CSOC
साइबर सुरक्षा संचालन केंद्र
Cyber Security Operations Centre
CISO OFFICE

Cyber Safety Booklet

FOR THE YOUNG CYBER WARRIORS

CISO OFFICE

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

ABOUT THE BOOKLET

Greetings from UCO Bank

In today's world, the internet and smartphones have become like our best buddies, helping us connect with friends, learn new things, and have fun. But, just like we take care of ourselves in the real world, it's important to be cautious and smart in the online world too.

Imagine your online life is like a garden, full of flowers (fun stuff) and some thorns (cyber threats). This ***Cyber Safety Booklet*** is your guide to help you enjoy the digital garden while avoiding those thorns.

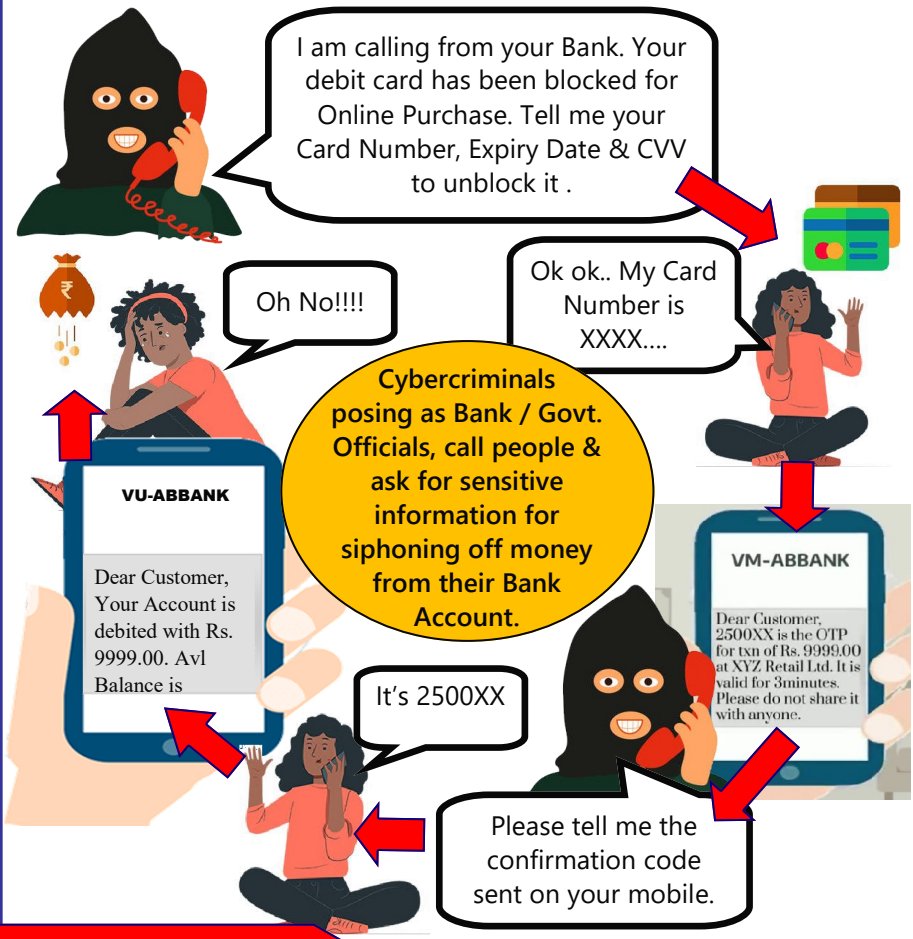
With the internet being a big playground, we need to play safely. This booklet is like your superhero cape, providing you with tips and tricks to stay safe from online villains. Don't keep all these cyber knowledge gems to yourself! Be a digital superhero not just for yourself but for your family and friends too. Share the cyber awareness messages from this booklet with your parents, friends, and relatives to create a safer online space for everyone. .

Let's embark on this cyber safety journey together and make our online adventures secure and enjoyable!

STAY CYBER SAFE, BE CYBER SMART !

WHAT'S INSIDE

OTP FRAUD



Best Practices

- ⇒ Do not trust or respond to any unknown caller.
- ⇒ Never share the ATM card number, CVV, PIN, OTP or any other sensitive or confidential banking credentials with anyone.
- ⇒ Remember, Bank never asks for Card number / CVV /PIN / OTP / Password or any other sensitive or confidential credentials.

FAKE SMS

Fraudulent text messages (SMS) are sent by fraudsters to individuals to trick them into revealing personal / sensitive information.

Fraudster sends fake messages containing malicious link

User opens the message and clicks on the link

The link either takes user to fraudulent website or malware gets downloaded on device

Indicators of Fake SMS

Best Practices

⇒ Do not trust or respond to unknown messages which are too good to be true.

⇒ Avoid clicking on unknown links.

FAKE EMAILS

Fraudster sends deceptive emails as Phishing Bait to capture sensitive / confidential information of user.

New Email ?

Won Lottery or Gift Coupon

Show Something Exciting

Urgency to Respond

Negative Consequences

Do not Click, Respond or Download !!!

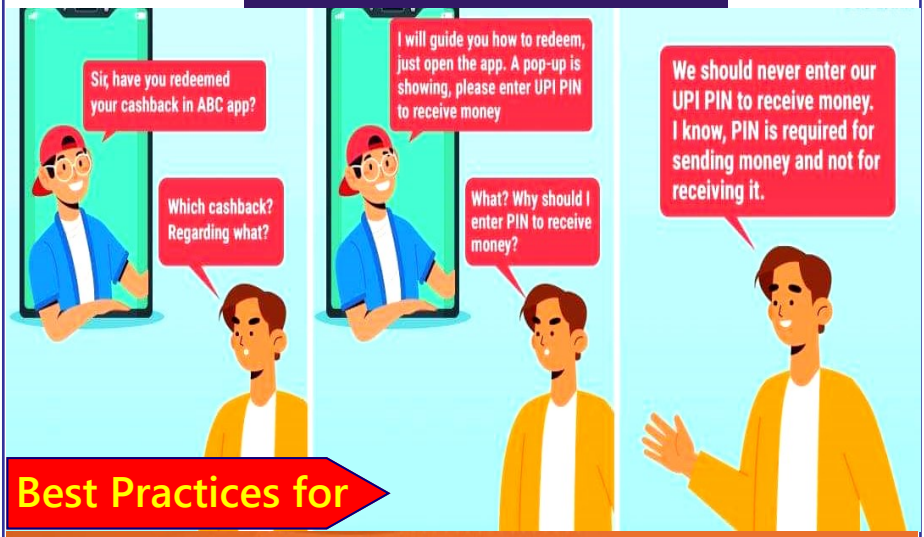
Stop..  ***Think...***  ***Connect*** 

Best Practices

FAKE LINKS


THE AFTERMATH OF A CLICK
could make you the victim of fraudster's trick !!
JUST THINK BEFORE YOU CLICK !
iPhone!
Ram, I clicked on a link offering iPhone at a very low price. Now my account got debited with Rs. 10,000.
We should not click on unverified links offering tempting deals
Immediately call 1930 and register your complaint at cybercrime.gov.in
Do not get lured via tempting messages, deals, lucrative advertisements & offers which are too good to be true and used as baits to defraud users

UPI FRAUD



Best Practices for

UPI SAFETY

- Never approve fund transfer requests from unknown UPI ids
- Never download unknown Apps by any means
- UPI PIN is only required for sending money, not receiving it

QR CODE FRAUDS

Cyber Threats hiding in QR codes

QRLjacking

Fraudsters leaving malicious QR codes on public places like walls, buildings and also computer screens that direct users to a malicious site.

Quishing

Fake QR Code directs unsuspecting victims to a fake version of a popular website and prompts users to enter their login details.

Free Wi-Fi set up

Cybercriminals often set up free Wi-Fi network for anyone that scans the QR Code. By this network fraudsters can silently steal sensitive information.

UPI related

Fraudsters sent malicious QR Code through Social Media, Emails, SMSs prompting for "SCAN & WIN Money". Scanning leads to debit money from account.

Tips to Avoid QR Code Fraud

FAKE ADVERTISEMENTS

Beware of Fraudulent Advertisements with FREE winning offers !

Fraudster may lure you with an unexpected cash Winning Offer in an Advertisement. Do not fall prey to it. Avoid clicking any links over it and always close or skip these type of Ads.

Beware of Social Media FAKE Ads!

Do not fall prey to Deep discounts and lucrative offers posted on Social Media. It might be Fake to to lure customers.

ALWAYS VERIFY CREDENTIALS AND READ REVIEWS OF THE SHOPPING PORTAL CAREFULLY.

Beware of Pop-up Advertisements !

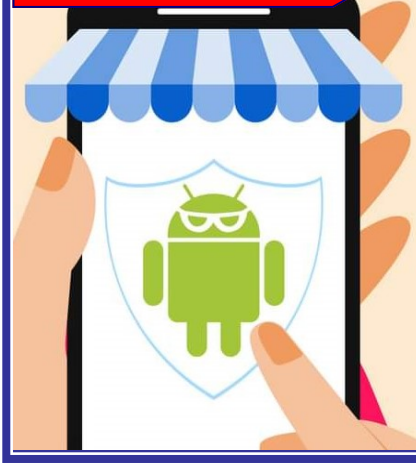
Avoid clicking links on malicious advertisement pop-ups, it can harm your device with malicious programs.

Always skip/close those Pop-up Ads window or use Ad Blocker to block them.

FAKE APPS

DO NOT INSTALL UNKNOWN APPS, IF ANYONE ASKS, FOR CLAIMING REWARD, CASHBACK OR TRANSACTION DISPUTE SETTLEMENT.

Best Practices



- Download apps from official stores only.
- Avoid installing apps through links in email, SMS, social media etc
- Read reviews of apps and their developers before downloading
- Review and manage permissions for downloaded applications
- Uninstall apps not being in use
- Use updated antivirus solution

MOBILE DEVICE SECURITY

Keep your mobile device secure.

It contains passwords, data, photos and other sensitive information.

SECURE YOUR PASSWORD

Beware of Credential Stuffing

Cybercriminals may use stolen usernames and passwords from one site to access other accounts of the same user.

Tips to protect your PASSWORD

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

LATEST CYBER SCAMS

Stay Vigilant against Digital Arrest

In recent incidents, cybercriminals posing as police officials have been alleging unsuspecting victims in fictitious money-laundering cases, manipulating and extorting money by threatening the victims with fake cases and interrogation !

- ✓ **Be wary of unsolicited calls claiming legal issues or urgent threats, especially if they demand immediate action or money transfer.**
- ✓ **If threatened with legal action, verify with the relevant authorities before complying with any instructions or transferring funds.**
- ✓ **Always ask for the Official notice, other necessary details etc. & directly communicate with the local police station for verification / clarification.**
- ✓ **Refrain from sharing personal, financial, or Aadhar card details over the phone unless you can confirm the legitimacy of the call.**

Always remember, real police authorities don't question individuals digitally. Official discussions happen through legitimate or formal channels, not through random online intimidation or coercion.

Guard Your Biometric Identity

Lock your Biometric or Aadhaar through official UIDAI website or mAadhaar app

To protect your Aadhaar, preferably use masked Aadhaar number generated from official UIDAI portal

LATEST CYBER SCAMS

Beware of Task Based Job Fraud through Video Liking

- ✗ Never trust / respond to unknown messages offering easy make money for just clicking "like"
- ✗ Avoid online transactions involving unknown parties
- ✗ Avoid clicking on suspicious links
- ✗ Never engage in user prompted tasks/actions at the behest of any stranger
- ✗ Never pay advance money as acceptance of job offer
- ✓ Refer authentic job portals / official websites / apps for job offer related information

BEWARE OF FEDEX INTERNATIONAL COURIER SCAM

Cybercriminal claiming to be International Courier Service Co. Executive may defraud individuals in the name of detection of Banned Narcotic Drugs in their parcel

- ✗ **Do not make money transfer on the basis of urgency, trust, fear, intimidation, pressure tactics etc.**
- ✓ **Always verify the information directly from the local police station mentioned.**

ONLINE SHOPPING SAFETY TIPS

Beware of online shopping frauds

while ordering from e-commerce platforms, there may be fake sellers online who may not deliver your order at all.

Use only trusted websites to shop

Best Practices

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

Read customer reviews, ratings about products and vendors

Use only trusted or reputed online shopping sites / Apps

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

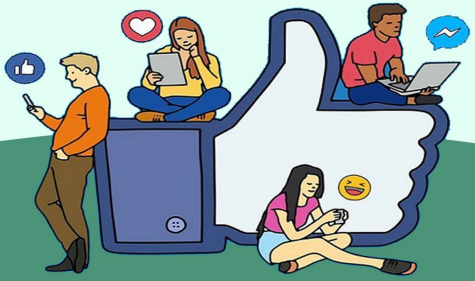
Always log out after completion of the session

SAFE HANDLING OF SOCIAL MEDIA

Be Careful while Accepting Friend Request from Strangers

Cyber criminals often create fake social media profile to befriend potential victims for obtaining their confidential data or gain trust to cause harm.

Be **Social**



Be **Safe**

- Block profiles from public searches
- Log out after each session
- Never share credentials with anyone
- Never mention home or work address
- Never accept friend requests from strangers
- Never click on suspicious links
- Keep the profile privacy settings at the most restricted levels
- Limit your share & be cautious about what you are sharing

CYBER FRAUD REPORTING

The complainant must provide

- ⇒ Mobile Number
- ⇒ Name of the Bank and Account Number from which amount has been debited
- ⇒ Transaction details (ID and Date of Transaction)
- ⇒ Debit / Credit Card Number in case of fraud made by using Card
- ⇒ Screen shot of transaction or any other image related to fraud, if available

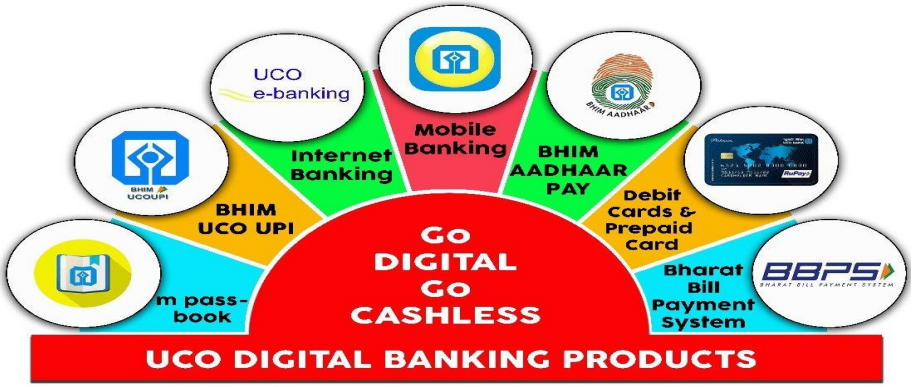
CONNECT WITH US

FOR OPENING ACCOUNT

Visit Official Website
www.ucobank.com

Call Toll Free Number
1800 103 0123

Please **DO NOT** Search for Customer Care numbers in Search Engines

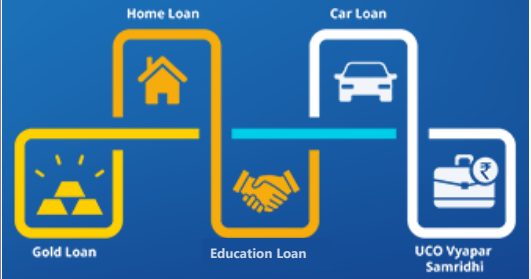


Digitally empowering all with our new apps..

UCO PAY+
An one stop solution for both customers & non-customers

UCO SECURE
increasing customer security

YOUR PARTNER FOR FINANCIAL ASSISTANCE!



Visit Nearby UCO Bank Branch.

STAY UPDATED

with all UCO Bank updates and offers

Connecting and Banking with every customer!

Follow us on our social media

CSOC

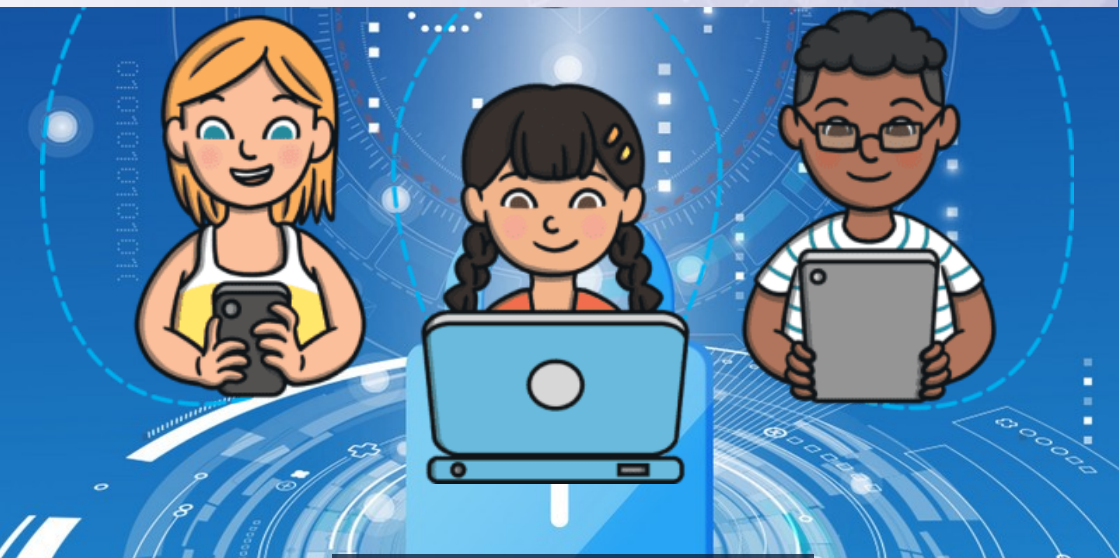
साइबर सुरक्षा संचालन केंद्र

Cyber Security Operations Centre

CISO OFFICE

Empower Your Cyber Journey

Be a CyberSafe Champion



CISO OFFICE

यूको बैंक UCO BANK

(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)

सम्मान आपके विश्वास का Honours Your Trust