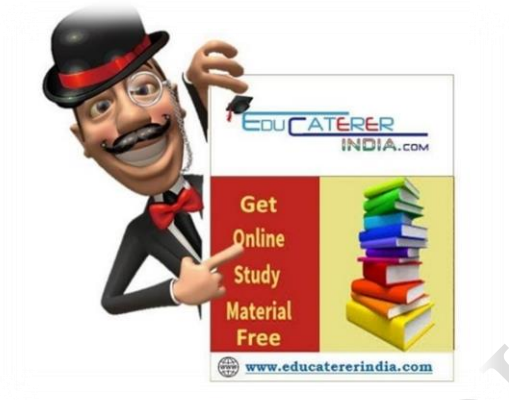
Online Banking Frauds- Things You Must Know



.

Bank being a vital element in a nation's economy deal with monetary transactions and services to the public. The personal and financial information of the bank's customer are under the threat of being misused by fraudsters.

What is a Bank Fraud?

Bank fraud is the criminal offence of knowingly executing or attempting to execute a scheme or artifice to defraud a financial institution or to obtain property owned by or under the control of a financial institution by means of false or fraudulent pretences, representations, or promises. RBI, the regulator of banks in India, defines fraud as “A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank."

Types of Frauds

Phishing :

Phishing is an attempt by fraudsters to 'fish' for account holder's bank details. A phishing attempt usually is in the form of an e-mail that appears to be from the bank. The e-mail usually encourages the Customers to click a link in it that takes them to a fraudulent log-in page designed to capture customer details. Individual's email addresses can be obtained from publicly available sources or through social networks.

Act of phishing- How is it done?

The fraudsters send fake e-mails claiming that customer information has been compromised, due to which the bank account has been de-activated/suspended, and ask customer to hence confirm the authenticity of their information/transactions like credit card number, Personal Identification Number (PIN), passwords or personal information, such as mother's maiden name. In order to prompt a response, such e-mails usually resort to using statements that convey an urgent or threatening condition concerning to bank account.

- When some emails are easy to identify as fraudulent, others may appear to be from a legitimate source. Reliability of the name or address in the "From" field should be checked, as this can be easily duplicated. Phishing e-mails may contain spelling mistakes.
- Even the links to the counterfeit websites would contain URLs with spelling mistakes, to take customers to a fake website which looks like that of a bank in which customer maintains an account.
- Phishing emails attempt to convey a sense of urgency or threat. For example: "Your account will be closed or temporarily suspended".
- Fake e-mails may direct the customer to counterfeit websites carefully designed to look real. Hence, such websites may look very similar and familiar to them but are in fact used to collect personal information for illegal use.
- Fake e-mails promise a prize or gift certificate in exchange for individuals completing a survey or answering a few questions. In order to collect the alleged prize, the customer may be asked to provide their personal information.

Spoofing:

Spoofing is the act of creating a website, as a hoax, with the intention of performing fraud. To make spoof sites seem legitimate, phishers use the names, logos, graphics and even the code of the actual website. They can even fake the URL that appears in the address field at the top of your browser window and the padlock icon that appears at the bottom right corner.

The act of spoofing- How is it done?

Fraudsters send e-mails with a link to a spoofed website asking a customer to update or confirm account-related information. This is done with the intention of obtaining sensitive account- related information like Internet Banking user ID, password, PIN, credit card / debit card / bank account number, card verification value (CVV) number, etc.

Vishing :

Vishing is a combination of Voice and Phishing that uses Voice over Internet Protocol (VoIP) technology wherein fraudsters feigning to represent real companies such as banks attempt to trick unsuspecting customers into providing their personal and financial details over the phone.

Act of Vishing- How is it done?

- The fraudster sets up an automatic dialer, which uses a modem to call all the phone numbers in a region.
- When the phone is answered, an automated recording is played to alert the customer that his/her credit card has had illegal activity and that the customer should call the recorded phone number immediately.
- The phone number is with a caller identifier that makes it appear that they are calling from the financial company they misrepresent.
- When the customer calls the number, it is answered by a computer-generated voice that tells the customer they have reached 'account

verification' and instructs the consumer to enter his/her 16-digit credit card number on the keypad.
- A fisher may not have any real information about the customer and would address the customer as 'Sir' and 'Madam' and not by name or the prefix 'Mr....' or 'Ms...'.
- Once a customer enters his/her credit card number, the "fisher" has all the information necessary to place fraudulent charges on his/her card. Those respondings are also asked for the security number (CVV) found on the rear of the card.
- The call can then be used to obtain additional details such as security PIN, expiry date, date of birth, bank account number, etc.

Skimming:

Skimming is a method used by fraudsters to capture customer's personal or account information of credit card. Customer's card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read into and stored on the skimmer or an attached computer. Skimming is a tactic used predominantly for credit-card fraud, but it is also a tactic that is gaining in popularity among identity thieves.

Act of Skimming- How is it done?

ATM machines

Fraudsters insert a skimming device to the ATM's card slot. This device scans the card and stores its associated information. While a customer keys in his PIN, the wireless skimming device transfers the data to the fraudsters. This information is then used by the fraudsters for online shopping or to make counterfeit credit cards.

At Restaurants / Shopping Outlets

At restaurants and shopping outlets, the credit card is swiped twice, once for the regular transaction and the other in the skimmer that captures the personal information which is retrieved later by the fraudsters.

Money Mules

After the fraudster has captured personal information using any of the ways like phishing, Vishing, spoofing or skimming, he/she needs an

account to which he/she can transfer funds from the compromised account. This is where a "Money Mule" comes into the picture. A Money Mule is an unwitting participant in the fraud who is recruited by fraudsters to launder stolen money across the globe.

Act of Money Mules - How is it done?

The Fraudster contacts prospective victims (money mules) with job vacancy ads via spam e-mail, Internet chat rooms or job search websites. Jobs are usually advertised as financial Services/management work, and ads suggest that no specific domain knowledge is required.
The crime rings even persuade the victim to come and work for their fake company. Some fraudsters even ask mules to sign official-looking contracts of employment.
Once recruited, money mules receive funds into their accounts. These funds are stolen from other accounts that have been compromised. Mules then are asked to take these funds out of their accounts and forward them overseas (minus a commission payment), typically using a wire transfer service.
As the account of the mule has been involved in the transaction, the mule also becomes an unwitting participant in the frauds.