International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 03 | Mar 2022 www.irjet.net p-ISSN: 2395-0072

Phishing: Analysis and Countermeasures

Sanjivani Bhumiraj Raut

Student, M. Sc IT, Keraleeya Samajam (Regd.) Dombivli's Model College, Maharashtra, India

---

Abstract – We cannot imagine our daily life without internet. E-Mail is one of the essential media through which we communicate every day. We have a tendency to solely use it daily for official communication however conjointly to be involved with our friends and relatives. As E-Mail plays an important role in communication globally for communication and sharing of information additionally. The security problems even have accrued. the most important downside or the attack on E-Mail by the hackers these days is understood as E-Mail Phishing. it's the correct time to secure the information communicated over mail even on sure network. Cyber criminals craft these emails to seem convincing, causing them dead set virtually millions of people round the world. The criminals don't have a particular target in mind, nor do they apprehend precisely United Nations agency can fall victim. They merely apprehend a lot of emails they channelize, the more people they will be able to fool. during this paper we have a tendency to square measure analyzing the various ways that within which the Phishing is achieved, the attainable solutions and also the awareness at the side of some tips to be away from a victim of Phishing attacks square measure mentioned.

Key Words: Phishing, attacks

1. INTRODUCTION

Phishing is an e-mail fraud technique within which the wrongdoer sends out legitimate trying email in an effort to assemble personal and money information from recipients. Typically, the messages seem to return from well-known and trustworthy websites. A phishing expedition, just like the fishing expedition it's named for, may be a speculative venture: the phisher puts the lure hoping to fool a minimum of a number of the prey that encounter the bait. Phishers use variety of various social engineering and e-mail spoofing ploys to do to trick their victims. As E-Mail plays a significant role in communication globally for communication and sharing of information furthermore. The safety problems even have magnified. The mail infrastructure utilized on the web primarily consists of email server's victimisation SMTP to just accept messages from senders, transport those messages to alternative servers, and deposit them into a user's server-based inbox. additionally, to email servers, the infrastructure includes email shoppers. Users retrieve email from their server-based inboxes victimisation POP3 or IMAP. A consumer communicates with email server's SMTP. Basically, the essential email system isn't secure because the protocols accustomed support email doesn't use coding. Thus, all the messages area unit transmitted within the type within which they're submitted to the e-mail server. Phishing websites is achieved simply by causation a spoofed link. An example of such once users visits a phishing web site then the phishing web site could steal users' personal info or cause drive-by downloads. Here the most drawback we've got to deal with isn't solely the web site phishing however additionally the foundation cause i.e., Email Phishing. This paper can attempt to spot the phishing mail at the utmost level by implementing some additional security layers.

2. HOW PHISHING ATTACKS WORKS

To understand the functioning of a malicious attack, we want to understand the explanations why attackers perform such attacks. There are a unit 2 primary functions of a phishing attack

1) To Extract Sensitive data

These attacks involve processes that force the victims to dispense with their personal and sensitive knowledge. Hackers would like the knowledge to breach a personal or structure network, to steal someone's cash, or to use somebody else's credentials for finishing up unlawful deeds. Some visibly suspicious data that hackers request from victims includes checking account data.

2) To Install Malware into The System

Another primary purpose that hackers accomplish with such attacks is putting in malware or virus into the victim's system. Such emails contain zipped MS workplace files or alternative similar contents that hold the malicious code.

Cybercriminals don't persist with just one methodology for finishing up such attacks. excluding emails, the needs mentioned on top of are consummated through voice decision phishing (vishing), SMS phishing (Smishing), computer programmer phishing, spear phishing, and whaling.

3. STAGES OF PHISHING ATTACK

To stop a phishing attack in is tracks, it's vital to 1st perceive however they work. Let's review the foremost common stages of a typical phishing attack [1]:

Figure 1 stages of phishing attack

- Building the spoof web site.

The hacker scrapes real code and legit pictures from a web site to construct spoof sites. By some estimates, cybercriminals produce 1.5 million spoof sites every month. This can be easier than ever, due to internet scraping tools that area unit on the market to anyone. Typically, hackers build spoof sites supported far-famed and trusty domains. And they're recouping at their craft. Even well-trained security professionals will have hassle characteristic the fakes.

- Sending the phishing email.

Once the hacker builds the spoof website, they then launch associate degree email phishing scam. These extremely convincing emails contain text and pictures and a link to the spoof website. The e-mail urges the victim to click on the link, with directions like, "Your account has been compromised!" This happens on an enormous scale. Hackers send associate degree calculable three billion phishing emails daily.

- Narrowing the seek for a victim

If the emails don't reach the target they're trying to find, the hacker keeps making an attempt their hand at finding the proper email addresses. However, this step could be a little bit of a "guessing game" for the offender.

- Taking the bait.

Sooner or later, if a hacker is persistent, unsuspecting victim steps into the lure. Undetected attack will yield thousands of victims. Sometimes, they need to steal the victim's monetary assets, like credit cards, bank accounts, or a legal document. Others wish to collect as several credentials as attainable to sell on the dark internet and switch a hefty profit. Some adversaries get to reveal or hurt victims by revealing direction to the general public.

4. PHISHING SCAMS TO AVOID

- Spear Phishing Attacks

Spear phishing refers to a lot of customized variety of phishing. In spear-phishing attacks, the hacker seeks to search out the maximum amount as they will regarding you – your name, company, position, number, something they will realize. They then use this information to their advantage to faux to be somebody you recognize and trust, to urge you to perform the requests the assailant asks for.

Example: Amazon is on a worldwide level that all cybercriminals don't have to be compelled to attend abundant effort to trick their users; the majority of phishing makes an attempt generic.

In 2015, an inventive spear phishing attack fooled many purchasers into putting in ransomware. The scammers sent out a dispatch email to users World Health Organization had recently placed associate degree order with Amazon, therefore the email appeared improbably real to them [3].

- Whaling

Whaling may be a style of phishing attack, targeted specifically to those in high positions of power in an exceedingly company. This typically suggests that a chief executive officer, a business executive or another senior-level manager who has access to or information of company sensitive information. The term "whaling" refers to the very fact that the targets area unit the "big fishes" within the phishing pool. Whaling attacks area unit typically particularly well thought of and have the target of gaining sensitive company information for the phisher's gain. Whaling attacks have typically been planned for a protracted time and that they area unit extremely customized and extremely elaborate.

Example: In month 2020, the co-founder of Australian hedge fund Levitas Capital followed a pretend Zoom link that put in malware on its network.

The attackers tried to steal $8.7 million within the event, they solely got away with $800,000. However, the reputational injury was enough to lose Levitas its biggest shopper, forcing the hedge fund to shut [4].

- Pharming

Phishing and pharming area unit other ways of manipulating targets on the net. The article of phishing is to urge the target to grant their information to a faux web site. Pharming includes modifying DNS entries, which suggests that once the user enters an online address, they're going to be directed to the incorrect web site. This implies that a DNS server that's chargeable for translating the web site address into the important information processing address is modified, and also the website traffic is redirected to a

different site. Pharming attacks occur thanks to vulnerabilities in DNS server package, and a pharming attack are often troublesome to notice. The simplest thanks to notice an attainable pharming attack is to lift alarm if a usual web site appearance considerably completely different than it used before. Pharming attacks could have an effect on many folks promptly, thus if you encounter a pharming attack, you must continually apprize of it forward. Even major corporations like Snapchat have fallen victims of pharming attacks.

Example: Many affected within the U.S and Asia thanks to pharming attacks.

A Mexican bank got affected once the DNS of a customer's home routers were modified and that they don't even understand their all knowledge got hacked. Symantec reports that it absolutely was a pharming attack [5].

- Spoofing

Spoofing refers to the gouger motility as somebody else, to urge the target to perform a selected action. several phishing attacks therefore use spoofing – a phisher could create as somebody from your IT department, asking you to travel to an internet site and re-confirm your login details for your laptop. This web site is then a pretend web site, and also the phisher has gained access to your login details while not you knowing something was wrong. several phishers then use spoofing as a way of manipulation, however not all spoofing attacks square measure essentially phishing. A spoofing attack may well be as an example a hacker motility as your co-worker and asking you to transfer a file, however this file is really a trojan or a bit of ransomware accustomed hurt you or your company. However, because the methodology isn't to urge you to present away your personal details, it's not a phishing attack, however another form of crime.

Example: In June 2018, hackers administered a two-day DDoS spoofing attack against the web site of the yank insurance supplier, Humana. Throughout the incident that was same to own affected a minimum of five hundred folks, the hackers have managed to steal complete medical records of Humana's purchasers, as well as the main points of their health claims, services received, and connected expenses [6].

- Vishing

Vishing is that the phone counterpart of phishing, which means that scammers decision the targets to solicit data. Vishers create as a legitimate entity and raise you for your personal data, victimization completely different ways of manipulation or "social engineering". Be terribly cautious of giving any personal data away over the phone, particularly if the variety telephone number is blocked otherwise you don't acknowledge the realm code or number. If attainable, evoke the amount you'll be able to decision back, and check it from the supply they claim to be, or decision the party's client service and raise if they have to contact you.

Example: This type of attack will occur by causation a link that opens a page informing you that a tangle has been detected along with your pc which you would like to decision variety to receive technical support. Another common technique is for the criminal to decision the victim on to alert the victim that there's a tool failure which contact is being created to assist the victim. At the tip of the service, a fee is charged for repairing a tangle that failed to exist at first [7].

5. PHISHING ATTACKS: WARNING SIGNS

A phishing web site (or a spoofed website) typically tries to seem a minimum of somewhat legitimate. It's going to be devised to seem like an existing legitimate web site, and mimic for instance your banks or health care center's web site. The web site is made thus you'd make known your login credentials or different personal data. You're possibly to receive a link to the present web site via email or a moment message, however you may land into the page by mistyping a computer address or clicking the incorrect web site in your search bar. The primary issue is then to be cautious of the sender of the e-mail or instant message and ensure you recognize the sender, or that the sender is who they claim to be.

- Email from unacquainted Sender

When receiving an email, there are a unit many details you'll be able to think again to work out, if you would possibly be targeted for a phishing attack. First, take a glance at the sender's email details. The phishing attack may well be from an email you've got ne'er seen before and which does not appear legitimate. As luck would have it, if you have got doubts, there are a unit forums and on-line resources which may assist you confirm if the supply is reliable or not. Merely copy the sender's email and google it with a keyword like "phishing attempt", "hacking" or "scam". If others have flagged the e-mail, you'll seemingly see that the e-mail is so from a cyber-criminal. There is a unit problem with this system, however, since phishers area unit terribly alert to the forums and alter their emails usually and simply. They will additionally use these facilitate forums as a kind to support their own scam, by giving themselves smart reviews and claiming the e-mail provide was so legitimate [8].

- Sender's Email looks Off

The phishing try may also return from an organization that looks completely reliable and an actual company however is instead not coming back from the corporate it claims to be. For instance, you'll be able to see an email coming back from "sanket.bank@logo.dn" and really hunt a Sanket bank and see that they are doing so work emblem, and assume the e-mail is coming back from a true supply, while not realizing that it may well be that either Sanket's

email has been hacked, or an email has been created to tally Sanket's email, however it's not the right email kind.

- Writing Tone Is Odd

If the e-mail address appearance acquainted however the content or the fashion appearance odd, this is often another massive red flag. If the e-mail is filled with grammatical errors or orthography errors your contact is unlikely create to or does not typically make, it's attainable the sender is, in fact, a phisher. As phishing scams become a lot of refined, their language, similarly as their layout, may additionally be alright thought out and appearance terribly reliable. However, individuals typically have a really distinct sort and elegance of communication, and you're seemingly to require note of it, either consciously or subconsciously. If an email feels "fishy", it may well be that you simply subconsciously detected the sender is employing a vogue and selection of words not usual to them. Trust your instincts and if one thing feels off, investigate the e-mail before responding.

- Greeting Oddly Generic

Phishing scammers send thousands of phishing emails, thus you're seemingly to be greeted with a really generic email, like "Dear Customer", relating "Your Company" or "Your Bank". This is often particularly ominous if the e-mail looks to be coming back from somebody who ought to have a lot of details on you, like somebody from your company or a partner you have got met before [8].

6. PHISHING EMAIL EXAMPLES TO LEARN FROM

1) A Phishing Email Example Where the Sender's Email Address Is Fishy.
2) A Phishing Email Example Where the Scammer Promises Financial Rewards.
3) Phishing Email Example Where You Are Asked to Verify Your Account Details.
4) A Phishing Email Example That Includes Fake Financial Documents.
5) A Phishing Email That Claims to From Someone Within Your Organization.
6) An Example of Phishing Email That Asks for a Payment Confirmation.
7) Phishing Email Examples of Voicemail Scams.
8) Account Deactivation
9) Compromised Credit Card
10) Transfer Funds
11) Social Media Request

7. HOW TO DEFEND AGAINST PHISHING EMAILS

To protect against phishing emails, bear in mind these 5 keys to assembling a cyber secure aware culture:

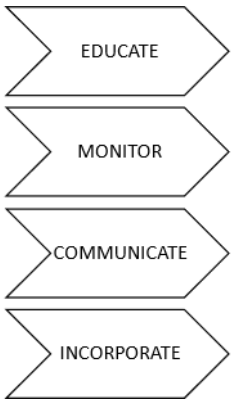

Figure 2. How to defend against phishing emails

- Educate: Use security awareness coaching and phishing microlearning's to coach, train, and alter behavior.
- Monitor: Use phishing simulation tools to watch worker information and determine an agency is in danger for a cyber-attack.
- Communicate: Offer current communications and campaigns concerning phishing emails, social engineering, and cyber security.
- Incorporate: Create cyber security awareness campaigns, training, support, education, and project management a part of your company culture.

You want to be shielded from phishing email attacks. an equivalent sentiment extends to your colleagues, organization, friends, and members of the family. Everybody should be able to keep their data safe

The best thanks to try this is to make optimum levels of cyber security awareness.

8. THE FREQUENCY OF PHISHING ATTACKS

Phishing could be a large threat and growing a lot of widespread once a year. 2021 Tessian analysis found that workers receive a median of fourteen malicious emails. Some industries were hit notably laborious, with retail employees receiving a median of forty-nine.

ESET's 2021 analysis found a 7.3% increase in email-based attacks between May and August 2021, the bulk of that were a part of phishing campaigns and 2021 analysis from IBM confirmed this trend, citing a pair of percentage-

point rise in phishing attacks between 2019 and 2020, part driven by COVID-19 and provide chain uncertainty.

CISCO's 2021 Cybersecurity threat trends report suggests that a minimum of one person clicked a phishing link in around eighty-six of organizations. The company's knowledge suggests that phishing accounts for around ninetieth of information breaches. CISCO found that phishing tends to peak around vacation times, finding that phishing attacks soared by fifty-two in December.

Around eighty-three of IT groups in Indian organizations aforesaid the quantity of phishing emails targeting their workers raised throughout 2020, consistent with the findings of a worldwide survey.

one in all the explanations for its success is its ability to unceasingly evolve and diversify, trade attacks to topical problems or considerations, like the pandemic, and enjoying on human emotions and trust," aforesaid urban center Wisniewski, principal analysis someone at Sophos.

Phishing is commonly the primary step in an exceedingly complicated, multi-stage attack. consistent with Sophos speedy Response, attackers oftentimes use phishing emails to trick users into putting in malware or sharing credentials that give access to the company network," another Wisniewski [2].

The findings additionally reveal that there's an absence of common understanding regarding the definition of phishing. as an example, sixty-seven of IT groups in India associate phishing with emails that incorrectly claim to be from a legitimate organization, and that area unit typically combined with a threat or request for data. Around sixty-one contemplate Business Email Compromise (BEC) attacks to be phishing, and half the respondents (50%) assume threadjacking—when attackers insert themselves into a legitimate email thread as a part of an attack is phishing.

The good news is that almost all organizations in India (98%) have enforced cybersecurity awareness programs to combat phishing. Respondents aforesaid they use computer-based coaching programs (67%), human-led coaching programs (60%), and phishing simulations (51%) [2].

The survey additionally showed that four-fifths of Indian organizations assess the impact of their awareness program through the quantity of phishing-related tickets raised with IT, followed by the amount of coverage of phishing emails by users (77%) and click on rates on phishing emails (60%).

All the organizations surveyed (100%) in metropolis, Hyderabad, and city aforesaid they need cybersecurity awareness programs in situ. This was followed by Chennai wherever ninety-seven have such programs, so Bengaluru and metropolis stood at ninety-six every.

9. CONCLUSION

Phishing attacks stay one amongst the key threats to people and organizations up to now. As highlighted within the article, this can be principally driven by human involvement within the phishing cycle. Typically, phishers exploit human vulnerabilities additionally to pro technological conditions (i.e., technical vulnerabilities). It's been known that age, gender, net addiction, user stress, and plenty of alternative attributes have an effect on the susceptibleness to phishing between individuals. Additionally, to ancient phishing channels (e.g., email and web), new forms of phishing mediums like voice and SMS phishing are on the rise. Moreover, the utilization of social media-based phishing has inflated in use in parallel with the expansion of social media. Concomitantly, phishing has developed on the far side getting sensitive data and monetary crimes to cyber coercion, hacktivism, damaging reputations, espionage, and nation-state attacks. analysis has been conducted to spot the motivations and techniques and countermeasures to those new crimes, however, there's no single answer for the phishing drawback because of the heterogeneous nature of the attack vector. This text has investigated issues bestowed by phishing and planned a replacement anatomy, that describes the whole life cycle of phishing attacks. This associate deprecatory provides a wider outlook for phishing attacks and provides a correct definition covering end-to-end exclusion and realization of the attack.

Although human education is that the best defense for phishing, it's troublesome to get rid of the threat fully because of the sophistication of the attacks and social engineering parts. Although, continual security awareness coaching is that the key to avoid phishing attacks and to cut back its impact, developing economical anti-phishing techniques that stop users from being exposed to the attack is a necessary step in mitigating these attacks. To the present finish, this text mentioned the importance of developing anti-phishing techniques that detect/block the attack. moreover, the importance of techniques to see the supply of the attack might offer a stronger anti-phishing answer as mentioned during this article.

10. ACKNOWLEGEMENT

I am overwhelmed all told humbleness and thankfulness to acknowledge my depth to any or all those that have helped me to place these concepts, well on top of the amount of simplicity and into one thing concrete.

I would like to express my special thanks of gratitude to Asst.Prof. Jyoti Samel who gave me the golden opportunity to do this wonderful research on the topic "Phishing: An open threat to Everyone", which also helped me in doing a lot of Research and I came to know about so many new things. I am really thankful to her. I express my deepest gratitude towards our research paper guide for her valuable and

timely advice during the phases in research. I would like to thank her for providing all the facilities and support as the co-coordinator.

Any try at any level can't be satisfactorily completed while not the support and steering of my oldsters and friends helped me in gathering totally different info, aggregation information and guiding me from time to time in making this paper, despite of their busy schedules, they gave me different ideas in making this project unique.

11. REFERENCES

[1] The Five Stages of Phishing Attack by Salvatore Staflo

[2] Phishing attack on the rise by APN News, Saturday, March, 2022

[3] Spear phishing examples by Phish Protection

[4] What is Whaling? Whaling Email Attacks Explained by Tessian, 11 August 2021

[5] Pharming Attack Prevention and Examples by Geeks for Geeks, 19 Oct, 2021

[6] What is a Spoofing Attack? The 5 Examples You Need to Know by SoftwareLab.org

[7] Vishing Attack by INCOGNIA

[8] Phishing attacks warning signs by David Zamerman, Feb 26, 2022