Remember the following:

- Do not carry personal details or the bank card with its secret number, PIN number or Security Code to the bank immediately.
- Be very suspicious of any e-mail from a person that asks for your Password, Passport number, Account or Credit Card information unless you have initiated the transaction. Similarly, be wary of any e-mail that asks you to update your personal bank account information.
- Use a unique password and PIN and change it regularly.
- Keep your passwords in a safe place and do not disclose them to anyone, such as: the bank card number, your card password or the password to your account via the bank's internet service.
- Immediately report any call you receive or a text message stating that a banking transaction has been completed from your account that you are not aware of.

Best practices to protect your bank account

- Do not carry personal details or the bank card with its secret numbers in one place.
- Always use strong passwords, which cannot be easily guessed and do not use the same password for multiple accounts.
- Keep your passwords in a safe place and do not disclose them to any other party.
- Pay close attention to the ATM that you intend to use if you notice strange things such as: devices, wires, adhesives, magnetic tapes, do not use that machine. Look at the card reader, if you see a plastic strip or the like, do not put your card in the machine and report it to the bank immediately.

Mobile Phone Fraud Attack

In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller’s identity to impersonate a bank employee. They try to obtain confidential information such as your card numbers, passwords, and any other information related to your account, citing many reasons, including updating records system and other reasons to obtain your private information.

How to protect yourself

- Verify the identity of the caller and the reason for calling before continuing to talk to him, especially since he is not known to you.
- Be very suspicious of any e-mail from an unknown person that asks you to update your personal account information.
- Do not disclose your password or PIN to anyone – not even the bank employees.
- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure they are correct.

How to protect yourself

- Be very suspicious of any e-mail from a person that asks for your Password, Passport number, Account or Credit Card information unless you have initiated the transaction. Similarly, be wary of any e-mail that asks you to update your personal bank account information.
- Use a unique password and PIN and change it regularly. You should never disclose your password or PIN to anyone – not even the bank employees.
- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure they are correct.
- Do not use that machine. Look at the card reader, if you see a plastic strip or the like, do not put your card in the machine and report it to the bank immediately.

Maintaining customer information and its confidentiality is a priority for the Arab Investment Bank. We are constantly updated with the latest developments in the field of information security and protection in order to provide the maximum and best ways to protect the information and data that belong to our customers and their accounts. The following are some general tips that our esteemed bank customers should follow in order to protect their bank accounts from any cyber-attacks.

Fraudulent emails are used by criminals to lure you to fake websites, which resemble original websites of financial institutions, and ask you to divulge personal information such as: Account number, Credit card number, PIN number or Security authentication.

In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller’s identity to impersonate a bank employee. They try to obtain confidential information such as your card numbers, passwords, and any other information related to your account, citing many reasons, including updating records system and other reasons to obtain your private information. In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller’s identity to impersonate a bank employee. They try to obtain confidential information such as your card numbers, passwords, and any other information related to your account, citing many reasons, including updating records system and other reasons to obtain your private information.

How to protect yourself

- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure they are correct.
- Do not use that machine. Look at the card reader, if you see a plastic strip or the like, do not put your card in the machine and report it to the bank immediately.

General Security tips to protect your bank account against the following attacks:

Phishing Attack

Fraudulent emails are used by criminals to lure you to fake websites, which resemble original websites of financial institutions, and ask you to divulge personal information such as: Account number, Credit card number, PIN number or Security authentication.

In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller’s identity to impersonate a bank employee. They try to obtain confidential information such as your card numbers, passwords, and any other information related to your account, citing many reasons, including updating records system and other reasons to obtain your private information.

How to protect yourself

- Be very suspicious of any e-mail from a person that asks for your Password, Passport number, Account or Credit Card information unless you have initiated the transaction. Similarly, be wary of any e-mail that asks you to update your personal bank account information.
- Use a unique password and PIN and change it regularly. You should never disclose your password or PIN to anyone – not even the bank employees.
- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure they are correct.
- Do not use that machine. Look at the card reader, if you see a plastic strip or the like, do not put your card in the machine and report it to the bank immediately.

General Security tips to protect your bank account against the following attacks:

Phishing Attack

Fraudulent emails are used by criminals to lure you to fake websites, which resemble original websites of financial institutions, and ask you to divulge personal information such as: Account number, Credit card number, PIN number or Security authentication.

In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller’s identity to impersonate a bank employee. They try to obtain confidential information such as your card numbers, passwords, and any other information related to your account, citing many reasons, including updating records system and other reasons to obtain your private information.

How to protect yourself

- Be very suspicious of any e-mail from a person that asks for your Password, Passport number, Account or Credit Card information unless you have initiated the transaction. Similarly, be wary of any e-mail that asks you to update your personal bank account information.
- Use a unique password and PIN and change it regularly. You should never disclose your password or PIN to anyone – not even the bank employees.
- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure they are correct.
- Do not use that machine. Look at the card reader, if you see a plastic strip or the like, do not put your card in the machine and report it to the bank immediately.

General Security tips to protect your bank account against the following attacks:

Phishing Attack

Fraudulent emails are used by criminals to lure you to fake websites, which resemble original websites of financial institutions, and ask you to divulge personal information such as: Account number, Credit card number, PIN number or Security authentication.

In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller’s identity to impersonate a bank employee. They try to obtain confidential information such as your card numbers, passwords, and any other information related to your account, citing many reasons, including updating records system and other reasons to obtain your private information.

How to protect yourself

- Be very suspicious of any e-mail from a person that asks for your Password, Passport number, Account or Credit Card information unless you have initiated the transaction. Similarly, be wary of any e-mail that asks you to update your personal bank account information.
- Use a unique password and PIN and change it regularly. You should never disclose your password or PIN to anyone – not even the bank employees.
- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure they are correct.
- Do not use that machine. Look at the card reader, if you see a plastic strip or the like, do not put your card in the machine and report it to the bank immediately.

General Security tips to protect your bank account against the following attacks:

Phishing Attack

Fraudulent emails are used by criminals to lure you to fake websites, which resemble original websites of financial institutions, and ask you to divulge personal information such as: Account number, Credit card number, PIN number or Security authentication.

In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller’s identity to impersonate a bank employee. They try to obtain confidential information such as your card numbers, passwords, and any other information related to your account, citing many reasons, including updating records system and other reasons to obtain your private information.

How to protect yourself

- Be very suspicious of any e-mail from a person that asks for your Password, Passport number, Account or Credit Card information unless you have initiated the transaction. Similarly, be wary of any e-mail that asks you to update your personal bank account information.
- Use a unique password and PIN and change it regularly. You should never disclose your password or PIN to anyone – not even the bank employees.
- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure they are correct.
- Do not use that machine. Look at the card reader, if you see a plastic strip or the like, do not put your card in the machine and report it to the bank immediately.

General Security tips to protect your bank account against the following attacks:

Phishing Attack

Fraudulent emails are used by criminals to lure you to fake websites, which resemble original websites of financial institutions, and ask you to divulge personal information such as: Account number, Credit card number, PIN number or Security authentication.

In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller’s identity to impersonate a bank employee. They try to obtain confidential information such as your card numbers, passwords, and any other information related to your account, citing many reasons, including updating records system and other reasons to obtain your private information.

How to protect yourself

- Be very suspicious of any e-mail from a person that asks for your Password, Passport number, Account or Credit Card information unless you have initiated the transaction. Similarly, be wary of any e-mail that asks you to update your personal bank account information.
- Use a unique password and PIN and change it regularly. You should never disclose your password or PIN to anyone – not even the bank employees.
- Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure they are correct.
- Do not use that machine. Look at the card reader, if you see a plastic strip or the like, do not put your card in the machine and report it to the bank immediately.