ABHYUDAYA
CO-OPERATIVE BANK LTD.
(MULTI - STATE SCHEDULED BANK)

सायबर जागरूकता

Cyber security is buzz word now days. Cyber security refers to the practices, technologies, and processes designed to protect digital information, computer systems, networks, and electronic data from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes protection against malware, viruses, trojans, phishing, ransomware, and other types of cyber threats.

Effective cyber security measures ensure the confidentiality, integrity, and availability of sensitive information and prevent cyber attacks that can compromise individual or organizational security.Effective cybersecurity measures involve a combination of technology, policies, and user awareness to stay ahead of emerging threats and protect against cyber attacks.

Cybersecurity is crucial in today's digital age due to the following reasons:

1. Protection of sensitive information:
2. Prevention of financial loss:
3. Maintenance of privacy:
4. Protection of critical infrastructure:
5. Business continuity:
6. National security:
7. Protection of intellectual property:
8. Compliance with regulations:
9. Reputation and trust:
10. Evolving threats:

Cybersecurity helps safeguard personal, financial, and confidential data from unauthorized access and theft.Cyber attacks can result in significant financial losses, damage to reputation, and legal liabilities.It ensures that personal information remains private and is not exploited for malicious purposes.It is essential for safeguarding critical infrastructure, such as power grids, healthcare systems, and transportation networks.It helps ensure uninterrupted business operations and minimizes downtime.It is vital for protecting national security and preventing cyber espionage.It helps safeguard intellectual property, trade secrets, and proprietary information.It helps organizations comply with data protection regulations and avoid legal consequences.It helps maintain customer trust and protects an organization's reputation.It is essential for staying ahead of emerging threats, such as AI-powered attacks, IoT vulnerabilities, and social engineering tactics.

Some Security tips…….

Password Security:

Protecting Yourself Online :

Here are some password protection tips:

1. Use strong passwords: Mix uppercase and lowercase letters, numbers, alphanumeric and special characters.Use different passwords for each account.Don't use easily guessable words like names, birthdays, or common phrases,places.Update passwords at specific interval of time.
2. Password length: Ideally 12 characters or more.
3. Don't reuse passwords: Never reuse passwords across multiple accounts.
4. Two-factor authentication (2FA): Enable 2FA whenever possible to add an extra layer of security such as OTP or Biometric.
5. Avoid phishing scams: **Be cautious of emails or links asking for password resets or logins.**
6. Keep passwords private: Don't share passwords with others or write them down in accessible locations.

Remember, strong passwords are your first line of defense against cyber threats!

Types of Cyber Threats:

Malware, short for "malicious software," refers to any software designed to harm or exploit a computer system or its user.
Types of malware include:
1. Viruses: Replicate and spread to other files or systems.
2. Trojans: Disguise themselves as legitimate software, allowing unauthorized access.
3. Spyware: Secretly monitor and collect user data.
4. Ransomware: Encrypt files, demanding payment for decryption.
5. Adware: Display unwanted advertisements when you are using mobile phones or laptops.
6. Worms: Self-replicate and spread without human interaction.
7. Rootkits: Hide malware or unauthorized access.
8. Keyloggers: Record keystrokes, often to steal sensitive information, while entering password ,use virtual keyboard.

Malware can enter systems through:

1. Email attachments or links
2. Infected software downloads
3. Vulnerable network connections
4. Infected external devices(e.g., USB drives)
5. Exploited system vulnerabilities

To protect against malware, attack:

1. Use antivirus software
2. Keep systems and software up-to-date
3. Avoid suspicious downloads and links
4. Use strong passwords and enable firewall
5. Regularly back up important data
6. Download app from official /trusted source only. Ensure its guinines.
7.To avoid mobile charging on public power points.

Remember, vigilance and caution are key to preventing malware infections!

Psychological tricks are where attackers play with the minds of the user to trap them with lucrative offers. Once trapped, the attackers can exploit the victim by either stealing money or stealing sensitive personal information (name, Aadhaar details, bank account details etc.) or harm the victim in any other way. The entire basis of this kind of attack is to make the victim fall into their trap by sending fake e-mails, calls or SMSs.

Phishing is the act of sending fraudulent e-mail that appears to be from a legitimate source, for example, a bank, a recruiter or a credit card company etc. This is done in an attempt to gain sensitive personal information, bank account details etc. from the victim.

Vishing is similar to phishing. But, instead of e-mail, in this type of crime, the fraudster uses telephone to obtain sensitive personal and financial information.

Smishing is the SMS equivalent of phishing. It uses SMS to send fraudulent text messages. The SMS asks the recipient to visit a website/weblink or call a phone number. The victim is then tricked into providing sensitive personal information, debit/credit card details or passwords etc.

Phishing, Vishing and Smishing are done in an attempt to steal money from the victim or cause any other harm to the victim.

As per latest advisory from Indian Government, an 'Android malware campaign' targets Indian Banking customers (Mobile users).Malware targets hindi speaking users through fraudulent banking application & mimics financial institutions, utilizing convincing phishing websites that incorporates legitimate assets from officials banking websites to deceive Victims in to downloading malicious applications. When malware enter victims mobile, then APK displays on victims device which looks like google play interface(fake) prompting victims to perform 'update' in background it spoils data whereas screen victims deceived to enter sensitive information then victims get message of confirmation page(fake page). Such type of frauds can takes place to any one . Phishing website created as - https://www.sbi.mycardcare.in , https://kotak.mycardcard.in , https://axis.mycardcare.in , https://indusind.mycardcare.in , https://icici.mycardcare.in
Risk for banking users are as credential theft- financial frauds, User trust & reputation risk

Impersonation and Identity theft – Theft through fraudulenty or dishonestly using electronic/digital signatures , passwords of any other person.

The Ministry of Electronics and Information Technology (MeitY) has issued draft DPDP Rules, 2025, setting clear obligations for businesses. Under the law, organisations must ensure that personal data, such as phone numbers, is collected only with explicit consent and with safeguards that prevent exposure in public settings. **Digital Personal Data Protection Bill, 2023 (DPDP act)** – Data privacy law.It focuses on protection of personal data-sensitive –confidential data and introduces penalties for non-compliance with data protection rules. India's comprehensive data privacy law designed to protect digital personal data,etc.

"Digital Arrest" :→ Latest cyber attack type .- Note no one can arrest over Phone..

Modus operandi :

In this end user (victim) receives call wherein attackers will pressurises victim by claiming that he/she is a Police-CBI-ED officials and inform victim that his relative /or victim has made crime/assault, money laundering, drug trafficking and claims that victims said relative is under police/CBI custody , to release from his/ her punishment ask victim to give ransome money / some times virtual money (like bit coins) along with asking victims personal info including account details. Attackers does video call to victim wherein exact setup of Police office/CBI/ED office/Court room is created. Till the money receives / victim traps , attackers impose victim to be present online infront of video camera through Skype or team call. Through video call, Attackers informed victim that he/she is in online arrest till victims not giving amount to attacker. So that victims has to be continuous seating in front of online camera 3-4 days also. Finally victims false pray to attackers and transfer money whatever attacker wants. It is just like online harassment. Do not pay any money.

Note "Digital Arrest" is a SCAM to extort money from victims. To file Digital arrest compliant, kindly report to National Cyber Crime Reporting Portal at www.cybercrime.gov.in or helpline 1930.

Recent 'Digital arrest attack' Incidences are, happened with well known doctor harassed for almost 4 days after digital arrest she transfer Rs 2.81 crore to cyber criminals who poses as CBI officer , exact online court room setup was created, they claims that doctors bank account was used in money laundering, subsequently asked her to be arrest to Police immediately once she could not attend police for arrest n interrogation she was in forcefully digital arrest in front of 'Skype video call' for few days.

Similar case is with Agra teacher , Scientist duped of Rs.71 Lakh after digital arrest by fraudster in Madhya Pradesh, One of the industry head was victimised for Rs. 7 Crore in Digital arrest, Bengaluru based MNC executive loses Rs.51 Lakh in' Digital arrest' and many more.

As per Indian Cyber Crime Coordination Center (I4C),Police /CBI/ED never arrest any one via video call.

The rise in Deepfakes- AI generated voice, video, and photo scams make filtering through misinformation a challenging task. It is edited and or generated using AI tools and which may depict real or non-existent people.(hoax images, videos ,etc)

Beyond spreading rumours, cyber attackers are now able to manipulate images available in the public domain and repost fabricated explicit versions of those images. false images and words can pose significant, lasting harm to kids and their families, harming their privacy, identity, and well-being.

Some key Digital Fraud trends are as :

TRAI Phone Scam, Parcel Stuck at Customs, Digital Arrest, Family Member Arrested, Get Rich Quick Trading, Easy Tasks/Online Jobs for Big Rewards, Lottery in Your Name, Mistaken Money Transfer, KYC Expired, Generous Tax Refund, fake wedding invitations (fraudulent invitations are typically shared through messaging apps like WhatsApp, email, or SMS, and they often come with enticing file attachments such as "Invite.apk.)

Festival-related Frauds, Banking Reward Application Scams, Fake IRCTC App, E-commerce related Fraud, QR Code Phishing (Quishing), Income Tax Refund Scam.

QR Code Phishing :A new phishing methodology exploits the widespread use of QR codes. This threat involves sending malicious QR codes via text messages, social media apps, or email. When scanned, these codes direct users to fake websites that appear legitimate but are designed to steal personal and financial information.

Festival related frauds : Cybercriminals distribute malicious links disguised as special festival gifts via WhatsApp, SMS, and email, often using short URLs to hide the original malicious links.Victims who click on these links are presented with forms requesting personal details and access to contacts, messages, and call records. The scammers create a false sense of urgency, prompting users to share the message with friends or groups to claim their "special Diwali gift".

E-commerce related Fraud:
Scammers are targeting e-commerce customers with fake messages claiming they have won prizes or gift cards. These frauds typically use SMS, email, or social media platforms to distribute messages with text like "Dear customer, congratulations! You have won…" Users are prompted to click on links to claim free gifts or gift cards, which redirect them to malicious sites that harvest personal information.

41% digital fraud are reported in Eastern region of India like, West Bengal, Odisha, Bihar, Assam, Kashmir, Arunachal Pradesh, Meghalaya, Tripura, Nagaland, Mizoram, Manipur, Himachal Pradesh, and Sikkim.

Not Just Passwords: Hackers Now Want Your Contracts, Bank Records, and Code. New data breaches incident analysed as 93% of incidents included financial documents, Bank statements were leaked in 49% of cases.

Data breaches occur when attackers exploit vulnerabilities in systems, steal credentials or do with social engineering tactics. Data Breaches can be done through theft, insider attack, target attack(like phishing, malware, Denial of Service attack, vulnerability exploits)85% of data breaches involve human interaction, social engineering attacks is one of the most cybersecurity threats.

While doing UPI & Digital payments through QR Code, take due care - Do not rely solely on screenshots. Always confirm payments in your bank account or UPI app. Wait for official payment confirmation messages, Keep your QR codes secure and avoid clicking on unknown links. Always confirm the legitimacy of the transaction and rely solely on trusted platforms to safeguard their money. Never scan QR codes sent by unknown individuals while conducting online transactions.

As per Aadhaar Act, 'e-Aadhaar' is equally valid like Physical Copy of Aadhaar for all purposes.

Steps to Lock Your Aadhaar- **step1** : Visit the MyAadhaar Portal, **step2**: Access the Lock/Unlock Aadhaar Option, **Step3** : Provide Your 16-Digit Virtual ID (VID), **Step4:** Select the "Lock Aadhaar" option to proceed with securing your Aadhaar, **Step5**: Fill in your VID, name, PIN code, and captcha code. You will also need to verify your identity through an OTP sent to your registered mobile number,**step6:** Check the consent box and hit "Submit" to complete the process, **Step7:** Once completed, a message will confirm that your Aadhaar has been locked successfully.

The government has asked not to deposit the Xerox of Aadhaar card anywhere. The government has issued these orders to prevent misuse of Aadhaar card. Government has suggested that masked xerox of Aadhaar card should be given if xerox of Aadhaar card is essential at a place.*

How to Download Masked Aadhar Card?*

Your 12 digit number will not appear in Masked Aadhar Card. Instead only the last 4 digits will appear. "Masked Aadhar Card" can be downloaded from UIDAI's website

Go to this link

https://myaadhaar.uidai.gov.in/ or https://myaadhaar.uidai.gov.in/masked-aadhaar

Click on "Download Aadhaar"

> Mention your Aadhaar number

You will see the option Do you want **Masked Aadhar** Card, select it

> Select download option and get copy of Aadhaar card with last four digits of Aadhaar number.

Beware some one can misuse your Aadhaar card Xerox for identity theft or fraudulent activities . It can be used to create fake IDs or to obtain services.

- **Verify the Caller :** Always check the caller's identity by contacting the relevant law enforcement agency using official contact details published on their official website.
- **Report Suspicious Calls :** Report any suspicious calls or scams to your local cyber police authorities immediately.
- Disable 'Auto Save' or 'Remember' function in your device to avoid storing of user ID and passwords.
- Always logout and close the browser when you are done with your work.
- Always verify the authenticity of e-commerce websites before performing the transactions.
- Your bank account number or PIN should never be stored on the mobile phone.
- Report the loss of your mobile phone to the bank to disable PIN and access to the bank's account .
- Keep your SIM card locked with a PIN to avoid misuse. In case of loss or theft of the mobile device; contact your service provider to block the SIM card immediately.
- Avoid downloading investment apps from unknown sources. Use only trusted platforms such as Google Store or AppStore to download apps.
- caution towards shortened URLs, such as those involving bit.ly and tinyurl.

Fake Investment Scams:
Fraudsters create fake investment groups on platforms like WhatsApp and Telegram, presenting themselves as financial experts. They attract victims with free stock tips and opportunities, then manipulate them into using fake trading applications. Once victims invest, they face difficulties withdrawing their funds, and the scammers vanish with the money.

Money mule transaction :- an individual with a bank account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. these money mules often have their bank accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of afraud.

Akira Ransomeware :- It is famous for obtaining sensitive personal information from victims and encrypting their data in order to demand for money, attacker threatens victim to expose data on dark web if victimes decline to pay the demanded money.

SOVA Android Trojan Targets Banking Customers:- SOVA Android Trojan is a new type of mobile banking malware.SOVA seems to be targeting more than 200 mobile applications, including Banking Apps and Crypto exchanges/wallets. Malware is distributed via smishing (phishing via SMS) attacks, like most Android banking Trojan.

Social Media Frauds :→ Fraudsters use Fake Profile of the victim to spread false or fake information.Sends friend requests to other friends of victim to gain financial benefits. To damage the reputation of the victim.
To avoid above social media fraud_:→ Avoid sharing your personal information like address, mobile number, personal mail id and other sensitive identity related information on social media. Do not share your personal pictures online publicly on social media accounts. Never accept friend requests without appropriate verification and confirmation. Enable multi-factor authentication for social media accounts. Disable profile visibility from public searches. Log out after each session. Never share social media credentials with any one. Keep the privacy settings of social media profile at most restricted level, especially for public viewing. Apply maximum caution while sharing photographs, videos, status, comments etc. Criminals may collect enough information about users from the posts and profile of the user.Review your social media privacy settings and restrict to family and known friends. Be careful & alert while using social media platform like facebook, whatsapp , Linked IN Instagram, Twitter.
Educate children about password safety.Check their social media accounts and keep track of it.

Morphing is altering or changing the pictures of the person using morphing tools available online. The morphed pictures are then used by perpetrators for blackmailing the victims, creating fake online profile, sexting, sex chats, pornographic content, nude pictures etc., Morphing can damage the victim's online reputation and cause emotional trauma, can also be prone to threats from perpetrators and may fall prey to their attempts at blackmailing them.

Cybercriminals are persistently looking for new ways to expose security risks. They perform cyberattacks to steal, expose, alter, disable, or destroy organisation's assets through unauthorized access to computer systems. Cyber-attack could cause financial loss and disruption of business.

TIPS TO KEEP YOU SAFE… Do's & Don'ts

1. Always keep your systems/devices (desktop, laptop, mobile) updated with latest patches.

2. Protect systems/devices through security software such as anti-virus with the latest version.

3. Always download software or applications from known trusted sources only. Never use pirated software on your systems/devices.

4. Ensure all devices/accounts are protected by a strong PIN or passcode. Never share your PIN or password with anyone.

5. Do not share your net-banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. with any person even if he/she claims to be an employee or a representative of the bank and report such instances to your bank.

6. Always change the default admin password on your Wi-Fi router to a strong password known only to you. In addition, always configure your wireless network to use the latest encryption (contact your network service provider, in case of any doubt).

7. Be cautions while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts such as e-mail or banking on these networks.

8. Always use virtual keyboard to access net-banking facility from public computers; and logout from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online banking activity.

9. Do scan all e-mail attachments for viruses before opening them. Avoid downloading e-mail attachments received in e-mails from unknown or un-trusted sources.

10. Be careful while sharing identity proof documents especially if you cannot verify the authenticity of the company/person with whom you are sharing information.

11. Note the IMEI code of your cell phone and keep it in a safe place. The operator can blacklist/ block/trace a phone using the IMEI code, in case the cell phone is stolen.

12. Observe your surroundings for skimmers or people observing your PIN before using an ATM.

13. Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.

14. Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.

15. Update Mobile number to your branch time to time in case of changes in your mobile number so that regular SMS updates will receive.

16. For secured transactions use official mobile apps only.

17. If you think you are compromised, inform authorities immediately.

18.**आरबीआई/बैंक कभी भी लोगोंसे व्यक्तिगत जानकारी/बैंक का विवरण नहीं मांगता है।आरबीआई के नकली लोगो और देशों से सावधान रहें।**

19. **रहें साइबर सुरक्षित! अपने डिवाइस को बॉटनेट संक्रमण और मालवेयर से सुरक्षित करने के लिए, सीईआरटी-इन, भारतसरकार https://www.csk.gov.in पर "फ्री बॉटरिमूवल टूल" डाउनलोड करने की सलाह देता है - दूरसंचारविभाग.**

20. TRAI doesn't send any message or make any call to any consumer for verification or disconnection or reporting unlawful activities of mobile numbers. Also, TRAI has also not authorized any agency to contact customers for such activities. Any message or call in this regard should not be entertained and may be reported to concerned mobile service provider and law enforcement agencies. 'Awareness is the Safety'

21. As a parent, nothing is more important than your child's safety. Extend your safety net online - install Parental Control Filters (PCF) on your computer OS/browsers from a trust-worthy source & protect your child from accessing unsafe material & contacts - Department of Telecommunications.

22.Disable ‘Auto Save’ or ‘Remember’ function in your device to avoid storing of user ID and passwords.

23.Always logout and close the browser when you are done with your work.

24.Always verify the authenticity of e-commerce websites before performing the transactions.

25.Your bank account number or PIN should never be stored on the mobile phone.

26.Report the loss of your mobile phone to the bank to disable PIN and access to the bank’s account .

27.Keep your SIM card locked with a PIN to avoid misuse. In case of loss or theft of the mobile device; contact your service provider to block the SIM card immediately.

28.Avoid downloading investment apps from unknown sources. Use only trusted platforms such as Google Store or AppStore to download apps.

29.Chasing unbelievable gains could mean unbearable pain.

30. जर ते तुम्हाला सांगत असतील की तुम्ही 'डिजिटल अरेस्ट' मध्ये आहात, आणि कुणालाही कॉल करू नका, जिथे आहात तिथून हलू नका पुढचे ४८ तास ! तर याला प्रतिसाद देऊ नका. हा स्कॅम आहे.

31. जर ते तुम्हाला सांगत असतील की तुमच्यासाठी पाठवलेल्या किंवा तुम्ही पाठवलेल्या एखाद्या पॅकेजमध्ये ड्रग्ज सापडली आहेत, तर प्रतिसाद देऊ नका. हा स्कॅम आहे. (लक्षात ठेवा.... कर नाही तर डर कशाची) हे विसरू नका !

32. जर ते म्हणाले की तुमचा मुलगा / मुलगी ऍक्सीडेन्ट मध्ये सापडला असून आता आमच्या हॉस्पिटल मध्ये आहे, पंधरा मिनिटात ऑपरेशन करावे लागेल, तर तोवर टोकन मनी म्हणून अमुक इतके पैसे पाठवा ! तर अजिबात पाठवू नका ! हा स्कॅम आहे. त्यासाठी आधी मुलाला कॉल करून खात्री करून घ्या. मग कळेल की तो तर ऑल रेडी सेफ आहे..... कॉलेजात / कँटीन मध्ये !

33. जर ते तुमच्याशी व्हॉट्सअँप किंवा एसएमएसद्वारे संपर्क साधत असतील, तर प्रतिसाद देऊ नका. हा स्कॅम आहे. (शक्यतो अननोन नम्बरवरून आलेले कोणतेही कॉल अटेंड करू नका ! व्हिडीओ कॉल तर मुळीच करू नका अटेंड

34. जर कोणी म्हणत असेल की ते स्विगी किंवा झोमॅटोवरून फोन करत आहेत आणि तुम्हाला 1 किंवा इतर कोणताही नंबर काहीही दाबून तुमच्या पत्त्याची पुष्टी करण्याची आवश्यकता असेल तर प्रतिसाद देऊ नका. हा स्कॅम आहे.

35. व्हिडिओ मोडवर कोणत्याही कॉलला कधीही उत्तर देऊ नका. त्यासाठी वाटलं तर अशावेळी तुमच्या मोबाईलचा स्क्रीन छताकडे धरून पहा. समोरून कोण कसल्या अवस्थेत (न्यूड टाईप) बोलत असेल तर तुम्हाला ते दिसेल पण त्यांना तुम्ही दिसणार नाही त्यामुळे नंतर होणारे इमोशनल ब्लॅक मेल थांबेल ! नंतर त्या नंबरला लगेच ब्लॉक करा !

36. जरी तुम्हाला सर्वोच्च अधिकारी पोलिस (डिपार्टमेंट), सी. बी. आय., ई. डी., आय. टी. विभागाकडून नोटीस पाठवली आहे असं कॉल / मेसेज करून सांगितलं असलं तरी पॅनिक होऊ नका ! संबंधित खात्याच्या अधिकृत वेबसाईटवर जाऊन त्याची

आधी खात्री करून घ्या. कारण या विभागातर्फे असे कधीही कॉल / मेसेज करून नोटीस पाठवली जात नाही. अधिकृत पोस्टातर्फे तरी येते किंवा त्यांची माणसे फिजिकली नोटीस घेऊन येतात. हे विसरू नका !

37. 'सोप्या कर्जाच्या' ॲप्सच्या जाळ्यात अडकू नका. तुम्ही परत करू शकत नाही अशी अनेक कर्जे घेण्यासाठी ते हळूहळू तुम्हाला फसवतात. कधीकधी, ते मोठ्या परताव्याचे आश्वासन देतात आणि तुम्हाला गुंतवणुकीसाठी कर्ज देतात. कधीही नफा मिळत नाही. तुम्ही गुंतवलेले पैसे गेले आहेत. तुम्ही केवळ काही घोटाळ्यात गुंतवणूक करण्यासाठी कर्ज घेता. तुमची "गुंतवणूक" नष्ट होईल परंतु कर्ज आणि व्याज भरण्यासाठी तुम्ही जबाबदार असाल.

38. समभाग (शेयर्स) किंवा क्रिप्टोकरन्सी खरेदी करण्याचा सल्ला देणाऱ्या कोणत्याही कॉल/संदेशांना प्रतिसाद देऊ नका. असा साठा खरेदी करू नका कारण "निश्चित नफा" अपेक्षित आहे. जो तुम्हाला भासवला जातो पण रियल मध्ये कधीही तो तुम्हाला मिळत नाही. उलट जे पैसे गुंतवले ते सगळे घेऊन हे भामटे फरार होतात.

39. "वर्क फ्रॉम होम" करण्याचे आश्वासन देणाऱ्या कॉल/संदेशांना शक्यतो प्रतिसाद देऊ नका. ते तुम्हाला जाळ्यात अडकवतात, तुम्हाला "नफा" दर्शविताना "गुंतवणुकीसाठी" पैसे पाठवतात. कधीही नफा मिळत नाही. हा स्कॅम आहे.

40. जर कोणी तुम्हाला फोन करून सांगितले की त्यांनी चुकून तुमच्या यू. पी. आय. आयडीवर पैसे पाठवले आहेत आणि त्यांना फक्त त्यांचे पैसे परत हवे आहेत, तर प्रतिसाद देऊ नका. हा स्कॅम आहे. तुमच्याकडे ते शंभर रुपये पाठवतील आणि लिंक अथवा क्यू आर कोड देतील आणि सांगतील की इथे रिटर्न करा ! ते अजिबात करू नका ! त्यातून तुमचा फोन हॅक करून तुमचे अकाउंट "रिकामे" करण्याचा हा स्कॅम आहे

41. आंतरराष्ट्रीय कॉल प्राप्त करताना, तुमच्या फोनवर भारतीय क्रमांक किंवा कोणताही क्रमांक दिसत नसल्यास, कृपया DoT संचार पोर्टल https://sancharsaathi.gov.in किंवा टोल फ्री क्रमांक 1800110420/1963 वर कळवा

42. कोणतेही न्यायालय/पोलिस स्टेशन/सरकारी तपासणी एजन्सी तुम्हाला फोन करून माहिती देत नाहीत किंवा आदेश काढून बोलवू पण शकत नाहीत. -ते कागदी पद्धतीने सरकारी नियमात राहून काम करतात.

43. अपनी शिकायत सबसे पहले, बैंक/एनबीएफसी/भुगतान प्रणाली सहभागी/क्रेडिट सूचना कंपनी के पास दर्ज करें। 30 दिनों में समाधान न मिलने पर cms.rbi.org.in पर शिकायत दर्ज करें। -RBI

44. आरबीआई द्वारा विनियमित बैंक/ एनबीएफसी के साथ ऋण देने वाले डिजिटल ऐप्स की जुड़ाव का आधिकारिक वेबसाइट पर पता लगाकर ही उनका सत्यापन करें। एसएमएस या सोशल मीडिया से मिलने वाले लिंक से डाउनलोड करने से बचें। -RBI

45. किसी भी लेनदेन के लिए फिंगरप्रिंट का उपयोग करने से पहले यह सुनिश्चित करें कि डिवाइस पर कोई पारदर्शी फिल्म नहीं है। ऑपरेटर की आईडी सत्यापित करें। लेनदेन की रसीद मांगें। -RBI

46. रहें साइबर सुरक्षित! अपने डिवाइस को बॉटनेट संक्रमण और मालवेयर से सुरक्षित करने के लिए, सीईआरटी-इन, भारत सरकार https://www.csk.gov.in पर "फ्री बॉट रिमूवल टूल" डाउनलोड करने की सलाह देता है - दूरसंचार विभाग

47. . कैशबैक, आकर्षक रिटर्न, तुरंत लोन, नौकरी के ऑफर या पैसे के अनुरोध वाले अज्ञात लिंक पर क्लिक न करें। -RBI

48. आरबीआई/ बैंक कभीभी लोगो से व्यक्तिगत जानकारी / बैंक का विवरण नहीं मांगता है।आर बी आई के नकली लोगो और संदेशों से सावध रहें।

49. TRAI never sends any message or makes any call, for verification /disconnecton /reporting involvement in unlawful activities of mobile users/numers. Beware of such fraudulent messages/calls

in the name of TRAI. These messages/calls should be reported to the Department of Telecom Chakshu Platform at https://sancharsaathi.gov.in/sfc/

50. Be cautious Friend's request on Social Media platform.

51. Think before you post/ upload on any social media (Whatsapp/ Facebook/Instagram/Telegram/Twitter-X platform). It may be misuse.

51. Be mindful of your appearance on video chat & video calls , Your video chats on Social Media can be recorded by the person on the other side, Be careful while accepting chat requests from strangers.

52. Be careful while you give/handover your mobile devices, PCs, laptop,Tabs for servicing /repairing/selling.

53. Not to upload any sensitive information, Official communications-messages-screenshots , confidential information , personal information like pictures/images, on Social media platform including "Whatsapp".

54. Enable SMS/email alerts to track unauthorized transactions immediately.

55. Fraudsters use Fake Profile of the victim to spread false or fake information. Sends friend requests to other friends of victim to gain financial benefits. To damage the reputation of the victim.

56. Always verify the authenticity of e-commerce websites before performing the transactions.

57. TRAI does not provide any NOC for installing mobile towers. If a fraudster brings a fake letter to you, inform the concerned service provider and the local police.

58. TRAI announced a major safeguard, telecom companies will now use the exclusive '1600' number series for all calls originating from the banking, financial services, and insurance (BFSI) sectors. TRAI urging citizens not to trust calls unless they originate from numbers using the 1600 prefix.

59. Lodge complaint against any bank, NBFC or payment system participant on https://cms.rbi.org.in under RB-Integrated Ombudsman Scheme. Call 14440 for more.

60. Beware- Not to upload any sensitive & or confidential information-personnel photos/images on any social media platform it may misuse.

61. Investment lost in fraudulent schemes, File your compliant at https://sachet.rbi.org.in RBI's Sachet portal forwards cases to authorities for action-RBI

As per Internet source@ Union Home Minister Amit Shah has announced that **5,000 cyber commandos** will be fully trained and deployed over the next five years to combat growing cyber threats in India. On the foundation day of I4C (**Indian Cyber Crime Coordination Centre**), Shah emphasized the need for a secure cyberspace as critical to national security, saying that the country's progress is inseparable from ensuring robust cyber security. The commandos will be equipped to swiftly address and prevent cyber attacks across the nation, strengthening **India's digital defenses**. Their mission will be to provide rapid response and prevention of cyber attacks, ensuring minimal damage and disruptions to critical digital infrastructure. his registry, developed in collaboration with banks and financial intermediaries, will be a central repository for states, union territories, and law enforcement agencies to access and track suspects involved in such crimes, thereby enhancing fraud risk management.

Where to Report a Cyber Fraud?

1. Visit the nearest police station immediately.

2. To report cybercrime complaints online, visit the National Cyber Crime Reporting Portal. This portal can be accessed at https://cybercrime.gov.in

You can also file a complaint by dialing the helpline number**1930**.

3. In case you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details, please report it on Maharashtra Cyber's web portal by visiting www.reportphishing.in

4. Refer to the latest advisories which are issued by CERT-IN on https://www.cert-in.org.in/

5. Report any adverse activity or unwanted behavior to CERT-IN using following channels

E-mail : incident@cert-in.org.in

Helpdesk : +91 1800 11 4949 Provide following information (as much as possible) while reporting an incident.

- Time of occurrence of the incident
- Information regarding affected system/network
- Symptoms observed

- Report such fake websites/frauds/ cyber attacks immediately at the National Cybercrime Reporting Portal: **www.cybercrime.gov.in** or call 1930/ Maharashtra Cyber helpline number 1945 (to receive and registered Cyber crime complaints) in case of any frauds. Refer **https://mhcyber.gov.in/**

6. To report lost or stolen mobile phones, file a First Information Report (FIR) with the police. Post filing the FIR, inform Department of Telecommunications (DoT) through the helpline number 14422 or file an online compliant on Central Equipment Identity Register (CEIR) portal by visiting https://ceir.gov.in After verification, DoT will blacklist the phone, blocking it from further use. In addition to this, if anyone tries to use the device using a different SIM card, the service provider will identify the new user and inform the police.

7. To hotlist cards you can follow any one of the steps mentioned below:
a) Dial "9223110011" from the MOBILE NUMBER registered with our Bank. After 2-3 rings call will be disconnected, the system will HOTLIST the card & you will get SMS confirmation for the same.
b) Customer can directly call 1800223131/ 022-68778900 and register a request to hotlist the card by providing necessary credentials asked by the staff member manning the desk.
c) If the card holder has availed our mobile banking services, he can hotlist the card by selecting card hotlist option.
d) Customer can also email to hotlist@abhyudayabank.net for necessary action.

Lodge a written complaint with the Base Branch in respect of the unauthorized electronic transaction.

Grievance Redressal Policy of Abhyudaya Bank in respect of Electronic Transactions
Bank has a separate Customer Grievances Redressal Cell (contact number 022- 27890636, 022-7890638, email address atmrecon@abhyudayabank.net for quick redressal of customer grievances including those arising from electronic transactions channel. The cell takes utmost care to settle the issues relating to wrong/fraudulent debits and credits through the NPCI Dispute Management Scheme.
The customer having a grievance in respect of any of the electronic payments option can approach any branch of Abhyudaya Bank to file a written complaint with details of the matter. The complainant should bring along passbook, and an officially valid ID document, and also a passport-size photograph. In case of a fraudulent debit to or withdrawal from the customer's account, the customer should lodge a police complaint or file FIR. However, filing an FIR by the customer is not a precondition but to lodge police complaint (acknowledgement) is mandatory for any branch of Abhyudaya Bank accepting the complaint. The branch with which the complaint is filed will first assess the issue, record relevant information on complaint letter with signature held and forward the same immediately to the ATM-RECON Dept. Vashi, which at presently working as Customer Grievances Redressal Cell.

Cyber security must be everyone's responsibility.

From : **Chief Information Security officer (CISO)**

****