Cyber Crime Information – 150

March 21st, 2022

Subject: Cybercriminals using Fake Customer Care Numbers / Helplines to defraud citizens

Threat Summary

Google and Social Media are the go-to places for most of us when we want to search for customer care number of a bank/merchant. Fraudsters are using this habit to siphon money off gullible consumers.

Fig. 01 – Fake customer care numbers/Helpline

Modus Operandi

- Cybercriminals modify customer care numbers/helpline of a bank/company on google (and other search engines) and use Search Engine Optimization (SEO) to push their fake number(s) at the top of the search results. They create fake numbers of banks, financial institutions, online shopping websites and big brands, these fake numbers pop up when users search.
- Fraudsters also alter the original contact numbers of popular banks and retail stores on Google Maps, as details on Google Maps are editable.
- Fraudsters also tamper with customer care numbers on social media (Facebook, twitter, etc.). They meticulously monitor consumer complaints on Social Media and respond quickly to those messages in order to supply their fake phone numbers.
- Unwitting victims call these numbers, fraudsters speak with them impersonating a bank/company employee, fraudsters then proceed to alert victims of issues with their bank account, credit or debit cards, loans or other related matter.
- Victims are instructed to temporarily transfer funds to bank accounts provided by fraudsters in order to resolve the issue, or make payments for outstanding loans.

- Some victims receive SMS messages with headers spoofing the bank's Sender ID, so these would appear as legitimate communications from the bank.
- The cybercriminals also leverage the stolen financial information to withdraw funds from victims' accounts.

Suggestions

- Always refer official bank/company website for authentic customer care numbers.
- Avoid providing banking information such as a card number, CVV, ATM PIN, banking passwords, or One-Time Passwords (OTP) with anyone over the phone or by e-mail.
- Avoid making payments in after being suggested in a customer service help. Scrutinize thoroughly before making any such payment.
- Avoid sharing meeting details on public platforms (social media, group emails, etc.).
- Report any such incidents on the ***www.cybercrime.gov.in*** portal and follow ***CyberDost*** & ***CyberDosti4c*** on various Social Media Platforms to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207