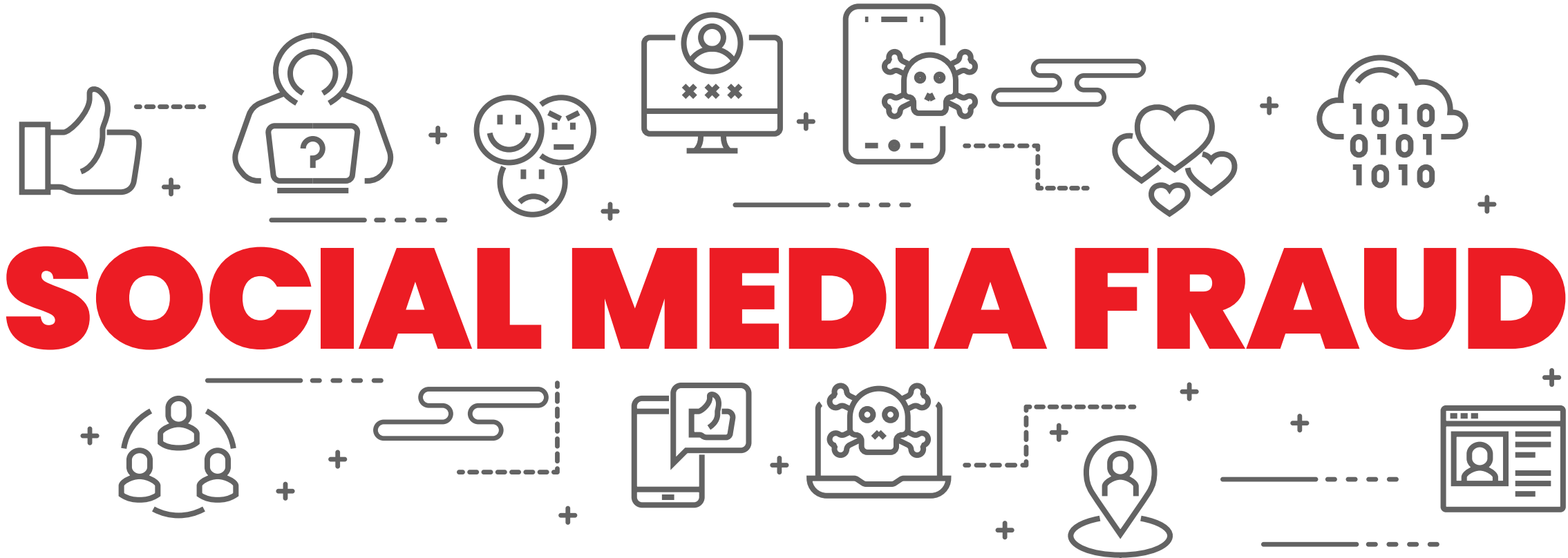


FRAUD AWARENESS

Steps businesses and individuals can take to protect themselves from cyber frauds.



Cybercriminals exploit social media to trick users into sharing personal information or sending money by pretending to be a friend.

MODUS OPERANDI



Fraudsters populate/spread fake customer care numbers of banks and UPI platforms on social media platforms.



Fake bank websites with similar design and fake UPI apps are uploaded.



Users call on these numbers, fraudsters pose as official representatives.



The fraudster extracts sensitive information and deducts money from the user's account.

Fake Profiles/users

Impersonation- Digital Identity Theft

A fraudster creates an impersonated profile of an individual without their knowledge by using acquired personal information.



The impersonator acts on behalf of the original user gaining trust of their social connects for his malicious intent.



Impersonators extort sensitive personal/business information, money, disrepute the owner or even commit crimes on behalf of the original user.



HOW TO STAY SAFE

Fake Profiles/users

Do not search for your app or bank's customer care numbers on search engines or social media.



Always visit the official website, check URLs and contact genuine numbers.



Do not share personal information containing location, frequently visited places, financial purchases, etc.



Be vigilant and watchful of any suspicious activity that you encounter related to your profile.



Immediately report impersonation or contact support and bring it to the platform's attention using your proof of identity.

Impersonation- Digital Identity Theft

