

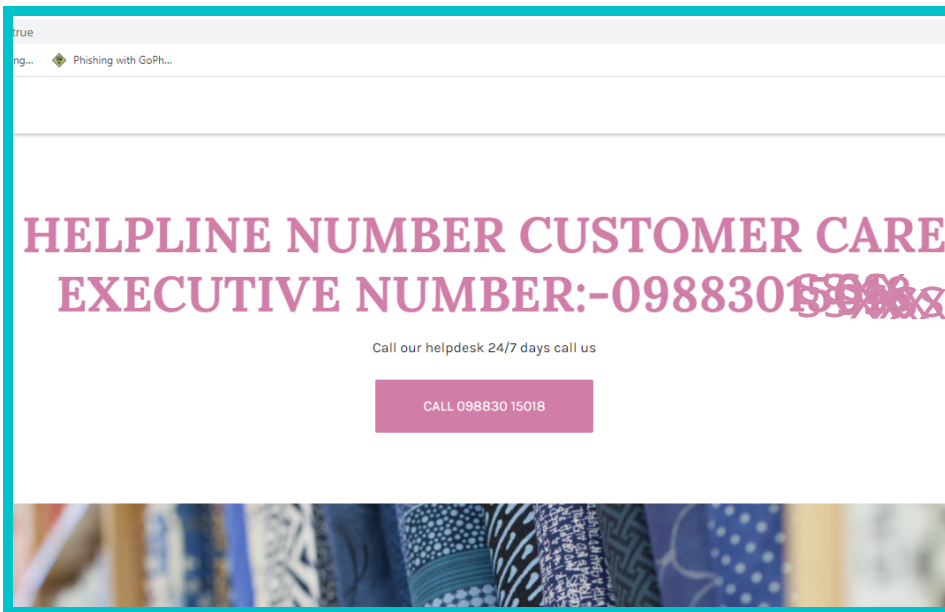
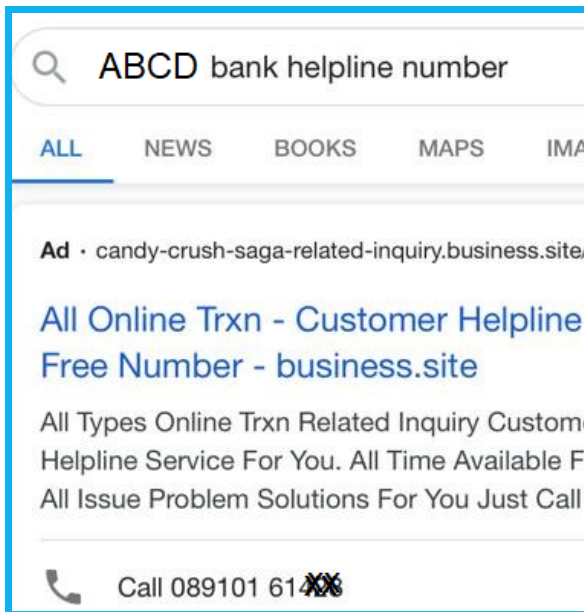
Advisory

Date: 20.11.20

**Beware of fraudulent search engine advertisements and phishing scams**

Scammers create fake business ads in search engines and these are displayed while inadvertent customers search for Bank Branch/ Office details like phone numbers. When customers contact these fraudsters unknowingly, they resort to social engineering and get sensitive details like Debit/ Credit Card number, CVV, OTP, etc. pretending to be a customer care personnel or Branch staff.

**Sample of fake advertisements:**



- Always ensure to search Branch/ Office details in official Bank website only
- Never reveal sensitive information like Card number, CVV, Expiry date, Date of birth, OTP, etc. to unknown callers
- Fraudsters may ask you to download remote screen sharing apps on your mobile. This would enable them to control your phone and steal money out of mobile banking/ wallet applications. Always be alert