Phishing: Analysis and Countermeasures

Bhagyashree Ankush Alandkar & Bhakti Desai

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

Abstract – Without the internet, our daily lives are inconceivable. One of the most important forms of communication we use every day is email. We prefer to just use it regularly for business communications, but we also use it to stay in touch with our friends and family. Due of the significant significance that email plays in international communication and information sharing. Even so, security issues have accumulated. E-Mail phishing is the most significant drawback or hacker attack on email in today's world. The moment is right to secure information sent via mail, even on specific networks. Cybercriminals create these emails to appear credible, which makes virtually millions of people throughout the world fall for them. The criminals don't have a specific victim in mind.

Key Words: Phishing, attacks

1. INTRODUCTION

Phishing is a type of email fraud in which the perpetrator sends out seemingly valid emails to target specific individuals in an effort to collect their personal and financial information. The communications typically look to originate from reputable and well-known websites. The phisher places the lure in the hopes of fooling at least some of the prey that come into contact with it, just like the fishing trip it gets its name from. Phishers deceive their targets by employing a variety of social engineering techniques and email spoofing techniques. Due to the important function that email plays in communication and information sharing on a worldwide scale. The safety issues have even gotten worse. The majority of the email servers used in the mail infrastructure on the internet are attacked.

2. HOW PHISHING ATTACKS WORKS

We need to comprehend the justifications for hostile attacks in order to comprehend how they operate. There are two main purposes of a phishing assault.

1) To extract sensitive data, first

These attacks employ techniques that compel the victims to reveal sensitive and private information. Hackers want the ability to break into a private or public network, steal money from someone, or use another person's credentials to carry out illegal activities. Checking account information is among the clearly questionable data that hackers request from victims.

2) To infect the system with malware

With such attacks, hackers also primarily aim to infect the victim's PC with malware or viruses. These emails include Microsoft Office zipped files.

3. STAGES OF PHISHING ATTACK

It's crucial to first comprehend how phishing attacks operate in order to stop one in its tracks. Let's go over the stages of a typical phishing attack that are most common [1]:

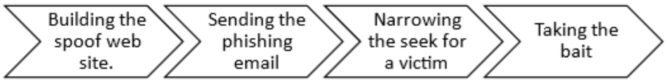
Building the spoof web site.
Sending the phishing email
Narrowing the seek for a victim
Taking the bait

Figure 1 stages of phishing attack

- Creating the fake website.

To create spoof websites, the hacker steals real code and legitimate images from websites. According to some estimates, hackers create 1.5 million spoof websites each month. Due to the availability of affordable internet scraping tools, this is now simpler than ever. Hackers frequently create fake websites with well-known and reliable domain names. They are also recovering at their trade. Even experienced security personnel will struggle to identify fakes.

- The phishing email's transmission.

The hacker launches the associate degree email phishing scam after creating the fake website. These emails, which are incredibly convincing, include content, images, and a link to the fake website. The victim is urged to open the link in the email with statements like, "Your account has been hijacked!" On a huge scale, this occurs. Every day, hackers send an estimated three billion phishing emails.

- Focusing the victim search

After developing the bogus website, the hacker starts the associate's email phishing scheme. These emails contain text, graphics, and a link to the false website, and they are quite convincing. In the email, the victim is prompted to click the link and is told things like, "Your account has been hijacked!" This happens on an enormous scale. An estimated three billion phishing emails are sent out daily by hackers.

- Taking the bait.

If a hacker is persistent, a victim will eventually fall for the lure. A silent attack will claim thousands of lives. The victim's financial assets, such as credit cards, bank accounts, or legal documents, may occasionally need to be taken. Others want to gather as many credentials as they can to sell online.

4. PHISHING SCAMS TO AVOID

- Spear Phishing Attacks

Many different types of tailored phishing are referred to as spear phishing. With spear-phishing assaults, the hacker tries to learn as much as they can about you, including your name, company, position, and phone number. They then take advantage of this knowledge by pretending to be someone you know and trust in order to persuade you to comply with the attacker's demands.

Example: Because Amazon is so widely known, all cybercriminals don't have to put up a lot of effort to deceive their customers; the bulk of phishing attempts are generic.

A clever spear phishing assault in 2015 tricked several customers into installing ransomware. Users who had recently placed an order with the World Health Organization received an email from the con artists.

- Whaling

Whaling is a type of phishing assault that targets people in positions of authority within a large corporation. This often denotes a senior management with access to or knowledge of sensitive firm information, such as a chief executive officer, business executive, or another senior manager. The fact that the targets are the "big fishes" in the phishing pool is what is meant by the phrase "whaling." Whaling attacks are frequently very carefully planned and aim to obtain important company information for the phisher's benefit. Attacks against whales are often planned out over a long period of time, and they are highly tailored and elaborate.

Example: The co-founder of Australian hedge fund Levitas Capital clicked on a fake Zoom link in the month of 2020.

- Pharming

Other methods of manipulating targets on the internet include phishing and pharmacy fraud. Phishing is a technique used to trick a victim into giving their information to a fake website. Pharming involves changing DNS information, so when a person types in an online address, they will likely be forwarded to the wrong website. This means that the DNS server responsible for converting the website address into the address for crucial information processing will need to be adjusted, and website traffic will also be diverted to another site. Due to flaws in the DNS server package, pharming attacks can happen and are frequently difficult to detect. The simplest way to identify a potential pharming assault is to raise the alarm if a common web.

- Spoofing

Spoofing is the act of a gouger acting as someone else in order to persuade the target to take a particular action. Many phishing attempts consequently make use of spoofing; a phisher could pose as a member of your IT department and urge you to visit a website and confirm your laptop login information. As a result, this website is a fake, and the phisher has obtained access to your login information without your knowledge. However, not all spoofing assaults are actually phishing; some phishers utilise spoofing as a means of manipulation. A spoofing attack might involve a hacker posing as a coworker and asking you to send a file, but the file is actually a trojan.

- Vishing

Vishing is the telephone equivalent of phishing, in which the targets are chosen by the con artists in order to obtain information. Vishers pose as a respectable organisation and harass you for your personal information by using various forms of persuasion or "social engineering." Be extremely careful when disclosing any sensitive information over the phone, especially if the number is restricted or you are unfamiliar with the area code or number. If at all possible, ask for the amount you can decide back and verify it with the source they say they are, or decide the party's customer service and ask if they need to get in touch with you.

Example: In this attack, a link will cause a page to open alerting you that a problem has been found with your computer and that you should choose a support option to resolve it. The offender may also decide to inform the victim that assistance is being sought for them due to a tool failure. This is a common tactic. A price is assessed at the end of the service for fixing a tangle that didn't initially exist [7].

5. PHISHING ATTACKS: WARNING SIGNS

A phishing website (also known as a faked website) often makes an effort to appear at least somewhat trustworthy. It will be designed to look like an authentic, already-existing website, imitating sites for your banks or healthcare facilities, for example. The website is designed for you to disclose your login information or other personal information. You might get an email or text message with a link to the current website, but you could also accidentally type in the wrong URL or use the wrong search term to land on the page. The main concern is then to be wary about the sender of the email or instant message and make sure you know who sent it, or that the sender is someone you trust.

- Email from unacquainted Sender

There are several things you might consider when you receive an email to determine whether you might be the victim of a phishing assault. Look at the email sender's information first. The phishing attempt can come from a suspicious-looking email that you have never seen before. As luck would have it, there are forums and online tools that can help you determine whether or not the source is trustworthy if you have any questions. Simply copy the sender's email and search for terms like "phishing attempt," "hacking," or "scam" on Google. You may be able to tell that the email is from a cybercriminal if others have reported it. However, there is a problem with this technique because phishers are quite aware of the forums and frequently and easily change their emails. Additionally, they would utilise these support forums as a way to legitimise their own fraud by giving themselves positive evaluations and insisting that the email offer was genuine [8].

- Sender’s Email looks Off

The phishing attempt may come from a business that appears to be fully trustworthy and legitimate but is actually not from the firm it purports to be. For example, if you search for a Sanket bank and see that they are using their logo, you might assume the email is coming from a legitimate source without realising that it could be that Sanket's email has been hacked or that a different email has been created that matches Sanket's email but isn't the right email type.

- Writing Tone Is Odd

Another major cautionary sign is when the email address looks familiar but the content or presentation seems strange. If the email contains grammatical or spelling mistakes that your contact is unlikely to make or does not frequently make, it's possible that the sender is actually a phisher. As phishing scams become more sophisticated, their language and design may also be well-thought-out and appear to be extremely trustworthy. Yet people often have a really certain style and elegance of communicating, and you seem to be drawn to it, either consciously or unconsciously.

If an email seems "fishy," you may have unconsciously noticed that the sender is using language and a style that are not typical of them. Follow your gut, and if something seems strange, look into the email before you answer.

- Greeting Oddly Generic

In order to trick you, phishing criminals send out a tonne of generic emails that start with "Dear Customer" and refer to "Your Business" or "Your Bank." This is frequently especially concerning if the email appears to be coming from someone who should have a lot of information about you, such as a partner you have met before or someone from your company [8].

6. PHISHING EMAIL EXAMPLES TO LEARN FROM

1) An example of a phishing email with a suspicious email address.

2) An example of a phishing email where the con artist promises financial rewards.

Sample of a phishing email asking you to confirm your account information.

4) An illustration of a phishing email with fake financial documents.

5) A phishing email that purports to be from an employee of your company.

6) A phishing email illustration requesting a payment confirmation.

7) Voicemail scam examples using phishing emails.

Account Deactivation (No. 8)

9) Fraudulent Credit Card

10) Transmit Money

11)Social media Request No.

7. HOW TO DEFEND AGAINST PHISHING EMAILS

Remember these 5 principles for creating a culture of cyber security awareness when constructing a defence against phishing emails:

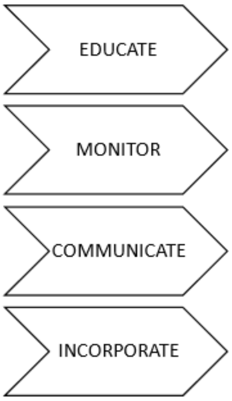

Figure 2. How to defend against phishing emails

- Educate: To coach, train, and change behaviour, use phishing microlearning and security awareness coaching.

- Monitor: Check employee information using phishing simulation tools to see if an agency is at risk of a cyber-attack.

- Communicate: Provide up-to-date communications and campaigns about social engineering, cyber security, and phishing emails.

- Integrate: Make project management, training, support, and awareness campaigns for cyber security a part of your business culture.

You need defence against phishing email attacks. The same sentiment also applies to your coworkers, organisation, friends, and family. Everyone ought to be able to safeguard their info.

Making the most of cyber security awareness is the greatest way to do this.

8. THE FREQUENCY OF PHISHING ATTACKS

Every year, phishing becomes more prevalent and poses a significant hazard. According to a 2021 Tessian analysis, the average number of phishing emails received by employees is 14. Certain industries were particularly hard impacted; retail workers received a median salary of $49.

The majority of the email-based attacks between May and August 2021, according to ESET's 2021 analysis, were part of phishing campaigns. IBM's 2021 analysis corroborated this trend by noting a two-point increase in phishing attacks between 2019 and 2020, which was partially fueled by COVID-19 and supply chain uncertainty.

According to CISCO's report on cybersecurity threat patterns for 2021, at least one employee of about 86 firms clicked on a phishing link. According to the company's knowledge, phishing accounts for over 90 percent of data breaches. Phishing attacks increased by 52 percent in December, according to CISCO, who discovered that the activity tends to peak around holiday times.

According to the results of a global poll, 83 percent of IT departments at Indian companies predicted a rise in the number of phishing emails aimed at their employees in 2020.

One of the reasons for its effectiveness is its capacity to continuously evolve and diversify, trade offences to contemporary issues or concerns, such as the pandemic, and capitalise on people's emotions and trust "Urban Center Wisniewski, the head of analysis at Sophos, said as much.

Phishing is frequently the first phase in a very intricate, multi-phase attack. According to Sophos quick Response, hackers frequently use phishing emails to coerce users into installing malware or disclosing login information for the workplace network "A second Wisniewski.

Also, the results show that there is no universal agreement on what is meant by "phishing." As an illustration, 67 percent of IT organisations in India equate phishing with emails that falsely purport to be from a genuine company and that frequently include a threat or a request for personal information. Sixty-one percent of respondents think that Business Email Compromise (BEC) attacks are phishing, and fifty percent of respondents think that threadjacking—where attackers inject themselves into a legitimate email thread as part of an attack—is phishing.

The good news is that almost all Indian businesses (98%) have implemented cybersecurity education campaigns to thwart phishing. Respondents reported using phishing simulations (51%), computer-based coaching programmes (67%), and human-led coaching programmes (60%).

According to the poll, four-fifths of Indian firms gauge the success of their awareness campaign by the number of IT tickets related to phishing, which is followed by user coverage of phishing emails (at 77%) and phishing email clickthrough rates (at 60%).

Every firm surveyed in the city, Hyderabad, and metropolis (100%) felt it is necessary to have cybersecurity awareness initiatives in place. When ninety-seven states had such programmes, Chennai was next, putting Bengaluru and the city at ninety-six each.

9. CONCLUSION

Phishing attacks continue to be a major concern to both individuals and businesses today. This can be primarily caused by human engagement in the phishing cycle, as the paper points out. Phishers typically target human weaknesses in addition to favourable technology situations (i.e., technical vulnerabilities). It is well established that a variety of factors, including age, gender, internet addiction, user stress, and many others, can affect a person's susceptibility to phishing. In addition to more recent phishing mediums like voice and SMS phishing, more traditional phishing channels like email and the web are still in use.

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.

The challenges caused by phishing have been examined in this book, and a new anatomy that outlines the entire life cycle of phishing attempts has been planned. This associate deprecatory offers a broader perspective on phishing attacks and a correct definition that covers the attack's realisation and end-to-end exclusion.

Although the best defence against phishing is human education, the sophistication of the assaults and social engineering components make it difficult to completely eliminate the threat. Developing affordable anti-phishing strategies that prevent users from being exposed to the attack is a critical step in minimising these attacks, even though ongoing security awareness training is the key to avoiding phishing attacks and to reduce their impact. This text concluded by mentioning the significance of creating anti-phishing techniques that recognise and stop the attack. Also, the significance of methods to identify the source of the assault may provide a stronger anti-phishing solution, as discussed in this article.

10. ACKNOWLEGEMENT

I am incredibly humbled and grateful to express my gratitude to everyone who has helped me put these ideas into one concrete item, way above the level of their simplicity.

I want to specifically thank Assistant Professor Jyoti Samel for giving me the chance to conduct this excellent research on the subject of "Phishing: An Open Threat to Everyone." Her support allowed me to conduct a lot of research and learn a lot of new information. I sincerely appreciate her. My sincere gratitude is extended to our research paper advisor for her insightful and timely counsel throughout the many research phases.

Without the support and guidance of my parents and friends, no attempt at any level can be satisfactorily completed. Despite their busy schedules, they gave me different ideas for how to make this project unique. They helped me gather a variety of information, aggregate it, and guide me periodically in making this paper.

11. REFERENCES

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

[2] Spear phishing examples by Phish Protection

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

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

[5] Vishing Attack by INCOGNIA

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