Beware of fake customer care numbers you find on Google

Shipra Singh
shipra.singh@livemint.com

Google is the go-to place for most of us when we want to search for customer care coordinates of a bank or merchant to register a complaint. Fraudsters are taking note and using this habit to siphon money off gullible consumers.

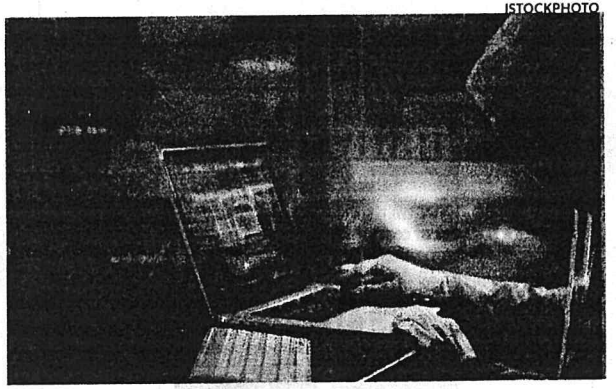
In a sophisticated phishing scam gaining ground on the internet, scamsters are meddling with the customer care numbers of reputed companies and financial institutions on platforms such as Twitter, Google and Facebook to misdirect consumers into calling them.

This is done in several ways. The most commonly practised method is where conmen modify customer care coordinates of a company on Google and use SEO to push their fake number at the top of the search results. As a consumer goes looking for a service provider's customer care coordinates on Google, they fall for the trap by dialling the first number from the search results.

Not just Google search engine, frauds also replace the original contact coordinates of popular retail stores and banks on Google Maps with their own. Google Maps allows editing rights to all users, making it the easiest platform for frauds to tinker with.

Twitter and Facebook are the other two mediums where frauds tamper with customer care coordinates. They closely follow complaints being raised by consumers on Twitter and immediately respond to those posts to provide their fake numbers before the company can take note.

Another method is where frauds create industry blogs, say on e-commerce shopping, on platforms such as Medium and post fake numbers posing as customer care coordinates of companies belonging to that industry (e-commerce merchants in this case). They are also part of community groups and follow company blogs to keep a track of consumers complaining in the comments section and are quick to leave their numbers as a response to those comments.



ISTOCKPHOTO

The usual modus operandi of phishing attacks involves a fraud posing as a customer care executive calling the customer up to elicit sensitive banking information. In this scam, since the consumers are manipulated into calling the frauds, and not vice versa, it gets so much easier for fraudsters to commit the crime.

Last week, State Bank of India (SBI) tweeted a video alerting their consumers of such scams. "Beware of fraudulent customer care numbers. Please refer to the official website of SBI for correct customer care numbers. Refrain from sharing confidential banking information with anyone," tweeted SBI.

How to prevent online fraud: The easiest way to prevent this fraud is by calling up the customer care number provided only on the website of the service provider. Alternatively, you can look for customer grievance redressal section on the merchant's mobile application.

Twitter handles of most big companies and banks are verified; so one must pay attention to the Twitter handle that responds to the post. Another red flag is if the customer care executive of the concerned company sends you a direct message (DM) on Twitter. Typically, merchants respond on the Twitter post as a comment and don't send a DM until you initiate a private conversation over DMs on the company's official handle.

Most important, do not share banking details, such as card number, CVV, ATM PIN, banking passwords and one-time-passwords (OTP) with anyone over the phone or e-mail under any circumstance.

As a general practice, no bank or reputed company asks its customers for confidential details over phone or email.

Where to report if you are defrauded: Write to your bank immediately. Most banks have listed their toll-free helpline numbers on their respective websites.

Payment companies, e-commerce merchants and food delivery companies also give their consumers an option on the website and mobile app to report a fraud.

In June, the government introduced a national helpline number 155260 and reporting platform to help victims of cyber fraud.