHISHING:

Punjab National Bank v. Poona Auto Ancillaries Pvt. Ltd. (2018): In the instance of Poona Auto Ancillaries, it is said that the police department's indifference towards phishing and other forms of cyber frauds contributed to the loss of more than Rs. 45 lakhs. As a consequence, Police Department of the state of Maharashtra has been instructed by the High Court of Bombay, to provide specialized training to all its members who really are part of the department's cybercrime units. Law enforcement officials in some Indian states are reportedly doing a good thing by expanding their reliance on commercial cyber forensics firms to enable

[15] Information Technology Act, 2000, Section 66A, Acts of Parliament (India)
[16] Information Technology Act, 2000, Section 66C, Acts of Parliament (India)
[17] Information Technology Act, 2000, Section 66D, Acts of Parliament (India)
[18] Information Technology Act, 2000, Section 81, Acts of Parliament (India)

them to cope with cybercrime. It was acknowledged, though, because trusting a private firm with confidential data may be challenging, giving law enforcement agencies further incentive to develop a talented squad of cyber security professionals.[19] For combating cyber security threats like phishing, Indian government has formed a central organization called the Indian Computer Emergency Response Team (CERT-In). As per their annual report of 2018, CERT-In handled 208456 incidents, 454 of which were phishing attempts. During the 2020 global COVID-19 pandemic, CERT-In also issued a warning regarding the possibility of a phishing attack. Based on their research, the authors think CERT-In could conduct similar grassroots education campaigns to increase public knowledge of cybercrimes like phishing. This will encourage individuals to be more circumspect when sharing private information.

Shreya Singhal v. Union of India (2015): The Indian Supreme Court held that Sec. 66A of the IT Act, 2000 is invalid in this instance. Claimants stated that Article 66A violated Article 19(2) of the Constitution of India because it was too broad and did not provide enough security against harassment, fear, threat, obstacle, humiliation, harm or ill will.[20] Supreme Court ruled that there is no legitimate exception than the right to freedom of speech that would allow for the restriction of spreading content via a computer system or communications system with the aim to harass, embarrass, or humiliate. The court also ruled that the section's reach was just too wide as well as it was vague, and also that "a large amount of protected and harmless expression" may be restricted since the law did not define words such as discomfort or annoyance.

National Association of Software and Service Companies vs. Ajay Sood & Others, (2005): National Association of Software and Service Companies vs. Ajay Sood & Others, was decided in 2005 by the High Court of Delhi, which ruled that phishing through the internet is illegal. There had been a study done on cybercrime. The Indian court characterized phishing as "a kind of online fraud where an individual pretends to be a genuine entity, like a bank, in order to steal private information from such a user, including passcodes, usernames, as well as other confidential data." Details on an individual that has been fraudulently gathered is often used to the collector's advantage. As even the Delhi HC put it, "a false representation made in the context of commerce, leads to misunderstanding about the origin and source of an electronic mail, resulting in severe injury and harm, not just to the customer, as well as to the individual whose login information and identity has been misused," phishing has been generally illegal

[19] Punjab National Bank v. Poona Auto Ancillaries Pvt. Ltd., 2018 SCC Online TDSAT 937
[20] Shreya Singhal vs Union of India, AIR 2015 SC 1523

although there's not any specific law that explicitly prohibits and criminalizes it. Phishing was found to be an act of deception and impersonation that damages the Plaintiff's reputation. The petitioner in this case was NASSCOM (National Association of Software and Service Companies), the biggest software trade group in all over India. The accused had been in charge of a placement agency that conducted executive search and recruiting. In order to acquire sensitive information that they may abuse for executive search purposes, the defendants produced and then they sent emails to persons using the name of NASSCOM.[21]

The HC acknowledged the petitioner's trademark protection and rights as well as it imposed an ex-parte ad interim injunction preventing the respondents from ever using brand names or another name that is suspiciously identical to NASSCOM. Additionally, the court ordered that the accused could not represent themselves as members of NASSCOM. The court appointed a special team to execute the warrant to search at the respondents' home. Two of the computers through which the accused issued phishing electronic mails were seized, and their hard disks were turned over to the local commissioner designated by the court. After locating the troublesome electronic mails on the hard discs, they were submitted as proof. It had become evident throughout the cyberlaw trial in India that the respondents, under whose names the infringement-related emails have been sent, were created people formed on the respondents' instructions through a worker to avoid discovery and law suits. False identities were taken off the record of respondents in the lawsuit when the false and fraudulent deed was found.

The accused admitted their unlawful activities, and the parties struck a resolution in court. The respondents somehow agreed to cover the petitioner Rs1.6 million for the trademark infringement. The hard discs obtained from the respondents' property have also been ordered to be given to the petitioner. This trial reaches two benchmarks: it puts "phishing" under Indian law, regardless of the absence of explicit legislation, and so it debunks the misconception that India has no "damages culture" for IP infringement. This ruling reinforces Intellectual Property owners' trust with in Indian judicial system's competence and commitment to protect intellectual property rights and sends a strong message that they may conduct operations in India without sacrificing their Intellectual Property rights.

[21] National Association of Software and Service Companies v. Ajay Sood, 2005 SCC Online Del 402

SOME REAL-LIFE INSTANCES OF PHISHING

The Target/ FMS Scam: One of several biggest incidents of phishing was the Target data breach that affected 110 million consumers and exposed 41 million retail card accounts. Though the incident received less coverage from the media, all of the investigation's conclusions now are public. Since it seems that the, hackers did not launch a direct assault against target. FMS (Fazio Mechanical Services) which is a third-party HVAC provider having authorized access to Target's network, was the intended victim[22]. Upon compromising FMS, getting full access to Target's servers was simple. There should be someone in your company who evaluates whether or not the benefits of maintaining a trusted link outweigh the risks.

The Ukrainian Power Grid Attack (2015): During the month of December in 2015, there was a cyberattack on Ukraine's electrical power system marked a turning point in the nation's history. Once again, malicious software was developed with the sole intention of damaging machinery and equipment; the very first instance was already in 2009, when the Israel and United States used Stuxnet to disable nuclear centrifuges of Iran. The Ukrainian harmful software assault, in contrast to Stuxnet, reportedly initiated by a phishing electronic mail. Intelligence of cybersecurity in Russia gained access to the information and data of the power plant, and infrastructure for months prior to the assault, allowing them to carefully prepare each step of the operation.[23] If hackers can write malicious software for individual nodes in a power grid, they could theoretically take control of every device connected to the same network, such as refrigerators, printers and even an aero plane. This massive cyberattack was triggered by a small mistake committed by an individual at the power facility. If widespread phishing protection and education had been in place, this whole thing could have been prevented.

Reserve Bank of India (RBI) Phishing Scam (2012): Hackers have made an unprecedented effort at phishing the RBI which stands for Reserve Bank of India. An e-mail claiming to be by the Reserve Bank of India lured unsuspecting members of the general public with the offer of a reward which was more than 10 lakh rupees within a span of 2 days, once they followed a link to a site designed to seem identical to the Reserve Bank of India's main website, down to almost the identical URL as well as the branding design and the logo. The next step requires a

[22] Kevin McCoy, Target to pay $18.5M for 2013 data breach that affected 41 million consumers, USA Today, (May. 23, 2017, 4:10 PM), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

[23] Joe Tidy, Ukrainian power grid 'lucky' to withstand Russian cyber-attack, BBC, (Apr. 8, 2022) https://www.bbc.com/news/technology-61085480

user to provide sensitive data like the bank account credentials or password credentials. However, a notification about the phishing attack was posted on the Reserve Bank of India's website. The RBI has issued repeated warnings to the people regarding fraudsters posing as RBI officials and stealing money from the public. Scammers use forged emails and Reserve Bank of India's address labels appearing to come from Reserve Bank of India's personnel to deceive the public into thinking they have won a lottery or are eligible to receive large sums of cheap foreign currency.[24]

Operation Phish Phry(2009): In 2009, the Federal Bureau of Investigation launched an operation known as "Operation Phish Phry," which has been called the largest global phishing operation to date. Numerous people who use debit and credit cards were tricked by e-mails that seemed legitimate but really directed users to malicious links and websites. The targets' account usernames, passwords and other details were easily accessible to the hackers since they had been entered into fake pages. The fraudsters had a really tight operation. Former director Robert Mueller used it to show that massive criminal organisations were unrecognizable from country actors when it comes to aggressive, widespread cyberattacks.[25] Until the inquiry is over, it is impossible to know about the real culprit. From the start, it was obvious that Phish Phry would be a huge operation. Almost one hundred persons were prosecuted by the FBI, and with the help of security officials from Egypt, about 50% of them were captured outside of the United States.

CONCLUSION

Phishing is a huge issue all over the globe in the context of the existing state of e-commerce, and this will continue to be a problem for as long as new web users lack knowledge as well as awareness. Phishers often take use of people's weaknesses in combination to the technical advancements they possess.[26] It's possible that an individual's vulnerability towards phishing might be impacted through various characteristics such as their gender, dependence towards the internet, age, anxiety of the user, and several other aspects. In the meantime, the objectives of phishing have evolved to include not only the theft of personal data and the commission of economic fraud, but also cyberattacks, hacktivism, reputational damage, cyberwarfare, and

[24] Reserve Bank of India,https://www.rbi.org.in/commonman/English/Scripts/PressReleases.aspx?Id=2440 , (last visited Jul. 20, 2022)
[25] Federal Bureau of Investigation, https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709 , (last visited Jul.20, 2022)
[26] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, Frontiers, (Mar. 19, 2021), https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

government funded cyber-attacks. Scams involving phishing are growing more complex, employing both conventional and innovative methods. Phishing scams that operate via various social media sites have also become more common in recent years. As a result, in order to effectively address the "phishing" issue, it is necessary to take into consideration measures that are both preventative and corrective in nature. In order to effectively combat the danger posed by phishing, enforcement agencies, the government, and the private sector should all work together. Phishing attacks should be avoided at all costs, and their consequences should be mitigated as much as possible by keeping cybersecurity via constant training. In order to combat these attacks, it is essential to develop anti-phishing technologies that are able to shield users from becoming the target of the attack.