Help! Help! How your online search can lead to 'helplines' that rip you off

Mayur Shetty & V Narayan TNN

Helpline frauds are increasingly the scourge of digital payments. Dozens of unsuspecting callers have been swindled after calling up fake helpline numbers placed online.

It happens when consumers seeking a solution to a problem do a Google search and call up any helpline number that it throws up; most do not bother to look up the organisation's website or the papers they may hold to locate the official phone numbers.

Mumbai resident Ruchira Damia lost Rs 40,000 when she tried to contact an HP Gas agency. "I called HP Gas after getting its number on Google search. The customer care executive asked me to fill a link that they sent me. The moment I clicked it four transactions were carried out from my account and I lost Rs 40,000," said Damia. She has filed a complaint with the police.

Methods used by confidence tricksters range from payment requests made on the Unified Payments Interface (UPI) to sharing of QR codes on WhatsApp. And going by reporting of incidents with Mumbai's cybercrime cell, scores of people are losing money because they called up numbers obtained through Google or Justdial.

AN UNREGULATED FIELD

Two developments have created an enabling environment for fraud—the explosion of smartphones with internet, and multiple modes of payment through apps.

Cyber expert Ritesh Bhatia said there are two ways fraudsters add a number under listings on a Google search page. They either create or claim a Google My Business account using their number, or 'suggest' their own number using the 'suggest an edit' feature. In either case, they are able to pass themselves off as, say, a liquor shop or a bank or a service centre. Google does a verification by post for Business accounts, but no physical verifications.

To make it easier for fraudsters, new forms of payments like UPI offer scope for confusion. Many are unaware that they do not need to share information in order to receive payments and that a UPI handle (xyz@abcbank) is enough to receive money.

WEEDING OUT LINKS

According to Dilip Asbe of the National Payments Corporation of India (NPCI), the corporation is now working with online providers to weed out fake helpline links.

NPCI and banks are also pooling funds to spread awareness.

Sameer Nigam, founder of PhonePe, which contributes nearly a third of total UPI transactions in India, said, "A lot of platforms which are designed to be based on crowdsourced information or user-generated content are being taken advantage of by fraudsters. The companies are cooperative whenever we reach out

with specific cases. However, what we want to see is more of a proactive approach from platforms like Google, Twitter, Facebook, etc in the detection of fraud."

PhonePe has urged them to enable businesses to automatically take down false details and react in real-time in cases where fake information is being displayed, he said.

"All establishments should perform a search on Google and if their business has been listed without their knowledge, they must contact Google and get their listing removed or corrected. It is also recommended that all establishments get themselves listed on Google My Business before a fraudster claims it for identity thefts," said Bhatia.

Google in response directed **TOI** to its blog, according to which it is a constant see-saw: when scamsters are shut down, they come up with new forms of deception. "But we can't share too many details about these efforts without running the risk of actually helping scammers find new ways to beat our systems," Google said. According to the company, it has taken down over 3 million fake business profiles—and more than 90% of them were removed before a user could even see the profile. Google's internal systems triggered 85% of the removals and 2.5 lakh fake profiles were reported by users.

Fraudsters also manipulate individuals into divulging confidential information by tapping into social media. Information generated on social media platforms gives criminals a peek into a potential victim's behaviour. To counter it, PhonePe has been engaging social media giants to take down fraudulent 'user-generated content' used as clickbait.

A Twitter spokesperson said recent initiatives have enabled it to act against scamsters who use phishing, or other fraudulent methods. "The policy is aligned to support the efforts of the government of India."

Mumbai police cybercrime cell's deputy commissioner Vishal Thakur said it is also incumbent on users to avoid looking for contact details of establishments through search engines. "Not knowing the authenticity of contact details found through a search engine, people get duped. If anyone is looking for customer care numbers to file a complaint or to place an order online, they should visit the webpage of the organisation," said Thakur.

Online platforms may be liable under IT law

Banks often record disputes from customers who have fallen for frauds. There are times when they halt or reverse suspicious transactions. But more often than not they disown liability in cases where customers have shared their PIN. Recovering money from a recipient through the legal route in such cases is a challenge as they are often in a different state. Besides, the fraudsters are quick to withdraw money from their own accounts.

According to advocate Prashant Malli, who specialises in cybersecurity, even if banks do not accept liability, online platforms like Google and other social media platforms are liable for enabling fraudsters.

"Section 79 of the Information Technolgy Act is a 'safe harbour' provision under which intermediaries are granted immunity from liability for third party acts. However, this is conditional, and they are required to have done their due diligence," said Malli. "Because they did not do due diligence as required under section 79(2)(c) the safe harbour provision under S79 is not applicable,"

DO NOT

- Share card number, expiry date, PIN, OTP, etc. with anyone
- 'Pay' or enter your UPI PIN to receive money
- Download and install third-party apps such as Screenshare, Anydesk, Teamviewer to enable/receive payments
- Search for helpline numbers on Google, Facebook, Twitter. Check official site
- Respond to texts, emails from unknov addresses to click on links

TYPES OF FRAUD

While there is enough protection built into UPI and card payments fraudsters use various tricks to get users to part with critical information

Request Money Fraud

Fraudsters misuse the request feature on UPI by sending fake payment requests with messages like 'Enter your UPI PIN to receive money, "Payment successful receive Rs. xxx" etc. You need to ent PIN only for sending money

QR Code Fraud

Fraudsters share a QR code over WhatsApp asking for the code to be scanned to receive money in their account. This QR code, a featu in some UPI apps, is in fact a collect request and scanning and entering

he added. TNN

TYPES OF FRAUDS

While there is enough protection built into UPI and card payments, fraudsters use various tricks to get users to part with critical information

Request Money Fraud

Fraudsters misuse the request feature on UPI by sending fake payment requests with messages like 'Enter your UPI PIN to receive money, "Payment successful receive Rs. xxx" etc. You need to enter PIN only for sending money

QR Code Fraud

CASES OF E-SCAMS

Seecha Vajpayee, a 25-year-old IIT student, became a victim of an Unified Payments Interface (UPI) fraud when three transactions for a total Rs 27,000 were done through her account. The fraud took place when Vajpayee tried to get in touch with the customer care of an online food service for a refund for a "bad quality pizza" delivered to her on October 27. Police found that the customer care number had been replaced to dupe callers

Fraudsters share a QR code over WhatsApp asking for the code to be scanned to receive money in their account. This QR code, a feature in some UPI apps, is in fact a collect request and scanning and entering your PIN is acceding to their request. Again you need to scan QR only to make payments

Remote Access App

Fraudsters ask users to install screen-sharing apps such as Screenshare, Anydesk, Teamviewer and use them to get access to bank credentials. These apps are not malware, but they do grant access of your mobile data to the third party

Social Media/ Impersonation Fraud

Fraudsters track complaints in social media and share fake contacts or impersonate bankers or RBI officials in response to a post and ask for confidential information which no banker is supposed to ask for

SIM Swap Fraud

Fraudsters manage to get a duplicate SIM which provides them access to one-time passwords. They do this by pretending to be from a mobile company and asking you to forward an SMS containing the SIM card number to activate the duplicate SIM

A deputy manager with a mobile service provider lost Rs 1.25 lakh when he placed a home delivery order for a wine bottle on October 12. The money was gone within seconds after he called the contact number of Ujwal Wines in Andheri (East), Mumbai, that he found through an online search. The police later informed the victim that the owner of Ujwal Wines had filed a complaint that someone had misused their shop name to draw customers keen on home delivery