# SECURITY TIPS

**STOP** **THINK** **PROTECT**

**Al Ahli Bank of Kuwait K.S.C.P. (ABK) will never ask you to disclose your personal card details such as the Card PIN number, CVV or any confidential banking details.**

**Your Card PIN must be kept secret and known only to you.**

**If in doubt about any email, call or text message, please call our 24/7 Call Center number +971 4 607 5507 (within / outside UAE).**

**SMISHING** | **PHISHING** | **VISHING**

**SIM SWAP** | **IDENTITY FRAUD** | **ATM SAFETY TIPS**

**PASSWORD TIPS** | **OTP – ONE TIME PASSWORD TIPS** | **ONLINE BANKING SECURITY TIPS**

**MOBILE BANKING SECURITY TIPS** | **CASH DEPOSIT FRAUD** | **CHEQUE FRAUD**

**BUSINESS EMAIL COMPROMISE INVOICE FRAUD**

## SMISHING

- Beware and do not be a victim of fraud communication. You may receive an SMS message informing that your Debit Card is blocked, deactivated, or that your Bank Account is blocked with instructions to call a specific number to reactivate your Debit Card or Bank Account.
- The Caller may present him/herself as an ABK staff member and request for your personal and banking information and One Time Password.
- This information will allow the scammer to have access and make unauthorized transactions from your bank accounts.
- Beware Scammers may use Caller ID spoofing technology to mask their actual phone number and display the Bank's number.

**Protect yourself from Smishing:**

- Do not disclose your banking details i.e. your account numbers, card numbers, your username, PIN (Personal Identification Number) or OTP (One-Time Password) to anyone via phone, SMS or Email.
- In case you receive such a suspicious call or message do not reveal any of the above mentioned details, hang up and please contact us on our 24/7 call center number +971 4 607 5507 (within / outside UAE) to verify the authenticity of the request.
- Do not call on the number provided by scammer.

## PHISHING

- Phishing is the act of sending an e-mail, text message or calling and falsely claiming to be an established, legitimate enterprise in this case, a Bank, to scam the user into sharing private information that will be used for identity theft. Requests from unauthorized channels for your personal information are known as phishing attempts.
- In cases of an e-mail or text message phishing attack, the message will direct the user to visit a Web site where they are asked to update personal information, such as passwords, credit card and bank account numbers. The website, however, is fake and set up only to steal the user's information.

**Protect yourself from Phishing**

- Look for warning signs like requests for personal information. Note: ABK will never ask for any of your personal information by email, text message, or random phone calls.
- Look out for the language and tone of the email/text message, fraud messages usually urge you to act quickly and make a suggestion that your account is vulnerable or is likely to be closed if you do not provide the personal information.
- In case you receive any suspicious e-mail, text message or call, do not reveal any of the above mentioned details, hang up and please contact us on our 24/7 call center number +971 4 607 5507 (within / outside UAE) to verify the authenticity of the request.

## VISHING

- A scammer can call you via internet by modifying his caller ID to match with our Bank's number and present him/herself as an ABK staff member.
- The scammer's intention is to mislead you to get hold of your account numbers, card numbers, PIN, online user ID and password or other personal information.
- A scammer can also give you a fake call saying that you have won a lottery or a cash prize on your card or phone number. The scammer will ask for your card number and PIN, which they will use for conducting fraudulent transactions on your account / card.
- Scammer may also ask you to transfer a certain amount of money as a processing fee to claim the prize you have won.

**Protect yourself from Vishing:**

- Understand the motive of the caller and establish his identity before disclosing any information the scammer is seeking from you.
- Do not disclose your banking details i.e. your account numbers, card numbers, username, PIN (Personal Identification Number) or OTP (One-Time Password).
- Always monitor your bank statement and check your account balances to identify any unauthorized transactions. In case you find any unauthorized transactions, you can contact us 24/7 on our call center number +971 4 607 5507 (within / outside UAE).
- In case you have already reveled your personal and banking details to the scammer and then realized that it was a scam, report immediately to ABK by calling our 24/7 call center number +971 4 607 5507 (within / outside UAE).

## SIM SWAP

Mobile banking has gained a lot of popularity because of its convenient accessibility. However, Fraudster can try to misuse these services:

- A fraudster can impersonate him/herself as you and approach your mobile service provider and request for a replacement of SIM (SIM swap).
- They can call your bank from the replaced SIM and get access to your bank account.
- Fraudster can add beneficiaries to your account and transfer funds from your account.

**Prevent SIM Swap Fraud:**

- Contact your mobile service provider immediately If:
  - Connectivity is lost on your mobile.
  - You have not received any calls or sms on your mobile.
  - If you receive “SIM not registered” or “SIM replacement” notification on your mobile phone.
- Always monitor your banking transactions, check your account statements, and if you find any discrepancy, report immediately to ABK by calling our 24/7 call center number +971 4 607 5507 (within / outside UAE).
- Register for SMS / Email notifications for activities on your bank account.

## IDENTITY FRAUD

**The Fraudster can use the following information to establish your identity and conduct a Fraud:**

- Name
- Date of birth
- Address
- Emirates / Civil ID number.
- Banking information
- Mobile number

**Protect your identity:**

- Upon loss or theft of your important documents such as your passport, Emirates / Civil ID debit / credit cards report to the Bank.
- Your financial and personal documents should be kept secured.
- Do not write your PIN on the card or save on your device or carry it in your wallet.
- Do not disclose your personal information over phone calls or emails to anyone.

## ATM SAFETY TIPS

- Memorize your PIN. Do not write it down anywhere, and certainly never on the card itself.
- Do not share your PIN or card with anyone, not even your friends or family.
- When at the ATM machine use your hand to shield the keypad as you enter the PIN.
- Do not take help from strangers for using the ATM card or handling your cash.
- If your ATM card is lost or stolen, report it to nearest ABK branch and inform call center to block the card immediately.
- When you deposit a cheque or card into your ATM, check the credit entry in your account after a couple of days. If there is any discrepancy, report immediately to ABK by calling our 24/7 call center number +971 4 607 5507 (within / outside UAE).
- If your card gets stuck in the ATM, or if cash is not dispensed after you have keyed in a transaction, report immediately to ABK by calling our 24/7 call center number +971 4 607 5507 (within / outside UAE).

| PASSWORD TIPS |
| --- |
| • Do not use passwords e.g. your name for birth dates, your children name or their birth dates, telephone numbers etc.<br>• Do not disclose your password to anyone.<br>• Change your password regularly<br>• In case your password has been used or accessed by anyone immediately contact us on our 24/7 call center number +971 4 607 5507 (within / outside UAE). |

## OTP – ONE TIME PASSWORD TIPS

- Never Share your OTP with anyone.
- ABK staff will never ask for your OTP/PIN/CVV/Password
- Inform us when you change your mobile number registered with ABK
- Beware of strange phone calls trying to obtain confidential or banking
- Ensure you operate banking transaction from trusted and secure devices

## ONLINE BANKING SECURITY TIPS

- Never fill out any personal banking information in an email, surveys or feedback forms.
- Memorize your passwords rather than writing them somewhere, and never share or give out your information.
- Every time you complete your online banking session, Sign off from www.eahli.com. Do not just close your browser.
- To access eahli online banking, always type in the correct URL (https://abk.eahli.com) into your browser window. Never click a link that offers to take you to our website.
- Change your Online Banking passwords regularly. Example: Once in 3 months.
- Your password should not be easy to guess. Use letters, numbers and special characters [such as !,@, #,$, %, ^, &,* (, )] in your passwords.
- Never share your Online Banking passwords with others, even family members.
- Always check the last sign-in to your Online Banking account. Log in to Online Banking account and see at the bottom “User Information” to view the date and time of your last sign-in.
- Ensure you have Anti-Virus Software installed, updated and running. Always use security software with an anti-virus, anti –spyware and firewall features to protect your computer.

## MOBILE BANKING SECURITY TIPS

- Set up a Pin/password/fingerprint to access your mobile phone
- Register for SMS alerts to keep track of your banking transactions.
- Do not click on any links in a message requesting any bank information.
- If you have to share your mobile with anyone else or send it for repair/maintenance
    - Clear the browsing history
    - Clear cache and temporary files stored in the memory as they may contain your account numbers and other sensitive information
    - Block your mobile banking applications by contacting your bank. You can unblock them when you get the mobile back
- Do not save confidential information such as your debit/credit card numbers, CVV numbers or PIN's on your mobile phone
- Keep your mobile's operating system and applications, including the browser, updated with the latest security patches and upgrades
- Do not enable auto-fill or save user IDs or passwords for mobile banking online
- Avoid using unsecured Wi-Fi, public or shared networks
- Only download apps from official app stores such as Apple iTunes, Google Play Store
- Never disclose personal information or online banking credentials via e-mail or text message as these can be used for identity theft
- Log out from online mobile banking or application as soon as you have completed your transactions and close that window.
- Take extra care while typing confidential information such as your account details and password on your mobile in public places
- In case you lose your mobile phone, please call our 24-hour Customer Care to disable the ABK mobile app.

## CASH DEPOSIT FRAUD

- Ensure you handover cash only to the teller and obtain cash deposit slip stamped and signed by the teller.
- Keep copy of all transactions.
- Always monitor your banking transactions, check your account statements, if you find any discrepancy, report immediately to ABK by calling our 24/7 call center number +971 4 607 5507 (within / outside UAE).

## CHEQUE FRAUD

Cheque fraud is done by depositing fake/manipulated cheques for payments and causes loss to you. There are various types of cheque frauds, some of which are mentioned below.

- **Cheque Washing**: A fraudsters manipulates all or some of the details related to the amount, date & beneficiary to cash the cheque.
- **Magic Ink Pen Usage**: Occurs when receiving a cheque for a genuine transaction, the cheque issuer is persuaded to fill up details related to amount and/or beneficiary by a pen provided by the 3rd party. The writing of such "magic ink" pens, disappears after a while and the fraudster fills up desired amount and beneficiary name to fraudulently cash such cheques.
- **Fake Cheques:** Fraudsters create genuine looking cheques by copying details from original cheques including signatures.
- **Cheque Theft:** Cheques are stolen from the victims or those in transit and then fraudulently deposited for payments.

**To prevent cheque Frauds:**

- Keep your cheque books safe & secure at all times.
- Do not leave signed cheques unattended.
- Upon receipt of new cheque book, ensure your cheque book is intact and no cheque leaves are missing. Notify the Bank immediately if cheque leaves are missing.
- Do not leave space before and after payee name, amount (in numbers and words) and draw lines at the end.
- Cross your cheque by drawing 2 parallel lines on top left corner of the cheque to prevent misuse
- Consider having different set of signatories depending upon amount thresholds.
- Destroy cheques with errors, overwriting or spoiled.
- Regularly check SMS and emails for communication from the Bank.
- Always monitor your banking transactions, check your account statements, and contact the Bank immediately if you find any discrepancy.
- Don't issue cheques to unknown people, sometimes fraudsters offer deals which are "Too good to be true" to get a cheque sample from victims.

- If someone offers you a pen to write on certain documents, be careful and check whether this could be a “magic Ink” pen. Remember that usage of such pens is prohibited in UAE & any person found to be using such pens may end up getting reported to relevant authorities.
- If you receive cheque payments from 3rd parties don’t deliver goods/services till the cheque is credited to your account.
- Don’t act as “Money mule” by depositing cheques on behalf of others and making them part payment in cash/transfers from your account. If such a cheque is later on proved to be fraudulent, person/entity whose accounts was used to deposit cheque might have to return the funds to the victim.
- All cheques have security features, some of which are printed on the front/back of the cheque. Please ensure that any cheque being presented by you contains those security features.
- Where possible try using electronic banking facilities offered by the Bank instead of issuing cheques for payments. In case you become a victim of cheque fraud, report immediately to ABK by calling our 24/7 call center number +971 4 607 5507 (within / outside UAE) and also consider filing a police complaint.

## BUSINESS EMAIL COMPROMISE – INVOICE FRAUD

For the purpose of unauthorized funds transfer, a type of payment fraud that compromises of legitimate business e-mail or creating lookalike domain name accounts.

**Funds Transfer Requests from Suppliers or Business Partners:**

- Email ID of an employee of the target company is compromised by the fraudster.
- Fraudster monitors emails of the business user, looking for supplier invoices
- Fraudster finds a legitimate invoice and modifies the beneficiary information, such as changing the IBAN / account number to which payment is to be sent.
- A vendor's email id is disguised to submit the modified invoice. It doesn't require compromising the supplier's email system, but instead sends the invoice from an email address that is so close to the domain of the vendor, that mostly the change would be missed out; for example, @companyXZY.com instead of @companyXYZD.com.
- When the company receives payment requests and fake invoices through emails, they would recognize the supplier's name and services provided. So they would process the invoice and submit a funds transfer request to them for payment

**Funds Transfer Requests From Executive / Management Staff:**

- A fraudster can compromise the email account of a Senior Management Executives (CEO, COO, CFO, etc.) and send a funds transfer request from the compromised email ID to the finance department staff.

**You should**

- Enhance your company security infrastructure and protect your company domain or servers.
- Always enquire about funds transfer requests to any new beneficiary account information
- For known suppliers, observe for change in payment request patterns i.e. high value, different currency, out of cycle.
- Increase awareness amongst staff
- Validate email IDs (spelling and disguised IDs) of the sender requesting the funds transfer.
- Before sending fund transfer instructions to your bank, get a telephonic confirmation from the sender of the email who could be your suppliers or company executives.

FOR FURTHER DETAILS ON TYPES OF FRAUD YOU MAY PLEASE VISIT : https://www.uaebf.ae/en/fight-fraud/fraud-2021-details/3