IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 8, August 2023

DOI: 10.17148/IARJSET.2023.10803

A Survey of Phishing Attack Techniques

Nikita Raikar[1], Shruti Kangralkar[2], Dr Pijush Barthakur[3]

Master of Computer Applications, KLS Gogte Institute of Technology, Karnataka, India[1,2,3]

Abstract: Phishing is a type of cybercrime in which an attacker pretends to be a real person or institution by presenting themselves as such through email or other forms of communication. In this kind of cyber assault, the perpetrator sends harmful links or attachments via phishing emails or some other websites that can accomplish a number of tasks, including stealing the victim's login credentials or bank account information. These emails cause people to lose money and have their personal identities stolen.

Keywords: Phishing techniques, Phishing Websites, Legitimate websites.

I. INTRODUCTION

The word Phishing came from the word ‘Fishing’ where the fishermen try to imitate themselves to be the food for the fish but their intention is to just attack the fish.

Similarly in cybercrime the ‘f’ is replaced by ‘ph.’ But the intention remains the same. Here the attacker tries to gain an access to the users system by sending them emails that seem to be from a genuine user or an genuine institution.

This email contains either an URL or the malicious data .Upon clicking the URL the attacker just gains access to the users personal information and also the confidential data.

The data stolen can be

- User credentials
- Bank account details
- Information of the credit and debit cards and so on.

Attack types: Phishing is a specific form of spam that uses two methods:

1. Deceptive phishing
2. Phishing based on malware

Deceptive phishing
This method is related to social engineering scams, which rely on faked email assertions that appear to come from an official company or bank.

Phishing based on malware The second method uses technological ruses that rely on malware or malicious code once users click on links contained in the email, or by identifying and exploiting security flaws in the user's machine to gain direct access to the victim's online account information.

II. PHISHING ATTACK TECHNIQUES

To deceive victims, phishing assaults employ a variety of strategies.

Email Phishing

Cybercriminals can fool people into disclosing sensitive information, such as login passwords, financial information, or personal information, by sending them false or misleading emails. This type of attack is known as email phishing. Phishing emails frequently imitate well-known businesses, governmental organizations, financial institutions, or well-liked internet services in order to appear to be from reliable sources. Email phishing is a technique used to steal sensitive information, perpetrate financial fraud, or gain unauthorized access to the accounts or systems of the victim.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 8, August 2023

DOI: 10.17148/IARJSET.2023.10803

Pros

1. High Probability of Success: Phishing emails can be designed to appear extremely convincing, increasing the likelihood of successfully tricking targets into completing the intended action.
2. Possibility of bank advantage: Successful phishing attempts may result in the theft of sensitive data, including login passwords or bank information, which attackers may then use for their own financial advantage.

Cons

- Technical Challenges: Crafting convincing phishing emails requires skills in social engineering, email spoofing, and website design, which may be beyond the capabilities of some attackers.

Spear Phishing

More focused than email phishing, but similar. Attackers acquire data on a particular person or organization in order to create tailored and persuasive messaging.

A highly personalized and targeted phishing assault that targets certain people or companies is known as spear phishing. Spear phishing entails modifying the email content to take advantage of the particular traits of the targeted recipients, in contrast to standard phishing efforts that cast a wide net.

By making the emails seem more reliable and trustworthy, spear phishing attempts to increase the likelihood that the scam will succeed by getting the recipients to either accidentally give vital information or fall for the hoax.

Pros

- Avoiding Detection: Because they are intended to be one-of-a-kind and do not adhere to the standard patterns associated with bulk phishing efforts, spear phishing emails can be harder to identify by security systems.
- Attackers may utilize social engineering strategies to influence their victims' emotions or psychological state, increasing the likelihood that they will be successful.

Cons

- Time-consuming: Spear phishing assaults take more time than generic phishing operations since they demand extensive investigation to learn details about the victim and create personalized communications.
- Damage to Reputation: Being connected to spear phishing can seriously harm an attacker's reputation, restricting potential prospects and online community contacts.

Whaling

A specialized type of spear phishing that targets prominent people, such business leaders or public figures. Gaining unauthorized access to valuable accounts or stealing confidential information are the objectives of this technique. Whaling, also known as CEO fraud, is a highly refined and focused type of spear phishing assault that targets high-level executives, company leaders, or those with a lot of power and influence within an organization.

Whaling attackers try to trick these important individuals into disclosing private information, starting unauthorized financial transactions, or gaining access to sensitive information or systems.

Pros

- High Chance of Obtaining Priceless Information: Prominent individuals are targeted in whaling because they typically have access to valuable and sensitive information. By successfully breaching their accounts, attackers may get vital information such as financial data, trade secrets, or other strategic data.
- High Financial Gain: Because the information gathered by whaling attacks is so sensitive, attackers may utilize it to conduct massive financial fraud or extortion operations, which could result in a sizable financial payoff.

Cons

- Damage to faith and Confidence: Whaling attacks can erode faith in digital communications and have a wider social impact. If they become targets, high-profile individuals may stop utilizing electronic communication tools, which could affect productivity and communication within firms.
- The public is acting more cautiously and putting stronger security measures in place as a result of increased awareness about whaling assaults. Attackers have a harder time succeeding in their objectives as a result.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 8, August 2023

DOI: 10.17148/IARJSET.2023.10803

Pharming

By changing the DNS (Domain Name System) settings of a website or user's device, cybercriminals can fool visitors into viewing a fake website even when they typed in the correct URL.

The fake website was created with the goal of obtaining sensitive data and login credentials. Pharming is a sort of cyberattack that includes secretly diverting user traffic from trustworthy websites to harmful ones.

The attackers reroute the victim's queries to a phony website by using a variety of techniques to manipulate the Domain Name System (DNS) or change the hosts file on the victim's device. In order to steal sensitive information, such as login passwords, financial information, or personal data, pharming tricks users into accessing malicious websites that look exactly like trustworthy websites.

Pros

- From an ethical or positive standpoint, pharming has no real benefits. Cybercriminals engage in pharming, a malicious behaviour with the goal of tricking and hurting users. Instead, let's concentrate on the negative effects and drawbacks of pharming

Cons

- Users aren't needed to click on links in emails or messages, making it harder for them to recognise that they are being routed to a malicious website, making pharming attacks difficult to detect.
- Impact: Pharming attacks have the power to persuade a sizable portion of website visitors, potentially leading to a sizable portion of accounts being compromised

Vishing

Vishing assaults happen when con artists call victims pretending to be representatives of official organizations, such bank employees or government officials. Over the phone, they pressure their victims into disclosing private information like credit card or social security numbers. The term "voice phishing," often known as "voice phishing," refers to a social engineering attack in which con artists use voice contact, usually over the phone, to trick and con people into disclosing personal information or taking certain activities. Vishing attacks mimic reputable organisations like banks, governments, or service providers in an effort to dupe victims into divulging personal information like credit card details, social security numbers, passwords, or other confidential data.

Pros

- Voice Manipulation: By using the human voice to convey a sense of urgency, authority, or emotional appeal, con artists can increase the likelihood that their targets will accede to their demands.
- Reactions right away: Unlike email scams, vishing enables scammers to acquire reactions right away from targets, enhancing the likelihood of success.

Cons

- Emotional discomfort: Victims of vishing may experience emotional discomfort and a sense of being violated.
- Vishing is becoming more widely known, and as a result, people are being more cautious, which makes it more difficult for scammers to pull off their schemes.

Smishing (SMS Phishing)

Smishing is email phishing using the text messaging (SMS) platform. Attackers attempt to deceive receivers into supplying personal information or downloading dangerous software on their mobile devices by sending misleading messages with links or phone numbers.

The term "SMS phishing," also known as "smishing," refers to a type of social engineering attack in which attackers utilise text messages (SMS) to trick and manipulate victims into disclosing personal information or taking particular activities. Smishing attacks use false and fraudulent text messages that appear to be from reliable sources to fool victims into divulging personal information, such as login passwords, bank information, or other confidential data.

Pros

- Wide Reach: Since practically everyone with a mobile phone can receive text messages, smishing attacks can rapidly and easily reach a large number of people.
- Sense of Urgency: Attackers frequently design text messages that portray a sense of urgency.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 8, August 2023

DOI: 10.17148/IARJSET.2023.10803

Cons

- Limited Message Length: Compared to email phishing, which allows for more comprehensive deception, smishing attacks may be harder to perform effectively because to the character constraint of text messages.
- Malware Distribution: Smishing messages may include links to websites or applications that download malware and install it automatically on the recipient's mobile device, jeopardizing the recipient's data and security.

Clone Phishing

Clone phishing is the practice of making an almost exact clone of a trustworthy email or website that the victim has previously used. Attackers replace specific components, including links or attachments, with malicious code to fool the recipient into believing the email or website is legitimate.

Pros

- Increased Credibility: Clone phishing emails and websites closely resemble real ones, increasing the likelihood that receivers would interact and trust them.
- Leveraging Familiarity: By copying an email or webpage the recipient has already viewed, attackers can profit on the recipient's familiarity with the material and increase the effectiveness of the hoax.

Cons

- Financial Loss: Unknowingly giving attackers access to victims' financial information, login credentials, or personal information can cause victims to suffer large financial losses.
- Identity theft is when con artists use stolen personal information for other illegal operations. Clone phishing attempts can cause identity theft.
- Malware Dissemination: Phishing emails and websites that look legitimate may contain links or attachments that infect the target's computer with malware, jeopardizing their data and security.

Search Engine Phishing

Attackers tamper with search engine results to make harmful links appear above legitimate ones. Unwary visitors may click on these links, which may take them to phony websites intended to steal their information. Attackers tamper with search engine results to make harmful links appear above legitimate ones. Unwary visitors may click on these links, which may take them to phony websites intended to steal their information.

Pros

- Access to Information: Users can get answers to their questions and learn new information thanks to search engines' rapid and simple access to the internet's massive amounts of information.
- Efficiency: Users may find information much more quickly via search engines than they can manually searching through websites, saving them time and effort.
- User-Friendly: Search engines are made to be easy to use, making them available to users of all ages and technical skill levels.
- Results that are Organized: Search engines display search results in an organized format, frequently with pertinent links and content snippets, assisting users in rapidly determining the most helpful sources.
- Business Promotion: Search engines offer a significant platform for businesses and websites to connect with clients and raise their online presence.
- Personalization: A few search engines provide tailored search outcomes based on

Cons

- Information Overload: Users may find it difficult to weed out the most pertinent and accurate content due to the abundance of information made available by search engines.
- Quality and Reliability: Not all online material is accurate or trustworthy, and search engines may not always give the most trusted sites a higher ranking in their results.
- Search engines capture user information, such as search queries and browsing patterns, which raises privacy issues and the possibility of data exploitation.
- Filter Bubbles: Personalized search results may lead to the construction of "filter bubbles," in which users are only exposed to information that supports their preconceived notions, potentially limiting their exposure to other points of view

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 8, August 2023

DOI: 10.17148/IARJSET.2023.10803

III. LIFECYCLE OF PHISHING

A phisher is someone who engages in malware- related activities.

Today's phishing assaults frequently use generalized "lures" to intimidate victims and sow panic; one such example is the statement "we need you to confirm your account details or we must shut down your account." A strategy that is said to be becoming more and more popular is context aware assault. This is a more difficult strategy because it tricks the victim into believing the messages are real by making them seem expected.

Phishers typically create fake websites that seem like the legitimate website by replicating the HTML code and using the same pictures parts and text. Some phishing websites register domain names that are similar to those of a firm or bank's official website.

Forms, such as those on the Internet Banking login page or a form for password verification, are the most popular tool employed by phishers. In many phishing attempts, domain spoofing or homographic attacks are used to trick users into divulging personal information .

Many other types of secret information, such as user names and passwords, credit card numbers, bank account numbers, and other personal information, could be the target of a phisher. About 19% of respondents polled in a Gartner study (Gartner Inc, 2004) claimed to clicking on a link in a phishing email, and 3% admitted to providing financial or personal information.

A typical phishing assault involves the attacker obtaining the victim's authentication information for one website, corrupting it, and using it at another website. Given that many computer users reuse passwords, whether they are used verbatim or with very minor changes, this is a significant assault. The planning, preparation, attack, collection, and cleanup phases make up the phishing attack lifecycle.

- Planning
- preparation
- attack
- collection
- Fraud and
- subsequent attacks.

The attack is planned, the attack code or message is made, and it is sent to the intended user. The intended target site receives a malware message.

As soon as the unaware target sees the message, they take a step that leaves them open to information compromise. The user is then solicited for private information via a web interface that looks dependable and familiar. user divulges his private information. From a phishing server, the private information is sent to the phisher. The fraudster impersonates the user by utilizing private information to commit fraud.

There isn't a method that can stop all phishing. However, diverse techniques used at various phishing attack phases can stop a phishing effort, and properly used technology can greatly lower the danger of identity theft.

IV. PROTECTION TECHNIQUES

The protection against phishing attacks is provided via various tools and techniques:

- Automated tools

There are numerous automated tools for phishing detection in use, including
Anti-phishing email programs are made to prohibit links and other phishing content from being stored on a server.

Databases that hold domain names and URLs that have been blocked. These blacklists are split into two categories: the domain/URL blacklist, which includes URLs and domain names that have been blocked because they are malicious, and the internet protocol blacklist, which includes IP addresses that have been blocked because they frequently change their status.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 8, August 2023

DOI: 10.17148/IARJSET.2023.10803

Systems for detecting and preventing intrusions have also been put in place as defenses against phishing. Organizations mostly use these tools, which they install on their networks in order to identify and stop attacker penetration.

- Training and Knowledge

One effective method for preventing phishing is to alert users of the various ways their information may be acquired. The simplest but least well-liked strategy for educating consumers about phishing is to post information about it online by academic institutions, governmental bodies, and even non- governmental organizations. According to procedural knowledge, which entails teaching users how to spot phishing websites, is essential for enhancing the efficiency of phishing warnings and increasing users' awareness of such websites.

- Multifactor Authentication (MFA)

A multifactor authentication system should be used in place of single-factor authentication, which typically requires a user to provide their login information (username and password) in order to access a system or website. Multifactor authentication requires users to submit two or more verification factors, such as face recognition, fingerprint, or one-time password (OTP), in addition to their login and password in order to access a system or an online account.

MFA is a useful tool for providing increased security and adding an additional layer of protection because it reduces phishers' attempts to enter a system or an online account. In MFA functionality, three different categories of authentication factors are possible, including: Your knowledge: Password or pin authentication is used to verify this.

V. PHISHING THREAT CHALLENGES

Finding effective and efficient defenses against attacks that take advantage of human fragility is the fundamental problem faced by cybersecurity specialists while protecting company networks. Taking on this challenge is crucial for a number of reasons.

The earlier a phishing effort is noticed in the attack chain, the better the odds are of stopping, containing, and responding to the assault. Phishing attempts are acknowledged to be the most common first step in breaching the defenses of a corporate network. In most cases, businesses have technical safeguards in place to identify and block phishing emails before they reach the employees' inboxes.

However, fraudsters are developing fresh strategies and honing their assault methods. As a result, phishing assaults have become increasingly complex and adept at dodging even the most powerful technical defenses. The literature outlines a number of potential strategies for spotting phishing attempts based on different telltale signs that are plain to see. These hints include the URLs of online browsers without HTTPS, their content, the warnings that browser toolbars display, the numerous indications of legitimate certificates (such as VeriSign certificates), and the content and context of the email message.

Unfortunately, a lot of people either ignore or are uninformed of security alerts and hints that are provided on online browsers. Additionally, it can be challenging for common online users to see phishing warning flags or a fake website aesthetically. Although it can be difficult to distinguish a fake URL from a real one just by looking, phishing assaults can be detected by looking at the Uniform Resource Locators (URLs).

People respond to phishing communications for a variety of reasons, which makes combating phishing attacks extremely difficult. Users are motivated to respond to phishing emails for several reasons, such as curiosity, anti-phishing countermeasures, knowledge of the sender, and interest in confirming the content.

VI. CONCLUSION

Attacks using phishing are still one of the biggest risks to people and businesses today. This is mostly driven by human engagement in the phishing cycle, as was mentioned in the article. In addition to favoring technology conditions phishers frequently prey on human weaknesses.

Age, gender, internet addiction, user stress, and many other characteristics have been found to affect a person's susceptibility to phishing. Along with more established phishing channels newer phishing mediums like voice and SMS phishing are becoming more popular. In addition, as social media usage has grown, so too has the use of social media-based phishing.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 10, Issue 8, August 2023

DOI: 10.17148/IARJSET.2023.10803

Alongside this, phishing has evolved to include nation-state attacks, cyber terrorism, hacktivism, reputation damage, stealing private information, and financial crimes. Although human education is the best phishing defense, the intricacy of the attacks and social engineering components make it challenging to totally eliminate the threat.

Developing effective anti-phishing tactics that shield users from the attack is a crucial first step in minimizing these attacks, even if ongoing security awareness training is the key to avoiding phishing attempts and reducing their effects. This essay covers the technique used by attackers for phishing and the countermeasure to reduce the attack.

REFERENCES

[1] (2021).Darem Abdulbasit. Computer Science Department, Northern Border University, Arar, Saudi Arabia, Anti-Phishing Awareness Delivery Methods

[2] Vaishnavi Bhavsar, Aditya Kadlak, and Shabnam Sharma. "Study on Phishing Attacks," International of Journal on Computer Applications (0975 - 8887), 2018.

[3] (2022). Said Khaled Shaalan, Tarek Gaber, Sunil Vadera, and Salloum. Phishing Email Detection Using Natural Language Processing Techniques: A Systematic Literature Review

[4] Alabdan Rana Saudi Arabia's Majmaah University, College of Computer and Information Sciences, Department of Information Systems. Types, vectors, and technical approaches of phishing attacks in 2020.

[5] Tan, C.L., Yong, K.S.C., and Chiew, K.L. a review of phishing assaults, including varieties, distribution methods, and technical strategies. 106, 1-20, Expert Syst. Appl., 2018.

[6] Liqaa Nawaf, Zainab Alkhalil, Chaminda Hewage, and Imtiaz Khan.Phishing Attacks: A New Anatomy and a Recent Comprehensive Study, March 9, 2021.