

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 account from any cyber-attacks.

ان المحافظه علي معلومات العملاء وسريتها من الأولويات لدي بنك الاستثمار العربي، لذلك فأننا نقوم بالاطلاع المستمر علي أخر المستجدات في مجال أمن و حماية المعلومات من أجل توفير أقصى و أفضل السبل لحماية المعلومات والبيانات التي تخص العملاء و حساباتهم لدي بنك الاستثمار العربي و فيما يلي بعض النصائح العامة التي يجب ان يتبعها عملاء بنكنا الموقر من أجل حمايه حسابهم البنكي من اي هجمات إلكترونية.

Please watch the following video before continuing to read the tips below

(This video was produced by the Central Bank of Egypt)

<https://youtu.be/O-rCALHmvHo>

• برجاء مشاهدة الفيديو التالي قبل المتابعه في قرأه النصائح المذكوره بالاسفل

(هذا الفيديو تم إنتاجه من قُبل البنك المركزي المصري)

<https://youtu.be/O-rCALHmvHo>

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

نصائح عامه لحمايه حسابك البنكي من الهجمات التالية:

Phishing Attack

هجمات التصيد الإلكتروني

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.

وتستخدم رسائل البريد الإلكتروني الاحتيالية من قبل المجرمين لاستدراجك لمواقع وهمية، والتي تشابه المواقع الأصلية للمؤسسات المالية، وتطلب منك الإفصاح عن معلوماتك الشخصية مثل رقم الحساب، رقم بطاقة الائتمان، رقم التعريف السري لبطاقة الائتمان.

How to protect yourself

كيف تحمي نفسك

• 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 email that asks you to update your personal bank account information’s.

• Use a unique password or PIN and change it regularly. You should never disclose your password or PIN to anyone – not even to the bank employees.

• Monitor your transactions. Review your order confirmations, Credit Card and Bank Statements as soon as you receive them to make sure you are being charged only for transactions that have taken place. Immediately report any irregularities to aiBANK

• كن حذرا جدا من استقبال أي بريد إلكتروني من أي شخص يسأل عن كلمة السر أو رقم جواز السفر أو رقم حساب أو معلومات بطاقة الائتمان إلا إذا كنت قد بدأت بتنفيذ المعاملة وهي موثوق منها. على نحو مماثل، كن حذرًا من أي بريد اليكتروني يطلب منك تحديث معلومات حسابك المصرفي الشخصي.

• استخدام كلمة مرور مميزة أو PIN وقم بتغييرها بشكل منتظم. يجب أن لا تكشف عن كلمة السر الخاصة بك أو رقم التعريف الشخصي، ليس حتى لموظفي البنك.

• قم برصد معاملاتك. ومراجعة تأكيد العمليات، وبطاقة الائتمان الخاصة بك وبيانات كشف حسابك البنكي بمجرد الحصول عليه للتأكد من انه تم محاسبتك على المعاملات التي قمت بها بالفعل. والإبلاغ فورا عن أي مخالفات إلى بنك الاستثمار العربي.

Mobile Phone Fraud Attack

هجمات الاحتيال عن طريق الهاتف الجوال

In this case, fraudsters use the Internet to contact the customer. Fraudsters modify the caller's identity to impersonate as 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 mislead you.

يستخدم المحتالون في هذه الحالة شبكة الإنترنت للاتصال بالعميل، ويعدلون هويته المتصل لانتحال شخصية الموظفين، ثم يحاولون الحصول علي أرقام بطاقتك، ورقمك السري، والرقم السري لحسابك عبر خدمه النت الخاص بالبنك، ورقم حسابك، وأي معلومات أخرى خاصة بحسابك، متذرعين بأسباب كثيرة منها تحديث سجلات النظام وغيرها من الأسباب بهف تضليلك.

How to protect yourself

كيف تحمي نفسك

• 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.

• Beware of suspicious calls asking for private information.

• Not to disclose any information related to your bank account to anyone, such as: the bank card number, your card password or the password to your account via the bank's internet service, knowing that the bank will never ask for any private information from you.

• 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.

• تحقق من هوية المتصل وسبب اتصاله قبل مواصلة الحديث معه، و خاصة أنه غير معروف بنسبه لك.

• احذر من المكالمات الهاتفية المشبوهة التي تطلب منك معلومات خاصة.

• عدم الافصاح أو الكشف عن معلومات تتعلق بحسابك المصرفي لأي شخص كان مثل: رقم البطاقة المصرفية، الرقم السري لبطاقتك أو الرقم السري لحسابك عبر خدمة الانترنت بالبنك مع العلم بأن البنك لن يطلب مطلقاً أي معلومات خاصه منك.

• أبلغ فوراً عن أي مكالمه تتلقاها أو رساله نصيه تفيد عن إتمام معاملة مصرفيه من حسابك لا علم لك بها.

Best practices to protect your bank account

افضل الممارسات لحماية حسابك البنكي

• 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.

• لا تحمل تفاصيل شخصية أو البطاقة البنكية مع الأرقام السرية الخاصة بها في مكان واحد.

• استخدم دائماً كلمات مرور قوية، والتي لا يمكن تخمينها بسهولة ولا تستخدمها لحسابات متعددة.

• الاحتفاظ بالكلمات السرية الخاصة بك في مكان آمن ولا تكشف عنها لأي طرف اخر.

• انتبه جيدا الى جهاز الصراف الالي الذي تنوي استخدامه اذا لاحظت وجود اشياء غريبة مثل: اجهزة، اسلاك، مواد لاصقة، اشربة مغناطيسية، لا تستخدم ذلك الجهاز. انظر الى قارئ البطاقات، اذا شاهدت شريطا بلاستيكيًا او ما شابه ذلك لا تضع بطاقتك في الجهاز وابلغ البنك عنه فورا.

Remember the following:

تذكر الآتي

• The bank will not ask you to reactivate your account or re-enter your data, credit card number, or bank account number, nor will it ask for your username or password at all.

• لن يطلب منك البنك إعادة تفعيل حسابك او إعادة إدخال بياناتك او رقم بطاقة الائتمان، او رقم حسابك المصرفي، كما لن يقوم بطلب اسم المستخدم (User Name) او رمز الدخول (Password) الخاصة بك على الإطلاق

<https://youtube.com/watch?v=O-rCALHmvHo&feature=share>