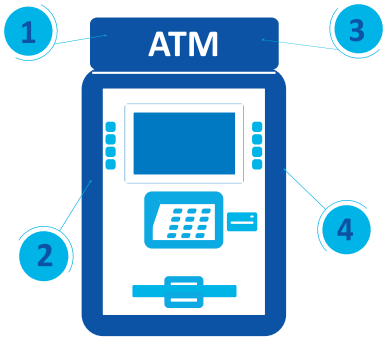
أجهزة الصرف الآلي:

1. عليك بتغيير جهاز الصرف الآلي إذا لاحظت أي شيء غير عادي بشأن جهاز الصرف الآلي أو إذا كانت هناك أي علامات على التلاعب فيها فلا تستخدم الجهاز و قم بإبلاغ البنك أو الشرطة.
3. احذر الآخرين المحيطين بك فإذا كان هناك من يراقبك عليك اختيار جهاز صرف آلي مختلفة.



2. في حالة عدم قيام جهاز الصرف الآلي بإعادة البطاقة الخاصة بك فعليك بإبلاغ البنك بذلك.
4. قف قريباً من ماكينة الصرف الآلي عليك بإخفاء لوحة المفاتيح على الدوام باستخدام يدك الأخرى و جسدك لتفادي قيام أي أحد برؤية الرقم السري.

نقاط البيع:

لا تدع بطاقتك تغيب عن نظرك أثناء عمليات الدفع (و أن أمكن قم بلمسها لتأكد من صحتها).

و كن مصراً على عدم غياب بطاقتك عن نظرك في جميع الأوقات.

من الممكن خداعك باستخدام البطاقات في منافذ البيع بالتجزئة و خصوصاً الأندية و المطاعم و الآليات الخاصة لتذاكر مواقف السيارات (الآلية بدون الأفراد) و محطات الوقود.

الاحتيال باستخدام بطاقات الدفع: Prevention Alert

نصيحة عامة

تقليص مخاطر الاحتيال

مع تزايد عدد الأشخاص الذين وقعوا ضحايا للاحتيال عن طريق بطاقات الدفع كل عام فقد نمت الحاجة إلى توعية الجمهور بطرق منع الاحتيال الأساسية عند استخدام بطاقات الدفع، سواء كانت بطاقات خصم أو بطاقات ائتمان أو بطاقات مسبقة الدفع أو أي نوع آخر من بطاقات الدفع.

و هذه النشرة البيانية مقصود منها منع الاحتيال باستخدام بطاقات الدفع و تفادي تكرار ذلك مع أي شخص آخر و خصوصاً أثناء مواسم العطلات عندما يتزايد احتمال استخدام الأشخاص لبطاقاتهم في أماكن ليسوا على معرفة بها و بالتالي يكونوا معرضين للاحتيال.

وضع التوقيع الخاص بك على البطاقات الجديدة فور استلامها.

اطلب من البائع تأكيد المبلغ الذي تم خصمه من بطاقتك.

لا تدع بطاقتك تغرب عن نظرك عند إجراء أي معاملة.

قم بحماية بطاقاتك و بيانات بطاقاتك.

لا تترك بطاقاتك بدون حراسة في الأماكن العامة، و احتفظ بأمتعتك الشخصية معك في جميع الأوقات.

تخلص من إيصالات الناتجة عن المعاملات التي تم إجرائها باستخدام البطاقات و المعلومات ذات الصلة بشؤونك المالية.

قم بمراجعة إيصالاتك مع كشوفات الحساب التي يتم توفيرها عبر الانترنت.

قم بالشراء من المصادر الموثوق بها فقط، و بالنسبة للمشتريات التي تتم عن طريق الانترنت، استخدم البروتوكول الأمني ثلاثي الحماية.

عند إجراء معاملات عبر الإنترنت تأكد من استخدامك لأحدث برامج مكافحة الفيروسات و برامج أنظمة التشغيل.

لا تدون رقمك السري أو تقوم بذكره لأي شخص.

عند وصول البطاقات البديلة، قم بتمزيق البطاقات المنتهية/ الغير مستخدمة/ و تجزئة البطاقات إلى قطع عديدة بما في ذلك الشريط المغناطيسي و/أو الشريحة.

لا تترك دفاتر الشيكات مع بطاقاتك.

السفر و الفنادق/ الأندية/ المطاعم

إذا قام أي فندق بتخزين بياناتك الشخصية في بطاقة المفتاح الإلكتروني الخاص بك فتأكد بالاحتفاظ بالبطاقة معك في جميع الأوقات أثناء الإقامة في الفندق و بعد ذلك قم أما بالتخلص منها أو ضمان محو/ شطب/ إلغاء البيانات الإلكترونية، و لا تتخلص من بطاقات المفاتيح الإلكترونية المستعملة في سلال القمامة العامة.

Photocopy of the card

لا تسمح للبائع بأخذ صورة من الوجه الخلفي لبطاقتك (فيكفي الوجه الأمامي فقط).

Electronic key cards

ID documents

لا تقم بتسليم مستندات إثبات الهوية (مثل جواز السفر أو رخصة القيادة) كتأمين، فيكفي الصور و ينبغي أن تكون أما بطاقات الهوية الخاصة بك أو بيانات بطاقات الائتمان خاصتك.

PIN

لا تعطي أي أحد الرقم السري الخاص بك مقدماً (و إذا قمت بذلك) فعند دفع الفاتورة فقط.

رقم بطاقتك و اسمك كافيين لضمان دفع أجرة الغرفة و المرافق و المصاريف.

Card validation

إذا قام البائع بتمرير بطاقتك على أحد الأجهزة للتأكد منها فسأله عما فعله بالبيانات و ما هي البيانات التي قام بتخزينها و كيف و أين و إلى أي فترة من الوقت.

Card as a deposit

تأكد من إعادة بطاقتك إليك و عدم الاحتفاظ بها كتأمين، لأن الاحتفاظ بها كتأمين عمل غير آمن.

ما الذي ينبغي عليك عمله إذا أصبحت مجني عليه؟

راقب تقاريرك الائتمانية لضمان عدم قيام أي أحد بفتح حسابات جديدة باسمك.

راقب كشوفات حسابك (عبر الإنترنت) و قم بإبلاغ مصرفك عن أي تحويلات مالية مشتبه بها.

قم بإبلاغ الشرطة المحلية ع الجريمة.

تفادي إيداع مبالغ كبيرة من المال في الحساب المتأثر إن أمكن.

اتصل بالبنك أو الشركة المصدرة لإلغاء البطاقة المتأثرة و تجميد الحسابات المصاحبة لها.

إدارة مكافحة الجرائم الإلكترونية :

هاتف: +(965) 25660142

البريد الالكتروني: Info@cybercrime.gov.kw

حسابنا في مواقع التواصل الاجتماعي: @ECCCD