Voice Phishing Attacks

Ujjwal Saini

Student BSC HONS (Computer Science)
Hansraj College Delhi University

Abstract - *Voice Phishing also known as vishing is a type of criminal fraud in which a fraudster or a bad guy use some social engineering techniques to steal the personal and sensitive information of a person over telephone lines. This research paper gives a brief information about the term voice phishing what exactly it is, describes the modus operandi that is used by these fraudsters nowadays. This paper also includes some case studies or some examples that are common in present times that based on survey. This paper also brief you the protective measures that a user can take to safeguard his/her personal information*

1. INTRODUCTION

Voice Phishing/Vishing is a technique in which a scammer or an attacker uses fraudulent calls and trick the user to give their personal information. Basically vishing is new name to an older scam i.e. telephone frauds which includes some new techniques to steal information from a user. Vishing is similar to fishing in which a fisher catch fishes in their trap similarly in vishing attacker catch user to give their personal information. Vishing frequently involves a criminal pretending to represent a trusted institution, company, and bank or government agency. You may be asked to buy an extended warranty, offered a "free" vacation or a lottery, or they may tell you that your credit card is expired or in locked stated and asked you to confirm your personal details which include:

1: OTP (One time password)

2: Credit/Debit card number

3: CVV (Card Verification Value)

4: Expiry Date

5: ATM pin

6: Internet Banking Login id and other personal details

1.1 How vishing impacts you?

Cybercriminals may use phishing scams to steal credentials (e.g., usernames, passwords) and other personal information to gain access to personal or work accounts to steal money, financial or health data, trade secrets, or other sensitive information, or to carry out other crimes, such as identity theft, corporate espionage, or extortion, among other acts. The information obtained through phishing scams can also lead to further victimization. For example, if a user's personal information (e.g., name, address, telephone number, email account) is posted online, other criminals may use this information to commit other crimes against the victim (e.g., stalking, harassment, burglary).Victims may even be at risk of becoming suspects in crimes committed by a criminal using their identity or credentials. For example, the cybercriminal may use the victim's credentials to steal money from their employer via an illegal wire transfer.

2. Examples of Vishing Attacks

2.1 Traditional method of fraud

Your phone rings the number that pops up appears to share your area code, or perhaps registers as the name of a business you recognize. Thinking it's from someone local, you pick it up and give a greeting.

On the other end of the line, the modus operandi may differ case to case as follows:

- May be a noticeably robotic voice tells you that your bank account has been compromised. To secure your account, you'll need to call the given number.
- There may be a person who pretend him as an executive of a xyz company and claims that you won a lottery amount/ reward points.
- There may be a person who claims to be an executive of an e-wallet services (PhonPe, Paytm etc.) and claims that your KYC is not completed.

In all the above cases after claiming any of the above scenario they will ask you for your personal details like your bank account details, sometimes they will ask you for OTP also and the moment when you share all the details you will become the victim of the fraudsters.

2.2 Reversing the direction of payment

In this situation the fraudsters call the victim. The fraudster try to make random family connections with victim. They will convince you that they are your colleague.

Fraudster will say that he has to take money from someone and try to convince you to take that money in your PhonPe, GPay or any other e-wallet. The moment victim agree then his game starts. They send small amount in victim's account first. Then they change the direction of the payment instead of sending money they will request the money. Victim will not notice that and he accept the request and the money will deduct from victim's account.

2.3 Fake YouTube sponsorship fraud

If you are YouTube Content Creator then you need to be careful because your YouTube channel might be in the eyes of a hacker. Hackers are largely targeting YouTube Accounts and hacking YouTube channels by fake Sponsorship calls and proposals.

Change ownership of YouTube account through malware

Your phone rings the number that pops up looks like a genuine number and you pick up the call. The person on the other side of the call claims himself/herself to be executive/worker of the reputed xyz company. They offer very good deal of sponsorship. Their way of talking is too convincing.

The moment when you agree to their offer they will send you the link of their app and they tell you to install their app on your device and you install the app on device on which your

YouTube account also logged in the malware also execute which sends your session details to attacker.

The attacker uses the session to log in to your account. Remember for this, attacker doesn't need your YouTube account password. The next step of the attacker is he/she change the ownership of the account unfortunately Google doesn't ask for password. And your YouTube account is transferred to the attackers Google account.

2.4 Corona Scams

Scammers are taking advantage of the fear and uncertainty surrounding the COVID-19 coronavirus. Some of the most common scams are described below:-

- **Fraudulent Medicines and Treatment**: There currently are no vaccines, pills, other prescription or over-the-counter products available to treat or cure Coronavirus disease 2019 (COVID-19)—online or in stores. Any caller that claims is a fraud/scam. And remember if in future any medicine will come that will not be sold online or on calls.
- **Insurance and Medical Billing Scams** : A number of scams now involve offers of insurance, frequently using phone calls that pressure the recipient by referring to the coronavirus outbreak. These scams may attempt to obtain personal information or payments for the fake insurance.
- **Fake job offers**: These are scams designed to trick you out of you money, personal information, or both. These are a variation on fake job offers
- **Fake Charities and Political Donations**: A similar form of fraud involves calls, texts, and ads asking for signatures to political petitions related to coronavirus and soliciting donations

2.5 Preventions against these frauds

- Always remember that any bank or their representatives never calls their customers to ask for personal information, password, OTP. Any such call is an attempt to fraudulently withdraw money or sensitive personal information from you.
- Use applications like Truecaller always flag these kind of fraud number's on these apps as spam or if you are receiving unknown call cross check if it not already flagged as spam.
- Keep a cool head and hang up the phone if you notice something suspicious. If you still feel afraid, or feeling confused, wait 10 minutes and then call your bank, credit card company, or whoever the caller claimed to be. Then verify whether there is a real problem.
- If someone force you into giving them sensitive information, hang up.
- Always notice the direction of the payment that is it a pay money request or not.
- Always aware of the guidelines published by the government against these frauds.

3. CONCLUSIONS

Security threats are constantly evolving, and wearing new shapes to avoid detection. Voice Phishing attacks are not new to the threat landscape, yet we can see this attack vector being continuously reinvented. Mobile devices will continue to play a significant role in the future attack vectors against because it becomes very easy for an fraudster to fool the individual over the call because victims often saw the risk eclipsed by the potential gain of a prize. We needs to continue to raise awareness for these lurking threats, and ensure that our peers, colleagues, friends and family understand the risks and avoid sharing their sensitive information. **After all our safety is in or hands.**

ACKNOWLEDGEMENT

We express our sincere gratitude to Gurugram Police(Haryana India) for providing us an opportunity to be part of this Gurugram Police Summer Internship 2020 to complete this Paper on "**Voice Phishing Attacks**".

REFERENCES

[1] https://safecomputing.umich.edu/be-aware/phone-scams
[2] https://www.consumer.ftc.gov/articles/0208-phone-scams
[3] https://safecomputing.umich.edu/be-aware/scams/coronavirus