Azadi Ka Amrit Mahotsav

यूको बैंक UCO BANK
(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)
सम्मान आपके विश्वास का Honours Your Trust

यूको बैंक UCO BANK

Be Cyber Aware

An Internal Handbook on

Cyber Security Awareness

BY CISO OFFICE


Azadi Ka Amrit Mahotsav
यूको बैंक
UCO BANK
STAY VIGILANT
TODAY
TO SECURE YOUR
TOMORROW
CISO OFFICE

From the Desk of MD & CEO

Dear UCOites,

In today's digital age, safeguarding our organization from cyber threats has become more critical than ever. Our staff members are not only the backbone of our operations but also the first line of defense against cyber risks. This internal handbook on Cyber Security Awareness is a testament to our commitment to their empowerment. By being well-informed and proactive, we not only protect our data and systems but also preserve the trust our customers place on us. Together, let's embark on this journey of cyber resilience and ensure the safety of our digital ecosystem.

Best Wishes,

(**Ashwani Kumar**)
MD & CEO

यूको बैंक UCO BANK
(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)
सम्मान आपके विश्वास का Honours Your Trust

From the Desk of Executive Director

Dear UCOites,

In our journey through the swiftly transforming digital terrain, the significance of Cyber Security Awareness remains paramount and cannot be overstated. This handbook serves as a comprehensive guide to equip you with the knowledge and tools needed to detect, prevent, and respond effectively to cyber threats. By enhancing our collective awareness, we not only strengthen our Organization's defenses but also contribute to a more secure digital world. Let's embrace these insights and practices to protect our assets and uphold our reputation.

Best Wishes,

(Rajendra Kumar Saboo)
Executive Director

From the Desk of Chief Information Security Officer

Dear Colleagues,

In an era where technology is an integral to our operations, Cyber Security Awareness is imperative for the well-being of our Organization. This handbook embodies the culmination of our efforts to provide the insights into the realm of cyber threats and the strategies to counter them. Comprehension and vigilance play a vital role in upholding the integrity of our systems and data. As we internalize these practices, we not only shield our digital ecosystem but also nurture a culture of cyber resilience. Let's recognize the profound significance of our proactive involvement & extract the utmost advantages from this invaluable resource.

यूको बैंक UCO BANK
(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)
सम्मान आपके विश्वास का Honours Your Trust

With Regards,

(**Mohammad Sabir**)
DGM & CISO

Bank's Cyber / Information Security Policies & its importance

A good understanding of Information Security and Cyber Security policies and procedures of the Organization ensures:

- Protection to individuals from being victims of cyber security incidents
- Understanding the steps to follow in the event of a security incident
- Understanding the levels of responsibility
- Provides visibility on the risks associated with handling sensitive data and steps to be taken to avoid its misuse

Protect Organization from any form of threats, irrespective of the realm

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

What is Cyber Security?

Cyber Security is the protection of devices from malicious attacks & cyber threats. These devices include-

- Computer/Endpoint devices
- Servers
- Data
- Mobile devices
- Electronic systems
- Network devices

CISO OFFICE

Significance of Cyber Security in Today's Digital Landscape

Rising Threats: With increasing digitization, cyber threats have become more sophisticated and prevalent.

Corporate Image: Strong cyber security measures enhance the organization's reputation as a safe place for business.

Data Breaches: Protecting sensitive data from breaches is essential to maintain customer trust and regulatory compliance.

Innovation Acceleration: As technology evolves, cyber security becomes crucial for safe innovation.

Financial Impact: Cyber attacks can result in significant financial losses and damage to reputation.

Privacy Protection: Safeguarding personal information of employees and customers is a crucial and ethical responsibility.

Operational Continuity: Ensuring cyber resilience keeps operations running smoothly.

CISO OFFICE

What is Information Security ?

Information is a critical resource for an organization which needs to be protected throughout its life cycle.

- **Information Security is protection of information from 'Unauthorised'**
  - **Generation**
  - **Access**
  - **Modification**
  - **Disclosure**
  - **Transmission**
  - **Disruption and**
  - **Destruction**

CISO OFFICE

Principle of Information Security

The CIA Triad - upon which Information Security functions are based

Integrity

Accuracy and completeness

Ways to ensure Integrity:

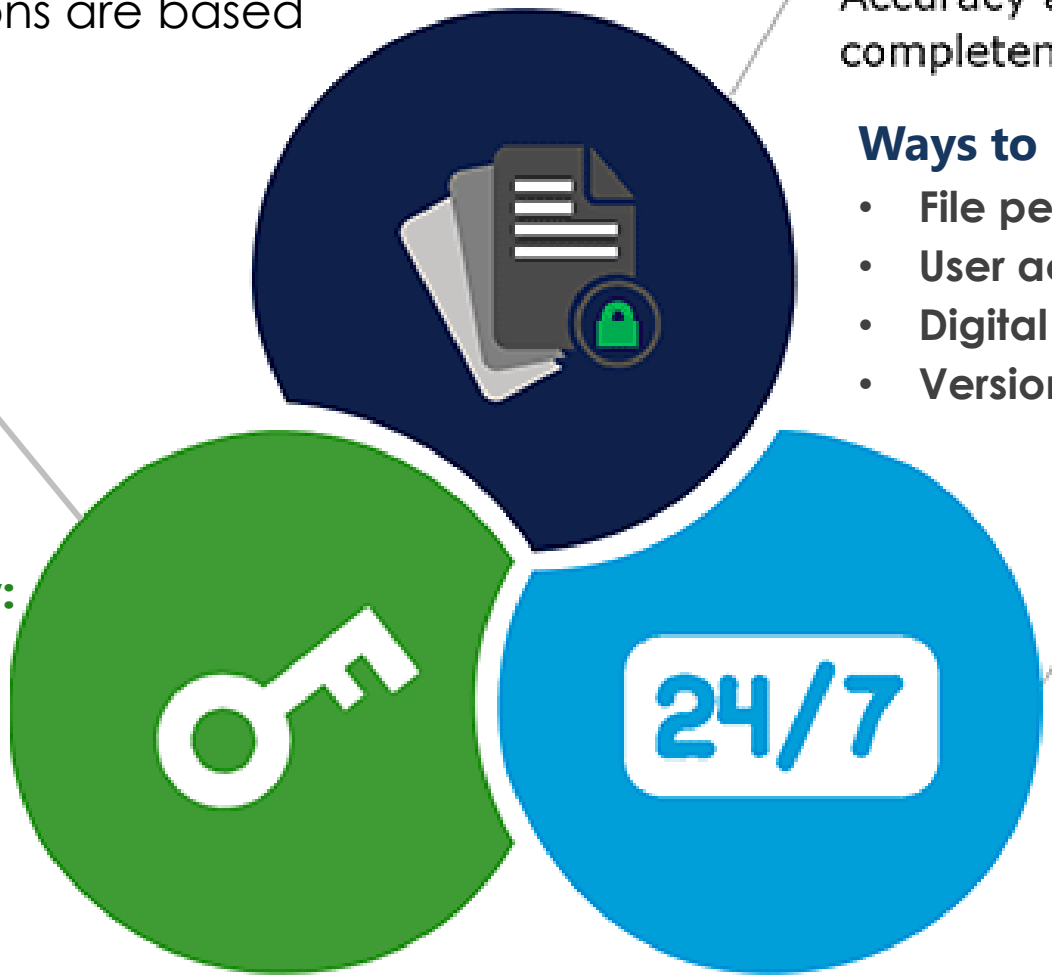
- File permissions
- User access controls
- Digital signatures
- Version Control

Confidentiality

Information is not made available or disclosed to unauthorized individuals, entities or processes

Ways to ensure Confidentiality:

- Authorisation via user id & password
- Biometric verification
- Multifactor authentication
- Data encryption



Availability

Ability of the system to provide access to its resources

Ways to ensure Availability:

- Off-site Backups
- Failover
- Environmental controls
- Redundancy

Data Classification & Secure Handling of Data

PUBLIC

Data that can be freely shared with anyone

Examples:

- Directories
- Press releases
- Mission statements

INTERNAL

Data shared within the organization

Examples:

- Work schedules
- Budgets
- Project plans
- Strategies
- Business processes

CONFIDENTIAL

Data shared with select internal individuals as needed for their jobs

Examples:

- Some regulated data
- Personally Identifiable Information (PII)
- Business details
- Personal Records
- Financial Information

RESTRICTED

Data that is highly sensitive

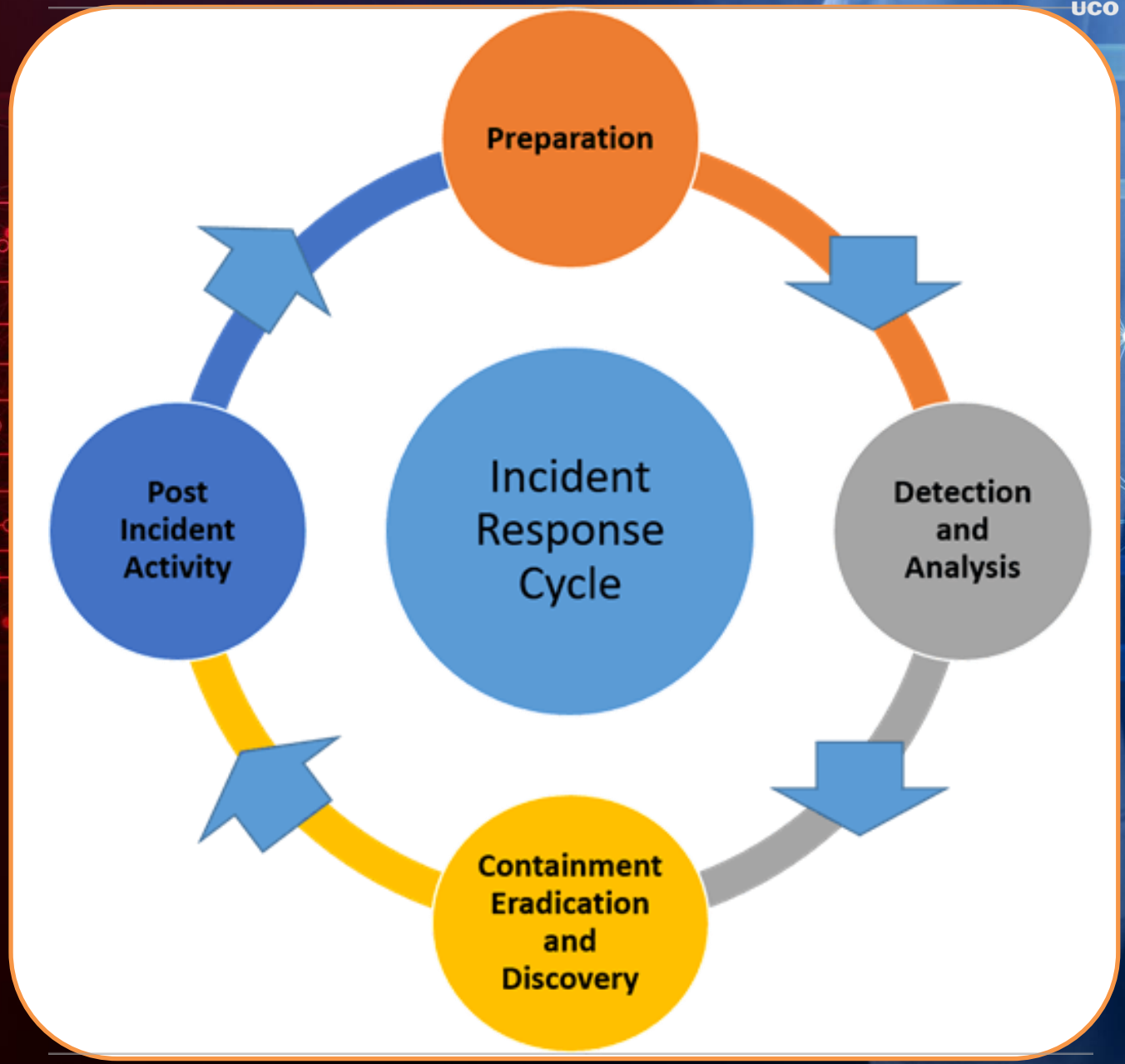
Examples:

- Passwords
- Some highly regulated data
- Internal Plans
- Infrastructural Information

CISO OFFICE

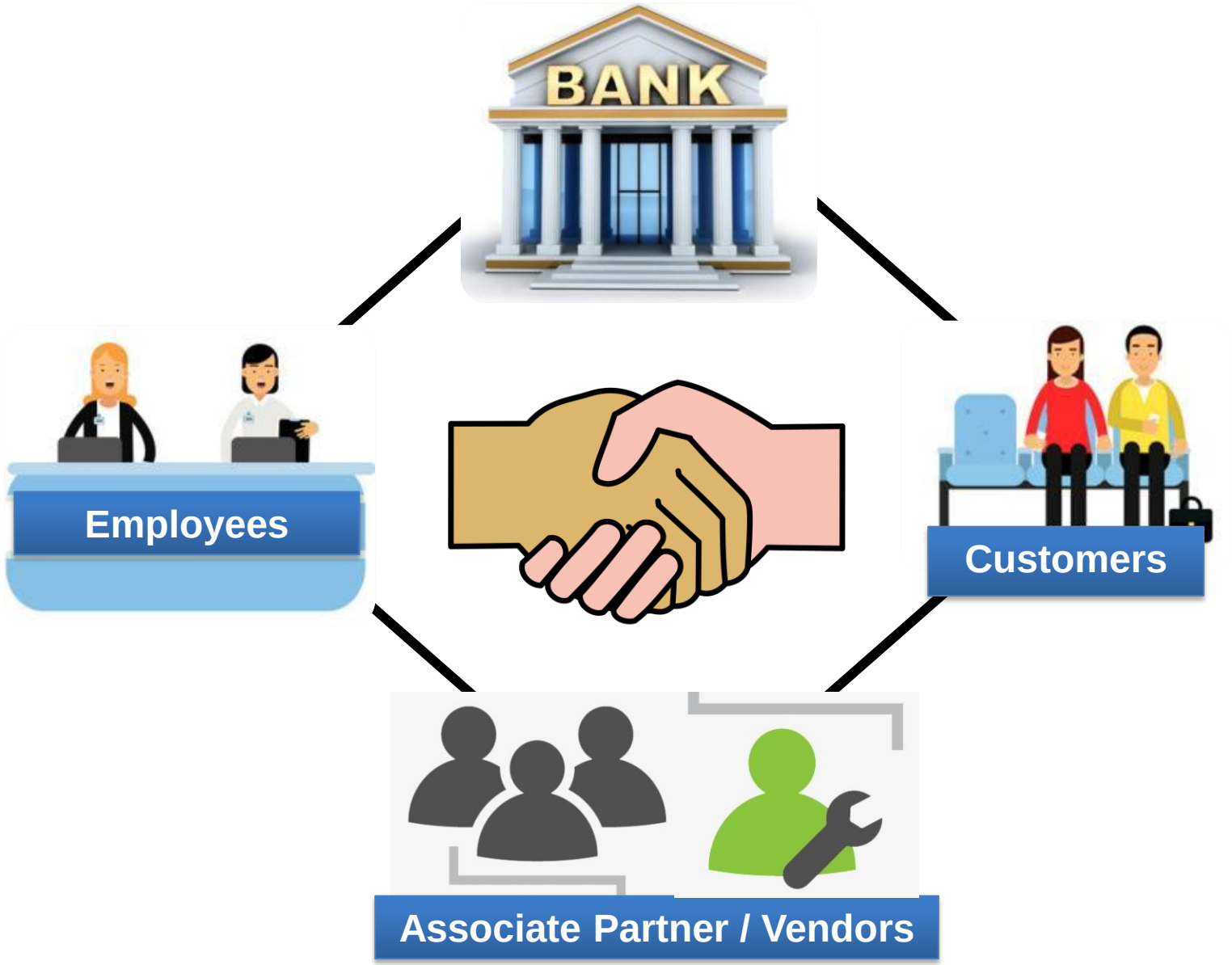
Cyber Crisis Management Plan (CCMP)

Outlines the stakeholders and actions required to ensure that cyber security events are addressed in a consistent, coordinated and timely manner.



CISO OFFICE

Cyber Security is Everyone's Responsibility



Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

In the modern era of digitization, with increased usage of internet & IoT devices, Cyber scams are also increasing rapidly.

So it is important to enhance our awareness on Cyber Security to defend such potential cyber risks arising out of human vulnerability.

CISO OFFICE

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

What is CYBER FRAUD ?

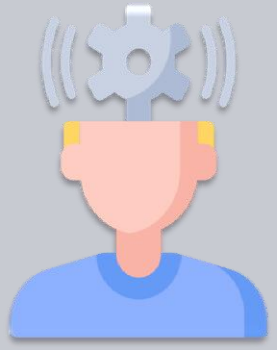
It occurs when someone defrauds people by using the internet / offline to get money, goods, etc. illegally by tricking them

CISO OFFICE

Why do we become Victims of Cyber Fraud?

Over Trusting Nature

Lack of Awareness



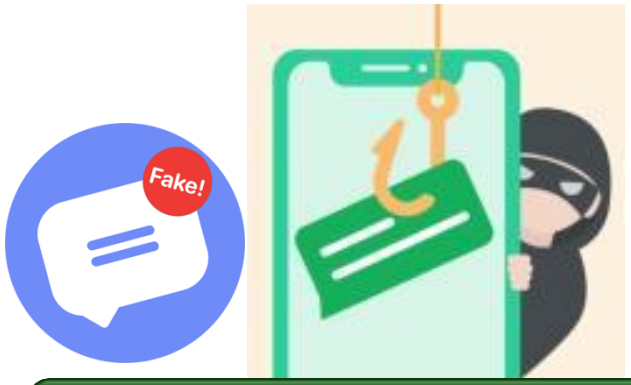
Psychological vulnerability like human emotions, fear etc

Least likely to report incidents

Common Modes used by Fraudsters

Fake Calls asking confidential information

Fake Emails with malicious links or attachments



Fake SMS Messages with Spurious Links

Luring Advertisements /Offers / News

Fake Websites for capturing sensitive information

CISO OFFICE

Cyber Threats & Attacks

Technology Driven Attacks
(Backed by Technology)

- Denial of Service Attack
- SQL Injection
- Man in the Middle Attack
- Advanced Persistent Threats
- Zero-day Exploit

Social Engineering Attacks
(Exploiting Human Elements)

- Phishing
- Malware
- Baiting

- Tailgating

- MINING SOCIAL MEDIA

CISO OFFICE

Social Engineering – Red Flags

Your 'friend' sends you a strange message.

Your emotions are heightened.

The request is urgent.

The offer feels too good to be true.

You're receiving help you didn't ask for.

The sender can't prove their identity.

Cyber Scams - Techniques

Remote Access Frauds

Now a days, Remote Access Apps like AnyDesk, TeamViewer, QuickSupport, MingleView etc. are misused by fraudsters to gather sensitive personal information of users

Frequently review App permissions & do not grant unwanted permissions to Apps which allow Remote Access

CISO OFFICE

Latest Techniques of Cyber Scams

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

BEWARE OF SMS FORWARDER APPS

Scammers can forward your OTPs into their devices by such Apps

Never install unknown Apps at the behest of any stranger & avoid clicking on suspicious links

Beware of FAKE Apps

- Never click on random links / "apk" files received from unknown sources/SMS/ WhatsApp
- Do not install unknown Apps at the behest of any stranger
- Do not grant unnecessary permissions to Apps
- Download apps only from trusted sources
- Uninstall the unused or unnecessary Apps at regular intervals
- Check online reviews & ratings before downloading the App

CISO OFFICE

Latest Techniques of Cyber Scams

Never search Customer Care or Helpline number on Search Engines or Social Media Sites

Always refer UCO Bank's Official website www.ucobank.com or contact Customer Care at 1800-103-0123

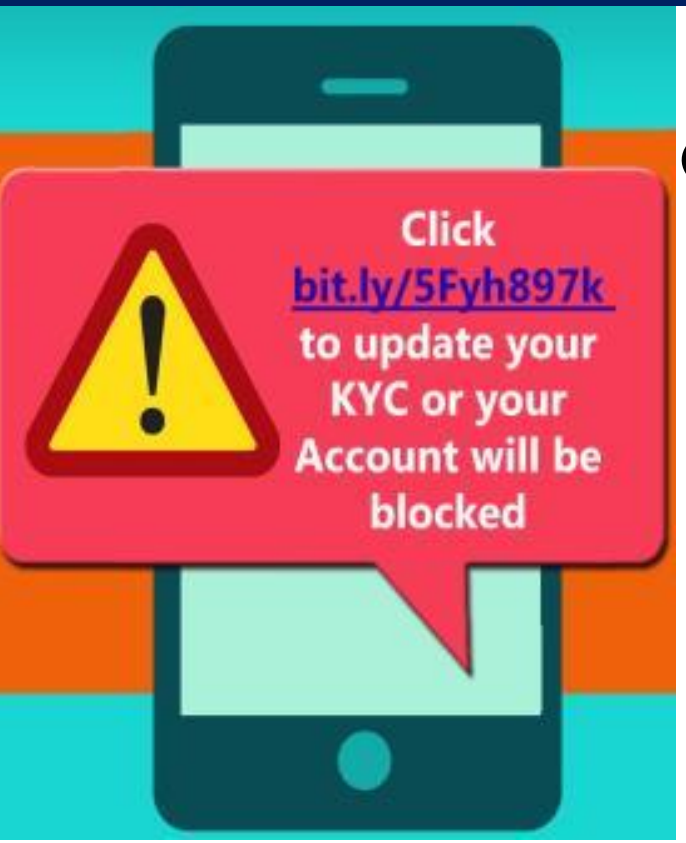
Never share OTP for parcel not ordered with anyone under any circumstances

Carefully read OTP messages which mention the reason for generation of OTP and the amount for which it is generated

CISO OFFICE

Few Latest Techniques of Cyber Scams

Fake Messages / Links



Always cross-check and confirm the KYC status by directly communicating with your Home Branch

Digital Payment Fraud

Scanning of QR Code or entering of UPI PIN is only required to make payment and not for receiving money

CISO OFFICE

Latest Techniques of Cyber Scams

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

Buying items through Online Marketplace Platforms like OLX, Quikr etc.?

BEWARE

Never pay advance money without seeing the item & always verify the seller by meeting in person

BE CAUTIOUS WHILE BOOKING HOTEL ONLINE

- ✗ **Do not trust unknown callers, random advertising links, messages etc. for quick & advance booking**
- ✗ **Never fall prey to deep discount offers which are too good to be true. Always check the authenticity of the company offering major discounts on hotel booking**
- ✓ **Visit official website / Apps of the hotel or reputable Tourism website for any type of advance booking**

CISO OFFICE

Latest Techniques of Cyber Scams

Be vigilant and skeptical about unsolicited emails claiming to be from the Income Tax Department

Do not click on any links provided in unsolicited emails. Always check the sender's email address carefully.

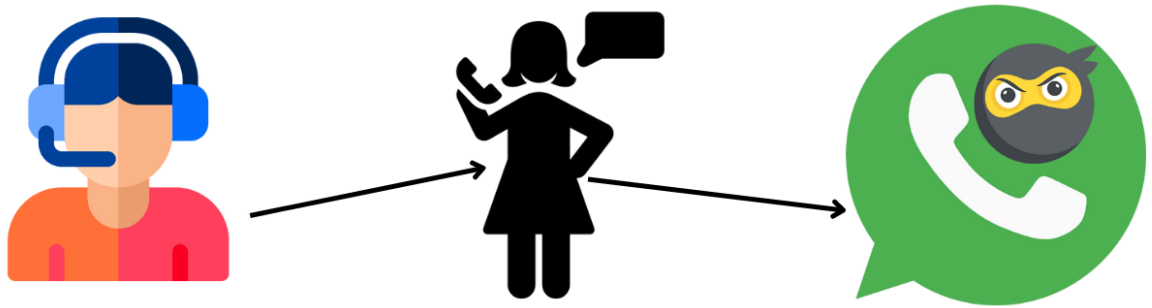
Do not respond/entertain calls from unknown International numbers particularly from countries like +84(Vietnam), +62(Indonesia), +223(Mali), GizChina etc.

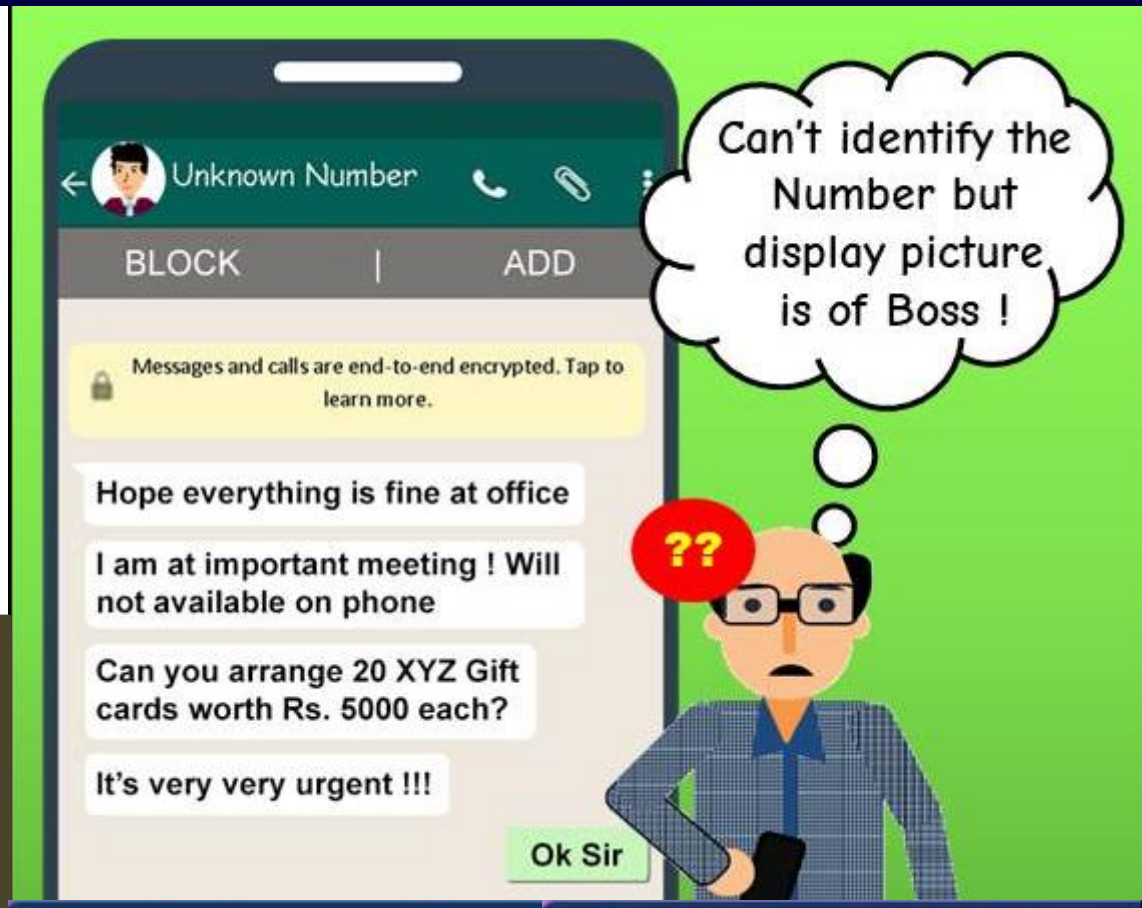
Block & Report such suspicious callers to avoid any potential cyber scam

CISO OFFICE

Call Forwarding & Impersonation Scam

Call Forwarding Scam hacks Whatsapp and asks for Money





- ✓ Never dial codes or send SMS from your number at the behest of strangers. Always check with your service provider before doing so.
- ✓ Be vigilant about call/SMS forwarding settings on your phone / SIM network service(s). If call/SMS forwarding features are enabled accidentally / unknowingly, immediately contact your mobile network provider (such as Jio, Airtel, etc.) from the official website / App to deactivate the same.

- ✗ Never trust messages from unknown WhatsApp number
- ✗ Don't build trust just by matching the display picture
- ✗ Never carry out monetary transaction at the behest of any stranger
- ✓ Always verify the authenticity of messages by calling person concerned or from known trusted sources

CISO OFFICE

Latest Techniques of Cyber Scams

CISO OFFICE

Beware of Task Based Job Offer through Video Liking

Never trust / respond to unknown messages offering easy make money for just clicking "like"

Avoid engaging in user prompted tasks/actions at the behest of any stranger

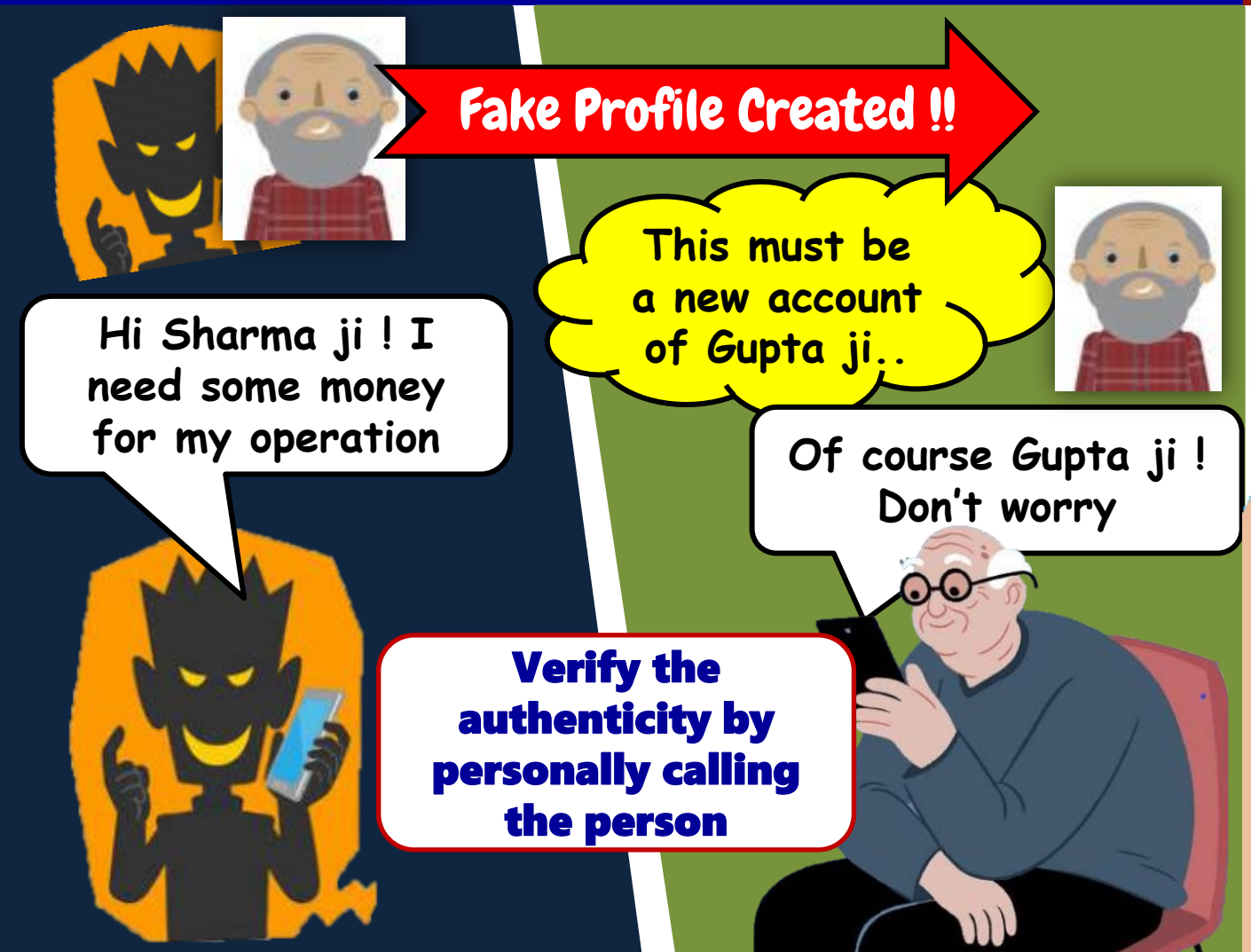
Always refer authentic job portals, official websites or apps for job related information

Beware of WhatsApp PINK Scam

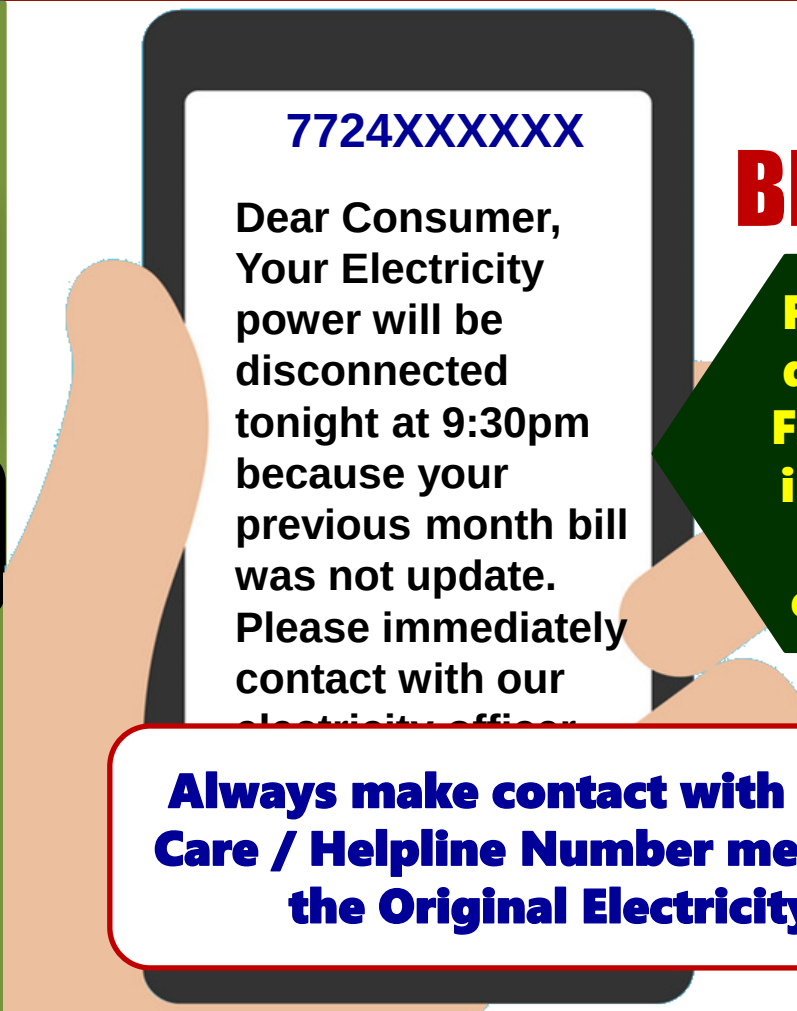
Refrain from downloading the fake (Pink) version of WhatsApp which may steal personal data, compromise device security, and lead to unauthorised access of the device

Latest Techniques of Cyber Scams

Scam through Social Media Channels



Bill Payment Scam



BE ALERT !

Fraudster may dupe you with FAKE messages in the name of unpaid electricity bill

Always make contact with Customer Care / Helpline Number mentioned in the Original Electricity Bill

CISO OFFICE

Beware of AI Generated Cyber Scams

Voice Phishing (Vishing)

AI-generated voice messages can mimic the voices of trusted individuals or organizations. These voice messages may prompt recipients to share sensitive information over the phone.

Chatbot Scams

Cybercriminals use AI-powered chatbots to impersonate customer support representatives or other legitimate agents, engaging victims in conversations that lead to disclosing sensitive data.

Malware Delivery

AI can automate the creation of malicious software, tailoring it to bypass security measures and exploit vulnerabilities in the victim's system.

Impersonation Attacks

AI-generated profiles and social media accounts can impersonate real people or entities, building trust to extract personal information, credentials, or financial details.

Deepfake Attacks

AI-generated deepfake videos or audio recordings can deceive individuals into believing they are communicating with a trusted source, potentially leading to financial loss or reputation damage.

Fraudulent Financial Transactions

AI-generated messages can manipulate victims into making unauthorized financial transactions by impersonating legitimate authorities or company executives.

CISO OFFICE

Deepfake Scams - Warning Signs & Precautionary Measures

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

Warning Signs

Caller's voice may sound different

Caller may ask for personal sensitive information

May request for money transfer, financial help, immediate action etc.

Inconsistencies in Speech like unnatural pauses, disjointed speech patterns, Distorted Audio or Visuals etc.

May show some abnormal behaviour or unnatural facial expressions

May not respond properly while discussing some personal matters / incident

- ✗ Do not transfer money without cross verifying the request from other trusted communication channel.
- ✗ Never share personal / sensitive information like Card Details, OTP, PIN, CVV, UPI PIN, Password, Financial Credentials with anyone.
- ✓ Look for inconsistencies, visual artifacts or anomalies that may indicate Deepfake signs
- ✗ Avoid oversharing information on social media and keep your profile privacy settings at the most restricted level
- ✓ Always cross-check information / media from official & trusted sources without blindly relying upon forwarded messages , online posts, advertisements etc.

CISO OFFICE

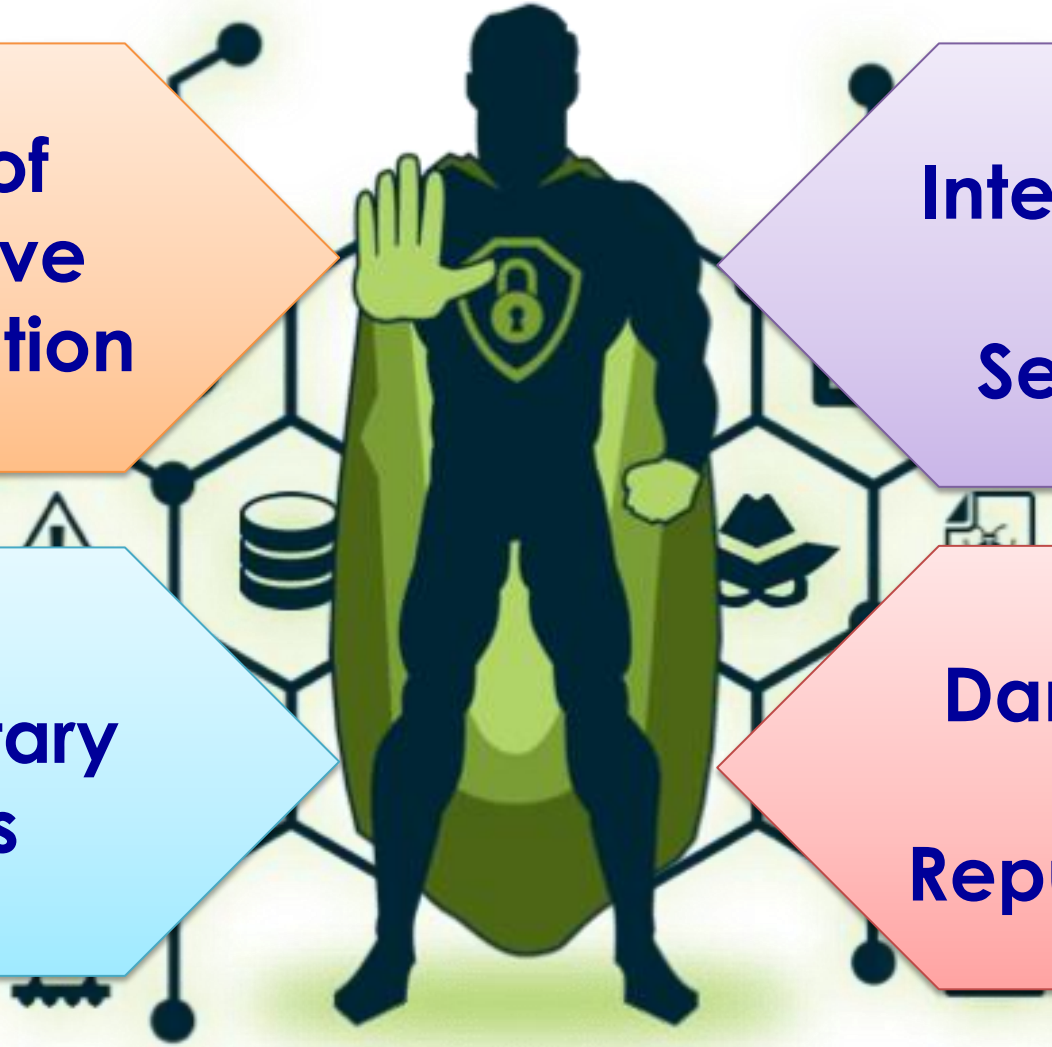
Potential Risks to the Bank – If not being Cyber Aware

Loss of Sensitive Information

Interruption of Services

Monetary Loss

Damage in Reputation



CISO OFFICE

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

How to become CYBERSMART ?

1. Follow Cyber Secure Culture at Workplace
2. Secure your Digital life with Cyber Safety Practices
3. Aware customers & citizens to develop a Cyber Secure Nation

CISO OFFICE

Organisation's Security Basics

ATM Security

Physical Security

Email Security

Clean Desk & Clear Screen

Password Security

CISO OFFICE

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

Physical Security

is the protection of people, property, and physical assets from actions and events that could cause damage or loss.

It includes -

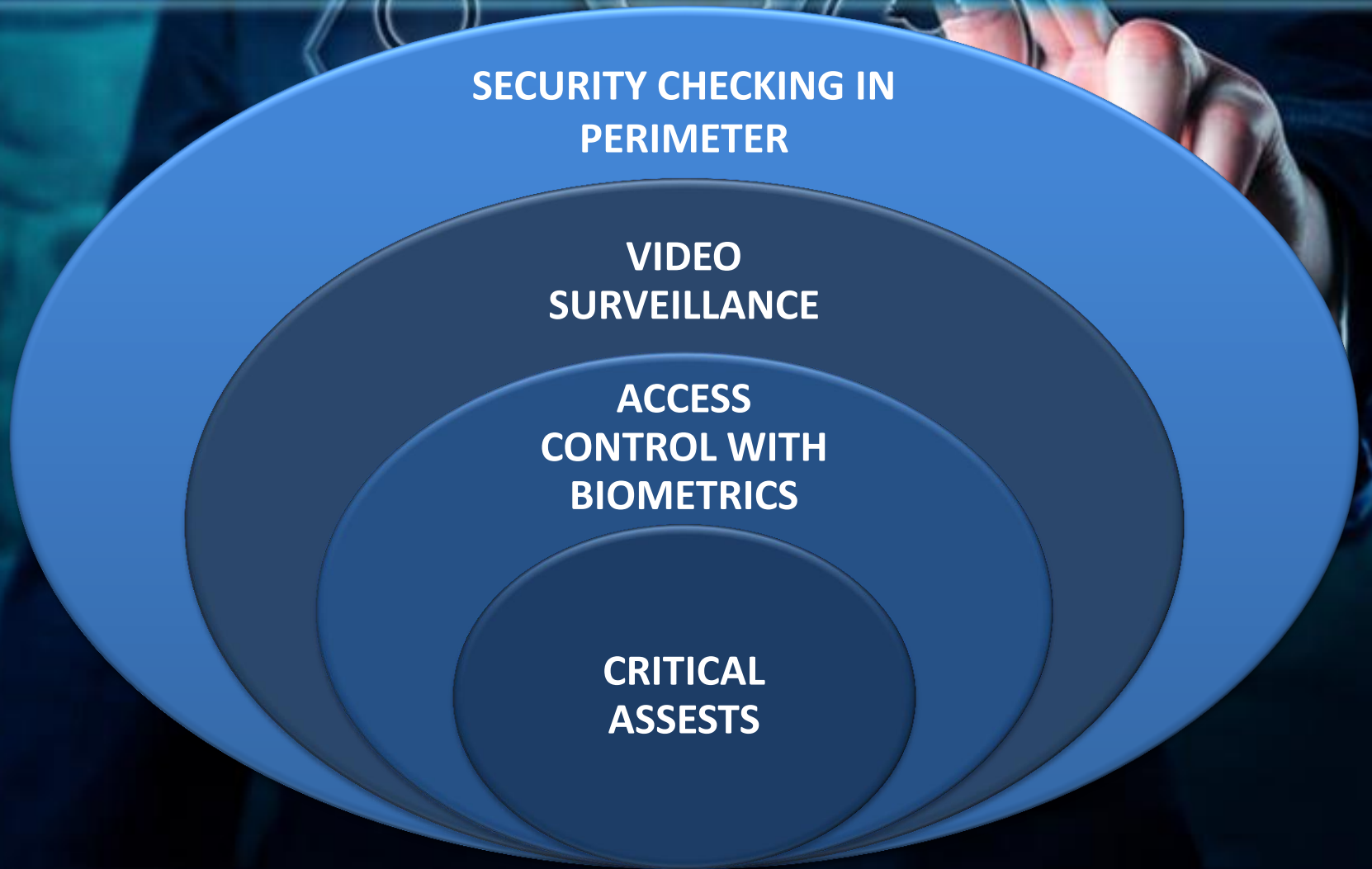
- ✓ **Physical Deterrence**
- ✓ **Intrusion Detection**
- ✓ **Intrusion Prevention**
- ✓ **Incidence Reporting**

CISO OFFICE

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

COMPONENTS OF PHYSICAL SECURITY



CISO OFFICE

Physical Security Best Practices

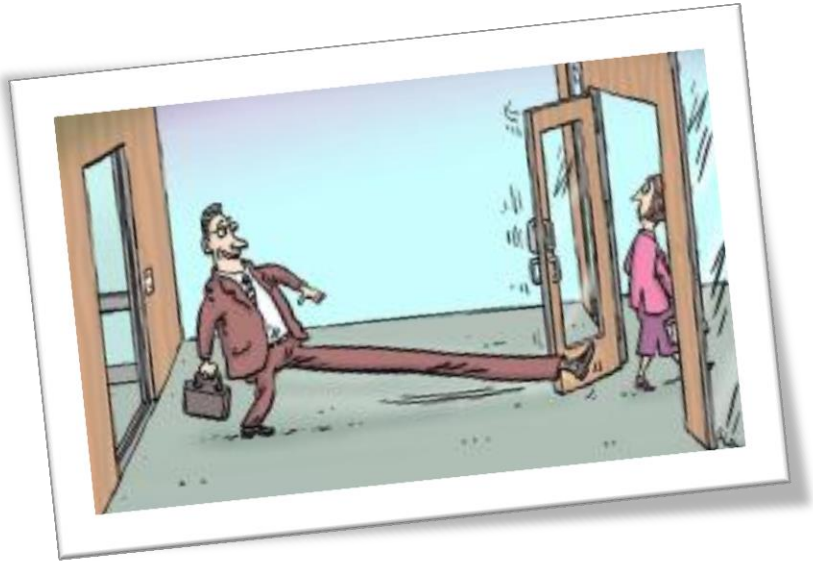
Security Guards at the door should be carefully monitor each person entering and leaving the Bank

CCTV cameras should be placed for proper monitoring of entrance at Branches/Offices, counters, ATM premises etc.

CISO OFFICE

Physical Security Best Practices

Beware of Tailgaters !



- Do not allow unauthorised person enter restricted area following you
- Control access to restricted areas by ensuring the door closes completely behind you when entering and exiting

Beware of Visual Hackers or Shoulder- Surfers !

- Look at your surroundings & guard the keypad while entering your Login Credentials like User Id, Password etc
- Never share your credentials not even with your colleagues or trusted one

CISO OFFICE

Clean Desk & Clear Screen Policy

A CLEAN DESK AND CLEAR SCREEN POLICY WORK HAND-IN-HAND TO SAFEGUARD ORGANISATION'S INFORMATION

Don't leave sensitive documents lying around. Store it securely

Clear sensitive documents from Printer immediately after printing

Keep sensitive documents locked away when not required

Shut down computer system before leaving

Lock your computer when not in use by Win + L key

Securely dispose of confidential data and file away all computer media in suitable locked cabinet

CISO OFFICE

Password Safety Practices

- Create complex passwords with combination of letters, numbers and special characters to prevent their guessing or cracking by fraudsters / adversaries
- Avoid using dictionary words, family name, vehicle number, personal or office information etc. in your password
- Change default password immediately & avoid setting passwords like Uco@..., Ucobank@... or any other passwords which can be easily guessed
- Never select 'YES' when any Application, Website, Browser etc. asks to remember your password
- Use different password for different account and change password at regular interval

CISO OFFICE

Email Security Best Practices

1. Do not open emails from unknown or untrusted senders.

4. Do not reply to suspicious requests.

2. Avoid responding or clicking links on unsolicited or spam email.

5. Do not rely on any information in the email from untrusted senders.

3. Do not open or download email attachment from unknown or untrusted senders.

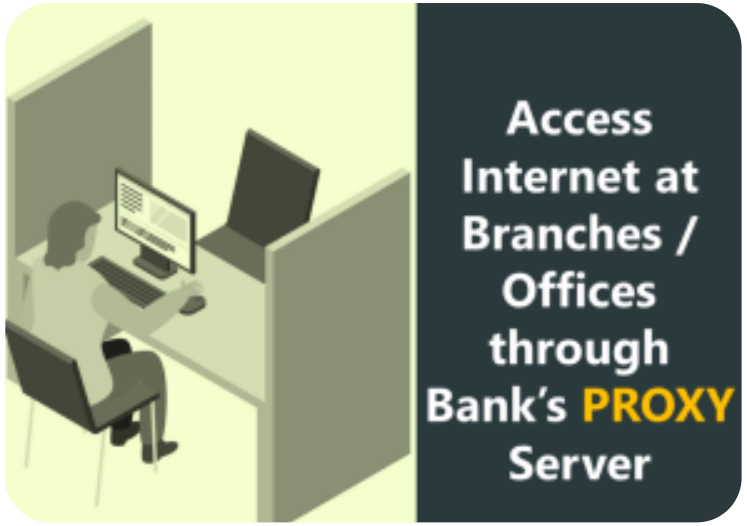
6. Do not share sensitive information through email.

CISO OFFICE

ATM Security Practices

- Allow only authorized person to enter the ATM room for installation and other related activities
- Ensure that the designated employee for ATM cash loading keep passwords safe and should not share it with anyone
- CCTV camera should be properly placed for proper monitoring
- Reconciliation should be conducted on daily basis
- Do not keep networking equipment like cables, routers, switches or any other hardware items left lying openly in publicly accessible locations. Shield network equipment's appropriately
- Ensure regular and proper disposal of trash cans from ATM room

Cyber Hygiene Practices for Endpoint Security



CISO OFFICE

WHAT IS PHISHING ?

It is a type of cyber-attack in which cybercriminals use social engineering techniques to trick people into divulging sensitive information, such as account & user/login credentials, Bank account numbers, Card Details, personally identifiable information, or any other information that could prove to be valuable to the attacker.

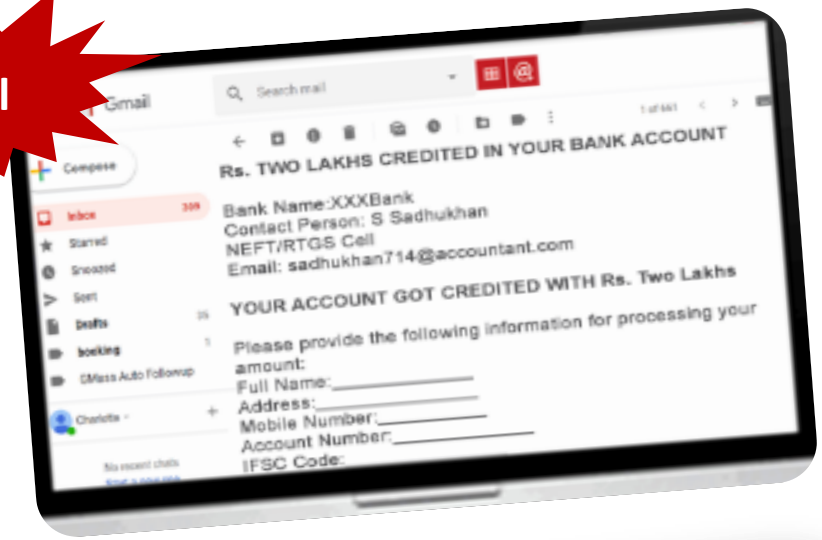
IT'S PHISHING, IF THE EMAIL:

- is sent from suspicious email address — *yourBank@ymail.com*
- asks for personal / sensitive information — *****
- has improper spelling / grammar — *you have not comfirned*
- includes suspicious links / attachments — CLICK HERE

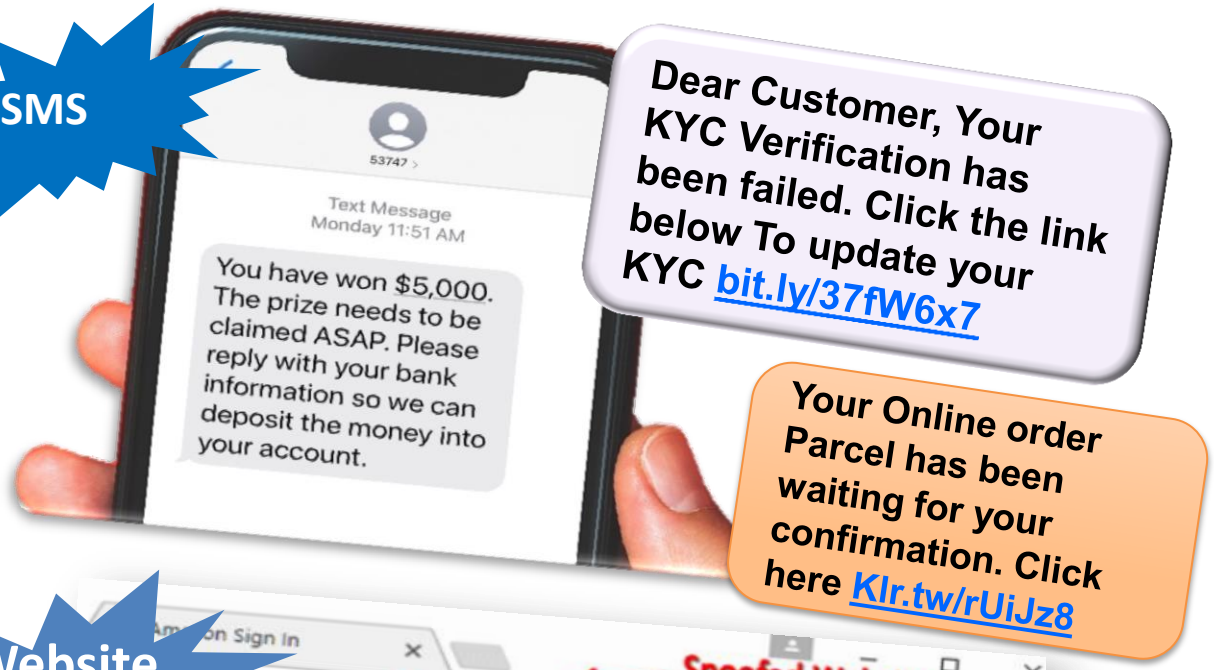
CISO OFFICE

Common Phishing Mediums

Email



SMS



Phone Call

Website Forgery

CISO OFFICE

Some Phishing Baits

SEEMS URGENT
By suggesting to do something immediately

PROVOKES FEAR
By threatening to face negative consequences

REQUESTS TO RESPOND
By asking personal information

TOO GOOD TO BE TRUE
By offering unusual lotteries or prizes

EXERCISING AUTHORITY
By impersonating as Top Management

Do not Click, Respond or Download !!!

Stop…  ***Think…***  ***Connect*** 

CISO OFFICE

Sample Phishing Email Indicators

1. 'EXTERNAL' indicator
2. Eye Catchy Subject
3. Suspicious email id
4. Correlate the Display Name & the email address. Claims as coming from UCO Bank's internal Dept.
5. Caution Alert
6. Attractive Offer
7. Includes Malicious Link
8. Calls for immediate action
9. Spelling Mistakes

[EXTERNAL]Greetings from Uc0 Bnak !

U

Uc0 Bnak Wealth Management Dept. <uc0bank.emp@uxcox.co>

To: Sugandha Sinha

**चेतावनी: यह ईमेल बाह्य डोमेन ("ucobank.co.in" से अन्य) से प्रेषित है। इसे या इसमें निहित संलग्नक खोलने से पूर्व इसके प्रेषक की विश्वसनीयता, वैधता एवं निरापदता सुनिश्चित कर लें । CAUTION: This email is received from outside of the "ucobank.co.in" domain. Do not click links or open attachments unless you recognize the sender and know the content is safe.

**

Congratulations ! Your branch / office has been selected for a **foreign trip** from Uc0 Bnak.

Click here to enrol the details as an acceptance to avail the foreign trip.

Enrolment link is open till **TODAY** .

Uc0 Bnak Wealth Management Dept.

CISO OFFICE

Sample Phishing Website Indicators

1 Not secure indicator - 'http'

2 Suspicious URL

3 Different Color of our Bank's Logo and wrong Hindi Tagline

4 Multiple Spelling Mistakes

5 Asking for Sensitive Info

CISO OFFICE

PREVENTION AGAINST PHISHING

Best Practices

- Always ignore suspicious calls, messages, emails or links
- Avoid clicking on unknown links & do not open or download unknown attachments / files from untrusted sender
- Examine Email / SMS sender address closely. UCO Bank's Official Email domain is " @ucobank.co.in " & legitimate SMS sender address will contain "UCOBNK" / "UCOPPC" / "UCORWD"
- Never reveal any personal / sensitive information on random websites, forms, documents or at the behest of any stranger
- Do not fall prey to attractive offers, deep discounts etc. which are too good to be true

CISO OFFICE

Azadi Ka Amrit Mahotsav

BEWARE OF VISHING

यूको बैंक
UCO BANK

Never share sensitive information with any unknown caller at any circumstances

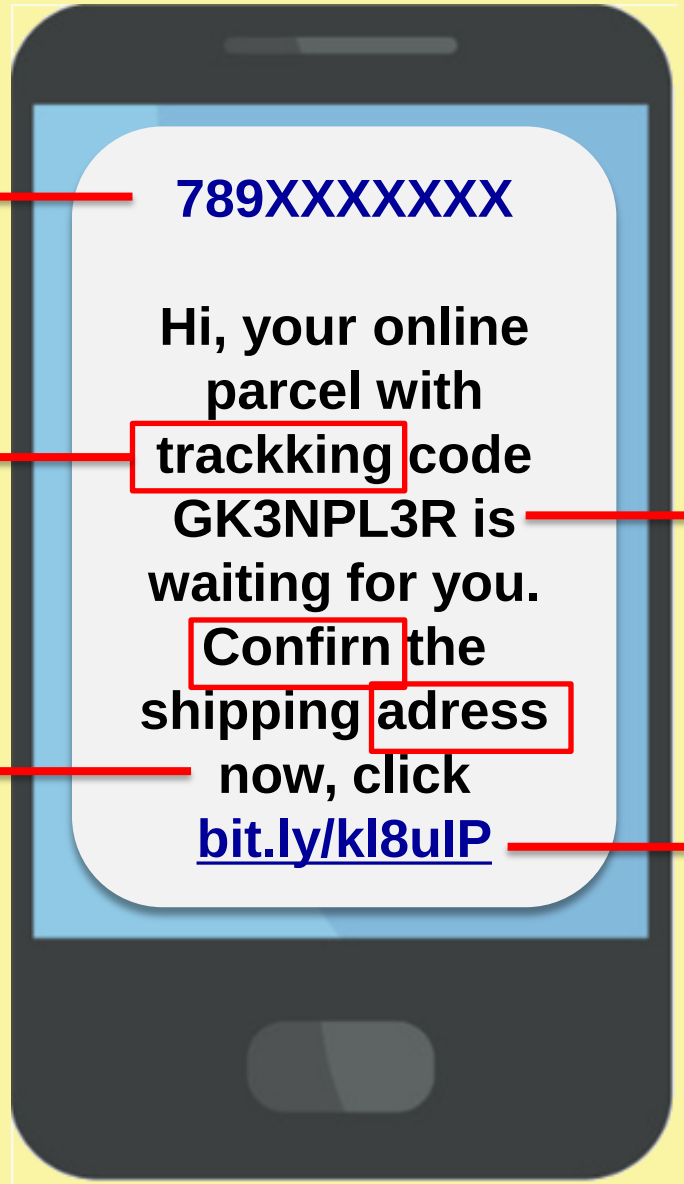
CISO OFFICE

SPOT FAKE SMS INDICATORS

Suspicious sender with ten (10) digit mobile no.

Spelling or grammatical errors

Sense of urgency



Unexpected message

Malicious link

CISO OFFICE

Secure Your Mobile Device

- Use strong passwords
- Avoid Public Wi-Fi
- Update Regularly
- Use Antivirus
- Always lock device when not in use
- Download Apps from reputable sources

CISO OFFICE

Safety Practices while using UPI

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

Enter UPI PIN only to make payment, not to receive money

Never share UPI PIN with anyone under any circumstances

Never approve payment request / fund transfer request from unknown UPI id

Never scan QR code for receiving money, it needs to be scanned only for making payments

Never download third party Apps from untrusted sources for UPI

Always refer Help section on the official App for assistance

CISO OFFICE

Secure Browsing Practices

- Always check for “https” & padlock symbol in the URL
- Keep browser Up-to-date with the latest patches
- Make a habit of browsing in Incognito or Private mode
- Clear browsing history, cookies, temporary files etc regularly

CISO OFFICE

Secure Your Biometric Information

Lock your Biometrics and Aadhaar through Official UIDAI website or the mAadhaar App

Generate the 16-digit Virtual ID (VID) number from official UIDAI website & use it in the place of original Aadhaar number

Generate and use 12-digit Masked Aadhaar from UIDAI portal to protect your Aadhaar information

CISO OFFICE

Secure Your Biometric Information

Never reveal your Biometrics, Aadhaar or OTP etc. at unknown or unauthoried places including Social Media

If mobile number, email id etc. which are linked with the Aadhaar are changed/modified, update them at UIDAI portal or by visiting nearest Aadhaar Enrolment Centre

Frequently check UIDAI portal to verify your authentication and implement new security features if introduced

CISO OFFICE

Tips to protect your PASSWORD

यूको बैंक
UCO BANK

Password are like socks, change them regularly

Never write passwords on paper or on devices

Memorize your password

Beware of Shoulder Surfers at public places while entering passwords

Making password complex increases difficulty of attacks & are hard to guess

Use different passwords for different accounts

Passphrase
My Car is Blue
Password
mYc@Ri5b!Ue

If hard to remember password, switch to passphrase

Never share password with anyone

ESSENTIALS FOR A SAFE HOLIDAY TRIP

- ✓ To book hotel online, always refer official website/App of the hotel or use reputable travel website / platform
- ✓ Avoid social media posts sharing location while traveling
- ✓ Never use free or public Wi-Fi network for doing financial transaction
- ✓ Carry your own charger and power bank while travelling
- ✓ Turn off bluetooth / NFC when not in use

CISO OFFICE

Cyber Security Best Practices for Prevention against Identity Theft

- Do not reveal sensitive / personal / financial information over unknown call, SMS, email etc
- Avoid sharing personally identifiable information on social media
- Avoid connecting devices with public / untrusted network
- Regularly update software / apps with latest patches
- Before disposing electronic devices, securely delete stored data/files

Be Cautious of URGENT HELP Request from stranger on Instant Messaging Platform !!

Do not entertain any urgent request from stranger for financial assistance. Always verify the sender's identity through alternative communication channel before taking any action.

CISO OFFICE

Preventive Measures against Malware Attack

PROTECT YOURSELF

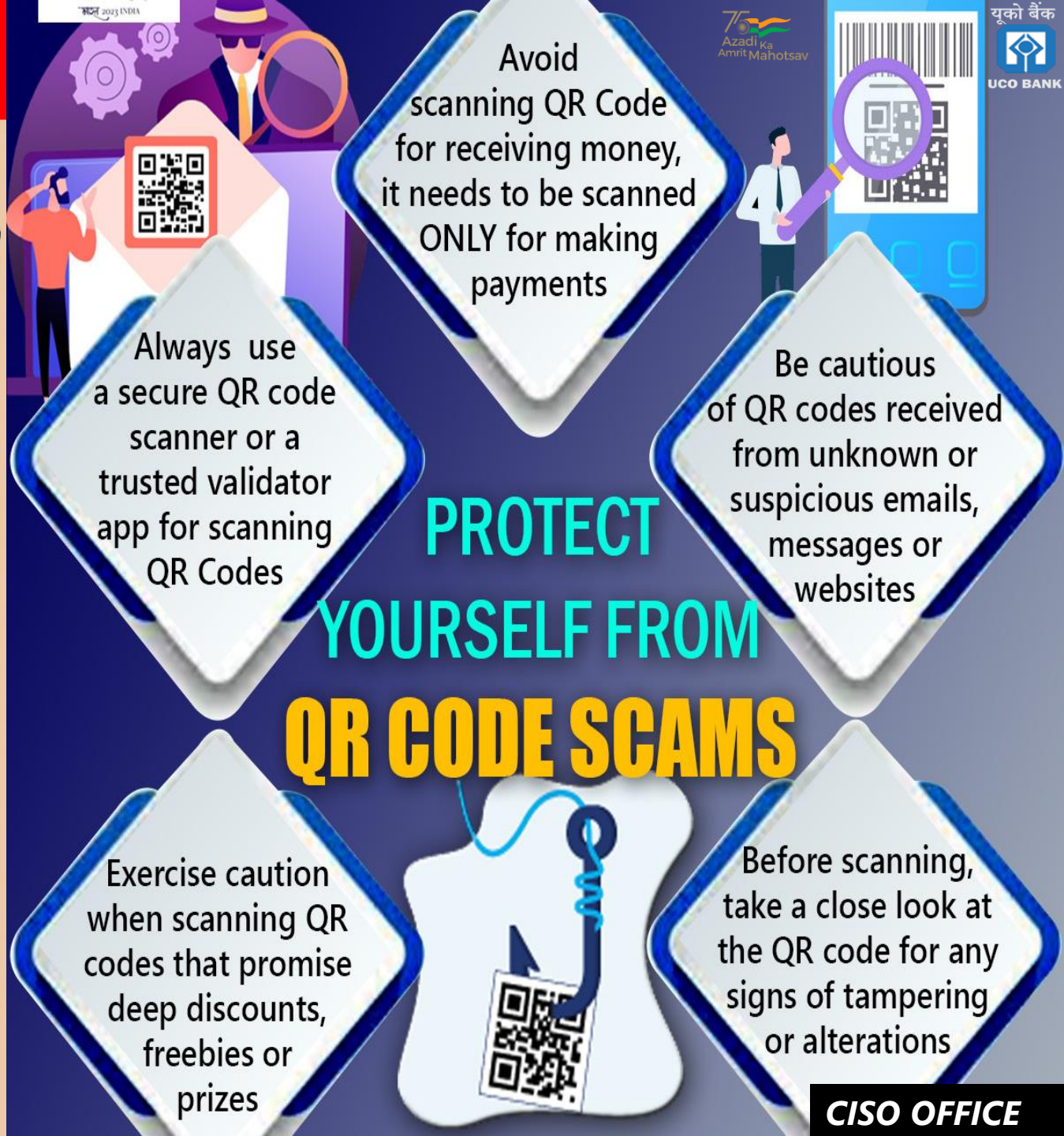
Keep OS & Apps software up-to-date with patches and fixes

Disable running executables from unconventional paths

Be cautious while opening email attachments & avoid clicking on unknown link

Never download software / apps from unknown or untrusted sources

Use a reputed Antivirus / Anti-malware solution for your devices & perform scanning regularly




Azadi Ka Amrit Mahotsav
THINK TWICE..
NEVER PAY THE PRICE !!
Don't fall prey to offers of unrealistic lucrative deals which are too good to be true
95 OFF %
Please verify details before getting engaged
USER CAUTION IS SUGGESTED


Be Cautious of Fake Apps offering Easy Money Earning !!
Refrain from installing suspicious apps which promise easy & quick high returns of your investment


यूको बैंक
UCO BANK
Be Cautious of
Fake Medicines Sold Online
Never fall prey to lucrative offers / deep discounts on social media platform for buying online medicines. Always shop online medicines from trusted websites / apps.


NEVER CLICK ON RANDOM POP-UP ADS
Visit the site
CLICK HERE!!
Click here to free download!!
Visit the site now!
CLICK HERE!
Click here to get your bonus!! Click for free
AD!
Visit the site to get 50% discount for all items
CISO OFFICE


9:07 AM
+91 XXXXX XXXXX
TODAY
Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.
Hello
8:45 AM
Forwarded
MygameAp .apk
4.1 MB APK
8:47 AM
Beware of random "APK" files
Never download Application or document by clicking on random "APK" files received on WhatsApp / SMS / Email.
Download Apps only from trusted sources


Enable Multi-factor Authentication (MFA)
Get THREE Benefits
1
Provides additional layer of Sign-in security
2
Protects sensitive data / information
3
Reduces the risk of security breach

EMAIL APPEARING FROM UCO BANK ??

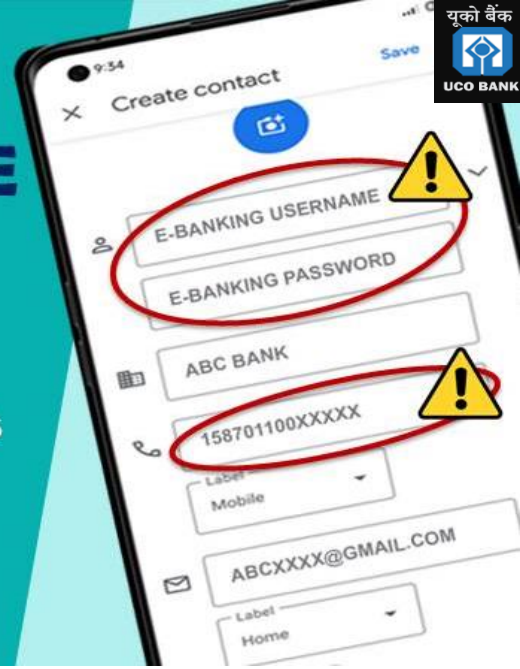
Before responding, Examine email address closely even if the mail appears to be from UCO Bank

KEEP YOUR INFORMATION SAFE

Never save any sensitive information like

- Bank Account number
- Debit/Credit Card details
- Financial Credentials
- Aadhaar / PAN etc.

as 'CONTACT List' in your mobile device.



Beware of Juice-jacking

Malicious USB port or cable can load malware to the smartphone and intercept data from the device

AVOID

Charging mobile phones using public USB ports or cables at public places

ALWAYS

Carry your own charger or power bank for charging

Blind trust is a dangerous step to take

Sharing your sensitive financial details with anyone may lead to financial loss !!

Never share your:

Card Details | PIN | OTP
Password | mBanking PIN | UPI PIN
| Bank Account Details

Over Phone | SMS | Email | WhatsApp | Social Media

CISO OFFICE


https://w .fcebook.com
"AVOID PHISHING ATTACKS"
VALIDATE THE URL
FOR THE WEBSITES YOU ACCESS BEFORE PROVIDING YOUR PERSONAL DATA


यूको बैंक
UCO BANK
YOUR FILES HAVE BEEN ENCRYPTED!
RANSOMWARE !!
A malware that encrypts data & demands money or ransom in exchange
Never click links or download attachments from unknown or untrusted email
Keep Operating System & Antivirus up to date with latest patches & fixes


Stay Cyber Secure
Safeguard yourself from cyber scams based on human overtrusting nature, emotional manipulation & sympathy exploitation by strangers
Be skeptical about emotional appeals from unknown individuals requesting for urgent financial assistance
Never give away money to any unknown person without verifying the original identity from known trusted sources
Avoid sharing personal or financial information with anyone or in random websites or social media platforms


Be Careful while using FREE / Public Wi-Fi
FREE
WiFi
Cybercriminals often spy on public Wi-Fi network & intercept data which are transferred across the network
Never use free / public Wi-Fi networks while doing online transactions
Always choose a secured or trusted Wi-Fi connection


Searching for FREE Downloads ??
Free Downloading software may contain Malware which can damage devices or may steal data
Download Free NOW!
SAFE DOWNLOAD TIPS
Never download cracked or pirated software and files
Download only from reputable sites and sources
Avoid downloading files with malicious extensions like ".exe", ".scr" etc.
Read user feedback, reviews, ratings etc. before downloading software


SMARTWATCH SECURITY
Update your Smartwatch Software / Apps
Lock your device by using multiple layers of security like PIN, Pattern Lock etc.
Be careful about the Apps you download & Always download Apps from trusted sources
CISO OFFICE

Online Shopping Safety Measures

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

Do not fall prey to deep discounts on random websites/ads which are too good to be true

Avoid saving your card details or bank details on random websites / apps

Check terms and conditions to ensure the product has clear return and refund policy

Read customer reviews, ratings about products and vendors

Use only trusted or reputed online shopping sites / Apps

Always log out after completion of the session

CISO OFFICE

BE SOCIAL but BE SAFE !!

- Block profiles from public searches
- Log out after completion of each session
- Never share credentials with anyone
- Avoid mentioning home or work address
- Be careful while accepting friend request from stranger
- Never click on suspicious links
- Keep the profile privacy settings at the most restricted level
- Limit your share & be cautious about what you are sharing

CISO OFFICE

How to Hotlist / Block UCO Bank Debit Card ?

Call **1800-103-0123** (toll free) from the registered Mobile Number

Email at **uco.custcare@ucobank.co.in**

Send SMS at **9230192301** from the registered Mobile Number

Format: HOT<space><last 4 digit of card no.>

Or HOT<space><14 digit account no.>

Download **UCO Secure App** or **UCO mBanking Plus App** from Play Store/App Store & go to "**Manage Card**" section

STAY UPDATED

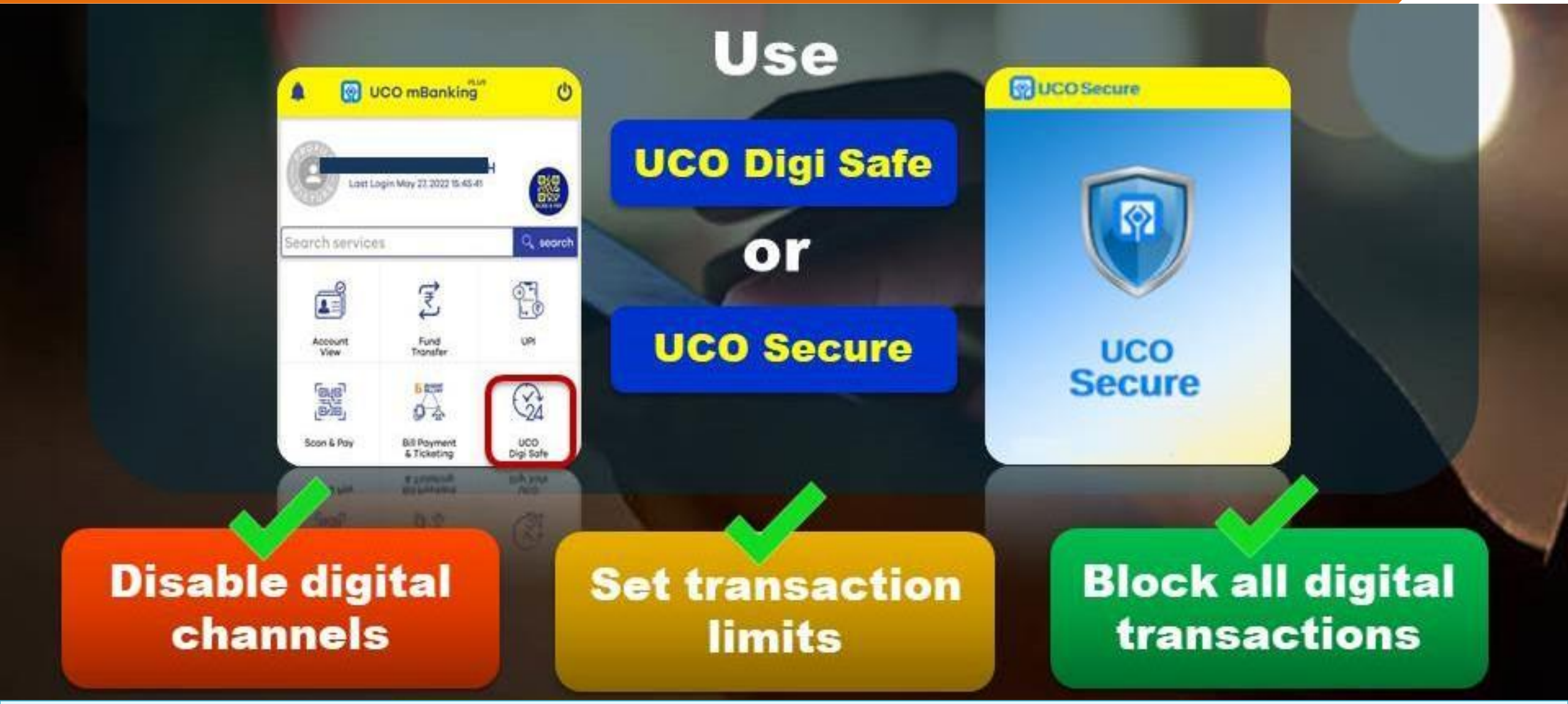
with all UCO Bank updates and offers

BY FOLLOWING US ON SOCIAL MEDIA!

official.ucobank | official.ucobank | UCOBankOfficial | company/uco-bank | UCO Bank Official

CISO OFFICE

Secure Your Digital Transaction



BE SAFE.. BANK SAFE..

CISO OFFICE

Reporting of Cyber Incidents

In case of occurrence of any Cyber Incident like Phishing Email, Virus, Ransomware etc, report immediately to

CISO OFFICE

Email: ciso.office@ucobank.co.in

CISO OFFICE

BE A HUMAN FIREWALL & CYBER JAGROOK

Azadi Ka Amrit Mahotsav

यूको बैंक
UCO BANK

NEVER BE THE WEAKEST LINK IN THE SECURITY CHAIN !

TAKE THE RESPONSIBILITY TO SAFEGUARD INFORMATION ASSETS FROM DISCLOSURE, ALTERATION & DISRUPTION

UCOite

STAY AWARE..
..STAY SAFE

CISO OFFICE

यूको बैंक
(भारत सरकार का उपक्रम)

UCO BANK
(A Govt. of India Undertaking)

सम्मान आपके विश्वास का

Honours Your Trust

यूको बैंक
(भारत सरकार का उपक्रम)
UCO BANK
(A Govt. of India Undertaking)
सम्मान आपके विश्वास का
Honours Your Trust

यूको बैंक
UCO BANK

Cyber Security is our shared Responsibility

BE CYBER SMART

CISO OFFICE