Security Tips for Safe Banking

Learn all about banking online safely, and the measures we take to protect you.

Common Frauds	Security Tips
Phishing	Secure Net banking Tips
Vishing	Secure ATM Banking Tips
Smishing	Secure Mobile Banking Tips
Identity Theft	Secure Internet Browsing Tips
Skimming	Password Security Tips
Computer Virus	

Common Frauds

Phishing:

Phishing is a form of fraud in which the attacker tries to obtain Personal information such as Customer ID, MPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. by masquerading as a reputable entity or person say Syndicate Bank in email, IM or other communication channels.

Spear phishing

A type of phishing attack that focuses on a single user or department within an organization, addressed from someone within the company in a position of trust and requesting information such as login IDs and passwords. Spear phishing scams will often appear to be from a company's own human resources or technical support divisions and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks. Another type of spear phishing attack will ask users to click on a link, which deploys spyware that can steal data; the subject line address is customized / personalized.

How fraudsters do it?

Fraudsters posing as Bank officials, send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email.

Clicking on the link diverts the customer to a fake website that looks like the official Bank website – with a web form to fill in his/her personal information

Information so acquired is then used to conduct fraudulent transactions on the customer's account.

How to identify a Phishing website?

Verify the URL of the webpage. The 's' at the end of 'https://' stands for 'secure' - meaning the page is secured with an encryption. Most fake web addresses start with 'http://'. Beware of such websites.

Check the Padlock symbol. This depicts the existence of a security certificate, also called the digital certificate for that website

Establish the authenticity of the website by verifying its digital certificate. To do so, go to File > Properties > Certificates or double click on the Padlock symbol at the upper right or bottom corner of your browser window

How to protect yourself from Phishing?

- Install the latest anti-virus/anti spyware/firewall/security patches on your computer or mobile phones
- Always check the web address carefully for logging in, always type the website address in your web browser address bar
- Always check for the Padlock icon at the upper or bottom right corner of the webpage to be 'On'
- DO NOT click on any suspicious link in your email
- DO NOT open, unexpected email attachments or instant message download links.
- DO NOT provide any confidential information via email, even if the request seems to be from authorities like Income Tax Department, Syndicate Bank, Visa or MasterCard etc
- DO NOT access Net-Banking or make payments using your Credit/Debit Card from computers in public places like cyber cafés or even from unprotected mobile phones.

Vishing

In **Vishing**, fraudsters try to seek your personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

How fraudsters do it?

The fraudster poses as an employee from the bank or a Government / Financial institution and asks customers for their personal information. They cite varied reasons. For e.g. reactivation of account, encashing of reward points, sending a new card etc.

These details thus obtained are then used to conduct fraudulent activities/ transactions on the customer's account without their knowledge.

How to protect yourself from fraud?

Never share any personal information like Customer ID, ATM PIN, and OTP etc. over the phone, SMS or email.

Smishing

Short for SMS Phishing, smishing is a variant of phishing email scam that instead utilizes Short Message Service (SMS) systems to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

How fraudsters do it?

- Fraudsters send SMS intimating customers of prize money, lottery, job offers etc. and requesting them to share their Card or Account credentials
- Unaware, the customers follow instructions to visit a website, call a phone number or download malicious content.
- Details thus shared with the person who initiated the SMS are then used to conduct fraudulent transactions on customer's account, causing them financial loss.

How to protect yourself from fraud?

Never share your personal information or financial information via SMS, call or email. Do not follow the instructions as mentioned in SMS sent from untrusted source, delete such SMS instantly

Identity Theft

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. *e.g* someone wrongfully using your personal information to obtain credit, loans and services in your name.

How fraudsters do it?

They try to gather customer's details through Phishing, Vishing, Smishing, Dumpster diving or any other means

They might visit customers with a fake card and might swap it with the live card of the customer, without their knowledge.

How to protect yourself from fraud?

- Destroy any piece of paper holding details of your identity.
- Never share your personal information with a stranger or any third party, posing as bank representative
- Update your bank records whenever you change your contact numbers, address or email ID.

ATM related frauds:

Skimming

ATM skimming is like identity theft for debit cards: Thieves use hidden electronics to steal the personal information stored on your card and record your PIN number to access all that hard-earned cash in your accounts.

How fraudsters do it?

At ATM Centers

Skimming takes two separate components to work. The first part is the skimmer itself, a card reader placed over the ATM's real card slot. When you slide your card into the ATM, you're unwittingly sliding it through the counterfeit reader, which scans and stores all the information on the magnetic strip.

However, to gain full access to your bank account on an ATM, the thieves still need your PIN number. That's where cameras come in -- hidden on or near the ATMs, tiny spy cameras are positioned to get a clear view of the keypad and record all the ATM's PIN action

Some ATM skimming schemes employ **fake keypads** in lieu of cameras to capture PIN numbers. Just like the card skimmers fit over the ATM's true card slot, skimming keypads are designed to mimic the keypad's design and fit over it like a glove.

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.

How to protect yourself from fraud?

- Protect your PIN by standing close to the ATM and shielding or cover the key pad with your other hand when entering your PIN
- If you see anything unusual, strange, suspicious, something that does not look right with the ATM or if the keypad does not feel securely attached, stop your transaction and inform the bank
- If it appears to have anything stuck onto the card slot or key pad, do not use it. Cancel the transaction and walk away. Never try to remove suspicious devices
- Be cautious if strangers offer to help you at an ATM, even if your card is stuck or you are having difficulties. Do not allow anyone to distract you
- Keep your PIN a secret. Never reveal it to anyone, even to someone who claims to be calling from your bank or a police officer
- Check that other people in the queue are at reasonable distance away from you
- Regularly check your account balance and bank statements, and report any discrepancies to your bank immediately
- Memorize your PIN – never write it down or store it with your card(s)
- Always press the 'Cancel' button once your transaction is over.

Common threats to computers:

Computer Virus

Different types of computer viruses: Trojan, Spyware, Malware... etc

Trojan:

Trojan is a program which often looks like a legitimate program such as a game or utility. It travels with another program which you may download from a website or receive as an attachment in an e-mail. When executed, Trojan scan gathers information about our computer (files, passwords, etc.) without our knowledge and transmits this information back to the fraudster who has sent the Trojan.

At times, this virus is designed specifically to capture credit card related data and build a mini- database at a pre-decided location for misuse by fraudsters. Once this type of Trojan has been installed on our computer, the attacker can access and use our computer as if they were the real owner!

Spyware

Spyware gathers personal information from our computer or information related to our activity on the Internet and sends the information without our knowledge to fraudsters. How does a Trojan or Spyware program get on the computer? Trojans and spyware are often hidden inside other computer programs. Trojans and spyware are commonly hidden inside software such as:

- Screen savers
- Time and date updaters
- Custom cursors (mouse pointers)
- Browser toolbars
- Internet games
- Online word documents
- Excel based documents

Malware

Malware, short for **malicious software**, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

Malware spreads through E-mails, visiting Malicious Websites, pop- up adverts, through social networking sites by installing dubious 3rd party add-on applications or by web links in messages. Peer to Peer software and cracked or pirate software often facilitate the spread of malware. Through the shared use of computer storage media such as DVDs, CDs and USB drives also malware spreads.

How to protect your computer from Virus/ Trojan/spyware and Malware?

- Use a Firewall- Install and activate a personal firewall on your computer.
- Ensure your anti-virus and spyware detection software is updated regularly; daily if possible.
- Know what you are installing before you click 'install'.
- Do not enter your passwords, card details and codes in pop-up windows that may appear for no reason in the midst of your activity on any website or social websites.
- Log off from the session immediately on completing your activity.
- Ensure to do your online shopping on known and reputed websites only.
- Do not install any software that comes as an attachment via e-mail/web promotion.
- Run spyware checks on your computer frequently. A weekly scan is highly recommended.
- Never buy software in response to unexpected pop-up messages or e-mails
- Never click links in messages from unknown or untrusted contacts, and avoid clicking on message links sent from trusted contacts unless you are certain where it will lead you
- Never install unauthorized, unlicensed or unapproved software on your computer
- Do not insert untrusted computer media into your computer

Ransomware:

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.

How to protect yourself from ransomware?

- Back up your files regularly and keep a recent backup off-site
- Don’t give yourself more login power than necessary
- Don’t enable macros
- Update OS Patches regularly
- Be very careful about opening unsolicited attachments

Security Tips:

Secure Net banking Tips:

- Access Syndicate Bank Internet Banking Website only by typing: www.syndicatebank.in in the address bar of your browser, never click a link that offers to take you to our website.

- You can view the Bank's name in the green address bar in your browser. Check for the Lock icon in the browser window. Click (or Double Click) on it to see details of the site's authenticity. This is important to know because some fraudulent web sites imitate the lock icon of your browser!

- Avoid online banking from public or shared computers or virus infected computer However, if you happen to do so change your passwords from your own computer. Do not open multiple browser windows while banking online. Every time you complete your online banking session, log off from www.syndicatebank.in. Do not just close your browser

- Our Banks site is secured and the address will begin with "https" meaning the user name and password typed will be encrypted before sending to our server. Our Bank also provides Virtual keypad to key in passwords, which protects your passwords from malicious 'Spyware' and 'Trojan' programs designed to capture keystrokes.

- The Basic purpose of providing the above security features is to transmit the information in the encrypted form in secure manner, so that others cannot view the important and confidential information pertaining to our valued customers. However, Web Browsers are capable of storing browsed information during the session (caching). To prevent caching, it is suggested that you always close your browser window after your Internet Banking session.

- Please note that Syndicate Bank neither sends Login-id or Password through email nor does it ask for any details regarding your Internet Banking account or password through email . Please beware of such fraudulent mails eliciting such information with the intention to defraud the customers by unscrupulous persons.

- Always ensure your PC is updated with latest anti-virus and operating system patches. Install personal firewall and anti-spy ware to protect your PC from internet attacks.

- If your log-in IDs or passwords appear automatically on the sign-in page of a secure website, you should disable the "Auto Complete" function in your browser to increase the security of your information.

  To disable the "Auto Complete" function in your browser(Internet Explorer):

  - Open Internet Explorer and click "Tools" > "Internet Options" > "Content".
  - Under "Personal Information", click "Auto Complete".
  - Uncheck "User names and passwords on forms" and click "Clear Passwords".
  - Click "OK".
- Configure your browser settings to ensure that you are warned each time you access secured or unsecured web pages.
- Buy from well-known companies if you are doing e-commerce transactions and only provide

  bank information during secure sessions.
- If you visit any questionable website before Internet Banking, we recommend you close your browser and restart it before proceeding to Internet Banking.

- Change your online banking passwords periodically (at least once in a month). Your password should be complex and difficult for others to guess. Use letters, numbers and special characters [such as !,@, #,$, %, ^, &,* (,)] in your passwords, The special characters are also provided in the virtual key board.
- Never leave your computer unattended while logged on to Internet Banking.
- Password-protect your computer: Use a password on your computer to prevent unauthorized
  Individuals from accessing your information

Secure ATM Banking Tips:

- Memorize your PIN. Do not write it down anywhere, and certainly never on the card itself.
- Do not share your PIN or card with anyone including Bank employees, not even your friends or family. Change your PIN regularly.
- Stand close to the ATM machine and use your body and hand to shield the keypad as you enter the PIN. Beware of strangers around the ATM who try to engage you in any conversation.
- Do not take help from strangers for using the ATM card or handling your cash
- Do not conduct any transaction if you find any unusual device connected to your ATM machine.
- Press the 'Cancel' key and wait for the welcome screen before moving away from the ATM. Remember to take your card and transaction slip with you.
- If you get a transaction slip, shred it immediately after use if not needed.
- If your ATM card is lost or stolen, report it to your bank immediately
- When you deposit a cheque or card into your ATM, check the credit entry in your account after a couple of days. If there is any discrepancy, report it to your bank.
- Register your mobile number with the Syndicate Bank to get alerts for your transactions.

Secure Mobile Banking Tips:

- Password protects the mobile phone. It is recommended to set the maximum number of incorrect password submissions no more than three.
- Choose a strong password to keep your account and data safe
- Review your account statements frequently to check for any unauthorized transactions
- Change your MPIN regularly.

- Report a lost or stolen phone immediately to your service provider and law enforcement authorities
- Never give your PIN or confidential information over the phone or internet. Never share these details with anyone
- Don't click on links embedded in emails/social networking sites claiming to be from the bank or representing the bank
- Don't transfer funds without due validation of the recipient, as funds once transferred cannot be reversed
- Don't store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone
- Don't forget to inform the bank of changes in your mobile number to ensure that SMS notifications are not sent to someone else
- Never reveal or write down PINs or retain any email or paper communication from the bank with regard to the PIN or password
- Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources.
- Be cautious while using Bluetooth in public places as someone may access your confidential data/information
- Be careful about the websites you are browsing, if it does not look authentic, do not download anything from it

Secure Internet Browsing Tips:

- **Keep your browser software up-to-date:** This is crucial, as new patches are often released to fix existing vulnerabilities in browser software. This recommendation doesn't apply solely to browser software – it is critical to keep operating system software and any other software you have up-to-date for the same reason.
- **Run anti-virus software:** Anti-virus software provides protection by scanning for and removing malicious files on your computer. There are many excellent options for virus protection software (both paid and free), so it is up to you to do a little research and select a program that best fits your needs.
- **Scan files before downloading:** It is important to avoid downloading anything until you're confident that it is secure. If you have any suspicion that a file may not be legitimate or may be infected, scan it with antivirus software before downloading.
- **Watch out for phishing:** Phishing attacks use online communications (usually email) to trick users into giving out their sensitive information. Often times these

messages appear to be from banks, social media sites, shopping sites, or payment processers. Phishing messages frequently contain links that lead to counterfeit versions of popular sites. You can avoid falling victim to phishing schemes by ignoring unsolicited messages and not clicking on hyperlinks or attachments in emails (type or copy/paste the URL as it appears instead).

- **Don't reuse passwords:** Using the same password for multiple sites only makes it easier for attackers to compromise your sensitive information. Instead, keep track of your different passwords with a handwritten list that you keep in a safe place or come up with your own algorithm for creating unique passwords that only you would know. It is also recommended that you change your passwords every 90 days.
- **Use HTTPS:** The "s" in "https" stands for secure, meaning that the website is employing SSL encryption. Check for an "https:" or a padlock icon in your browser's URL bar to verify that a site is secure before entering any personal information.
- **Read privacy policies:** Websites' privacy policies and user agreements should provide details as to how your information is being collected and protected as well as how that site tracks your online activity. Websites that don't provide this information in their policies should generally be avoided.
- **Regularly monitor your bank statements:** Keeping an eye on your online statements will allow you to react quickly in the event that your account has been compromised.
- **Avoid public or free Wi-Fi:** Attackers often use wireless sniffers to steal users' information as it is sent over unprotected networks. The best way to protect yourself from this is to avoid using these networks altogether.
- **Disable stored passwords:** Nearly all browsers and many websites in general offer to remember your passwords for future use. Enabling this feature stores your passwords in one location on your computer, making them easier for an attacker to discover if your system gets compromised. If you have this feature enabled, disable it and clear your stored passwords.
- **Turn on your browser's popup blocker**: Popup blocking is now a standard browser feature and should be enabled any time you are surfing the web. If it must be disabled for a specific program, turn it back on as soon as that activity is complete.

Password Security tips

Creating a Secure Card PIN:

When you receive your Card PIN, change it immediately. Never use the following for your PIN:

- Your kids' or loved ones' date of birth
- 1234 or 4321, 9876 or 6789 – easy to guess
- Digits of your mobile number
- Your date of birth or anniversary
- First or last 4 digits of your card number

Creating a Secure NetBanking Password:

- Be creative and think of a password that is really different as well as difficult to guess.
- Mix upper and lowercase letters, and special characters like $, @, *, etc.
- Place punctuation or numbers randomly.
- Pick letters that are in different places on keyboard. Do not use sequences like 'qwerty'.
- Don't use sequences of letters or numbers. E.g.: abcd1234. asdfg123 etc.
- Don't use personal information like your name, date of birth, PAN number, etc.
- Avoid using the same password for several different accounts. Once hackers have guessed one password, they'll often try to see if it works on other accounts.

Protecting your password:

- Memorize your PIN. Don't write down your password or PIN anywhere especially not on your card.
- Change your PIN/passwords at regular intervals.
- If you suspect that someone knows your PIN/Password, change it immediately.
- Don't send your password or PIN to anyone via email or text message.
- Don't say your password or PIN aloud in public where other people can hear you.
- Don't have your browser remember your card/account password.