## Online scams

1. Vishing i.e., Phone Call Scam

Scammers use a phone call to get out sensitive information like your login details, username, transaction passwords, card PINs, OTPs, CVVs, URNs, grid card values, or personal data like your birth date or mother’s maiden name. Often, fraudsters pose as bank representatives and trick you into giving your personal and financial information. You must not provide any of your personal or banking information over the phone when you receive a call asking for the same.

2. Phishing i.e., Email Scam

Phishing is the activity that intends to ‘fish’ your confidential banking information. It may involve receiving an email that allegedly seems to be from a well-known institution like a bank or a trusted website. You must be aware and not click on such emails. Note that your bank would never request your private information, such as your password, login details, or OTP, among other such information.

3. Spear Phishing i.e., Targeted Email Scam

Spear phishing is a focused phishing attempt that is delivered by email. It seems to have come from a reliable source and often originates from a colleague, boss, close friend, or relative. If you click on attachments or malicious links in the email, fraudsters can easily access sensitive information stored on your device. Always avoid clicking on such fishy emails.

4. Skimming i.e., ATM Scam

For committing this fraud, scammers usually hide a small gadget called a skimmer in the card slots of ATMs or merchant payment terminals, which can read and record your card information. Fraudsters even use a carefully placed camera to record your PIN. It is advisable to stay alert whenever you visit an ATM booth to prevent such banking fraud.

5. SIM Swap i.e., Mobile Number Scam

Under SIM swap, a fraudster gets a new SIM card from your mobile service provider in your name using your registered mobile number. The scammer conducts financial transactions from your bank account by receiving the OTP and alerts needed. You must immediately report to your mobile service provider if your phone or SIM card is lost or has stopped working.

6. Smishing i.e., SMS Scam

Smishing uses SMS or text messaging to scam you. Smishing scammers use toll-free phone numbers and message links to target you. You may receive a message stating that your accounts need to be updated with a link directing you to sign up for some new scheme. By clicking on such phishing links sent in the message, your confidential details may get compromised. To save yourself from smishing, you must not click on any link without knowing its source.

7. Website Spoofing i.e., fake Website Scam

Building a fake website to commit fraud is called website spoofing. Phishers use names, pictures, logos, and even website codes to make spoof sites appear authentic. You are urged to enter your details on such fake websites. One must enter details on a website only after checking the presence of ‘HTTPS’ in the URL.

8. Malware Attack i.e., Gadget Virus Attack

A malware attack is malicious software developed by cyber criminals that can cause damage to the operating system of your smart device. Through this software, fraudsters can access your confidential banking information and use it to remove money from your bank account. It would be best to keep your devices secure with malware protection software.

Ways to safeguard yourself from Digital Banking Fraud

The best way to avoid fraud is to stay vigilant, but at the same time, you must follow some of the best practices to safeguard yourself from digital fraud in banking.

1. Never share User ID, Password, OTP, PIN or any other confidential data

2. Lost or stolen Credit Cards / Debit Cards should be blocked immediately

3. Never use open public Wi-Fi

4. Don’t reply to fishy emails or text messages

5. Avoid visiting unsafe websites & unreliable links

6. Never allow anyone to remotely access your laptop or PC