فريق الاستجابة للحوادث
السيبرانية للقطاع المالي
والمصرفي الاردني

Jo-FinCERT

البنك المركزي الأردني
CENTRAL BANK OF JORDAN
دائرة حماية المستهلك المالي

دليل التوعية في الاحتيال المالي

باستخدام الوسائل الالكترونية

النسخة 2.0 2025

المقدمة

في ضوء توسع الخدمات المالية وتنوعها، لاسيما في أعقاب جائحة كوفيد-19، أصبح العملاء يعتمدون بشكل أكبر على القنوات المالية الرقمية لما توفره من سهولة في الاستخدام وكفاءة في إدارة شؤونهم المالية من حيث الوقت والتكلفة.

إلا أن الاعتماد على هذه الخدمات أسهم في انتشار أنماط أكثر تعقيداً من الاحتيال المالي التي تستهدف عملاء القطاع المالي والمصرفي. حيث أصبحت عمليات الاحتيال أكثر تعقيداً وقدرة على التكيف، حيث يتم استغلال المنصات الرقمية والقنوات عن بُعد لخداع الأفراد ودفعهم إلى كشف معلوماتهم المالية والشخصية.

وانطلاقاً من دور البنك المركزي الأردني لحماية عملاء القطاع المالي والمصرفي،تم إعداد هذا الدليل للتوعية حول حالات الاحتيال المالي، بهدف رفع مستوى الوعي بأنماط الاحتيال المالي الشائعة، وتسليط الضوء على الأساليب التي يستخدمها المحتالون، إضافةً إلى تقديم إرشادات عملية تمكّن العملاء من حماية أنفسهم من الوقوع ضحايا لمثل هذه التهديدات.

الفهرس

التصيد الاحتيالي (Phishing)

التصيد الاحتيالي هي عملية توظيف روابط إلكترونية مزيفة ينشئها المحتالون لانتحال شخصية مؤسسات أو أفراد موثوقين، بهدف خداع المستخدمين لكشف معلومات شخصية أو مالية حساسة. وغالبًا ما تُرسل هذه الروابط عبر البريد الإلكتروني، أو الرسائل النصية القصيرة (SMS)، أو وسائل التواصل الاجتماعي، وتكون مصمّمة لتبدو مشابهة جداً للروابط الحقيقية، مما يزيد من احتمالية وقوع المستخدمين ضحية للاحتيال.

توصيات أمنية

- قم بالتحقق من المصدر المرسل قبل النقر على أي رابط أو فتح أيّة مرفقات مستلمة عبر البريد الإلكتروني أو الرسائل النصية. كما يُنصح باستخدام حلول مكافحة الفيروسات الموثوقة لفحص المرفقات والتحقق من صحة عناوين URL قبل التفاعل معها.

- قم بالدخول مباشرة إلى موقع البنك أو المؤسسة المالية عبر كتابة العنوان الرسمي في المتصفح، خاصة عند طلب تقديم معلومات سرية. وينبغي التأكد من أن الموقع يستخدم بروتوكول HTTPS ويعرض رمز القفل الأمني في شريط العنوان قبل إدخال أي بيانات حساسة.

- قم بفحص عناوين URL وأسماء النطاقات المدرجة في الرسائل الإلكترونية أو النصية بدقة للبحث عن أخطاء إملائية طفيفة أو أحرف غير مألوفة، إذ تُعد هذه مؤشرات شائعة على محاولات التصيد الاحتيالي التي تهدف إلى انتحال صفة المؤسسات الحقيقية.

انتحال هوية المتصل
(Vishing - Caller ID Spoofing)

انتحال هوية المتصل (Vishing) هو أحد أشكال الاحتيال عبر الهاتف حيث ينتحل المحتالون شخصية مؤسسات موثوقة لخداع الأفراد بهدف الكشف عن معلومات شخصية أو مالية حساسة. قد تتضمن هذه المكالمات ادعاءات كاذبة مثل الفوز بجائزة، أو تأكيد بيانات بنكية، أو تقديم مساعدة في مشكلة غير حقيقية. الهدف من هذه المكالمات هو استغلال ثقة الضحية، أو حالة عدم اليقين لديه لاستخلاص معلومات سرية.

الأساليب الشائعة في انتحال هوية المتصل (Vishing):

- إشعارات مزيفة تتعلق بالفوز بالجوائز.
- مكالمات تطلب التحقق من حسابات بنكية أو تحديث بيانات الحساب.
- طلبات مساعدة تتعلق بمشاكل تقنية أو مالية غير موجودة.

توصيات أمنية

- اعلم أن البنوك والمؤسسات المالية لن تطلب أبدًا معلومات حساسة مثل أسماء المستخدمين، أو كلمات المرور، أو كلمات المرور لمرة واحدة (OTPs)، أو رموز التحقق من البطاقة (CVV) من العملاء عبر الهاتف.

- إذا تلقيت مكالمة تطلب منك اتخاذ إجراء فوري أو بطلب مدفوعات غير معتادة، فلا تستجب دون التحقق من هوية المتصل أولًا. ينبغي دائمًا التواصل مباشرة مع البنك أو المؤسسة باستخدام قنوات الاتصال الرسمية لديهم لتأكيد صحة الطلب.

الهجمات من خلال شبكات الانترنت العامة

تحدث الهجمات عبر شبكات الانترنت العامة عندما يستغل المحتالون الاتصالات اللاسلكية غير الآمنة والمتاحة عادةً في المقاهي والمطارات والفنادق؛ لاعتراض اتصالات المستخدمين أو اختراق الأجهزة المتصلة. وعلى الرغم من أن هذه الشبكات قد تبدو آمنة أو مناسبة للاستخدام، إلا أنها غالبًا ما تفتقر إلى الضوابط الأمنية الأساسية.

قد يقوم المهاجمون بمراقبة حركة البيانات على الشبكة لسرقة بيانات حساسة مثل بيانات الاعتماد، أو المعلومات المالية، أو الملفات الشخصية. وفي بعض الحالات، قد ينشر المهاجمون نقاط وصول وهمية، أو يقوموا بتثبيت برمجيات خبيثة دون علم المستخدم. ويمكن أن تؤدي هذه الاختراقات في نهاية المطاف إلى أنشطة احتيالية، أو انتهاكات للخصوصية، أو سرقة الهوية.

توصيات أمنية

- تجنب الاتصال بشبكات الإنترنت العامة أو المجانية، حتى تلك التي تتطلب كلمة مرور، ما لم تكن تثق بمزود الخدمة وتحقق من كون الشبكة آمنة.
- أوقف خاصية الاتصال التلقائي بشبكات الإنترنت على جهازك، واتصل يدويًا فقط بالشبكات الموثوقة والمثبتة، وذلك لتقليل مخاطر الوصول غير المصرح به أو اعتراض البيانات.

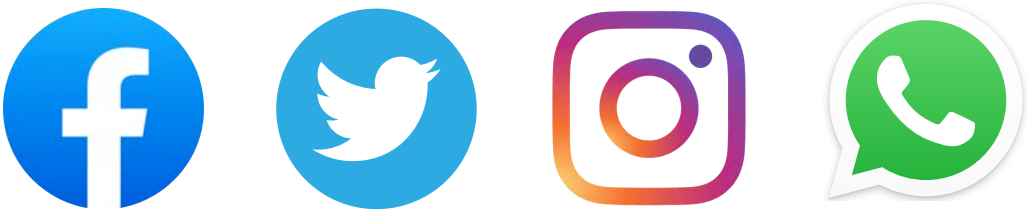
الهندسة الاجتماعية

الهندسة الاجتماعية تحدث عندما يقوم المحتالون بخداع الأشخاص لمشاركة معلومات حساسة أو إرسال أموال أو القيام بأعمال محفوفة بالمخاطر من خلال استغلال الثقة البشرية بدلاً من استغلال الثغرات التقنية. وغالباً ما يتقمص المهاجمون هوية أفراد أو مؤسسات موثوقة مثل الزملاء أو مؤسسات مالية ومصرفية أو مزودي الخدمات وذلك باستخدام المكالمات الهاتفية أو رسائل البريد الإلكتروني أو الرسائل النصية أو المنصات الرقمية.

بمجرد التواصل، يلجأ المحتالون إلى أساليب الضغط النفسي مثل الإلحاح، أو إثارة الخوف، أو التذرع بالسلطة، أو الوعد بمكافآت. وقد يتم إقناع الضحايا بالنقر على روابط خبيثة، أو تحويل أموال، أو الإفصاح عن بيانات شخصية. بحيث تُستغل هذه المعلومات لاحقاً في الاحتيال، أو الابتزاز، أو سرقة الهوية، أو شن هجمات سيبرانية أوسع.

علامات تحذيرية شائعة:

- رسائل أو مكالمات غير متوقعة تطلب معلومات حساسة.
- مناشدات عاجلة لتحويل الأموال أو تقديم المساعدة الفورية.
- طلب كلمات مرور أو أرقام PIN أو رموز التحقق لمرة واحدة (OTP).
- عروض، روابط أو مرفقات تبدو مشبوهة أو جيدة لدرجة يصعب تصديقها.



توصيات أمنية

- دائمًا تأكد من هوية أي شخص يطلب المال، حتى لو بدا كصديق أو قريب، وذلك باستخدام قنوات موثوقة للتحقق قبل اتخاذ أي إجراء.
- لا تقم بإرسال أموال لأشخاص عبر الإنترنت، بغض النظر عن مدى اقتناعك بمصداقية حساباتهم الشخصية.
- تجنب مشاركة المعلومات الشخصية أو السرية على وسائل التواصل الاجتماعي، فقد يتم استغلالها في عمليات الانتحال أو الابتزاز.

رمز الاستجابة الخبيث - Malicious QR Code

تُستخدم رموز الاستجابة السريعة الخبيثة (Malicious QR Codes) من قبل المهاجمين لخداع الأفراد من خلال تمويه روابط ضارة أو وجهات دفع احتيالية على شكل رموز QR تبدو حقيقية. وعلى الرغم من الانتشار الواسع لاستخدام رموز QR للوصول السريع إلى المواقع الإلكترونية، والمعاملات المالية، والخدمات الرقمية، قد يقوم المهاجمون بالتلاعب بالرموز الأصلية أو إنشاء رموز مزيفة لتحويل المستخدمين إلى منصات خبيثة.

عند مسح هذه الرموز، قد توجه المستخدم إلى مواقع تصيد احتيالي، أو تنفيذ معاملات مالية غير مصرح بها، أو دفع المستخدمين إلى مشاركة معلومات حساسة، مما يعرضهم لمخاطر سرقة البيانات، أو الاحتيال المالي، أو اختراق الأجهزة.

طرق الاستغلال الشائعة:

- استبدال رموز QR الشرعية في الأماكن العامة.
- تضمين روابط خبيثة في الإعلانات المطبوعة أو الملصقات.
- إنشاء طلبات دفع احتيالية تحاكي البائعين الحقيقيين.

توصيات أمنية

- تجنب مسح رموز QR من مصادر غير معروفة أو غير موثوقة، خصوصًا في الأماكن العامة أو الرسائل غير المطلوبة.
- قم دائمًا بمعاينة عنوان URL قبل الفتح، حيث تعرض معظم الأجهزة الحديثة الرابط للتحقق من صحته قبل المتابعة.
- قم باستخدام تطبيقات مسح رموز QR التي تتضمن ميزات أمنية، مثل الكشف عن الروابط الخبيثة أو تصفية عناوين URL.
- افحص رموز QR المادية للتحقق من وجود أي تلاعب، أو طبقات إضافية، أو اختلاف في العلامة التجارية، والتي قد تدل على محاولات التزوير.
- لا تقم بإدخال معلومات حساسة مثل بيانات الدخول أو تفاصيل الدفع إلا إذا كان المصدر موثوقًا وتم التحقق منه.

تطبيقات الأجهزة المحمولة المزيفة أو الخبيثة

يقوم المحتالون بتطوير تطبيقات مزيفة أو خبيثة تُحاكي خدمات حقيقية مثل تطبيقات الشبكات الافتراضية (VPN) أو التطبيقات المصرفية بهدف سرقة البيانات الشخصية، أو بيانات الاعتماد ، أو الوصول إلى المعلومات الحساسة.

قد تظهر هذه التطبيقات في متاجر التطبيقات الرسمية أو تُوزع عبر روابط غير رسمية. وبمجرد تثبيتها، قد تمنح المهاجمين حق الوصول إلى محتويات الجهاز، بما في ذلك الرسائل، والبيانات المخزنة، ورموز التحقق لمرة واحدة (OTPs).

غالبًا ما يخدع المحتالون المستخدمين لتحميل هذه التطبيقات من خلال تمويهها على أنها خدمات موثوقة أو تحديثات عاجلة.

توصيات أمنية

- لا تقم بتحميل التطبيقات من مصادر غير موثوقة أو غير معروفة، أو من روابط يشاركها أفراد مجهولون. وقم بتثبيت التطبيقات فقط من متاجر التطبيقات الرسمية والموثوقة.
- قبل تحميل أي تطبيق، تحقق من هوية الناشر أو المطور. كما يُنصح بمراجعة تقييمات التطبيق، وتعليقات المستخدمين، وعدد التنزيلات، والصلاحيات المطلوبة. قد يشير عدد قليل من المراجعات أو معلومات المطور الغامضة إلى تطبيق احتيالي.
- تأكّد من الصلاحيات التي يطلبها التطبيق قبل التثبيت، وتوخّ الحذر من التطبيقات التي تطلب الوصول إلى ميزات حساسة – مثل الرسائل النصية، وجهات الاتصال، أو ذاكرة التخزين إذا لم يكن هذا الوصول ضروريًا لغرض التطبيق المعلن.

الاحتيال باستخدام منافذ / كوابل الشحن

تُصمم بعض كوابل الشحن لتبدو كملحقات طبيعية لكنها تحتوي على مكونات خبيثة. يستخدم المحتالون هذه الكوابل لسرقة البيانات أو تثبيت برمجيات خبيثة عند توصيلها بالجهاز.

بمجرد توصيلها، يمكن لهذه الكوابل نقل المعلومات بصمت إلى نظام بعيد أو تنفيذ نصوص برمجية ضارة، مما يمنح المهاجمين وصولًا غير مصرح به إلى البيانات الشخصية، أو بيانات الاعتماد، أو تحكمًا كاملاً في الجهاز.

توصيات أمنية

- تجنب استخدام كوابل الشحن المقدمة في الأماكن العامة، مثل محطات الشحن في المطارات أو المقاهي، فقد يكون تم التلاعب بها بهدف اختراق جهازك أو استخراج معلومات حساسة دون علمك، استخدم كوابل الشحن الخاصة بك والموثوقة فقط.

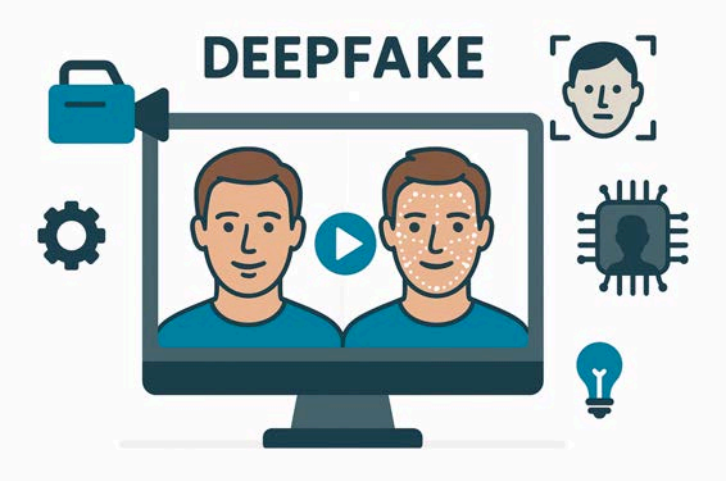
التزييف العميق - Deepfake

تشير تقنية التزييف العميق (Deepfakes) إلى استخدام تقنيات الذكاء الاصطناعي لإنتاج مواد مرئية أو صور شديدة/فائقة المطابقة لكنها مزيفة، بهدف انتحال هوية أشخاص حقيقيين. يتم إنشاء هذه الوسائط باستخدام تقنيات متقدمة في التعلم الآلي للتلاعب بالمحتوى، بحيث يبدو وكأن شخصًا ما قال أو فعل شيئًا لم يحدث فعليًا.

تشكل هذه التقنية تهديدًا متزايدًا في مجالات متعددة، من بينها سرقة الهوية، والهندسة الاجتماعية، والمعلومات المضللة، حيث إنها تقوض الثقة بالمحتوى الرقمي ويمكن استخدامها لخداع الأفراد أو المؤسسات.

أمثلة شائعة على إساءة الاستخدام:

- مكالمات فيديو مزيفة تحاكي المدراء التنفيذيين أو الشخصيات العامة، تطلب معلومات سرية، أو اجراء حركات مالية.
- تسجيلات صوتية مفبركة تُستخدم لخداع الضحايا أو اجراء حركات مالية.
- صور مزورة تُستَخدم في أغراض التحقق من الهوية لفتح الحسابات أو في الهجمات التي تستهدف الاساءة للسمعة.



توصيات أمنية

- **طلبات غير معتادة أو عاجلة:** توخى الحذر عند تلقي رسائل فيديو خاصةً من أشخاص معروفين تطلب القيام بأفعال حساسة مثل تحويل الأموال أو الكشف عن معلومات سرية، فقد تكون هذه الرسائل مُنشأة باستخدام تقنيات اصطناعية.

- **عدم الاتساق البصري:** راقب وجود علامات شاذة مثل تعابير وجه غير طبيعية، أو إضاءة غير متناسقة، أو عدم تطابق حركة الشفاه مع الصوت، أو أنماط كلام آلية؛ حيث تُعد هذه من المؤشرات الشائعة على التلاعب باستخدام تقنية التزييف العميق.

- **سلوك خارج عن المألوف:** إذا انحرف محتوى الرسالة بشكل ملحوظ عن نبرة أو أسلوب المرسل المعتاد، فينبغي التعامل معها بحذر والتحقق من صحتها بشكل مستقل.

انتحال الصوت باستخدام الذكاء الاصطناعي

يستغل المحتالون تقنيات الذكاء الاصطناعي لاستنساخ الأصوات بدقة عالية، مما يجعل المقاطع الصوتية الاصطناعية شبه مطابقة للأصوات الحقيقية وهذا يمكّنهم من انتحال هوية أفراد/جهات موثوقة مثل المدراء التنفيذيين، أو الزملاء، أو أفراد العائلة وخداع الضحايا لدفعهم إلى القيام بإجراءات غير مقصودة. وتشمل السيناريوهات الخبيثة الشائعة المكالمات المزيفة التي تنتحل شخصية الإدارة العليا، أو الرسائل الصوتية التي تقلد أقارب في ضائقة. إن هذا التلاقي بين تقنيات استنساخ الصوت بالذكاء الاصطناعي وانتحال هوية المتصل يعزز بشكل كبير من احتمالية نجاح عمليات الاحتيال المالي، وكشف المعلومات الحساسة، مما يشكل خطراً بالغاً على المؤسسات المالية والأفراد على حد سواء.

توصيات أمنية

- **طلبات غير متوقعة أو عاجلة:** ينبغي توخي الحذر عند تلقي مكالمة هاتفية من شخص تثق به مثل زميل في العمل أو أحد أفراد العائلة يطلب تحويل الأموال أو مشاركة بيانات حساسة.

- **فروقات صوتية دقيقة:** انتبه لأي انحرافات طفيفة في أنماط الكلام، أو النبرة، أو سرعة التحدث، أو الإيقاع العاطفي؛ فقد تبدو الأصوات المُنشأة بالذكاء الاصطناعي واقعية، لكنها غالبًا تفتقر إلى التفاصيل الطبيعية الدقيقة.

- **غياب السياق الشخصي:** قد تفشل الأصوات الاصطناعية في الإشارة إلى تجارب مشتركة، أو حقائق معروفة، أو إشارات حوارية يدرجها الشخص الحقيقي بشكل طبيعي، ويُعد هذا النقص في الألفة علامة تحذيرية في غاية الأهمية.

الاحتيال من خلال منصات البيع الإلكترونية

يشير الاحتيال من خلال منصات البيع الإلكترونية إلى الأنشطة الاحتيالية التي تُنفذ عبر منصات التسوق الإلكتروني حيث يستغل المحتالون ثقة العملاء بإنشاء مواقع مزيفة أو حسابات بائعين وهمية على منصات شرعية. قد تتضمن هذه العمليات عروضًا مزيفة، أو عدم تسليم المنتجات بعد الدفع، أو سرقة معلومات الدفع، مما يؤدي في النهاية إلى خسائر مالية للعميل.

الأشكال الشائعة لحالات الاحتيال من خلال منصات البيع الإلكترونية:

- اعلانات منتجات مزيفة أو خصومات مصممة لجذب وخداع المتسوقين.
- سرقة بيانات الدفع أثناء عملية الشراء عبر مواقع غير مؤمنة أو احتيالية.
- عدم تسليم السلع المشتراة بالرغم من تأكيد الدفع بنجاح.

توصيات أمنية

- توخّ الحذر عند الشراء أو البيع عبر الأسواق الإلكترونية، حيث تُعد الاعلانات المزيفة من التكتيكات الشائعة لخداع المستخدمين.
- لا تُشارك أبدًا كلمة المرور أو رقم التعريف الشخصي (PIN)، إذ أن المعاملات الحقيقية لا تتطلب هذه المعلومات.
- قبل الشراء، ينبغي التحقق من مصداقية البائع من خلال مراجعة التعليقات، والتقييمات، وآراء المشترين لتحديد وجود أي تاريخ من الاحتيال أو السلوك غير الأخلاقي.

الاحتيال عبر منصات التداول

يشير الاحتيال عبر منصات التداول إلى الممارسات الخادعة التي تتم من خلال تطبيقات/صفحات تداول غير مصرح بها أو غير مرخصة، وخاصة تلك التي تتعامل بالأصول الرقمية أو العملات المشفرة. غالبًا ما تسمح هذه المنصات للمستخدمين بإيداع الأموال بسهولة، لكنها تفتقر إلى آليات آمنة وشفافة للسحب، مما يعرض أموال المستخدمين لمخاطر عالية مع غياب أو ضعف الحماية القانونية.

في بعض الحالات، قد ينخرط الوسطاء المحتالون في أنشطة تداول غير مصرح بها أو يقومون بالتلاعب بالأموال عبر اتفاقيات غير رسمية أو معاملات غير موثقة، مما يؤدي إلى خسائر مالية جسيمة أو سرقة الأموال مباشرة.

المخاطر الشائعة المرتبطة بمنصات التداول الاحتيالية:

- عدم القدرة على سحب الأموال المودعة.
- غياب الحماية القانونية أو الرقابة التنظيمية.
- أنشطة تداول غير موثقة أو مُدارة بشكل احتيالي.

توصيات أمنية

- احذر من التعامل مع أفراد أو مؤسسات تعِد بعوائد مرتفعة غير واقعية خلال فترة زمنية قصيرة. تُعد هذه الادعاءات من التكتيكات الشائعة في عمليات التداول الاحتيالية – خاصةً تلك المتعلقة بالعملات الرقمية – وقد تؤدي إلى خسائر مالية كبيرة.

الاحتيال عن طريق اليانصيب الوهمي

يُعتبر الاحتيال عن طريق اليانصيب الوهمي شكلًا من أشكال الاحتيال الإلكتروني الذي يستغل رغبة الأفراد بربح مبالغ مالية كبيرة. حيث يتم خداع الضحايا للاعتقاد بأنهم ربحوا في اليانصيب أو سحب جوائز. في الواقع، لا توجد جائزة حقيقية، اذ يكون الهدف هو سرقة الأموال أو المعلومات الشخصية.

غالبًا ما يطلب المحتالون من "الرابح" دفع تكاليف مقدمة – مثل الضرائب، أو رسوم المعالجة، أو التكاليف القانونية – لاستلام الجائزة. وبمجرد دفع هذه المبالغ، يختفي المحتال ولا يحصل الضحية على أي شيء.

الخصائص الرئيسية للاحتيال عن طريق اليانصيب الوهمي:

- إشعارات غير مرغوب فيها تدعي فوزك بجائزة كبيرة.
- طلبات للدفع قبل استلام الجائزة.
- عدم وجود جهة اتصال أو مصدر اليانصيب يمكن التحقق منه.

توصيات أمنية

- توخّ الحذر من الرسائل أو المكالمات غير المتوقعة التي تزعم فوزك في اليانصيب الذي لم تشترك فيه مطلقاً، إذ غالبًا ما تكون محاولات احتيالية لجمع معلوماتك الشخصية أو المالية.

- لا تقم بإجراء أي مدفوعات أو الكشف عن بيانات حساسة ردًا على مثل هذه الادعاءات، حيث إن الجوائز الحقيقية لا تتطلب أبدًا دفع رسوم مسبقة أو تقديم معلومات بنكية.

الاحتيال الوظيفي عبر الإنترنت

يشير الاحتيال الوظيفي عبر الإنترنت إلى الممارسات الخادعة التي تهدف إلى استغلال الباحثين عن عمل من خلال سرقة معلوماتهم الشخصية أو المالية تحت ستار فرص عمل شرعية. غالبًا ما ينتحل المحتالون هوية شركات حقيقية أو ينشئون إعلانات وظائف ومواقع إلكترونية مزيفة لكسب ثقة المتقدمين.

تشمل هذه الاحتيالات عادة جمع بيانات حساسة مثل السيرة الذاتية، ومستندات الهوية، وتفاصيل الحسابات البنكية. وفي كثير من الحالات يجري المحتالون مقابلات وهمية ثم يطلبون من المتقدمين تحويل أموال بحجة أنها مطلوبة لمعالجة الطلب، أو تصاريح العمل، أو استكمال اجراءات التوظيف.

الأساليب الشائعة في الاحتيال الوظيفي عبر الإنترنت:

- إعلانات وظائف مزيفة على منصات التوظيف.
- انتحال هوية شركات شرعية.
- طلبات دفع أثناء أو بعد مقابلات مزيفة.

توصيات أمنية

- قبل التفاعل مع أي عرض وظيفي تأكد من أن الفرصة حقيقية وأن المؤسسة ذات سمعة.

- يُنصح باستخدام مصادر موثوقة ومواقع رسمية للتحقق من وجود الشركة وشرعيتها. كما ينصح بتوخي الحذر من بيانات الاتصال الغامضة أو النطاقات (المواقع الالكترونية) غير الموثوقة.
- تجنب تحويل أموال لغايات الحصول على وظيفة حيث أن جهات التوظيف الحقيقية لا تطلب أية مبالغ مالية مسبقاً.

انتحال اسم شركة تمويل مرخصة من البنك المركزي

يتضمن هذا النوع من الاحتيال قيام المحتالين بانتحال شخصية شركات مالية مرخصة من البنك المركزي الأردني (CBJ) عبر مكالمات هاتفية، رسائل نصية، أو رسائل بريد إلكتروني مزيفة. حيث يتم خداع العملاء للاعتقاد بأنهم يتلقون عرض قرض أو تمويل حقيقي غالبًا ما يُروّج له بمعدلات فائدة منخفضة، وشروط سداد ميسّرة، أو بدون متطلبات ضمان.

بمجرد تفاعل العميل، يصدر المحتال عقودًا مزورة ويطالب بدفع رسوم أو عمولات مختلفة بحجة معالجة القرض. وبعد استلام المدفوعات، يختفي المحتال تاركًا الضحية دون أموال أو مصدر للتحقق.

علامات تحذيرية شائعة:

- رسائل غير مرغوب فيها تدّعي توفر تمويل بسهولة.
- الضغط على العميل لدفع "رسوم" مقدمة قبل استلام أي مبالغ مالية.
- غياب الوثائق القابلة للتحقق أو قنوات الاتصال الرسمية للشركة.

توصيات أمنية

- لا تثق بعروض القروض أو التمويل المقدمة من قبل أفراد عبر المكالمات الهاتفية أو الرسائل.
- تحقق دائمًا من أن الجهة المقدمة خاضعة لإشراف ورقابة البنك المركزي الأردني.حيث يُفضل استخدام الموقع الرسمي للبنك المركزي للتحقق من المؤسسة، والحرص على زيارة فرع فعلي مدرج في الموقع الرسمي المعتمد.

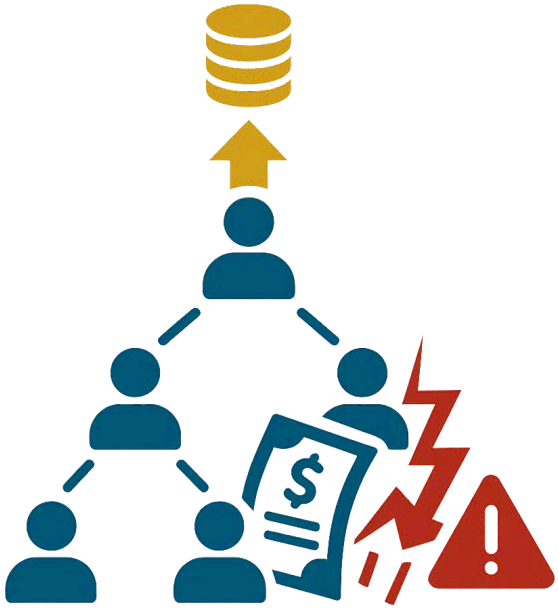
مخطط بونزي الوهمي / التسويق الهرمي

يُعد مخطط بونزي الوهمي / التسويق الهرمي عملية استثمارية احتيالية يتم اقناع الأفراد للمساهمة بمبالغ مالية صغيرة مع وعود بعوائد مرتفعة ومخاطر قليلة. وغالبًا ما يتم تحفيز المشاركون على تجنيد آخرين للانضمام إلى المخطط مقابل عمولات أو حصة من الأرباح المستقبلية.

بدلًا من توليد أرباح حقيقية، تُدفع العوائد الأولية باستخدام الأموال التي يجمعها المجندون الجدد مما يخلق انطباعًا زائفًا بنموذج عمل مربح ومستدام. وفي النهاية، عندما يتباطأ أو يتوقف التجنيد، ينهار المخطط، ويختفي المحتالون بالأموال المتراكمة، تاركين معظم المشاركين بخسائر مالية كبيرة.

الخصائص الشائعة لمخطط بونزي الوهمي / التسويق الهرمي:

- وعود بعوائد مرتفعة بشكل غير طبيعي أو مضمون.
- حوافز لتجنيد آخرين في المخطط.
- غياب نشاط تجاري شفاف وقابل للتحقق.



توصيات أمنية

- توخّ الحذر من أي شركة أو فرد يعِدك بمضاعفة أموالك خلال فترة زمنية قصيرة بشكل غير معقول. تُعد هذه الادعاءات من السمات المميزة لمخطط بونزي الوهمي/ التسويق الهرمي، وقد تؤدي إلى خسائر مالية جسيمة.

تحذيرات بشأن المعاملات المالية

تحذيرات أمنية عامة

- **التحقق من مصداقية المصدر:** قبل مشاركة أي بيانات شخصية أو مالية تحقق دائمًا من هوية الشركة أو المؤسسة عبر موقعها الرسمي وأرقام الاتصال المدرجة من مصادر معتمدة.

- **تجنب الروابط غير الموثوقة:** توخّ الحذر عند تصفح مواقع غير مألوفة، وتجنب النقر على روابط مشبوهة أو تحميل مرفقات غير مُثبتة المصدر. كما يُنصح بإدخال البيانات الحساسة فقط على المواقع التي تستخدم اتصالًا آمنًا عبر HTTPS.

- **حماية المعلومات الحساسة:** لا تشارك معلوماتك الشخصية أو المالية عبر الهاتف، البريد الإلكتروني، أو منصات غير موثوقة. استخدم كلمات مرور قوية وفريدة، وحافظ على تحديث برامج الأمان على أجهزتك.

- **تجاهل الرسائل الإلكترونية المشبوهة:** لا تتفاعل أبدًا مع الرسائل غير المطلوبة، خاصة تلك التي تحتوي على روابط أو مرفقات، إذ قد تقود إلى مواقع تصيد احتيالي أو تحتوي على برمجيات خبيثة تهدف لسرقة بياناتك.

- **تحديث معلومات الاتصال فورًا:** تأكد من تحديث بيانات البنك أو المحفظة الإلكترونية الخاصة بك فورًا عند حدوث أي تغيير (مثل رقم الهاتف)، لضمان استلام رموز التحقق (OTP) وتنبيهات المعاملات على الجهاز الصحيح.

- **تجنب المكالمات الاحتيالية الدولية:** يُنصح بعدم الرد على مكالمات غير متوقعة من أرقام دولية، حيث تُستخدم هذه الطرق كثيرًا في مخططات الاحتيال.

حماية الجهاز / الحاسوب أو الهاتف

- **تغيير كلمات المرور بانتظام:** قم بتحديث كلمات المرور بشكل دوري واستخدم تركيبات قوية وفريدة لكل حساب.

- **تثبيت وتحديث برامج مكافحة الفيروسات:** تأكد من تثبيت برامج مكافحة الفيروسات، وتفعيلها، وتحديثها بانتظام. كما ينبغي تطبيق جميع تحديثات أمان نظام التشغيل فور صدورها.

- **توخي الحذر مع الأجهزة الخارجية:** لا تستخدم وحدات تخزين USB غير معروفة قبل فحصها أولًا بأدوات أمان محدثة.

- **تأمين الأجهزة ماديًا:** لا تترك جهاز الحاسوب أو الجهاز المحمول الخاص بك مفتوحاً أو دون مراقبة أو غير مقفل. واستخدم دومًا شاشات القفل وقم بتعيين كلمات مرور قوية للأجهزة.

- **تفعيل ميزة القفل التلقائي:** قم بضبط أجهزتك لتقفل تلقائيًا بعد فترة من عدم النشاط لمنع الوصول غير المصرح به.

- **تجنب تثبيت البرامج غير الموثوقة:** لا تقم بتحميل أو تثبيت التطبيقات أو البرامج من مصادر غير رسمية أو مجهولة.

- **تجنب تخزين البيانات الحساسة دون حماية:** تجنب حفظ كلمات المرور، أو بيانات الحسابات البنكية، أو المعرفات الشخصية مباشرة على الجهاز دون حماية أو كلمة مرور.

- **النسخ الاحتياطي للبيانات المهمة:** قم بعمل نسخ احتياطية منتظمة للملفات الهامة على وسائل تخزين خارجية آمنة أو خدمات سحابية مشفرة لحماية البيانات من الفقدان.

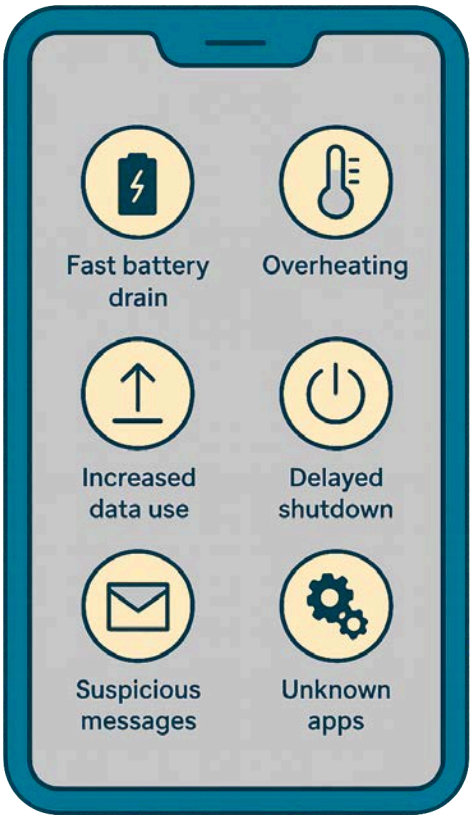
تصفح الإنترنت بشكل آمن

- تجنب الوصول إلى مواقع إلكترونية غير موثوقة أو مشبوهة.
- لا تقم باستخدام متصفحات إنترنت غير مألوفة أو غير موثوقة.
- لا تقم بإدخال معلومات شخصية أو حساسة على مواقع غير مؤمنة أو عبر أجهزة مشتركة/عامة.
- لا تقم بالكشف عن معلوماتك المالية لأي شخص وخاصة عبر وسائل التواصل الاجتماعي أو جهات اتصال غير موثوقة.

الحصول على خدمات بنكية آمنة عبر الانترنت

- قم بتسجيل الخروج فور الانتهاء من أي جلسة مصرفية إلكترونية.
- حدّث كلمات المرور بانتظام، وتأكّد من أنها قوية وفريدة لكل حساب.
- تجنب إعادة استخدام كلمات المرور نفسها بين حسابات البريد الإلكتروني والخدمات المصرفية الإلكترونية.
- امتنع عن إجراء المعاملات المالية على الأجهزة العامة أو المشتركة (مثل مقاهي الإنترنت)، إلا إذا كان ذلك ضروريًا للغاية.

المؤشرات التي تدل على أن هاتفك مخترق



- نفاد البطارية أو الشحن السريع غير المعتاد.
- ارتفاع حرارة الجهاز بشكل غير طبيعي.
- زيادة غير متوقعة في استهلاك البيانات.
- تأخر أو فشل في إيقاف التشغيل.
- نشاط لرسائل نصية مشبوهة.
- ظهور تطبيقات او أنشطة غير معروفة على الجهاز دون القيام بها.

الإجراءات الواجب اتباعها
بعد تعرضك لعملية احتيال مالي

- قم بحظر بطاقة الدفع الخاصة بك وتجميد رصيد حسابك البنكي أو المحفظة الإلكترونية المرتبطة بالبطاقة من خلال زيارة الفرع أو الاتصال برقم خدمة العملاء الرسمي المتوفر على موقع البنك أو الشركة المالية. بالإضافة إلى ذلك، تحقق من أمان قنوات البنك الأخرى مثل الخدمات المصرفية الإلكترونية، وتطبيق البنك على هاتفك المحمول، وتطبيق المحفظة الإلكترونية.

- قدّم شكوى لدى البنك أو الشركة المالية وكذلك لدى البنك المركزي الأردني.

- تواصل أو قدّم بلاغًا إلى وحدة الجرائم الإلكترونية.

- قم بإجراء إعادة ضبط المصنع لهاتفك المحمول (الإعدادات - إعادة التعيين - إعادة ضبط المصنع) لاستعادة الهاتف في حال حدوث احتيال ناتج عن تسرب بيانات منه.

What TO DO !!!

الاحتياطات المتعلقة ببطاقات الدفع

- قم بتعطيل الميزات الاختيارية على بطاقة الدفع الخاصة بك مثل عمليات الشراء عبر الإنترنت (محلية ودولية) عندما لا تكون قيد الاستخدام. وإذا لم تقم بإستخدام البطاقة الخاصة بك لفترة طويلة، فمن المستحسن تعطيلها عبر تطبيق البنك الرسمي أو المنصة الإلكترونية.

- يجب دائمًا التحقق من مبلغ المعاملة المعروض على شاشة جهاز نقاط البيع (POS) قبل إدخال رقم التعريف الشخصي (PIN) أو استخدام الدفع اللاتلامسي.

- لا تسمح للتجار بأخذ بطاقتك بعيدًا عن نظرك لإتمام عملية الشراء.

- كن يقظًا عند إدخال رقم التعريف الشخصي في أجهزة الصراف الآلي أو نقاط البيع لمنع التصنت أو استخدام أجهزة النسخ (Skimming).

كلمات المرور الآمنة

- استخدم كلمات مرور قوية تتكون من 14 حرفًا على الأقل، تجمع بين الحروف الكبيرة والصغيرة، والأرقام، والرموز الخاصة (مثل @، #، !).
- تجنب استخدام معلومات شخصية يمكن التعرف عليها (PII) في كلمات المرور—مثل اسمك، تاريخ ميلادك، أو أسماء الأقارب.
- قم بتفعيل المصادقة الثنائية (2FA) أو المصادقة متعددة العوامل (MFA) حيثما توفرت، خاصة للحسابات الحساسة.
- قم بتغيير كلمات المرور بانتظام وتجنب إعادة استخدام نفس الكلمة عبر منصات متعددة.

تنبيهات قبل الايداع

- عند إيداع الأموال في البنك، ينبغي دائمًا طلب إيصال مطبوع يؤكد إتمام العملية، ويحفظ حقك في حال حدوث أي أخطاء.
- تأكد من أن الايصال يتضمن كل من:

مبلغ الإيداع بالأرقام والكلمات.
تاريخ المعاملة.
اسم المودع.

تقديم الشكاوى

- إذا واجهت أي مشاكل مع البنوك أو المؤسسات المالية غير البنكية التي تتعامل معها، فلديك الحق في تقديم شكوى إلى البنك المركزي الأردني على كافة البنوك والمؤسسات المالية الخاضعة لرقابته واشرافه (شركات التمويل الأصغر، شركات الصرافة، وشركات خدمات الدفع، شركات التأمين)

- في البداية، يجب عليك تقديم الشكوى إلى البنك/المؤسسة المالية التي تتعامل معها. وفي حال عدم الاستجابة أو عدم رضاك عن الرد، بإمكانك تقديم شكواك الى البنك المركزي الأردني أو اللجوء الى القضاء.

- يمكن تقديم الشكوى إلى البنك المركزي عبر الوسائل التالية:

  - الاتصال بقسم حماية المستهلك المالي على الرقم: 064630301
  - الأرقام الفرعية: 1113 / 1515 / 4825
  - الموقع الإلكتروني: www.cbj.gov.jo
  - البريد الإلكتروني: fcp@cbj.gov.jo
  - زيارة مقر البنك المركزي أو فروعه في إربد والعقبة.
  - الفاكس: 064602482
  - العنوان البريدي: صندوق بريد 37، عمان 11118، الأردن

- بالنسبة للشكاوى المتعلقة بشركات التأمين، يمكن التواصل مع دائرة الرقابة على أعمال التأمين عبر القنوات التالية:

  - الاتصال بالدائرة، بما في ذلك إدارة حل نزاعات التأمين، على الأرقام الفرعية: 4649 / 4969 / 4968 / 4972
  - البريد الإلكتروني: Insurance.Supervision@cbj.gov.jo

قائمة المصطلحات

Uniform Resource Locator (URL)	رابط الموقع الإلكتروني
Personal Identification Number (PIN)	رقم التعريف الشخصي
One-Time Password (OTP)	رموز التحقق لمرة واحدة
Hypertext Transfer Protocol Secure (HTTPS)	بروتوكول نقل النص التشعبي الآمن
Card Verification Code (CVC)	رمز التحقق من البطاقة
Short Message/ Messaging Service (SMS)	الرسالة القصيرة
Universal Serial Bus (USB)	الناقل التسلسلي العام (أجهزة الفلاش)
Personally Identifiable Information (PII)	معلومات شخصية يمكن التعرف عليها
Two-Factor Authentication (2FA)	المصادقة الثنائية
Muti-Factor Authentication (MFA)	المصادقة متعددة العوامل