

Protect yourself from Vishing Attack!!

 blogs.quickheal.com/protect-yourself-from-vishing-attack/

December 23, 2022



“Humans are the weakest link in cybersecurity.” Data breaches worldwide prove this accurate, as human errors, lack of awareness, ignorance, or negligence cause these breaches. Social engineering is the attack that exploits human behavior and human nature, and there are different ways to perform this attack. Attackers often manipulate and convince users with valid authority, intimidate users, build relationships with them or try to create a perception. Users fall prey and tend to believe the object is scarce, there is an urgency, and immediate action is required.

Vishing is social engineering attack and is a type of [phishing attack](#). In this attack, the attacker uses psychological manipulation and calls the victim with the intent to steal information. They use this manipulation to trick victims into handing over sensitive information or performing some action on the attacker’s behalf. This attack is also called voice phishing.

Vishing has been actively used in the recent past, and many unsuspecting users have ended up becoming the target of such attacks. In one common method for such attacks, the attacker asks the victim to install a screen-sharing application like AnyDesk or TeamViewer from Google Play Store from which they make the crime. One of them recently observed

was trending on Twitter. In this case, the attackers target users complaining about bad service on Twitter. In this campaign, various applications are used, as illustrated in the following example:

Social Engineering - Vishing (Voice Phishing)

Fig. 1 Attack Flow

It has been observed that many people prefer to share their displeasure with a deficiency in service or product in online forums rather than contacting the official customer support channels. Typically, the thought behind publicizing their dissatisfaction on public platforms is to highlight their issues, force corrective action, and expedite the grievance resolution. Some users post their contact details, like email or phone numbers, in their tweets for faster action – anticipating that the right officials would contact them to address their concerns. However, the users tend to miss them because these tweets are posted in the public domain, and everyone – including the mal-intentioned folks can see their details.

Threat actors keep looking for such tweets. Most of the time, they get the contact details of the target from different social media accounts or by purchasing dumps from the dark web. They then call the user and try to convince them to download a contact support application presented as a tool to resolve their issue. They share the application via Email or WhatsApp as well. However, this application is an SMS Trojan that forwards incoming messages from the user's mobile to the attacker's number & this methodology is used for stealing the OTP.

As users tweet and share their contact details, they expect calls from “official” representatives. Attackers often take advantage of this situation in this campaign.

Our team observed some tweets complaining about the services of IRCTC, PhonePe, SBI Bank, PNB Bank, Mobikwik, Meesho, CRED, Airtel India, Flipkart, etc.

The following screenshots of such tweets illustrate the vishing attempts that have become prevalent in recent times:

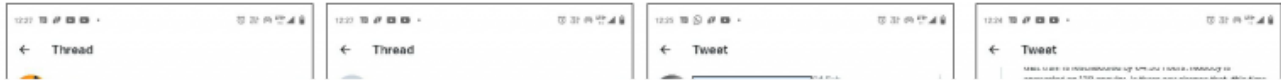


Fig. 2 User Tweets

Some users have shared screenshots of WhatsApp messages in which the attacker sent the application to them via WhatsApp. File names used by these attackers for these applications are –

“Online Complaint.apk,” “PNB_Support.apk”, “Customer Support.apk,” etc.

Fig. 3 Screenshots of WhatsApp message sent by the attacker

The attacker uses official logos of popular banks like ICICI bank and Punjab National Bank, finance institutions like Mahindra Finance and Bajaj finance, and some courier delivery service providers like Blue Dart Express and JNI Express to deceive unsuspecting users.



Fig.4 Icons Used by Malicious application.

When this application is launched, it asks permission to send and receive messages. Once the users grant these permissions, it sends these messages to the attacker. The application also asks the user to enable auto-start in settings.



Fig. 5 Application asking for SMS permissions

Fig.6 shows the code used to access the SMS messages; depending on conditions, this data is sent to a constant phone number from the code or number obtained from shared preference.

Fig.6 SMS access and sent.

Fig. 7 shows the code used to delete the SMS data, showing that the messages were sent from the user's mobile inbox to the attacker's number. This effectively erases the track of this fraudulent activity.

```
public void deleteSMS(Context context, String str, String str2) {
    try {
        Log.d("Sms", "Deleting SMS from inbox");
        Cursor cursor = context.getContentResolver().query(Uri.parse("content://sms/inbox"), new String[]{"_id", "address", "body", "date", "read", "status", "type", "uri"}, null, null, null);
        if (cursor != null) {
            cursor.moveToFirst();
            while (cursor.moveToNext()) {
                String id = cursor.getString(0);
                String address = cursor.getString(1);
                String body = cursor.getString(2);
                String date = cursor.getString(3);
                String read = cursor.getString(4);
                String status = cursor.getString(5);
                String type = cursor.getString(6);
                String uri = cursor.getString(7);
                context.getContentResolver().delete(Uri.parse("content://sms/inbox/" + id), null, null);
            }
        }
    } catch (Exception e) {
        Log.e("Sms", "Error deleting SMS from inbox: " + e.getMessage());
    }
}
```

Fig.7 Code to delete sent SMS data

In this campaign, voice calls, i.e., the vishing technique, propagate these applications. Earlier, our investigations revealed a phishing page asking for credit and debit card credentials and distributing such applications. It was a fake page of Patanjali Yog gram registration. The application dropped by this site was also an SMS stealer Trojan.



Fig. 8 Patanjali phishing page

Attackers use different means to reach users. For example, they share SMS or WhatsApp messages about electricity bill updates or bank wallet KYC updates and ask to call the phone number mentioned in their ASAP. They try to create a fake sense of urgency in the message, which is one of the principles of social engineering. Following figure # 9 shows examples of such messages: –



Fig. 9 messages shared by scammer about the electricity bill

Such applications are evolving, and attackers are adding new features in the latest versions to continue targeting users. Attackers are improvising day by day and using different techniques to attack. Everything we do in public online forums is susceptible to being misused by these attackers, and we need to be very cautious while using social media.

Quick Heal detects all such applications with **Android.SMForw.GEN50605**.

Tips to be safe:

- Do not post personal details like contact number, email Id, or address on public platforms.
- Caller IDs can be tampered with – so don't trust them, as they can give a false sense of security.
- Don't download any application sent/shared from an unknown sender.
- If you receive a phone call from anyone requesting personal information or asking to download the application, don't respond.
- Wherever possible, try to record the details of fraudsters and share them with your bank (whom they were trying to impersonate) so they can take action against them.
- Try to limit yourself to known apps from known developers and keep only those really required apps.
- Use a reliable mobile antivirus (like [Quick Heal Total Security](#)) that can prevent fake, malicious apps, adware, etc., from getting installed on your phone.

IOCs

Package names:

One.enix.smsforward

com.myapplication.customersupport

Com.helpdev.sbquicksupport

MD5s:

A6658102CE9FC5CE78BE37186F30354A

33132BFE2E46C010D05E589162F012F1

743E185E03C05D9D2DEF00A157B8A03F

E7ACE2B70410465953623BFED6F3CBEC

3C4EE2DCF5B6B68A7C6C6E1AFB15EB4D

26D58549A1280362911D4C97FD1C8C94

6186AF5576D4E050CD335686296F1120

B250D9216695CC97B03BAB5F787FB553

4384E3B02CEE05630C08FF4AD536297C

F89E929B7D4C8C0092975DA91040C7D9
CC3F33F088EF7EEBAE63C92F8CF33DD7
6889570124B98857A4F4413F377E5FAC
4B5A7B6656ED90A2BC0E47C4773DF7C9
C6DCEC98AE97150A26049BB697E3CDCF
6864BDB5E33456C635EA3CF38826D3C8
C5C4DD3B9C6599B718DD7A9BAC3FA615
B12DD1A89ABB76741E5E8CD9AD6B6C09
A54EB0072B66DC0D1DFBCE9D948E67C8
0E41B1D777381AD71CFA7A89921013FE
4B24778268E7250EAECC17B086252C49
B72681BF5CDFE044EBF6F6AE35BEFD1E
157731bb6f7163134df4274ca763340e
2882f0acc188590ea0f8d6ef059a841b
2ade1007f5181234bd15c931311dc2c4
39645e267f41c0899910063497538571
4c14d7bbcc303b4f4a010542d2b469d6
608d4f8b1b5c169678ffc08283a37eda
a74141a04a85ad9468e62b7cbf9bddfa
c1bdd659c25ce5aaf78653d9c1d604f0
D67985629353161c8c27ef24b51155ea



Digvijay Mane
