

وزارة الداخلية
Ministry of Interior
دولة قطر • State of Qatar



نصائح توعوية

للمكافحة الجرائم الإلكترونية

حماية جهازك الشخصي



- حدث نظام التشغيل والتطبيقات أولاً بأول وفعل خاصية التحديث التلقائي.
- ثبت برنامج حماية موثوقاً من الفيروسات وحافظ على تحديثه.
- اقفل جهازك برمز سري أو بصمة ولا تتركه مفتوحاً دون مراقبة.
- حمل التطبيقات من المتاجر الرسمية فقط وراجع الصلاحيات التي تطلبها قبل الموافقة.
- احتفظ بنسخة احتياطية دورية لبياناتك المهمة.
- لا توصل ذاكرة تخزين (USB) مجهولة المصدر بجهازك.

حماية الشبكة اللاسلكية



- غير اسم المستخدم وكلمة المرور الافتراضيين لجهاز الراوتر فور تركيبه.
- اجعل كلمة مرور الشبكة طويلة ومعقدة وغيرها بشكل دوري.
- حدث برنامج تشغيل الراوتر (Firmware) بانتظام.
- خصص شبكة منفصلة للضيوف وللأجهزة المنزلية الذكية.
- راجع قائمة الأجهزة المتصلة بشبكته دورياً وافصل أي جهاز غير معروف.
- تجنب الشبكات العامة المجانية وإن اضطرت فلا تجر عبرها أي عملية مالية أو دخول لحسابات حساسة.

حماية بيانات البطاقة الائتمانية

- لا تشارك رقم البطاقة أو تاريخ انتهائها أو الرمز السري (CVV) مع أي شخص أو جهة.
- رمز التحقق (OTP) لا يُطلب منك أبداً من البنك أو أي جهة رسمية ولا ترسله لأحد مهما كان السبب.
- تسوق من المواقع الموثوقة فقط وتأكد أن العنوان يبدأ بـ (https) وأن اسم الموقع مكتوب بشكل صحيح.
- استخدم بطاقة مسبقة الدفع أو بطاقة افتراضية للشراء عبر الإنترنت وحدد لها سقفًا ماليًا.
- لا تحفظ بيانات بطاقتك في المواقع أو المتصفحات أو التطبيقات.
- عند ملاحظة أي عملية غير معروفة أوقف البطاقة فوراً وأبلغ البنك.

حماية البريد الإلكتروني

- استخدم كلمة مرور قوية ويفضل ان لا تكون مستخدمة في أي حساب آخر.
- فعّل التحقق بخطوتين (Two-Factor Authentication)
- لا تفتح الروابط أو المرفقات الواردة من مصادر مجهولة أو غير متوقعة.
- تحقق من عنوان المرسل حرفاً بحرف فالمحتالون يستخدمون عناوين مشابهة للعناوين الرسمية.
- احذر ولا تتجاوب مع الرسائل التي تستعجلك أو تهددك بإغلاق الحساب أو تعديك بجوائز ومكاسب.
- خصص بريدًا منفصلاً للأمور المالية والرسمية وآخر للتسجيل في المواقع والخدمات.
- لا تفتح بريدك من أجهزة عامة أو مشتركة وإذا اضطررت احرص على تسجيل الخروج دائماً.

حماية حسابات التواصل الاجتماعي

- فعّل التحقق بخطوتين واستخدم كلمة مرور مختلفة لكل حساب.
- لا تنشر بيانات حساسة مثل مكان السكن أو أرقام الوثائق أو تذاكر السفر أو تفاصيل العائلة.
- عطل مشاركة الموقع الجغرافي وتجنب نشر تحركاتك اللحظية أو مواعيد سفرك.
- احذر برامج زيادة المتابعين أو معرفة من زار حسابك فهي وسيلة شائعة لسرقة الحسابات.
- تحقق من هوية من يرأسك فقد يكون حساباً منتحلاً لشخص تعرفه بهدف طلب مال أو بيانات.
- راجع التطبيقات والخدمات المرتبطة بحسابك واحذف ما لا تستخدمه.
- بادر بالإبلاغ فور تعرض حسابك للاختراق أو ظهور حساب ينتحل شخصيتك.

الحماية من الرسائل والمكالمات الاحتيالية

- الجهات الرسمية والبنوك لا تطلب بياناتك الشخصية أو المصرفية أو رمز التحقق عبر الهاتف.
- لا تضغط على الروابط الواردة في الرسائل النصية بحجة تحديث البيانات أو استلام طرد أو سداد مخالفة.
- أنه المكالمات المشبوهة وتواصل مع الجهة عبر رقمها الرسمي المعروف للتأكد.
- احذر من مطالبتك بتحميل تطبيق يتيح للمتصل التحكم بجهازك عن بعد.
- لا تنساق وراء أسلوب الاستعجال والضغط النفسي فهو السلاح الأول لدى المحتال.
- تعامل بحذر شديد مع المكالمات من أرقام تدعي وجود جائزة أو مشكلة في حسابك.
- احظر الرقم المشبوه وأبلغ عنه لدى إدارة مكافحة الجرائم الاقتصادية والإلكترونية.

الحماية من عروض البيع الوهمية على الإنترنت

- احذر العرض المبالغ في انخفاض سعره عن السوق هو غالباً عرض احتيالي.
- تعامل مع المتاجر المعروفة وتحقق من بياناتها ووسائل التواصل معها ورخصتها التجارية.
- اقرأ تقييمات المشتريين السابقين وانتبه لتاريخ إنشاء المتجر أو الحساب وعدد متابعيه الحقيقي.
- حاول تجنب التحويل المباشر إلى حسابات شخصية.
- احذر من روابط الدفع التي يرسلها البائع فقد تكون صفحات مزيفة لسرقة بيانات بطاقتك.
- احتفظ بالمحادثات وإيصالات الدفع وبيانات البائع فقد تكون دليلاً عند الإبلاغ.
- لا تتردد في الإبلاغ فور الاشتباه أو الوقوع ضحية.

الحماية من جرائم التزييف العميق (Deepfake)

- التزييف العميق هو صوت أو صورة أو مقطع مرئي منتج بالذكاء الاصطناعي ينتحل شخصاً حقيقياً، ويُستخدم في الاحتيال والابتزاز والتشهير ونشر الشائعات.
- احذر المكالمات الصوتية أو المرئية من قريب أو مسؤول تطلب تحويل مبلغ أو بيانات بصفة عاجلة وسرية، وتحقق دائماً بالاتصال به على رقمه المعروف لديك.
- اسأل المتصل سؤالاً لا يعرف إجابته إلا الشخص الحقيقي واطلب في مكالمات الفيديو حركة مفاجئة كإدارة الرأس أو تمرير اليد أمام الوجه.

■ انتبه لعلامات التزييف:

- عدم تطابق حركة الشفاه مع الصوت.
- رمش غير طبيعي.
- إضاءة وظلال غير متناسقة.
- اضطراب عند حواف الوجه والشعر.
- جودة منخفضة متعمدة لإخفاء العيوب.

■ قبل تصديق أو تداول مقطع منسوب لشخصية عامة أو جهة رسمية تأكد من نشره في القنوات الرسمية للجهة.

■ لا تعيد نشر المقطع المزيف ولو بقصد التحذير فأعادة النشر تضاعف الضرر وتخدم هدف المزيف.

■ عند التعرض للابتزاز بمقاطع مزيفة:

لا تستجب ولا تدفع ولا تتفاوض واحتفظ بالمقطع والروابط وبيانات الحساب الناشر كدليل وبلغ إدارة مكافحة الجرائم الاقتصادية والإلكترونية فوراً.