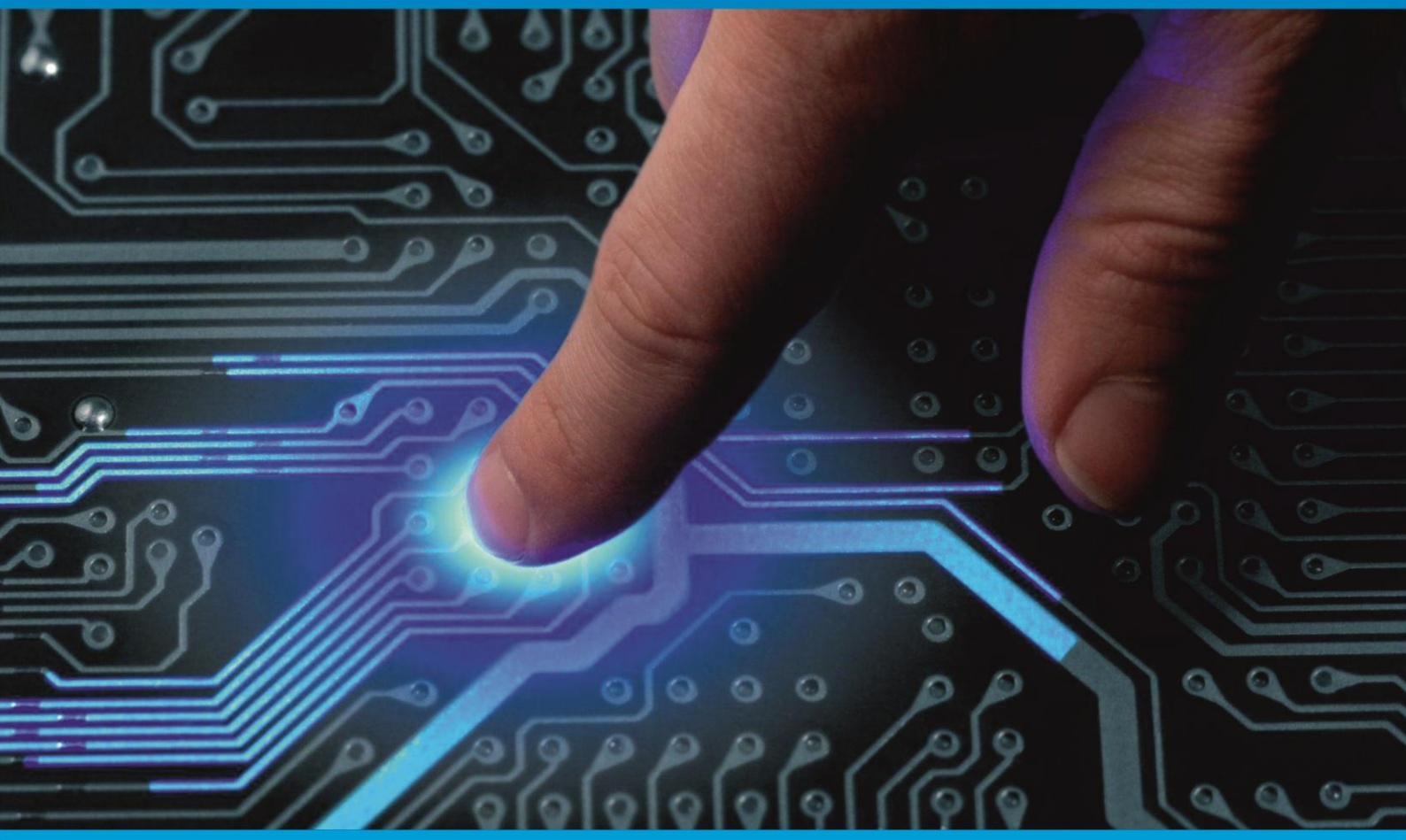
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 10, October 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

Phishing Methodologies Used to Grab User Credentials

Varun Herlekar

UG Student, Dept. of Computer Engineering, Government College of Engineering Yavatmal, Maharashtra, India

ABSTRACT: Phishing is a well-known cybersecurity attack that has rapidly increased in last few years. It poses legitimate risks to businesses, government agencies, and all users due to sensitive data breaches, subsequent financial and productivity losses, and social and personal inconvenience. Often, these attacks use social engineering techniques to deceive end-users, indicating the importance of user-focused studies to help prevent future attacks.Although numerous tools have been created to aid people in recognizing phishing attacks, users disregard the recommendations of these tools. This paper summarizes the core of phishing research, provides an update on trending attack methods, acredibility in a phishing context.

KEYWORDS: Phishing, Phishing Attacks, Social Engineering, Authentication

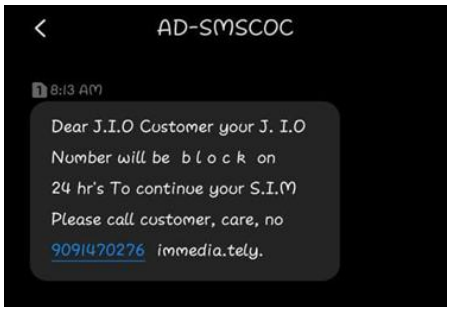
I. INTRODUCTION

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.(phishing.org) Kay et al. report that the term "Phishing" originated in 1996, when hackers were stealing online data from American accounts. These hackers used emails as “hooks” to catch their "fish" from the “sea” of internet users. Today, there are a number of known types of phishing attacks, such as Deceptive Phishing, Malware Based Phishing, Key loggers and Screen loggers, Session Hacking, Web Trojans, Spear Phishing, Search Engine Phishing, Content Injection Phishing, DNS-Based Phishing, and Vishing.

II. FUNCTIONING

A person who engaged in malware activities is called a *phisher*.Phishing attacks today are majorly working by frightening users and creating fear in their brains – a common example is “*we need you to update your e-wallet KYC or your account will shut down permanently*”. The method used by phishers is usually to make fake websites, similar to the original site by duplicating the source code containing the same graphics, texts, buttons etc. In some cases, phishers purchase a similar domain name to the original website of a company or an organisation, for example, Original Site Domain: “*paytm.com”*Phishing Site Domain: “*patym.com”*. The common & simple method used by phishers is developing forms, for example, a form for password validation.

A phishing attack could target many kinds of confidential information, such as social media credentials, bank account details and other personal information. A phishing attack is to obtain a victim's information by sending a simple link or a contact number via an email or text message.



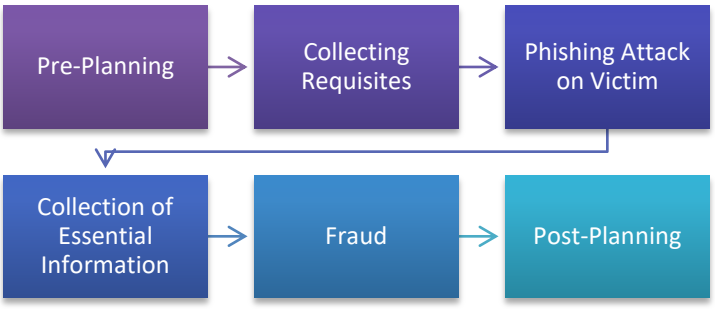
Phishing attacks are carried out in 6 steps:

- Pre-Planning

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

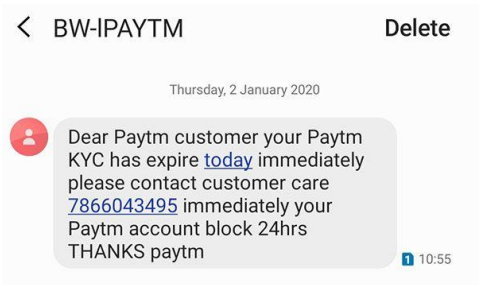
- Collecting Requisites
- Phishing Attack on Victim
- Collection of Essential Information
- Fraud
- Post-Planning



Phishers create a complete working attack plan, generates the attack code/message and sends to the target user. A suspiciousemail arrives at the victims site. The victim reads the message and takes some action which makes him or her vulnerable to adata breach. The user is then prompted for information through a trustworthy looking website. The user reveals his confidential information. The confidential information is transmitted from a phishing server to the phisher. The phisher engages in fraud using confidential information to impersonate the user.

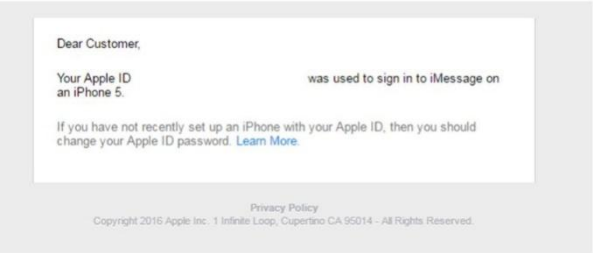
III. CATEGORIES OF PHISHING

1. Vishing:
   Phishing done over phone calls. Since voice is used for this type of phishing, it is called vishing. *(voice + phishing = vishing).*During a vishing phone call, a phisher uses social engineering to get you to share personal information and financial details, such as account numbers and passwords. The scammer might say your account has been compromised, claim to represent your bank or offer to help you install software.



2. Smishing
   SMS phishing or Smishing is one of the easiest types of phishing attacks. The user is targeted by using SMS alerts.In Smishing, users may receive a fake password change links or fake order detail with a cancellation link.The link would actually be a fake page designed to gather personal details.

3. Spear-Phishing
   It involves sending emails to thousands of unknown users, the emails are carefully designed to target a particular victim.These attacks have a greater risk because phishers do a complete social profile research about the user and their organization through their social media profile and company website and other open sources. Out of the different types of phishing attacks, Spear phishing is the most commonly used type of phishing attack.



IV. CASE STUDIES

DMART VOUCHER SCAM

Supermarket chain D-Mart has warned against spam messages promising discounts from the store. A week after messages about D-Mart giving away free vouchers worth Rs 2,500 went viral on social media, the grocery chain registered an FIR with theMumbai police station on June 11 2018 and warned customers. The police, on its part, registered a complaint under section 66 (C) of the Information Technology Act against unknown person/s.

AYUSHMAN BHARAT PHISHING SCAM

The Ayushman Bharat phishing attack uses the Indian government's free health coverage scheme to attack users. In this, a message is forwarded with the message that '10-crore people between the age of 13 -70 years are being provided with free insurance worth ₹5,00,000 to cover the Covid-19 pandemic.'

V. CONCLUSION

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money).Phishers continue to be successful as their attack methods are constantly evolving and users frequently disregard the recommendations provided by expert systems. Here are some awareness points:

- Organizations have their own domain and do not use public domains to send emails to their customers. If you receive an email from a company with a public domain (@yahoo.com at the end), avoid clicking on any links or attachments.
- Stay alert when you see a shortened URL, bad actors use this trick to make the attack look more legitimate.
- Do not enter personal information in pop-up screens. Companies generally do not use pop-up screens to ask for user information.
- Check the email or message for spelling mistakes, unusual phrases and discrepancies in the domain name.
- Even if you mistakenly visited such a malicious website, that potentially attacked your credentials, immediately change your password and enable two-factor authentication.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

REFERENCES

1. Urvesh Thakkar,'Modernized Homoglyph URL Attack byHackers to Steal User Credentials',International Journal of Innovative Research in Computer and Communication Engineering, Vol.8, Issue 5.
2. https://economictimes.indiatimes.com/topic/India-phishing-attack/news
3. https://thecyberagents.com
4. https://mumbaimirror.indiatimes.com/mumbai/other/dmart-hit-by-free-voucher-hoax/articleshow/64655335.cms
5. https://www.businessinsider.in/tech/news/what-is-phishing-attack-and-checkout-the-examples-of-phishing-attacks/articleshow/76545843.cms

BIOGRAPHY

Varun Prasad Herlekaris anUnder Graduate Student in the Computer Department, Government College of Engineering, Yavatmal. His research interests are Computer Networks (wireless Networks), Android Technology, Algorithms, Cyber Security etc.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details