MCB Islamic

DIGITAL FRAUD PREVENTION ADVISORY

MCB Islamic Bank is committed to provide better and secure digital banking services available 24/7 to its valued customers. The purpose of this advisory is to create digital fraud prevention & security awareness among customers on digital fraud scams and trends. It will enable customers to learn how to safeguard themselves against fraud. It is the customer’s sole responsibility to read, understand and take necessary measures to enhance their security.

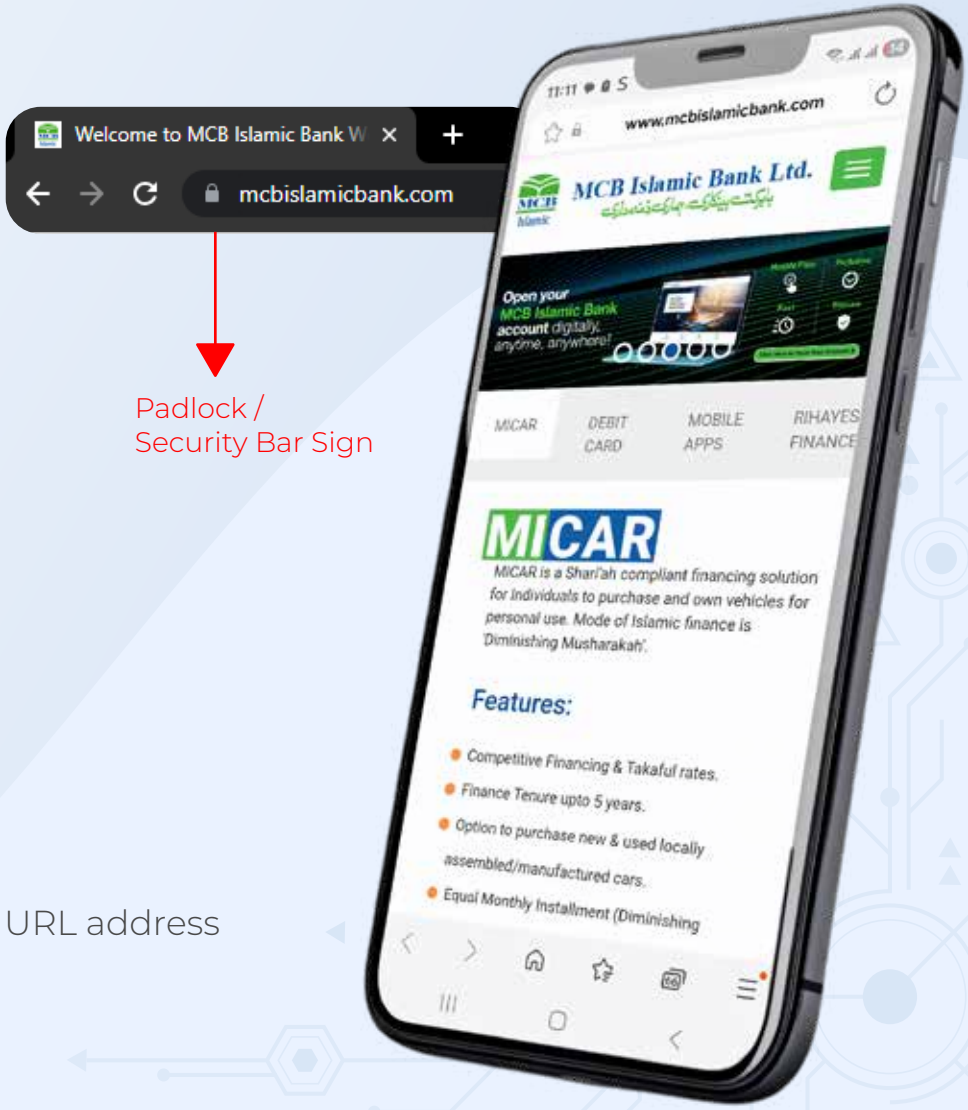
MCB ISLAMIC BANK'S OFFICIAL LINKS

MCB Islamic Bank Corporate Website Link

www.mcbislamicbank.com

MCB Islamic Internet Banking Link

digital.mcbislamicbank.com



Note: MCB Islamic Bank encourages looking for the correct URL address and verifying Padlock for genuineness of the website link.

SUBUK - MCB ISLAMIC MOBILE APP

Download Subuk Mobile App only from

Google Play Store

GET IT ON Google Play

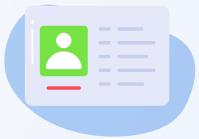
Apple App Store

Download on the App Store

CUSTOMER'S ROLES & RESPONSIBILITY

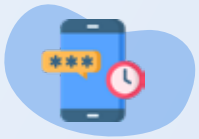
What are Credentials?

Credentials refer to information for accessing Digital Banking services. These credentials serve as a means of identifying you as a user. Credentials include:



User Name / ID

Passwords



One-time password (OTP) security code that we give to you when you use two-step verification

Debit card number & CCV code

A T-PIN (Transaction PIN) is a 6-digit code you set in App at the time of registration to authorize transactions such as fund transfers, bill payments, and other transactions etc.

Do not share your password, OTP and T-PIN with your family or loved ones. You should keep your password and OTP and T-PIN confidential to reduce the chance of your account(s) / confidential information(s) from being compromised.

Responsibilities

You play the primary role in protecting your credential and security when you use Digital Banking.

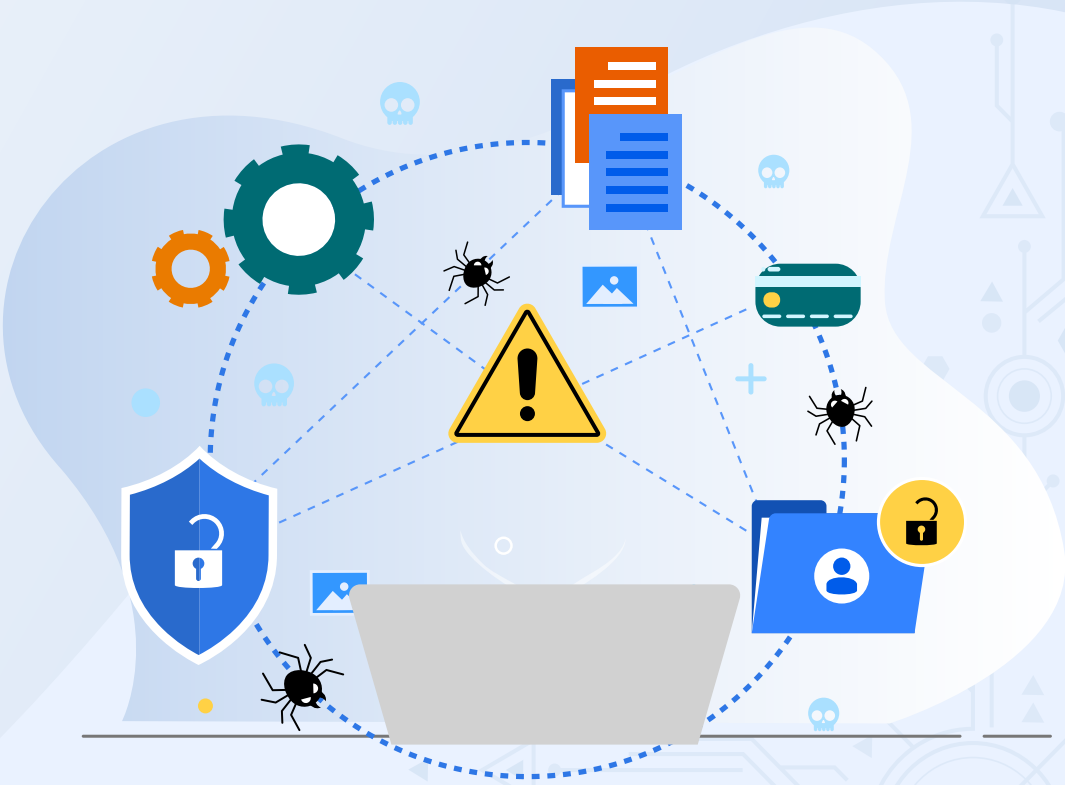
GENERAL GUIDELINES

- Your password must be 8 to 16 characters.
- Use a strong password or PIN; avoid easy numbers such as 1234 or your date of birth.
- Your password must include 1 uppercase (capital letter), 1 lowercase (small letter), 1 number/digit, and 1 special character.
- Avoid using obvious information (easy to guess) like your name or date of birth for password.
- Never share your user ID, password, OTP and T-PIN with anyone.
- Change passwords immediately if you suspect or if they may have been compromised.
- Use different passwords for different accounts.
- Do not save login credentials within a browser.
- Enable screen lock and always keep your phone locked when not in use.
- Keep your computer up to date with security patches and updates on your operating system and software.
- Keep your mobile up to date with latest firmware and avoid installing application other than Google Play Store or App Store.
- Keep anti-virus and anti-spyware software installed and updated.
- It is crucial to utilize anti-virus and anti-spyware programs from reputable and trustworthy companies.
- Be careful when opening emails, unverified links through SMS and forwarded messages.
- Some emails may contain malicious data. Be extra careful when an email asks for sensitive information such as your password.
- Stay away from suspicious websites. Some websites can contain malicious codes that can infect your computer.
- Consider using a firewall to protect your network.
- Be careful when using public Wi-Fi connection. Also, be careful when using public computer as public computers could be infected with malware.
- Always log out of your banking app or website when you're done, and close the app/browser completely. This Ensure to secure your phone device with basic security standards like password, PIN, pattern or biometric.
- Turn on auto-wipe so your device erases data after multiple incorrect password attempts.

DIGITAL BANKING FRAUD SCAMS & TRENDS – BE AWARE / BE CAREFUL

Social Media Scams

Fraudsters use fake emergencies, job offers, purchases, and investment schemes on social media to trap users.



Stay Safe

- Verify urgent money requests through another channel.
- Shop only from trusted sites; avoid “too good to be true” deals.
- Don’t click suspicious links or share personal info.
- Research before investing; avoid “guaranteed returns.”
- Report fake profiles immediately.

Fake Calls / SMS / WhatsApp link

Fraudster will call you from unknown mobile number, Bank UAN number 042-111-222-642 claiming to be MCB Islamic Bank Ltd, SBP, Law enforcement agencies, NAB, Benazir Income Support Program, NADRA, FIA, Army, Police or any other Government organization for verification, account maintenance and updation through WhatsApp link, Email, SMS, Web link etc.

MCB Islamic Bank will never contact you via UAN number 042-111-222-642 or on an unsolicited basis to ask for your digital banking credentials.

Indicators

- Fraudster will call you and mention some of your confidential information to gain your trust.
- They will create a sense of urgency that you have missed a deadline and demand immediate action.
- They may resort to using threats of terminating bank services or closing accounts to create panic.
- They will persuade you to share confidential info like Password, PIN and T-PIN/OTP.

Precautions

- Do not share your confidential details with anyone over the calls / SMS, WhatsApp link and emails etc.
- MCB Islamic Bank never obtains or asks for personal / banking details.
- Do not panic as MCB Islamic Bank never make a call from UAN number

Impersonation on social media

- Fraudsters create fake accounts using details of the users of media platforms such as Facebook, Instagram, Twitter, etc.
- Fraudsters then send a request to the users' friends asking for money for urgent medical purposes, payments, etc.
- Fraudsters, using fake details, also contact users and gain users trust over a period of time. When the users' share their personal or private information, the fraudsters use such information to blackmail or extort money from the users.

Precautions

- Always verify the genuineness of a fund request from a friend / relative by confirming through a phone call / physical meeting to be sure that the profile is not impersonated.
- Do not make payments to unknown persons online. Do not share personal and confidential information on social media platforms.

Smishing

Smishing refers to fraud conducted through SMS, where you may receive fake text messages that look like they have come from your bank, or another trusted organisation. The primary objective here is to get you to reply with your personal or financial information.

Precautions

- Typically, the text message may include an urgent call-to-action by either clicking on a certain link or dialing a number. If you receive any suspicious message, do not click on any link or number.
- Once the victim has contacted them, they would pose as someone from the Bank or an authority requesting them their personal information.
- Do not give any personal information to anyone in any situation (e.g. for Cancellation/Activation of your Card).
- MCB Islamic Bank never claims that your account may be closed or blocked if you fail to confirm, verify, or authenticate your personal information via a Phone call, SMS or Email.

Fake Mobile Banking App

- Fraudsters use various means such as SMS / email / social media / Instant Messenger, etc., to circulate certain app links cleverly masked to appear similar to the existing apps of authorized entities.
- Fraudsters trick the customer to click on such links which results in downloading of unknown / unverified apps on the customer's mobile / laptop / desktop, etc.,
- Once the malicious application is downloaded, the fraudster gains complete access to the customer's device. These include confidential details stored on the device and messages / OTPs received before & after installation of such apps.

Precautions

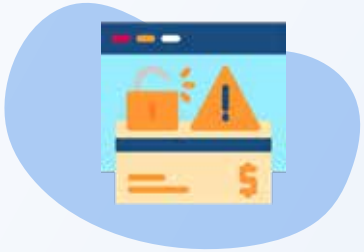
- Always download MCB Islamic Subuk App from "Google Play Store" GET IT ON Google Play and "Apple App Store" Download on the App Store only
- Do not download from a third-party website / WhatsApp link or somewhere else.
- Never download an application from any unverified / unknown sources or on being asked/ guided by an unknown person.

Phishing

- Fraudsters create a third-party phishing website which looks like an existing genuine website, such as - a bank's website or an e-commerce website or a search engine, etc.
- Links to these websites are circulated by fraudsters through Short Message Service (SMS) / social media / email / Instant Messenger etc.
- Many customers click on the link without checking the detailed Uniform Resource Locator (URL) and enter secure credentials such as Personal Identification Number (PIN), One Time Password (OTP), User ID, CNIC , Mother name , Password, etc., which are captured and used by the fraudsters.

Spear Phishing

Spear phishing is highly targeted phishing attack. Spear phishers send email that appear genuine and come from a trusted source like a work colleague, boss, friend, family, your bank, or government organization. The aim of the spear phishing is to trick the victim into performing actions he/she will not usually do.



First

Criminals gather information about the target victim and/ or organization. They often obtain it through websites, blogs, and social networking sites.

Then

They send e-mails that look like the real thing to targeted victims, offering all sorts of urgent and legitimate-sounding explanations as to why they need the information.

Finally

The victims are asked to either reply to the message, click on a link inside the e-mail, or open a file.

Precautions

- Do not click on unknown / unverified links and immediately delete such SMS / email sent by unknown sender to avoid accessing them by mistake in future.
- Unsubscribe the mails providing links to a bank / e-commerce / search engine website and block the sender's e-mail ID, before deleting such emails.
- Always go to the official website of your bank / service provider. Carefully verify the website details especially where it requires entering financial credentials. Check for the secure sign (https with a padlock symbol) on the website before entering secure credentials.
- Check URLs and domain names received in emails for spelling errors. In case of suspicion.

Sim Swapping / SIM cloning Fraud

- SIM swapping is when a scammer transfers your phone number to another device to access your accounts. This means the attacker hijacks the victims' phone number and assigns it to the SIM card owned by them.
- In SIM swap scams, fraudsters get a new SIM card issued against your registered mobile number via the mobile service provider.

Indicators

- Loss of signals
- Inability to send or receive SMS and calls
- Security notifications
- Inability to use apps on your phone

Precautions

- Never share identity credentials pertaining to your SIM card.
- Be watchful regarding mobile network access in your phone. If there is no mobile network in your phone for a considerable span of time in a regular environment, immediately contact the mobile operator to ensure that no duplicate SIM is being / has been issued for your mobile number.

Shoulder Surfing / Card Trapping

Refers to using direct observation techniques such as looking over someone's shoulder to get confidential information at any places like ATM room, restaurant and shopping mall etc. Shoulder surfing is particularly effective in crowded places.

Precautions

- Please make sure to lock ATM door until completion of necessary usage of ATM.
- Never accept help from strangers during the ATM transactions.
- Be aware of others around you, if someone is watching you, choose a different ATM.
- Do not share your ATM PIN with anybody.
- If your card gets captured or stuck in the ATM, never share PIN or password with strangers, call Phone Banking immediately at 042 111 222 642 for assistance and for temporary blocking of Digital Banking services.

Card Not Present Fraud

Purchases over the internet, phone, or mail from a stolen, lost or compromised debit card are considered to be scams under Card Not Present.

Precautions

- The customers should not store codes such as CVV on any device.
- Avoid Phishing attacks, look out for not providing your card details on the websites or emails requiring your card details.
- Never provide your transaction generated OTP to any individual or imposter
- Remember, imposters can use any identity such as Law Enforcement agencies or Banking Authority.
- Always signup for transaction alert for all activities on your cards.
- Always use card on trusted platforms/ websites and never share card information with anyone.
- Further, it is strongly advised to activate the e-commerce service on card only for the time period during which intent to conduct an online transaction

ATM Scams / Card Skimming

- Fraudsters install skimming devices in ATM machines and steal data from the customer's card.
- Fraudsters may also install a dummy keypad or a small / pinhole camera, well-hidden from plain sight to capture ATM PIN.
- Sometimes, fraudsters pretending to be other customer standing near-by gain access to the PIN when the customer enters it in an ATM machine.
- This data is then used to create a duplicate card and withdraw money from the customer's account.

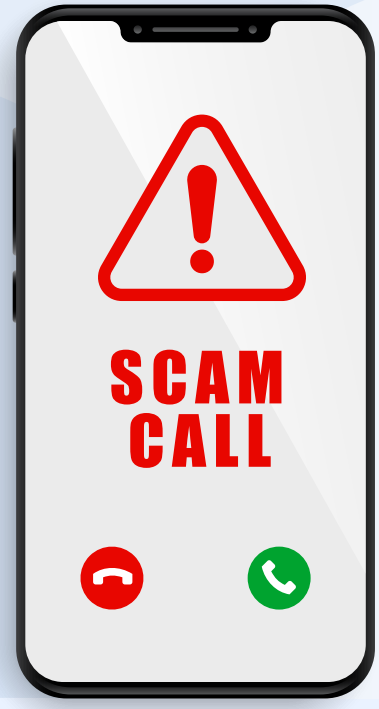
Precautions

- Always check that there is no extra device attached, near the card insertion slot or keypad of the ATM machine, before making a transaction.
- Cover the keypad with your other hand while entering the PIN.
- NEVER write the PIN on your ATM card.
- Do not enter the PIN in the presence of any other / unknown person standing close to you.
- Do not follow the instructions given by any unknown person or take assistance / guidance from strangers / unknown persons at the ATMs.
- Always use familiar ATMs

Call Spoofing

(Benazir Income Support Program,
Ehsaas Program & Jeeto Pakistan)

Call Spoofing in general is often used as a part of an attempt to trick someone into giving away valuable information so that it can be used in the fraudulent activity. In the current era, call spoofing has become very common based on the ability to create spoofed caller ID very easily. The caller usually pretends to be someone else.

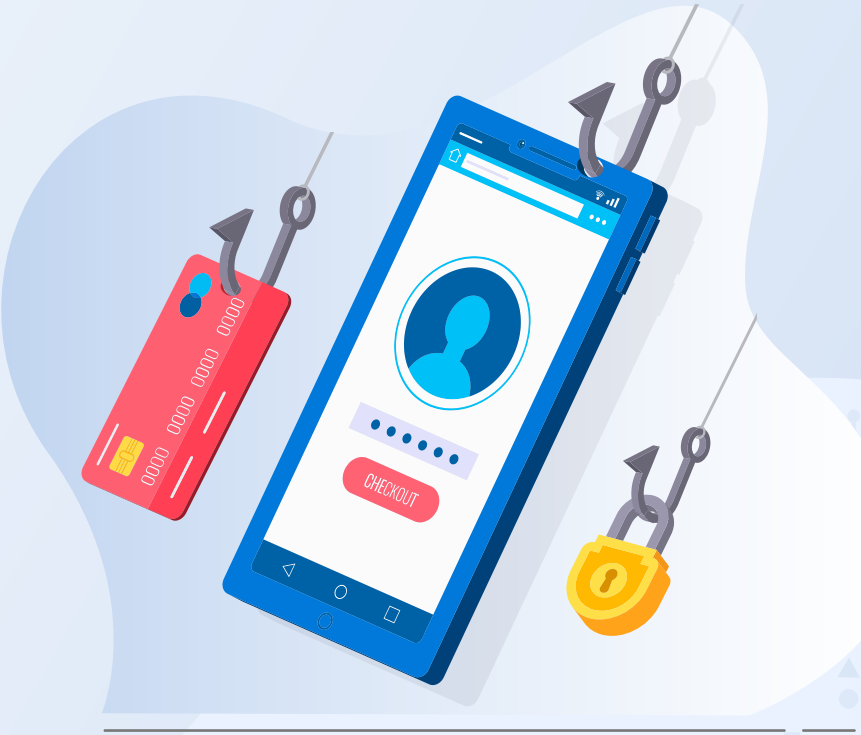


Precautions

- Imposters can also pretend to be calling from security or law enforcement agencies or a central bank with intention of calling for a purpose that can trick or lure the customers to give away the personal information such as: Name, CVV, Date of Birth, Mother's Name and OTP generated. Once this information is shared, the fraudulent activities such as Bank Transfer or Online Purchases are initiated.

Vishing

- Imposters call or approach the customers through telephone call / social media posing as bankers / company executives / insurance agents / government officials, etc. To gain confidence, imposters share a few customer details such as the customer's name, account number or date of birth.
- In some cases, imposters pressurize / trick customers into sharing confidential details such as passwords / OTP / PIN / Debit Card number etc., by citing an urgency / emergency such as - need to block an unauthorized transaction, payment required to stop some penalty, an attractive discount, etc. These credentials are then used to defraud the customers.

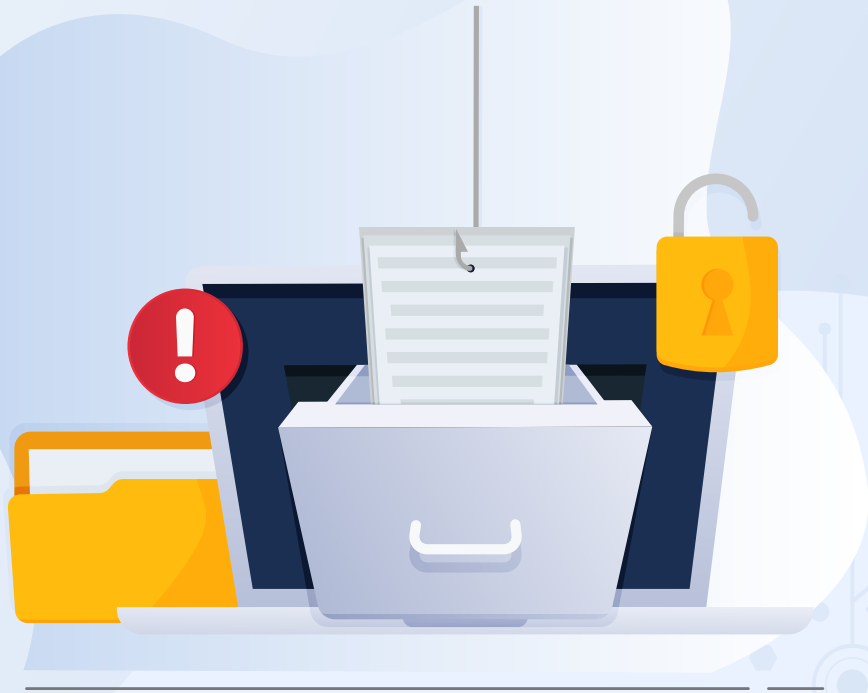


Precautions

- Bank officials / financial institutions / SBP/ any government entity never ask customers to share confidential information such as username / password / debit card details / CVV / OTP etc.
- Never share these confidential details with anyone, even your own family members, friends and bank officials.

Limit Enhancement Frauds

- In the recent fraud trend, it has been observed that the fraudsters approached Bank customers while pretending to be Bank representative and convinced them to hand over their Debit along with the PIN for Limit Increase / Activation.
- Once the cards are handed over to an authorized person, later on these cards are used on different merchants/ATMs for fraudulent activities.

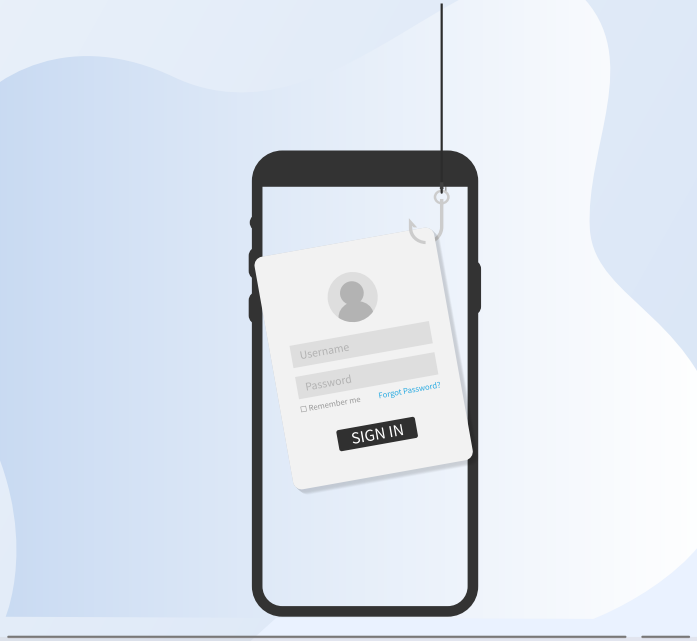


Precautions

- No Bank Representative is authorized to ask for a physical possession of Debit Card for replacement, activation or limit increase.
- Never give away your cards physically to any person in any situation claiming to be a Bank Representative or any person from a Government Agency

Account Take Over

A form of identity theft where access to clients' banking services is gained by imposters where fraudsters are able to access client's information and banking account without authorization. This is usually caused by either: Falling in trick used by the scammers using fictitious emails to force client to disclose personal information or banking details which allows them access to the accounts.



Precautions

- Devices can get compromised by installing malicious software emailed to client with a link. This can steal your personal data once you visit the link.
- Access to personal information can lead the fraudsters to request SIM replacement cards to gain access to authentication messages sent to your mobile.
- Keep your financial records, Social Security and Medicare cards in a safe place.
- Shred papers that have your personal or medical information.
- Take mail out of your mailbox as soon as you can.
- Do not give your personal information to someone who calls you or emails you.
- Use passwords that are not easy to guess. Use numbers and symbols when you can.
- Do not respond to emails or other messages that ask for personal information.
- Do not put personal information on a computer in a public place, like the library.

Juice Jacking

The charging port of a mobile, can also be used to transfer files / data. Fraudsters use public charging ports to transfer malware to customer phones connected there and take control / access / steal data sensitive data such as emails, SMS, saved passwords, etc. from the customers' mobile phones (Juice Jacking).

Precautions

- Avoid using public / unknown charging ports / cables.

Online Job Fraud

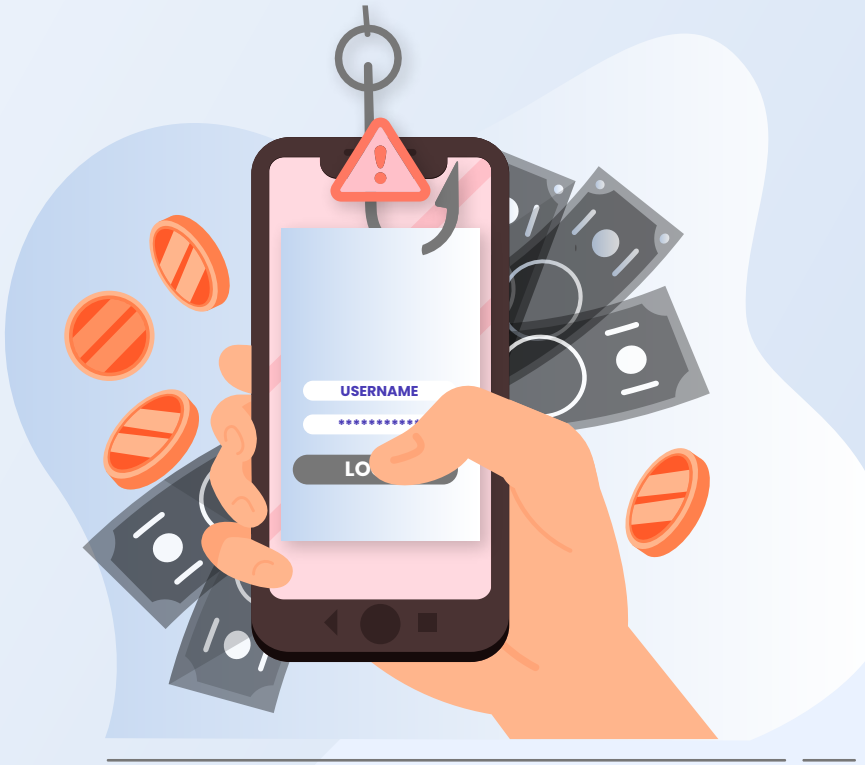
- Fraudsters create fake job search websites and when the job seekers share secure credentials of their bank account / debit card on these websites during registration, their accounts are compromised.
- Fraudsters also pose as officials of reputed company(s) and offer employment after conducting fake interviews. The job seeker is then induced to transfer funds for registration, mandatory training program, laptop, etc.

Precautions

- In case of any job offer, including from overseas entities, first confirm the identity and contact details of the employing company / its representative.
- Always remember that a genuine company offering a job will never ask for money for offering the job.
- Do not make payments on unknown job search websites.

Ponzi & Pyramid Scheme Scams

Fraudsters lure victims with fake investments, offering unrealistic profits or referral rewards. These schemes eventually collapse, causing heavy losses.



Precautions

- Be skeptical of “too good to be true” returns.
- Verify the legitimacy of any investment before committing.
- Avoid schemes based on recruiting others for rewards.

Discount Scams

Fake discounts and cloned shopping websites spike during holiday and clearance sales. Fraudsters use these traps to steal money and banking details.

Precautions

- Shop only from official and trusted websites.
- Carefully check URLs avoid fake or redirected pages.
- Never click on suspicious links or share your Password, OTP, or PIN.

REPORTING OF FRAUD

In case of any fraud related issues / complaint, immediately contact us

24/7 +92-42-111-222-642

info@mcbislamicbank.com

FAX +92-21-34972150