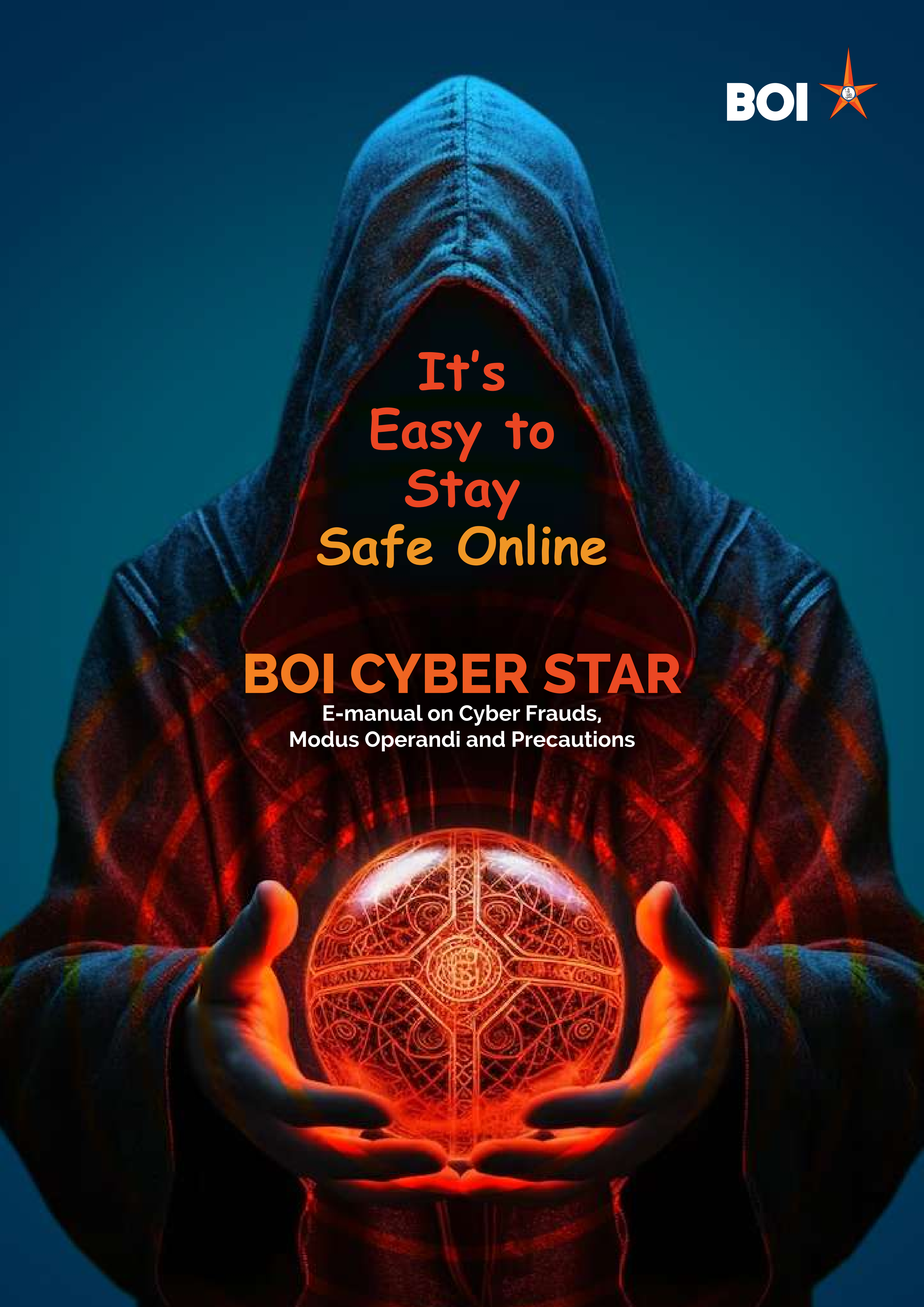
BOI



It's Easy to Stay Safe Online

BOI CYBER STAR

E-manual on Cyber Frauds, Modus Operandi and Precautions

Index

Report Cyber Fraud under Grievance Section of our website and on Govt. of India portal www.cybercrime.gov.in OR call on **1930**. For more information visit https://bankofindia.co.in/safe-banking

Preface

Information Security is the practice of protecting data, systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

The global cyber threat continues to evolve with a rising number of data breaches each year. According to statistics from Symantec and McAfee, global losses, due to cybercrime exceeds $1 trillion annually. In India, losses reported due to cybercrimes are more than 12,000 crore rupees annually. According to Govt. report, over 13.91 lakh cyber security incidents are witnessed in India in 2022. These incidents included Phishing Attacks, Website Intrusions, Malware Attacks, and Ransomware Attacks.

Understanding cyber security principles and best practices is vital to all users. Information Security Cell in Bank of India strives towards keeping the Bank's IT infrastructure and information of all stakeholders safe and secure. Confidentiality, Integrity and Availability of the Data is maintained at all levels. A dedicated SOC team pro-actively monitors various alerts and incidents.

This e-manual is a concise overview of various Cyber Frauds, their Modus Operandi and Precautions to be taken, considering the present trends in the burgeoning digital world. Timely reporting of Cyber Incidents and Cyber Frauds may save us from financial losses and reputational losses. This e-manual is an endeavour from Information Security Cell, Risk Management Department, Head Office to promote cyber security best practices among all stakeholders.

Keep yourself and your family safe in Tech driven world.

STAY VIGILANT! STAY SAFE!

MD & CEO's Message

Cyber Security is everyone's responsibility

In today's digital age, the cyber landscape is constantly evolving, and cyberattacks have become more sophisticated than ever before. Our collective vigilance and proactive measures are crucial to safeguarding our sensitive information, maintaining our reputation, and ensuring the trust of our customers, regulators and other stakeholders.

Cyber security awareness is the state of both knowing and responding to protect information assets. We must be vigilant and careful while connecting digitally to the world.

The information provided in this handbook is intended to create awareness among readers on various cyber threats that may impact drastically and provide tips to safeguard themselves against cybercrimes. By following these guidelines and staying informed about cybersecurity best practices, you are contributing to our collective defense against cyber threats. Remember that cybersecurity is not just an IT issue—it's a responsibility shared by each one of us.

Your vigilance and dedication to maintaining a secure work environment are deeply appreciated. Let's work together to keep Bank of India safe and secure.

My best wishes to all.

(Rajneesh Karnatak)
MD & CEO

ED's Message

Adopt Cyber Hygiene & Be Secure

I am happy that, Information Security Cell is publishing this Cyber Security Awareness e-manual during Cyber Security Awareness month of October 2023.

Today, Cyber Security is widely viewed as a matter of pressing importance. With the advancement and complexity of IT, many elements of cyberspace are vulnerable to an expanding range of attacks by a spectrum of hackers, criminals, terrorists, and state actors.

Information and Data are key assets of any organisation. It is utmost important to protect the information from compromising at any level, whether it is personal or organisational. Cyber Security is a process that is designed to protect networks and devices from any external threats.

The three main pillars of Cyber Security are CIA triad, which refers to protection of Confidentiality, Integrity and Availability of data. Each component represents a fundamental objective of information security. Further, success of any organisation is dependent on three elements The People, Process and Technology. Amongst all these three elements, 'people' is the most important but weakest link. As in today's scenario, we handle gigantic data, which is to be well protected, it is everyone's responsibility to ensure data security and privacy in all their areas of work.

This e-booklet has been designed by sharing the latest modus operandi of the Cyber frauds with users and advising them on precautions to be taken to avoid being a victims of such frauds.

I personally request each and every one to adopt cyber hygiene best practices highlighted in the Book, while doing their day to day activities. It will significantly help in ensuring data security and data privacy in the organisation and will build confidence among our esteemed customers.

My Best Wishes and season greetings to you all and your family members.

S Kumar

(Subrat Kumar)
Executive Director

BOI

CISO's Message

See Yourself in Cyber- It's easy to Stay Safe online

October is observed as Cyber Security Awareness Month, a dedicated month for all of us to work together to raise awareness on the importance of following cyber hygiene best practices in our day to day life to achieve cyber security.

Each one of us is a front-line defender against incoming threats, and the danger comes in the most unexpected way without warning. Our little negligence may roll out the red carpet for hackers and scammers. Despite the fact that cyber-threats have become much more widely recognized, cyber security is often viewed as a technology problem and responsibility of the organisation only. But the fact is, Cyber Security is everyone's responsibility.

This "BOI Cyber Star" e-manual will act as easy reference of cyber hygiene best practices to all. The contents of this book covers most prevalent cyber frauds like Social Engineering Frauds, E-Commerce Frauds, Fake Loan app/ job offer, Phishing attacks, QR code scam etc.

The Bank of India has implemented various security measures like 24x7 C-SOC (Cyber Security Operations Centre) with state of the art security solutions, Data Leakage Prevention Solution (DLP) etc., to proactively monitor cyber threats impacting corporate IT Assets and data. Still support from all stakeholders is essential to achieve overall cyber security objectives.

I personally appeal to everyone to be very cautious while making online payments, using card payments or withdrawing cash from ATM, sharing your valuable information over the phone or on social media. All should make ourselves cyber security aware to safeguard our valuable personal information, data and hard-eared money.

Best wishes, to you all,

With Warm Regards.

Kuldeep Pal
CISO

General Precautions to avoid falling prey to Cyber Frauds

General Precautions

- Be wary of suspicious looking pop ups that appear during your browsing sessions on Internet.
- Always check for a secure payment gateway (https:// - URL with a pad lock symbol) before making online payments/transactions.
- Keep the PIN (Personal Identification Number), password, and credit or debit card number, CVV, etc., private and do not share this confidential financial information with friends or even family members.
- Avoid saving card details on websites/devices/public laptop/desktops.
- Turn on two-factor authentication where such facility is available.
- Never open/respond to emails from unknown sources as these may contain suspicious attachment or phishing links.
- Do not share copies of chequebook, KYC documents with strangers.

General Precautions to avoid falling prey to Cyber Frauds

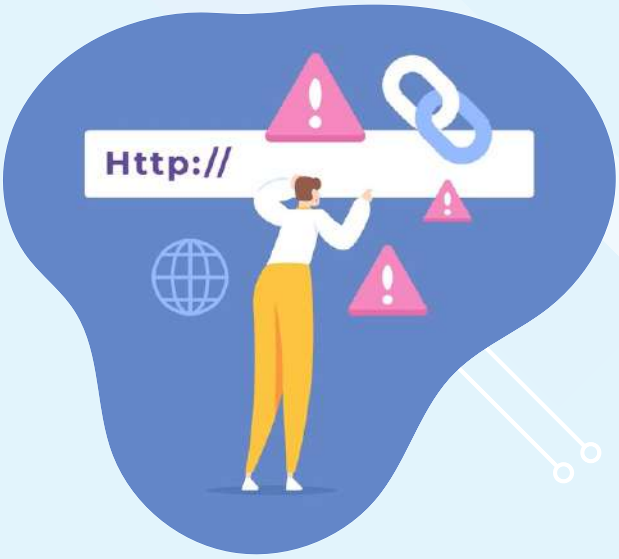
For device/computer security

- Change passwords at regular intervals.
- Install antivirus on your devices and install updates whenever available.
- Configure auto lock of the device after a specified time.
- Do not install any unknown applications or softwares on your phone / laptop.
- Do not store passwords or confidential information on devices.
- Always scan unknown Universal Serial Bus (USB) drives / devices before usage.

Factors indicating that a phone is being spied

- Unfamiliar applications are being downloaded on the phone.
- There is a faster than usual draining of phone battery.
- Phone turning hot may be a sign of someone spying by running a spyware in the background.
- An unusual surge in the amount of data consumption
- Spyware apps interfere with phone's shutdown process by taking longer time than usual.
- Note that text messages can be used by spyware to send and receive data.

General Precautions to avoid falling prey to Cyber Frauds



For safe internet browsing

- Avoid visiting unsecure / unknown websites.
- Avoid using unknown browsers.
- Avoid using / saving passwords on public devices
- Avoid entering secure credentials on unknown websites/ public devices.
- Do not share private information with anyone, particularly unknown persons on social media.
- Always verify security of any webpage (https:// - URL with a pad lock symbol), more so when an email or SMS link is redirected to such pages.
- Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc.
- Log out of the internet banking session immediately after usage.
- Update passwords on a periodic basis.
- Do not use same passwords for your email and internet banking.
- Avoid using public terminals (viz. cyber cafe, etc.) for financial transactions.

ATM Skimming

Skimming is a method used by fraudsters to capture your personal or account information from your credit/debit card. Fraudsters may steal your confidential details at ATM Centres or at Point of Sale Machines at Restaurants or shopping malls or any shops etc.

Precautions

- 👍 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, 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 but inform the bank.
- 👍 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.

Cloning of Biometrics

Cyber criminals are misusing Aadhaar Enabled Payment System (AePS) to carry out financial frauds. The system allows any user to deposit cash, withdraw cash, transfer funds and check statement using Aadhaar number and biometrics.

Modus Operandi

- ⚠ Cybercriminals get your biometric information from documents having thumb impressions and then they get soft copies of your Aadhaar card along with your thumb expression, PAN card, mobile number, bank account details, etc.
- ⚠ With soft copies, cybercriminals print the thumb imprint on butter paper and use a stamper machine to clone the thumb impression.
- ⚠ Then fraudsters alter the Aadhar card details by changing the photo, name, and address and create a new QR code. When the code is scanned, the desired name appear.
- ⚠ By using AePS, fraudsters transfer money from the victims' account using the fake thumb impression of the victim and immediately withdraw the money.

Precautions

- 👍 Regularly check your bank statement.
- 👍 Be careful while giving Aadhaar details.
- 👍 Always try to use a masked Aadhar/ DigiLocker instead of Aadhaar card.
- 👍 Lock Aadhaar and biometrics via the m-Aadhaar application or https://uidai.gov.in/ and unlock them as and when required.

Executive Impersonation

Cyber Criminal creates fake profile on Social media platform of a well-respected corporate executive & uses his/ her identity to steal confidential corporate data or gain financial benefits from employees or partners of the corporate.

Modus Operandi

- ⚠ Sense of urgency to get sensitive information.
- ⚠ Unusual money transfer requests.
- ⚠ Suspicious/erroneous email/domain address.
- ⚠ Unprofessionally drafted communication.
- ⚠ Malicious links/attachments.

Precautions

- Never transfer money in a hurry
- Check the identity of person using official contact numbers of the executive & double check with common contacts
- Follow your organization's SOPs for fund transfer or data sharing
- Report to the platform's customer support with evidential screenshots

Report Cyber Fraud under Grievance Section of our website and on Govt. of India portal www.cybercrime.gov.in OR call on **1930**. For more information visit https://bankofindia.co.in/safe-banking

E-Commerce Transaction scams

Fraudesters' fake promises result in your real loss.

Modus Operandi

- ⚠ Scammers publish their advertisements with bargain deals on well-known social media platforms or create fake websites.
- ⚠ They use enticing deals, counterfeit product images, fake reviews, professional-looking designs, and phishing emails to trick you into sharing your financial information.
- ⚠ In these scams, you may receive compromised or no product at all.
- ⚠ If you attempt to reach out to the vendor for returns, you may encounter invalid contact information or unfriendly return policy.
- ⚠ In the case of a fake e-commerce website, they might confirm your order initially but then disappear with your money and personal information.
- ⚠ As a result, you lose money and confidential personal and financial information.

Precautions

- 👍 Beware while clicking on any advertisement posted on various social media platforms.
- 👍 If you are redirected to another website, always look for secure URLs (https://).
- 👍 Be careful with the amazing deals, they might be scams.
- 👍 Legitimate e-commerce stores provide you with contact information like an address, phone number, and email with 24x7 customer support numbers.
- 👍 Poorly written content on a website is a red flag. Scammers may not have paid attention to details in their text.
- 👍 When searching for products online, use reputable search engines, as they are more likely to filter out scam websites.

Hash Code Fraud

In this kind of fraud victim won't receive any warnings or SMS regarding the financial transaction since fraudsters hacked his/ her smartphone and carry out the financial transaction anonymously.

Modus Operandi

- ⚠ In this scam, the victim is informed via a message from an anonymous number that a specific service has been activated on their number. Another number is given, and it is claimed that in order to stop the service, a message must be sent to that number.
- ⚠ The individual who texts the number gets a call from the fraudster. The victim is asked to enter a hash code (*21*Fraudster_phone_number#) into their dial pad by the scammer impersonating as a customer service representative in order to stop the service.
- ⚠ When the victim dials the code, all calls are forwarded to another number that belongs to the fraudster.
- ⚠ By this, the fraudster starts getting access to the victim's bank account - related OTPs.

Precautions

- 👍 Don't blindly believe in such messages. Instead of following the directions of the fraudster, always contact the official helpline of Bank for any complaint/ inquiry.
- 👍 Before responding to such communications, always examine the SMS header. It should be of your Bank only.
- 👍 Check your mobile's call forwarding settings frequently.

Instant Loan App Fraud

Instant Loan App Fraud is the racket for luring people to take instant loans via mobile apps and then extorting money from them.

Modus Operandi

- Doesn't have legitimate functional corporate website, physical address and RBI registration.
- Doesn't follow KYC guidelines.
- Doesn't check credit scores and documentation.
- Demands advance processing fees & miscellaneous payments.
- Asks for more personal and financial data.
- Doesn't provide loan agreements & RBI - mandated disclosures.
- Demands exorbitant interest rates & EMIs.
- Never discloses actual total fees.

Precautions

- Stay vigilant and cautious of unknown lending apps.
- Read the terms and conditions and check permission settings carefully before you proceed with using such apps.

Job Offers Scam

Scammers send fake messages or emails offering jobs claiming to be from reputed companies and ask for money.

Modus Operandi

- ⚠ Fraudsters use text messages to entice victims with various job offers.
- ⚠ Victims who join a chat group are given simple prepaid tasks and an initial payment.
- ⚠ They are then presented with a fake high-return investment plan by return of small initial investments.
- ⚠ As minor profits roll in, victims are manipulated into larger investments.
- ⚠ When victims attempt to withdraw funds, the platform requests payments for withdrawal fees.
- ⚠ Fearful of financial loss, victims pay these fees, only to discover that the platform crashes, taking all their money. This is how the scam reveals itself.

Precautions

- 👍 Be alert on job offers with high pay for minimal effort, qualifications, or guaranteed employment.
- 👍 Thoroughly investigate any potential employer by checking their official website, address, and contact details.
- 👍 Exercise caution with emails or texts from unknown companies, as scammers might use them to collect personal information.
- 👍 Don't share sensitive data like bank details, or user IDs on initial job applications.
- 👍 Legitimate employers won't request upfront payments, like fees for background checks or training.
- 👍 Be suspicious of any such requests.

Juice Jacking

Juice jacking occurs when a malicious actor has infected a USB port (or the cable attached to the port) with malware. That typically occurs on public charging stations you find in airports, shopping centers, and coffee shops, among other places.

Modus Operandi

⚠ When you connect your phone to your computer via USB, typically gets mounted as an external drive, and you can access and copy files to and from your phone. That's because, as mentioned above, your typical USB port isn't simply a power socket but a data channel as well.

Precautions

- Avoid public charging stations.

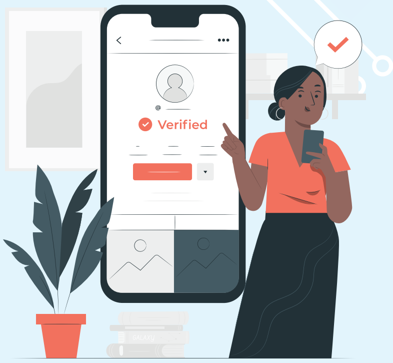
  Enable and use your device's software security measures.
- Disable your device's option to automatically transfer data when a charging cable is connected. This is the default on iOS devices. Android users should disable this option in the Settings app.
- Lock your device once connected to the charging station. That will prevent it from being able to sync or transfer data.
- If your device displays a prompt asking you to trust this computer, it means you've connected to another device, not simply a power outlet. Deny the permission, as trusting the computer will enable data transfers to and from your device.
- You can also turn your device off before charging it. However, many mobile phones automatically turn on when connected to power so, If your mobile phone does not turn on automatically when connected to power , this is an effective safeguard.

KYC Expiry Scam

Fraudsters contact the person through fake SMS/ Calls/ Emails, posing themselves as Bank/ RBI officials and ask him/her to update their KYC details, otherwise their account will be blocked.

Modus Operandi

⚠ You receive SMS/Email/Call stating that:
A. Your KYC has expired.
B. Or it needs to be renewed/updated.
Otherwise your account will be blocked.



Precautions

- Never trust these type of communications. Through this fraudsters attempt to get your bank details. In case, such caller request you to download any app such as QuickSupport or Anydesk etc, [To access Your device Remotely] to complete or renew KYC details, just ignore the same and never download such apps as they could be used by fraudsters to take over your UPI/ Mobile Banking account and steal money from your account.
- Never click on unauthorised links for Apps shared over mails or Social media apps like WhatsApp, Facebook, etc.
- Bank or payment service providers never send the link and ask their customers to update their KYC details online.
- Always treat unsolicited callers/ emails/ SMS with suspicion.
- Never share debit card/ Credit card/ Internet banking details with anyone or write login ID, Password or PIN anywhere as it may lead to un-authorized transactions.

Money Mules

Money Mule is a term used to describe innocent victims who are duped by fraudsters into laundering stolen/illegal money via their bank account/s.

Modus Operandi

- ⚠ Fraudsters contact customers via emails, social media, etc., and convince them to receive money into their bank accounts (money mule), in exchange for attractive commissions
- ⚠ The money mule is then directed to transfer the money to another money mule's account, starting a chain that ultimately results in the money getting transferred to the fraudster's account.
- ⚠ When such frauds are reported, the money mule becomes the target of police investigation for money laundering.

Precautions

- 👍 Do not allow others to use your account to receive or transfer money for a fee/payment.
- 👍 Do not respond to emails asking for your bank account details.
- 👍 Do not get carried away by attractive offers/commissions and give consent to receive unauthorised money and to transfer to others or withdraw cash and give it out for a handsome fee.
- 👍 If the source of funds is not genuine, or the rationale for underlying transaction is not proved to authorities, the receiver of money is likely to land in serious trouble with police and other law enforcement agencies.

Phishing

Phishing is an unethical way of stealing confidential, personal, professional & financial data through fake emails and links.

Modus Operandi

- Lucrative offers difficult to be true.
- Urgent/threatening language.
- Strange or abrupt business requests.
- Requests to install some App / click on unfamiliar hyperlinks or attachments.
- Requests to share Money / Banking credentials / personal information.
- Spelling errors and poor grammar.
- Sender's e-mail address doesn't match the display name of sender.

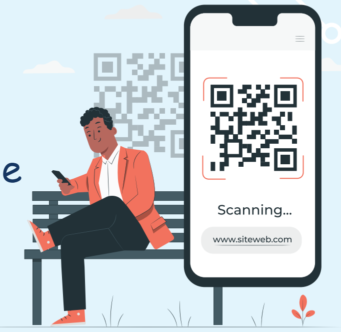
Precautions

- Avoid clicking on any links or replying, rather just delete the email.
- Block the sender.
- Never install any App through link shared via E Mail or SMS Link.
- Don't Share OTP / PIN / Passwords to Anyone.

QR Code Scams

Don’t scan the QR code to recieve money

Modus Operandi



- ⚠ Fraudsters often contact customers under various pretexts and trick them into scanning Quick Response (QR) codes using the apps on the customer's phone.
- ⚠ By scanning such QR codes, customers may unknowingly authorize the payment to fraudsters account.

Precautions

- 👍 Be cautious while scanning QR codes using any payment app. QR codes have account details embedded in them to transfer money to a particular account, check it before authorizing the payment.
- 👍 Never scan any QR code for receiving money. Transactions involving receipt of money do not require scanning barcodes / QR codes or entering mobile banking PIN (m-PIN), passwords, etc.
- 👍 If you use UPI mobile app, ensure to secure it with a code.
- 👍 Never share your UPI ID or bank account details with people whom you do not know.
- 👍 Never share OTPs with anyone.

Royal Ransomware Attacks

Royal ransomware is the latest ransomware, being used to extort money from its victims by blocking access to their systems' data. It spreads through phishing emails, malicious software downloads, and other forms of social engineering.

Modus Operandi

- ⚠ Fraudster uses callback phishing, a new type of phishing attack. In this, Victim receive a phishing email from fraudster posing as employee of Bank or service provider and alerting them about a Problem like KYC Expiry or non-paid electricity bill etc.
- ⚠ Instead of providing more information about the situation in the email, the threat actor gives his contact number, hoping for a return call from the victim.
- ⚠ Once the victim calls the fraudster, they lure the victim to install remote access software on his desktop/mobile device.
- ⚠ With remote access, on the device, fraudster uninstalls antivirus and installs ransomware on the victim's device.
- ⚠ The ransomware encrypts victim's data files and blocks their access to the device.
- ⚠ The attacker then demands a ransom and promises to share the decryption key upon payment of the ransom to restore their access.
- ⚠ Even on payment of ransom, the customer's data is sold on darknet by the fraudster for additional money.

Precautions

- 👍 Use only licensed Operating Systems and other software & keep them regularly patched.
- 👍 Install good antivirus software on your Laptops / Desktops. Always download files from legitimate website whose URL starts with https://.
- 👍 Keep your browser updated and use legitimate browser extensions downloaded from OEM websites only.
- 👍 Take data backups regularly and keep it offline (not connected with the computer).
- 👍 Never click on attachments or links in emails or SMSes from unknown senders. Keep yourself updated on cyber security threats, especially how to identify phishing emails, etc.

Rogue Mobile Apps

A customer might download a Mobile Banking App thinking it was issued by their bank, but it could be a modified replica of the original App.

Precautions

- 👍 Never click on unauthorised links for apps shared over mail or WhatsApp.
- 👍 Always download Apps from a legitimate App-Store.
- 👍 Check what permissions the app asks for and never give more permissions than it needs. For example a "Weather App should never ask for access to Contact list and Text messages".
- 👍 Before installing, read reviews of the app on App-Store. Avoid apps with multiple five-star reviews but no written comments.
- 👍 Preferably install trusted anti-virus software on your mobile.

SIM Swapping Fraud

A type of cybercrime where fraudsters get duplicate SIM of mobile number issued by deceiving the telecom provider

Modus Operandi

- ⚠ The scammers impersonate as real owners and claim to have lost or damaged their SIM card.
- ⚠ Further, a new SIM card is activated in the fraudster's possession.
- ⚠ Once the new SIM starts functioning, the original one gets blocked.
- ⚠ With the new SIM card, fraudsters get OTP & other confidential details required for financial transaction from your bank account.

Precautions

- 👍 The 20-digit SIM number is a very sensitive data. Keep it confidential.
- 👍 If your mobile number gets inactive/out of range for a few hours, enquire from your mobile operator immediately.
- 👍 Register for regular SMS as well as e-mail alerts for your banking transactions this way, even if your SIM is deactivated, you shall continue to receive the alerts via your email.

Screen Sharing App / Remote Access Fraud

Modus Operandi

- ⚠ Fraudsters trick the customer to download a screen sharing app.
- ⚠ Using such app, the fraudsters can watch/ control the customer's mobile/ laptop and gain access to the financial credentials of the customer.
- ⚠ Fraudsters use this information to carry out unauthorized transfer of funds or make payments using the customer's Internet banking/ payment apps.

Precautions

- 👍 If your device faces any technical glitch and you need to download any screen sharing app, deactivate/log out of all payment related apps from your device.
- 👍 Download such apps only when you are advised through the official Toll-free number of the company as appearing in its official website. Do not download such apps in case an executive of the company contacts you through his/her personal contact number.
- 👍 As soon as the work is completed, ensure that the screen sharing app is removed from your device.

Tailgating

Sometimes referred to as piggybacking, is a social engineering technique in which an unauthorized person follows an authorized individual to enter secured premises.

Modus Operandi

- ⚠ Stealing of valuable equipment such as unattended laptops.
- ⚠ Exfiltration of sensitive data.
- ⚠ Installation of malware / ransomware on specific unattended computers or installation of hidden cameras.
- ⚠ Get access to the server room and create a backdoor to the entire enterprise network.
- ⚠ May result in physical violence or vandalism.

Precautions

- 👍 Stay vigilant and cautious of unknown persons in premises.
- 👍 Create a culture of awareness amongst ourselves.

UPI Fraud: Request Money

Scanning to receive?
You can end up paying a high price.

Modus Operandi

⚠ Use UPI app's "request money" feature.

⚠ Persuade you to enter your UPI PIN.

⚠ Your money ends up in the scammer's account.

Precautions

- To avoid Request money scam, always remember followings points:
  - While receiving money, UPI PIN is not required.
  - Your UPI PIN is only required when you make the payment.
- Never pay advance money without verifying the identity of the person.
- On platforms like OLX, Quikr, and others:
  - do not pay a vendor in advance.
  - Always pay for your purchases when they are delivered to you.

Vishing Calls

A cyber security attack where scammers use voice calls to gain sensitive information.

Modus Operandi

- ⚠ Imposters call or approach the customers through telephone call/social media posing as bankers/company executives/insurance agents/government officials, etc. To gain confidence, imposters share a few customer details such as the customer's name or date of birth.
- ⚠ In some cases, imposters pressurize/trick customers into sharing confidential details such as passwords/OTP/PIN/Card Verification Value (CVV) etc., by citing an urgency/emergency such as, need to block an unauthorised transaction, payment required to stop some penalty, an attractive discount, etc. These credentials are then used to defraud the customers.

Precautions

- 👍 Bank officials/financial institutions/RBI/any genuine entity never ask customers to share confidential information such as username/password/card details/CVV/OTP.
- 👍 Never share these confidential details with anyone, even your own family members, and friends.

Actions to Be Taken After Cyber Fraud

Actions to be taken after occurrence of a fraud

- Block not only the debit card/credit card but also freeze the debit in the bank account linked to the card by visiting your branch or calling the official customer care number available on the bank's website. Also, check and ensure the safety of other banking channels such as Net banking, Mobile banking etc., to prevent perpetuation of the fraud once the debit/ credit cards, etc., are blocked following a fraud.
- Reset Mobile: Use (Setting-Reset-Factory Data) to reset mobile if a fraud has occurred due to a data leak from mobile.
- **Report cyber fraud under Grievance section of our website and also on Govt. of India portal: www.cybercrime.gov.in OR CALL: 1930 For more information, visit our website: https://bankofindia.co.in/safe-banking**
- **For more details, please visit our social media channels**
  - **https://www.facebook.com/BankofIndia**
  - **https://instagram.com/bankofindiaofficial**
  - **https://www.linkedin.com/company/bankofindiaofficial**
  - **https://youtube.com/@BankofIndia_IND**
  - **https://twitter.com/BankofIndia_IN**
  - **https://www.kooapp.com/profile/bankofindiaofficial**

Conclusion

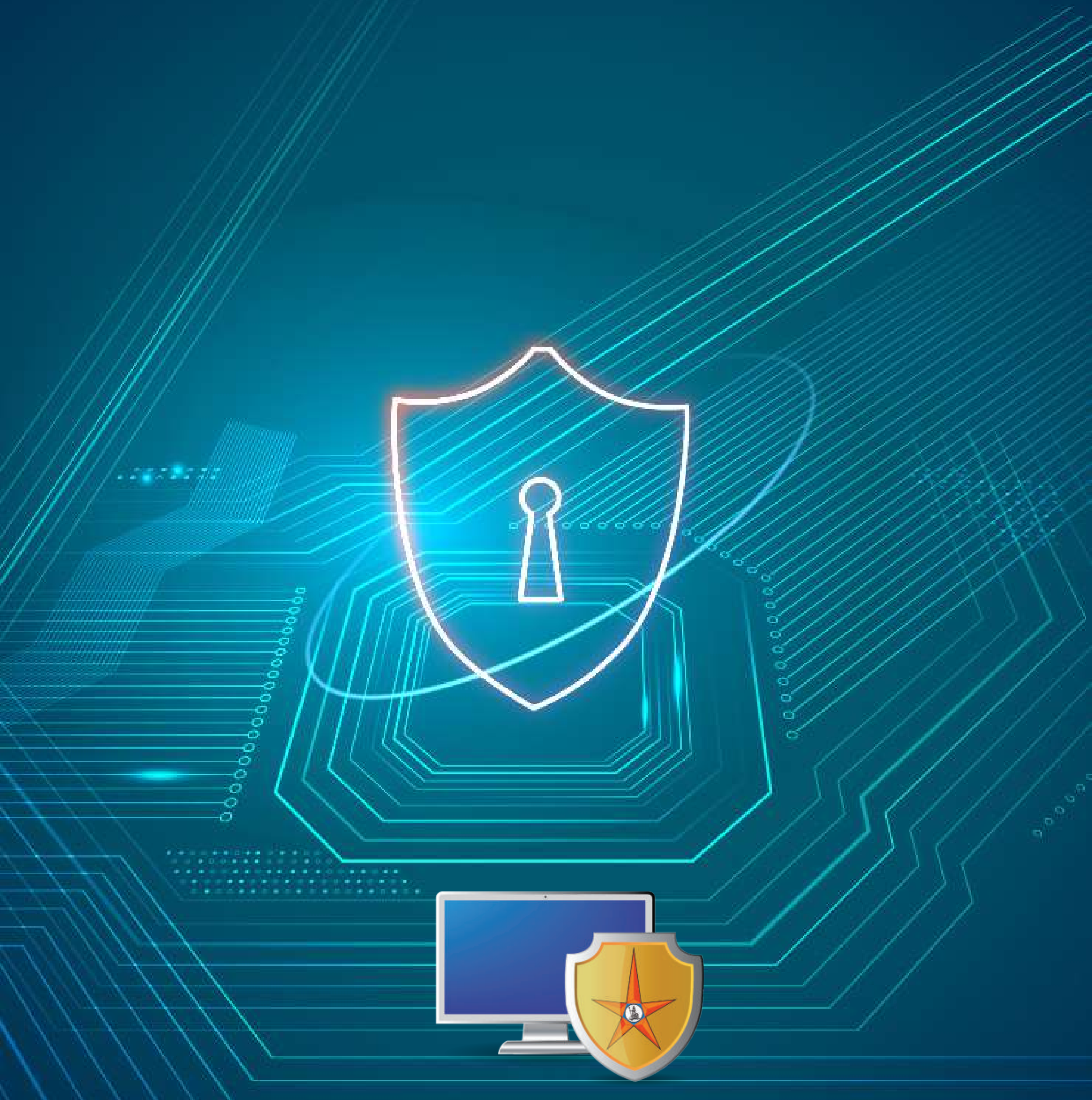
This book has delved into the world of cyber security covering a wide range of prevalent cyber frauds and recommended precautions to stay safe. Never be the weakest link in the cyber security chain. As technology advances, the challenges and complexities of securing digital assets will only intensify. We hope this book equips you with the necessary information to stay alert and be cyber smart.

Let's Pledge to build a Cyber Secure World by following the best practices at workplace and in personal lives.

Stay Vigilant! Stay Safe! Prevent Fraud!

Regards,

Team - Information Security



**Information Security Cell, Risk Management Department,
Head Office, Bank of India.**

C-5, G Block , Bandra Kurla Complex, Bandra East,
Mumbai, Maharashtra - 400 051.