Types of Internet Fraud

Fraud can be classified into two: **Offline fraud and Online fraud.**

Most **offline fraud** incidences happen as a result of theft of your mail, sensitive information related to your bank or credit card accounts, stolen atm/debit/credit cards, forged/ stolen cheques etc. You can protect yourself from such instances by exercising caution while receiving, storing and disposing your account statements as well as your cheques, atm/debit and credit cards.

Online fraud occurs when someone poses as a legitimate company (that may or may not be in order to obtain sensitive personal data and illegally conducts transactions on your existing accounts. Often called **"phishing"**(An online identity theft scam. Typically, criminals send emails that look like they're from legitimate sources, but are not. The fake messages generally include a link to phony, or spoofed, websites, where victims are asked to provide sensitive personal information. The information goes to criminals, rather than the legitimate business.) Or **"spoofing"** (An online identity theft scam. Typically, criminals send emails that look like they're from legitimate sources, but are not (phishing). The fake messages generally include a link to phony, or spoofed, websites, where victims are asked to provide sensitive personal information. The information goes to criminals, rather than the legitimate business.) , the most current methods of online fraud are usually through fake emails, Web sites and pop-up windows , or any combination of such methods.

The main objective of both offline as well as online fraud is to steal your 'identity'. This phenomenon is commonly known as "identity theft". **Identity theft** (A criminal activity where a thief appropriates vital information such as your name, birth date, account number, or credit card number without your knowledge) occurs when someone illegally obtains your personal information — such as your credit card number, bank account number, or other identification and uses it repeatedly to open new accounts or to initiate transactions in your name.

Identity theft can happen even to those who do not shop, communicate, or transact online. A majority of identity theft occurs offline. Stealing wallets and purses, intercepting or rerouting your mail, and rummaging through your trash are some of the common tactics that thieves can use to obtain personal information. The more you are aware about identity theft the better prepared you will be.

Types of Fraud in Detail

Phishing Emails

Every user of the Internet should be aware about the common attempts of fraud through means like ‘phishing' or 'spoofing'.

'Phishing' is an attempt by fraudsters to 'fish' for your banking details. 'Phishing' attempts usually appear in the form of an email appearing to be from your bank. Within the email you are then usually encouraged to click a link to a fraudulent log on page designed to capture your details. Email addresses can be obtained from publicly available sources or through randomly generated lists. Therefore, if you receive a fake email that appears to be from your Bank, this does not mean that your email address, name, or any other information has been taken from the bank.

Although they can be difficult to spot, ‘phishing' emails generally ask you to click on a link which takes you back to a spoof web site that looks similar to your bank's website, wherein you are asked to provide, update or confirm sensitive personal information. To prompt you into action, such emails may signify a sense of urgency or threatening condition concerning your account.

The information most commonly sought through such means are:

- Your PIN numbers
- Your Internet Banking Passwords
- You Bank Account/Credit Card/Debit Card number
- Other verification parameters, like; your date of birth, mother's maiden name etc.

Some fake emails may also contain a virus known as a “Trojan horse” that can record your keystrokes or could trigger background installations of key logging software or viruses onto your computer. The virus may live in an attachment or be accessed via a link in the email.

Never respond to emails, open attachments, or click on links from suspicious or unknown senders. If you're not sure if a email sent by your Bank is legitimate, **Report it to your Bank**, without replying to the email.

Counterfeit Web sites

Online thieves often direct you to fraudulent Web sites via email and pop-up windows and try to collect your personal information. One way to detect a phony Web site is to consider how you arrived there. Generally, you may have been directed by a link in a fake email requesting your account information. However, if you type, or cut and paste, the URL into a new Web browser window and it does not take you to a legitimate Web site, or you get an error message, it was probably just a cover for a fake Web site.

Cyber Cafe Security

If you are accessing any website (including your bank wesite) from cyber cafe, any shared computer or from a computer other than that of your own, please change your passwords after such use from your own PC at workplace or at home.

It is very important to do so especially when you have entered your transaction password from such shared computer or cyber cafe computer. Change these Passwords from your own PC at workplace or at house.

Email Fraud

Beware of fraudulent e-mails requesting online banking security details!

Internet Banking is a safe way to manage your money. However, there are Internet fraudsters around who will try to gain access to your accounts by e-mailing you and prompting you to disclose your on-line banking security details to them. Banks will never send e-mails that ask for confidential information. If you receive an e-mail requesting your Internet Banking security details, you should not respond.

Please note Your Bank is NOT liable for any loss arising from your sharing of your User Ids, passwords, cards, card numbers or PINs with anyone, NOR from their consequent unauthorized use.

How do fraudulent e-mails work?

Typically you will receive an e-mail claiming to be from your bank, either requesting your security details (perhaps as part of an update or confirmation process) or asking you to follow a link to a site where you will be encouraged to provide a range of information such as your credit card number, personal identification number (PIN), passwords or personal information, such as mother's maiden name.

Clicking on the link then takes you to a fake website, designed to look like that of your bank, but operated by the fraudster.

Fraudulent e-mails and websites can be very convincing and fraudsters are continually inventing new approaches to get you to divulge your security details.

Treat all unsolicited emails with caution and never click on links from such emails and enter any personal information.

If you have replied to a suspicious e-mail and provided personal or sensitive information about your account, please call your Bank Customer Care or write to the Bank Director giving all details.

IF A CYBER CRIME HAS BEEN COMITTED THEN REPORT TO YOUR BANK AND TO CYBER CRIME DIVISION AT YOUR LOCAL POLICE STATION IMMEDIATELY.