Secure Usage of Credit & Debit Card/ATM

Security Threats

Identity theft

The fraudulent acquisition and use of person's private identifying information, usually for financial gain. It can be divided into two broad categories :

Application fraud

Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information.

Account takeover

Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for the mail to be redirected to a new address. The criminal then reports the card loss and asks for a replacement to be sent.

Credit card fraud

Credit card fraudis commited by making use of credit/debit card of others for obtaining goods or services. The threat emerge due to stealing of information like Credit card number, PIN number, password etc. Theft of cards and cloning of cards are also employed to commit such frauds.

Hackers use complex techniques like Phishing, Skimming etc. to gain credit card information from innnocent users.

Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Skimming

Skimming is the theft of credit card / Debit card information. Thief can procure victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victim's credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card and makes note of card details for further use.

Vishing

It is one of the method of social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and "phishing".

Social Engineering

Social engineering involves gaining trust – hence the fraudster poses as a member of staff or even security guard. The fraudster would then ask the customer to check the card for damages. The fraudster would have gained confidence from his prey using various tactics such as offering assistance to the customer who perhaps would have tried to use the ATM without success or perhaps the customer who is not familiar with use of ATM machine and requires assistance.

Steps to be followed before Credit card & Debit card/ATM card usage

- Whenever you receive the card from the bank make sure the mail is completely sealed and there is no damage.
- Whenever you receive the card from the bank immediately sign on the card.
- Try to cover the last three digit number on the card.
- Register your phone number to check the account transactions.
- Change the pin number immediately.

Secure usage of credit/Debit cards at Shopping malls and Restaurants

- Always keep an eye how the vendor swipe your card.
- Always make sure that the transactions happen at your presence.
- Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt where additional charges could be fraudulently added.
- Don't give away your personal information in the survey forms given in restaurants/shopping malls.

Handling Computer Security Incidents

Secure usage of credit / Debit card over internet

- Always use secure websites for transaction and shopping.
- Please look for signs of security.
  Identify security clues such as a lock image at the bottom of your browser,
  A URL that begins with https:
  (These signs indicates that your purchases are secured with encryption to protect your account information)
- Always shop with merchants you know and trusts.
- Always log off from any website after completing online transaction with your credit / debit card and delete the browser cookies.
- Treat all e-mail messages with suspicion to avoid phishing scams. Do not respond to e-mail messages asking for personal information including financial information, as banks do not ask for such information.
- Never send payment information via e-mail. Information that travels over the Internet (such as e-mail) may not fully protected from being read by outside parties.
- Please be careful when providing personal information online.
- Please be wary of promotional scams. Identity thieves may use phony offers asking for your personal information.
- Please keep your passwords secret. Some online stores may require you to register with them via a username and password before buying. Online passwords should be kept secret from out side parties the same way you protect your ATM PIN.
- Always make sure to use the virtual keyboard for netbanking.

DO's

- Before you use an ATM, please ensure that there are no strange objects in the insertion panel of the ATM.(to avoid skimming)
- Shield the ATM pin number during transaction. Don't carry the transaction receipts along.
- Please change your ATM PIN once in every 3 months. As advised by banks.
- Keep your credit card receipts to guard against transaction frauds, check your receipts against your monthly statement.
- Only carry around credit cards that you absolutely need.
- Shred anything that contain your credit card number written on it. (bills)
- Notify your credit card issuers in advance of your change of address, then you change home address.
- If you lose your credit card, please report the loss immediately.
- When you dispose a card at the time of renewal/upgradation, please make sure to cut it diagonally before disposal.

Handling Computer Security Incidents

Don'ts

- Don't accept the card received directly from bank in case if it is damaged or seal is open.
- Don't write your PIN number on your credit card.
- Don't carry around extra credit cards that you rarely use.
- Don't disclose your Credit Card Number/ATM PIN to anyone.
- Don't hand over the card to anyone, even if he/she claims to represent the Bank.
- Don't get carried away by strangers who try to help you use the ATM machine.
- Don't use the ATM machines if the device is not in good conditions.
- Don't transfer or share your account details with unknown/non validated source.
- Don't access Netbanking or make payment using your Credit/Debit card from shared or unprotected computers in public places.
- Don't open unexpected e-mail attachments from unexpected sources or instant message down load links. Delete suspicious e-mail immediately.
- Don't give out your account number over the phone unless you initiate the call and you know the company is reputable. Never give your credit card info out when you receive a phone call. (This is called Vishing)
- Don't provide your credit card information on a website that is not a secure site.
- Don't share any confidential information such as password, customer id, Debit card number, Pin CVV2, DOB to any email requests, even if the request is from government authorities like Income Tax department, RBI or any card association company like VISA or Master card.
- Don't address or refer to your bank account problems or your account details and password on social networking site or blogs.
- Don't store critical information like your ATM PIN number on your mobile phone.