Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 43 No. 4 (2022)

Impact of Phishing Activity on Youth: A Study in Srikakulam District of Andhra Pradesh.

[1]Dr. U. Kavya Jyotsna, [2]Miss. G. Naveena, [3]Dr. Ramana Yadla

[1]Assistant Professor, Department of Social Work, Dr. B.R. Ambedkar University, Etcherla - 532410, Srikakulam, Andhra Pradesh, India.
[2] Research Scholar, Department of Social Work, Andhra University, Vishakapatnam - 530003, Andhra Pradesh, India. [3]Research Investigator, Population Research Centre, Andhra University, Visakhapatnam – 530003, Andhra Pradesh, India.

Email: [1]kavyamunny@gmail.com, [2]navehema678@gmail.com, [3]yramana1986@gmail.com.

Abstract: During Pandemic, there was a significant raise in online purchases that enabled the hackers to launch a series of fake logistic attacks, posing as delivery firms like UPS or DHL Similar patterns were seen occurring during the Christmas, Sankranti/Pongal holidays every year. Keeping these facts in view, the present study focused on phishing attacks on festive changes. The qualitative study developed semi structured interview schedule and adopted snow ball sampling technique to collect data. Data was analyzed using manual content analysis. The study reveals that the Phishing attacks increased during festive season due to excessive time and online access to shopping.
Keywords: Cyber Crime, Students, Climate changes, Festive season.

1. Introduction

Criminality is a global phenomenon. With the advancement of time and development of knowledge and technology, complexities of life have multiplied with the result that may anti-social elements think it profitable to embrace criminality as a profession. Based on this, usage of internet is vastly increased. Nowadays due to the development of internet does, not only give a positive impact but also gives anegative impact in the form of cybercrime. Cybercrimes are any crimes that involve acomputer and a network. Similarly, the computer may have been used in order to committhe crime, and in other cases, the computer may have been the target of the crime. The rampant use of the internet coupled with almost perpetual digital illiteracy has given a rise to increasing cybercrimes. These Cybercrimes include extortions like ransom ware, online frauds like phishing, exploitations like hacking, and much more. Phishing has been making an enormous impact on data privacy. Phishing falls under social engineering attacks. In phishing, the confidential data of an individual, group, or organization is obtained through online fraud. When an individual or a group, commonly known as a hacker(s) steals confidential information by claiming to be a genuine organization, individual, or group, then it is called phishing. For example, when there was a global increase in online purchases during the pandemic, attackers launched a series of fake logistics attacks, posing as delivery firms like UPS or DHL Similar patterns are seen occurring during the Christmas, Sankranti holiday season every year. Phishing emails and SMS messages use the hook of late deliveries or meal booking services, with people more likely to be ordering gifts and going to restaurants during the holidays. Keeping these facts in view, the present study focused on finding the impact of phishing attacks during festive season.

Most cybercrimes are committed by cybercriminals or hackers who want to make money. For many, festival events provide a chance to reconnect with family and friends by hosting festivities and quality time. Yet, unfortunately, not everyone views seasonal events in the same manner. For cyber-criminals, they are seen as an opportunity to execute pertinent attacks. On behalf of the cyber-attacks,present studies discuss about the phishing attacks. Children are the most vulnerable sections of society and are easily exploited in the cyber world due to lack of maturity level and heavily rely on networking sites for social interaction. Children often unknowingly or deliberately share personal information without realizing that by just forwarding this message they can be made to suffer penal charges.

Phishing attack:

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine. Phishing is a common type of cyber-attack that everyone should learn about in order to protect themselves.

Types of Phishing:

1. **Deceptive phishing:** Deceptive phishing is the most common type of phishing. In this case, an attacker attempts to obtain confidential information from the victims. Attackers use the information to steal money or to launch other attacks. A fake email from a bank asking you to click a link and verify your account details is an example of deceptive phishing.
2. **Spear phishing:** Spear phishing targets specific individuals instead of a wide group of people. Attackers often research their victims on social media and other sites. That way, they can customize their communications and appear more authentic. Spear phishing is often the first step used to penetrate a company's defenses and carry out a targeted attack.
3. **Whaling:** When attackers go after a "big fish" like a CEO, it's called whaling. These attackers often spend considerable time profiling the target to find the opportune moment and means of stealing login credentials. Whaling is of particular concern because high-level executives are able to access a great deal of company information.
4. **Pharming:** Similar to phishing, Pharming sends users to a fraudulent website that appears to be legitimate. However, in this case, victims do not even have to click a malicious link to be taken to the bogus site. Attackers can infect either the user's computer or the website's DNS server and redirect the user to a fake site even if the correct URL is typed in.

Phishing attack statistics:

Roughly 15 billion spam emails make their way across the internet every day, which means that spam filters are "working overtime" and are liable to permit malicious phishing attack emails to slip through. In 2021, 83% of organizations reported experiencing phishing attacks. In 2022, an additional six billion attacks are expected to occur. Last year, roughly 214,345 unique phishing websites were identified, and the number of recent phishing attacks has doubled since early 2020.Thirty-percent of phishing emails are opened. This increases the probability of an individual unintentionally clicking on a malicious link or downloading a compelling-looking document that's laced with malware. Forty-two percent of workers self-reported having taken a dangerous action (clicked on an unknown link, downloaded a file, or exposed personal data) while online, failing to follow phishing prevention best practices. One in 99 emails is a phishing attack. If a <1% attack rate doesn't scare you, the fact that 25% of these emails manage to make their way into Office 365 inboxes just might. Office 365 represents one of the most commonly used email clients, with 60 million commercial users, and 50,000 small business customers worldwide.Roughly 90% of data breaches occur on account of phishing. According to the US Federal Bureau of Investigation, phishing attacks may increase by as much as 400% year-over-year. Roughly 65% of cyber attackers have leveraged spear phishing emails as a primary attack vector. When asked about the impact of successful phishing attacks, 60% of security leaders stated that their organization lost data, 52% experienced credential compromise, and 47% of organizations contended with ransomware.When it comes to phishing attack remediation, IBM's 2021 Cost of a Data Breach Report found phishing to be the second most expensive attack vector to contend with, costing organizations an average of $4.65 million. In more eye-opening phishing attack statistics, although 93% of organizations measure the cost of phishing attacks in some way, only 60% of such organizations offer formal cyber security education to their users.In relation to phishing, the most heavily targeted sectors have historically included financial institutions, social media enterprises, SaaS/webmail services, and retail vendors.(www.aag.com)

Starting in 2016, cyber attackers staged malware and conducted spear phishing attacks in order to gain remote access into the US energy sector's systems. After gaining access, nation-state threat actors managed to move laterally and to collect information pertaining to Industrial Control Systems. According to the Swiss Cyber

Institute, LinkedIn phishing messages represent 47% of all social media phishing attempts. Eighty-four percent of US-based organizations state that security awareness training has lowered phishing failure rates.

Cybercrime in Andhra Pradesh:

A total of 52,974 cases were registered under Cyber Crimes, showing an increase of 5.9% in registration over 2020 (50,035 cases). Crime rate under this category increased from 3.7 in 2020 to 3.9 in 2021. During 2021, 60.8% of cyber-crime cases registered were for the motive of fraud (32,230 out of 52,974 cases) followed by sexual exploitation with 8.6% (4,555 cases) and Extortion with 5.4% (2,883 cases). (Times of India and NCRB Report)

2. Review of Literature:

When Kiren et. al (2016) presented a review on *different types of phishing attacks and detection techniques.*Also, they presented some *mitigation techniques of phishing*. The paper proposed that 100% accuracy to detect phishing can be made possible by using machine learning approach among all other antiphishing approaches.

Belal Amro (2014), presented*types of phishing attacks in mobile devices and different mitigation techniques and anti-phishing techniques*. Also, they provided important steps to protect against phishing in mobile systems. The paper highlighted that current anti-phishing techniques have some shortcomings which makes them less efficient in detecting phishing attacks.

A book published by the Neeraj Kumar Gupta on *criminology*, statescybercrime increases day by day.

Dr. Akash deep et al, (2012)presented that *Phishers and Cyber attackers continue to bring new strategies and tactics that are difficult to track the Cyber-attacks*like Phishing attacks, Whaling and Spear Phishing.

Margaret S, Geoff A, Mark K. (2010; 4-49) in his article "*students attitudes towards the use of the internet for learning: A study at a University of Malaysia"*, states that "The phishing campaign is expected to use malicious emails under the pretext of local authorities in charge of dispensing government-funded Covid-19 support initiatives. Such emails are designed to drive recipients towards fake websites where they are deceived into downloading malicious files or entering personal and financial information," said CERT-In, in the advisory asking the public to refrain from opening unsolicited emails, attachments and sharing private information.

"*Threat actors use social media for phishing attacks because it's a low-effort and high return way to target billions of people around the world*," said Darren Shou, head of technology, Norton LifeLock.(https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html).

UNICEF estimates that more than four million websites showing juvenile victims, even children younger than two years, can be found on the Internet (Cehovin, 2010). The experience of abuse causes longterm effects on a person's later life, both physical and psychological. The latter includes feeling of guilt or responsibility for the abuse, low self-esteem, feelings of inferiority and depression. With Internet pornography, one has to realize that the child is victimized each time anybody watches material depicting his/her sexual abuse. Due to the ease of disseminating materials on the web and the impossibility of removing material once it is published, it is very difficult to stop the circle of abuse (Dimc & Dobovsek, 2012). UNICEF estimates that more than four million websites showing juvenile victims, even children younger than two years, can be found on the internet (cehovin, 2010).

3. Objectives of this study:

- To understand that cyber-attacks such as Phishing are increased during festive seasons.
- To understand the reasons for rampant phishing attacks during festive seasons.
- To understand the type of Phishing attacks are prominent currently.
- To understand whether the Youth (x standard students) are more vulnerable to Phishing attacks.
- To understand the Government measures to prevent these attacks.

4. Research Methodology:

This survey is the short survey on understanding the occurrence of Cyber Crime –phishing on X standard students during climate changes in festive seasons. This study is conducted in urban schools in Srikakulam district. Initially, it was concepted that data to be collected from both boys and girls, however after interacted with the students orally; it was found that girls are more vulnerable to the phishing attacks rather than the boys. Hence, Using Snowball Sampling Technique 20 girl students were interviewed. The main instrument for data collection included the use of in – depth interview. The in-depth interview guide consisted of set of questions that elicit responses on the student's socio-economicbackground, category and method of phishing experience, seasonal implications on attacks etc. The information obtained is analyzed using manual content analysis.

5. Discussions:

1. **Caste:** As per the results, 99% Students belong to the OBC category, remaining 1% people belongs to the SC category. Area of research was based on urban community, in this area most of the Students belonged to same caste due to the hereditary, past relationships, work preferences etc.

2. **Religion:** The Study shows that, 98% of the Students follow the Hindu religion. Remaining 2% of the Students follow the Christianity

3. **Occupation:** The Study shows that, 40% of respondent's fathers are self-employed like auto drivers& mason, 10% of them are businessman,10% areGovernment Employees and Remaining, 40% are Farmers.

4. **Family Size:** The Study shows that 80% of the family consists of four members,10% consists of five members and 5% consists of 3 members and 5% consists of 6 members. Due to the work preferences, children education, life style, individuality family size is decreased.

5. **Living area:** The Study shows that 65% Students belongs to urban area; remaining 35% belongs to rural area

6. **House hold income:** The study shows that Students belong to middle and above middle class because house hold income is mostly based on their jobs. Fathers of students are depending on selfemployment.earning income was low. Their income is sufficient for their daily Expenditure and Hospital expenses. There is less amount in Savings. That's why people belong to middle and above middle class.

7. **Availability of mobile:** The study reveals that all children have mobile phones. On that, 80% of the children's family members have more than one android phone.20% of people have both android and keypad mobile.Due to the effect of covid-19, parents gave mobile phones for study purpose.Schools forced the parents to buy mobiles for online class.

8. **Mobile purchase:** The study reveals that70% of the children have mobiles before covid.30% purchase mobile phones during Covid for online classes.

9. **Awareness of usage of mobile:** The study reveals that,all are aware about how to use the mobile. Due to the availability of mobile phones, educational changes, living environment, parent's mobile usage, parents gave mobile phones to make them stick in one place, to focus on studies, for making children not to disturb their studies by these incidents children always use mobile phones and they are well aware of it.

10. **Mobile network:** The study reveals that, most of the students use Airtel, Jio and some students use BSNL.Having Jio and Airtel Sim cards because of unlimited network, unlimitedcalls, and good network connections.

11. **Time usage on mobile:** The study reveals that, after school hours they use mobile up to 4 hours per day. Full day spending on schools, students need refreshment so they use mobile phones after school hours up to bed. During holidays they use 6 hours per day as per the availability of mobile phones.

12. **Social media accounts:** The study reveals that, 90% students have whatsapp,2% have Facebook,5% have instagram and remaining and 3% doesn't have any social media accounts.

13. **Most used social media account:** The study reveals that, 98% have used Whatsapp and 2% used Instagram for long time. Whatsapp was the social media which has easy access with free of cost due to the availability conditions most of the students were attracted to the social media accounts and they use WhatsApp highly.

14. **Awareness on cybercrime:** The study reveals that, only 40% of students have an idea about cybercrime and remaining 60% of students unaware of it.

15. **About cybercrime:** A Student said that, "They think cyber-crime is a crime related to the bank loans, kyc loans only". Another Student said that, "cyber-crime affected to the mobile phone which was mobile hacking, face bookhacking, messages etc."Some of the students said that, getting wrongcalls and messages from unknown contacts.

16. **Attack by cybercrime:** The study reveals that, 80% of students are attacked by the cybercrime, they received messages from unknown numbers regarding bank loans, kyc, gaming websites, amazon gifts etc.

17. **Types of cybercrime attacks:** The study shows that, Fake Emails, Wrong calls, Kyc loan messages, URL's for Amazongifts, messages through WhatsApp like play games and win money etc. are the types of cybercrimes faced by the students.

18. **Period of time for attacks:** The study shows that, during month of January, May and December are the main timings where an attack takes place highly.

19. **Reasons for cyber-attack:** On the student perspective, main reasons for their cyber-attacksare, clicking unknown links, login to fake websites with their mobile numbers and passwords. Entering emails in the gaming websites is the main reason for phishing attacks.

20. **Mental condition during attacks:** The study shows that, Cyber victim students said that they are very stressful due to these attacks. They are not interested in studies. They were scolded by elders.

21. **Support:** The study shows that, their siblings supported them and they help them to come from that situation. 98% of the students said that their siblings help them to come out of it. Only 2 % of students had to face it by their own because they don't have sibling.

22. **Remedial measures what victim thinks:** The Study reveals that, they need more seminars and awareness sessions (98%) to them about cybercrime. They need much information regarding the problems faced by Cybercrime and how to get out of it.

23. **Government measures:** Students are less aware of the government measures.98% of the students don't know about it. Remaining 25 % know about it but they are not giving information properly due to the communication gap.

6. Results

The study shows that, one thing is to be noticed that seasonal changes also effects the cybercrime because all schools have declared holidays in the festival timingslike Pongal, Summer, Dussehra and Christmas. These are the main festive seasons with high number of holidays. Children are attracted to the mobiles during these seasons. They are playing games, chatting with friends in WhatsApp, Facebook, Instagram etc.

The study shows that, some of the mobile networks provide unlimited access of internet perday this causes high usage of mobiles and internet. Parents have less supervision in usage of mobiles during holidays. Mostly, childrenattracted to the social media accounts like Instagram, Face book,they follow the unknown persons and gave personal details and turned as victims. By forwarding messages like Amazon gifts in festive seasons, they click on the links and attacked by the cybercrime. Playing online games and click on links which leads to data theft.

Covid also one of the reason for the cybercrime because children have online classes during covid pandemic. So, parents purchase mobile for children. this cause for the attraction towards mobiles, this leads to the increasingof using mobiles. And also, children use their sibling's mobiles during their free time and use their sibling's social media account which leads to clicking of unknown websites, links unknowingly leads for cyberattack.

During working days, students use mobile up to 4 hours on an average. In this context, during holidays students may be or might be they use up to 7 hours per day.

Government measures:

According to the Information Technology Act 2000,provides legal framework to address various types ofcrime and prescribes punishment also such crimes. Under Section 66 IT Act, describes that "If a personchanges by way of deletion of record or alterationof electronic information or data in the account ofvictim residing in the server." Under section 66C IT Act, describes that "If aperson disguises himself as anorganization such asbanker and uses the unique identifying feature of anorganization like Name and Goodwill, Logo etc." Under Section 66D IT Act,describes that a person through the use of the electronic mail containing the link to the replica web page of real website to cheat upon the innocent persons.These are the government measures but people are less aware of it.

Remedial measures:

There is lot of communication gap between government and people regarding cybercrime acts to eradicate this, seminars, workshops regarding cyber-attacks, cybercrime portal, toll-free number, types of cybercrimes, occurrenceetc. will be conducted.

7. Conclusion

Phishing attacks are among the major cyber-attacks that take place in India. Phishing is a practice to collect sensitiveinformation by luring people. Phishing is one of the most treacherous cyber-attacks that take place in organizations,personal devices, etc. The criminals who carry out these attacks are hard to catch. This is due to many inexperiencedand unsophisticated users. Though technologies are advancing for phishing detection, but users also have to take someawareness to protect themselves. Whenever there is an email or any message from an unknown sender, do not react toit, checking the URL before entering your personal details on any website, if theURL is suspected then don'tuse thesite, while doing something on any website checking the digital certificate, not forwarding the message withoutverifying, all these are some of the ways to keep yourself and others safe.This study shows clearly that Phishing is aneasy method of stealing someone's information due to their lack of awareness. The present study suggests that it's imperative to provide awarenessabout the problems that cause phishing and the solutions to phishing attacks that is one of the biggest threats to digital information.

References

[1] Aggarwal G, 2015, (5(8)) General Awareness on Cyber Crime
[2] Ayo E,2010, (P. 28-50) Convergence and Policy Issues in ICT sector.

[3] Chiemeke B,2012, (22(1):3-23) A security beget insecurity? Security and crime prevention awareness and fear of burglary among university students. The East Midlands.
[4] Crime in India,2011. National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.
[5] Cyber Talk ,2021,Phishingattack Statistics.
[6] Government India, Income Tax Department, 2016, Feb 05, Phishing report.
[7] India Risk Survey,2015, Phishing activity trends report.
[8] Jaishankar K,2007,(1(2):7-9) Establishing a Theory of Cyber Crime.
[9] Margaret S, Geoff A, Mark K,2010,(6(2):4-49) A Students' attitudes towards the use of the internet for learning.
[10] Mehta S, Singh V ,2013, (4(1)) A Study of Awareness about Cyber laws in the Indian Society.
[11] NCRB Report ,2020,Tabular Data.
[12] Ofoegbu T,2007, Internet as a source of Knowledge Generation for Students in Higher Institutions in Nigeria.
[13] Okpala G,1998, (1(3):237-244) The role of self-control in college students' perceived risk and fear of online victimization.
[14] Pubilshed by the CISCO, Conduct awareness on the cyber crime [15] Reserve Bank of India, 2014, Phishing Email.
[16] Shivani Singh,2020, (6(3):264-267) International journal of home science.
[17] Shreeram V, Suban M, Shanthi P, Manjula K,2010, Anti-phishing detection of phishing attacks using Genetic Algorithm.
[18] Timesof India, 2021, Latest report on Phishing attacks in India.
[19] The Economic Times,2013,Phishing report
[20] Young, Kimberly,2012, (33(2):223-233), American Journal of Criminal Justice.