BOI

CYBER STAR

SECURE OUR WORLD

E-MANUAL ON CYBER SECURITY AWARENESS

Index

Preface

In today's digital age, cyber security is more crucial than ever. As technology evolves, so do the threats that target individuals and organizations alike. This Manual serves as a comprehensive guide to enhancing your understanding of cyber awareness and best practices.

Our goal is to empower you with knowledge about common cyber threats and how to protect yourself and your information. Whether you are an individual user or part of a larger organization, the principles outlined here are vital for fostering a culture of cyber security.

This e-manual serves as a comprehensive guide to various Cyber Frauds, their Modus Operandi and Precautions to be taken, navigating the complexities of implementing cyber security measures and Cyber Smart Tips. It aims to demystify concepts, provide practical strategies, and empower readers to protect their digital lives.

By prioritizing awareness and vigilance, we can collectively create a safer online environment. We encourage you to engage with the content, share insights, and implement the strategies discussed within these pages. Together, we can navigate the digital landscape securely and confidently.

Stay safe, stay informed.

Remember! Cyber Security begins with US!

STAY VIGILANT! STAY CYBER SAFE!

MD & CEO's Message

Secure Our World

As we advance in a rapidly digitizing world, the importance of cybersecurity cannot be overstated. Cyber threats have evolved significantly, posing serious risks to businesses, governments, and individuals alike. At the heart of our digital transformation efforts lies the protection of our data, systems, and networks, ensuring the continuity and security of operations.

Our Bank is committed to maintaining the highest standards of cybersecurity. However, we must recognize that security is a shared responsibility. Each one of us plays a crucial role in safeguarding our digital environment. By being vigilant, informed, and proactive, we can collectively reduce vulnerabilities and strengthen our defense against cyber threats.

This cybersecurity awareness booklet is designed to equip you with the knowledge and tools necessary to identify, prevent, and respond to potential cyber risks. Whether it is understanding the phishing attempts, creating strong passwords, or recognizing suspicious activity, the information contained here will help you become a frontline defender of our organization's digital assets.

I encourage you to review the materials carefully and integrate these best practices into your daily operations. By fostering a culture of cybersecurity awareness, we can protect not only our Bank but also the wider community we serve.

My Best Wishes to all.

(Rajneesh Karnatak)
MD & CEO

ED's Message

Cyber Security Begins with US

Cyber Security Awareness Month 2024 runs through October with the theme "Secure Our World." It's a call to action - protect over selves, and our Bank from online dangers with simple but effective steps.

Cyber Security is transforming. The last decade of cyber-attacks, threat actors, and an endless stream of breached data was just a catnap compared to what's coming next.

Sophisticated cyber actors are developing capabilities to disrupt, destroy, or threat to individuals and to organisations. Defending against these attacks is essential to maintaining Bank's security. Preventing attacks or mitigating the spread of an attack as quickly as possible, can prevent reputational and financial losses. Any cyber-attack, no matter how small, is a threat to our cyber security and must be identified, managed, and mitigated immediately.

Awareness amongst staff members and other stakeholders is of utmost importance and necessary for ensuring cyber security of the Bank. As Bank's IT systems are now declared as "Protected Systems" by NCIIPC, Govt. of India, it is utmost important that all our IT systems are hardened before putting to use and patched in line with OEM recommendations and Bank's policy guidelines.

This e-manual is the 2nd edition of our series "BOI Cyber Star". This booklet depicts Top 10 most prevalent types of cyber frauds with brief description and best practices to avoid them. Also selected cyber awareness related articles, poems and cartoons from Bank's staff members are also included to the manual for benefit of all. You will also find the reporting mechanism in case of cyber frauds.

I implore you all to take cyber security seriously and implement all possible security measures to safeguard Bank's valuable assets and increase the cyber resilience of the Bank.

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

(P. R. Rajagopal)
Executive Director

CISO's Message

It's Easy to Stay Safe Online

In today's increasingly interconnected and fast-paced world, cybersecurity has become one of the most critical challenges we face. Cyber-attacks are becoming more frequent, more sophisticated, and more disruptive, affecting businesses and individuals alike. From ransomware and phishing schemes to data breaches and insider threats, no organization or individual is immune.

While our security systems and IT teams work round the clock to defend our infrastructure, technology alone is not enough. Cybersecurity is a shared responsibility—one that involves each and every one of us. Every time you log in to the network, handle customer data, communicate with colleagues, or use online resources, you are a crucial part of our defense against cyber threats. It's essential that we all remain vigilant and proactive in recognizing potential risks and following best practices for security.

This Cyber Awareness booklet has been designed with you in mind. It's not just a set of policies and procedures, it's a practical guide that empowers you with the knowledge and skills needed to protect both our Bank and you.

Cybersecurity is a journey, not a destination. Threats will continue to evolve, and so must we. At Bank of India, we are committed to providing you with the training, tools, and resources you need to stay ahead of these challenges. I encourage you to actively engage in our ongoing cybersecurity programs, participate in training sessions, and always keep an eye out for new and emerging threats. By working together, we can create a security-first culture where cybersecurity becomes second nature in everything we do.

In closing, I want to personally thank each one of you for your dedication to maintaining the safety and security of our Bank. Your role in protecting our assets, our people, and our reputation cannot be overstated. Together, we can keep Bank of India secure, resilient, and ready to thrive in today's digital landscape.

(Kuldeep Pal)
CISO

Cyber Security Pledge

In the recent past, cybercrimes have increased many fold. Corporate employees are being targeted by hackers to get into corporate networks to perpetrate cyber-attacks. It is widely acknowledged that a human being is the weakest link in cyber security. Therefore, it is duty of each and every Employee and Stakeholder of Bank of India, to dedicate ourselves and pledge to safeguard Bank's digital assets.

I commit and take this pledge to uphold that I will remain committed towards following Cyber Security practices to ensure protection of corporate information, systems and networks:

I will handle and store corporate data with utmost care and ensure its confidentiality, integrity, and availability.

I will create strong, unique passwords for each account and will regularly update them. Also, I will maintain secrecy of these passwords.

I will only visit trusted websites and download software from official, verified sources.

I will keep my devices and software up to date with security patches and updates.

I will remain vigilant against suspicious emails, messages and links.

I will verify the authenticity of unexpected communications before taking any action.

I will report any suspected security incident or breach promptly to senior designated official of department and to the Head Office SOC team.

I will actively participate in all security trainings and exercises to stay updated and improve my cyber security awareness.

I will continuously educate my colleagues, customers, vendors on cybersecurity best practices and remain vigilant against emerging threats.

By adhering to these guidelines, I pledge to take an active role in maintaining a safer and more secure digital world.

Cyber Smart Tips

1. Think before you click. Fight the phish. Don't get phished.
2. Review your bank statements and transaction history regularly to spot any unauthorized transactions.
3. Protect your device with a strong PIN/Password or Biometrics and enable auto lock setting in mobile phones/ Laptops/ other devices.
4. Keep your system and Antivirus up-to-date with regular patches. Use authorized and licensed software only.
5. Don't share any sensitive information with any unauthorized or unknown person over telephone or through any other medium.
6. Don't use the same password in multiple services/websites/apps.
7. Regularly clear browser history/cookies/cached memory after confidential activities/transactions.
8. Download Apps from official app stores. Before downloading an App, check the popularity of the app and read the user reviews. Observe caution before downloading any app, which has a bad reputation or less user base, etc.
9. Keep the GPS, bluetooth, NFC and other sensors disabled on your computers and mobile phones, when not required.
10. Don't share system passwords or printer passcode or Wi-Fi passwords with any unauthorized person.
11. Scan USB device with Antivirus/Endpoint Protection before its use. Disable USB devices if not needed.
12. Be wary of fake advertisements/sponsored contents on search results or websites.
13. Be cautious of public Wi-Fi. Information shared over public network may be misused. Do not use any public computer or Wi-Fi for carrying out financial transactions or do online shopping.
14. Be cautious before revealing your location over internet. Be Vigilant, Not a Victim.
15. Always use Multi Factor Authentication for social media accounts.
16. Immediately, change password which might have been shared or compromised.

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.

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**

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.

UPI Request Money Fraud

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.
- If you receive a fake money request, refuse it and report it as fraud attempt on Govt. portal given below.
- 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.

Job Offer Scams

Job Offers that ask for money, can be a SCAM!

MODUS OPERANDI:

- Fraudsters use text messages to entice victims with part-time jobs.
- 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, leading to 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 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.

Ransomware Threats

Defend Your Data, Shed Light on Ransomware Threats

MODUS OPERANDI:

- Threat actors send emails with malicious links or attachments disguised as legitimate files (e.g., PDFs, Office documents). They also use malicious advertisements on legitimate websites which redirect victims to websites hosting ransomware.
- Once executed on a system, ransomware starts encrypting files using strong encryption algorithms. Encrypted files become inaccessible to the victim, who receives a ransom note demanding payment in cryptocurrency (e.g., Bitcoin) to decrypt files.
- Fraudsters further instruct to pay the ransom and often threaten to delete files or sell it on dark-web.
- Paying the ransom does not guarantee file recovery or removal of malware, and this encourage further attacks.

PRECAUTIONS:

- Ensure regular back up of important files to an external hard drives, tapes, or cloud storage service.
- Regularly update operating system, antivirus software, and applications from legitimate OEM websites to protect against vulnerabilities.
- Avoid opening attachments or clicking on links in emails from unknown or dubious senders.
- Install licensed and effective antivirus software and keep it up to date to detect and block ransomware and other malware threats.
- Learn to recognize phishing attempts, where attackers attempt to trick you for revealing sensitive information or installing malware.
- Install software and files from trusted sources only. Verify the authenticity of websites before downloading anything.

QR Code Scams

Don’t Scan the QR code to receive 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 code/s 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.

Investment Scams

Crypto Dreams, Scam Schemes:
Guard your Portfolio from Digital Extremes

MODUS OPERANDI:

- Fraudsters lure people by promising for quick and high returns.
- They persuade you to invest money in such schemes, which actually are Investment scheme scams.
- They offer money against simple jobs i.e. like the YouTube videos shared via links to earn money.
- Fraudster gives you high profits in first few days to gain your trust and adds you in a fake Whatsapp/Telegram group. showcasing false profits made by others.
- Then they slowly pressurize you to invest more money.
- As you sufficiently invest more money, fraudster asks extra fees from you to withdraw your profit.
- They disappear in between, leaving you with no money.

PRECAUTIONS:

- Do Your Research: Before investing in any scheme, check thoroughly about the company and person offering the opportunity. Look for any warnings from regulators on that company, application, personnel etc.
- Verify Credentials: Make sure that the person/company is having license and duly registered.
- Avoid Hasty Decisions: Don't rush into making decision and invest money. Legitimate investment schemes will provide you sufficient time to think and consult.

AePS Frauds

Guard Your Biometrics: Outsmart AePS Fraud Tactics

MODUS OPERANDI:

- Cybercriminals use Aadhaar numbers and other information obtained from various sources such as scanned copies and digital records.
- By using dummy fingers (silicone fingers) that contain impressions of your fingerprints and unauthorized biometric devices, they gain access to your bank accounts.
- Once successfully authenticated, they transfer money from the bank account using the dummy fingers and immediately withdraw the money.

PRECAUTIONS:

- Regularly check your bank statement.
- Be careful while sharing Aadhaar details.
- Always try to use a masked Aadhaar/ DigiLocker instead of an Aadhaar card.
- Lock Aadhaar and biometrics via the m-Aadhaar application or https://uidai.gov.in/ and unlock them as and when required.
- Register your AePS fraud complaint on https://www.npci.org.in/register-a-complaint

Digital House Arrest

Unlocking Digital Vigilance with Digital House Arrest Awareness!

MODUS OPERANDI:

- Fraudsters set up a fake police station with actors posing as officers. They create a convincing background to appear legitimate during video calls.
- Victims receive video calls from these officers who present fabricated charges with arrest warrants.
- To avoid digital arrest or legal action, the victims are coerced into transferring money to the fraudsters accounts.

PRECAUTIONS:

- Always verify the identity of the caller independently. Contact the relevant law enforcement agency directly using official contact details.
- Never provide personal or financial information over the phone or video call unless you are certain of the caller's identity.
- If you suspect a scam, report it to local cyber police authorities immediately.
- Report fraudulent communication on Chakshu Portal https://sancharsaathi.gov.in/sfc/

Deep fake AI-powered Vishing Attacks

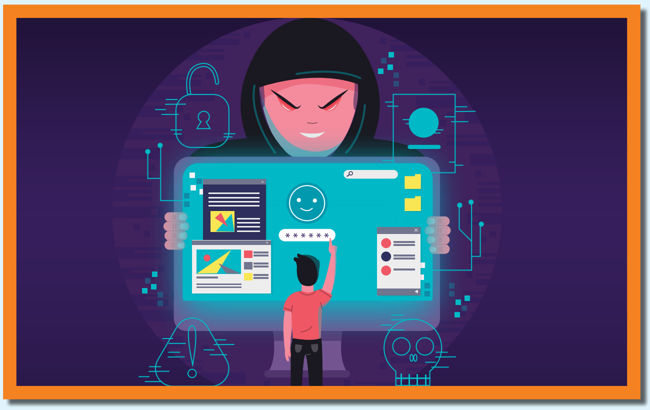
Attackers impersonate familiar voices to trick you into revealing personal information or sending money to them.

MODUS OPERANDI:

- Fraudster pretend to be from government agencies, banks, or even your known persons by using Deepfake Al to mimic their voice.
- They create urgency and pressure, to manipulate you to take quick decisions.
- They often sight emergencies, legal issues, financial problems, or reputational harm, urging you to act fast without thinking clearly.

PRECAUTIONS:

- Never share personal information or transfer money hastily without verifying caller identity through official channels like helpdesk numbers on official websites etc.
- Be wary of urgency tactics, take your time to verify the situation before making a decision. Discuss with your well-wishers / other persons having exposure to referenced agencies.
- Be cautious with unknown calls and messages. Don't click on suspicious links or attachments received on Emails and SMSs.



Need to improve Cyber Security

As the world is moving ahead in the field of digitization, the threat of cyber-attacks is also increasing and India is not immune to it.One of the primary reasons why cyber security is essential is the increasing dependence on technology in various aspects of our lives.

As the use of internet is increasing, a new face of crime is spreading rapidly from in-person crime to nameless and faceless crimes involving computers. The internet brings joy to our lives but at the same time it has some negative sides too. The Cyber-crimes today are on rise and the latest & perhaps the most complicated problem in the cyber world. It is observed that the internet world is ever-evolving and fraudsters continuously use newer ways to commit frauds.

A successful Cyber-attack can result in significant damage to a company's reputation, financial loss and disruption of services. Therefore, businesses need robust cyber security measures to ensure the security of their assets and the smooth functioning of their operations. This means that our sensitive personal and financial information is constantly at risk. Without adequate security, hackers can easily exploit this information, resulting in serious consequences such as identity theft and financial loss.

There is a need to further improve cyber security by Coordination enhancement, Development of infrastructure, creating digital literacy,Responsibility on service providers & Amendment to the Information Technology Act. Stronger training of law enforcement agencies is the need of the hour.The security of the banking community requires everyone's participation and starts with each individual organization's own security. The banking industry, in particular, should continuously increase the strength and diversity of its defences and ensure it understands the nature of the changing threat.

Most of the time governments face difficulties due to inadequate infrastructure, lack of awareness and insufficient funds. It is important for government agencies to provide reliable services to society, maintain healthy citizen-to-government communication and protect confidential information. Individuals or organizations should not only depend on the government for their data security but should also be aware of themselves.

Vinod Chandrashekhar Dixit
Senior Manager
Planning & Publicity
FGMO – Ahmedabad

A brief note on Cyber Security

Cyber security refers to the practice of protecting computer systems, networks, programs, and data from digital attacks, damage, theft, or unauthorized access. It encompasses a range of measures and practices designed to safeguard information technology assets and ensure the confidentiality, integrity, and availability of data.

◎ Key elements of cyber security include:

Protection: Implementing security measures to prevent unauthorized access to systems and data.

Detection: Monitoring systems for security breaches or suspicious activities to identify and respond to threats in a timely manner.

Response: Developing and implementing protocols to address security incidents and mitigate their impact.

Recovery: Planning and procedures for restoring systems and data in the event of a security breach or cyber-attack.

◎ Common cyber security measures include:

Firewalls: Network security systems that monitor and control incoming and outgoing network traffic.

Antivirus Software: Programs that detect and remove malware, viruses, and other malicious software.

Encryption: Protecting sensitive data by encoding it in a way that only authorized users can access.

Multi-factor Authentication (MFA): Requiring multiple forms of verification to access systems, adding an extra layer of security.

Security Patches: Regularly updating software and systems to address known vulnerabilities and protect against cyber threats

Security Awareness Training: Educating users about cyber security best practices and potential threats to increase awareness and reduce risks.

◎ Emerging Technologies in Cyber security:

Artificial Intelligence (AI) and Machine Learning: Used for threat detection, anomaly detection, and predictive analytics in cyber security.

Block Chain: Provides a decentralized and secure way to store and verify data, often used for securing transactions and sensitive information.

Internet of Things (IoT) Security: Focuses on securing connected devices and networks to prevent cyber-attacks targeting IoT ecosystems.

As cyber threats continue to evolve and increase in sophistication, cyber security measures play a crucial role in safeguarding organizations, individuals, and critical infrastructure from cyber-attacks and data breaches.

Amit Kumar
Chief Manager,
MDI, Belapur

Cyber Security Awareness: Keeping the Digital Fort Safe

Imagine a bank as a big, magical castle filled with gold coins and treasures. Just like any castle, it needs to be protected from sneaky thieves trying to break in. In the digital world, these thieves are called hackers, and they're always looking for ways to sneak past the castle walls. That's why banks need to be super smart and use cyber security - like knights in shining armour - to keep everyone's treasure safe.

◎ Strong Passwords: The Castle's Secret Code

Think of your bank password as a secret code that only you know. It's like a special key to the castle that only works for you. If it's too easy, like "1234" or "password," it's like leaving the castle gate wide open! In 2016, a hacker group called "Lizard Squad" easily broke into thousands of accounts because people were using simple passwords. Banks make sure their employees and customers use strong passwords with a mix of letters, numbers, and symbols to keep the gate tightly shut.

◎ Two Locks are better than One: Multi-Factor Authentication

Let's say there's a big, heavy door to the treasure room. Just having one lock isn't enough, right? What if you need a key AND a magic word to open it? That's what banks do with multi-factor authentication. Even if a sneaky thief figures out your password, they still can't get in without the second key - like a code sent to your phone. For example, in 2019, hackers tried to break into Reddit accounts, but those with multi-factor authentication were safe because the hackers didn't have the second key!

◎ Spotting the Tricky Trolls: Phishing Scams

Hackers often pretend to be someone else to trick you, like trolls hiding under a bridge. They might send fake emails that look like they're from your bank, asking for your secret code or other information. In 2020, many people received fake emails that looked like they were from Netflix, tricking them into giving away their passwords. But banks train their employees and customers to spot these tricky trolls by looking for signs like strange email addresses or urgent messages that just don't seem right.

◎ The Castle's Defenders: Regular Security Checks

Just like a castle needs regular patrols to keep watch for invaders, banks do regular security checks to find and fix any weak spots in their defences. For this, banks should conduct frequent security tests to make sure their digital fort is as strong as possible and train their employees to stay alert and know what to do if a hacker tries to break in.

- **Teaching the Citizens: Customer Education**

  Finally, banks also help their customers - like you and me - learn how to keep our own gold coins safe. They might send out friendly reminders about using strong passwords, avoiding those tricky trolls, and always keeping an eye out for anything suspicious. For instance, banks can offer online tutorials and alerts to help customers protect their accounts.

  In the end, cyber security is like a team of brave knights and clever wizards working together to protect the castle. By staying smart and prepared, banks can make sure the digital treasure stays safe and sound!

Akash Singh
Manager,
HO IT

मनी म्यूल

आज के इंटरनेट और डिजिटल तकनीक के युग मे साइबर सुरक्षा बहुत महत्वपूर्ण है।

वर्तमान समय में जैसे जैसे प्रौघोगिकी पर हमारी निर्भरता बढ़ती जा रही है वैसे ही हमारे व्यक्तिगत और व्यवसायिक सभी तरह के वित्तीय लेनदेन अब ऑनलाइन होते जा रहे है और इन्ही कारणों से जाने अनजाने में हमारी जानकारी दूसरो के पास चली जाती है और हम हैकिंग, फिशिंग, मैलवेयर अटैक और ऑनलाइन वित्तीय धोखाधड़ी के शिकार हो जाते है इन्ही में से आज के समय में एक और प्रकार की ऑनलाइन धोखाधड़ी बड़े रूप में सामने आ रही है वो है "मनी म्यूल"।

"मनी म्यूल को यदि साधारण भाषा मे परिभाषित किया जाए तो, किसी और के अकाउंट का उपयोग अपने हित के लिए करना"

मनी म्यूल और मनी म्यूल एकाउंट –

मनी म्युल एक ऐसा व्यक्ति होता है जो अन्य लोगों की धोखाधड़ी या अपराधिक गतिविधियों में पैसा ट्रांसफर करने का काम करता है। मनी म्यूल का उपयोग अपराधी नेटवर्क द्वारा किया जाता है ताकि वे अपनी गतिविधियों को छिपा सकें और खुद को कानून से बचा सकें और मनी म्यूल अकाउंट वह है, जिस अकाउंट के माध्यम से यह पैसे बार बार अलग अलग एकाउंट से होते हुए अपराधी के एकाउंट में पहुचता हैं औसतन ऐसे अवैध धन को चौदह बार अलग अलग खाते से ट्रान्सफर किया जाता है। कई बार अपराधी गरीब, बुजुर्ग, अशिक्षित लोगो को पैसे का प्रलोभन देकर, बेरोजगारों को नौकरी का लालच देकर, भ्रामिक ईमेल भेजकर, कस्टमर केयर के नाम पर, ऑनलाइन खाता खोलकर जाने अनजाने में उनके खातों का उपयोग करते हैं।

संसद द्वारा अगस्त 2024 में दी गई जानकारी के अनुसार पिछले 5 वर्षों में वित्तीय धोखाधड़ी में 11 गुणा बढ़ोतरी हुई है। 2019-20 में वित्तीय धोखाधड़ी ₹ 2677 करोड़ थी वही 2023-24 यह राशि बढ़कर ₹ 29,082 करोड़ हो गई इस दौरान ऑनलाइन धोखाधड़ी भी ₹ 129 करोड़ से बढ़कर ₹ 1457 करोड़ तक पहुंच गई है। आरबीआई ऐसे म्यूल अकाउंट और डिजीटल धोखाधड़ी रोकने के लिए ग्रह मंत्रालय के, IC4 (INDIAN CYBER CRIME COORDINATION CENTRE) और अन्य जांच एजेंसी के साथ मिलकर काम कर रहे है।

मनी म्यूल यह एक दंडनीय अपराध है इससे बचने के लिए हमे किसी भी प्रलोभन में ना आकर, जागरुक रहकर ही बचा जा सकता है। अपने खातों में यदि बिना आपकी जानकारी से किसी भी तरह की राशि आती है तो इसकी जानकारी तुरंत अपने बैंक शाखा अधिकारी को लिखित में देना चाहिए, ताकि ऐसी अप्रिय घटनाओ से बचा जा सके।

Amit G Bharti
CSA,
Nagpur

Securing Women in the Digital Age: Effective Cyber Security Strategies

In today's interconnected world, the internet is a double-edged sword for women. On one hand, it offers unprecedented opportunities for education, communication and empowerment. On the other hand, it exposes them to a range of cyber threats, from harassment and stalking to identify theft and non- consensual distribution of private content. The rise in digital crimes necessitates robust cyber security measures tailored to protect women in the online space.

Cyber Harassment: Women are disproportionately targeted by cyberbullying and harassment on social media platforms.

Cyberstalking: This involves persistent, unwanted monitoring or contact by an individual using electronic communication tools.

Doxing: The practice of publishing private information about an individual without their consent, often with malicious intent, has targeted numerous women activities and journalists.

Strategies for Enhancing Women's Cyber Security

◎ **Strengthening Data Privacy and Security Protocols**

In 2020, the Indian Government launched the Cyber Crime Reporting Portal, a platform for women to report cybercrimes such as stalking and harassment. This initiative also emphasizes the importance of personal data protection, offering tools and resources for securing personal information online.

◎ **Advanced Social Media Controls and Reporting Mechanisms**

Twitter and Instagram have both implemented stricter policies against harassment. Twitter for instance introduced features allowing users to filter notifications and limit who can reply to their tweets, which helps women control their online interactions.

◎ **Education and Awareness Programs**

The Cyber Savvy Campaign provides resources and workshops focused on educating women and girls about safe online practices. These programs cover topics like recognizing phishing scams, creating strong passwords, and understanding privacy settings.

Ensuring women's safety in the digital age requires a multi- faceted approach that combines robust cyber security measures, legal frameworks, education and support systems. By continuing to innovate and collaborate, we can build a safer online environment where women can thrive without fear of cyber threats.

Nidhi Mishra
Officer,
HO IT

Protecting Children: The Role of Cyber Security in preventing Sexual Abuse

With the increasing use of the Internet and digital platforms, predators have found new avenues to exploit children. To combat this, cybersecurity measures have become crucial in preventing and stopping child sexual abuse. These measures not only protect children online but also help law enforcement track down and apprehend offenders. Here's how cybersecurity plays a vital role in this critical issue:

◎ Monitoring and Filtering Online Content

The Internet is vast, with countless websites, social media platforms, and messaging apps where harmful content can circulate. Advanced monitoring and filtering technologies can help identify and block illegal content, including child pornography.

◎ Enhancing Parental Controls

Parental control tools are essential in shielding children from harmful content and online predators. These tools allow parents to monitor their child's online activity, set usage limits, and block access to certain websites or apps. With advancements in cybersecurity, these tools have become more sophisticated, enabling real-time alerts if a child attempts to access restricted content or if unusual online behaviour is detected.

◎ Implementing Strong Authentication and Privacy Measures

Children often use devices that are shared within a family, making it crucial to have strong authentication protocols to protect sensitive data. Implementing multi-factor authentication (MFA) and encouraging the use of complex, unique passwords can prevent unauthorized access to accounts that could be used to exploit children.

◎ Blocking Access to Illegal Websites and Dark Web Content

Many offenders use the dark web to share illegal content and communicate with other predators. Cybersecurity measures, such as blocking access to known illegal websites and disrupting dark web activities, are crucial in curbing the distribution of child sexual abuse material. Governments and tech companies are increasingly focusing on dismantling these hidden networks by using advanced cybersecurity techniques.

Cyber security is a powerful tool in the fight against child sexual abuse. By combining technology, education, and collaboration, we can create a safer online environment for children. It's a collective responsibility - tech companies, governments, parents, and communities must all play their part in protecting the most vulnerable members of society from this heinous crime. With continued advancements in cybersecurity, we can hope to significantly reduce the incidence of child sexual abuse and bring offenders to justice.

Anand Kumar
IT Officer,
HO IT 1

Blockchain: The Next Frontier in Cybersecurity

In the fast-changing digital landscape, cybersecurity is a top priority for banks and financial institutions. Traditional data security methods are increasingly under threat from sophisticated cyberattacks. Consequently, there is a growing demand for innovative solutions that offer strong protection against these evolving risks. Blockchain technology, originally known for its role in powering cryptocurrencies like Bitcoin, is now emerging as a promising frontier in enhancing cybersecurity for the banking sector.

Blockchain is a decentralized and distributed ledger technology that records transactions across multiple computers in a way that ensures security, transparency, and immutability. Unlike centralized systems, where data is stored in a single location, blockchain distributes data across a network of nodes, making it nearly impossible for a single point of failure or attack to compromise the entire system.

How Blockchain Enhances Cybersecurity

1. **Decentralization:** The biggest advantage of Blockchain technology is that the data is stored at various nodes in a decentralized network. This decentralized approach reduces the risk of hacking, as there is no central database that attackers can target.
2. **Immutability:** Once data is added to a blockchain, it cannot be modified or deleted without consensus from the entire network. This immutability ensures that records are tamper-proof, providing an additional layer of security for sensitive information.
3. **Transparency:** Blockchain's transparent nature allows for real-time verification of transactions, making it easier to detect and prevent fraudulent activities.
4. **Smart Contracts:** Smart Contracts are self-executing contracts with the terms of the agreement directly written into code. These contracts can help prevent cyberattacks by automating cybersecurity tasks. They can be used to verify user identities, manage access controls, enforce data encryption standards and restrict access to sensitive data.

Conclusion

As cyber threats increase in value, volume, and complexity, blockchain technology emerges as a powerful and innovative solution for enhancing cybersecurity. With cybercriminals becoming more sophisticated each day, it is essential to harness the decentralized, immutable, and transparent nature of blockchain to safeguard critical data and systems from evolving risks. As we move towards complete digitization of our economy, Blockchain technology is likely to play an important role in realizing this dream.

Nikesh Ramayan Patel
Branch Manager,
Marcela Branch

ऑनलाइन सुरक्षा

उँगलियों के क्लिक पे,

होते हैं करोड़ों के लेनदेन।

पर ज़रा से हमारी लापरवाही,

और साइबर चोर मचा देते तबाही ॥

ऑनलाइन सेवाओं के हैं अपने कई फ़ायदे,

लेकिन इसके इस्तेमाल के भी हैं कई कायदे।

यू0पी0 आई और मोबाइल बैंकिंग ने की ज़िंदगी आसान,

ध्यानपूर्वक इस्तेमाल करें, वरना हो सकता है नुकसान ॥

ये नहीं की छोड़ दे हम अपनाना नई तकनीक,

थोड़ी सी सावधानी से, न होगा अपना विवरण लीक।

ओ0टी0पी और पासवर्ड कभी नहीं करें शेयर,

कार्ड और खाते के भी कभी न करें डीटेल शेयर ॥

सोशल नेटवर्किंग से दुनिया है सिमट गयी,

दूर थे जो हमसे, उनसे अब दूरी भी मिट गयी।

अंजानों से भी हम कर सकते हैं संपर्क,

गोपनीय दस्तावेज़ के लेनदेन में लेकिन रहें सतर्क ॥

साइबर सुरक्षा नियमों का सदैव करें पालन,

ऑनलाइन लेनदेन में भी बरते अनुशासन ।

अगर फिर भी हो जाए कोई साइबर धोखाधड़ी

ऑनलाइन या निकटतम शाखा से करें संपर्क तुरंत ही॥

Mohit Badyal
STC Noida

साइबर सुरक्षा: सुरक्षित भविष्य का आधार

साइबर सुरक्षा: सुरक्षित भविष्य का आधार

रहें सतर्क, हर जगह हर क़दम, साइबर सुरक्षा के सारे ढाल

अपडेट रखें, अपडेट रहें, चले ऑनलाइन, कोई कितना भी चाल

एप्लिकेशन सुरक्षा, डेटा की सुरक्षा का ध्यान,

साइबर अपराध से लड़ने का सही समाधान

हर कोई सीखे, हर कोई चाहे, साइबर सुरक्षा युक्तियाँ

सिस्टम मोनिट्रिंग के साथ, ज़रूरी नीचे पंक्तियाँ

मैलवेयर, फ़िशिंग, रैनसमवेयर या वाइरस

ऑपरेटिंग सिस्टम अपडेट करें, अपडेट रखें एंटीवाइरस

साइबर अपराध, रैनसमवेयर के जाल,

पहचान की चोरी, वित्तीय नुकसान की चाल

सुरक्षित जीवन की राह में, साइबर सुरक्षा का सहयोग,

संवेदनशील जानकारी की रक्षा का है, यही मुख्य योग।

Pranshu Shekher Vats
Officer,
Barasat Branch

Digitalization Era

The Era is of Digitalization,
its all about Tech-transformation.
Fintech playing a vital role,
makes it easy to achieve the goal.

Online shopping is so easy,
its all done in simple clicks!
If its Online payment to be done at the quickest,
Saving of credentials may result in a threat!

Do purchase the lavish Gadgets,
Don't forget to update the Patches!
Password is your Secret key,
Sharing of OTP may become risky!

Don't do Clicks in hustle and Bustle,
email attachment may become a rascal !
Think before you click on link,
As It may be a hacker's trick.

Surfing, gaming all you try,
But never use unsecure Wi-fi !
At Airports, railways or while tracking,
Be aware of Juice jacking.

Don't let virus enter in your PC,
As it may make your data messy !
Either through SMS, call or Email,
Never share your KYC Detail !

Keep the data backup at regular interval,
Or loss of data may put you in trouble,
Stay vigilant of Cyber fraudsters,
Technology is meant for boon not bane.

Neha Mishra
Senior Manager,
ZO IT Kanpur

Clicks of Betrayal

In the land of wires and screens,
Where data flows like endless streams,
Lurk cyber frauds both sly and mean,
Their tricks are more than just a dream.

First comes **Ransomware**, so grim,
Locking files on just a whim.
"Pay the price, or lose it all,"
But don't give in to this cruel call!

Next is **Phishing**, subtle, sly,
"Click this link!" the emails cry.
But behind that tempting bait,
A trap is set—you took the bait!

Identity Theft's a silent thief,
Stealing names, causing grief.
Your life online, it's torn apart,
Leaving scars upon your heart.

A **DDoS** storm begins to brew,
Servers crash, connections skew.
With traffic floods from every side,
Websites crumble, can't abide.

Then comes **IP Spoofing's** trick,
A hacker's mask, it's sly and slick.
They hide behind a false façade,
Disguising their true digital trod

Don't trust links from unknown folks,
They might be Phishing's cruel jokes.
Verify before you click,
Stay secure, and think real quick.

Protect your ID with care,
Shred old docs, stay aware.
Use strong passwords, don't repeat,
Keep your data safe and neat.

Visit **cybercrime.gov.in** today,
Report the crime, don't delay!
With just a few clicks, you'll see,
Justice can be swift and free.

Or if you need a quicker line,
Dial **1930** anytime!
The cyber cops are on your side,
They'll chase the crooks, far and wide.

So remember, in this digital age,
If you fall into a cyber cage,
There's help that's just a call away,
To keep the fraudsters all at bay!

Milind B Gajbhiye
Senior Manager,
ITTC, Pune

In the World of Wires

In the Vast web, where data flows,
A World unseen, but everyone knows.
Invisible paths, where dangers hide,
For every Woman, a need to guide.

A click, a tap, could seem so small,
But within the net, they echo tall.
Guard your presence, your digital face,
In this vast, open, virtual space.

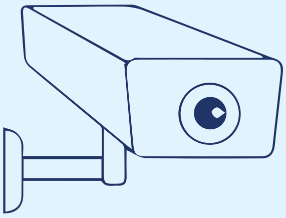
Passwords strong, like shields in hand,
Against the threats that always stand.
Two-steps gates, a fortress strong,
In this fight, you do belong.

Empower yourself, with knowledge bright,
In the darkness, be your own light.
For every woman, near and far,
Cybersecurity is your guiding star.

Nidhi Mishra
Officer,
HO IT

In a world where data flows

In a world where data flows like streams,
And digital life is more than dreams,
We must protect with constant care,
The realms we build in cyberspace air.



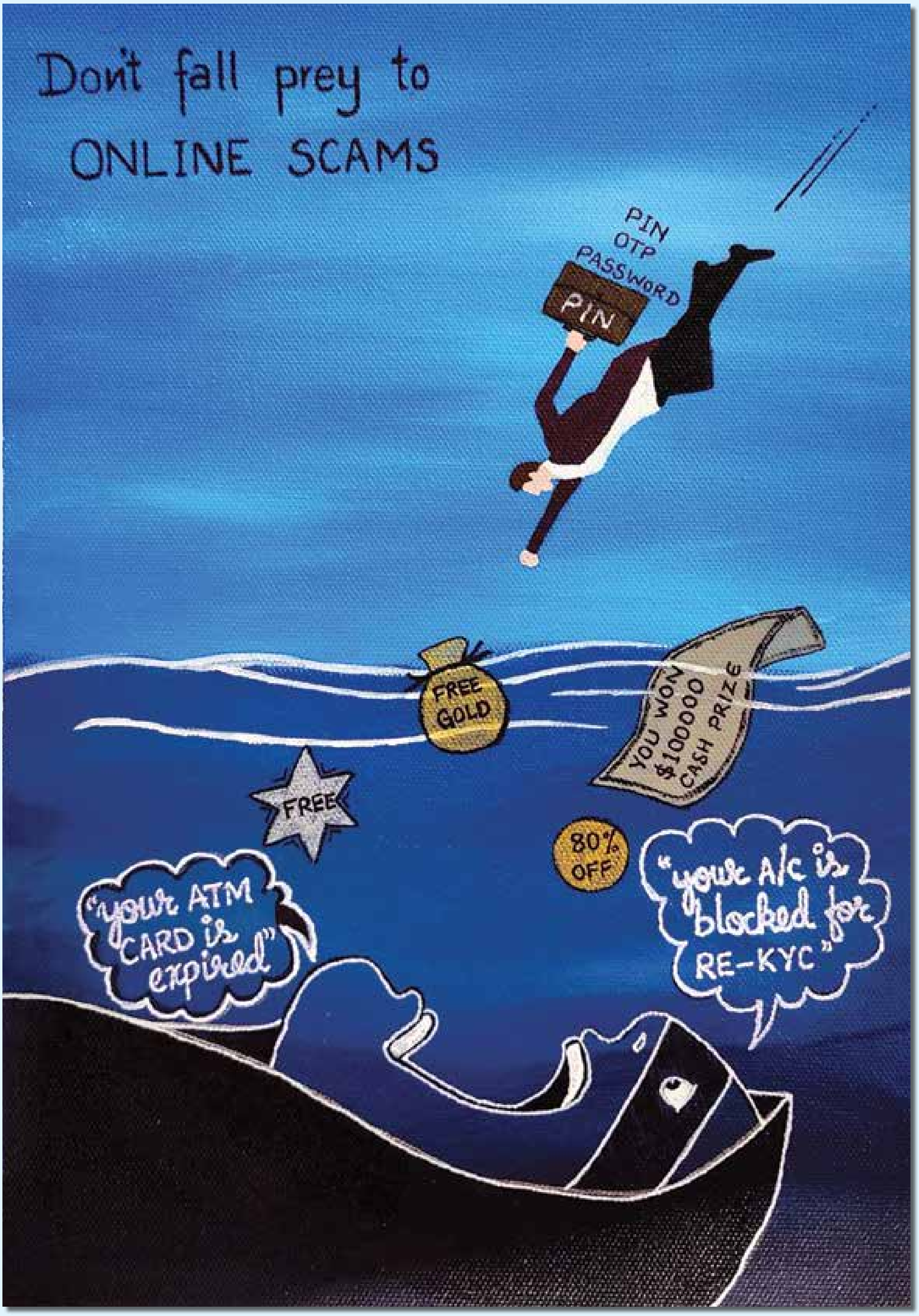
Beware the phishers' cunning bait,
And hackers lurking at the gate.
Passwords strong and secrets tight,
Guard your info day and night.

Update your systems, patch with speed,
For gaps in code are what they need.
Encrypt your files, both near and far,
And know each link before you bar.

Awareness grows with every click,
Each mindful move can do the trick.
In cyber fields where shadows play,
Stay vigilant, and light the way.

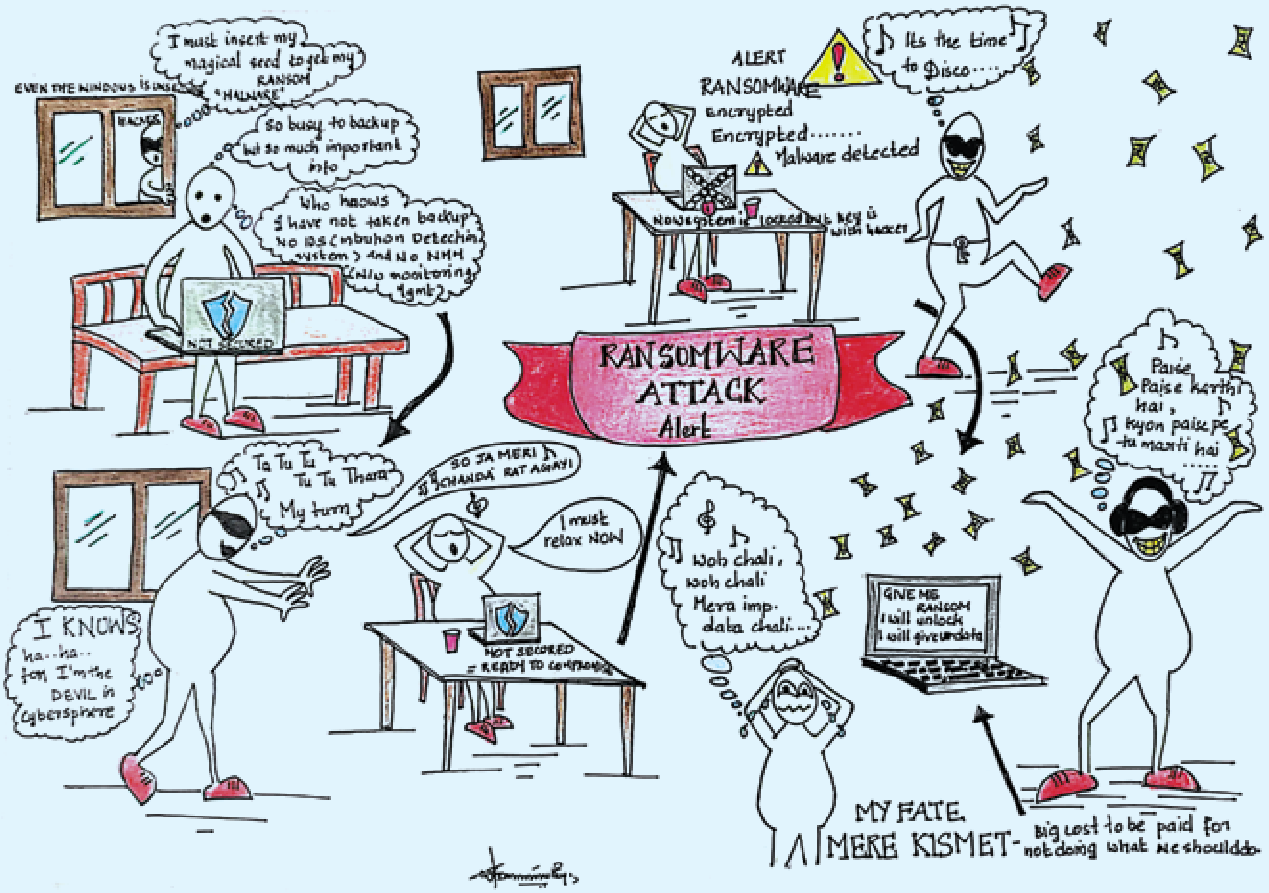
Manish Kumar
Branch Manager,
Ranghola Branch

Be Aware of Online Scams


Don't fall prey to
ONLINE SCAMS
PIN
OTP
PASSWORD
PIN
FREE GOLD
YOU WON $100000 CASH PRIZE
FREE
80% OFF
"your ATM CARD is expired"
"your A/c is blocked for RE-KYC"

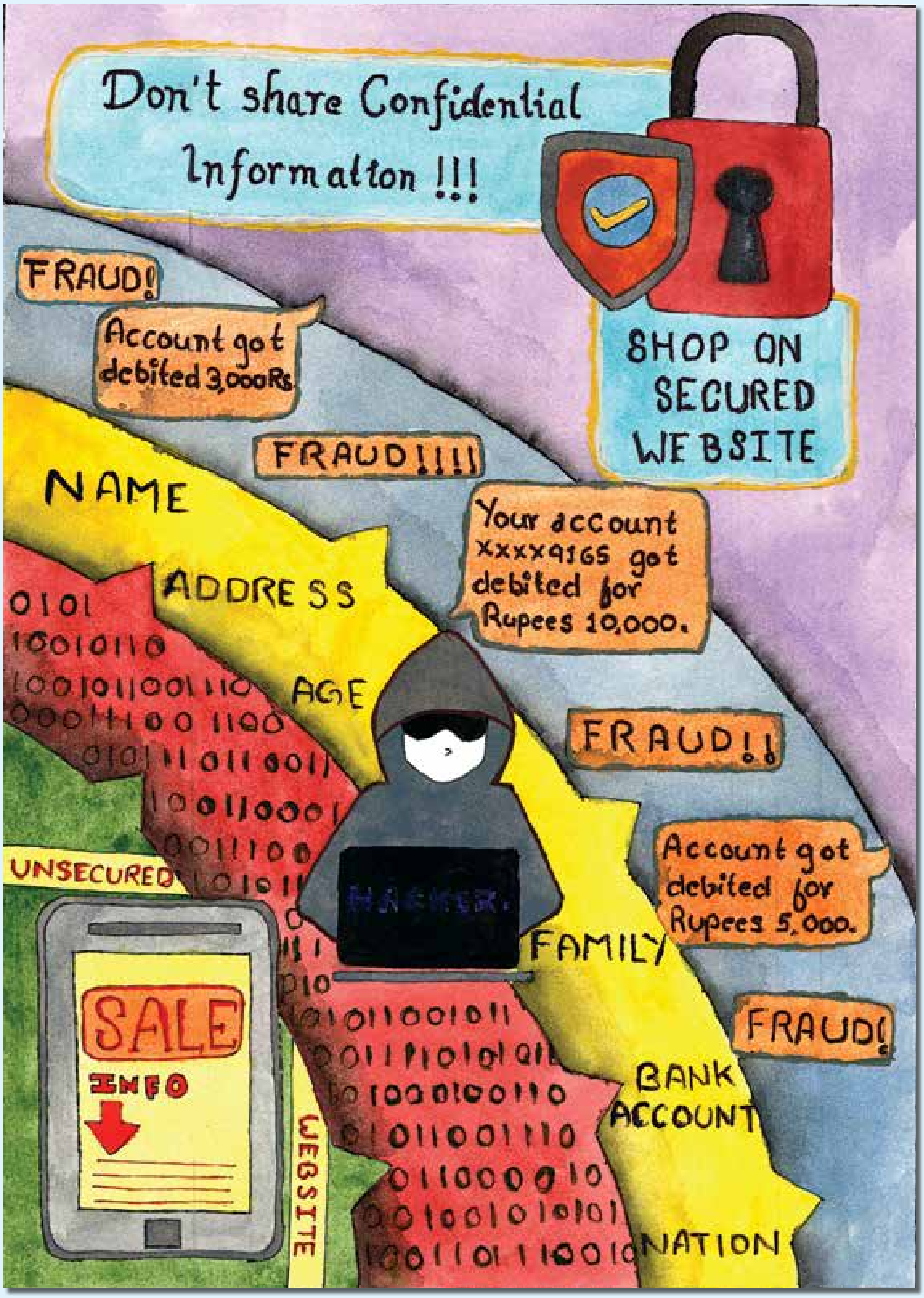
Prajakta Moon
Manager,
Head Office

Ransomware Attack Alert


I must insert my magical seed to get my RANSOM "MALWARE"
EVEN THE WINDOWS IS UNSECURE
HACKER
So busy to backup but so much important info
Who knows I have not taken backup No IDS (Intrusion Detection system) And No NMH (N/w monitoring Sys)
NOT SECURED
ALERT
RANSOMWARE
Encrypted
Encrypted.......
Malware detected
Now system is locked but key is with hacker
Its the time to Disco....
RANSOMWARE ATTACK Alert
Ta Tu Tu Tu Tu Thara My turn
SO JA MERI CHANDA RAT AGAYI
I must relax NOW
NOT SECURED = READY TO COMPROMISE
I KNOWS ha..ha.. for I'm the DEVIL in Cybersphere
Woh chali, woh chali Mera imp. data chali...
GIVE ME RANSOM I will unlock I will give ur data
Paise Paise karthi hai, kyon paise pe tu marti hai ......
MY FATE, MERE KISMET-
Big cost to be paid for not doing what we should do.

Snithya K S
Officer,
Chandranagar Branch, Kerala

Don't Share Confidential Informations!!!


Don't share Confidential Information !!!
FRAUD!
Account got debited 3,000Rs
FRAUD!!!!
SHOP ON SECURED WEBSITE
NAME
Your account xxxx9165 got debited for Rupees 10,000.
ADDRESS
0101
10010110
AGE
FRAUD!!
HACKER.
Account got debited for Rupees 5,000.
UNSECURED
FAMILY
SALE
INFO
WEBSITE
FRAUD!
BANK ACCOUNT
NATION

Archita Singh
Officer Agra, SME Branch

Monster Hacker

MONSTER HACKER
Unsecured Environment
Security Breached
Ensured Protection From Hackers
IF Secured
Respect all cyber space
No to cyber Bullying
Secured wifi
No Personal data sharing
The Secured Environment

Snithya K S
Officer
Chandranagar Branch, Kerala

Accolades & Events

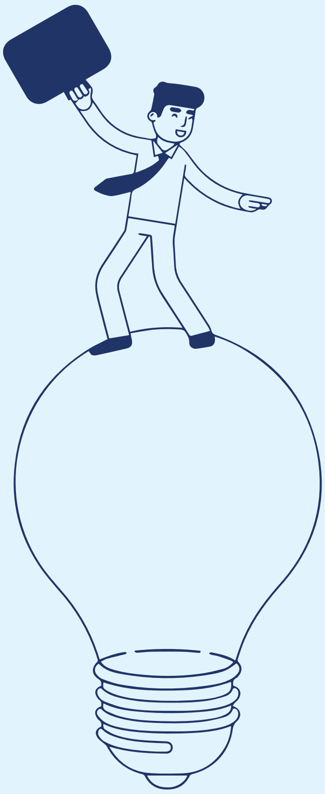
Bank Of India
Management Development Institute
CBD Belapur, Navi Mumbai
TRAIN THE TRAINER WORKSHOP ON CYBER SECURITY & CYBER FRAUDS AWARENESS
Dated 25.08.2023

A one-day Workshop on "Cyber Security and Cyber Frauds Awareness" was organized by the Information Security Cell, Risk Management, Head Office at MDI Belapur, Navi Mumbai on 25th August 2023 (Friday).

Bank of India received the Runner-Up Award in Best IT Risk Management under the Special Mention Category by IBA.

First Cyber Security Awareness E-manual "BOI Cyber Star" was launched on 04th January 2024 by MD & CEO, Shri Rajneesh Karnatak in the presence of Board members.

REMEMBER
Actions to Be Taken After Cyber Fraud



1. Ensure to change your credentials for Net banking, Mobile banking, etc.

2. Block or Hotlist your debit card/credit card which has been compromised.

3. Debit freeze your compromised bank account by visiting your branch.

4. Report cyber fraud on National Cyber Crime Reporting portal: **www.cybercrime.gov.in** or Call: 1930.

5. Report cyber fraud under Grievance section of our website **https://bankofindia.co.in.**

6. Note down necessary details about unauthoised transaction for quick reporting at government Portal. Take help of step-by-step procedure documents available at Bank of India's website under safe banking.

7. For more updates on Cyber Security Awareness, please follow 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

Conclusion

In conclusion, cybersecurity is a dynamic and evolving field that requires constant vigilance and adaptability. As technology advances and threats become more sophisticated, safeguarding digital assets and personal information remains a critical priority for individuals, businesses, and governments alike. By understanding the principles of cybersecurity, implementing robust security measures, and fostering a culture of awareness, we can collectively enhance our defences against the ever-present risks of cyber threats.

In today's digital age, cybersecurity is not just a technical requirement but a fundamental aspect of our daily lives. As we continue to integrate technology into every facet of our existence, the importance of protecting our digital assets cannot be overstated. Cyber threats are constantly evolving, and so must our strategies to combat them.

Ultimate goal of cybersecurity is to create a secure digital environment where we can confidently engage in online activities without fear of compromise. The journey towards secure cyberspace is ongoing, but with informed strategies, proactive measures, simple actions, such as using strong passwords, continuous education, collaboration among individuals, businesses, government and by fostering a culture of awareness and vigilance, we can better protect our digital future and ensure that technology continues to serve as a force for good.

Stay Vigilant! Stay Safe! Prevent Fraud!

Regards,
Team Information Security

BOI

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

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