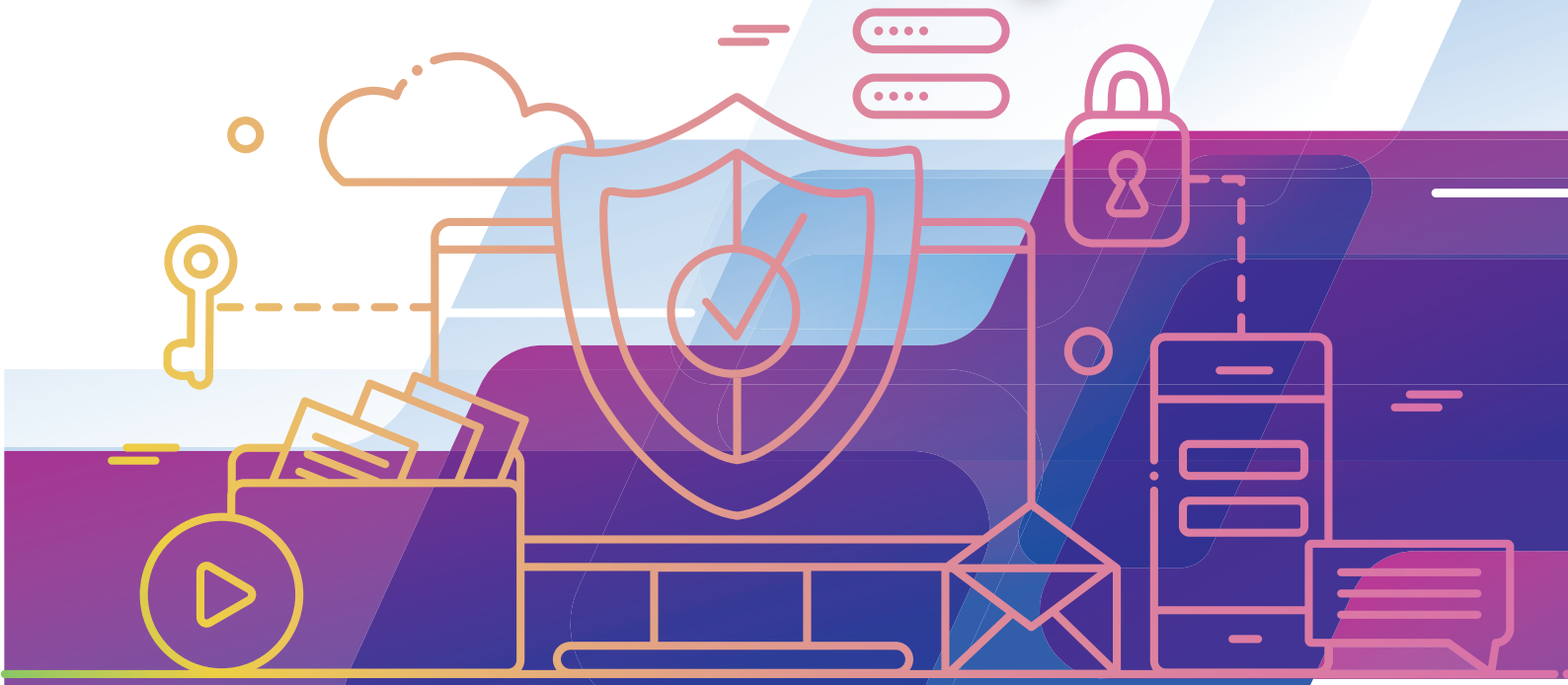
SBI
The banker to every Indian

Empowering every Indian to

BE Scam SAFE

Shield yourself with awareness



बेटी बचाओ बेटी पढ़ाओ

FOREWORD

In an era marked by rapid digital transformation, the Indian banking sector stands at the forefront of enhancing accessibility and convenience through technology. However, with the increasing adoption of digital platforms, the challenge of protecting our citizens from cyber fraud has become more urgent than ever.

Government of India is undertaking special campaigns during the month of October, since 2021, and urges all its offices and organisations to take focussed action to improve efficiency in customer service, by taking up Citizen Centric initiatives during the month. Cyber frauds make customers vulnerable while accessing banking services digitally.

The "Be Scam Safe" compilation, of the State Bank of India, is an exemplary initiative that not only highlights the banking sector's dedication to technological security but also emphasizes the crucial role of consumer awareness. While banks work tirelessly to implement advanced security measures, true protection can only be achieved with informed and vigilant consumers. Understanding common threats and practicing secure banking habits are essential steps toward minimizing vulnerabilities and ensuring a safe digital experience.

This Cybersecurity booklet serves as a valuable guide in this endeavour, providing readers with practical insights and safety tips to recognize and avoid cyber scams. As you explore these pages, you may find both guidance and inspiration to approach digital banking with caution and confidence.

The Ministry of Finance, through the Department of Financial Services, wholeheartedly supports such initiatives aimed at strengthening cybersecurity and enhancing public awareness.

Together, we can create a secure and resilient digital banking environment for every Indian.

M. Nagaraju
Secretary, Department of Financial Services

FOREWORD

The world is becoming increasingly digital. In banking alone, digitization has added new layers of security, making transactions faster and safer. However, the same technology has, in recent times, being misused for criminal activity. A defining feature of these frauds is their focus on bypassing technological safeguards by actively targeting the users.

Scammers maliciously manipulate the innate element of trust - the foundation of human interaction using social engineering tactics that can leave lasting psychological effects on the victims.

Awareness and mindfulness are powerful tools in the fight against these scams.

Over time, distinct patterns have emerged in the execution of these frauds. Alerting customers and users to these methods can be instrumental in preventing such scams.

Sharing this knowledge is essential, as it helps people understand how digital technology and cybercrimes work. This, in turn, strengthens public confidence in modern banking tools and encourages the use of digital services.

Talking openly about these issues also reduces the stigma associated with these incidents. It encourages victims to step forward and report these crimes to the appropriate authorities.

We hope this Cybersecurity Booklet helps educate you, on the various types of cybercrimes and equips you with the knowledge to avert them.

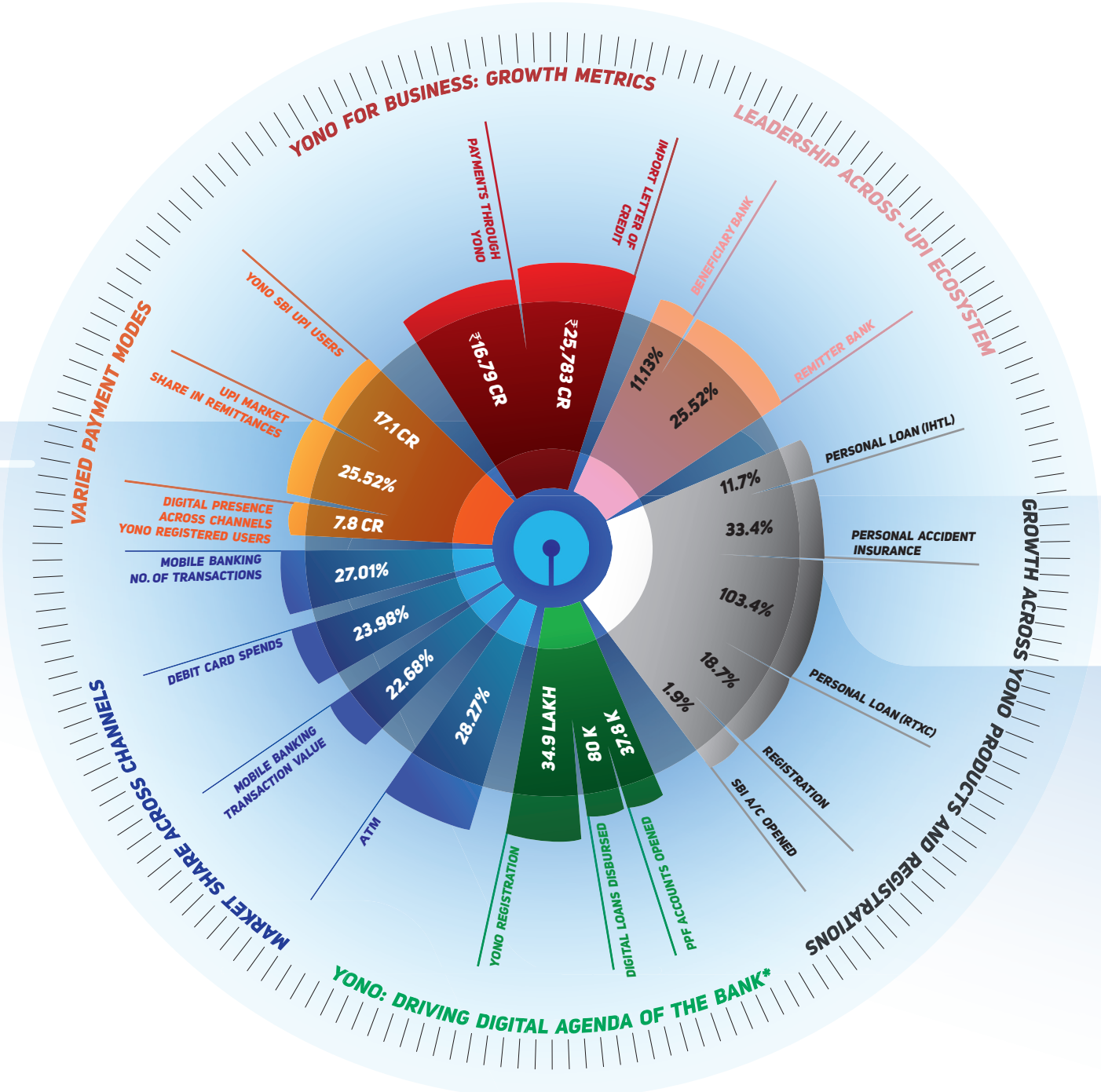
Awareness campaigns about cybercrimes have numerous valuable benefits and at SBI, we consider it our social responsibility to communicate strategies for combating these crimes.

Let us work together to make every Indian scam -safe.

C.S. Setty
Chairman, SBI

INDEX

MAPPING SBI'S DIGITAL FOOTPRINT



THE TYPES OF CYBER FRAUDS

As we have emphasised, awareness is essential to cybersecurity. In this section, we outline various types of cyber fraud in a sequence that addresses each aspect of digital exposure.

From internet banking to securing your Wi-Fi and passwords, we guide you through cybersecurity measures step-by-step, discussing different types of cyber fraud along the way. Each fraud type includes a set of tips to help you safeguard your data while using digital tools. It's essential to establish a security protocol using these recommended tips. Developing safe habits involves creating a consistent series of steps to follow, ensuring that you remain vigilant and are able to prevent most cybercrime which, paradoxically, exploit human errors rather than technological loopholes.

This is why 19 out of 20 cyber frauds are preventable with basic user awareness

Here are some general tips to help keep you safe from these attacks:

- Avoid downloading mobile apps on the advice of unknown individuals
- Do not click on unfamiliar links sent via SMS or email
- Refrain from sharing financial details such as card numbers, PIN, CVV or OTP with others via email, calls, SMS or social media
- Limit app permissions to only those necessary for the app's function, avoiding access to your gallery, messages, contacts, maps, etc.
- Avoid connecting to unauthorised public Wi-Fi networks for digital transactions
- Use strong, unique passwords and update them regularly
- Never search contact details of Bank officials/helpline number of any organisation on google. Always use official website to find the contact details

ATM SECURITY

Take this small quiz to know how secure your PIN is

1. You must cover the keypad while entering your PIN at ATM or on POS.

True

False

2. Writing your PIN number behind the card is the best way to remember it.

True

False

3. Your DOB as a PIN is the easy guess to the hacker.

True

False

4. You should save your card details on e-commerce website for future usage.

True

False

Secure ATM transactions by taking the right action

ATMs are a trustworthy and seamless ways to disburse funds. Even so, in recent years, scammers have found ways to acquire your ATM PINs through malicious means.
Their methods can easily be countered by being aware and taking precautions.

Here are a few tips to safeguard against scammers:

1. Mind your surroundings while performing transactions
2. Check the machine for suspicious installations
3. Place your card correctly
4. Cover the keypad while entering your ATM PIN
5. NEVER write down your ATM PIN
6. Ensure your ATM PIN is strong
7. DO NOT save your card on E-comm websites
8. Change your PIN periodically
9. Regularly check your account statement
10. Check your card before leaving the ATM / POS premises to avoid card-swap frauds
11. Never hand over your physical card for swiping at POS machines

Follow these tips and always Be Scam-safe.

E-COMMERCE FRAUD

E-commerce has become increasingly prevalent as internet coverage reaches every corner of our country. While some of the more popular websites ensure security for shoppers, it is not uncommon for customers to try new e-commerce platforms.The first question you need to ask yourself for a safer online shopping experience is:

Do you trust the website you're interacting with?

We come in contact with multiple e-commerce platforms daily, and unfortunately, not all of them can be trusted. Some may misuse your personal information to carry out fraudulent transactions from your account.

Be alert while shopping online and safeguard yourself against the simple tricks used by scammers.

Effectively safeguard yourself against E-commerce fraud by being aware and following these tips:

- Always look for “https” in the website URL and check for the padlock symbol
- Make transactions only through trusted websites
- Avoid making purchases by clicking on links embedded in social media platforms offering heavy discounts
- Do not store your card details on websites for future use
- Regularly monitor your account statements
- Never share the photocopy of card on social media

Be scam-safe on E-commerce platforms with these tips. Happy shopping!

SMS OR SMISHING FRAUD

The importance of SMSs has increased manifolds over the years. Brands, institutions and even government authorities have relied on this medium of communication to send urgent notifications.

SMS alerts are perceived now as both important and secure. Scammers use this perception to craft their social engineering attacks.

Their goal is either to steal your personal information or convince you to pay them with your hard-earned money.

These attacks are called Smishing attacks.

The ‘phishing’ bait used in SMS fraud

As we mentioned before Smishing is made up of two words: SMS + Phishing. The phishing part is important to understand.

Fraudulent SMS alerts in themselves cannot cause any harm. The content written in these SMSs is used to convince you to click on links or download unverified apps.

So the first step in preventing Smishing attacks is:

Verify the link before you click

How to prevent smishing attacks?

Fraudsters try to steal your financial information by sending you an SMS to update KYC or unblock YONO by clicking on the link embedded in the SMS.

This is how we can prevent falling prey to this kind of a scam:

- Check sender details to verify if the SMS is from a trusted source
- SMS from SBI will always bear the short code 'SBI' or 'SB'
- Do not share your personal/financial information over SMS
- Do not click on any links embedded in the SMSs from unknown sources

Remember, SBI never asks for your personal information through SMS
Following these tips, you won't just be safe; you'll be cyber-safe!

INTERNET BROWSING SECURITY

The Internet, though extremely useful, holds hidden cyber threats like malware, viruses, phishing and identity theft, all of which can compromise personal data and security. Safe browsing practices play a vital role in shielding users from these dangers, protecting them from online scams that target sensitive information.

When individuals visit unreliable websites or click on suspicious links, they risk exposing their devices to malware that can infiltrate systems, track keystrokes, or even hijack sessions involving online banking. Phishing scams, where attackers disguise themselves as legitimate sources, further amplify this threat by prompting users to unknowingly enter sensitive information on counterfeit sites. Such tactics can lead to serious repercussions, including identity theft, financial loss or unauthorised access to bank accounts.

By recognising unsafe practices and understanding how cyber threats operate, users can stay better informed and more secure. Knowledge and awareness are essential tools in limiting exposure to these dangers and preserving the safety of personal and financial data.

This is how we can avoid falling prey to this kind of scam:

- Always use secure HTTPS connections
- Clear browsing history, cache and cookies
- Ensure privacy by enabling 'Do Not Track' feature
- Do not save payment methods
- In Site Settings enable the 'ask permission' option for camera
- In Site Settings enable the 'ask permission' option for Microphone
- In Site Settings enable the 'ask permission' option for USB
- In Site Settings enable the 'ask permission' option for Automatic Downloads
- Complaints to be lodged on the official platform of banks/organisation rather than disclosing sensitive informations on social media platforms like X, Facebook, etc.

By following these tips, you'll Be Scam-safe!

MOBILE SECURITY

Mobile phones have become an indispensable part of our lives. We handle our work on them, store personal information and are almost always connected to the internet. This makes them susceptible to cyber-attacks where scammers attempt to hack into the device and extract information.

Why Mobile Scams are becoming prevalent

Among all forms of technology, mobile phones have become the most accessible. Mobile penetration is increasing every year. Furthermore, mobile phones are a truly personalised form of technology. Users become dependent on them, as they provide connection not only to family and loved ones but also offer curated applications and content.

The inherent privacy and accessibility of mobile phones make them prime targets for phishing attacks. These attacks are often backed by phone calls in which scammers win the user's trust to elicit personal information or initiate fraudulent transactions.

As with many other scams, mere contact with fraudsters will not lead to a loss of personal information or money. Scammers use social engineering techniques to coax or coerce users into clicking unverified links or downloading malicious apps. Following a simple protocol for mobile banking can make it much safer.

Here are some tips to add to your mobile safety routine:

- Do not click on unverified links
- Install applications and software only from trusted sources
- Use strong passwords
- Regularly update your software
- Install security software where needed
- Do not reveal key data points like your PAN, Aadhar card number or debit card PIN
- Always remember that you only need to input your mobile banking PIN to initiate transactions

By following these tips, you can bank on your mobile securely and Be Scam-safe.

SAFE INTERNET BANKING

With the increasing use of online banking services, its crucial to understand safe internet banking practices to protect yourself from potential cyber threats. This guide provides easy-to-follow instructions to help you stay safe while performing transactions online.

Secure Passwords

- Always create strong, unique passwords for your internet banking accounts
- Avoid using easily guessable information like birthdays or names
- Change your passwords regularly and avoid reusing passwords across different sites
- Enable two-factor authentication if your bank offers it. This adds an additional layer of security; 2FA usually involves receiving a one-time password (OTP) on your registered mobile number or email address, which is required to access your account

Use Secure Network

- Avoid accessing your internet banking account from public Wi-Fi networks, as these are often unsecure
- Use a secure, private internet connection whenever possible

Monitor Account Activity

- Regularly check your bank statements and transaction history for any suspicious activity
- Report any unauthorised transactions to your bank immediately

Logout After Every Session

- Always logout of your Internet banking session when you're done, especially on shared or public computers
- Simply closing the browser may not end your session, so look for the "Logout" button

Keep Your Devices Secure

- Install antivirus software on your devices and keep it updated
- Avoid downloading apps or software from untrusted sources
- Keep your operating system and apps updated to protect against security vulnerabilities
- Do not download .apk files

Avoid Saving Login Information

- Do not save your login credentials on browsers or devices, especially if others have access to them
- Use a trusted password manager if you find it difficult to remember complex passwords

Following these practices can help protect your online banking experience and keep your finances secure.

Stay vigilant and remember that your bank is there to assist you if you suspect any security threats.

Use these tips to set an Internet banking safety protocol and Be Scam-safe.

PASSWORD SECURITY

Passwords protect your personal information, such as your name, email address, phone number and other sensitive data. Strong passwords make it harder for hackers to gain access to your online accounts. Cybercriminals use stolen login credentials to access your sensitive information.

A password is the key that unlocks vital information, so always keep it safe

Just like any set of keys, it is important to keep your password secure at all times. The first step in doing so is using a password that is long and complicated to guess. If you use personal information to create your passwords, hackers can often guess the password if they obtain your data or your family's data.

Avoiding these common pitfalls is crucial for keeping your passwords safe. Hacking passwords does not just affect individuals; organisations also fall prey to these scams. Hence, take the first step towards making your personal and professional information safer by learning to use passphrases.

Here is a simple DIY exercise for crafting a passphrase:

Step 1- Think of any phrase that can be used to create a password

Step 2- Let's use the following phrase:

Phrase: I was at Borivali Street and spent ₹20 on Coffee

Step 3- Select a few letters from the phrase above and replace some letters with numbers and characters

Password: Iw@BOTR&sp20Rna

This is how we can avoid falling prey to this kind of scam:

- Always use passwords that are at least 8 characters long
- Make a password that is difficult to guess for others but easy to remember for you
- Use a mix of alphabets, numbers and special characters
- Avoid using dictionary words when creating a strong password
- Change your password regularly and do not use the same passwords in multiple places

UPI SECURITY

UPI simplifies financial transactions but there are ways fraudsters can manipulate you for their benefit. Protecting your UPI account ensures your money stays in safe hands. Your hands.

Measures to avoid UPI scam

- Always verify the UPI ID of the person before making the payment
- Create your UPI PIN to be unique, and difficult to guess
- Enter the UPI PIN only at authorised pages and do not share it with anyone Entering UPI PIN means money getting deducted from your account
- Scanning of QR code is required to make payments, not to receive money
- Use UPI Help for transaction-related queries and concerns
- No UPI PIN is required to receive money
- Do not keep photocopy of Unmasked Aadhaar on your phone as UPI can be activated through Aadhaar & mobile
- In case your mobile is lost/stolen, block the device along with the SIM as fraudsters can still carry out UPI transactions using the device by connecting to the internet, even if the SIM network is blocked
- If your SIM loses network unexpectedly, block it immediately to prevent e-SIM fraud

Follow these tips for UPI security and Be Scam-safe

LET'S TEST YOUR UPI KNOWLEDGE:

1. UPI payment can be made by using:

- A Mobile number
- B Account number & IFSC
- C UPI ID
- D All of the above

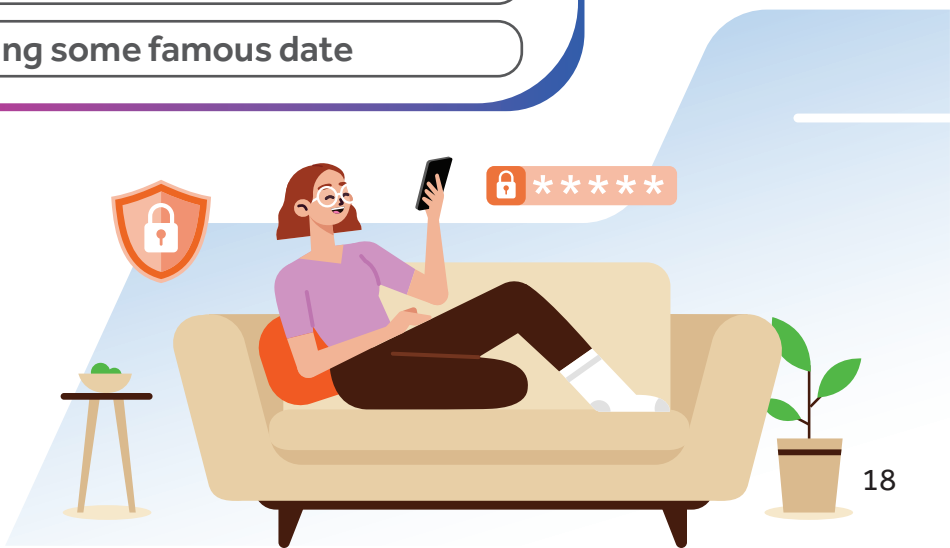
2. What will you do to receive money?

- A Scan the QR code
- B Enter UPI PIN
- C Share account number or UPI ID
- D Accept the collect request

3. How will you create your UPI PIN?

- A By using date of birth like 1992
- B By using pattern like 1357, 2468 etc.
- C Random
- D By using some famous date

Answers: Q1. D / Q2. C / Q3. C



PHISHING SCAM

Phishing scams are a growing threat. Scammers trick you into sharing your personal details, and commit fraud at your expense. Typically, these scams involve convincing emails or messages that look like they come from trusted organisations. They often ask you to click on a link or enter sensitive information, like passwords or banking details. These links or forms are designed to collect your data, giving scammers the access they need to compromise your accounts. Falling victim to phishing scams can result in significant financial losses, even the depletion of lifetime savings, as well as ongoing risks to your identity and security.

This is how we can avoid falling prey to this kind of scam:

- Do not click on unknown hyperlinks or mail attachments
- Check the authenticity of email ID of the sender
- Check the URL embedded in the email to confirm if it is a legitimate website
- Check for typos and grammatical errors in the body and subject of the email always remember, SBI never asks for your personal information over email / call / SMS

Here's a quiz about Phishing Fraud:

What information does a phishing attack target?

- A Usernames and Passwords
- B Credit Card details
- C Passwords/PIN
- D All of the above

How can you identify a phishing email?

- A Citing undue urgency
- B Generic salutations
- C Includes a suspicious hyperlink
- D All of the above

Answers: Q1. D / Q2.D

DIGITAL ARREST

Intimidation Tactics

Scammers pose as personnel from Law enforcement agencies.

Victims receive calls through Skype/WhatsApp with backgrounds replicating CBI/Police emblems, alleging their involvement in illegal activities, such as sending or receiving contraband items like drugs or fake passports, misutilisation of Sim/E-Sim.

Claims may also involve a loved one supposedly caught in criminal activities or accidents, with the fraudsters demanding money to resolve the 'case'.

Some victims are subjected to 'digital arrest,' where they are forced to stay on video calls with the scammers until their demands for money are met.

What to do in case of receiving digital arrest calls?

If a call is received through IVRS/ MANUAL we should never panic, and it is better to disconnect the call & forget about it.

If, in any case the fraudsters are blackmailing that they have kidnapped your family member, please investigate the truth independently before taking any action.

Fraudster may use WhatsApp. Don't be fooled by these tactics, stay mentally strong and never reveal any information or details which may be used against you.

Never call back to the numbers shared by Fraudsters through IVRS/WhatsApp/Messages.

Never keep these messages/calls in secret but share about this with your family and friends.

Always be vigilant & do not install any apps or open any links shared through WhatsApp which may give access to personal information stored in messages to third party, which may in turn make you a target to fraudsters.

Dial National Cyber Crime Helpline Number 1930 /Lodge complaint at cybercrime.gov.in

WI-FI AND HOTSPOT SECURITY

Unsafe Wi-Fi networks can be used to intercept personal and sensitive information, such as passwords and credit card details. Public networks, often unsecured, can expose your devices to risks like unauthorised access and data theft. This is one of the scams where data can leak into the public sphere and invite hacking attacks or worse. The best thing to do while using unsecured Wi-Fi networks or hotspots is to avoid using banking websites and other sites that have your essential data. Remember, cybercriminals often set up fake Wi-Fi hotspots in public places to lure unsuspecting users. Even networks that seem legitimate can be risky if they lack proper encryption. To safeguard your information, always assume that public Wi-Fi is insecure. By practising safe browsing habits and using a few protective measures, you can significantly reduce the risk of exposure.

This is how we can prevent falling prey to this kind of a scam:

- Remove all untrusted networks from the list of saved networks
- Enable the option of 'Detect Suspicious Networks'
- Always disable the 'Passpoint Security' feature
- Turn off automatic Wi-Fi connections
- Be wary of unknown networks
- Avoid public Wi-Fi networks

Follow these tips and Be Scam-safe

Take this quiz on Wi-Fi and Hotspot Security:

What should you avoid doing when connected to public Wi-Fi?

- A Checking the weather
- B Watching videos
- C Accessing your bank account
- D Reading the news

What's the best way to keep your mobile hotspot secure?

- A Use a simple password like "123456"
- B Set a strong password
- C Keep it on all the time for easy access
- D Share the hotspot with anyone who ask

Answers: Q1.C / Q2.B

DIGITAL INVESTMENT FRAUDS

In recent years, Digital Investment Frauds have grown manifold, often taking advantage of unsuspecting investors. Fraudsters use fake websites, social media platforms, SMS, and emails to offer investment schemes that promise high returns with little to no risk. Once an investor shows interest, these fraudsters ask for personal information and bank details, often leading to financial losses.

Common Types of Digital Investment Frauds:

1. **Ponzi Schemes:**
   Investors are promised high returns, which are paid using the funds of new investors. When there are no new investors, the scheme collapses, resulting in losses for most.
2. **Pump and Dump:**
   Fraudsters artificially inflate the price of a stock by spreading misleading information, only to sell it at the peak, leaving other investors with losses.
3. **Phishing and Vishing:**
   Fraudsters pose as legitimate financial institutions, asking for sensitive information to gain unauthorized access to accounts.
4. **Fake Investment Platforms:**
   Fraudulent apps and websites that look legitimate but are designed to steal money from users.

Red Flags to Watch Out For:
Unrealistic Returns -: If it sounds too good to be true, it probably is.
Pressure to Invest Quickly -: Scammers often pressure targets to act fast to avoid “missing out.”
Unverified Sources -: Always cross-check the legitimacy of the investment platform.

How to Protect Yourself:

Do Not Share Personal Information
Legitimate financial institutions never ask for sensitive information via SMS, email, or social media.
Verify the Source
Always check the legitimacy of websites and investment apps before investing.
Report Suspected Frauds
If you suspect fraud, report it to the authorities or your bank.

Stay informed and be vigilant. Protect your investments by staying aware of digital fraud schemes and reporting any suspicious activity.

STEPS TAKEN BY SBI TO ENHANCE DIGITAL SECURITY

The Bank's security strategy focuses on proactive cyber risk management and maintaining strong cyber resilience and hygiene. A layered security approach, defence in depth, and security by design are key elements of our strategy.

The primary security features include:

Application Whitelisting Solution

This detects unauthorised applications on workstations or mobile devices by matching application signatures, preventing the execution of such applications.

Data Encryption

Data transmitted over the internet or between locations is encrypted (secured) to prevent theft.

Multifactor Authentication

Enabled for all customer-facing digital applications, multifactor authentication adds an extra layer of security in the digital journey, ensuring that only authorised users access the application.

Profile Password

Our internet banking and mobile banking systems include an additional profile password, providing enhanced security for authorised users accessing the profile section.

Proactive Monitoring Systems

These systems analyse traffic on banking applications to detect fraud and take protective measures to safeguard customers' interests, helping prevent unauthorised access.

Rooted Device Detection

The Bank's mobile applications check devices to confirm they are not rooted or jailbroken (altered to access unauthorised data) before launching, ensuring a secure financial journey.

SIM Binding

User IDs are mapped to the SIM of the registered mobile and device at registration, creating a secure digital identity and ensuring applications are accessed only through registered devices.

Solution for Identifying Rogue Applications

This feature detects the presence of rogue or remote access applications on devices, helping prevent unauthorised access.

Proactive Monitoring System (PRM)

Upon any suspicious transactions through digital channels, PRM alerts the customers within seconds of the transactions being attempted by calling the customers on their registered mobile number. If the transaction is a potential fraud, digital channels are blocked to protect the customers. In case of digital arrest and fake investment transactions, customers are counselled about potential frauds

AWARENESS: THE MOST POTENT WEAPON

MOTIVATING INDIA TO BE SCAM-SAFE

Introduction

Awareness is essential in preventing cyber fraud, serving as a critical defence in the digital landscape. While digital technology is equipped with strong safety features, such as encryption and secure access protocols, cybercriminals often bypass these by targeting human vulnerabilities. This manipulation, known as social engineering, involves using psychological tactics to gain sensitive information. Scammers commonly impersonate trusted entities, like banks, to create urgency or fear, prompting quick responses without verification.

By understanding these tactics, individuals can recognise suspicious patterns, such as unexpected messages or requests for personal details. Simple steps like verifying the authenticity of communications, avoiding unfamiliar links and safeguarding personal data can help prevent cyber fraud. Ultimately, greater awareness enables individuals to actively protect themselves and contribute to the wider security of our digital environment, making fraud attempts far less effective.

Strategic Communication

A campaign becomes impactful when it is executed in a planned manner. This includes the medium of delivery, the choice of spokespersons, the frequency of messaging and the message itself.

To meet these vital parameters and to promote awareness in an engaging, effective manner, SBI has developed a campaign property that it executes regularly.

Be Scam-Safe

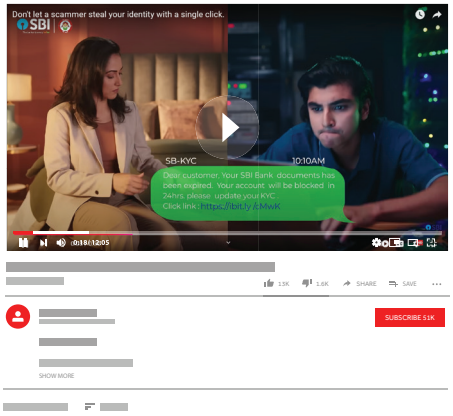
This campaign puts our customers in the spotlight, showing them successfully defending themselves against scammers with the support of an SBI representative. In its outdoor renditions, prominent public figures like MS Dhoni are featured to amplify the campaign's message.

Simple, easy-to-remember rhymes encapsulate the message, making it memorable and demystifying scams for the audience. The use of colloquial language also makes the campaign relatable. The digital renditions ensure the message consistently reaches people throughout the year, adding a personal touch.

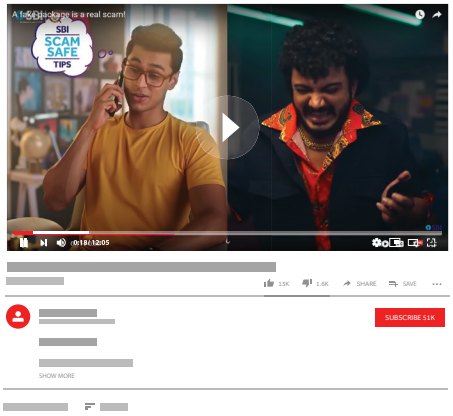
Each aspect of the campaign not only promotes awareness but also tackles the stigma surrounding scams. Here is an overview of the work done to address cybersecurity through this campaign and beyond.

CAMPAIGN WITH OUR BRAND AMBASSADOR

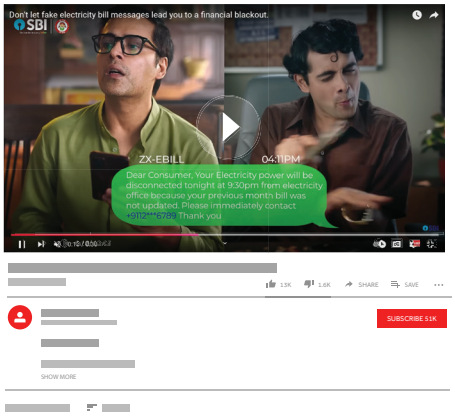
THE BE SCAM-SAFE VIDEO LIBRARY



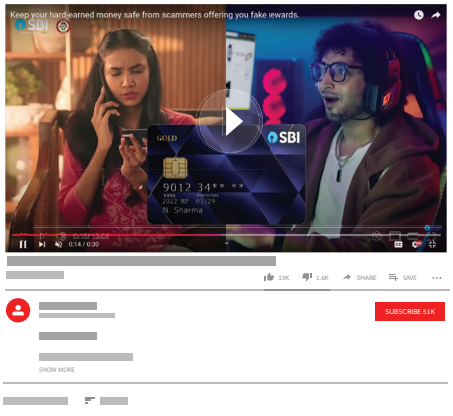
KYC update scam



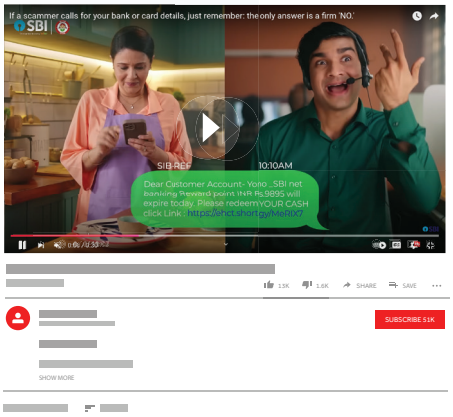
Fake courier scam



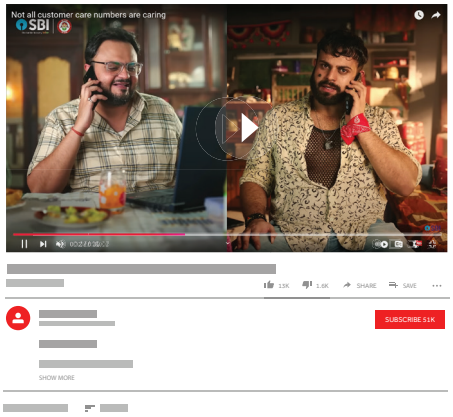
Fake electricity bills scam



ATM card details scam



Rewards scam



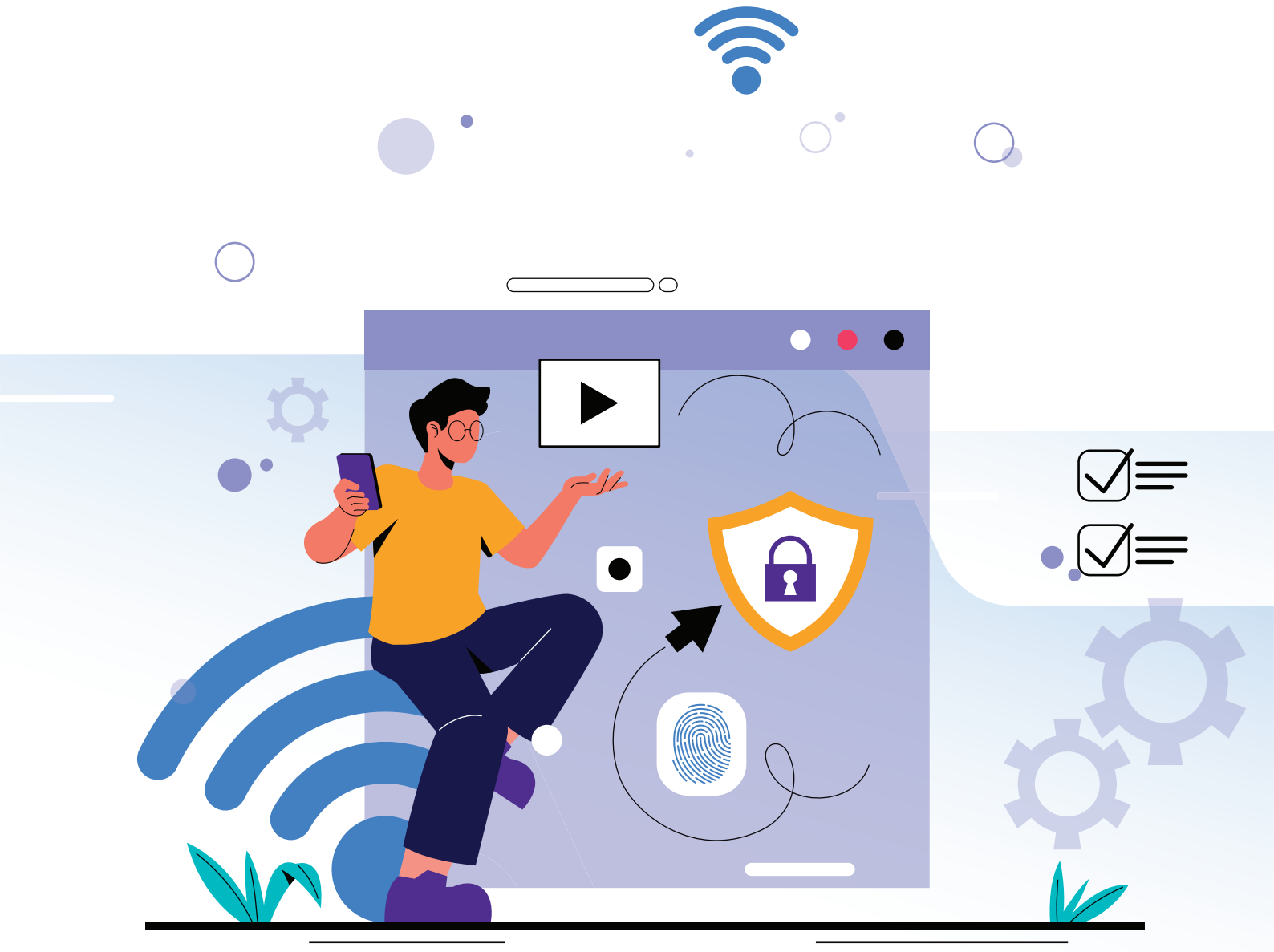
Call center scam

SCAN TO WATCH

OOH ACTIVATIONS

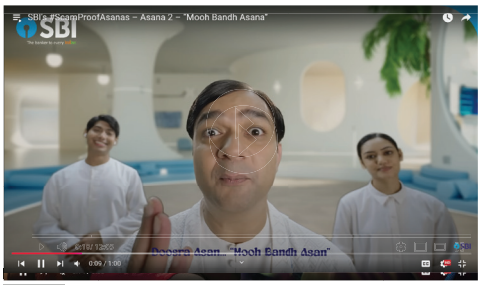
SBI's train branding initiative reaches lakhs of eyeballs daily - reminding people about the safety measures they can adopt to keeping themselves safe from any and every scam; and how the banker to every Indian stands beside them in their journey to be scam-safe.

EDUCATIONAL CAMPAIGNS THAT ENGAGE



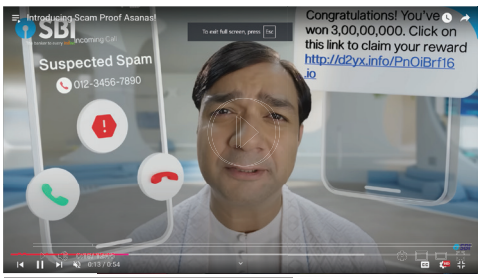
SCAM-PROOF ASANAS VIDEO LIBRARY

Teaser



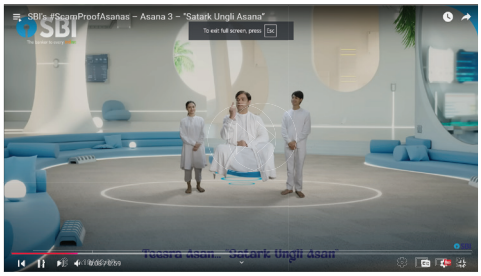
Introduction

Kaan Khule Asana



Mooh Bandh Asana

Satark Ungli Asana



Sadev Sachet Asana

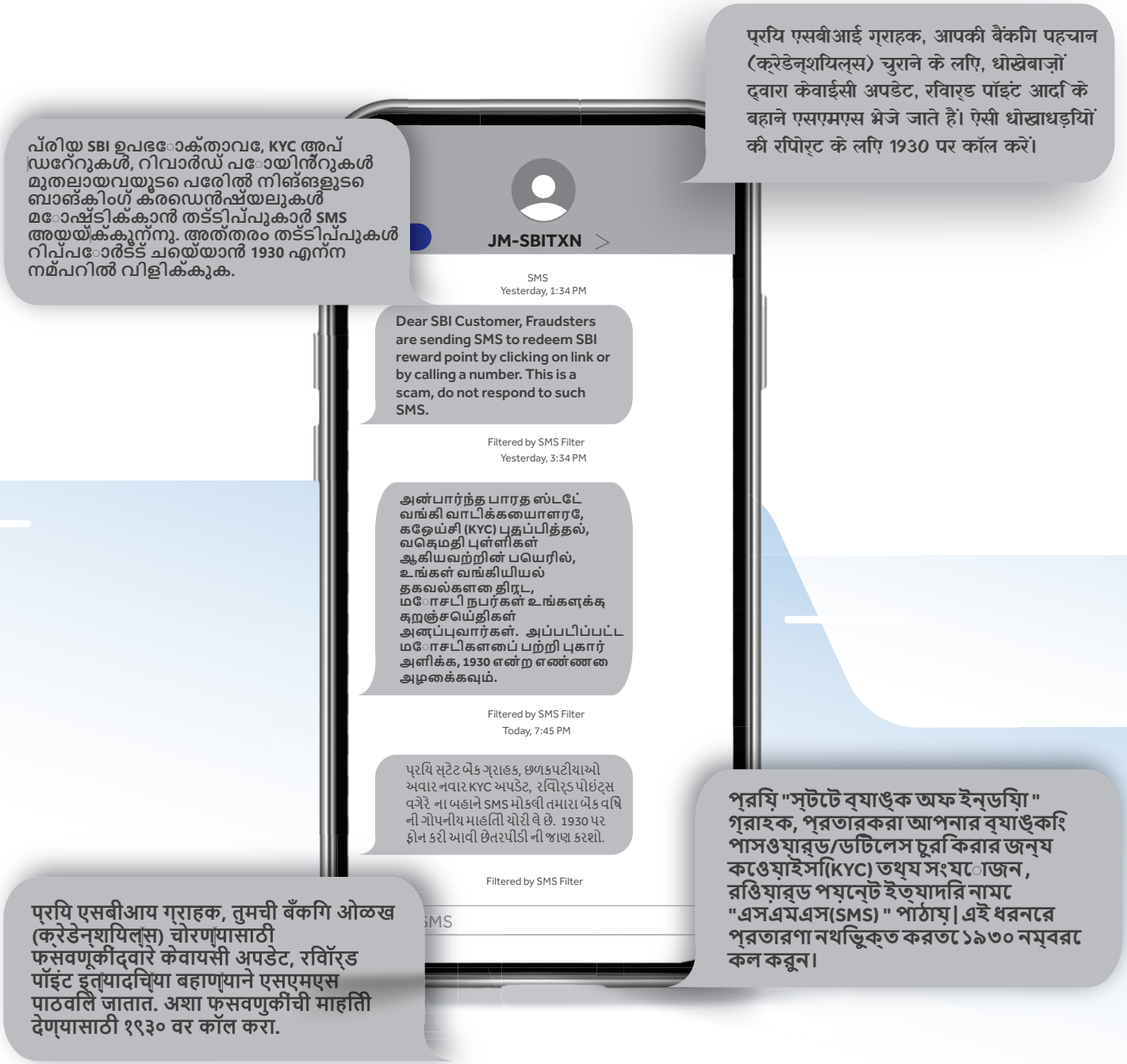
SCAN TO WATCH

REACHING THROUGH PRINT MEDIA

10.03+ cr readers reached through print ads across India in multiple languages

SBI's print ads serve as a quick guide to cyber security, providing readers with clear and actionable steps to safeguard their information. These informative ads make basic information and knowledge accessible to all.

SMS ALERTS TO EVERY INDIAN



SMSs have been misused by scammers repeatedly to perpetuate their frauds. We take this tool and use it to promote awareness. This addresses the problem at the source because our SMSs educate the customers about these frauds. The messaging is curated to our customers, furthermore, local languages are used so that our messaging is more relatable and memorable to our audiences.

EDUCATING OUR EMPLOYEES, STAKEHOLDERS AND CUSTOMERS

Cybersecurity awareness among staff members

- **Information Security Awareness Sessions:**
  ISD has been conducting awareness sessions on topics like comprehensive IS awareness sessions with aspecial focus on demos on phishing and mobile security, IS policy, data security etc. During the sessions, emphasis was given to security concerns related to payment apps, ransomware, IS Policies, API security, OWASP vulnerability etc.
- **Session on Secure Coding Practices:**
  ISD has been conducting training sessions on secure coding practices for the employees working as developers to educate them about the secure coding practices, guidelines and processes to be followed to prevent the known vulnerabilities.
- **Broadcast Emails:**
  Emails guiding about recent vulnerabilities like: acceptable usage policy, ransomware, data security, WhatsApp scams etc. are being broadcast to all employees regularly.
- **SMS to employees:**
  SMSs to guide secure practices to be followed during day-to-day activities are being sent to all the employees of the Bank.
- **AD screensavers:**
  AD screensavers on IS policy, data security and acceptable usage policy will be launched.
- **Quiz on Security Awareness:**
  Quizzes to assess Information Security Awareness among employees will be conducted for the full month of November'24.
- **IS awareness sessions for employees posted in Circle / Corporate Centre Establishments (CCEs):**
  Different teams of ISD conducted a full day IS awareness sessions in all 17 circles and CCEs. Sessions will be conducted in offline mode and attended by employees of the bank and vendors. During these visits in addition to is awareness, various topics/issues related to the circle will be discussed by visiting officials with senior functionaries of the Circle.

Alerting our stakeholders, vendors and other partners

- **Information Security Awareness Sessions:**
  ISD is conducting awareness sessions with a live demo on hacking techniques covering topics like cloud security, Comprehensive IS Awareness sessions with a special focus on demos on Phishing and Mobile Security and a special focus on security concerns related to payment apps, etc.
- **Session on Secure Coding Practices:**
  We have conducted an IS awareness session on secure coding practices for the vendor's employees to educate them about the best practices, guidelines and processes to be followed to prevent known vulnerabilities.

Regularly alerting the customers

We recognise the fact that awareness cannot be ensured with a single campaign. We have repeatedly alerted customers and citizens using various media and creative methods. Here is an overview of our work in the public sphere to prevent cyber fraud.

Awareness is essential in preventing cyberfraud, serving as a critical defence in the digital landscape. While digital technology is equipped with strong safety features, such as encryption and secure access protocols, cybercriminals often bypass these by targeting human vulnerabilities. This manipulation, known as social engineering, involves using psychological tactics to gain sensitive information. Scammers commonly impersonate trusted entities, like banks, to create urgency or fear, prompting quick responses without verification. For instance, an email might falsely claim a bank account issue, urging immediate action.

DIGITAL FRAUDS: PREVENTIVE MEASURES

- Do not click on links received through SMS/Mail/Digital Medium.
- Never receive unknown video calls on WhatsApp / Telegram / Skype.
- Never act on online advice for performing financial transactions.
- Never share personal credentials, OTPs, Login Passwords / ID, PIN / MPIN.
- Never scan QR codes received from unknown persons for making or receiving payments.
- If you suspect a caller or message, disable your location/internet services.
- Always receive landline calls from State Bank of India (verified by the carrier checkmark).
- Never install apps from unknown sources or on the advice of unknown persons.
- Never call back numbers shared by unknown sources through IVRS/WhatsApp/Messages.
- Law enforcement agencies never contact via social media, WhatsApp, or Skype. Disconnect immediately if you get such a call.
- Regularly change your passwords and PIN / MPINs.
- Do not write down personal information like login ID/Password, PIN/MPIN, etc., anywhere
- Transactional/promotional messages sent by SBI will always bear short codes containing "SBI, SB", for e.g. SBIBNK, SBIINB, SBYONO, ATMSBI
- The URL of official websites of SBI will always contain .sbi as top-level domain, for e.g. https://onlinesbi.sbi, https://bank.sbi

IN CASE YOU ARE VICTIMISED

- Block all digital channels on suspicion to avert losses
- Call **1930** immediately, or register the complaint at **https://cybercrime.gov.in/**
- Call the bank's customer care number: **1800 11 1109 / 1800 1234** to report unauthorised transactions
- Report the fraudulent mobile number on DOT's Sanchar Sathi Portal **https://sancharsaathi.gov.in/**
- Contact the nearest branch

CONCLUSION

As we advance into an increasingly digital world, understanding and practicing cyber security is essential. The internet offers immense convenience and opportunities, but with it come threats that can compromise personal data, financial assets, and even peace of mind. This booklet has provided practical guidance to help you identify potential threats, from phishing scams to malware and data breaches, empowering you with the knowledge to stay one step ahead of cybercriminals.

Every online action-whether it's clicking on a link, making a transaction, or downloading a file-plays a part in your digital safety. By following best practices like using strong, unique passwords, enabling two-factor authentication, being cautious of suspicious emails, and regularly updating software, you build a proactive defense against threats.

Cyber security isn't just a personal responsibility; it's a shared one. Each of us has a role in creating a secure digital environment, and your commitment to staying informed helps strengthen security for all. Remember that protecting yourself online is an ongoing process that evolves as cyber threats change.

So stay alert, stay educated, and stay safe online-because a secure digital world is within reach, and it starts with each of us. Let's work together to foster a culture of cyber awareness and resilience, and remain scam-safe.

SBI
The banker to every indian

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Indian
Cyber
Crime
Coordination
Centre

CYBER
DOST

DIAL 1930 TO REPORT ONLINE FINANCIAL FRAUD

REPORT ANY CYBERCRIME ON WWW.CYBERCRIME.GOV.IN

Call : Bank Contact Centre numbers 1800 1234 | 1800 111109