Emerging Trends in Phishing: A Look at Smishing, Vishing, Quishing

Bello Bello Musa[1], Adamu Ahmad Bahago[2], Nasir Auwal Muhammad[3], Dr. Fakhrun Jamal[4]

[1,2,3]Student, [4]Professor

Student Department of Computer Science and Engineering, Shobhit University Meerut, Uttar Pradesh, India. (MSc. Cyber security and Forensics)

Abstract: *Sophisticated and varied approaches including Smishing (SMS phishing), vishing (voice phishing), and quishing (QR code phishing) have emerged as a result of phishing attacks' major evolution beyond conventional email-based methods. These new attack methods circumvent traditional security measures and compromise private data by taking use of social engineering, mobile technologies, and human trust. This essay examines how phishing strategies have changed over time, looking at the methods, resources, and psychological tricks used in Smishing, vishing, and quishing. Additionally, it draws attention to real-world case studies, detection difficulties, and threat actors' growing use of automation and artificial intelligence. The study also looks at future trends in phishing, such as cross-channel phishing campaigns and deep fake-enabled voice phishing and considers the consequences for cyber security knowledge. This study intends to educate cyber security experts and stakeholders about the pressing need to develop and adapt defense mechanisms in an increasingly complex threat landscape by examining various contemporary threats.*

Keyword: Phishing, Smishing, Vishing, Quishing, Cybercrime, Cybersecurity, Human vulnerability, Threat.

Introduction

Phishing, which has long been acknowledged as one of the most common and successful types of cyber-attack, typically uses phoney emails to trick users into disclosing private information. Threat actors have, however, modified their strategies in response to the diversification of digital communication channels and the rise in cyber security awareness, which has resulted in the creation of new phishing variations as quishing (based on QR codes), vishing (based on voice), and Smishing (based on SMS). These approaches utilize less-monitored platforms and human trust, making them harder to identify and prohibit using standard security measures.

Smishing uses SMS messages to trick recipients into clicking on harmful links or disclosing personal information by posing as reliable organizations. Vishing uses social engineering in phone calls, using authority or urgency to obtain information or access to systems. By inserting malicious URLs into visually appealing codes that appear to be authentic, Quishing takes advantage of the increasing popularity of QR codes and gets beyond email filters and other online security measures. When taken as a whole, these phishing variations show how sophisticated and adaptive attackers have become, marking a dramatic change in the cyber security landscape. This study looks into these new phishing trends, examining their tactics, psychological tricks, and the technology that makes them possible. Along with suggestions for improving resilience against such attacks, it also examines the difficulties currently facing detection and mitigation.

Understanding these new attack methods is essential for businesses and individuals looking to safeguard their digital assets in a constantly shifting threat landscape as phishing continues to develop. While significant progress has been made in understanding and mitigating phishing attacks, several limitations persist in addressing the emerging forms such as Phishing on social media, In-Game Phishing, Emerging Technologies and Phishing, Cross-Channel Social Engineering, Psychological Manipulation in Non-Email Phishing.

Rest of paper arranged in the following way: Section 2 gives the introduction of smishing, including definition, characteristics, techniques, vectors, challenges as well as limitations.
In section 3, vishing was introduced, including definition, characteristics, techniques, vectors, challenges as well as mitigations. In section 4, quishing was introduced, including definition, characteristics, mechanics, challenges, real world example, as well as mitigations. In section 5, we compared smishing, vishing, and quishing in tabular form. Finally, presents conclusion in section 6.

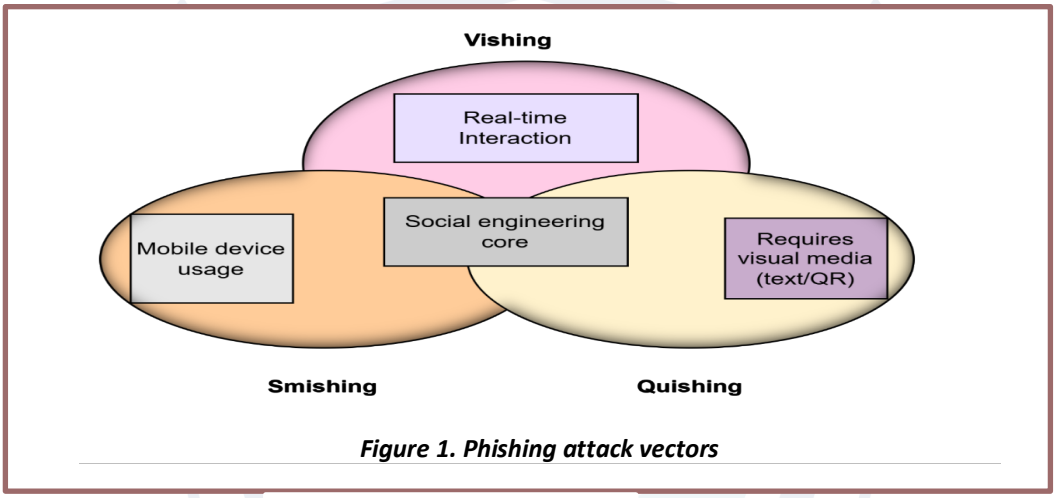

Figure 1. Phishing attack vectors

1. Definition and Characteristics of Smishing

This section provides a general definition and characteristics of Smishing or SMS phishing in the context of phishing.

1.1 Definition

Smishing is a cyber-security attack which operate SMS in stealing personal documentation of mobile beneficiaries. The confidence level of end-users on their smart appliances captivates attackers for committing diverse mobile security attacks such as the smishing.[1] In the technology of today, attackers are more concerned in attacking mobile phones than computer systems due to the increase in technology. Due to the smart phone's multipurpose feature, the small screen size, lower production cost and portability, make the mobile phone more reliable and most useful to users than the computer system.[1] Smishing or SMS phishing also entails the transferring misleading or unreliable text message to attract someone into revealing individual information or installing worms or malwares.[2]

1.2 Characteristics of Smishing

- *Text Message Smishing*: Attackers send instant messages instead of emails, which appear to have been sent by a genuine organization and demand that the clients tap on a link or disclose the credentials

through the text message reply. Sometimes the attackers send misleading text for attraction of users for money transfer notifications.

- *Facebook Smishing:* The attackers sometimes send a friend request on Facebook, or send link through Facebook account to request some important information by the users which seems a genuine notification.
- *Website Notification*: Attackers sometimes send website notification with a website address which may look a genuine and verified site requesting the user to visit a particular website for a full detail about an information, or even about recruitment for jobs or scholarship application. Email notification requesting users to visit their emails for a link to tap and be directed to a particular form to fill or information to provide.

1.3 Smishing Techniques and Tactics

Spoofing of phone numbers and sender IDs is also a common technique used for swatting, which is an attempt to trick an emergency service with false reporting of an incident. for instance, police officers were tied-up in responding to a non-existent robbery reported by pranksters; drugs were misused as a result of spoofed pharmacists' phone numbers; other incidents include identity theft, purchase scams, etc.[3]

Unfortunately, existing caller ID protocols do not provide real authentication and hence are untrustworthy for authenticating callers' locations or identities, because caller IDs are vulnerable to spoofing attacks; i.e., an attacker can easily send a fake caller ID to a call. This vulnerability has already been exploited in a variety of misuse and fraud incidents: In the US, thousands of people were victimized by credit card fraud with the help of caller ID spoofing [2], causing a loss of more than $15 million dollars annually.[3]

A. Social engineering Tactics

Social engineering tactics used in smishing (e.g., impersonation, fear, rewards). The foremost step of a social engineering attack is information gathering. At this stage, the attacker gathers information about target to gain credibility and to establish a trust relationship. The attacker may receive information about preferences, understanding, political affiliation, educational backgrounds, family information, financial information and other social information. The information acquired by different means will be used by an attacker to get the trust of the target.[4]

a) *Information gathering:* Attackers frequently begin by exploiting the wealth of publicly accessible information from individuals' online presence, particularly on social media platforms. This information may be employed directly in the execution of the attack or used to obtain further information from secondary sources[5]. This is the harvest of phone numbers via breaches, social media, contacts include research target via social media and leaks.

b) *Developing relationship:* This is the focusing on cultivating trust with the target by building rapport or trust. Impersonating banks, government agencies, or known brands via spoofed SMS, building rapport with urgency or familiarity. Example: ("Your account will be locked", "Dear Customer")[6]

c) *Exploitation:* The exploitation stage aims to accomplish the attack's objective by employing convincing and manipulative techniques to retrieve sensitive information from the target or mislead them into making security mistakes. This is the phishing request or malicious link by insertion of malicious links asking for credentials, OTPs, or app install.[5]

d) *Execution:* Finally, the attacker terminates the interaction with the victim and may attempt to cover their tracks by erasing any evidence or traces that could lead to identification or tracking. It is the final data theft or malware deployment[5]. The stealing of OTPs or login data, such as; install malware, simulate SIM swap, or initiate premium-rate call scams.

The backbone step of social engineering attacks life cycle or tactics is exploitation. At this stage, the attacker calls for a task to be carried out. This may be a malicious activity, such as logging in, or may be software installation or other malicious activities. Consequently, an attacker has already built the trust of the target, many psychological factors may carry out such activities. This action has different types of features including spam email, trickery, password reset, logging in and cloud access. The subsequently step of the social engineering attacks life cycle is execution. During the execution phase the attacker receives sensitive information, log-in credentials and access to the cloud or system.[4]

The URL sent by the attacker must be real URL if the attacker is asking for the request such as identity approval, so URL of request page should be “Facebook.com”. When the receiver does not identify the URL and found out “No Doubt” option is selected. No Doubt will be considered.

The misspelled or shortened URL are commonly used in social engineering attacks, for example Facebook will be converted to Facebook or fecebuk, and might be ignored by the target. In this scenario, target consider the URL as doubted but due to bi-directional communication and relation between attacker and target, attacker made him trusted that URL is not Misspelled, shortened or Obnoxious.[4]

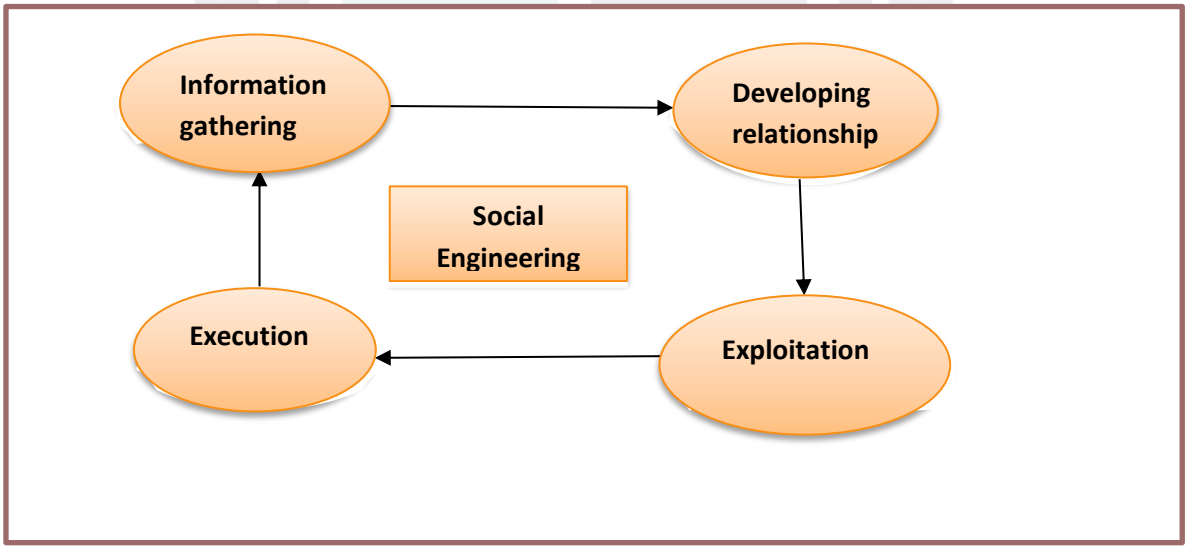

Figure 2. Life cycle/tactics of social engineering

1.4 Smishing Attack Vectors

The smishing via messages contain either a phone number, email id, or URL. The text in the message prompts the user to contact the attacker for not getting their account blocked. When the user contacts the attacker, they later ask the user to download an application through which the attacker gets access to the user’s device remotely.

Attacks now occur not only via SMS and email but also on platforms like What Sapp, Facebook, Skype, Snap chat, LinkedIn, and other messaging applications. The attackers often disguise themselves as friends, relatives, or package couriers, sending documents that, upon inspection, turn out to be malicious files (e.g., with a apk

extension) designed to phish users[7]. These messaging apps are almost more harmful than the normal short message service (SMS).

The study focuses on developing an Android application to protect WhatsApp users from spam and phishing messages, enhancing data security through the integration of machine learning techniques. The research seeks to create a robust supervised learning model capable of filtering labelled datasets, including SMS, email, and text messages categorized as spam, phishing, or safe[7].

Smishing is also used as an attack vector to execute other attacks such as ransomware attacks.

Ransomware attack is when an attacker seizes or hack someone's information and requesti11ng some amount of money in order to release the data he seized or hacked. More recently phishing has targeted organizations and made them suffer in terms of cost to contain malware, productivity loses, cost to contain credential compromise, and cost of ransomware from phishing, besides loss of reputation in front of their customers and competitors[6]

1.5 Challenges in Smishing Detection and Prevention

The abbreviated form of text messages makes it difficult to analyse the maliciousness of the message. This leads to limited number of features extracted from the message, and hence, the identification of malicious SMS becomes difficult. Leets words, idioms, and misspelled words are used in the text message which leads to hassle in the identification of smishing keywords.

- Spam messages contain a similar set of features in comparison with smishing messages. Hence, different initiation among spam messages and smishing messages is a tedious task thereof.
- The scarcity of real-time, public smishing datasets makes it a challenge to evaluate the smishing detection systems.

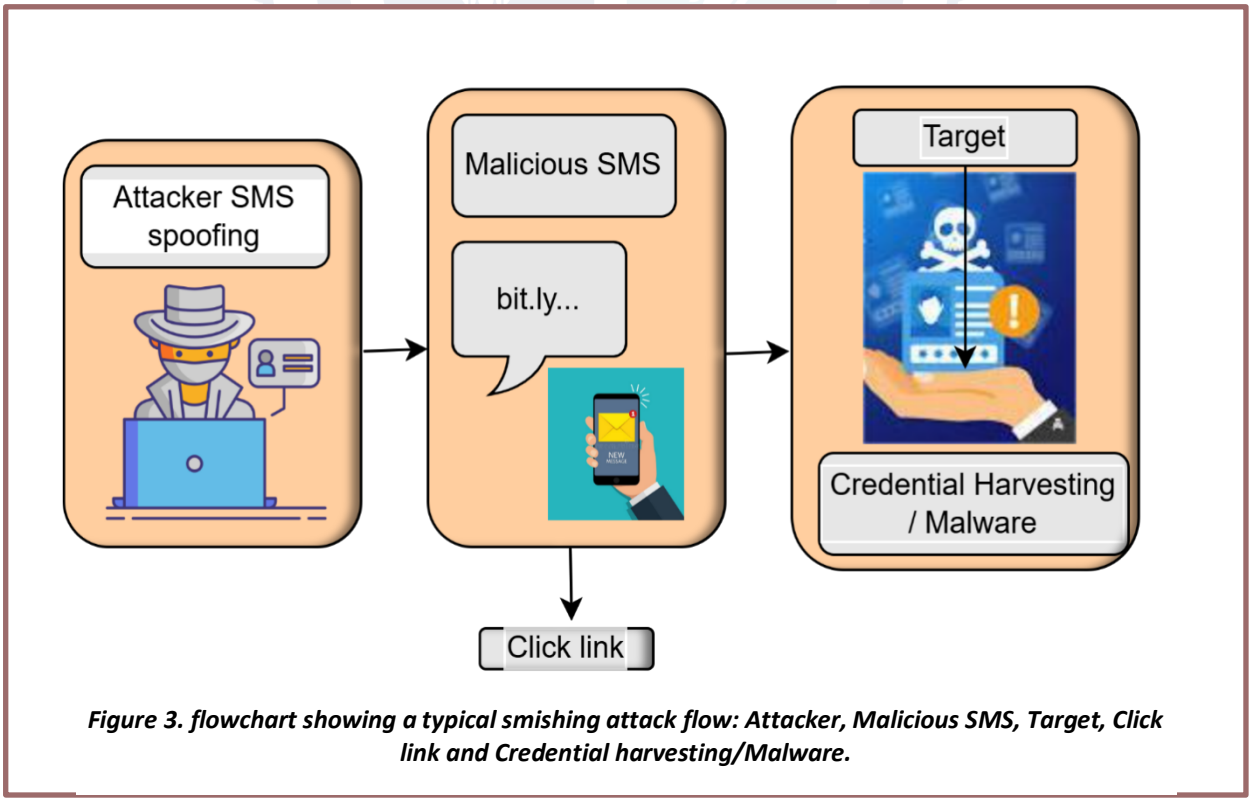

Figure 3. flowchart showing a typical smishing attack flow: Attacker, Malicious SMS, Target, Click link and Credential harvesting/Malware.

1.6 Proposed Prevention Methods

- Always verify the source of unsolicited messages before clicking any links or providing personal data.
- Install reputable security applications that can detect and block potential malware or phishing attempts on mobile devices.
- Regularly update operating systems and applications to protect against vulnerabilities that may be exploited by attackers.
- Educate oneself about common smishing tactics and tactics employed by scammers, as awareness is crucial in recognizing suspicious messages.
- Report any suspicious SMS communications to mobile carriers or relevant authorities to aid in combating this form of cybercrime.

By implementing these measures, individuals can significantly reduce their risk of falling victim to smishing attacks and better safeguard their personal and financial information. With the growing sophistication of cyber threats, staying informed and proactive is essential in the digital age. Another method for preventing the smishing attack is by the use of heuristic methods in which researchers choose some features of the text messages with the aid of classification algorithms and categorize the SMS based on these features.[8]

1.7 Limitations of traditional email security measures

Traditional email security tools have several limitations in addressing modern cyber threats.

1.7.1 Lack of adequate security mechanism in the traditional email security measures

Several technological and policy changes were made to SMTP servers to make e-mail system secure without creating incompatibility between older and newer systems. These include SMTP session refusal to unauthorized servers through IP address verification, refusal of e-mail relaying, restriction on use of certain SMTP commands like EXPN, verification of e-mail envelope and headers, limiting the size of e-mail message and filtering[9].

1.7.2 The ease of spoofing and the trust associated with SMS

Spoofing is a malicious action that causes any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.[3] The sender information in an SMS can be spoofed by attackers. The sender information of an SMS is specified by the sender's phone number (henceforth referred to as the "originating number") or a display name called the "sender ID" composed of alphanumeric characters. The sender ID can be specified as any string using the SMS gateway service. Thus, it can be spoofed as the name of a trusted entity. However, short messages with specified sender IDs cannot receive a reply and are unavailable in some countries. Therefore, the originating number is generally used as the sender information to enable two-way communication between subscribers or machines via SMS. Previous studies have shown that originating numbers can also be spoofed as arbitrary phone numbers. Short messages with spoofed sender information have been exploited in various cybercrimes, such as phishing scams.

Example: An attacker can impersonate a widely trusted entity and send a message including the URL of a Web site that requires the victim to enter authentication or payment information. Unfortunately, because the

sender's information displayed in short messages cannot be trusted, detection and mitigation measures for such attacks have become crucial research topics.[10]

1.7.3 User Behavior and Awareness Challenges on Mobile Devices

The mobile phones have become one of the primary ways in which people around the globe communicate with each other. These devices, particularly the smart mobile phones have transformed over a period of time from merely communication tools to smart and highly personal devices enabling to assist the users in their variety of day-to-day situations in their daily life.

In the real word, users' interest on "Mobile Phones" is more and more than other platforms like "Desktop Computer" or "Tablet Computer" over time. People use mobile phones not only for voice communication between individuals but also for various activities such as applications (mobile apps) using, Internet browsing, e-mailing, using online social network, instant messaging etc.

Example: (A smart phone call handling service): A mobile phone user typically 'declines' the incoming phone calls, if she/he is in a 'meeting'; however, she/he 'answers' the incoming call if the call comes from her/his 'boss' as it seems to be significant for her/him. Hence, [decline, answer] are the user phone call behaviors, and [meeting, boss] are the associated social contexts, i.e., meeting represents the social activity or situation, and boss represents the social relationship of that user[11].

2. Definition and Characteristics of Vishing

This section provides a general definition and characteristics of Vishing or Voice phishing in the context of phishing.

2.1 Definition

Vishing, also termed as voice phishing is a style of cybercrime in which false telephone calls are made to a person to mislead the target into divulging his or her details. While vishing is distinct from traditional phishing in which false emails, text messages, and other forms are used to steal information, vishing takes advantage of the direct and trusted face-to-face nature of voice calls. Such con often takes the form of cloning the organizations the scammers are portraying as the real deal to make the victims provide sensitive information. Vishing calls frequently display particular traits that can be used to recognize them as frauds. These include impersonation, in which con artists pose as representatives of respectable companies, such as banks or government offices, and authority, in which they appear authentic by using persuasive scripts and phony caller IDs [12].

Urgency is another crucial characteristic, whereby attackers incite fear or a sense of urgency to compel immediate response without challenging the request. Threats of quick account closure, legal action, or arrest are a few examples of this. Being wary of unwanted calls is crucial for identifying vishing [13]

2.2 Characteristics of Vishing

Vishing calls, or voice phishing, usually show specific signs that indicate they are scams. Attackers often pretend to be representatives from trusted organizations, like banks or government agencies, claiming they can fix an issue or offer a service. They create a sense of urgency that pushes for quick action and might ask for sensitive information like passwords, credit card numbers, or Social Security numbers. They may also use threats or intimidation to pressure victims into agreeing. Some vishing calls may even use fake caller ID to look legitimate. To protect yourself, verify the caller's identity, be careful with unsolicited calls, and never

share sensitive information over the phone unless you are sure of who you are talking to. If you think a call is a vishing attempt, hang up and report it to the proper authorities [14]

2.3 Vishing Techniques and Tactics

- **Caller ID Spoofing**: Identity spoofing is one of the most typical types of vishing where the attackers deceive the caller ID information to seem like the call is originating from a legal source. This is done by making use of a code or service that changes the shown number so that the victim is likely to believe the caller. Now and then some organizations experience high levels of pharming, and these are the organizations that they mimic; these include banks, government institutions, and technological support. For instance, a victim occasionally receives a phone call that comes along with a message that their bank account appears to have been compromised and needs them to give more account information to sort it out[13] [15].

- **Pretexting**: This form of social engineering entails coming up with a pretence to induce the victim into a particular action, to get the victim to disclose more details. Worms and viruses pose believable stories to do what they want, backed by often impressive research. Examples of such pretexts are emergent events like suspicious account activity or security alerts where the victim is pressured to act quickly because there is something to lose or face the law. Its effectiveness in this is astonishing since it creates a quick feel, and the victim is forced to do as the caller instructs without worrying whether the caller the real thing [13] [15].

- **Social Engineering**: vishing in social engineering is different from the other categories because it relies on an ability to change the victim's behaviour by appealing to the emotions of the victim. Subtle tactics trigger rational or irrational feelings like the fear of being harmed the trust in the sender, or even compassion. Such strategies are the pressure that comes with threats such as a fake call demanding urgent pay to avoid adverse outcomes being a call from banks or government officials or even posing to be a relative in dire straits. These are sick strategies that are meant to work around the rational mind of the recipient with a view of eliciting personal details from him/her [13] [15].

- **Robocalls and Automated Messages**: Pre-recorded messages or Robocalls and Automated messages are adopted by Visher's to contact a massive number of prospects within a short duration. This is normally a recorded message that sounds rather official and that triggers a sense of urgency on the part of the recipient. Subtypes include the receipt of alerts by banks regarding unusual transactions, tech support messages stating that computer systems are infected by viruses, and government messages stating the balance of past-due taxes. The aim is to make the victim return the courtesy of a call to a specific number, enter a website link, or give out personal details on the phone. This method takes advantage of the auto-generated calls to make the calls seem somewhat official and impending [13] [15].

2.4 Vishing Attack Vectors

The techniques or avenues through which attackers carry out voice phishing scams are referred to as vishing attack vectors. These vectors try to fool victims into disclosing private information by taking advantage of human weaknesses rather than technological ones. Vishing attacks are especially successful because they take advantage of the immediacy and trust that come with phone connection [12] [13]. Direct phone calls are a common vishing attack vector, where attackers frequently utilize fake numbers or pose as trustworthy organizations like banks, government offices, or IT firms. Additionally, voicemails can be utilized to ask victims to return calls or submit information. Social engineering techniques are commonly used to increase

victims' likelihood of complying with the attacker's requests by fostering a sense of urgency or trust. Combining Vishing with Other Attack Techniques. Vishing is frequently used in conjunction with other techniques by attackers to boost efficacy. Using Smishing (SMS phishing) to establish contact and win the victim's trust before moving on to a voice conversation is one popular strategy [13] [12].

2.5 Challenges in Vishing Detection

Due to the advanced strategies used by attackers, detecting and preventing vishing attacks can be extremely difficult. The capacity of attackers to trick victims via social engineering techniques, spoof caller IDs, and convincing scripts is one of the main obstacles. People and organizations may find it challenging to discern between malicious and legitimate calls as a result of these approaches [13].

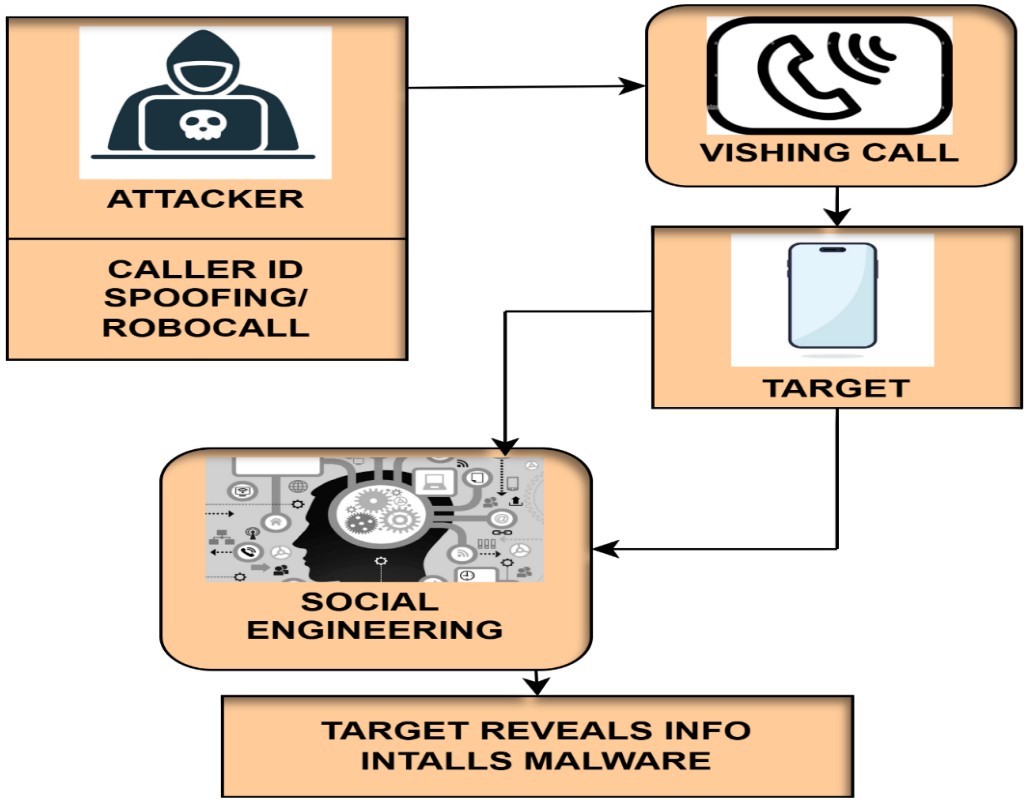

Figure 4. A flowchart: Attacker (caller ID spoofing/robocall), Vishing Call Target (phone), Social Engineering, Target reveals info/Installs malware

- **Human Vulnerability:** Human weakness is a major contributor to vishing attack success. Psychological cues like fear, urgency, and trust are used by attackers to coerce victims into disclosing private information. Because of this human component, vishing attacks are very difficult to identify and stop because technical security measures by themselves are frequently insufficient[13]
- **Changing Threat Environment:** Attackers create new strategies and methods to get around security barriers, the vishing threat landscape is always changing. Because vishing attacks are dynamic, detection and prevention techniques must be updated often. Effective vishing identification and prevention depend on staying ahead of these changing threats[13].

- **Limited Awareness and Education**

- Vishing attacks are successful in part because of a lack of knowledge and instruction about them. Many people and organizations don't completely understand the dangers of vishing, or they don't know how to spot and handle vishing attempts. Reducing susceptibility requires raising awareness and educating people about vishing techniques and preventative methods [13]

2.6 Prevention Techniques

- **Verify Caller Identity:** Avoid vishing incidents by always confirming the caller's identity before you give him/her any details. When the received call is fake, one should ask for the name of the called person, department, and telephone number for a return call. That information should not be a problem with any genuine representative of the modafinil community. Also, do not use the phone number that the caller provides to you but use other numbers that belong to the organization that you can find on the organization's website or any official document. If for example, your caller pretends to be from your bank, just hang the call and instead dial the bank service contact number indicated in your statement or the bank's website [16]
- **Do Not Share Personal Information:** Do not provide your personal or any financial information to anyone over the phone unless sure of their identity. Normal organizations cannot call their clients and tell them to give them their details. Avoid believing the caller's requests for personal information like social security numbers, bank account numbers, and passwords. Because it is safer to take any unexpected call, which requires personal details, as a possible vishing attempt[16]
- **Use Call Blocking and Screening Tools:** Use call blocking and call screening to prevent cases of vishing. Some of the common smartphones have options that allow users to block such calls as those from unidentified numbers or unwanted callers. Furthermore, it is necessary to mention that there are many applications and services for call filtering. In this case, applications such as Hiya, True Caller, as well as Nano robot will be useful since they can help identify the scam numbers. These tools can dramatically minimize the probability of falling victim to vishing since these calls do not get through to you [16]
- **Report Vishing Attempts:** Hence, it is helpful to report vishing attempts to the right authorities in fighting such scams. If the call was from a scammer, the identity of the caller together with details of the call should be forwarded to the FTC via the internet or the helpline. Also, contact your telephone line service provider, they will safeguard you by blocking the number used in the scams. Reporting vishing attempts prevents scammers as authorities are alerted to shut down such activities, hence saving more people [16].

2.7 AI-Related Mitigation Techniques

- **AI-Powered Call Screening:** Real-time analysis of incoming calls by AI-powered call screening systems finds vishing signals. These instruments assess many facets of a call, including caller number, call history, and voice patterns, using sophisticated algorithms. AI can flag dubious calls and notify the user by matching this data with known vishing traits. Real-time analysis, which enables instantaneous identification and intervention, and voice recognition which can find irregularities or inconsistencies in the caller's speech are features of AI-based call screening. To improve their detecting powers, these systems can also interact with databases containing known fraud figures.
- **Natural Language Processing (NLP):** NLP is a great tool in identifying vishing efforts since it helps artificial intelligence to grasp and analyze human language. Through language pattern analysis of a call, NLP can find often-used suspect phrases or scripts connected to fraud. NLP can highlight, for example, calls including urgent demands for personal information or legal action threats. Using natural

language processing, identify scam calls by tracking customer service contacts for possible fraud and red flag scanning of recorded calls suggestive of vishing. This feature helps to spot and stop vishing attempts before they may damage the victims.

- **Behavioral Analytics:** Behavioral analytics is the application of artificial intelligence to examine caller behavior and identify anomalies suggestive of a vishing effort. This approach looks at calls' frequency and caller interaction with the recipient. An artificial intelligence system might, for instance, detect whether a caller deviates from usual conversation patterns, is too persistent, or employs manipulative strategies. AI can assist find and stop vishing scams by spotting certain behavioral warning flags. In call centers, where it can track interactions and notify workers to real-time possible risks, behavioral analytics is especially helpful.
- **Automated Threat Intelligence:** Using artificial intelligence, automated threat intelligence systems compile, examine, and share knowledge on recognized vishing methods. These systems regularly update databases with the newest vishing trends and techniques, which can subsequently be applied to improve call screening instruments. Threat intelligence combined with call screening lets one create a more complete security since artificial intelligence can use current data to find and stop developing dangers. Faster response times, better detection accuracy, and the capacity to change with new vishing techniques as they develop are advantages of this strategy.
- **Voice Biometrics:** Through analysis of distinctive vocal traits including pitch, tone, and speech patterns, voice biometrics authenticates callers. By matching the caller's voice to a pre-recorded voice print, this technology can separate between genuine callers and frauds. Using voice biometrics to guard against vishing means confirming callers' identities before sensitive data distribution. Voice biometrics, for example, allow financial organizations to verify the identity of a caller asserting to be a customer. This extra layer of protection helps stop illegal access and lowers the possibility of vishing schemes.

3. Definition and Characteristics of Quishing

This section provides a general definition and characteristics of Quishing or QR code phishing in the context of Quishing.

3.1 Definition

The adoption of QR codes has grown 16% annually, particularly accelerated by the COVID-19 pandemic. The two-dimensional barcode garners attention as a future replacement for manual passwords and as convenient shortcuts for faster mobile keyboard entries[17]. The COVID-19 pandemic enabled quishing with malicious QR codes, as they became a convenient go-between for sharing URLs, including malicious ones [18]. Quick response (QR) codes are two-dimensional barcodes that encode different types with high density. In 1994, Masahiro Hara invented them to improve the production control of the company Denso Wave. Since then, its usage has become more diverse. For example, QR codes are applied on websites, for marketing, as links for information, or for authentication purposes in companies and research and education environments, because they offer simplicity and convenience. Almost all smartphones possess built-in QR code scanners featuring sensors and decoders. During the COVID-19 pandemic, QR codes were frequently applied to, for example, make an appointment for a test, and get the COVID-19 test results, an order in a restaurant, or display the vaccination status in the COVID-19 contact tracing app.[19] Phishing has been an increasingly successful tactic for initiating cyber-attacks. In 2022, the FBI's Internet Crime Complaint Center (IC3) found that

phishing attacks were the number one reported cybercrime, with over 300, 00 complaints reported. These attacks are also very impactful. According to a 2021 survey conducted by the Ponemon Institute and Proofpoint, the cost of phishing attacks quadrupled from 2015 to 2021. The same research found that the average cost of a successful phishing attack in 2021 was $14.8 million. Quishing is a common tactic for hackers to use against the health sector because it often leads to data breaches, and the stolen health data has the potential to be lucrative for the attackers. The 2021, the Healthcare Information and Management Systems Society found that the most common attack impacting healthcare organizations was phishing(quishing), comprising almost half of all attacks. [20]

3.2 Characteristics of Quishing

I. **Strategies for Social Engineering:** Quishing uses legitimacy or urgency (e.g., "Scan for a free reward," "Scan to verify your account") to entice users to comply without question.

II. **Getting Around Conventional Email Security:** The malicious link is not immediately accessible in text form, QR codes frequently avoid being detected by email filters and URL scanning software. Because of this, automated systems find it challenging to identify or examine the payload before the user scans it.

III. **Hard to Confirm without Scanning:** Consumers cannot readily preview the URL behind a QR code, unlike links in emails or text, there is a greater chance of inadvertent engagement.

3.3 Mechanics of a Quishing Attack

- **How attackers create malicious QR codes**

  Fundamentally, quishing is very similar to phishing in the abuse of links to trick the victim into interacting with them. The ability to track a user into scanning a QR code is often based on false context; an e-mail containing text and graphics falsely creating the impression that it is something the user would be interested in.[18]

- **Social engineering tactics used to lure victims into scanning the codes**

  Another conducive factor to quishing, at least for now, is that humans do not get much help in spotting malicious QR codes. Incorporating security primitives in QR codes could help, but creates an overburdening computational delay (e.g. users start aborting the scanning). A trusted organization could create a QR code with distinctive properties, e.g. logos or a complex color scheme but it is increasingly trivial for attackers to duplicate and impersonate such codes[18]

- **The Technical execution of a Quishing attack**

  These phishing websites could request customers' credit card details. Furthermore, we are aware that different phishing URLs use different protocols. This query string will redirect you to another malicious website. Vectorizing URLs was made feasible by translating a collection of texts from URL records into a matrix of token counts. [19]

3.4 Impact of Quishing Attacks

Cyber criminals exploit QR codes to deceive users into scanning them, often leading to credential theft, malware downloads, or financial fraud. Unlike traditional phishing attacks that rely on deceptive emails or messages with visible URLs, quishing leverages the opaque nature of QR codes, making it difficult for users to assess their legitimacy before scanning. While URLs are the most common payload in quishing attacks,

QR codes can encode a variety of data types beyond web links, broadening the attack surface. They can be used to store Wi-Fi credentials, trigger app deep links, initiate crypto currency transactions, add contact details, share geolocation data, send SMS messages, schedule calendar events, or even display plaintext phishing messages. This versatility allows attackers to craft social engineering tactics that do not rely solely on malicious URLs, further complicating detection efforts[20]

3.5 Challenges in Quishing

- **Direct theft:** Attackers steal money by gaining access to bank accounts or payment systems.

  Fraudulent transactions: Criminals use stolen credit card details to make unauthorized purchases.

  Business losses: Companies may suffer financial damage due to ransom ware, fund diversion, or regulatory fines.

- **Data Breaches & Identity Theft**

  Personal data exposure: Phishing can lead to the theft of Social Security numbers, addresses, and medical records. Corporate data leaks: Employees falling for phishing scams may expose sensitive company data (customer records, intellectual property). Identity fraud: Stolen information can be used to commit identity theft, open fake accounts, or apply for loans.

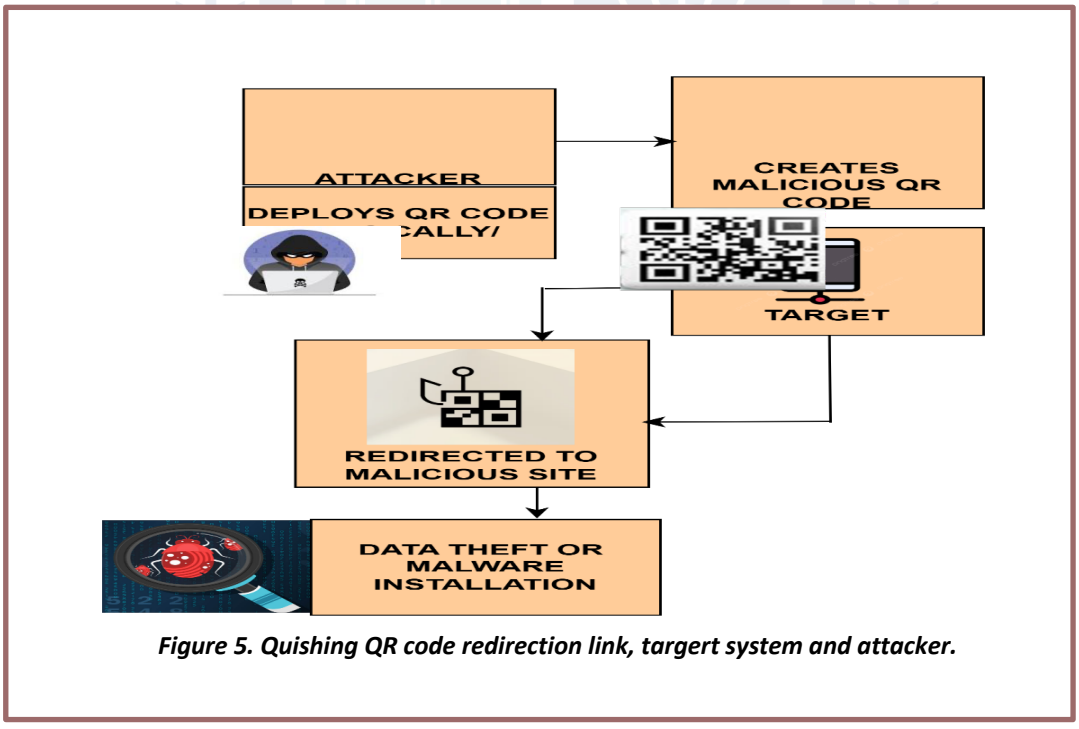

Figure 5. Quishing QR code redirection link, targert system and attacker.

3.6 Real World Example on Healthcare

According to a 2021 survey conducted by the Ponemon Institute and Proof point, the cost of phishing attacks quadrupled from 2015 to 2021. The same research found that the average cost of a successful phishing attack in 2021 was $14.8 million. Phishing is a common tactic for hackers to use against the health sector because it often leads to data breaches, and the stolen health data has the potential to be lucrative for the attackers. The 2021, the Healthcare Information and Management Systems Society found that the most common attack impacting healthcare organizations was phishing, comprising almost half of all attacks.[17]

3.7 Mitigation Strategies on Healthcare

Preventing successful phishing attacks begins with defense in depth.

I. The first layer of protection for any enterprise will likely be at its e-mail server, which will have a connection to the Internet. Ensuring that your mail server is configured to filter unwanted e-mails, or an additional platform is integrated into your information infrastructure, such as a spam gateway filter, will serve this purpose. These will not prevent all phishing e-mails, but they should strip away some unwanted traffic.[17]

II. Second, awareness training for end users is imperative. They should be trained to detect a phishing e-mail and interact with all e-mail with a healthy degree of skepticism[17]

III. Third, multi-factor authentication is highly recommended. This will protect against stolen credentials, which can be the initial purpose of a phishing attack [17]

IV. Fourth, security software should be in place, filtering, and endpoint security software deployed to and frequently updated on every end user's system is highly recommended. This type of software may detect malware as it is being executed on a system, if a phishing e-mail is interacted with by a user[17]

4. Comparison Table of Smishing, Vision and Quishing

Criteria	Smishing	Vishing	Quishing
Definition	Phishing via SMS or text messages	Phishing via voice calls or VoIP	Phishing using QR codes
Medium Used	Mobile phone messaging apps	Phone calls or voice messages	Printed or digital QR codes
Primary Goal	Trick users into clicking links or revealing data	Coerce users into giving up personal information	Redirect users to malicious websites via QR scan
Common Techniques	Spoofed numbers, fake delivery alerts, offers	Impersonation of banks, tech support, govt. agents	QR codes on posters, emails, fake ads
Target Devices	Smartphones, tablets	Any phone (landline or mobile)	Smartphones with camera and QR scanner
Social Engineering Use	High: urgency, fear, fake rewards	High: emotional pressure, authority impersonation	Moderate: relies more on curiosity or convenience
Detection Difficulty	Moderate: can be filtered with SMS scanning tools	High: hard to trace VoIP calls	Moderate to High: QR code content is hidden
User Awareness Level	Growing, but many still fall victim	Lower: people trust voices more than texts	Low: users often unaware QR codes can be malicious
Examples	“Your package is pending, click here…”	“This is your bank, confirm your PIN…”	“Scan to win”, “COVID tracing update QR code”
Mitigation Measures	SMS filtering, link scanners, user education	Call authentication tools, awareness campaigns	QR code scanners, educate not to scan unknown codes

5. Conclusion

The strategies used by cybercriminals to take advantage of people and organizations are constantly changing along with the digital landscape. By taking use of the growing popularity of mobile devices, telecommunications platforms, and new technologies, emerging phishing trends like smishing (SMS phishing), vishing (voice phishing), and quishing (QR code phishing) mark a dramatic departure from conventional email-based attacks. These techniques are becoming more complex, individualized, and challenging to identify, underscoring the pressing need for improved user knowledge, strong security procedures, and flexible technology solutions. Beyond prevailing patterns, the emergence of deep fake schemes, multi-channel attacks, and AI-driven phishing indicates that phishing will continue to be a dynamic and changing danger. A proactive and comprehensive strategy is needed to counter these threats, combining industry collaboration, state-of-the-art security tools, and ongoing education to protect against this dynamic cyber threat.

6. Reference

[1] A. K. Jain and B. B. Gupta, "Rule-Based Framework for Detection of Smishing Messages in Mobile Environment," *Procedia Comput. Sci.*, vol. 125, pp. 617–623, 2018, doi: 10.1016/j.procs.2017.12.079.

[2] D. N. Njuguna, J. Kamau, and D. Kaburu, "A Review of Smishing Attaks Mitigation Strategies," *Int. J. Comput. Inf. Technol.-0764*, vol. 11, no. 1, Mar. 2022, doi: 10.24203/ijcit.v11i1.201.

[3] H. Mustafa, W. Xu, A.-R. Sadeghi, and S. Schulz, "End-to-End Detection of Caller ID Spoofing Attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 3, pp. 423–436, May 2018, doi: 10.1109/tdsc.2016.2580509.

[4] A. Jamil, K. Asif, Z. Ghulam, M. K. Nazir, S. Mudassar Alam, and R. Ashraf, "MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook," in *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA: IEEE, Dec. 2018, pp. 5040–5048. doi: 10.1109/bigdata.2018.8622505.

[5] M. Zaoui, B. Yousra, S. Yassine, M. Yassine, and O. Karim, "A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Toward Effective Mitigation Strategies," *IEEE Access*, vol. 12, pp. 72224–72241, 2024, doi: 10.1109/access.2024.3403197.

[6] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Comput. Secur.*, vol. 132, p. 103387, Sep. 2023, doi: 10.1016/j.cose.2023.103387.

[7] F. A. Manurung, Munawir, and D. Pradeka, "Spam and Phishing Whatsapp Message Filtering Application Using TF - IDF and Machine Learning Methods," *Green Intell. Syst. Appl.*, vol. 5, no. 1, pp. 1–13, Jan. 2025, doi: 10.53623/gisa.v5i1.551.

[8] S. Mishra and D. Soni, "DSmishSMS-A System to Detect Smishing SMS," *Neural Comput. Appl.*, vol. 35, no. 7, pp. 4975–4992, Mar. 2023, doi: 10.1007/s00521-021-06305-y.

[9] M. Tariq Banday, "Effectiveness and Limitations of E-Mail Security Protocols," *Int. J. Distrib. Parallel Syst.*, vol. 2, no. 3, pp. 38–49, May 2011, doi: 10.5121/ijdps.2011.2304.

[10] A. Tsunoda, "Investigating Threats Posed by SMS Origin Spoofing to IoT Devices," *Digit. Threats Res. Pract.*, vol. 5, no. 4, pp. 1–12, Dec. 2024, doi: 10.1145/3696011.

[11] I. H. Sarker, "Research Issues in Mining User Behavioral Rules for Context-Aware Intelligent Mobile Applications," Oct. 30, 2018, *arXiv*: arXiv:1810.12692. doi: 10.48550/arXiv.1810.12692.

[12] "CONCEPT OF VISION."

[13] "2103.12739v2."

[14] "The_analysis_of_social_engineering_."

[15] A. E. Chichwadia and N. Mpekoa, "Detecting Smishing and Vishing Attacks using Machine Learning," *Int. J. Intell. Comput. Res.*, vol. 15, no. 1, pp. 1234–1241, Jun. 2024, doi: 10.20533/ijicr.2042.4655.2024.0151.

[16] "767f1a0b59241845f47547ff90cac3042afd."

[17] "Quishing on health sector."

[18] F. Sharevski, A. Devine, E. Pieroni, and P. Jachim, "Gone Quishing: A Field Study of Phishing with Malicious QR Codes," Apr. 08, 2022, *arXiv*: arXiv:2204.04086. doi: 10.48550/arXiv.2204.04086.

[19] G. A. Amoah and H.-A. J.B., "QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)," *Int. J. Comput. Appl.*, vol. 184, no. 33, pp. 34–39, Oct. 2022, doi: 10.5120/ijca2022922425.

[20] F. Trad and A. Chehab, "Detecting Quishing Attacks with Machine Learning Techniques Through QR Code Analysis," May 06, 2025, *arXiv*: arXiv:2505.03451. doi: 10.48550/arXiv.2505.03451.