الخليج

اقتصاد, أسواق الإمارات

6 فبراير 2023 00:05 صباحا

اختراق بيانات عملاء البنوك..إلى متى «النزيف»؟

المحتال أو المخترق يعرف كل بيانات العميل بداية من الهاتف والاسم الكامل وتاريخ الميلاد وصولاً إلى أرقام البطاقات، لكنه يتوقف عند «الرقم الخلفي في البطاقة البنكية» الذي ينتظر التمكن منه ليقوم بعمليات الشراء من المتاجر الإلكترونية مباشرة، ويجد العميل نفسه أمام حالة إفلاس في مواجهة التزاماته «السكن – القرض – شراء مستلزمات البيت.. وغيرها الكثير».

ولوحظ أيضاً في عمليات النصب أن المحتال يختار صورة معروفة تخص «مديراً في البنك»، ليقوم بوضعها بجوار شعار البنك وشعار الدولة.

السؤال الذي يفرض نفسه هنا.. هل حملات التوعية التي يقوم بها المصرف المركزي والبنوك كافة حتى الآن لتوعية أفراد المجتمع.. كافية أم أن هناك من يتلاعب ببيانات العملاء داخل هذا البنك.

ففي حالتين من ثلاث حالات سقطوا في الفخ يختار المحتال «وقت الأذان»، ويحاول خداع العميل ويسرد عليه كل بياناته «وهي صحيحة» اسمه بالكامل ورقم هاتفه ورقم الهوية، وجهة عمله، والإمارة التي يسكن فيها.. فمن أين يأتي بهذه البيانات، إن لم يكن البنك نفسه مخترقاً؟

- **البنوك: سرعة الإبلاغ تلغي العملية الاحتيالية.. لكن لم يحدث**
- **استخدام اسم شخصية معروفة من البنك أحدث صيحات الاحتيال**
- **اختيار وقت «الأذان» كان سمة محتالين على عملاء بنك إسلامي**
- **«المخترقون يعرفون كل بيانات العميل عدا «الرقم الخلفي للبطاقة**

ورد عدد من الشكاوى إلى جريدة «الخليج» تتعلق باختراق أحد البنوك في الدولة عبر تسريب «بيانات العملاء» إلى ضعفاء النفوس الذين يستغلونها في الاستيلاء على الأموال، عبر أكثر من حيلة، لكن كلمة السر في الاحتيال والتي كانت وراء اختفاء رواتب وأموال العملاء هي «تحديث البيانات».

- **الحالة الأولى: 5 أيام وسحب الراتب بالكامل**

منذ بضعة شهور تفاجأ أحد عملاء بنك إسلامي باتصال هاتفي وقت «الأذان» من أحد المحتالين عبر الهاتف بداعي تحديث البيانات، ونجح الأخير بسرعة في أخذ بيانات البطاقة المصرفية منه وقام ب«الشراء عبر أحد مواقع التسوق الإلكترونية» ليجد العميل حسابه فارغاً من الراتب الذي لم يبقَ سوى ساعات فقط.. علماً بأن بطاقة العميل كانت جديدة وقام بتفعيلها قبل ساعة من عملية الاحتيال.

وقام العميل بالاتصال بالبنك للتأكد مما حدث، «ولماذا تم سحب هذه المبالغ مقابل مشتريات من أحد مواقع التسوق الإلكترونية»، فقاموا بتحويله إلى قسم الاحتيالات، وتم حجز المبلغ في حينها، وإيقاف الحساب، إلا أنه فوجئ بعد 5 أيام بسحب المبلغ، وأبلغه البنك أنه «لا يمكننا حجز المبلغ أكثر من ذلك» رغم شكوى العميل نفسه صاحب الحساب للبنك وقيامه بالاتصال بالشرطة وفتح بلاغ وتسجيل الواقعة، إلا أنه لم يفدْ ذلك بشيء.

- **الحالة الثانية: صورة مدير البنك.. والشك**

قامت إحدى عملاء بنك بزيارة إلى أحد الفروع بهدف تحديث بياناتها، لتتفاجأ بعدها بساعات فقط من اتصال هاتفي «يدّعي أنه من البنك»، لكنها وبسبب ما سمته من حوادث كانت واعية قليلاً، وطالبته بإثبات أنه من البنك ليرسل لها المخترق بطاقة التعريف الخاصة به مرسلة على ال«واتس آب»، وهنا تسلل الشك لديها، حيث إن بطاقة التعريف كان عليها شعار الدولة بجوار شعار البنك وصورته الشخصية.

الغريب في الأمر أيضاً أن الاتصال جاء وقت «الأذان» فجاءت الفكرة «هذا وقت الصلاة يمكن الاتصال بعد الصلاة» لتستغل هذا الوقت لتهرول إلى أقرب «صراف آلي» لتسحب نقودها منه، لتنجح في ذلك، لكن كانت المفاجأة، المحتال يتصل عليها ويقول: «هل أنتِ خارج المنزل.. هل سحبتِ نقودك من الماكينة» لتقول له نعم.. وأنا في البنك أحدث بياناتي، ليغلق الهاتف تماماً، وعند عرض صورة «البطاقة التعريفية» على موظفي البنك يؤكدون أنه أسلوب احتيالي، والبنوك لا تقوم بذلك.

- **الحالة الثالثة: اختراق هواتف الأصدقاء**

قام المحتال باختراق أحد الهواتف عبر ال«واتس آب»، ومن ثم قام بإرسال رسائل إلى جميع الأقارب والأصدقاء له على الهاتف يطلب المساعدة في «شراء منتجات ببطاقته.. بسبب توقف بطاقته عن العمل» ليفاجأ من يسقط في الفخ ويعطي له رقم البطاقة بسلب رصيده بالكامل.. ومن ثم استوعب أنه سقط في فخ «المحتالين» وضياع أمواله.

الصورة

الخليج» استطلعت آراء البنوك ـ التي رفض أغلبها التعليق على الموضوع أو تقديم شرح مفصل حول ما تقوم به من» أجل حماية العملاء ـ لكننا حرصنا على أن نقوم باستقصاء ما تقوم به البنوك من أجل توعية المتعاملين عبر الموقع .الإلكتروني لكل بنك

الصورة

رد البنوك •

وأوضحت المصارف التي استجابت ل«الخليج» بتأكد أهمية الحملات التوعوية للعملاء، وعدم الانصياع وراء الاستثمارات الوهمية والإدلاء بالبيانات المصرفية عبر الهاتف وعدم استخدام البطاقات في المواقع الإلكترونية المشبوهة وغير الموثوقة في الشراء والدفع، وعروض التخفيضات الوهمية عبر مواقع التواصل الاجتماعي، وتأكيدهم على أهمية قراءة الرسائل النصية المرسلة من قبل المصرف أو البنك بعناية قبل القيام بأي عمليات شرائية وخصوصاً .(OTP) الرسائل التي تحتوي على رمز المرور لمرة واحدة

وأكد عدد من البنوك أنه يمكن إلغاء العملية الاحتيالية في حال قيام العميل بالإبلاغ بالسرعة المناسبة. وتبرز من هذا المنطلق أهمية قيام العملاء بالتحقق من كشوف الحسابات المصرفية وكشوف بطاقات الائتمان بشكل منتظم، والتأكد من استلام التنبيهات عبر الرسائل النصية أو البريد الإلكتروني حول معاملات بطاقاتهم أو حساباتهم. وفي حال ملاحظة .أي نشاط مشبوه، يجب على العملاء إبلاغ البنك على الفور، وإيقاف الحساب لمنع أي إنفاق أو تحويلات إضافية

ورغم تأكيد عدد من البنوك أنه يمكن إلغاء العملية الاحتيالية في حال قيام العميل بالإبلاغ بالسرعة المناسبة، لكن هذا لم «.يحدث الحالة في الأولى التي تم «سحب المبلغ بعد تجميده لمدة 5 أيام

الصورة

«أبوظبي الإسلامي» •

قال مصرف أبوظبي الإسلامي، نحرص على إطلاق حملات توعوية لحماية المتعاملين من أي عملية نصب أو احتيال، ويشير إلى أن أكثر الحالات انتشاراً لمحاولات الاحتيال التي من الممكن أن يتعرض لها المتعاملون هي؛ انتحال شخصية في المصرف، والاستثمارات الوهمية، والإدلاء بالبيانات المصرفية عبر الهاتف، واستخدام البطاقات في المواقع الإلكترونية، المشبوهة وغير الموثوقة، لغرض الشراء والدفع، إلى جانب عروض التخفيضات الوهمية عبر .وسائل التواصل الاجتماعي

:وعليه، ينصح المصرف جمهور المتعاملين باتباع الخطوات أدناه لضمان الحماية القصوى لبياناتهم المصرفية

- عدم الإفصاح عن أي من البيانات المصرفية، مثل كلمات المرور وغيرها، إذ إن موظفي المصرف لن يقوموا بطلب مثل هذه المعلومات عبر الهاتف.
- مراجعة دائمة لكشوف حسابات بطاقاتكم المصرفية (سواءً البطاقات المغطاة أو بطاقات السحب المباشر) بغرض الكشف عن أي حركة مشبوهة على الحساب.
- قراءة الرسائل النصية المرسلة من قبل المصرف بعناية قبل القيام بأي عمليات شرائية وخصوصاً الرسائل التي تحتوي على رمز المرور لمرة واحدة (OTP).
- التيقظ والانتباه دائماً ومراقبة كشوف الحسابات، وفي حال تبين لكم أي تعامل غير موثوق في حساباتكم، يرجى الاتصال بنا في الحال سواء من داخل أو من خارج الدولة.

كما يؤكد مصرف أبوظبي الإسلامي أنه يولي اهتماماً كبيراً لموضوع ضمان سرية المعلومات الخاصة بالمتعاملين. ونسعى لكي نواصل جهود التوعية لدى الجمهور لتعزيز مستوى حماية معلومات متعاملينا ومكافحة سوء استخدام البيانات الخاصة بهم.

ويستخدم مصرف أبوظبي الإسلامي أحدث التقنيات لحماية بيانات المتعاملين، كما يعمل على تقييم وتطوير وتطبيق إجراءات أمنية مصرفية متطورة بصورة مستمرة بالإضافة إلى حملات التوعية المستمرة.

- **الهندسة الاجتماعية**

ومن الأسباب الشائعة التي تؤدي إلى تسرب البيانات لدى المتعاملين، هي عمليات الهندسة الاجتماعية، مجموعة من الحيل والتقنيات المستخدمة لخداع الناس وجعلهم يقومون بعمل ما أو يفصحون عن معلومات سرية وشخصية، التي تستهدف معلومات المتعاملين على حساباتهم الخاصة، مثل حساب البريد الإلكتروني الخاص بهم.

ويشير المصرف أيضاً إلى ضرورة عدم مشاركة المتعاملين لمعلوماتهم الخاصة على حسابات التواصل الاجتماعي، حيث يمكن أن يتم استخدام مثل هذه المعلومات لنيل ثقة المتعامل والاحتيال عليه عن طريق عمليات النصب الهاتفي. وتتم عمليات الاحتيال بطرق عديدة عند انتحال الشخصية، ومنها استخدام الصور التعريفية المزورة أو إقناع المتعاملين أنهم يمثلون المصرف، ويعمل المحتالون على تطوير أساليب الاحتيال بشكل مستمر.

وأوضح مصرف أبوظبي الإسلامي: نواصل تكثيف جهودنا التوعوية في مصرف أبوظبي الإسلامي ونحرص على التعاون والتنسيق المستمر مع شركائنا الإستراتيجيين في القطاع الأمني ومختلف الجهات المعنية التي تبذل جهوداً حثيثة لمكافحة هذه الجرائم، وتنبيه المتعاملين إلى ضرورة إبلاغ المصرف والجهات الأمنية في حال التعرض لأي عملية احتيال بشكل فوري. كما يمكن للجمهور الاطلاع على مختلف البرامج والنشرات التوعوية على منصات مصرف أبوظبي الإسلامي للتواصل الاجتماعي.

- **أبوظبي الأول**

وقال نافين غويال، رئيس قسم مخاطر الاحتيال والتحقيقات بالإنابة، في بنك أبوظبي الأول: «يعتمد نجاح برامج مكافحة الاحتيال بشكل رئيسي على عنصري الوقاية وتعزيز الوعي العام؛ ومن هذا المنطلق، يفخر بنك أبوظبي الأول باعتماده على أفضل أنظمة مكافحة الاحتيال التي تشمل بشكل رئيسي حلولاً متخصصة لحماية بيانات العملاء. أما بالنسبة لاستعادة الأموال المسروقة، فإننا على تعاون وثيق ومستمر مع الهيئات المختصة لاتخاذ القرارات المناسبة وفقاً لكل

.«حالة

وعن الإجراءات التي يتبعها بنك أبوظبي الأول لحماية العملاء من الاحتيال، يعتمد بنك أبوظبي الأول على أفضل أنظمة الأمن لحماية حسابات وبطاقات العملاء من الاحتيال، ويحرص باستمرار على الاستثمار في الإجراءات الجديدة التي تواكب تطور أساليب المحتالين، بما في ذلك إضافة خصائص جديدة ومفيدة لمنصات الخدمات المصرفية، لمساعدة العملاء على حماية معلوماتهم وبياناتهم. كما يعزز البنك استثماراته في الأنظمة الداخلية لمكافحة الاحتيال، للتحذير .الفوري من أي أنشطة أو معاملات مشبوهة، وبالتالي اتخاذ الإجراءات الضرورية لحماية العملاء

وتعتبر خصائص الحماية المعروفة مثل كلمة المرور لمرة واحدة أو الرقم التعريفي الشخصي لمرة واحدة عناصر هامة للحماية عند الشراء عبر الإنترنت والحد من مخاطر الاحتيال على البطاقات المصرفية، وذلك عند استخدامها بالشكل المناسب وعدم مشاركتها مع أي شخص. وتتضمن كلمات المرور لمرة واحدة الصادرة عن بنك أبوظبي الأول حالياً معلومات إضافية للتاجر، وقيمة المعاملة، الأمر الذي يعزز مستوى حماية العملاء من الاحتيال. وبالنسبة للتحويلات المالية عبر الإنترنت أو الخدمات المصرفية عبر الأجهزة المتحركة، يظهر اسم المستفيد فور إدخال رقم الحساب مما يزيد من مستوى الحماية ضد المحتالين، ويضمن للعميل إرسال المبلغ بأمان إلى (IBAN) المصرفي الدولي .الشخص المعني

• مفتاح الأمان الرقمي

من أحدث الابتكارات التي اعتمدها بنك أبوظبي الأول في تطبيق الخدمات (DSK) ويعتبر مفتاح الأمان الرقمي المصرفية عبر الهاتف المتحرك، والذي يتضمن فحصاً شاملاً للتحقق من هوية المستخدم، بما في ذلك التحقق الرقمي من الهوية الإماراتية، باستخدام كاميرا الجهاز. وأصبحت هذه العناصر إلزامية لتسجيل جهاز جديد لخدمات بنك أبوظبي الأول المصرفية عبر الهاتف المتحرك، الأمر الذي أثمر عن انخفاض كبير في عمليات الاحتيال. كما أضاف البنك مجموعة جديدة من ضوابط التسجيل في الخدمات المصرفية عبر الإنترنت، لضمان الحماية التامة من الوصول .إلى حسابات العملاء

وعن توعية العملاء بأهمية حماية معلوماتهم وحساباتهم قال البنك، يكمن الخطر الأكبر في قيام العملاء بمساعدة المحتالين عبر الإنترنت بأنفسهم، ومن دون قصد، في تخطي الحواجز الأمنية للبنك. ويحاول معظم المحتالين خداع ضحاياهم بطرق عدة للحصول على معلومات خاصة مثل تفاصيل البطاقة أو معلومات تسجيل الدخول أو كلمة المرور أو إقناع العملاء بشكل أو بآخر بأن معاملة الدفع التي يقومون بها (CCV) لمرة واحدة أو رمز التحقق من البطاقة تحت أي (CCV) أو رمز التحقق من البطاقة (OTP) شرعية وموثوق، ويجب عدم مشاركة كلمة المرور لمرة واحدة .ظرف ومع أي شخص

• عدم تجاهل التنبيهات

ونود التأكيد على أهمية عدم تجاهل العملاء لتنبيهات مكافحة الاحتيال الصادرة عن بنوكهم؛ حيث يستخدم المحتالون طرقاً جديداً لسرقة الأموال، ومن الضروري أن يكون العملاء على دراية بهذه الأساليب التي تتغير وتتطور باستمرار. ويتسم بعض هذه الأساليب بدرجة عالية من الذكاء، كما هو الحال في عمليات الاحتيال التي تطلب من العميل الدفع المسبق للرسوم عبر إرسال رسالة نصية للعميل حول شحنة بانتظاره، يتوجب عليه دفع مبلغ لاستلامها. وفي حال كان

العميل بانتظار شحنة بالفعل، فقد يظن بأن الرسالة حقيقية، ويباشر بالدفع. كما انتشرت مؤخراً حالات الاحتيال بادعاء صفة المطاعم أو منصات توصيل الأطعمة، التي تدفع العملاء إلى طلب وجبة عبر موقع وهمي. ويمكن اتباع هذه الطريقة الاحتيالية على أي نوع من عمليات الشراء عبر الإنترنت. وفي كثير من الحالات، يظن العميل أن الخطأ من التاجر، دون أن يدرك وقوعه ضحية لعملية احتيال.

• استعادة الأموال المسروقة

نجح بنك أبوظبي الأول خلال عام 2022 في حماية 35 مليون درهم من أموال العملاء، بفضل سرعة إبلاغهم عن عمليات الاحتيال، والاستجابة الفورية لموظفينا وأنظمتنا الداخلية لمكافحة الاحتيال التي ترسل تنبيهات تساعد الموظفين المعنيين في اتخاذ الإجراءات اللازمة لتقليل الخسائر، أو منعها كلياً.

يحرص بنك أبوظبي الأول على التعاون والتنسيق الوثيقين مع الهيئات والجهات القانونية المختصة في التحقيق بعمليات الاحتيال والوقاية منها. ويعد كل من مصرف الإمارات العربية المتحدة المركزي وأعضاء منتدى مكافحة الاحتيال وشركات الاتصالات من أبرز الجهات التي يتواصل معها البنك لحل قضايا الاحتيال أو طلب معلومات حول مخاوف أو شكوك متعلقة بالاحتيال.

وفي حال ملاحظة أي نشاط مشبوه، يجب على العملاء إبلاغ البنك على الفور، وإيقاف الحساب لمنع أي إنفاق أو تحويلات إضافية. ويتيح تطبيق بنك أبوظبي الأول للخدمات المصرفية عبر الهاتف المتحرك للعملاء إمكانية الحظر الفوري المؤقت للبطاقات أثناء تواصلهم مع البنك. كما يجب عليهم إبلاغ السلطات المختصة بهذا الشأن أيضاً.

• بنك الإمارات دبي الوطني

تركز مجموعة بنك الإمارات دبي الوطني في هذا العصر الرقمي على تقديم الخدمات والحماية للعملاء.. تضمن إجراءات الأمن وقواعد السلوك الخاصة بنا أقصى درجات السرية في كافة الأوقات بشأن المعلومات التي ائتمنتنا عليها؛ مع ذلك فإنك تلعب دوراً مهماً في الحفاظ على المعلومات الخاصة بك في أمان.

ويطالب البنك العملاء دائماً بالحذر من رسائل البريد الإلكتروني غير المرغوبة، وتأكّد من أن المصدر موثوق قبل فتح الرابط أو البريد الإلكتروني، وعدم الإفصاح عن المعلومات الشخصية لأي شخص عبر الهاتف، سارداً عبر موقعه الإلكتروني نحو 10 أساليب يستخدمها المحتالون في الوقوع بضحاياهم.

• بنك دبي الإسلامي

ينصح بنك دبي الإسلامي، عبر موقعه الإلكتروني، بعدم الرد على أي رسالة بريد إلكتروني تطلب من تزويد طرف ببياناتك المصرفية الشخصية. أي طلب من هذا القبيل يعد رسالة بغرض التصيد والنصب تهدف لسرقة البيانات الحساسة كرمز تعريف الهوية الشخصية واسم المستخدم وكلمات المرور منك، حيث إن البنك لن يقوم أبداً بطلب تزويده بأي بيانات شخصية عبر البريد الإلكتروني، موضحاً أنه في حالة ضياع/ فقدان / سرقة بطاقتك، اطلب من البنك على الفور أن يقوم بإيقاف البطاقة.

وفي حال ملاحظة أي معاملة (معاملات) مشبوهة / غير مصرح بها / احتيال في حساباتك أو على بطاقاتك، فيرجى إبلاغ

.البنك بالتفاصيل على الفور

وأكد أيضاً أهمية عدم الرد على أي بريد الكتروني يطلب منك تزويد بياناتك المصرفية مثل رقم الحساب ورقم بطاقة الائتمان وكلمة المرور وتعريف الهوية الشخصية، وتجنب استخدام كلمات مرور بسيطة أو أرقام مرتبطة بالتواريخ الشخصية حيث يمكن تخمينها بسهولة من قبل المتسللين، وعدم مشاركة كلمة المرور أو رقم التعريف الشخصي .الخاص بك مع أي شخص أو تتركها مكتوبة في أي مكان (PIN)

- **بنك المشرق**

أكد بنك المشرق أنه تم ملاحظة ارتفاعاً في عدد رسائل الاحتيال التي تدّعي أنها مرسلة من مؤسسات مالية مرموقة، بما فيها بنك المشرق، وأوضح لعملائه، بأنه عادة ما تدّعي رسائل الاحتيال أن الدخول إلى حسابكم محجوب، أو أن رصيداً خاطئاً قد تم إدخاله في حسابكم، أو أنكم تحتاجون لإعادة تفعيل حسابكم، ثم يطلبون منكم تسجيل الدخول في حسابكم .المصرفي عبر الإنترنت لتأكيد تفاصيلكم

وأوضح عبر الموقع الإلكتروني للبنك، أنه لن يتصل بكم بنك المشرق أبداً ليطلب معلوماتكم الشخصية كمعلومات الحساب أو كلمة السر أو ما شابه ذلك في أي وقت من الأوقات، هذه المعلومات مطلوبة فقط من أجل عملية تسجيل الدخول الاعتيادية في الخدمات المصرفية عبر الإنترنت. يرجى عدم الرد أو عدم مشاركة أي معلومات شخصية بالنقر .على أي من الروابط الموجودة في هكذا رسائل إلكترونية

وطالب البنك من عملائه، في حال استلام رسالة إلكترونية تطلب منكم تفاصيل الأمن المصرفي الخاصة بكم عبر الرمز السري للتحويل أو كلمة السر أو رقم الحساب، نرجو عدم الرد على /(PIN) الإنترنت كرقم التعريف الشخصي .تلك الرسالة وعدم النقر على أي رابط فيها.نرجو عدم الرد على تلك الرسالة وعدم النقر على أي رابط فيها

- **أبوظبي التجاري**

أوضح بنك أبوظبي التجاري، عبر موقعه الإلكتروني، بأهمية عدم الإفصاح عن رقم تعريفك الشخصي إلى أي شخص كان، سواء كان من أفراد العائلة أو موظفاً في البنك، وعدم قبول المساعدة من الغرباء عند أجهزة الصرّاف الآلي، ونصح البنك عملاءه بعدم استعمال أرقاماً مثل تاريخ ميلادك أو الأرقام الأربعة الأخيرة من رقم هاتفك، حيث يكون من .السهل على المحتال الوصول إليها

وأكد البنك أهمية أبلغ مركز الاتصال في فوراً بأي عدم انتظام في البيانات المالية، أو التعرض لأي انتهاك للخصوصية .أو أي مشاكل أمنية

أساليب للاحتيال 7

1. **انتحال الشخصية:** هو استخدام المعلومات الشخصية لشخص آخر، حيث يتم استخدام بيانات الهوية المسروقة بشكل غير قانوني لشراء السلع أو الخدمات عن طريق الخداع. غالباً ما تكون معظم عمليات انتحال الشخصية مرتبطة بالمعلومات المالية أو المصرفية، مثل الوصول إلى بطاقة ائتمان الضحية، أو حسابه المصرفي أو قروضه، أو فتح حساب بطاقة ائتمان جديد باسم الضحية، ثم تحميل ثمن المشتريات على ذلك الحساب، أو

.الحصول على قرض باسم الضحية

2. **رسائل البريد الإلكتروني:** يحاول المحتالون إخافتك من خلال إرسال رسائل عبر البريد الإلكتروني أو عبر الرسائل النصية القصيرة SMS الخاصة بالائتمان أو الخصم أو بطاقة حسابك أو حظر تجميد أو تم :فيها يذكرون وسيذكرون فيها مثل: لقد ربحت سيارة، لقد ربحت جائزة نقدية، لقد فزت برحلة، وسيتم إقناعك في هذه الحالة بضرورة مشاركة معلومات حسابك المصرفي ومعطيات بطاقتك السرية من أجل أن تحصل على جائزتك.

3. **ربح الجوائز:** سيغريك المحتالون بفكرة أنك قد ربحت مبالغ مالية من خلال التواصل معك عبر البريد الإلكتروني أو عبر الهاتف أو عبر الرسائل النصية القصيرة SMS.

4. **تشتيت انتباهك عند جهاز الصراف:** سيحاول المحتالون من خلال طريقة الاحتيال هذه للحصول على أموالك وذلك عن طريق، محاولة تشتيت انتباهك من أجل إلقاء نظرة على تفاصيل بطاقتك أو لمعرفة رقم التعريف الشخصي PIN الخاصة بك عند إدخال أي PIN لذلك عليك تغطية لوحة إدخال رقم التعريف الشخصي PIN.

5. **البديلة:** سيحاول المحتالون خداعك عن طريق، انتحال شخصيتك للحصول **(SIM) شريحة الهاتف المتحرك** بديلة من مزود خدمة الاتصالات الخاص بك، واستخدام شريحة الهاتف SIM على شريحة هاتف متحرك البديلة المستبدلة من أجل إعادة ضبط اسم المستخدم وكلمة المرور الخاصة بالخدمات SIM المتحرك بديلة، فقم SIM المصرفية، فإذا أكد مزود الخدمة الخاص بك بأنه قد تمّ بالفعل إصدار شريحة هاتف متحرك بتسجيل شكوى بهذا الخصوص وتحقق من حسابك المصرفي على الفور.

6. **خصوصية البيانات:** يستخدم المحتالون كل خدعة ممكنة، من أجل أن تقوم بمشاركة المعلومات المالية الخاصة بك معهم عبر البريد الإلكتروني أو عبر المكالمات الهاتفية أو من خلال وسائل التواصل الاجتماعي، أو أن يرسلوا لك روابط إلكترونية خبيثة، ومطالبتك بتنزيل تطبيق معيّن على هاتفك المتحرك، لسرقة بياناتك دون علمك، وسيتم بعدها استخدام معلوماتك بشكل سيئ من أجل انتحال هويتك والحصول بالتالي على منتجات أو تسهيلات مالية.

7. **الاتصال الهاتفي:** سوف يتصل بك المحتالون، منتحلين هوية ممثلين عن هيئات أو مؤسسات حكومية أو بنوك وما شابهها، وللتأكيد على هويتهم ولكسب ثقتك سيقومون بذكر بعض معلوماتك المتاحة بالفعل على منصات التواصل الاجتماعي، سيحاولون ترك انطباع لديك بأن الأمر عاجل ثم الإلحاح بأنه قد فاتتك الموعد النهائي ويجب عليك القيام بإجراء فوري، ويجب عدم مشاركة أي معلومات سرية مثل اسم المستخدم أو كلمة المرور، المكون من ثلاثة أرقام، أو كلمة المرور الصالحة لمرة واحدة CVV أو رقم ال PIN أو رقم التعريف الشخصي OTP مع أي شخص عبر الهاتف أو غير أي وسيلة تواصل أخرى.