




مذكرة


الإلتزام بالإجراءات الأمنية لمنع الاحتيال عن بعد


لا يطلب منك موظف البنك الحقيقي أبداً تزويده بأي من تفاصيل بطاقتك المصرفية. لا تعطي الكلمة السرية لأي احد إلا إذا اتصلت بنفسك بالخط الساخن للبنك. 




إذا تلقيت مكالمة وتم إخبارك أن قريبك وقع في مشكلة، فإن أول شيء يجب عليك فعله هو معاودة الاتصال بقريبك. 

يتم دفع أي مدفوعات لأصحاب المعاشات أو التعويضات الاجتماعية فقط من قبل الأخصائي الاجتماعي المخصص لمتابعة ملفك. 

إذا تلقيت رسالة نصية قصيرة SMS حول الفوز بجائزة أو الفوز باليانصيب، فلا ترد على الرسالة النصية القصيرة المستلمة، ولا تتصل أو تكتب إلى رقم غير معروف. 

لا تقم بتحويل الأموال إلى الغرباء تحت أي ذريعة. 

تحقق دائماً من المعلومات وكن حذراً 

في حالة فقدان بطاقتك المصرفية:



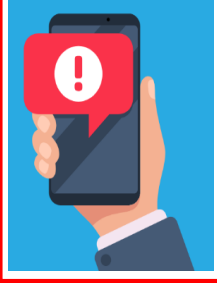
1. قم بحظر البطاقة.
2. التحقق من المعاملات المصرفية الأخيرة.
3. تواصل مع البنك الذي تتعامل معه لإصدار بطاقة جديدة.

في حالة سرقة أموال من حسابك البنكي:

1. عليك الاتصال بالبنك فوراً ووصف الموقف
2. الذهاب إلى الشرطة والإبلاغ أو الاتصال بالرقم 102 (من الهاتف المحمول 112).
3. إرسال إشعار بقبول الطلب في مركز الشرطة للبنك .

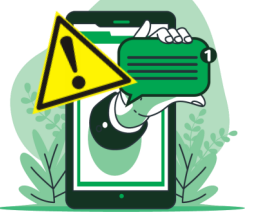


في حالة فقدان هاتفك:



1. اتصل بالبنك الذي تتعامل معه لحظر التطبيق المصرفي وحذف بيانات بطاقتك المصرفية من جهازك المحمول.
2. اتصل بمشغل الهاتف المحمول الخاص بك لحظر بطاقة SIM الخاصة بك.
3. التحقق من سجل المعاملات على البطاقات والحسابات المصرفية.

تذكر:



1. لا تخبر أحداً بتفاصيل بطاقتك المصرفية، ورموز الرسائل النصية القصيرة، ورمز PIN، والرمز المكون من ثلاثة أرقام الموجود على ظهر البطاقة، ولا تدخل أي مجموعات مشكوك فيها على جهازك المحمول ولا تتبع روابط غير معروفة.
2. ولا تتسرع في الثقة بالمتصل، حتى لو عرّف عن نفسه بأنه "موظف في البنك، بما في ذلك جهاز الأمن". «إذا تلقيت مكالمة مشبوهة من "البنك"، دون مواصلة المحادثة، دون الإجابة على الأسئلة، أوقف المحادثة فوراً واتصل بالبنك مرة أخرى بنفسك باستخدام الرقم الرسمي - الموجود على موقع البنك أو على ظهر البطاقة، بعد توضيح المعلومات التي تلقيتها من المتصل، لا تتصل مرة أخرى عن طريق الاتصال برقم المتصل، يمكنك الحصول على المحتالين مرة أخرى.
3. لا تخبر الغرباء بتفاصيل عنك على الشبكات الاجتماعية: الاسم الأخير، الاسم الأول، اسم العائلة، مكان وسنة الميلاد، تفاصيل جواز السفر.
4. لا تقم بتنصيب تطبيقات غير معروفة على هاتفك بناءً على طلب "موظف البنك" أو "المستشارين الماليين".
5. استخدم الخدمات الرسمية للبنك "إشعارات المعاملات".
6. لا تعطي الأجهزة المحمولة التي تحتوي على تطبيقات مصرفية مثبتة إلى أيدي أشخاص مجهولين، بما في ذلك المشاركين في سلاسل الدفع لبعض السلع والخدمات. لا تقم بتخزين تفاصيل البطاقة على هاتفك: الرقم وتاريخ انتهاء الصلاحية ورمز التحقق ورقم التعريف الشخصي للبطاقة.
7. لا تستخدم ماكينة الصراف الآلي في وجود أشخاص مشبوهين ولا تقبل المساعدة من الغرباء، وأعط الأفضلية لأجهزة الصراف الآلي المثبتة في أماكن آمنة (على سبيل المثال، في مكاتب البنوك والهيئات الحكومية ومراكز التسوق الكبيرة)، وقم بتغطية لوحة المفاتيح بيدك عند إدخال رمز PIN.
8. التأكد من سلامة البطاقات المصرفية، ولا سيما تلك التي توفر طرق الدفع غير التلامسية.
9. قم بإجراء عمليات الشراء، أو قم بالوصول إلى الموقع الإلكتروني للبنك أو التطبيقات المصرفية فقط من جهاز الكمبيوتر الشخصي أو الجهاز اللوحي أو الهاتف. قم بتعيين كلمات المرور لجميع أدواتك.

إذا تم ارتكاب أعمال غير قانونية ضدك وضد أحبائك،

اتصل على 102:



من الجوال