SBI

The banker to every indian

Because Security Matters

(In the fight against Cyber Crime, Stay Aware)

#SafeWithSBI

Here, are some simple tips for cyber safety, which will help you stay safe & secure:

Do not download any app on your mobile on the advice of any unknown person(s)

Use strong and complex passwords

Do not click on links and open E-mail attachments from unknown sender(s)

Use Anti-Virus on your mobile device

Change your password frequently

Avoid using public Wi-Fi to conduct financial transaction

S. Srinivasa Rao
Dy. Managing Director & Chief Risk Officer

SBI
The banker to every Indian

Dear Customers,

Cyber Security is a shared responsibility

With the world moving towards digitization and everything becoming more connected, Cyber Security has become a major concern for everyone.

Device manufacturers can provide highly sophisticated security measures. Banks and other financial institutions can establish effective defensive and protective policies and processes. But it takes only one mistake- at the wrong place, at the wrong time-to give a cyber criminal the opening needed to cause a possible breach.

Social engineering attacks, which are the most common types of cyber-attacks, exploit social interactions to gain access to valuable data. At the root of all social engineering attacks is deception. Cyber criminals trick and manipulate their targets into taking certain actions, such as bypassing security measures or disclosing certain sensitive information. Similarly, clicking on links in phishing emails, opening attachments from unknown senders, using weak passwords - these are just the simplest examples of how an individual's actions can create vulnerabilities, which even the best cyber security systems cannot stop, because the target itself lets the attacker into the system.

Effective cybersecurity measures therefore require that every individual, and every user of digital applications/platforms is aware of cyber security threats and the best practices on safe usage of IT, Digital platforms. This booklet is prepared with a view to provide you with the basics of cyber security and the best practices that should be followed to conduct safe digital transactions. I am sure that the booklet will help you understand the cyber risks and lead you to a safe and secure digital journey with State Bank of India.

With Best Wishes,

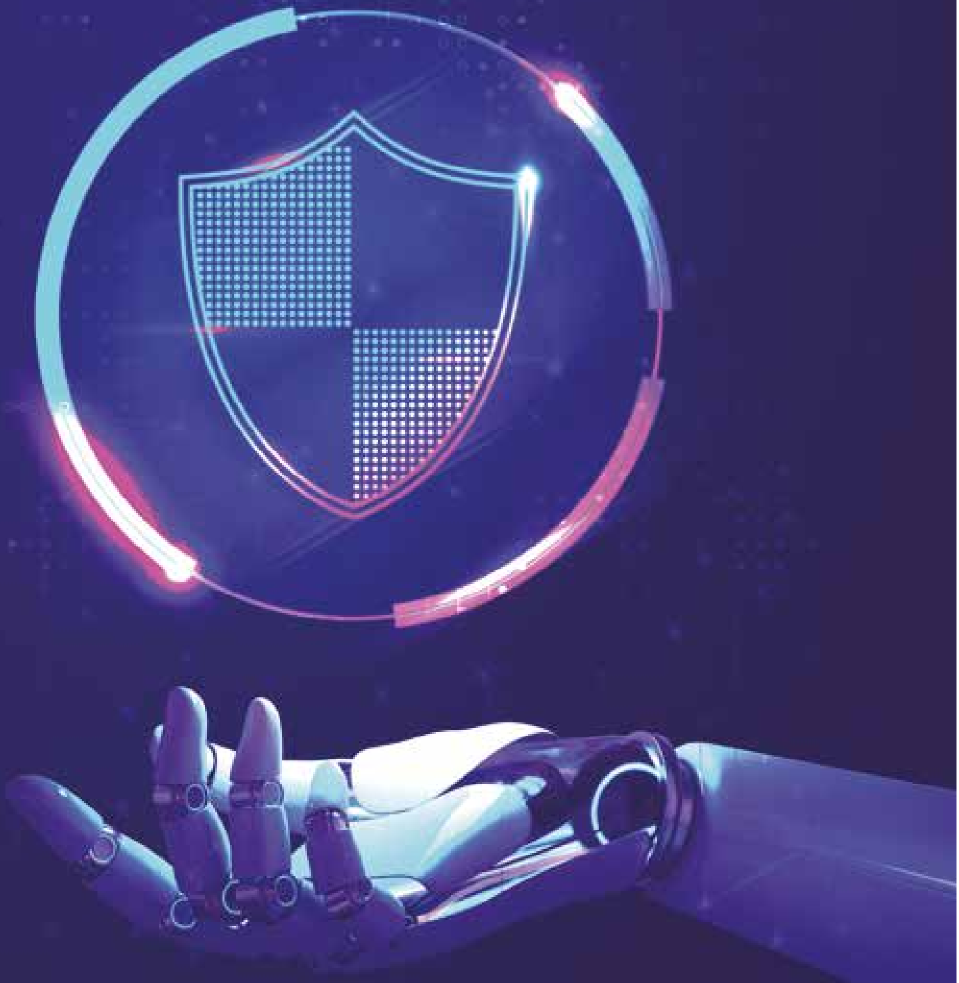
S. Srinivasa Rao
Dy. Managing Director & Chief Risk Officer

Table of Contents

Topics	Page No
Introduction to Cyber Security	05-08
Social Engineering Attacks and Prevention Tips - Phishing	09-13
Social Engineering Attacks and Prevention Tips - Vishing	14-19
Social Engineering Attacks and Prevention Tips - Smishing	20-23
Mobile Banking Security	24-27
Unified Payments Interface (UPI) - Security Tips	28-31
Debit / Credit Cards – Best Practices to ensure safe usage	32-35
Social Media Frauds and Privacy Guidelines	36-41
Password Security – Best Practices	42-43
Wi-Fi - Guidelines on Safe Usage	44-45
Cyber Security at Fingertips	46-47

Introduction to Cyber Security

Cyber security refers to the protection of your servers,data,computers, mobile devices, networks, electronic systems, from malicious attacks. It involves taking adequate measures to ensure online and digital safety from frauds, hackers etc.



Stay Alert, Stay #SafeWithSBI.

19 Out of 20 Cyber Breaches Will Not Take Place at All, If Human Error Is Eliminated Entirely.

Let Us Strive to Reduce Human Error & Create A Holistic Defence Against Cyber Crime.
Stay Alert, Stay #SafeWithSBI.

Human Error in Cyber Security: Human error is an unintentional action(s) or the lack of action(s) by the users which may cause, allow or spread a cyber incident. In the context of cyber security, several studies indicate that 95% of the cyber incidents are caused by human errors and, if we can somehow eliminate the human error entirely, 19 out of 20 cyber breaches can be avoided or may not take place at all.

Some Common Human Errors:

- Usage of weak or easily guessable passwords and not changing them frequently.
- Sharing of financial details such as Card No/PIN/CVV/OTP with others on E-mails/calls/SMS/Social Media.
- Connecting devices to untrusted public WIFI to perform digital transactions.
- Improper management of mobile applications like allowing Apps permission to access features which are not required to be accessed by the app.
- Clicking on unknown links sent by SMS or E-mail.
- Downloading mobile applications from unverified locations.
- Downloading mobile apps on the advice of strangers.

Now, let us introduce you to some of the common cyber frauds happening today and how to keep your personal information and money safe from cyber frauds, such as:

Social Engineering Attacks

Mobile Banking Frauds

Identity Theft

Digital Banking Frauds Like UPI Fraud, Card Related Frauds/CVV/ OTP Frauds

Debit Card Related Frauds/CVV/ OTP Frauds

Phishing Attacks

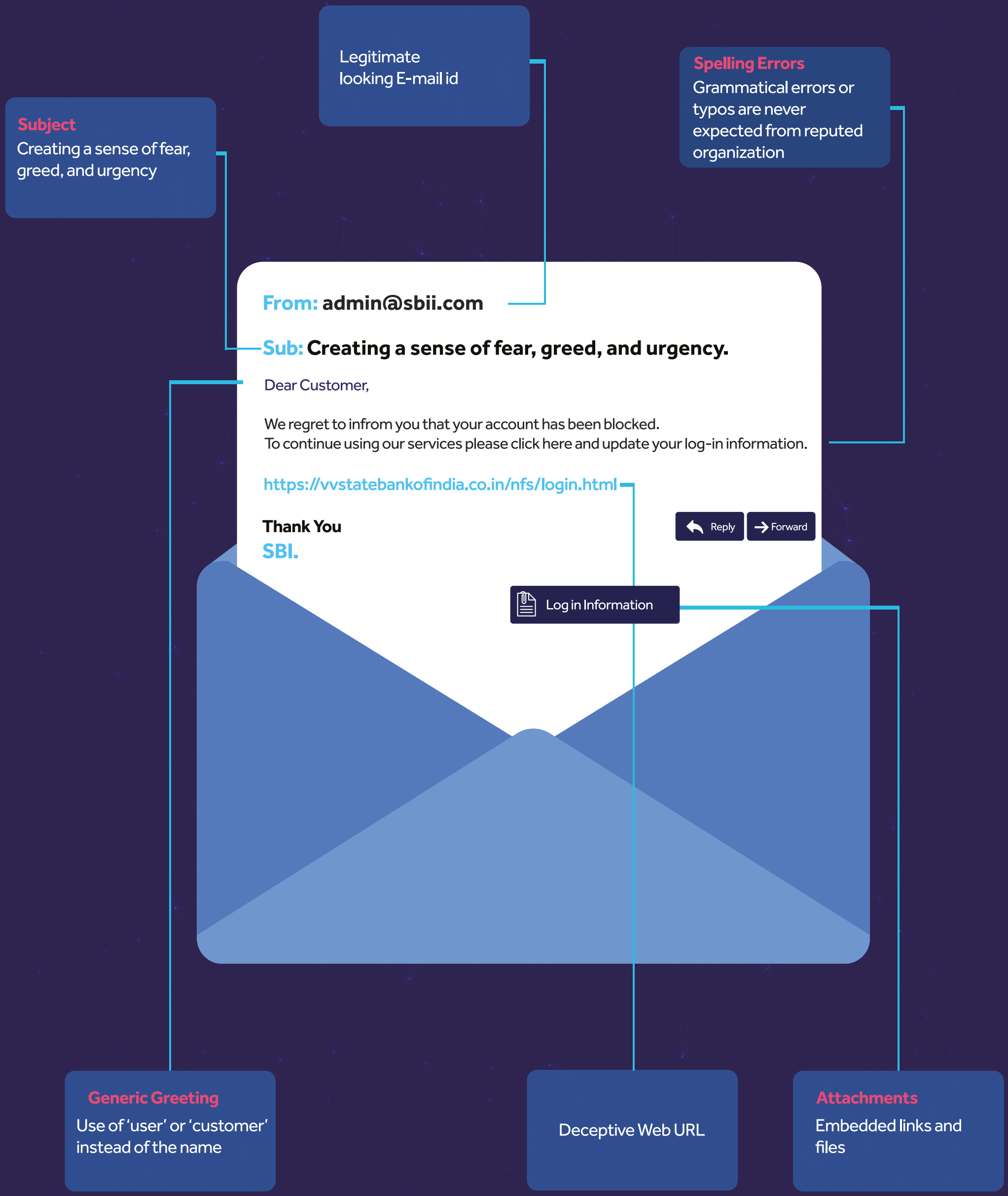
One E-mail Could Take Away All Your Savings.

**Don't Fall For the Bait.
You Could Be the Prey.**

Stay Alert, Stay #SafeWithSBI.

Typical examples of a Phishing Scam

Example 1: Fraud E-mail



Subject
Creating a sense of fear, greed, and urgency

Legitimate looking E-mail id

Spelling Errors
Grammatical errors or typos are never expected from reputed organization

From: admin@sbii.com

Sub: Creating a sense of fear, greed, and urgency.

Dear Customer,

We regret to infrom you that your account has been blocked.
To continue using our services please click here and update your log-in information.

https://vvstatebankofindia.co.in/nfs/login.html

Thank You
SBI.

Generic Greeting
Use of 'user' or 'customer' instead of the name

Deceptive Web URL

Attachments
Embedded links and files

Beware of Phishing Links. Think Before You Click!

How Phishing Scam Works?

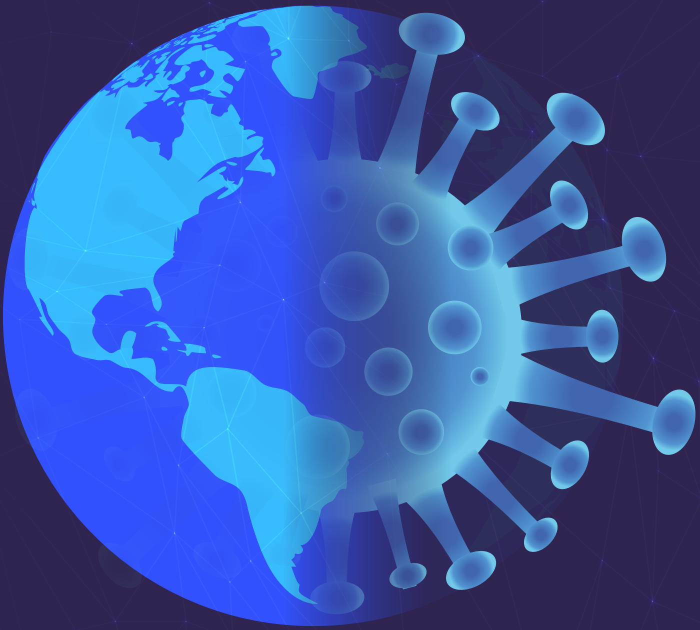
- Fraudsters create a fake E-mail in the name of a legitimate entity.
- The E-mail containing a link to a malicious website is sent to the user.
- The user acts upon the E-mail and clicks on the fake link.
- The user enters his/her personal details on the fake link and his sensitive information is compromised.

Once an E-mail account has been hacked, the criminal can misuse the user's E-mail account for the following purposes:

- Obtaining personal information such as names, bank account details (User ID, Password, OTP), PAN, Aadhaar etc.
- Sending emergency mails to user's contacts asking for money citing some emergency.
- Sending offensive messages to friends and relatives asking for ransom.
- To gain access to other online accounts such as net-banking, social media accounts, etc.

Example 2: Corona

The "Ayushman Bharat Fraud" phishing attack uses the Indian government's free health coverage scheme to deceive users.



In this, a message like '10-crore people between the age of 13 -70 years are being provided with free insurance worth ₹ 5,00,000 to cover the COVID-19 pandemic.' is shared.

It asks users to register themselves using the given link. However, this link is designed only to obtain the user's personal information.

Beware of Phishing Links. Think Before You Click!

Best Practices To Ensure Safety Against Phishing

- Verify the sender's E-mail address/name before opening the E-mail.
- Do not open/download attachment from untrusted sources.
- Do not click on the link given in an E-mail received from an unknown sender.
- Do not share your personal/financial details like username, password, OTP, Card Number, CVV, PIN etc. over E-mail.
- Beware of mails which are anonymous, create a sense of fear or urgency.

Vishing

Some Calls Are Better Ignored

Stay Alert, Stay #SafeWithSBI.

Vishing Attacks:

How Vishing Works?

- Vishing is an act of using phone calls to trick the user into surrendering private information that could be used for fraudulent purposes.

- The scammer usually pretends to be from a legitimate entity and tries to befool the victim by luring or threatening, tricking them to surrender critical information or convince them to perform a specific action.

- Fraudsters create fake Caller ID profiles which make the phone numbers seem legitimate.

Typical Examples of Vishing

Example 1: OTP / CVV Fraud

Fraudster impersonating as a bank official tells the victim that his/her bank account or debit card is being blocked due to some technical difficulties or because his KYC has not been updated. If they wish to unblock it, they need to verify some details.

On this pretext the fraudster induces the victim to share sensitive personal information like the debit/credit card number, expiration date, CVV and OTP.

If You Are Being Asked for Any Confidential Data over phone, Beware! It Could Be a Vishing Scam!

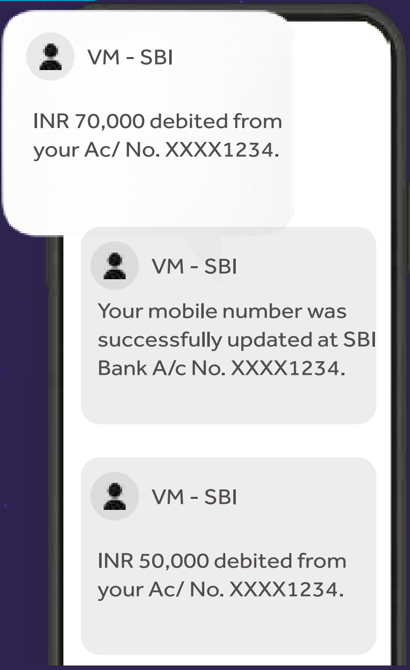
Example 2: KYC Fraud

Please Update Your KYC Details So That Your Account Does Not Get Blocked.

Oh! How To Update My KYC Details?

Don't Worry! Please Share Your Screen Through Remote Access And I Will Update The Details For You.

Sure, I Will Share My Screen.



VM - SBI

INR 70,000 debited from your Ac/ No. XXXX1234.

VM - SBI

Your mobile number was successfully updated at SBI Bank A/c No. XXXX1234.

VM - SBI

INR 50,000 debited from your Ac/ No. XXXX1234.

If You Are Asked for Any Confidential Data, Be Aware! It Could Be a Vishing Scam!

Example 3: IT Return Fraud

Taxpayers are called and redirected to a fake / malicious website to get the Income Tax refund.

This kind of fraud occurs mainly during the period of filing tax returns.

Such fake websites cheat taxpayers into entering their bank details and other sensitive information which is further misused.

If You Are Asked for Any Confidential Data, Be Aware! It Could Be a Vishing Scam!

Best Practices To Ensure Safety Against Vishing

- Verify the identity of the caller. Always be suspicious of any person asking for your personal or Financial details over call.
- Do not share your personal/Financial details such as OTP, ATM PIN, CVV over phone. SBI never asks for your Financial/personal details over call.
- Do not call on phone numbers that are provided in online ads, pop-up windows, E-mails, etc.
- Do not install any application on request of strangers.

Smishing:

If you suspect deceit, press delete.

Stay Alert, Stay #SafeWithSBI.

Smishing Attacks:

Smishing is a type of Phishing attack. SMS + Phishing = Smishing.
Fraudsters send messages impersonating as legitimate organisations.

How Smishing Works?

Smishing, or SMS phishing, is a form of phishing that uses text messages / SMS to get personal information or banking information.

Typical Example Of Smishing Attacks:

A fraudulent message from a seemingly legitimate source such as a bank will be sent to the victim.

Typically, the message will claim an emergency and provide a link to the victim to click.

On clicking the link, the victim will either be directed to a malicious site or a virus/malware will be downloaded.

1(410) 200-500
Text Message
Today: 54 PM

FRM:18443693848
MSG: Your card has been put on hold. CALL now free: 1-844-369-3848 and follow instructions to resolve this issue.

Are You Receiving SMS with a Sense of Urgency and Suspicious Links? Beware! It Could Be a Smishing Scam!

Best Practices To Ensure Safety Against Smishing

- Verify the message sender and do not act on unknown messages.
- Do not respond to unsolicited sales, marketing, or outreach messages.
- Do not share your personal/financial details over SMS.
- Do not click on any links received from unknown sources.
- Do not download any app through link provided through SMS.
- Please remember your bank never asks for your personal, financial, OTP or CVV details through SMS.
- Be careful while responding to a message which creates a sense of urgency, fear or greed.

Mobile Banking Security

**Go The Extra Mile,
Ensure Security of Your Mobile.**

Stay Alert, Stay #SafeWithSBI.

Mobile Banking Security

Introduction of Mobile banking has brought convenience to the users, however, security of personal and business information stored on smartphones, should also be taken care of.

Threats to Mobile Security:

- Mobile Malware consist of virus, trojans, spyware, adware and rootkits which can be downloaded in your mobile device by clicking on unsolicited links or through malicious apps.
- Using default configurations such as no passwords, excessive app permissions, access to Contacts and/or Gallery, and geo location permissions, etc.
- Use of Unsecure Wi-Fi Networks especially in public places.
- Using outdated version of the Mobile OS and patches.

Best Practices in Mobile Banking

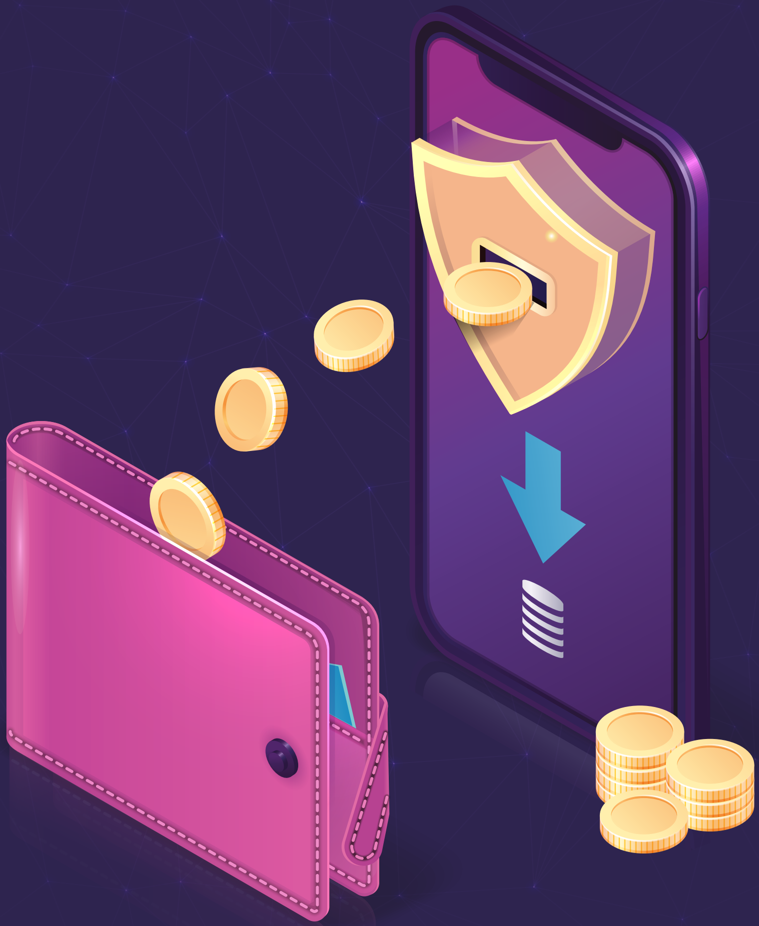
Your Security At Your Fingertips

Best Practices in Mobile Banking

- Strong passwords/ Biometric permission should be enabled on your phone, tablets.
- Do not share your Mobile PIN with anyone, use biometric authentication wherever feasible.
- Ensure that Auto Updates are enabled for your mobile OS, Anti-Virus, and applications.
- Avoid installing apps on the advices of strangers or through links received in E-mails, messages or through social media etc. Applications should be downloaded only through official stores.
- Regularly monitor the permissions of critical apps installed in your mobile and keep a track of unnecessary and unused apps.
- Never use Banking apps on jailbroken or rooted devices.
- Do not store your Bank account number or PIN on mobile phone.
- Report the loss of mobile phone to the Bank to disable Mobile Banking services.
- Avoid connecting phones to public wireless networks.
- Get an Anti-Virus software installed on your mobile and keep it updated.

Unifed Payments Interface (UPI) Security

UPI is a real-time payment platform that helps in instantly transferring the funds between the two bank accounts through the mobile platform.



Stay Alert, Stay #SafeWithSBI.

Feature of UPI:

Any UPI client app may be used and multiple bank accounts may be linked to a single app.

Money can be sent or requested with the following methods:

Virtual Payment Address (VPA) or UPI ID: Send or request money from/to bank account mapped using VPA.

Mobile Number: Send or request money from/to the bank account mapped using mobile number.

Account Number & IFSC: Send money to the bank account.

Aadhaar: Send money to the bank account mapped using Aadhaar number.

QR Code: Send money by QR code which has enclosed VPA, Account number and IFSC or Mobile number.

How UPI frauds happen?

QR Code & UPI PINs: Many users are unaware that they do not need to scan a QR code or enter their UPI Pin to receive money on the UPI app.

Often, fraudsters will send fake links stating an option for 'request money'. Once the user clicks on this link, it will ask for UPI Pin or to scan a code.

Doing so can result in financial loss to the user

Fake calls: Fraudsters will call you pretending to be bank representatives and ask for your UPI Pin or ask you to download a third-party app, stating it is for verification purposes. Downloading the app, which is a remote assist application, gives control of your mobile device to the fraudster and allows them to steal your personal data, OTP and account details.

Example 1: Misusing the Request Money Links

The victim lists an article to sell in one of the online classified portals (OLX, Quikr).

A fraudster claiming to be a prospective buyer, contacts the victim offering to buy the article

The fraudster asks the victim for his UPI ID for immediate payment

The fraudster sends the victim a link or a QR code. On clicking the link and providing the UPI Pin or scanning the QR code, the victim loses his hard earned money.

Beware of Fraudulent Links That Lead to Fake Applications!

Best Practices To Ensure UPI Security

- Install UPI apps from trusted sources only.
- Keep your Mobile PIN and UPI PIN different and random.
- Never share your device Mobile PIN or your UPI PIN with anyone.
- Always check the details of payment collection requests while conducting any transactions on UPI apps.
- Do not respond to any unknown UPI requests and report suspicious requests.
- Do not scan a QR code when you are going to receive an amount.
- Always remember that a UPI PIN or scanning of a QR code is required only for transferring amounts, not for receiving.
- Always change UPI PIN if compromised.
- Instantly disable UPI service on your account if any transaction has happened without you doing it.

Debit/Credit Card Fraud/Reward Point Attacks

Your Savings Could Be Swiped Out With Just A PIN!

Stay Alert, Stay #SafeWithSBI.

Debit/Credit Card Fraud/Reward Point Attacks

- Debit cards and Credit cards have become an indispensable part of our life.
- Debit/Credit Card Frauds occur when fraudster obtains your card details, CVV, PIN, etc. to withdraw money from that account.
- Often, reward points or loyalty points are offered by the credit card companies to promote the usage of a debit/credit card.
- Sometimes fraudsters take benefit of this and fraud is perpetrated in the name of debit/credit card reward point.

How Do Debit/Credit Card Attacks Work?

- Fraudsters call cardholders claiming to be from their card company and tell them that they would help them in redeeming their reward points.
- They create urgency among cardholders stating that offer will end very soon. To redeem the reward points, cardholders will be asked to provide their card details and OTP which fraudsters may misuse.

Best Practices To Ensure Debit / Credit Card Security

Swipe Secure

Best Practices To Ensure Debit / Credit Card Security

- Beware of your surroundings while performing transactions through ATM machines or POS devices. Cover the Keypad while entering the PIN.
- Do not share your card number, CVV, or OTP details. Always remember that your bank never asks for these details.
- Do not E-mail your card number.
- Always verify the authenticity of e-commerce websites before performing the transactions.
- Manage your debit card transactions through online Banking. Set a limit for card transactions at e-commerce platforms, POS and ATM both for domestic and international transactions.
- Enable SMS alert on your account to get regular updates.
- Check your account statement after performing the transactions.

Social Media Attacks

Social Media interactions can be used to trick people into sharing personal details like bank accounts, card details etc. through phishing posts, fake profiles, and direct messages.

Stay Alert, Stay #SafeWithSBI.

Social Media Attacks

- Social media frauds are rising with the increase in number of people using the platforms.
- Fraudsters often use these platforms to trick people into parting with their personal details using a variety of phishing posts and direct messages.

Typical Examples of Social Media Attacks

Example 1: Lottery Scam

- Often there are posts on social media claiming to give out gift cards or direct transfer of money announcing that you've won a lottery.
- Such posts are always a scam and when you follow these, you are taken to a malicious website that asks you to enter your sensitive personal information to claim the lottery amount.
- The information sought may include your banking information which can be misused for carrying out fraudulent activities.

They Are Not Who They Are Pretending to Be Online.
Watch out for Fake Profiles!

Example 2: Digital Payment Frauds

Fraudster sends "Collect Request (receive money request)" link through UPI, QR code etc. through different social media platforms.

- Once you click on it and authorize the transaction, thinking that you will receive money, the amount gets deducted from your account instead.
- Remember, you do not need to authorize the transaction or enter your UPI Pin when you are expecting a receipt transaction.

They Are Not Who They Are Pretending to Be Online.
Watch out for Fake Profiles!

Example 3: Fake Social Media Handles

There are enough counterfeit handles/accounts on social media platforms like Twitter, Facebook, etc.

- Do not trust a Social media handle just because it contains the word 'UPI', 'NPCI', 'BHIM' and/or has names similar to a banking, financial or government organization. Please always search for the official handle.

- Fraudsters create such handles as bait to get you to reveal your account details through a fake social media handle.

They Are Not Who They Are Pretending to Be Online.
Watch out for Fake Profiles!

Best Practices To Ensure Social Media Security

- Confirm the identity of the person you are interacting with.
- Do not discuss confidential information on public platforms.
- Do not discuss confidential information with strangers, people whom you have met briefly.
- Do not share your personal/financial information on any social media platform.

Password Security:

Difficult to Guess,
Easy to Remember,
Your Password Mantra.

Keep Strong Passwords to Ensure Complete Privacy.

Stay Alert, Stay #SafeWithSBI.

Best Practices On Password Security

A strong password is the first step towards safe digital transactions, Please follow the below mentioned best practices to have safe and secure digital experience,

- Keep your password strong and complex with minimum length of 8 characters combining at least one numeric, one special character and mix of Upper and Lower cases.
- Dictionary words like umbrella, sunshine, kite, monkey, prince or phrases like iamaboy, letmein, etc. should not be used.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc or combination with numbers like secret1, 1secret etc. should not be used in password.
- Do not share passwords with anyone, including family, colleagues, friends and bank employees.
- Change your password at frequent intervals or if you suspect it is compromised.
- Memorize your password, instead of writing it
- Do not use common passwords for all
- "Remember my credentials" or "Remember Password" facility of internet browsers should not be used.

'Password Is Your Signature, Keep This Unique'

Wi-Fi Security:

Who Else Is In Your Network?

Prevent Unauthorised Access to Your Wi-Fi, Ensure Complete Wi-Fi Security.

Stay Alert, Stay #SafeWithSBI.

Best Practices To Ensure Wi-Fi Security

- Do not connect to open/public Wi-Fi network.
- Turn off your device Wi-Fi and Bluetooth when not in use.
- Change the default network name, username and password of your own Wi-Fi connection.
- Switch off your wireless router when not in use.
- Always separate private network from guest network.

Cyber Security:

**It All Starts With A Click;
Be Careful, Be #SafeWithSBI.**

Stay Alert, Stay #SafeWithSBI.

Cyber Security at Fingertips

- Be a good cyber citizen. Do not do anything in cyber space that you consider wrong or illegal.
- Do remember the URL of financial websites and avoid clicking on unknown links received through E-mail/ SMS.
- Hover over the links on E-mail to confirm/see the actual URL.
- Verify URL by typing them in browser, do not follow the links sent on E-mail.
- Use 2 Factor Authentication (2FA) wherever you can.
- Lock your phone with strong password or biometric authentication.
- Use passphrases to form strong passwords & Change your password(s) frequently.
- Lock your devices when not in use.
- Back up your critical data regularly.
- Clear cookies and delete browsing history at the end of each session.
- Keep your system updated with latest Anti-Virus solution.
- Install apps and software from trusted sources only.
- Update your computer operating system (OS) with latest patches.
- Avoid using Free or public Wi-Fi & Install Anti-Virus protection and keep it updated.
- Check your bank statement regularly. Monitor all your accounts for any suspicious activity.
- Scan the file downloaded from internet before opening.
- Watch out for online scams, lottery traps etc. Do not fall prey to these.
- Do not be a victim of social engineering. Do not trust strangers and do not share your confidential information with anyone.

SBI

The banker to every Indian

Verify that the message is from SBI by checking for the shortcode starting with

"SBI/SB" only, ex: SBIBNK, SBIINB, SBIPSG, SBYONO.

Do NOT act on messages from unknown sources.

Check your messages to monitor your account's activities.

Stay #SafeWithSBI

K Y C

Know Your Click

is Important.

Verify The Link Before You Click.
Be Cautious and Stay #SafeWithSBI

report.phishing@sbi.co.in

Know What Websites To Visit
and What NOT To Visit.
Be Cautious and Stay #SafeWithSBI

You're Being Phished If The Email Is...

- From An Unknown Source
- Has Spelling/Grammatical Errors
- Asking For Personal/Confidential Information
- Wants You to React NOW!

Think Before You Act!

Stay #SafeWithSBI

To Report Any Suspicious Activity, Kindly Email On report.phishing@sbi.co.in or Call the Cyber Crime Helpline Number 155260.

For more information visit: **https://www.cybercrime.gov.in**