البنك الوطني الجزائري
Banque Nationale d'Algérie

الاحتيال والنصب عبر الإنترنت

مذكرة توعوية: الاحتيال والنصب عبر الإنترنت يشكلان خطراً متزايداً

إحصائيات عالمية

- **+ 600 %** زيادة عالمية في هجمات التصيّد الاحتيالي بين عامي 2019 و 2023.
- **8000 مليار دولار أمريكي**, تقدير التكلفة العالمية للجريمة الإلكترونية في عام **2023**. قد يصل هذا الرقم إلى **10500 مليار دولار أمريكي بحلول عام 2025.**
- **91 %** من الهجمات الإلكترونية في العالم تبدأ برسالة بريد إلكتروني تصيد احتيالي
- 1**من كل 4** أشخاص في العالم تعرض لمحاولة احتيال عبر الإنترنت خلال الـ **12 شهرًا الماضية**
- **53%** من عمليات الاحتيال عبر الإنترنت تتعلق بعمليات الشراء من مواقع تجارة إلكترونية احتيالية. **70%** من عمليات النصب عبر الإنترنت يتم اكتشافها الآن عبر الهواتف الذكية، حيث يستهدف المحتالون المستخدمين بشكل متزايد عبر الرسائل النصية، ومواقع التواصل الاجتماعي، والتطبيقات.

لاحتيال والنصب عبر الإنترنت هو جميع الممارسات غير القانونية التي تتم عبر الإنترنت من قبل أفراد ذوي نوايا سيئة بهدف خداع أو التلاعب أو استغلال مستخدمي الإنترنت. يمكن أن تتخذ هذه الأفعال أشكالًا مختلفة، مثل التصيد الاحتيالي (Phishing)، الاحتيال عبر المواقع الإلكترونية الزائفة، انتحال الهوية، أو الرسائل والمكالمات الكاذبة التي تهدف إلى الحصول على معلومات شخصية أو مصرفية أو مهنية. يستغل مجرمو الإنترنت الثقة أو قلة الانتباه أو قلة المعرفة لدى الضحايا لتحقيق أهدافهم. يمكن أن تؤدي هذه عمليات الاحتيال إلى خسائر مالية كبيرة، أو سرقة الهوية، أو انتهاك الخصوصية. إن التوعية واليقظة هما أفضل وسيلة للحماية من هذه التهديدات.

أنواع عمليات النصب

تحذير هام

يُعتبر الإفصاح غير الحذر عن المعلومات الشخصية على الإنترنت من أبرز الأبواب التي تُستغل في عمليات النصب. فعند كشف بيانات حساسة، يعرّض المستخدمون أنفسهم لأنواع متعددة وخطيرة من الاحتيال. إن فهم أنواع الاحتيال المرتبطة بهذا الخطر يُساهم في تعزيز الحماية. ومن بين أكثر أنواع الاحتيال شيوعًا:

الأنواع	تعريف	أمثلة	الاهداف
1. التصيّد الاحتيالي (Phishing)	تقنية يقوم فيها المحتال بانتحال صفة جهة موثوقة (مثل بنك، إدارة، أو شبكة تواصل اجتماعي) من أجل الحصول على معلومات سرية.	- رسالة بريد إلكتروني تدعي أنها من البنك الخاص بك، تطلب منك « التحقق «من معلوماتك الشخصية. - رسائل SMSأو رسائل واتساب مزيفة تحتوي على رابط لموقع وهمي (يشبه الموقع الحقيقي).	جمع أسماء المستخدمين، كلمات المرور، أرقام بطاقات الائتمان، وسرقة الأموال.
2. انتحال الهوية	استخدام البيانات الشخصية لشخص ما لانتحال هويته.	- إنشاء ملف شخصي مزيف على وسائل التواصل الاجتماعي باستخدام صورك ومعلوماتك. - استخدام اسمك للحصول على قرض أو للاحتيال على أشخاص آخرين.	سرقة الأموال، الإضرار بسمعتك، أو ارتكاب جرائم باسمك.
3. خدع الدعم التقني الزائف	يدعي المحتال أنه فني من شركة كبيرة (مثل مايكروسوفت، أبل، إلخ) للوصول إلى جهاز الكمبيوتر الخاص بك.	- مكالمات أو رسائل تخبرك أن جهاز الكمبيوتر الخاص بك مصاب بفيروس. - طلب تثبيت برنامج يسمح للمحتال بالتحكم عن بُعد بجهازك.	الوصول إلى بياناتك الشخصية والمالية.
4. عمليات الاحتيال عبر وسائل التواصل الاجتماعي / تطبيقات المراسلة	التلاعب عبر الرسائل الخاصة أو المنشورات لحث المستخدمين على مشاركة معلومات حساسة.	مسابقات وهمية ("ما هو لون سيارتك الأولى؟" – وهي أيضاً أسئلة أمان). رسائل من أصدقاء مخترقين يطلبون منك المساعدة أو المال.	جمع المعلومات لاختراق حساباتك.

نصائح

النصائح الأساسية لحماية نفسك وبياناتك عبر الإنترنت

① فكّر جيدًا قبل المشاركة

هل تطرح على نفسك دائمًا السؤال: "هل ما أشاركه قد يُستخدم ضدي؟" بمجرد نشر محتوى على الإنترنت، يصعب حذفه تمامًا (حتى لو قمت بحذف المنشور). لا تشارك تحت الضغط أو العاطفة.

② قم بإدارة إعدادات الخصوصية الخاصة بك:

في كل مواقع التواصل الاجتماعي (فيسبوك، إنستغرام، تيك توك، إلخ)، اذهب إلى إعدادات الخصوصية:

- حدد من يمكنه رؤية منشوراتك (الأصدقاء فقط، المجموعات الخاصة).
- قم بإيقاف تشغيل التحديد الجغرافي التلقائي.
- تجنب أن يتم فهرسة صورك بواسطة محركات البحث.
- فعّل خاصية التحقق بخطوتين FA2 على جميع حساباتك لتعزيز الأمان.

③ قلّل من المعلومات الشخصية الظاهرة:

تجنب نشر:

- عنوانك، رقم هاتفك، بريدك الإلكتروني الشخصي، كلمة المرور ذات الاستخدام لمرة واحدة (OTP)أو غيرها... إلخ.
- الوثائق الرسمية (رقم الهوية الوطنية، جواز السفر، بطاقة CHIFA، بطاقة CIB، التوقيع...).
- موقعك الجغرافي في الوقت الحقيقي... إلخ.

احرص على الحفاظ على خصوصيتك:

- استخدم المجموعات المغلقة أو تطبيقات المراسلة المشفرة لتبادل الرسائل الشخصية.
- حافظ على حدود واضحة بين حياتك الخاصة والعامة.

④ فخ أم فرصة جيدة؟ تعلّم كيف تميز بينهما:

النقاط الأساسية لتجارة إلكترونية آمنة:

1. اشترِ فقط من مواقع موثوقة
تحقق من وجود HTTPSورمز القفل في شريط العنوان.
2. احتفظ بإثبات الشراء
قم بحفظ الفواتير وتأكيدات الطلب/الدفع.
3. اقرأ تقييمات العملاء
احذر من التقييمات المثالية جدًا أو الغائبة. قارن تجارب المشترين الآخرين.
4. تحقق من شروط الإرجاع والتوصيل
اقرأ سياسات الإرجاع، والاسترداد، والرسوم المحتملة.
5. لا تعطي إلا المعلومات الضرورية
لا ترسل رموزك البنكية كاملة عبر الرسائل أو الهاتف أو أي وسيلة أخرى.
6. استخدم اتصالاً آمناً
تجنب استخدام الواي فاي العام عند إجراء الدفع عبر الإنترنت.

تعليمات الأمان

إذا أدركت أنك قد تعرضت لعملية احتيال، من الضروري أن تتصرف بسرعة لتقليل الأضرار واسترداد أكبر قدر ممكن من الأموال، إليك فيما يلي ما يجب فعله:

❶ توجه إلى أقرب مركز بريد أو أقرب وكالة بنكية:

- التقدم إلى مركز البريد والتبليغ عن الاحتيال في أقرب وقت ممكن من أجل تجميد حساباتك.
- في حال تعرضكم لعملية نصب أو احتيال أين تم اختراق حسابكم عبر تطبيق بريدي موب، يرجى التوجه الى أقرب شباك آلي والضغط على خانة خدمات النقال قصد توقيف التطبيق،
- في حال ضياع أو سرقة البطاقة الذهبية او البنكية، يرجى منكم حظر البطاقة من خلال الاتصال بخدمة الزبائن

❷ قم بتغيير كلمات المرور والتفاصيل الأمنية:

- قم بتحديث كلمات المرور الخاصة بك، البريد الإلكتروني، استخدم كلمات مرور قوية وفريدة

❸ الحفاظ على الأدلة:

- الاحتفاظ بسجلات لجميع المراسلات والمعاملات المتعلقة بالاحتيال، ستكون هذه الوثائق مفيدة في التحقيقات أو الإجراءات القانونية.

❹ أبلغ مصالح الأمن:

1530	baridinet.poste.dz
1055	ppgn.mdn.dz
1548	algeriepolice.dz
allo chorta	

لا تشارك معلوماتك الشخصية عبر الإنترنت، كن يقظًا، فالمحتال ينتظر الفرصة