البنك المركزي الاردني

دليل التوعية في الاحتيال المالي

بإستخدام الوسائل الالكترونية

2023

دائرة حماية المستهلك المالي FCP
ووحدة الاستجابة للحوادث السيبرانية للقطاع المالي والمصرفي
Jo-FinCERT

الفهرس

المقدمة

في ظل توسع نطاق الخدمات المالية وتنوعها والتي أصبحت أهميتها أكثر وضوحاً بعد جائحة كورونا، وزيادة انتشار الخدمات المالية الإلكترونية الناجمة عن التطورات التكنولوجية المتسارعة والتي تبينت مزاياها للعملاء من حيث إمكانية استخدامها بأمان وسهولة وسرعة وبتكلفة معقولة.

وفي ضوء التزايد المستمر في استخدام الخدمات الإلكترونية والذي أدّى إلى ظهور أساليب احتيالية تطال المستهلك المالي وتعرضه لمخاطر وقوعه ضحية للنصب والاحتيال، وانطلاقاً من دور البنك المركزي الأردني في رفع وعي المستهلك المالي يصدر البنك هذا الدليل التوعوي بهدف توعية المستهلك المالي بأساليب الاحتيال والطرق التي يتبعها المحتالون وكيفية التعامل معها.

كما يؤكد البنك المركزي الأردني على المستهلك المالي عدم مشاركة أو إفشاء أي بيانات شخصية وخصوصاً المالية مع أي طرف غير موثوق.

طرق التعامل والإجراءات الوقائية

روابط التصيد

- روابط التصيد: هي روابط تبدو مشبوهة وغالبًا ما تظهر عبر البريد الإلكتروني، الرسائل النصية، ووسائل التواصل الاجتماعي ، تهدف هذه الروابط إلى خداع الأشخاص للنقر عليها، حيث يتم توجيههم إلى مواقع وهمية تحاكي المواقع الفعلية وعادةً ما تطلب هذه المواقع من المستخدمين تسجيل الدخول أو تقديم معلومات شخصية أو مالية حساسة.

اشكال روابط التصيد:

- الرسائل البريدية الاحتيالية.
- رسائل الهاتف النصية الاحتيالية.
- الوسائط الاجتماعية.

التحذير

- قبل النقر على أي رابط أو فتح مرفق في رسالة أو رسالة نصية، تأكد من أنها آمنة وموثوق بها يمكن استخدام برامج مكافحة البرامج الضارة للتحقق من صحة المرفقات وروابط الويب.

- قم بزيارة الموقع الإلكتروني الرسمي للبنك أو الشركة المالية الذي تتعامل معه، وتحقق بعناية من تفاصيل الموقع الإلكتروني، خاصة عندما يتطلب ذلك إدخال بيانات أو بيانات سرية، وتحقق من وجود العلامة الآمنة (https) مع رمز القفل على الموقع الإلكتروني قبل إدخال أي بيانات أو بيانات سرية.

- تحقق من عناوين المواقع الإلكترونية(URL) واسم النطاق (Domain) الواردة في رسائل البريد الإلكتروني بحثاً عن الأخطاء الإملائية.

مكالمات التصيد

مكالمات التصيد : هي مكالمات هاتفية يتم استخدامها من قبل محتالين لخداع الأشخاص والاستيلاء على معلومات شخصية أو مالية حساسة ، يتنوع نوع المكالمات التصيدية، وتشمل مطالبات زائفة بالفوز بجائزة ، أو التحقق من بيانات الحساب البنكي، أو طلب المساعدة في مشكلة مزيفة ، يهدف المحتالون إلى استغلال ضعف الثقة أو الارتباك لدى الأشخاص وإقناعهم بالتعامل معهم.

أشكال مكالمات التصيد:

- مكالمات الفوز بجوائز.
- مكالمات التحقق من الحسابات البنكية.

التحذير

- اعلم بأن البنك أو الشركات المالية لا يقومون بالطلب من العملاء مشاركة البيانات السرية، مثل اسم المستخدم، كلمة المرور، تفاصيل بطاقات العميل (رسائل التحقق لمرة واحدة (OTP) ، (CVV)).

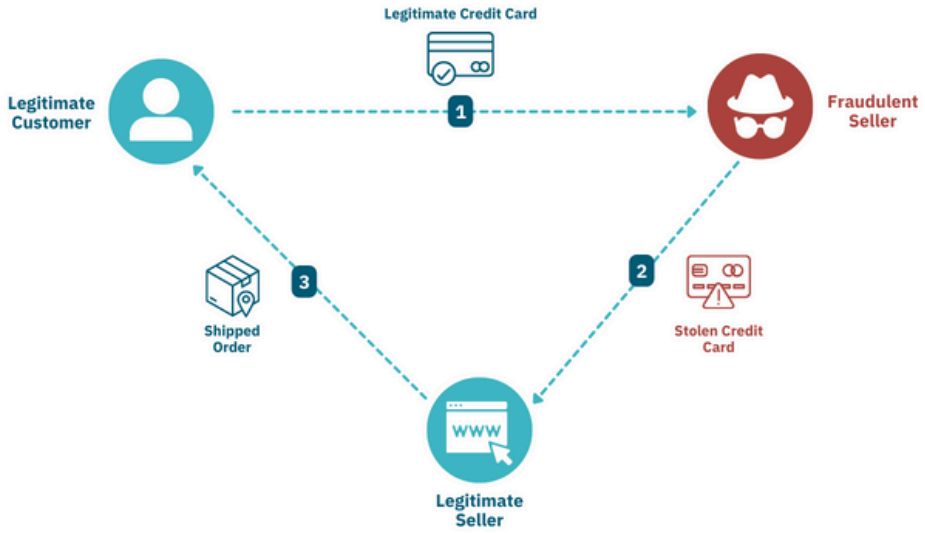
- إذا تلقيت مكالمة تطلب منك تنفيذ إجراء غير معتاد أو دفع مبلغ مالي فورًا، تحقق قبل اتخاذ أي إجراء إتصل بالبنك أو المؤسسة المذكورة في المكالمة باستخدام معلومات الإتصال الرسمية وتحقق من طلبهم.

الاحتيال من خلال منصات البيع الإلكترونية

الاحتيال عبر منصات البيع الإلكتروني : هو نوع من الاحتيال يستهدف المستهلكين الذين يقومون بالتسوق عبر الإنترنت ، يتم تنفيذه عن طريق إنشاء مواقع وهمية أو حسابات مزيفة على منصات البيع الإلكتروني المعروفة، مما يمكّن المحتالين من الاحتيال على المشترين من خلال عروض ومنتجات زائفة، أو سرقة بيانات الدفع، أو عدم تسليم السلع المطلوبة.

أشكال الاحتيال عبر منصات البيع الإلكتروني:

- البيع الوهمي .
- سرقة بيانات الدفع.



التحذير

- كن حذراً دائماً عند شراء المنتجات أو بيعها باستخدام منصات البيع الالكترونية.
- تذكر دائماً أنه ليست هناك حاجة لإدخال رقم التعريف الشخصي/ كلمة المرور في أي مكان لاستلام أموال.
- قبل القيام بأي عملية شراء عبر منصات البيع الإلكتروني، قم بالبحث والتحقق من سمعة المتجر أو البائع قراءة تقييمات المستخدمين الآخرين والتعليقات قد تكشف عن سلوك احتيالي سابق أو تعامل غير مشروع

الاحتيال باستخدام تطبيقات الهاتف

- تطبيقات الهاتف المحمول المزيفة : هي تطبيقات تدعي أنها تقدم خدمات معينة ولكنها في الحقيقة تستخدم للحصول على المعلومات الشخصية للمستخدمين أو للوصول إلى البيانات المالية الحساسة .

- يقوم المحتالون بخداع العميل لفتح هذه الروابط مما يؤدي إلى تحميل تطبيقات مزيفة بمجرد تحميل التطبيق، ممكن أن يحصل المحتال على وصول كامل إلى جهاز العميل بما في ذلك البيانات السرية المخزنة على الجهاز والرسائل و رسائل التحقق لمرة واحدة (OTP) المستلمة قبل وبعد تثبيت هذه التطبيقات.

التحذير

- لا تقم بتحميل تطبيق من أي مصدر لم يتم التحقق منه/ غير معروف أو تم ارساله من قبل شخص مجهول.

- كممارسة واعية ومنطقية قبل التحميل، تحقق من ناشري/مالكي التطبيق بالإضافة إلى تقييمات المستخدمين وما إلى ذلك.

- تحقق من الأذونات التي يحتاجها التطبيق قبل تنزيله، وتأكد من أنه لا يطلب إذناً غير متناسب مع وظائف التطبيق.

الاحتيال باستخدام جهاز الصراف الآلي (ATM)

- سرقة بيانات بطاقات الدفع (البطاقات المدفوعة مسبقا ، المدينة والدائنة): هذا النوع من الاحتيال يحدث عندما يقوم المحتالون بتركيب أجهزة مزورة على أجهزة الصراف الآلي، تسمى أيضًا "جهاز التقاط البطاقة" هذه الأجهزة لسرقة معلومات البطاقات والرقم السري الخاص بها.

- قد يقوم المحتالون أيضاً بتثبيت لوحة مفاتيح وهمية على جهاز الصراف الآلي أو كاميرا صغيرة مخفية عن الأنظار لالتقاط رقم التعريف الشخصي (PIN).

في بعض الأحيان، يتظاهر المحتالون بأنهم يرغبون باستخدام الصراف الآلي ويقفون بالقرب من العميل للوصول إلى رقم التعريف الشخصي (PIN) عندما يدخلها العميل في جهاز الصراف الآلي، ثم يتم استخدام هذه البيانات لإنشاء بطاقة مكررة وسحب الأموال من حساب العميل.

التحذير

- تحقق دائماً من عدم وجود جهاز إضافي متصل أو بالقرب من الجزء المخصص لإدخال البطاقة أو لوحة المفاتيح الخاصة بجهاز الصراف الآلي قبل إجراء أي معاملة.
- قم بتغطية لوحة المفاتيح بيدك الأخرى أثناء إدخال رقم التعريف الشخصي (PIN).
- لا تكتب رقم التعريف الشخصي (PIN) على بطاقة الدفع الخاصة بك.
- لا تدخل رقم التعريف الشخصي (PIN) في وجود أي شخص آخر/ غير معروف بالقرب منك.
- لا تقم بإعطاء بطاقة الدفع الخاصة بك لأي شخص.
- لا تقم باتباع التعليمات التي يقدمها أي شخص مجهول أو تطلب المساعدة/ الإرشاد من المجهولين عند استخدام أجهزة الصراف الآلي.
- اذا لم يتم صرف النقود في جهاز الصراف الآلي، اضغط على زر "إلغاء" وانتظر الشاشة الرئيسية حتى تظهر قبل مغادرة الصراف الآلي.

الاحتيال من خلال تطبيقات الشبكة الافتراضية (VPN)

تطبيقات الشبكة الافتراضية (VPN) : هي تطبيقات تستخدم لغايات خلق إتصال بخوادم وسيطة بين المستخدم والمواقع المراد استخدامه من خلال جهاز الحاسوب أو الهاتف تستخدم عادة لغايات الوصول لمواقع أو تطبيقات محظورة محليا .

بعض هذه التطبيقات غير موثوقة تستخدم لغايات الحصول على بيانات الهاتف ضمن الأذونات الخاصة بالتطبيق .

كما تستخدم في الاحتيال في حال تم تسجيل الدخول على التطبيقات الخاصة بالبنوك أو المحافظ عند تفعيل الإتصال من خلال تطبيق الشبكة الافتراضية (VPN) غير الآمن كسرقة معلومات الدخول الخاصة بالتطبيق أو معلومات بطاقات الدفع المسجلة على الهاتف .

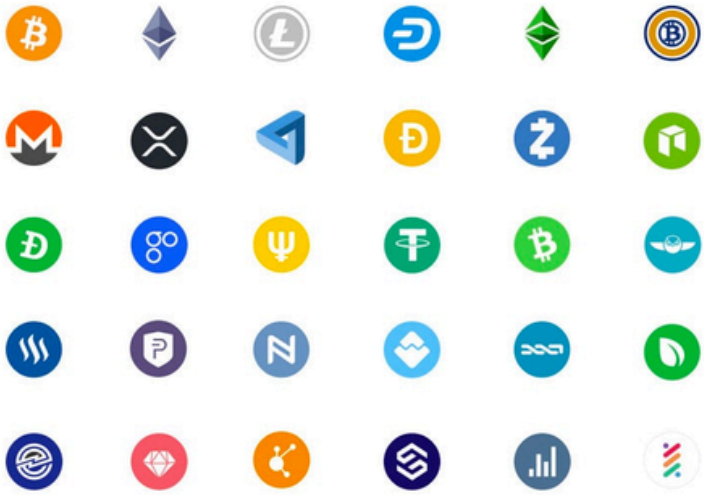
التحذير

- تجنب استخدام تطبيقات الشبكة الافتراضية (VPN) المجانية التي قد تكون غير موثوقة وتسرب بيانات المستخدم.
- لا تقم بالقيام اي معاملة بنكية خلال فترة الإتصال بتطبيق الشبكة الافتراضية (VPN) تجنبا لسرقة بياناتك البنكية .
- عدم تزويد تطبيق الشبكة الافتراضية (VPN) بمعلومات حساسة مثل معلومات بطاقات الدفع أو كلمات السر.

الاحتيال من خلال منصات التداول أو الوسطاء

عادة ما يتم التحايل على المستخدمين لتطبيقات التداول وبشكل خاص التداول من خلال العملات الرقمية كونه غير مصرح بها من خلال وسطاء لسحب وإيداع الأموال وعليه تتضمن خطورة على الأموال المنقولة كونها غير خاضعة لأي سياسة أو قوانين واضحة عدا انها مخالفة للقانون كذلك .

كما يتم التحايل كذلك من خلال وسطاء لتشغيل الاموال من خلال التداول بحيث يتم الاتفاق على ايداع رأس المال من خلال الطرف الأول والتداول لكسب المال من الطرف الثاني بصورة غير مكتوبة أو موثقة مما يؤدي لخسارة الطرف الأول للمال المودع أو سرقته من الطرف الثاني .



التحذير

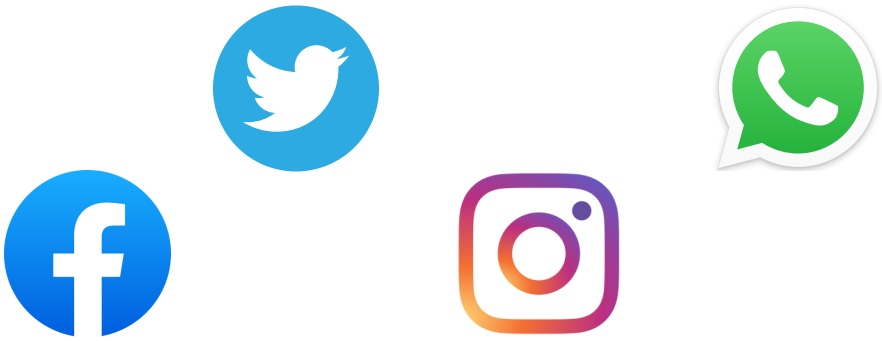
- احذر من التعامل مع الشركات أو الأفراد التي تدعي إمكانية مضاعفة الأموال بشكل غير منطقي خلال فترة زمنية قصيرة وذلك تجنباً للتعرض للاحتيال وخطر خسارة الأموال من خلال التداول بالعملات الرقمية .

انتحال شخصية على مواقع التواصل الاجتماعي

- انتحال الشخصية يحدث عندما يستخدم شخص ما معلومات شخصية أو الهوية لشخص آخر على مواقع التواصل الاجتماعي، قد يتم استخدام هذه المعلومات لخلق حساب مزيف، تقديم معلومات زائفة، أو إرسال رسائل خادعة باسم الشخص المنتحل.

- يرسل المحتالون طلباً لك على أنهم أحد أصدقائك يطلبون فيه المال بشكل عاجل لأغراض علاجية، دفع لبعض الحاجات الاساسية، وما إلى ذلك.

- يقوم المحتالون أيضاً باستخدام تفاصيل غير حقيقية للتواصل مع بعض مستخدمي هذه التطبيقات وكسب ثقتهم على مدار فترة زمنية من الوقت، وفي حال مشاركة المستخدمون بياناتهم الشخصية أو الخاصة، يقوم المحتالون باستخدام هذه البيانات لابتزازهم وأخذ الأموال منهم.



التحذير

- تحقق دائماً من صحة من يطلب منك مال إن كان صديق أو قريب من خلال التأكد بمكالمة هاتفية أو بشكل شخصي للتأكد من عدم انتحال أي شخص آخر هويته.

- لا تقم بدفع مبالغ مالية لأشخاص مجهولين عبر الإنترنت.

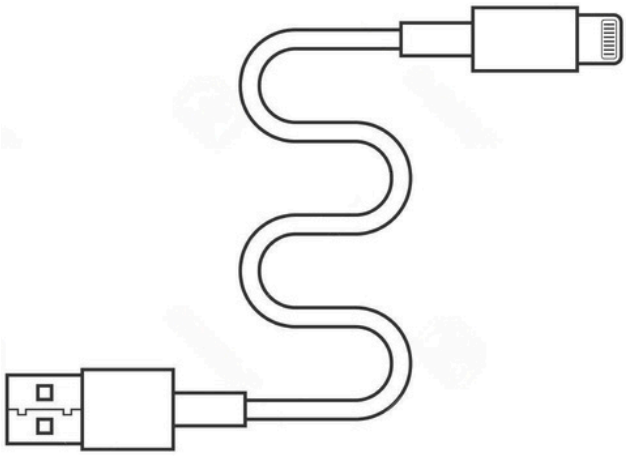
- لا تشارك البيانات الشخصية والسرية على منصات التواصل الاجتماعي.

الاحتيال باستخدام منافذ / كوابل الشحن

Charging Cable Fraud

يشير الاحتيال عن طريق استخدام كابلات الشحن إلى استخدام كابلات الشحن المزيفة أو المعدلة بغرض سرقة معلوماتك الشخصية, أو إصابة جهازك الذي تقوم بشحنه ببرامج ضارة, يتم تعديل الكابلات بشكل يتيح للمهاجمين الوصول غير المصرح به إلى جهازك, أو تسجيل بياناتك الحساسة دون علمك.

قد تكون على شكل كوابل أو محطات للشحن في الأماكن العامة .



التحذير

- يجب تجنب استخدام كابلات الشحن المتوفرة في الأماكن العامة كمحطات الشحن العامة حيث لا يمكن معرفة ما إذا كانت هذه الكابلات تم تعديلها أو لا، وبالتالي يمكن أن تشكل خطرًا على جهازك ومعلوماتك.

الاحتيال عن طريق اليانصيب الوهمي

- يعتبر الاحتيال عن طريق اليانصيب الوهمي نوعًا من أنواع الاحتيال الإلكتروني يستهدف طموحات الأشخاص في الفوز بجوائز كبيرة من خلال اليانصيب، يتم إغراء الضحايا بالمشاركة في يانصيب وهمي حيث يتم تزوير النتائج وإخبار الضحية بفوزها الكبير، ولكنها في الحقيقة لا تحصل على أي جائزة ويتم سرقة أموالها أو استغلالها بطرق غير قانونية.

- يطلب المحتالون منك دفع الضرائب أو رسوم الاستلام مقدماً وما إلى ذلك لاستلام اليانصيب.

التحذير

- يجب أن تكون حذرًا تجاه أي رسائل أو مكالمات غير معروفة تعلن عن فوزك في يانصيب لم تشترك فيه، قد تكون هذه رسائل احتيالية تستهدف سرقة معلوماتك الشخصية.

- لا تقم بإجراء أي عمليات دفع أو مشاركة بياناتك المالية رداً على أي مكالمات أو رسائل بريد إلكتروني.

الاحتيال الوظيفي عبر الانترنت

- يشير احتيال التوظيف إلى استخدام ممارسات غير قانونية أو مضللة لخداع الأشخاص الباحثين عن وظائف وسرقة معلوماتهم الشخصية أو استغلالها، يستخدم المحتالون أساليب متنوعة لجذب الضحايا وإقناعهم بتقديم المعلومات الحساسة مثل السيرة الذاتية، وثائق الهوية، ومعلومات مالية، وذلك بهدف استغلالها لأغراض مشبوهة مثل الاحتيال المالي أو سرقة الهوية.

- يتواصل المحتالون من خلال مواقع الكترونية للتوظيف يتم إنشاؤها بهدف استقطاب الباحثين عن وظائف .

- يتم استقبال المتقدمين لوظائف عمل وإجراء مقابلات وهمية ومن ثم يتم طلب تحويل أموال إلى حسابات الشركة الوهمية لاستكمال إجراءات التعيين.

التحذير

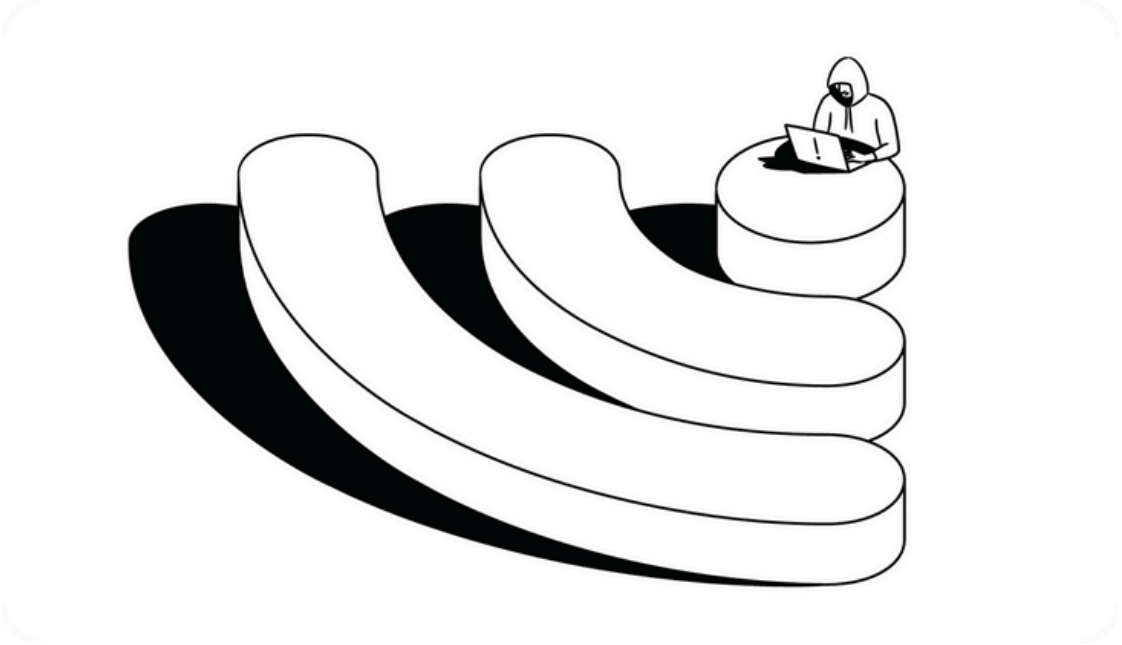
- قبل التفاعل مع أي عرض وظيفي، قم بإجراء بعض الأبحاث عن الشركة المعلنة والتحقق من صحة المعلومات التي تقدمها.

- استخدم مواقع ومصادر موثوقة للتحقق من وجود الشركة ومصداقيتها.

الاحتيال من خلال شبكات الانترنت العامة

شبكات الانترنت العامة هي شبكة تكون متوفرة بالأماكن العامة تتيح الإتصال عبر الانترنت قد يبدو بأنها خدمة مجانية للوصول للانترنت لكنها قد تستخدم لغايات الحصول على معلومات الأجهزة التي تحاول الإتصال بالشبكة العامة .

من خلال الشبكة العامة يمكن الحصول على معلومات خاصة بالجهاز كالمعلومات المحفوظة على الجهاز أو تحميل ملفات تعريف على الجهاز دون علم المستخدم .



التحذير

- لا تقم بالإتصال بأي شبكة عامة أو شبكة مجانية سواء تطلبت الدخول عبر رمز سري أو لم تتطلب ذلك.
- قم بإيقاف تشغيل إتصال Wi-Fi التلقائي: قم بإيقاف تشغيل إتصال Wi-Fi التلقائي على جهازك لمنعه من الإتصال تلقائيًا بشبكات Wi-Fi العامة بدلاً من ذلك ، إتصل يدويًا بالشبكات الموثوقة فقط.

انتحال اسم شركة تمويل مرخصة من البنك المركزي

- الإتصال هاتفياً أو ارسال رسائل نصية أو ارسال بريد إلكتروني منتحلة اسم شركة تمويل وإيهام العملاء بمنحهم قرض/تمويل حيث ان هذه الشركات تعرض معدلات فائدة منخفضة، و/أو خيارات سداد ميسرة و/أو دون الحاجة إلى ضمانات.

- في حال تجاوب العميل، يتم تزويده بعقود وهمية وطلب مجموعة من العمولات والرسوم وبعد دفعها يختفي المحتال.

التحذير

- لا تصدق العروض التي يقدمها أشخاص بأنفسهم سواء من خلال الإتصال أو عبر الرسائل.

- يجب التأكد من الشركة التي تقدم القرض /التمويل في حال كانت شركة مرخصة من قبل البنك المركزي الأردني ويفضل زيارة أحد فروع الشركة كما هو منشور على موقعهم الإلكتروني المبين على موقع البنك المركزي.

مخطط بونزي الوهمي/ التسويق الهرمي

- يقوم المحتالون بإقناع العملاء استثمار مبلغ مالي، حيث من الممكن أن يكون مبلغ بسيط ويقوم بوعدهم أن عائد الاستثمار سيكون ضخماً.

- يعرض المحتالون على العميل أن يقوموا بتسويق هذا الاستثمار وإدخال أعضاء جدد مقابل عائد وعمولة عن كل عميل مضاف عن طريقهم في السلسلة.

- بعد دخول المزيد من الأعضاء يقوم المحتالون بإغلاق المخطط والحصول على كافة الأموال المستثمرة من العملاء.

التحذير

- إحذر من التعامل مع الشركات التي تدعي إمكانية مضاعفة الأموال بشكل غير منطقي خلال فترة زمنية قصيرة وذلك تجنباً للتعرض للاحتيال والنصب وخطر خسارة الأموال.

تحذيرات بشأن المعاملات المالية

تحذيرات عامة

- قبل تقديم أي معلومات شخصية أو مالية أو القيام بأي عملية مالية، تأكد دائمًا من صحة ومصداقية المصدر، تحقق من هوية الشركة أو المؤسسة وتحقق من وجودها الفعلي عن طريق الاستعانة بمواقع رسمية، والإتصال بالأرقام المعلنة والتحقق من الأطراف المعنية.

- كن حذرًا عند التعامل مع المواقع غير موثوقة، وتجنب فتح روابط غير معروفة أو تحميل ملفات مرفقة غير مشروعة، تأكد من أن الموقع يستخدم إتصال آمن (HTTPS) قبل إدخال أي معلومات شخصية أو مالية .

- تجنب مشاركة معلوماتك الشخصية أو المالية الحساسة عبر الهاتف أو البريد الإلكتروني أو المواقع غير موثوقة، قم بتحديث برامج الحماية على أجهزتك الإلكترونية واستخدم كلمات مرور قوية ومتنوعة .

- لا تقوم بالرد على رسائل البريد الإلكتروني الواردة من مصادر غير معروفة لأنها قد تحتوي على مرفقات تحتوي على برامج خبيثة لسرقة بياناتك أو روابط تصيد احتيالية.

- تأكد دائما من تحديث بياناتك لدى البنك أو المحفظة فورا في حال تغيرها كرقم الهاتف كون الرسائل الخاصة بحسابك (رسائل الحركات أو رسائل التحقق لمرة واحدة (OTP)) سوف يتم ارسالها على رقم هاتفك المسجل لدى البنك أو المحفظة .

- لا تقم بالاجابة عن مكالمات واردة على هاتفك في حال ورودها من جهات إتصال دولية كونه عادة ما يتم التحايل بمثل هذه الطرق .

- لا تشارك اي صور شخصية أو صور عن اثبات الشخصية الخاص بك (الهوية الشخصية أو جواز السفر) مع أي جهة .

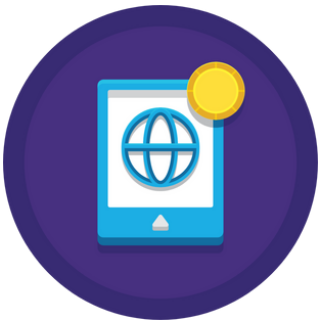
حماية الجهاز / الحاسوب أو الهاتف

- قم بتغيير كلمات المرور بشكل مستمر.
- قم بتثبيت برنامج مكافحة الفيروسات على أجهزتك وتحديثه بشكل مستمر وتأكد من تحميل آخر التحديثات الأمنية الخاصة بنظام تشغيل هاتفك .
- قم دائماً باختبار الاقراص المحمولة (USB) غير المعروفة قبل الاستخدام.
- لا تترك جهاز الحاسوب مفتوحاً، ولا تترك هاتفك بدون قفل .
- ضع آلية القفل التلقائي على هاتفك/ جهاز الحاسوب بعد مدة محددة .
- لا تقم بتثبيت أي تطبيقات أو برامج غير معروفة على هاتفك/ جهاز الحاسوب.
- لا تقم بحفظ كلمات المرور أو البيانات السرية على الأجهزة.
- احتفظ بنسخة من بياناتك المهمة على الجهاز بنسخة احتياطية على جهاز صلب خارجي أو من خلال منصات خدمات التخزين السحابية .

تصفح الإنترنت بشكل آمن

- تجنب زيارة المواقع الإلكترونية غير الآمنة/ غير المعروفة.
- تجنب استخدام متصفحات غير معروفة.
- تجنب إدخال بياناتك الشخصية على مواقع الانترنت/ الأجهزة العامة غير المعروفة.
- لا تشارك بياناتك المالية مع أي شخص، ولا سيما الأشخاص غير المعروفين على وسائل التواصل الاجتماعي.

الحصول على خدمات بنكية آمنة عبر الانترنت



- استخدم دائماً لوحة المفاتيح الافتراضية على أجهزة الحاسوب العامة وذلك في ظل وجود آليات اختراق من خلال التقاط سجل المدخلات الخاصة ب لوحة المفاتيح .
- قم بتسجيل الخروج من الخدمات البنكية عبر الإنترنت مباشرة بعد الاستخدام.
- تحديث كلمات المرور بشكل دوري.
- لا تستخدم كلمات المرور نفسها للبريد الإلكتروني والخدمات البنكية عبر الإنترنت.
- حاول قدر الإمكان تجنب استخدام الأجهزة العامة (مثل مقهى الإنترنت) لإجراء المعاملات المالية.

المؤشرات التي تدل على أن هاتفك يتم التجسس عليه

- ينفذ شحن بطارية هاتفك بشكل أسرع من المعتاد.
- قد يكون ارتفاع درجة حرارة هاتفك من العلامات التي تدل على قيام شخص ما بالتجسس عليك.
- يمكن أن تكون الزيادة غير المعتادة في مقدار استهلاك البيانات في بعض الأحيان علامة على تشغيل برنامج تجسس.
- قد تتداخل تطبيقات برامج التجسس أحياناً مع عملية إيقاف تشغيل الهاتف بحيث يفشل جهازك في إيقاف التشغيل بشكل صحيح أو يستغرق وقتاً أطول من المعتاد.
- يمكن لبرامج التجسس والبرامج الضارة استخدام الرسائل النصية لإرسال البيانات واستلامها.
- وجود تطبيقات على الجهاز لم تقم بتحميلها أو تطبيقات فعالة على الجهاز لم تقم بالنقر عليها .

الإجراءات الواجب اتخاذها بعد تعرضك لعملية احتيال

- قم بحظر بطاقة الدفع وتجميد الرصيد في الحساب البنكي / المحفظة الإلكترونية المرتبط بالبطاقة عن طريق زيارة فرعك أو الإتصال برقم خدمة العملاء الرسمي المتاح على موقع البنك/ الشركة المالية، بالإضافة إلى ذلك تحقق وتأكد من سلامة القنوات البنكية الأخرى مثل الانترنت البنكي وتطبيق البنك على هاتفك المحمول وتطبيق المحفظة الإلكترونية.
- قم بتقديم شكوى لدى البنك / الشركة المالية والبنك المركزي الأردني.
- إتصل أو قم بالإبلاغ عن عملية الاحتيال من خلال وحدة مكافحة الجرائم الالكترونية.
- قم بعمل إعادة تعيين هاتفك المحمول (Setting-Reset-Factory Data) لإعادة تعيين هاتفك في حالة حدوث عملية احتيال بسبب تسرب البيانات منه.

What

TO

DO !!!

الاحتياطات المتعلقة ببطاقات الدفع

- يجب عليك إلغاء تفعيل الميزات المختلفة لبطاقة الدفع في معاملاتك عبر الإنترنت المحلية والدولية، وفي حالة عدم استخدامك للبطاقة لفترة من الوقت فيجب عليك إيقاف تفعيلها على الانترنت.
- إذا كنت لا تستخدم بطاقتك، فيجب إلغاء تنشيط ميزة اللاتلامسية لبطاقتك.
- قبل إدخال رقم التعريف الشخصي في أي موقع من مواقع نقاط البيع (POS) أو أثناء استخدام البطاقة بميزة اللاتلامسية، يجب عليك التأكد بعناية من المبلغ المعروض على شاشة جهاز البيع.
- لا تدع التاجر يأخذ البطاقة بعيداً عن عينيك لتمريرها أثناء إجراء المعاملة.
- إحذر وانتبه أثناء إدخال رقم التعريف الشخصي في موقع نقاط البيع/ جهاز الصراف الآلي.

حماية حساب البريد الالكتروني

- لا تفتح الروابط المرسلة عبر رسائل البريد الإلكتروني من جهات غير معروفة.
- تجنب فتح رسائل البريد الإلكتروني على الشبكات العامة.
- لا تقم بتخزين بياناتك/ كلمات مرور حساباتك المالية، وما إلى ذلك في رسائل البريد الإلكتروني.

أمن كلمة المرور

- إستخدم مزيج من الأحرف الأبجدية الرقمية والرموز الخاصة في كلمة مرورك، وعلى الأقل أن تتكون من (14) خانة.
- إحتفظ بمصادقة ثنائية لجميع حساباتك، إذا كانت هذه متاحة.
- قم بتغيير كلمات المرور الخاصة بك بشكل دوري.
- تجنب إختيار أي من البيانات الشخصية عند تحديد كلمة المرور مثل تاريخ ميلادك واسم فرد من عائلتك.

الإحتياطات الواجب اتخاذها من قبل المودعين

- عند إيداع أموالك، كن حريص في الحصول على الإيصال لكل عملية إيداع تقوم بإجرائها لدى البنوك .
- يجب أن يكون الإيصال موقعاً حسب الأصول، وأن يكون يحتوي على قيمة الإيداع وتاريخه واسم المودع والمبلغ بالكلمات والأرقام .

تقديم الشكاوى

في حال واجهت أي مشكلة مع البنوك أو المؤسسات المالية غير البنكية التي تتعامل معها، لديك الحق بتقديم شكوى إلى البنك المركزي على كافة البنوك والمؤسسات المالية الخاضعة لرقابته: البنوك، شركات التمويل الأصغر، شركات الصرافة، وشركات خدمات الدفع.

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

يمكنك تقديم شكوى للبنك المركزي من خلال الوسائل التالية:

الإتصال بدائرة حماية المستهلك المالي: 06 4630301
على الأرقام الفرعية التالية: 1113 / 1515/4825
الموقع الإلكتروني للبنك المركزي: www.cbj.gov.jo
البريد الالكتروني لدائرة حماية المستهلك المالي: fcp@cbj.gov.jo

الحضور الشخصي لمبنى البنك المركزي الرئيسي، وفرعيه في إربد والعقبة.

الفاكس: 06 4602482
البريد العادي: ص.ب. 37 عمان 11118 الأردن

للشكاوى المتعلقة بشركات التأمين، يمكنك التواصل مع دائرة الرقابة على أعمال التأمين من خلال الوسائل التالية:

الإتصال مع الدائرة مع قسم حل نزاعات التأمين على الأرقام الفرعية التالية: 4649/ 4969/ 4968/ 4972
البريد الالكتروني لدائرة الرقابة على أعمال التأمين 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)	رسائل 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)