

Spot Frauds
Protect Your Data & Money

اكتشف الاحتيال
لحماية بياناتك وأموالك

Preventing fraud and scams is a shared responsibility. Keep these critical indicators in mind when you receive any digital communication.

إن حماية نفسك من عمليات النصب والإحتيال مسؤولية مشتركة. ضع هذه المؤشرات المهمة في اعتبارك عند تلقي أي تواصل رقمي.

تحقق من علامات الخطر

- » **Sender Authenticity**
Unknown mobile numbers, generic emails or slight typos in web links.
- » **Tone**
Aggressive demands or panic-inducing threats such as immediate blocking of card /account etc.
- » **Links & QRs**
Open/missing padlocks, "Not Secure" warnings, unverified scan codes or direct file downloads.
- » **Trap Offers**
"Too good to be true" schemes, using intense time limits ("Expires Soon!", "Limited Time Offer", etc.) or peer pressure ("Thousands are doing it") to force a rushed decision.
- » **AI & Deepfakes**
Highly realistic, AI-generated fake video ads or celebrity/leader interviews endorsing platforms. Look for unnatural lipsync or robotic audio.

- » **المُرسل**
أرقام هواتف مجهولة أو رسائل بريد إلكتروني عامة أو أخطاء إملائية بسيطة في روابط الويب.
- » **النبرة**
مطالب عدوانية أو تهديدات مثيرة للذعر بالخطر الفوري للبطاقة / الحساب إلخ...
- » **الروابط ورموز الاستجابة السريعة**
أقفال مفتوحة/غير موجودة تحذيرات "غير آمنة" أو رموز مسح ضوئي غير مُتحقق منها أو روابط تحميل ملفات مباشرة.
- » **فخ العروض**
عروض "جيدة لدرجة لا تُصدق" باستخدام مهلة زمنية ضاغطة ("يُنتهي قريباً!" "عرض لفترة محدودة"، إلخ) أو ضغط الأقران ("الآلاف يفعلون ذلك") لدفع المستخدم على إتخاذ قرار متسرع.
- » **الذكاء الاصطناعي والتزييف العميق**
إعلانات فيديو مزيفة واقعية للغاية، أو مقابلات مع مشاهير أو قادة يدعمون منصات معينة، تم إنشاؤها بواسطة الذكاء الاصطناعي. انتبه لمزامنة الشفاه غير الطبيعية أو الصوت الآلي.

خطوات السلامة التي يجب اتباعها

- » Do not hurry! Give it time. Fraudsters thrive on manufactured urgency.
- » Verify messages independently.
- » Never click links or use contact numbers found inside suspicious messages.
- » Never scan unverified QR codes sent via chats, messages or posted on public websites.

- » لا تتسرع! امنح الأمر بعض الوقت. المحتالون يستغلون الشعور بالاستعجال المصطنع.
- » تحقق من صحة الرسالة بنفسك.
- » لا تنقر على الروابط أو تستخدم أرقام الاتصال الموجودة في رسالة مشبوهة.
- » لا تسمح رموز الإستجابة السريعة غير المحققة المرسله عبر المحادثات أو الرسائل أو المنشورة على مواقع إلكترونية عامة.

خطوات السلامة التي يجب اتباعها

- » **The Gold Standard for Updates:** Official updates never happen via direct links, SMS, WhatsApp or emails. Download mobile apps from official application stores (GooglePlay/AppStore etc.) only and use internal 'Settings' option of devices for reliable software updates.
- » **Our Promise:** The Bank will never send a link or a QR code via SMS, WhatsApp or Email and no bank employee will ever ask you for your MPIN, PIN or OTP.

- » **المعيار الذهبي للتحديثات:** لا يتم إرسال التحديثات الرسمية عبر روابط مباشرة أو رسائل نصية أو واتساب أو بريد إلكتروني. استخدم فقط متجر جوجل بلاي/متجر أبل الرسمي لتطبيقات الجوال أو من خلال إعدادات جهازك > تحديث البرامج.
- » **وعدنا:** لن يقوم البنك بإرسال أي رابط أو رمز إستجابة سريعة عبر الرسائل النصية أو الواتساب أو البريد الإلكتروني، ولن يطلب منك أي موظف في البنك إدخال رقم التعريف الشخصي للهاتف المحمول (MPIN) أو رمز التعريف الشخصي (PIN) أو كلمة المرور لمرة واحدة (OTP).