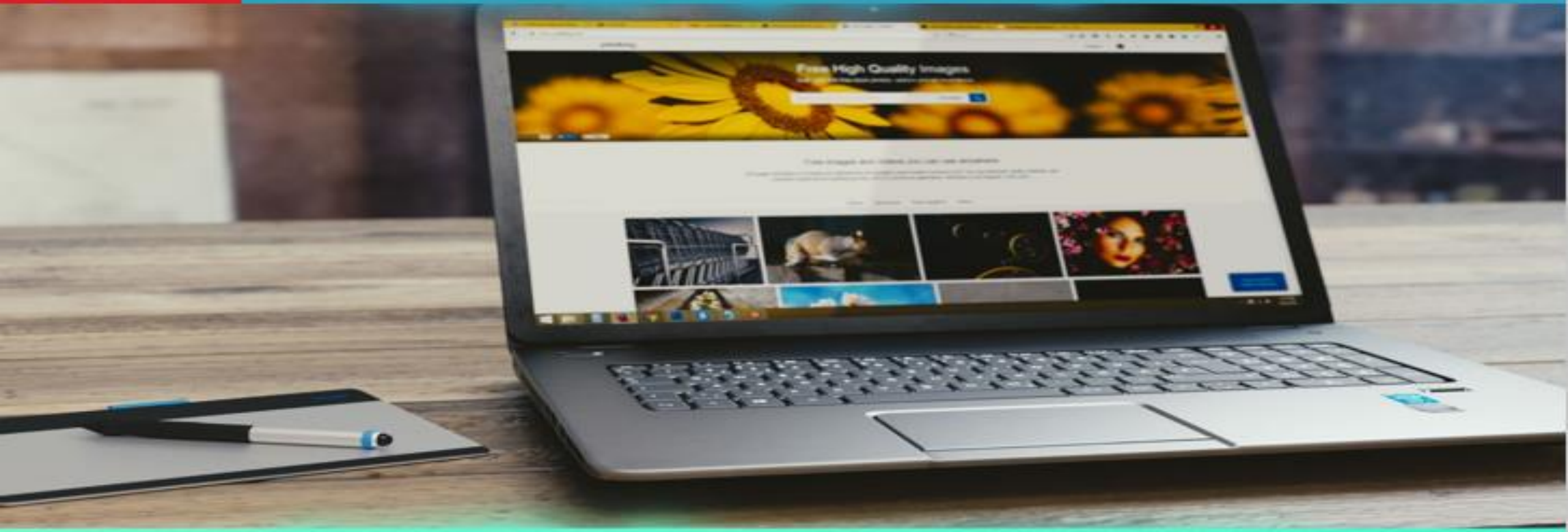
NATIONAL INSTITUTE OF ELECTRONICS AND INFORMATION TECHNOLOGY
Sumit Complex, A-1/9, Vibhuti Khand, Gomti Nagar, Lucknow,



Cyber Security Awareness Program
29.08.2022 to 02.09.2022

Index

E- Payment Frauds

- As of June 2020, 75% of businesses around the world reported experiencing at least as much loss because of fraud through online payment channels during the past year as they did during the previous year*.
- When faced with increasingly secure fraud-protection systems implemented by much larger businesses, fraudsters begin to target smaller, less-secured businesses to try their luck. However, there are ways to protect your small business from these fraudulent attacks.

What is payment fraud?

- Payment fraud occurs when someone steals another person's payment information and uses it to make unauthorized transactions or purchases.
- The actual cardholder or owner of the payment information then notices their account being used for transactions or purchases they did not authorize, and raises a dispute.
- This is where the issue arises for business owners, as they will have to settle the dispute, pay numerous penalties such as chargeback fees and investigation fees, and face an overall loss of time and resources. In some cases, customers themselves can falsely initiate a chargeback, denying ever having received the product. This is also a form of payment fraud.
- If merchant account providers such as banks find it increasingly insecure to be involved in a business's transactions, the business might have their merchant account deactivated due to the risk of fraud. It's easy to see how problematic payment fraud can be for business owners.

Types of payment frauds

- **Identity Theft**: This occurs when an individual conducts a fraudulent transaction under the guise of somebody else. Rather than create a new identity altogether, fraudsters simply steal the personal and banking information of someone else, and use this new identity to make false purchases and transactions. This is the most common type of payment fraud.
- **Friendly Fraud**: Sometimes, after having received a product or service, the customer will falsely initiate a chargeback and deny ever having received it. Not only do they get their amount refunded, but they also get to keep the product or service. This is also a prevalent type of payment fraud, and despite the name, it's anything but friendly.
- **Clean Fraud**: This type of transaction fraud is the hardest to detect. Fraudsters carefully analyze businesses' fraud-detection systems, and use stolen valid payment information to navigate around them.
- These are some of the most common ways payment fraud occurs. While it is not possible to completely eliminate these attacks, you can mitigate the risks of them impacting your business by taking the right steps. Let's look at some of them.

How do I reduce the chances of fraud affecting my business?

- **Monitor transactions carefully**: Make sure you monitor and verify all important information during a transaction, such as shipping address, IP address, amount, and date. This helps keep track of transactions and reduces the chances of any important detail being altered without you noticing.
- **Restrict access to confidential information**: By restricting access to confidential details, you'll be able to reduce the chances of any important information being leaked or accidentally landing up in the wrong hands. Only provide access to confidential information to people you trust, and employees whose role in your business requires them to have access.
- **Encrypt transactions and emails**: Encrypting any document before sending it to someone else ensures that the person can only view the document, and not manipulate or alter the data in it. This ensures that there is no chance of customers changing important information and using it for unethical purposes.
- **Avoid paper checks and invoices**: Apart from being a hassle, conducting business transactions and recording them on paper makes your information very susceptible to being stolen.

- **Use strong authentication procedures**: Using a multiple-factor authentication system further ensures no unknown individual can have access to your finances.
- **Keep up to speed on fraud trends**: It also helps to keep up to date on the latest types of fraud. With business functioning primarily online and becoming increasingly connected, fraudsters are always finding new and lucrative methods to obtain and use private information. It is in your best interest to ensure you stay on top of the latest kinds of fraud affecting other businesses around the world, so that you can implement the necessary security to protect your business from them.

What is ATM Fraud?

- ATM fraud is described as a fraudulent activity where the criminal uses the ATM card of another person to withdraw money instantly from that account. This is done by using the PIN. The other type of ATM fraud is stealing from the machine in the ATM by breaking in.

What are the various types of ATM frauds?

- **Card Shimming:** This is done by installing a foreign device, known as the shimming device, on the ATM machine for getting data from the card's chip. It can capture magnetic strip equivalent data.
- **Card Skimming:** This includes stealing the electronic data of a card in order to imitate the card completely. The customer will not realise until money is withdrawn from their account without their knowledge.

- **Card Trapping:** This includes stealing the ATM card by installing a device at the ATM. The card gets trapped in the cash dispenser. When you leave the ATM to receive help for getting your card out, the fraudster will enter.
- **Jamming of Keyboard:** The fraudster will jam important buttons on the ATM machine keyboard such as Cancel and Enter buttons so that the transaction is unsuccessful and the customer may leave the ATM to get help. The criminal then enters the ATM to withdraw money immediately from the machine as the details are already entered.
- **Phishing:** Card cloning or phishing scammers target all those people who get fooled, who are not careful in financial transactions, mostly, elderly people and women.

How to protect myself against ATM fraud?

- Avoid using ATMs in deserted regions.
- In case you are suspicious of any activity inside the ATM, then leave or complain.
- Check the card reader and see if any skimmer is attached to it.
- Look for hidden cameras in the ATM.
- If you see people loitering around the ATM, then it is better to not withdraw money from there.

What do I need to Know about ATM skimming?

- ATM skimming is done by placing a tiny device for stealing data from the card when it is being swiped. For this to work out, the criminal also needs to keep a camera inside the ATM or hack the bank camera for getting the ATM card PIN. Then the fraudster uses the details for cloning the card or for making online purchases.

How do i know if there is a skimmer in the ATM?

- You have to check the ATM machine very carefully. If the machine has a skimmer or has been tampered, you will notice that the card reader is extended a little more. Also, you may notice that the machine keypad is standing outside slightly. Look for glue, tape, or a pinhole camera in and around the machine to detect a skimming activity.

How does ATM skimming work?

- For ATM skimming, a fraudster uses a skimming device. This device typically has 2 parts. The first part of the device is a tiny one and is placed on the card swiping area.
- When the card is inserted, the skimmer will copy the magnetic strip data of your card. The other part is a tiny camera, which will click a picture of you keying in the PIN. Thus, the fraudster will use your card PIN and card magnetic chip data for making a fake card and use it in other ATMs to withdraw from your account.

What tips can i follow to prevent ATM card skimming?

- Take a proper look around the ATM machine to see if anything looks suspicious. Check if the card reader looks unusual or damaged.
- Examine the keypad of the ATM machine. If you think it’s too thick, then don’t enter anymore details.
- Do check your account frequently to be aware of withdrawals made by someone else.
- Cover the machine keypad when you are entering the card PIN.
- It is advisable to register for instant SMS updates to be aware of all your transactions. If someone withdraws without your knowledge, you can report fraud after you check your SMS.

What do I do if I have been skimmed?

- If you think you have been skimmed, you need to immediately contact your bank customer care centre. Once you report the crime, the bank will look into it and replace your card according to your specific situation. Moreover, the RBI has stated that the customer liability is zero if a third party has committed the unauthorised transaction. This is because the bank or the customer is not at fault. However, there are certain terms and conditions related to this. The bank executive will explain the procedure to you.

How does ATM Skimming Work

- For ATM skimming, a fraudster uses a skimming device. This device typically has 2 parts. The first part of the device is a tiny one and is placed on the card swiping area.
- When the card is inserted, the skimmer will copy the magnetic strip data of your card.
- The other part is a tiny camera, which will click a picture of you keying in the PIN. Thus, the fraudster will use your card PIN and card magnetic chip data for making a fake card and use it in other ATMs to withdraw from your account.

Internet banking frauds

- Internet Banking Fraud is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. Internet Banking Fraud is a form of identity theft and is usually made possible through techniques such as phishing.
- Now internet banking is widely used to check account details, make purchases, pay bills, transfer funds, print statements etc. Generally, the user identity is the customer identity number and password is provided to seure transactions. But due to some ignorance or silly mistakes you can easily fall into the trap of cyber criminals.
- Here are some simple tips to prevent you from falling into the trap of cyber criminals. Remember, a simple ignorance or oversight can make a huge dent in your hard- earned savings.

Securing your account

- Avoid online banking on unsecured Wi-Fi systems and operate only from PCs at home. Never reveal password to anyone. Do not even write it on a piece of paper on diary. Just memorise it. It should be alphanumeric and change it frequently.
- Never reply to queries from bank online about account or personal details. The personal information should not be kept in a public computer or in emails.
- Phishing: A person's personal details are obtained by fraudsters posing as bankers, who float a site similar to that of the person's bank. They are asked to provide all personal information about themselves and their account to the bank on the pretext of database upgradation. The number and password are then used to carry out transactions on their behalf without their knowledge.

- Phishing involves using a form of spam to fraudulently gain access to people's online banking details. As well as targeting online banking customers, phishing emails may target online auction sites or other online payment facilities. Typically, a phishing email will ask an online banking customer to follow a link in order to update personal bank account details. If the link is followed, the victim downloads a program which captures his or her banking login details and sends them to a third party.
- **Spam**: Spam is an electronic 'junk mail' or unwanted messages sent to your email account or mobile phone. These messages vary, but are essentially commercial and often annoying in their sheer volume. They may try to persuade you to buy a product or service, or visit a website where you can make purchases; or they may attempt to trick you into divulging your bank account or credit card details.
- **Nigerian Scam**: Nigerian or Frauds 409 or 419 are basically the lottery scam in which some overseas persons are involved to cheat innocent persons or organizations by promising to give a good amount of money at nominal fee charges. Their intention is to steal money in the form of fee against the lottery prize.

- **Spyware**: Spyware such as Trojan Horse is generally considered to be software that is secretly installed on a computer and takes things from it without the permission or knowledge of the user. Spyware may take personal information, business information, bandwidth; or processing capacity and secretly gives it to someone else.
- "Trojan Horse" scheme unfolds when malicious software (malware) embeds to a consumer's computer without the consumer being aware of it. Trojans often come in links or as attachments from unknown email senders. After installation the software detects when a person accesses online banking sites and records the username and password to transmit to the offender. People using public computers, in places like Internet cafes, are often susceptible to Trojans like malware or spyware.

Tips to get over Tele Banking Attacks

- Check sites
- Fool-proof password
- Always check 'last logged‘
- Keep your system up to date
- Public access can be injurious
- Follow Bank instructions

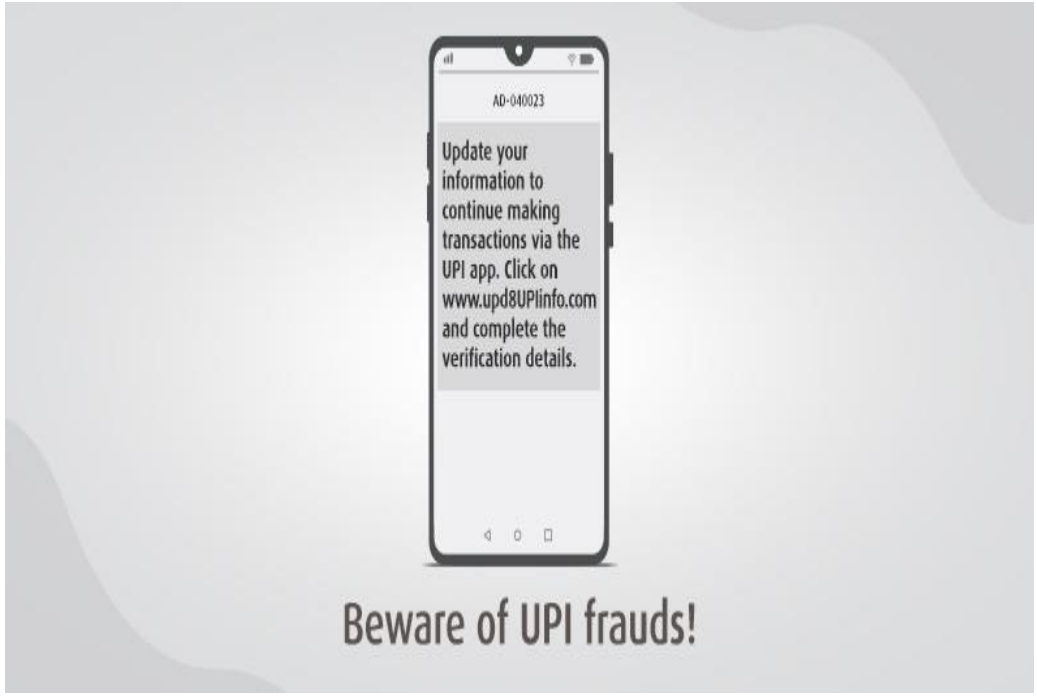
Mobile Money Transfer and E-Wallet Frauds

- With the growing number of online transactions, e-wallet frauds and online payment frauds in India are becoming widespread.
- Being able to avoid online payment fraud while using e-wallets or UPI apps has become very critical.
- As per the data provided by the National Payments Corporation of India, the total number of Unified Payment Interface (UPI) transactions made in February 2021 were a whopping 2.29 billion.
- With people resorting more and more to make payments via UPI apps and e-wallets in India, it has only given rise to more online fraud incidences.

What is the e-wallet and UPI app payment fraud?

Few Examples

- True fraud or identity theft
- This is when scammers get access to your financial information to steal money from your account or make unauthorised purchases.
- “Complete your ‘e-wallet name’ KYC or lose the money in your e-wallet account. Please call on 987******* and take action immediately.”
- “Update your information to continue making transactions via the UPI app. Click on www.upd8UPIinfo.com and complete the verification details. If not done within 24 hours, your account will be deactivated and you will not be able to carry out further transactions.”



- These messages tend to cause panic and the fear of losing money makes people do irrational things such as clicking on the unverified link and following the respective directions.
- These are common ways used by fraudsters to trick oblivious customers.
- Either they send a payment request via their UPI app that requires a UPI PIN or OTP or QR code scan or they send these ‘update your details’ threats to eventually get unauthorised financial access.

How are these frauds conducted?

- Online payment frauds in India, especially e-wallet frauds and UPI app frauds, are becoming very sophisticated as cybercriminals are building new ways and figuring out new mechanisms to target people. With more people transacting online, unscrupulous people are stooping to any level to obtain sensitive information from people. They do this via the following common ways:

Phishing cons

- Fraudsters send unauthorized payment links via text. These bogus bank URLs are eerily similar to the original website link making it easy for people to fall into this trap. Once permission is given to debit money, the amount gets deducted from the e-wallet or UPI app instantly.

Bank impostors

- Scammers pretend to be bank officials and rip off people by using an app to get remote access to a person's mobile phone screen. First, they give an excuse that the debit card is blocked or that the KYC is not up to date and then guide the gullible person, step-by-step and ask them to download an app on their phone. Since the screen has been shared, the scammer can monitor what the victim is doing, eventually gaining control of the device and stealing information.

Misleading UPI handles

- Many scammers create UPI handles with a valid name in them such as @paymentsBHIM_best or @disputesNPCI and people fall prey to this because the words like NPCI or BHIM exist and hence, believe these handles to be authentic. Scammers make you disclose your account details via a fake UPI app and then compromise the accounts.

Frauds that involve OTP, PIN, UPI

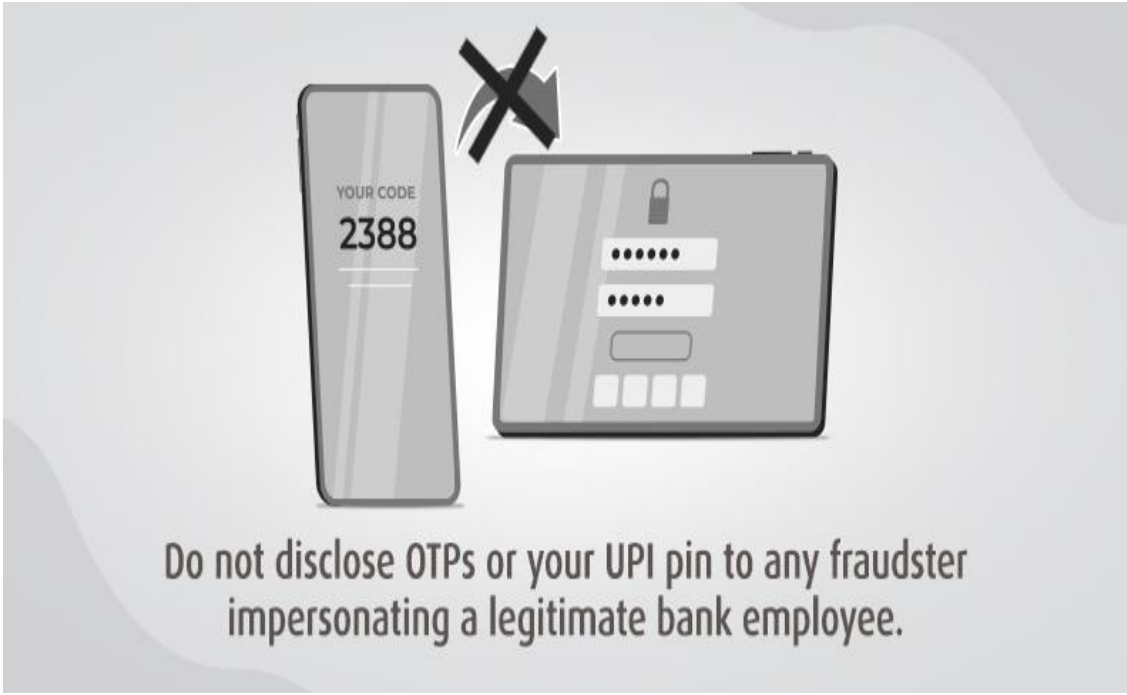
- When one transacts via a UPI app, an OTP or UPI PIN is required. Once either of the two is verified, the transaction is successful. This way to dupe people is one of the fraudsters' favourites. They have the skills to convince people to share either the UPI pin or OTP over the phone with them and through that, they can validate transactions and steal money. Always remember legitimate banks never call to ask for this information.

How to stay protected?

- There are a few tips and precautions that one can incorporate to prevent online payment fraud while using e-wallets and UPI. These include the following:

No engagement with strangers

- The first and foremost step is to not deal with unknown people online – be it via text, email, or phone. Often people pretend to be officials of reputed companies in the pretext of selling a loan, credit card, or updating KYC details. Keep in mind that any other legitimate bank will never ask you to disclose financial, personal or transactional details such as UPI PIN or OTP.
- If you do receive any communication from a stranger, call the organisation they are impersonating and validate everything being said by them. Better still, do not reply to an unknown email address or unknown phone number to avoid getting caught in their tricks.



Do not share OTP with anyone

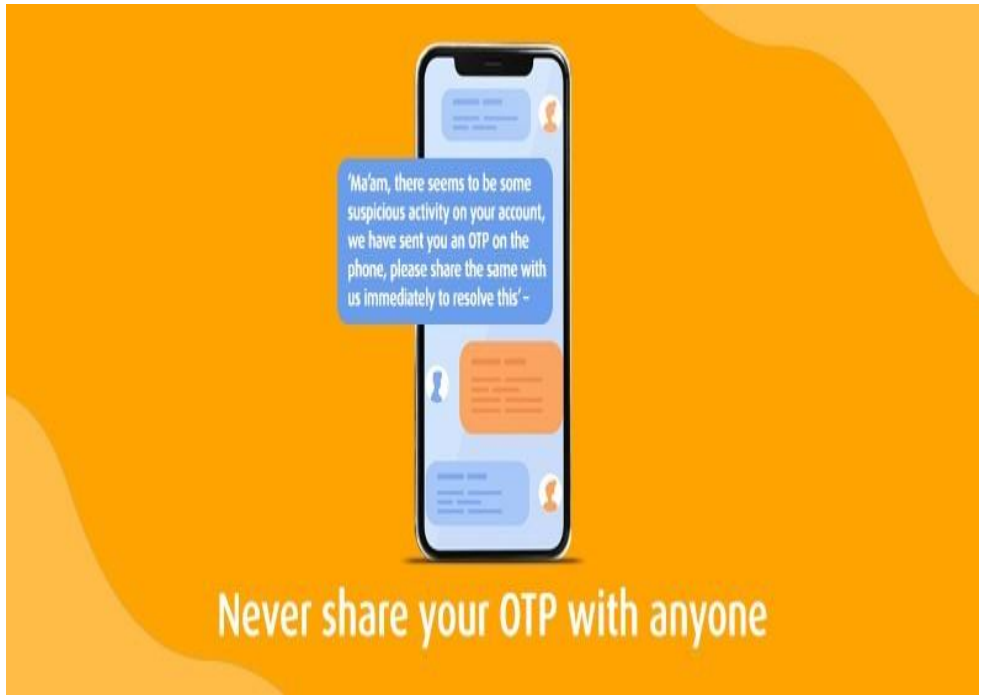
- One-time passwords are used by banks and financial institutions to authenticate transactions and unfortunately these have become the main entry-points for fraudulent activities online.
- Refrain from clicking on unknown links or accepting payment requests. Impostors very often send fake links that appear to be identical to the original links in order to obtain money unethically.
- One should under no circumstance click on a link sent by someone to proceed with a payment request unless it was initiated by you. Especially if you are supposed to receive money, you are not required to share your UPI pin.

Common Types of UPI Frauds and How to Stay Safe

- UPI is an easy way to facilitate inter-bank, person-to-merchant, and peer-to-peer transactions
- A common UPI fraud gets the target to download a screen mirroring app on the pretext of solving an issue and gaining full access to the phone
- Remember the golden rule – to receive the money, you never need to disclose your UPI PIN
- The world moving online has led to two things. On one hand, it offers convenience, ease of use and has become an imperative way of survival, especially owing to the pandemic. On the other hand, it opens up multiple avenues of cyber frauds such as UPI frauds, fake scams and bogus employment opportunities.

Common Types of UPI Frauds

- For those who aren't well versed with the concept of UPI, **Unified Payments Interface** was developed by NPCI to ensure real-time instant payment between banks. It facilitates inter-bank person-to-merchant and peer-to-peer transactions. While it is one of the easiest ways to receive and send money, learning and making ourselves aware of the common UPI frauds will help in being vigilant and steering clear of them.



Impersonating genuine sellers UPI fraud

- Sometimes people are in the habit of Googling a shopkeeper's number to reach out to them and order things. At times this number is that of an impostor who lists it under multiple businesses. After taking down your order, they ask you to prepay the amount via UPI and then no delivery ever reaches you.

Phishing UPI fraud

- Unsanctioned payment links that appear very similar to the original URL of the merchant are sent to the victim. When they click on the link, they are directed to the UPI app where they enter the PIN, thereby permitting auto-debit from the existing UPI app leading to unauthorized debit transactions.

UPI fraud via unauthorized access due to screen mirroring apps

- Fraudsters either reach out as bank employees or list their numbers as customer care numbers of legitimate companies on Google. The idea is to solve victim issues such as a complaint raised by the victim, KYC update, payment pending, etc. Once the victim and the fraudster connect, they are asked to download 3rd party apps such as **Any Desk and Team Viewer to address the grievance. These screen mirroring apps give the impersonators complete access to the victim's phone and they can carry out multiple unapproved financial transactions.**

The classic OTP, PIN UPI fraud

- These are widespread ways to con people across digital payment platforms from UPI to credit cards to e-wallets. People unknowingly share their UPI PINs or OTPs with scammers, who then gain unauthorized access to the victim's account.

UPI fraud via initiating a collect request

- Fraudsters use the collect request option to scam people into getting money into their accounts. They either say it is a debit reversal, refund or cite other reasons **and insist that the victims approve this 'Collect request' by entering their PIN to receive money.**

UPI fraud via misleading UPI handles

- Fraudsters **make fake UPI social media pages such as @BHIM2help or @NPCIDisputeTeam to reach out to customers who have complained** or asked queries on the actual UPI pages. They con customers on the pretext of grievance redressal and get them to give out personal financial information. People fall prey to these because they genuinely have posted queries and the handles are deceptive.

How to Stay Safe?

- This Financial Literacy Week is all about convenience of digital transactions, security of digital transactions and protection of customers, as per RBI's theme 'Go Digital, Go Secure'. The RBI guidelines for UPI frauds in banks, clearly state that while making UPI transactions, one should be alert. To receive a payment, no PIN is required. If you are being asked for a PIN or OTP, your account will be debited and you will be sending money. This is the golden rule of being paid via UPI.

- Secondly, be extra cautious while accepting payment requests. The 'collect request' feature on the UPI app is being misused by imposters, to siphon off money. Remember, if you are being asked to enter a PIN, you are sending money and not receiving, no matter how convincing the impostor sounds.

- Thirdly, be wary of fake apps. These malicious apps mirror your phone and give access to scammers to misuse it.

Thank You ! ! !