Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 4 Issue 3 (2024)

An Analysis of Online Monetary Fraud and the Application of Marketing Strategies by Indian Banks to Mitigate Fraudulent Activities: A Literature Review

Dr. Anvesha Sharma
Associate Professor, Times School of Media
Dr. Pritha Chakraborty
Assistant Professor, Times School of Media
Vidhanshu Kumar
Assistant Professor, Times School of Media
anveshaprakash@gmail.com

Abstract

This study examines online monetary fraud and its impact on Indian and international financial institutions. Through a comprehensive literature review and case studies, it analyzes definitions, classifications, and preventive measures related to online fraud from various institutional perspectives. The research investigates the evolution of fraud techniques, compares approaches to prevention between Indian and international institutions, assesses regulatory frameworks, and explores the role of emerging technologies in both perpetrating and preventing fraud. Key findings highlight the increasing prevalence of online fraud due to the expansion of digital transactions, particularly during the COVID-19 pandemic. The study identifies common types of fraud and outlines preventive measures implemented by financial institutions, including two-factor authentication and customer awareness campaigns. It emphasizes the importance of collaboration between stakeholders and the need for continuous adaptation of security measures in response to evolving fraud techniques. The research concludes that online monetary fraud has significant economic implications for both consumers and financial institutions, underscoring the critical need for ongoing efforts to combat this issue.

Keywords: Online Monetary Frauds, Marketing, Advertising, Indian Banks

Introduction

This study focuses on online monetary fraud and its implications for Indian and international financial institutions. The primary research objective is to conduct a comprehensive review and analysis of the definitions, classifications, and preventive measures related to online monetary fraud from the perspectives of various financial institutions. Additionally, this study aims to examine the evolution of online monetary fraud techniques over the past decade, compare and contrast the approaches to fraud prevention adopted by Indian financial institutions versus their international counterparts, assess the effectiveness of current regulatory frameworks in addressing online monetary fraud, and investigate the role of emerging technologies in both perpetrating and preventing online financial fraud. The research questions for this study cover various aspects of online monetary fraud, including definitions and classifications, prevalent types, evolution of techniques, preventive measures and strategies, effectiveness of regulatory frameworks, impact of emerging technologies, challenges in implementing fraud prevention measures, influence of consumer behaviour and awareness, economic implications, and potential for enhanced collaboration between stakeholders. The rationale for this investigation stems from the increasing prevalence of online financial transactions and the associated risks of fraud. As digital banking and e-commerce continue to expand, understanding and addressing online monetary fraud becomes increasingly critical for financial institutions, regulatory bodies, and consumers alike. The methodology employed in this research primarily consists of a literature review, supplemented by case studies.

Review of Literature

Online Monetary Fraud and Indian Financial Bodies

Monetary or Financial Fraud doesn't come under criminal offence as per the Reserve Bank of India (Gulpham, 2022). Reserve Bank of India (RBI) defines financial fraud as "fraudulent encashment through forged instruments, manipulation of books of account or through fictitious accounts and conversion of property, and unauthorized credit facilities extended for reward or for illegal gratification" (*Reserve Bank of India*, 2009). RBI also says that cheating, forgery, criminal breach of trust, money embezzlement, or account manipulation, are also considered offences (*Reserve Bank of India*, 2001). However, any type of negligence that results in the loss of a company's assets does not constitute financial fraud (*FINANCIAL FRAUDS IN INDIA*, 2022). According to the Reserve Bank of India, online monetary fraud is defined as "a deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank" (*Reserve Bank of India*, 2011).

State Bank of India (SBI) defines online monetary fraud as any illegitimate transaction or fraudulent activity that occurs through digital channels, such as internet banking, mobile banking, debit/credit card transactions, and electronic fund transfers (*State Bank of India*, 2022).

Online monetary fraud is any fraudulent scheme that uses secure internet connections to gain access to sensitive financial information from individuals or businesses, such as credit card numbers and bank account details, defined by (*Central Bank of India*, 2020). Additionally, it asserts that this fraud entails schemes to manipulate digital markets, rigging prices on virtual assets or stock exchanges, manipulating consumer transactions to defraud consumers, transferring money between accounts without authorization, and building faux websites through which malicious actors try to steal personal information.

(*Union Bank of India*, 2022) explained online monetary fraud as any wrongful or unauthorised use of a person's financial information to transfer money or goods without their permission. It has also stated that the primary reason to do such fraud is to access funds and transfer them illegally for personal gain.

Online monetary fraud is any falsified action that involves unauthorised access to a customer's bank account or sensitive financial information, with the intent to steal money or personal data. It also discussed that such activity is punishable by law and can result in serious financial and reputational damage for both the customer and the bank (*Punjab National Bank*, 2020).

(*Indian Bank*, 2023) describes online monetary fraud as any deceptive act or omission used to secure unauthorised access and misuse of electronic funds. It also says that the result of such fraud can be substantial losses for the banks and customers, as well as legal action will be taken against those who perpetrate these crimes.

(*ICICI Bank*, 2023) refers to online monetary fraud as the illegal use of other people's identities or financial account information over the Internet for malicious purposes such as attempting to steal money. To combat this type of fraud, they have implemented various security measures including advanced encryption technology which encrypts customer data during transmission across networks, two-factor authentication protocols for login accesses and chip & pin technology for credit/debit cards among others.

Online monetary fraud is an illegitimate use of a person's banking details to steal money without their knowledge. It often involves the theft of personal information such as credit card numbers and passwords collected through malicious websites or emails sent by criminals impersonating trusted sources (*Axis Bank*, 2021).

(*Kotak Mahindra Bank*, 2022) describes online monetary fraud as an attempt to obtain someone's financial information, identity and personal funds through the use of technology unlawfully. It also suggests that customers should remain aware at all times when interacting with any digital banking services to protect themselves from becoming victims of this kind of fraud.

Online monetary fraud is defined by IDFC First Bank as an attempt to steal money from an individual's bank account through illicit transactions or other illegal methods. The bank also states that the common tactics employed by cybercriminals in the attempt of stealing funds include sending fake invoices created for nonexistent services/merchandise which requires payment upfront as well as creating a spoof website with a similar URL & design that requests customers' banking login credentials (*IDFC FIRST Bank*, 2023).

(*Yes Bank*, 2018) described online monetary fraud as the illegal use of technology to steal, misuse or transfer money without authorization. It usually involves theft from banks through cyberattacks or using stolen credit card information to make illegal payments. Another form of online monetary fraud includes identity theft which occurs when confidential information is obtained to gain access to someone else's finances.

Online Monetary Fraud and International Financial Bodies

(*Federal Bureau of Investigation (FBI)*, 2022) stated that financial fraud becomes online monetary fraud or online financial fraud with the "use of internet services or software with internet access to intentionally defraud individuals, organizations or entities". (Cole, 2023) described in his study that cyber financial frauds are different from the previous financial frauds committed as they include the use of technology. He also stated that conceptualising online financial fraud aids in describing and distinguishing criminal tactics in both online and physical environments. (McGuire & Dowling, 2013) also highlighted in their study that cyber financial fraud necessitates the use of a technical device.

According to (*The World Bank*, 2021), online monetary fraud is financial fraud which occurs when someone uses technology-enabled methods to unlawfully obtain money or assets. It also states that online monetary fraud is a growing threat due to the global nature of digital networks, so individuals need to be aware and cautious when engaging in electronic forms of communication-related to their finances.

(The Council of Financial Regulators, 2020) defines online monetary fraud as "the dishonest or illegal use of electronic communications, including through the internet and telephone networks to obtain money from others by deception." It also states that online financial fraud covers any other form of deception that can be used to commit financial fraud over an online medium. This can be concluded that it is a form of financial deception which involves the use of technology, such as websites and email, to deceive individuals into sending money or other goods. It involves using false pretences or information misrepresentation in an attempt to acquire funds, and personal data or take control over accounts.

According to (*International Monetary Fund (IMF)*, 2020), online monetary fraud is any intentional misstatement or misrepresentation made over digital networks and technology that leads to direct economic losses. This involves perpetrators taking unauthorized control over an individual's bank accounts, debit cards, or other types of remote payments. The IMF recommends effective measures for preventing this type of criminal activity to protect businesses from large-scale financial loss and potential reputational damage.

(*USA Government*, 2022) describes online monetary fraud as a form of fraudulent activity typically conducted via digital communications technology. It involves using false information or manipulation with the intent to deceive others into giving up their money or valuable related data and information. It also says that online monetary fraud is an attempt by individuals or businesses to gain money illegally via digital networks using fraudulent methods and deception.

Classification of Online Monetary Fraud

Online monetary fraud is a growing problem in today's digital world. Individuals need to be aware of the different types of online monetary fraud so that they can protect themselves from becoming victims.

1. **Credit/Debit Card Fraud**
   It involves the use of credit or debit card information to purchase something without an individual’s knowledge to gain access to his/her financial accounts (*Reserve Bank of India*, 2011). Rising adoption of digital payments with more people shifting towards debit/credit cards as their primary payment option, criminals are finding new ways of exploiting vulnerable systems and data sources to gain access to customer account details or personal identity information (*Kotak Mahindra Bank*, 2022).

2. **Payment Gateway Fraud**
   It occurs when hackers attempt to steal money from any individual through fraudulent payment gateways (*Reserve Bank of India*, 2011). This crime has become increasingly common in recent years, partly due to the rising number of online shoppers and e-commerce sites giving criminals more opportunities to commit this kind of fraud. The perpetrators are often able to hide their identity by using proxies and other means when conducting these transactions (*ICICI Bank*, 2023).

3. **Phishing**
   According to (*Reserve Bank of India*, 2011), an attempt at identity theft via email messages sent out asking for confidential personal information such as bank account numbers, passwords or PIN codes; these emails either direct people to counterfeit websites that look similar & authentic to some original sites where victims enter their details which are then stolen by criminals posing as legitimate organizations are classified under phishing scams. There has been an increase in the incidence of phishing over the past year (*Indian Bank*, 2023). This is due to several factors described by (State *Bank of India*, 2022) which include the following: phishers are taking advantage of the fact that many people may not be familiar with current security protocols or protective measures against online scams and frauds, increasing use of social media platforms by Indian banks as a way to reach out to their customers can make them more vulnerable to phishing attacks due to lack of proper authentication procedures from such platforms as well as user inexperience, and a significant amount of commercial activities carried out through internet banking, makes it easier for fraudsters posing under guise company officials trying lure unsuspecting victims into revealing confidential information like PINs, etc.

4. **Social Engineering Fraud**
   When an individual impersonates any authority which involves engaging with the targets while making fake promises and offering deals too good to ignore to mislead them and gather financially sensitive data may fall under the ambit of a Social Engineering Scam (*Reserve Bank of India*, 2011). This type of fraud has been a major issue in 2020. The factors driving the growth in social engineering fraud include an increase in online transactions due to Covid-19,

weak customer authentication processes at bank websites and mobile applications, inadequate employee training regarding cyber security threats, and lack of awareness about such risks among customers (*IDFC FIRST Bank*, 2023).

5. Money Muling

(*Reserve Bank of India*, 2011) states that money muling occurs when criminals recruit victims for passing stolen funds internationally in exchange for some commission amounts without knowing they're partaking in money laundering. This practice has become more popular due to the rise of e-commerce transactions, as there is often an overlap between countries involved in such financial transactions. Money mules are generally recruited through job postings on classified websites that promise large payments without asking for credentials or references (*State Bank of India*, 2022).

6. Malware

A breach of computer systems using malicious software including viruses and Trojans introduced with the intent of gaining finance-related data from users' devices falls under this category of online financial fraud reported by (*Reserve Bank of India*, 2011). These Viruses are programs designed to replicate themselves on other computers without permission from the user. Worms spread through computer networks by exploiting security vulnerabilities in operating systems or applications (*USA Government*, 2022).

7. Internet or Mobile Banking Fraud

According to (*Reserve Bank of India*, 2011), this fraud involves fraudulent transactions taking place on mobile banking apps or internet bank accounts without consumer permission. (*State Bank of India*, 2022) states that this type of fraud is a major concern due to the increasing number of online financial transactions.

8. Online Investment Scams

This type of fraud includes investors getting duped into investing their money without any tangible returns on online investments, like, trading forex, cryptocurrency, etc., whereby nothing substantial materializes after the fund transfer occurs leaving customers at a large loss-making, such venture fall under major scrutiny by (*Reserve Bank of India*, 2011). The World Bank has discussed the increasing prevalence of investment scams. Common types of investment fraud include Ponzi schemes, pyramid schemes, advance fee frauds, fake initial coin offerings (ICOs), and other forms of deception. (*The World Bank*, 2021) warns that these scams often target vulnerable populations such as retirees or those living on fixed incomes who may be more likely to fall victim to them due to their lack of knowledge about investing.

9. Smishing

As per (*State Bank of India*, 2022), smishing is a form of phishing attack that uses SMS messages to lure victims into sharing personal information or downloading malicious software. In this type of attack, the attacker sends out an SMS message with a link designed to look like it came from a legitimate source such as the bank, and when clicked by the user, he/she is prompted to enter their banking credentials or download malware onto their device which grants access to sensitive data. One example of this type of attack includes using text messages with language such as "your account needs updating", prompting users to click on the link provided within the message (*Central Bank of India*, 2020).

10. Vishing

Vishing is a form of online financial fraud where scammers use call automated systems to try and convince people that they are legitimate representatives from trusted organizations, such as banks. The goal is usually to get personal information or money from victims by requesting them to make payments online (*State Bank of India*, 2022). This has recently been reported within (*Central Bank of India*, 2020), where an international organized crime group was targeting customers with vishing calls. This scam involved calling unsuspecting customers and pretending to represent Central Bank of India or its staff members, to get victims' details such as credit/debit card numbers and passwords. The criminals then used this information to gain access to customer accounts and withdraw funds illegally.

11. Ransomware

(*Reserve Bank of India*, 2011) defines ransomware as "unauthorised software or malicious code which can be used to hold computer systems, mobile phones, tablets or networks, hostage, until the hackers secure payment in return for unlocking them." This definition covers not only traditional forms of malware such as viruses and Trojans but also newer attacks that use advanced encryption techniques. In 2020, (*Punjab National Bank*, 2020) was the victim of a ransomware attack. This cyber-attack involved hackers encrypting important data and asking for ransom in exchange for decrypting it. The cyber-attack impacted multiple branches of the bank across India and caused significant disruption to their services.

12. Social Networks Fraud

Social network frauds refer to any fraudulent activity that takes place on social media platforms such as Facebook, Twitter, Instagram and other similar sites (*Yes Bank*, 2018). According to the (*Reserve Bank of India*, 2011), these types of frauds are becoming increasingly common in India due to the rise in popularity of online banking services and social media usage among customers.

Steps taken to prevent Online Monetary Fraud by Indian Financial Bodies

(*Department of Financial Services | Ministry of Finance | Government of India*, 2022) has implemented new regulations that require financial institutions to take additional measures when processing payments and transfers online which involves verifying customer identities and monitoring transactions for suspicious activity, increased its enforcement efforts against fraudulent activities by increasing penalties for those found guilty of such crimes, launched an awareness campaign aimed at educating consumers about how to protect themselves from online fraudsters and scams, as well as providing resources on how they can report any suspicious activity or potential victims of frauds, and worked with law enforcement agencies across the country to investigate cases related to online monetary fraud and bring perpetrators to justice quickly and effectively.

(*Ministry of Home Affairs*, 2021) has established an inter-ministerial committee to monitor and investigate cases of online financial fraud which aims to identify fraudulent activities, take appropriate action against perpetrators & provide guidance on preventive measures for citizens, set up a dedicated cybercrime cell in each state that will be responsible for investigating cyber-crimes related to online financial transactions, issued advisories and guidelines regarding safe practices while conducting online financial transactions such as using strong passwords, avoided sharing personal information over unsecured networks etc., which can help reduce the risk of falling victim to fraudsters or hackers, and worked closely with Indian banks and other payment service providers to ensure secure digital payments by introducing additional security features like two-factor authentication (OTP) when making payments through mobile wallets or net banking services etc.

(*Reserve Bank of India*, 2011) has formed an Online Fraud Monitoring System that monitors and detects suspicious transactions in real-time, introduced two-factor authentication for all online banking transactions, which requires customers to enter their mobile phone numbers or email addresses as well as passwords when making payments online, encouraged all Indian banks to use advanced analytics tools such as machine learning algorithms and artificial intelligence systems to detect fraudulent activities quickly and accurately, established a special committee of the board members for reviewing financial fraud of Rs.1 crore and above, issued guidelines on customer due diligence measures that banks should take while onboarding new customers which involves KYC verification processes & identity checks using biometrics data such as fingerprints or iris scans, and persuaded all Indian banks to implement robust cyber security measures such as firewalls, encryption technologies, intrusion detection systems etc., to protect against malicious attacks from hackers.

To prohibit online financial fraud (*All India Council for Technical Education*, 2017) has created an online portal that allows students and institutions to report any suspicious activity related to cyber financial fraud, developed guidelines on how best to protect against cyber-attacks, such as using strong passwords and two-factor authentication systems, closely worked with Indian banks and other payment service providers to ensure secure transactions are taking place when making payments through AICTE's website or mobile app, launched a 24*7 cyber financial crime helpline number to report any online financial fraud, educated students about the risks associated with online banking and provided them with information on how they can protect themselves from becoming victims of cyber financial frauds, and set up a dedicated team within AICTE that is responsible for monitoring all activities related to cyber security to identify potential threats before they become serious issues.

(*State Bank of India*, 2022) has implemented two-factor authentication for all its customers, which requires users to enter an OTP sent via SMS or email to access their accounts, used advanced encryption technology and secure sockets layer (SSL) certificates on its websites and mobile applications to protect customer data from unauthorized access, monitored transactions closely and flags any suspicious activity immediately so that it can be investigated further by the bank’s security team, and encouraged its costumers to use strong passwords when accessing their accounts, as well as regularly asked them to change the passwords so that the risk of fraudsters gaining access through brute force attacks or phishing scams can be reduced.

(*Ministry of Corporate Affairs*, 2023) has instigated an e-filing system for companies that allows them to file their documents electronically and securely to reduce the risk of fraudulent activities related to company filings, introduced Know Your Customer (KYC) norms which require companies to verify customer information before allowing transactions or payments from customers’ accounts, organizing a dedicated team called ‘Fraud Prevention Cell’ which monitors suspicious activity on corporate websites and takes action against any fraudulent activities detected by it and operated awareness campaigns about cyber security and financial frauds to educate people about how they can protect themselves from becoming victims of online scams or money laundering schemes.

(*ICICI Bank*, 2023) has offered two-factor authentication for all its customers, which requires users to enter both their username and password as well as an additional code sent via SMS or email to access their accounts, provided secure encryption technology that ensures customer data is kept safe from hackers, and monitored user activity on its platform to detect any suspicious behaviour or potential fraud attempts quickly and efficiently.

Secure sockets layer (SSL) certificates are used by (*Axis Bank*, 2021) to ensure secure communication between customers and its servers when accessing their accounts online, moreover, customers are encouraged to use strong passwords with a combination of letters, numbers, and special characters to further enhance security measures against potential threats such as phishing attacks or malware infections on computers/mobile devices being used for online banking activities.

(*Kotak Mahindra Bank*, 2022) uses advanced fraud detection systems to identify any suspicious activity on customer accounts and take appropriate action if necessary, and regularly reviews its security protocols and updates them as needed to keep up with the latest threats from cyber criminals.

Steps taken to prevent Online Monetary Fraud by International Financial Bodies

To prevent online monetary fraud, (*Federal Bureau of Investigation (FBI)*, 2022) has established an Internet Crime Complaint Center (IC3), which allows victims of online crime to report their experiences and receive assistance from law enforcement agencies, worked with other federal, state, local and international law enforcement partners to investigate cybercrime cases and bring perpetrators to justice, provided educational resources for consumers on how they can protect themselves against online frauds such as phishing scams or identity theft schemes, and worked closely with financial institutions to detect suspicious activity that may be taking place through digital currencies like Bitcoin or Ethereum.

(*International Monetary Fund (IMF)*, 2020) has created an Anti-Money Laundering Unit within the IMF, which is responsible for monitoring suspicious transactions & identifying potential money laundering activities, functioned with other international organizations such as Interpol and Europol to share information about fraudulent activity across borders &coordinate efforts to combat it more effectively, urged countries around the world to adopt stronger anti-money laundering laws and regulations to reduce opportunities for criminals to commit online frauds using digital currencies or other payment systems like PayPal or Venmo.

To avoid online financial fraud, (*The World Bank*, 2021) has launched an Anti-Fraud Unit within the bank that is dedicated to preventing and detecting fraudulent activities related to online payments, and built up secure payment systems, such as two-factor authentication and encryption technologies, which help protect customer data from being stolen or misused by criminals.

(The Council of Financial Regulators (CFR), 2020) has made guidelines for financial institutions on how to detect and respond to suspicious activity related to online payments, and developed new technologies that can help identify fraudulent activities in real-time and alert authorities when necessary.

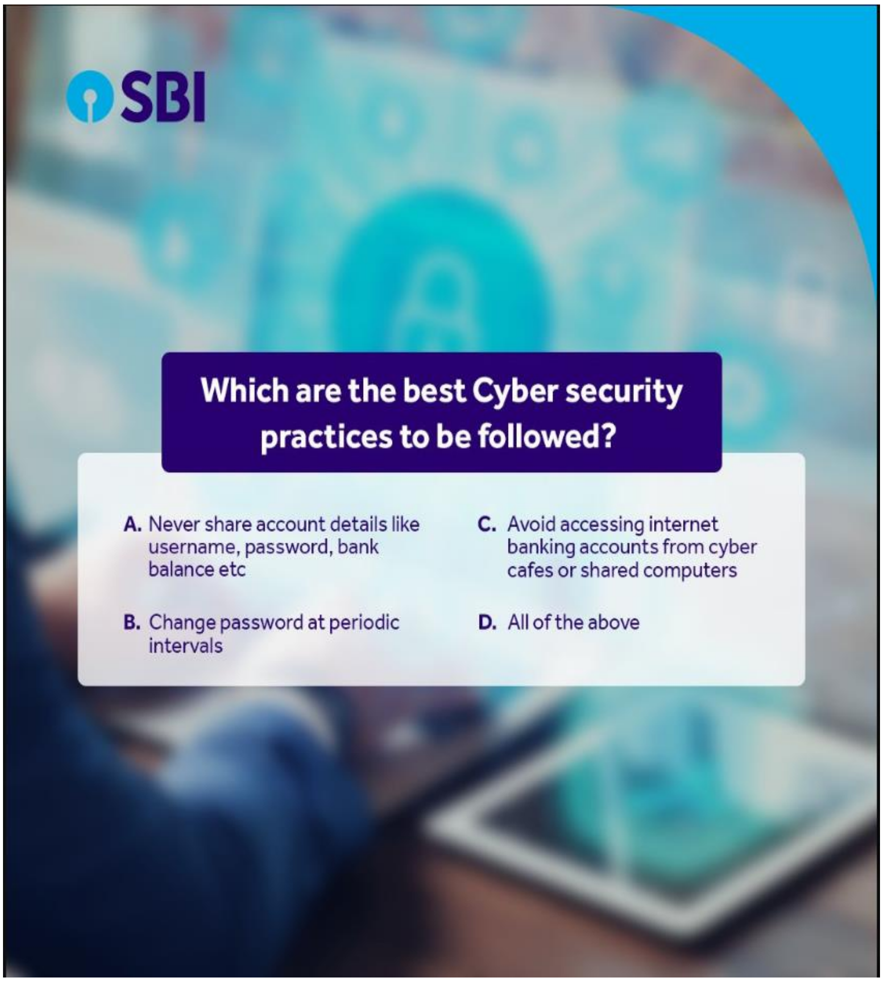
Advertisements to prevent Online Monetary Fraud by Financial Bodies

(*State Bank of India*, 2022) has launched an advertisement #IAmResponsible to aware its customers about digital safety and security.

Be Aware &
Stay Protected from
Cyber Frauds
Be an Alert Customer.
#IAmResponsible

Source. (*State Bank of India*, 2022)

Apart from this, (*State Bank of India*, 2022) has also launched several advertisements in which they talked about safe banking and shared some useful tips and tricks to prevent online monetary fraud.



Which are the best Cyber security practices to be followed?

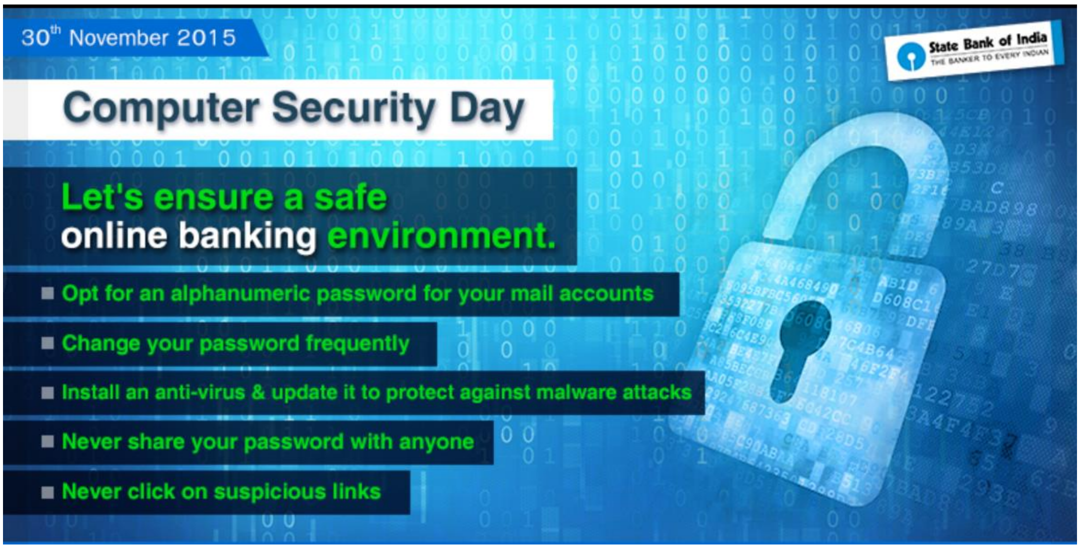
A. Never share account details like username, password, bank balance etc

B. Change password at periodic intervals

C. Avoid accessing internet banking accounts from cyber cafes or shared computers

D. All of the above

Source. (State Bank of India, 2017)



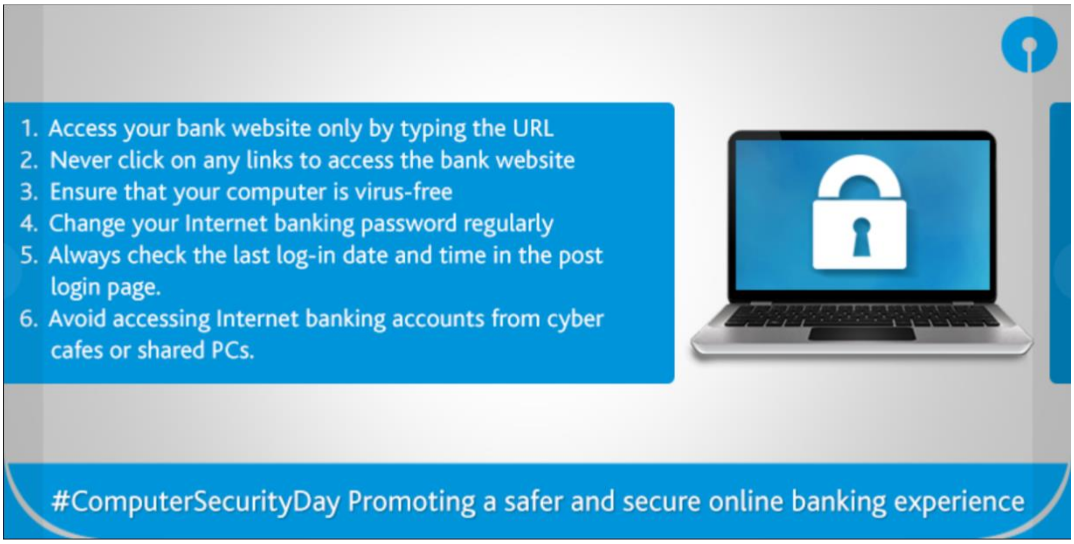
30th November 2015

Computer Security Day

Let's ensure a safe online banking environment.

- Opt for an alphanumeric password for your mail accounts
- Change your password frequently
- Install an anti-virus & update it to protect against malware attacks
- Never share your password with anyone
- Never click on suspicious links

Source. (*State Bank of India*, 2015)

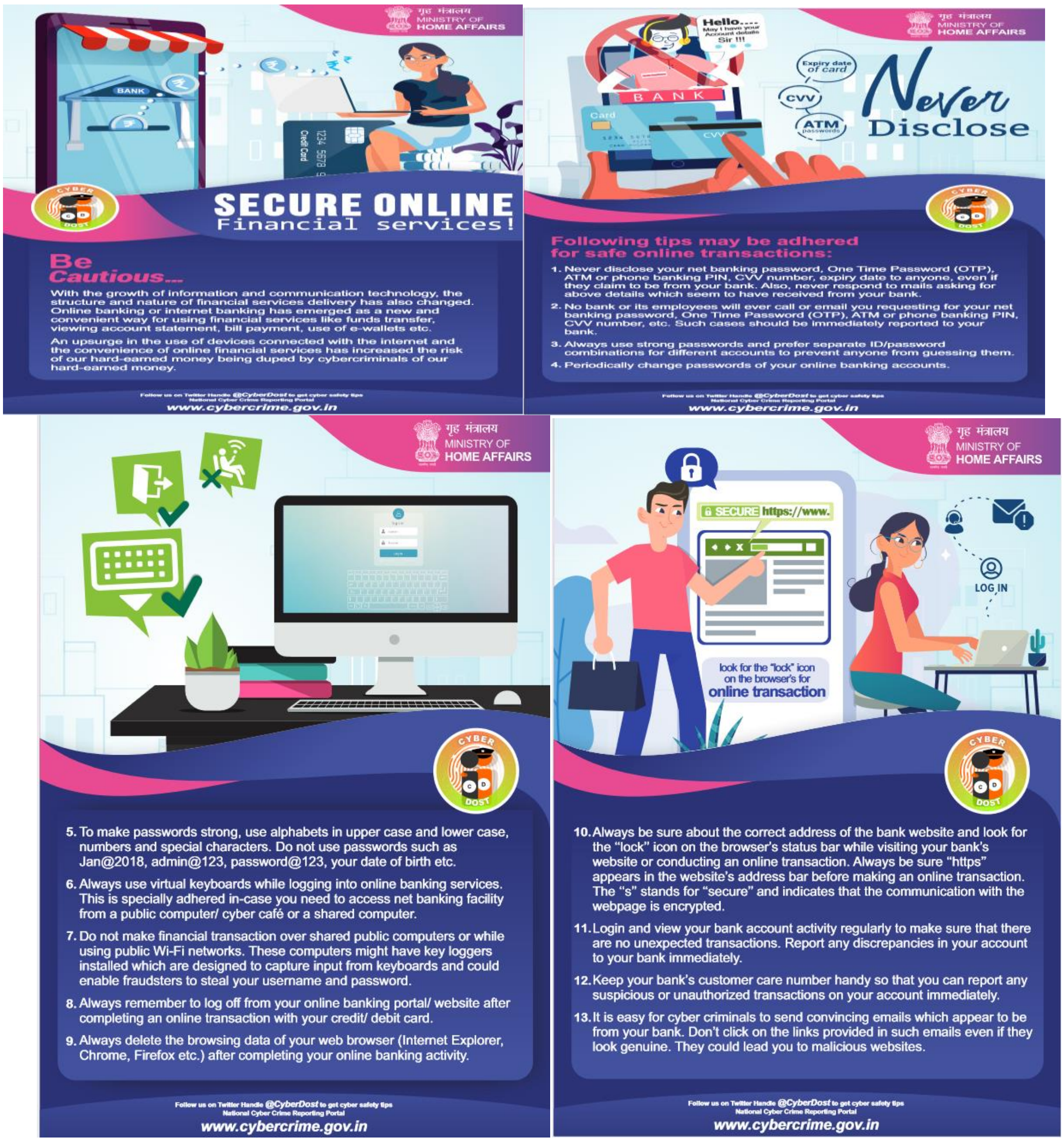


1. Access your bank website only by typing the URL
2. Never click on any links to access the bank website
3. Ensure that your computer is virus-free
4. Change your Internet banking password regularly
5. Always check the last log-in date and time in the post login page.
6. Avoid accessing Internet banking accounts from cyber cafes or shared PCs.

#ComputerSecurityDay Promoting a safer and secure online banking experience

Source. (*State Bank of India - #ComputerSecurityDay*, 2014)

(*All India Council for Technical Education*, 2017) created a series of advertisements through which they talked about Indian Government's Twitter Handle @CyberDost so the customers can get cyber safety tips, as well they shared some guidelines to prevent financial fraud.


गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
BANK
Credit Card
1234 5678 9
CYBER
DOST
Hello.... May I have your Account details Sir !!!
BANK
Card
CVV
Expiry date of card
CVV
ATM passwords
Never
Disclose
SECURE https://www.
look for the "lock" icon on the browser's for
online transaction
LOG IN

SECURE ONLINE
Financial services!

Be Cautious....

With the growth of information and communication technology, the structure and nature of financial services delivery has also changed. Online banking or internet banking has emerged as a new and convenient way for using financial services like funds transfer, viewing account statement, bill payment, use of e-wallets etc.

An upsurge in the use of devices connected with the internet and the convenience of online financial services has increased the risk of our hard-earned money being duped by cybercriminals of our hard-earned money.

Follow us on Twitter Handle @CyberDost to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

Following tips may be adhered for safe online transactions:

1. Never disclose your net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number, expiry date to anyone, even if they claim to be from your bank. Also, never respond to mails asking for above details which seem to have received from your bank.
2. No bank or its employees will ever call or email you requesting for your net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number, etc. Such cases should be immediately reported to your bank.
3. Always use strong passwords and prefer separate ID/password combinations for different accounts to prevent anyone from guessing them.
4. Periodically change passwords of your online banking accounts.

Follow us on Twitter Handle @CyberDost to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

5. To make passwords strong, use alphabets in upper case and lower case, numbers and special characters. Do not use passwords such as Jan@2018, admin@123, password@123, your date of birth etc.
6. Always use virtual keyboards while logging into online banking services. This is specially adhered in-case you need to access net banking facility from a public computer/ cyber café or a shared computer.
7. Do not make financial transaction over shared public computers or while using public Wi-Fi networks. These computers might have key loggers installed which are designed to capture input from keyboards and could enable fraudsters to steal your username and password.
8. Always remember to log off from your online banking portal/ website after completing an online transaction with your credit/ debit card.
9. Always delete the browsing data of your web browser (Internet Explorer, Chrome, Firefox etc.) after completing your online banking activity.

Follow us on Twitter Handle @CyberDost to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

10. Always be sure about the correct address of the bank website and look for the "lock" icon on the browser's status bar while visiting your bank's website or conducting an online transaction. Always be sure "https" appears in the website's address bar before making an online transaction. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted.
11. Login and view your bank account activity regularly to make sure that there are no unexpected transactions. Report any discrepancies in your account to your bank immediately.
12. Keep your bank's customer care number handy so that you can report any suspicious or unauthorized transactions on your account immediately.
13. It is easy for cyber criminals to send convincing emails which appear to be from your bank. Don't click on the links provided in such emails even if they look genuine. They could lead you to malicious websites.

Follow us on Twitter Handle @CyberDost to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

Source. (*All India Council for Technical Education*, 2017)

(*Punjab National Bank*, 2020) advertised to report any online financial fraud at cybercrime.gov.in or to dial 1930. Apart from this, they also urged their costumers to follow @cyberdost on Facebook, Instagram, LinkedIn, KOO, and Twitter.

Suspicion can lead to detection.
Find something fishy?

Report Cyber Crime at
National Cyber Crime Reporting Portal:
https://cybercrime.gov.in

Or Call at Helpline no.: 1930

75 Azadi Ka Amrit Mahotsav

pnb

punjab national bank
...the name you can BANK upon !

www.pnbindia.in

Call 1-800-180-2222 or 1-800-103-2222 Toll Free

Source. (Punjab National Bank, 2022)

pnb

75 Azadi Ka Amrit Mahotsav

Don't bow down to
cyber fraudsters'
demands

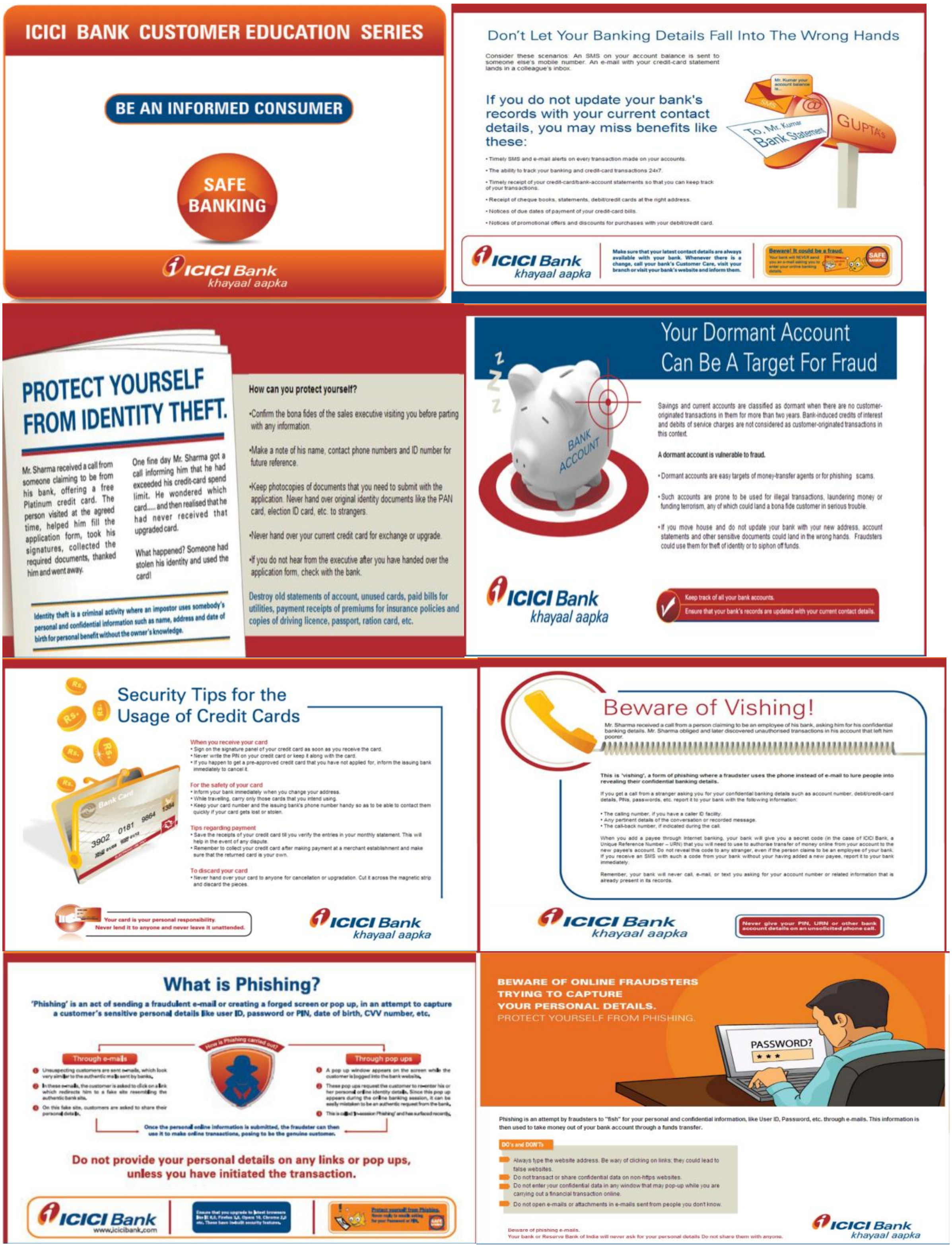
Report incidents of
Cyber Crime with
cybercrime.gov.in
or dial 1930
(Earlier 155260)
for assistance

Credit Card
10.25
Thursday
Credit Card
******
Confirm

Follow @cyberdost

Source. (*Punjab National Bank #cyberfraud #cybersecurity #foolthefraudster*, 2022)

(*ICICI Bank*, 2023) launched a costumer education series in which they guided their costumers on how to prevent themselves from the online financial fraudsters.



ICICI BANK CUSTOMER EDUCATION SERIES

BE AN INFORMED CONSUMER

SAFE BANKING

ICICI Bank
khayaal aapka

Don't Let Your Banking Details Fall Into The Wrong Hands

Consider these scenarios: An SMS on your account balance is sent to someone else's mobile number. An e-mail with your credit-card statement lands in a colleague's inbox.

If you do not update your bank's records with your current contact details, you may miss benefits like these:

- Timely SMS and e-mail alerts on every transaction made on your accounts.
- The ability to track your banking and credit-card transactions 24x7.
- Timely receipt of your credit-card/bank-account statements so that you can keep track of your transactions.
- Receipt of cheque books, statements, debit/credit cards at the right address.
- Notices of due dates of payment of your credit-card bills.
- Notices of promotional offers and discounts for purchases with your debit/credit card.

ICICI Bank
khayaal aapka

Make sure that your latest contact details are always available with your bank. Whenever there is a change, call your bank's Customer Care, visit your branch or visit your bank's website and inform them.

Beware! It could be a fraud.
Your bank will NEVER send you an e-mail asking you to enter your online banking details.

SAFE BANKING

PROTECT YOURSELF FROM IDENTITY THEFT.

Mr. Sharma received a call from someone claiming to be from his bank, offering a free Platinum credit card. The person visited at the agreed time, helped him fill the application form, took his signatures, collected the required documents, thanked him and went away.

One fine day Mr. Sharma got a call informing him that he had exceeded his credit-card spend limit. He wondered which card..... and then realised that he had never received that upgraded card.

What happened? Someone had stolen his identity and used the card!

Identity theft is a criminal activity where an impostor uses somebody's personal and confidential information such as name, address and date of birth for personal benefit without the owner's knowledge.

How can you protect yourself?

- Confirm the bona fides of the sales executive visiting you before parting with any information.
- Make a note of his name, contact phone numbers and ID number for future reference.
- Keep photocopies of documents that you need to submit with the application. Never hand over original identity documents like the PAN card, election ID card, etc. to strangers.
- Never hand over your current credit card for exchange or upgrade.
- If you do not hear from the executive after you have handed over the application form, check with the bank.

Destroy old statements of account, unused cards, paid bills for utilities, payment receipts of premiums for insurance policies and copies of driving licence, passport, ration card, etc.

Your Dormant Account Can Be A Target For Fraud

Savings and current accounts are classified as dormant when there are no customer-originated transactions in them for more than two years. Bank-induced credits of interest and debits of service charges are not considered as customer-originated transactions in this context.

A dormant account is vulnerable to fraud.

- Dormant accounts are easy targets of money-transfer agents or for phishing scams.
- Such accounts are prone to be used for illegal transactions, laundering money or funding terrorism, any of which could land a bona fide customer in serious trouble.
- If you move house and do not update your bank with your new address, account statements and other sensitive documents could land in the wrong hands. Fraudsters could use them for theft of identity or to siphon off funds.

ICICI Bank
khayaal aapka

✓ Keep track of all your bank accounts.
Ensure that your bank's records are updated with your current contact details.

Security Tips for the Usage of Credit Cards

When you receive your card
- Sign on the signature panel of your credit card as soon as you receive the card.
- Never write the PIN on your credit card or keep it along with the card.
- If you happen to get a pre-approved credit card that you have not applied for, inform the issuing bank immediately to cancel it.

For the safety of your card
- Inform your bank immediately when you change your address.
- While travelling, carry only those cards that you intend using.
- Keep your card number and the issuing bank's phone number handy so as to be able to contact them quickly if your card gets lost or stolen.

Tips regarding payment
- Save the receipts of your credit card till you verify the entries in your monthly statement. This will help in the event of any dispute.
- Remember to collect your credit card after making payment at a merchant establishment and make sure that the returned card is your own.

To discard your card
- Never hand over your card to anyone for cancellation or upgradation. Cut it across the magnetic strip and discard the pieces.

Your card is your personal responsibility.
Never lend it to anyone and never leave it unattended.

ICICI Bank
khayaal aapka

Beware of Vishing!

Mr. Sharma received a call from a person claiming to be an employee of his bank, asking him for his confidential banking details. Mr. Sharma obliged and later discovered unauthorised transactions in his account that left him poorer.

This is 'vishing', a form of phishing where a fraudster uses the phone instead of e-mail to lure people into revealing their confidential banking details.

If you get a call from a stranger asking you for your confidential banking details such as account number, debit/credit-card details, PINs, passwords, etc. report it to your bank with the following information:

- The calling number, if you have a caller ID facility.
- Any pertinent details of the conversation or recorded message.
- The call-back number, if indicated during the call.

When you add a payee through Internet banking, your bank will give you a secret code (in the case of ICICI Bank, a Unique Reference Number – URN) that you will need to use to authorise transfer of money online from your account to the new payee's account. Do not reveal this code to any stranger, even if the person claims to be an employee of your bank. If you receive an SMS with such a code from your bank without your having added a new payee, report it to your bank immediately.

Remember, your bank will never call, e-mail, or text you asking for your account number or related information that is already present in its records.

ICICI Bank
khayaal aapka

Never give your PIN, URN or other bank account details on an unsolicited phone call.

What is Phishing?

'Phishing' is an act of sending a fraudulent e-mail or creating a forged screen or pop up, in an attempt to capture a customer's sensitive personal details like user ID, password or PIN, date of birth, CVV number, etc.

How is Phishing carried out?

Through e-mails
1. Unsuspecting customers are sent e-mails, which look very similar to the authentic mails sent by banks.
2. In these e-mails, the customer is asked to click on a link which redirects him to a fake site resembling the authentic bank site.
3. On this fake site, customers are asked to share their personal details.

Through pop ups
1. A pop up window appears on the screen while the customer is logged into the bank website.
2. These pop ups request the customer to re-enter his or her personal online identity details. Since this pop up appears during the online banking session, it can be easily mistaken to be an authentic request from the bank.
3. This is called 'In-session Phishing' and has surfaced recently.

Once the personal online information is submitted, the fraudster can then use it to make online transactions, posing to be the genuine customer.

Do not provide your personal details on any links or pop ups, unless you have initiated the transaction.

ICICI Bank
www.icicibank.com

Ensure that you upgrade to latest browsers like IE 8.0, Firefox 3.0, Opera 10, Chrome 2.0 etc. These have inbuilt security features.

Protect yourself from Phishing.
Never reply to emails asking for your Password or PIN.

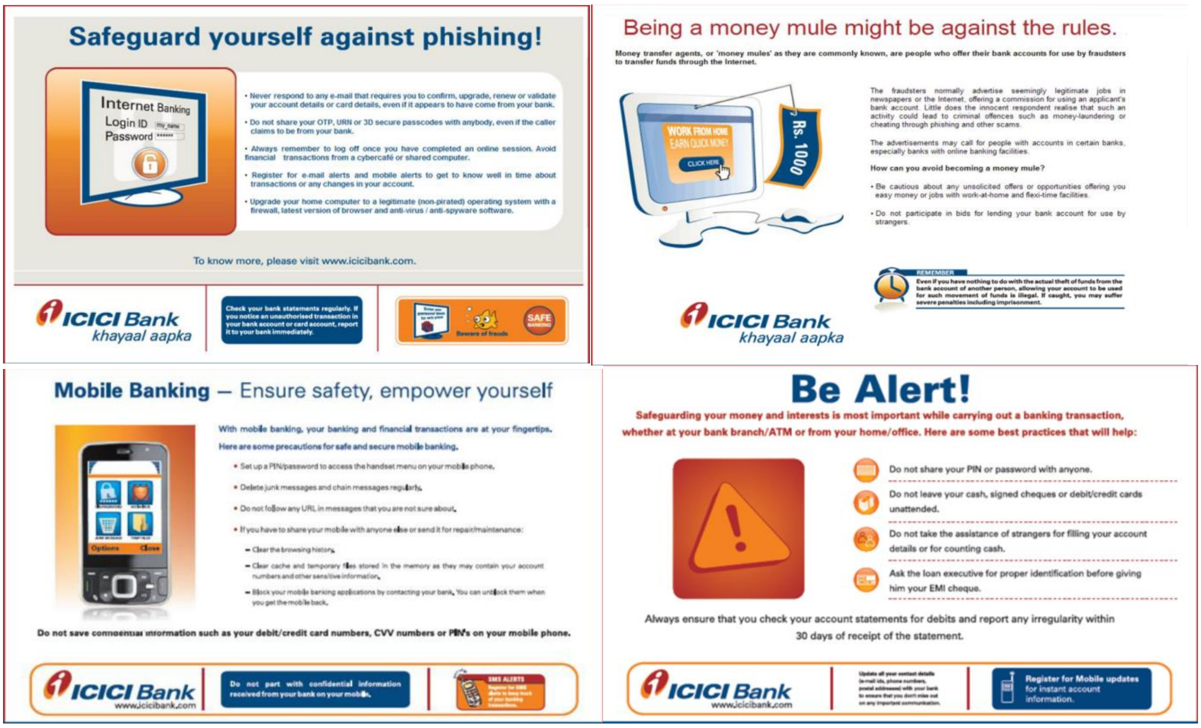
BEWARE OF ONLINE FRAUDSTERS
TRYING TO CAPTURE
YOUR PERSONAL DETAILS.
PROTECT YOURSELF FROM PHISHING.

Phishing is an attempt by fraudsters to "fish" for your personal and confidential information, like User ID, Password, etc. through e-mails. This information is then used to take money out of your bank account through a funds transfer.

DO's and DON'Ts
- Always type the website address. Be wary of clicking on links; they could lead to false websites.
- Do not transact or share confidential data on non-https websites.
- Do not enter your confidential data in any window that may pop-up while you are carrying out a financial transaction online.
- Do not open e-mails or attachments in e-mails sent from people you don't know.

Beware of phishing e-mails.
Your bank or Reserve Bank of India will never ask for your personal details Do not share them with anyone.

ICICI Bank
khayaal aapka


Internet Banking
Login ID my_name
Password ******
WORK FROM HOME
EARN QUICK MONEY
CLICK HERE
Rs. 1000
Options
Close
Beware of frauds
SAFE BANKING
SMS ALERTS
ICICI Bank
khayaal aapka
www.icicibank.com

Safeguard yourself against phishing!

- Never respond to any e-mail that requires you to confirm, upgrade, renew or validate your account details or card details, even if it appears to have come from your bank.
- Do not share your OTP, URN or 3D secure passcodes with anybody, even if the caller claims to be from your bank.
- Always remember to log off once you have completed an online session. Avoid financial transactions from a cybercafé or shared computer.
- Register for e-mail alerts and mobile alerts to get to know well in time about transactions or any changes in your account.
- Upgrade your home computer to a legitimate (non-pirated) operating system with a firewall, latest version of browser and anti-virus / anti-spyware software.

To know more, please visit www.icicibank.com.

Check your bank statements regularly. If you notice an unauthorised transaction in your bank account or card account, report it to your bank immediately.

Being a money mule might be against the rules.

Money transfer agents, or 'money mules' as they are commonly known, are people who offer their bank accounts for use by fraudsters to transfer funds through the Internet.

The fraudsters normally advertise seemingly legitimate jobs in newspapers or the Internet, offering a commission for using an applicant's bank account. Little does the innocent respondent realise that such an activity could lead to criminal offences such as money-laundering or cheating through phishing and other scams.

The advertisements may call for people with accounts in certain banks, especially banks with online banking facilities.

How can you avoid becoming a money mule?

- Be cautious about any unsolicited offers or opportunities offering you easy money or jobs with work-at-home and flexi-time facilities.
- Do not participate in bids for lending your bank account for use by strangers.

REMEMBER

Even if you have nothing to do with the actual theft of funds from the bank account of another person, allowing your account to be used for such movement of funds is illegal. If caught, you may suffer severe penalties including imprisonment.

Mobile Banking — Ensure safety, empower yourself

With mobile banking, your banking and financial transactions are at your fingertips.

Here are some precautions for safe and secure mobile banking.

- Set up a PIN/password to access the handset menu on your mobile phone.
- Delete junk messages and chain messages regularly.
- Do not follow any URL in messages that you are not sure about.
- If you have to share your mobile with anyone else or send it for repair/maintenance:
  - Clear the browsing history.
  - Clear cache and temporary files stored in the memory as they may contain your account numbers and other sensitive information.
  - Block your mobile banking applications by contacting your bank. You can unblock them when you get the mobile back.

Do not save confidential information such as your debit/credit card numbers, CVV numbers or PIN's on your mobile phone.

Do not part with confidential information received from your bank on your mobile.

Register for SMS alerts to keep track of your banking transactions.

Be Alert!

Safeguarding your money and interests is most important while carrying out a banking transaction, whether at your bank branch/ATM or from your home/office. Here are some best practices that will help:

- Do not share your PIN or password with anyone.
- Do not leave your cash, signed cheques or debit/credit cards unattended.
- Do not take the assistance of strangers for filling your account details or for counting cash.
- Ask the loan executive for proper identification before giving him your EMI cheque.

Always ensure that you check your account statements for debits and report any irregularity within 30 days of receipt of the statement.

Update all your contact details (e-mail ids, phone numbers, postal addresses) with your bank to ensure that you don't miss out on any important communication.

Register for Mobile updates for instant account information.

Source. (*ICICI Bank*, 2023)

Additionally, they created awareness among their customers through the advertisement on International Fraud Awareness Day giving Be Aware. Be Safe as its tagline.

ICICI Bank
INTERNATIONAL FRAUD AWARENESS WEEK
November 15-21, 2015
ATM PIN
****
Be Aware. Be Safe.
This International Fraud Awareness Week, learn safe banking practices to avoid being a victim of fraud.

Source. (*ICICI Bank*, 2015)

Discussion

The paper attempts to contextualize online monetary fraud, which is defined differently by various Indian and international financial institutions but generally involves the unauthorized use of digital channels to gain access to financial information or funds. It highlights common types of online monetary fraud, including credit/debit card fraud, payment gateway fraud, phishing, social engineering, money mulling, malware attacks, internet/mobile banking fraud, and online investment scams. The study observed that the rise in digital transactions, particularly due to COVID-19, has led to an increase in online monetary fraud incidents. Indian financial bodies have implemented various measures to prevent online fraud, including two-factor authentication, advanced encryption technologies, and customer awareness campaigns. International financial bodies have established dedicated units to monitor and investigate online fraud and have developed guidelines for financial institutions to detect and respond to suspicious activities. Both Indian and international financial institutions are emphasizing the importance of customer education and awareness in preventing online monetary fraud. Advertisements by financial institutions frequently focus on promoting safe banking practices and providing recommendations to prevent online fraud. Collaboration between financial institutions, law enforcement agencies, and international organizations is crucial in combating online monetary fraud. Emerging technologies are being utilized both to perpetrate and prevent online financial fraud, highlighting the need for continuous adaptation of security measures. The economic implications of online monetary fraud are significant, affecting both individual consumers and financial institutions.

References

1. Here is the citation in APA 7th edition format:
2. All India Council for Technical Education. (2017). *Cybersecurity*. https://www.aicte-india.org/CyberSecurity
3. Axis Bank. (2021). *Fraud and cybersecurity*. https://application.axisbank.co.in/webforms/axis-support/sub-issues/FND-Fraud-ccdcsa-4.aspx?_ga=2.268124298.562521432.1678781800-881009208.1678781800
4. Central Bank of India. (2020). *Cybersecurity resources*. https://www.centralbankofindia.co.in/
5. Cole, T. (2023). How are financial institutions enabling online fraud? A developmental online financial fraud policy review. *Journal of Financial Crime*, ahead-of-print. https://doi.org/10.1108/JFC-10-2022-0261
6. Department of Financial Services | Ministry of Finance | Government of India. (2022, August 17). *Public grievances redressal mechanism*. https://financialservices.gov.in/about-us/public-grievances-redressal-mechanism
7. Federal Bureau of Investigation (FBI). (2022). *Cyber investigations*. https://www.fbi.gov/investigate/cyber
8. FINANCIAL FRAUDS IN INDIA – LEGAL ACTION. (2022). S.S. Rana & Co. https://ssrana.in/ufaqs/financial-frauds-india-legal-action/
9. Gulpham, S. (2022). Financial fraud, economic offence in India: Crime prevention through heuristic method. *The American Journal of Management and Economics Innovations*. https://doi.org/10.37547/tajmei/Volume04Issue04-01
10. ICICI Bank. (2023). *Safe banking*. https://www.icicibank.com/content/icicibank/in/en/online-safe-banking
11. ICICI Bank | Facebook. (2015, November 18). *ICICI Bank Facebook post*. https://www.facebook.com/icicibank/photos/a.287946551256524/1010684588982713/
12. IDFC FIRST Bank. (2023, March 14). *Safe banking*. https://www.idfcfirstbank.com/safe-banking
13. Indian Bank. (2023, February). *Safe banking* resources. https://www.indianbank.in
14. International Monetary Fund (IMF). (2020). *Scams and fraud prevention*. https://www.imf.org/external/scams.htm
15. Kotak Mahindra Bank. (2022). *Safe banking*. https://www.kotak.com/en/safe-banking.html
16. McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Home Office Research Report 75, Chapter 3*.
17. Ministry of Corporate Affairs. (2023, March 6). *Affiliated offices and information*. https://www.mca.gov.in/content/mca/global/en/about-us/affiliated-offices/sfo.html

18. Ministry of Home Affairs. (2021, June 17). *Cybersecurity initiatives*. https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1727990
19. Punjab National Bank. (2020). *Advisories on cybersecurity*. https://www.pnbindia.in/advisories.html
20. Punjab National Bank #cyberfraud #cybersecurity #foolthefraudster | Facebook. (2022, November 2). *Facebook post*.
21. https://www.facebook.com/pnbindia/photos/a.1115688955137006/5825446960827825/
22. Punjab National Bank [@pnbindia]. (2022, March 2). *Cybersecurity tweet*. https://twitter.com/pnbindia/status/1498985051433803776/photo/1
23. Reserve Bank of India. (2009, July). *Cybersecurity notification*. https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=578
24. Reserve Bank of India—Reports. (2001, August 31). *RBI report on cybersecurity*. https://m.rbi.org.in/Scripts/PublicationReportDetails.aspx?ID=247
25. Reserve Bank of India—Reports. (2011, January 21). *RBI cybersecurity report*. https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=621
26. State Bank of India. (2022, September). *Cybersecurity resources*. https://sbi.co.in/web/personal-banking/cyber-security
27. State Bank of India | Facebook. (2015, November 30). *State Bank of India Facebook post*. https://www.facebook.com/StateBankOfIndia/photos/a.513178328732970/1035778506472947/
28. State Bank of India [@TheOfficialSBI]. (2017, November 30). *Cybersecurity trivia tweet*. https://twitter.com/TheOfficialSBI/status/936199322038702082
29. State Bank of India—#ComputerSecurityDay. (2014, November 30). *Facebook post on computer security*.
30. https://www.facebook.com/StateBankOfIndia/photos/a.513178328732970/842765942440872
31. The Council of Financial Regulators (CFR), T. C. of F. R. (CFR). (2020). *Cybersecurity in financial stability*. https://www.cfr.gov.au/financial-stability/cyber-security.html
32. The World Bank. (2021, August 25). *Legal scams information*. https://www.worldbank.org/en/about/legal/scams
33. Union Bank of India. (2022). *Cybersecurity tips*. https://www.unionbankofindia.co.in/english/cyber-security-tips.aspx
34. USA Government. (2022, December 16). *Online safety resources*. https://www.usa.gov/online-safety
35. Yes Bank. (2018). *Secure banking*. https://www.yesbank.in/digital-banking/secure-banking