إضاءات

نشرة توعوية يصدرها
معهد الدراسات المصرفية

عمليات الاحتيال الإلكتروني

Fraud and Scams

السلسلة 15 | العدد 3 | دولة الكويت | يناير - 2023

1. مقدمة

بسبب التقدم المتسارع في التكنولوجيا الحديثة وسهولة التعامل معها، أصبحت المعاملات الإلكترونية بمختلف أنواعها جزء أصيل من حياتنا اليومية، حيث دخلت الكثير من المعاملات الإلكترونية في أغلب التخصصات والمجالات، وقد ساهم ذلك بشكل كبير في انتشار الهواتف الذكية وتوفر خدمات الانترنت على نطاق واسع. وبالتالي أصبحت المعاملات الإلكترونية بكافة مميزاتها ضرورة من ضرورات الحياة التي لا يستغني عنها البشر في حياتهم اليومية، ولا شك أن إنجاز الكثير من المهام اليومية أصبح أكثر سهولة وكفاءة. ولكن لا يوجد شيء له مميزات إلا وفيه بعض العيوب التي يجب التنبيه عليها والحذر منها لتفادي حدوث الأضرار المترتبة عليها التي تضر بالأفراد والمؤسسات والدول في بعض الأحيان. ومن أهم هذه العيوب ما يسمى بالاحتيال الإلكتروني، الذي عادة ما يكون في أشكال كثيرة وبطرق متعددة، يأتي في مقدمتها المعاملات المالية بشتى أنواعها والمعاملات المصرفية على وجه الخصوص. في هذه الإضاءة نقوم بتسليط الضوء على أنواع الاحتيال الإلكتروني والمخاطر المترتبة عليه، كما نتعرض لكيفية التحوط وتفادي الوقوع في عمليات الاحتيال الإلكتروني، والجهود المبذولة في دولة الكويت لتوعية الجمهور ضد هذه الممارسات الضارة بالأفراد والمجتمع ككل.

2. ما هو الاحتيال الإلكتروني؟

توجد تصورات كثيرة متقاربة عن طبيعة الاحتيال الإلكتروني توضح شكل الجرائم الإلكترونية بصور متعددة، منها على سبيل المثال: أن الاحتيال الإلكتروني «هو عبارة عن جميع أشكال السلوك غير المشروع التي تتم عبر الوسائل الإلكترونية بغرض تحقيق ربح»، وقد عرفته منظمة التعاون الاقتصادي والتنمية التابعة للأمم المتحدة بأنه: « كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنيات الإلكترونية»، كما تم تعريفه في القانون القطري في المادة الأولي من قانون الجرائم الإلكترونية أنه «أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية بطريقة غير مشروعة، بما يخالف أحكام القانون» . وبالتالي يمكن القول أن الاحتيال الإلكتروني يأخذ أشكالاً كثيرة -قد لا يمكن حصرها-حيث يرتبط وجود عمليات الاحتيال الإلكتروني بوجود التقنيات الإلكترونية التي أصبحت جزء رئيسي في حياتنا اليومية، وهو ما يجعل عمليات الاحتيال سهلة الحدوث في حالة عدم التصدي المستمر لها والتوعية ضدها.

3. أنواع الاحتيال الإلكتروني

تختلف أنواع الاحتيال الالكتروني بحسب الغرض من الاحتيال، فقد يكون الغرض من الاحتيال هو سرقة حسابات شخصية أو حسابات مؤسسات سواء للحصول على هوية المستخدم أو للحصول على معلومات سرية أو سرقة أموال، وأيضاً يختلف نوع الاحتيال بحسب الطريقة المستخدمة، فقد يكون الاحتيال عبر الانترنت أو عبر الرسائل النصية الإلكترونية. وفيما يلي أهم أنواع الاحتيال الالكتروني.

أولاً: الاحتيال عن طريق التسوق أونلاين

لا شك أن أزمة كوفيد-19 أدت بشكل ملحوظ إلى زيادة انتشار التسوق الإلكتروني بكافة أنواعه، وبالتالي شهد التسوق عبر الأونلاين تسهيلات غير مسبوقة، مما جعل العديد من المحتالين لابتكار طرق مختلفة لمحاولة خداع العملاء، منها:

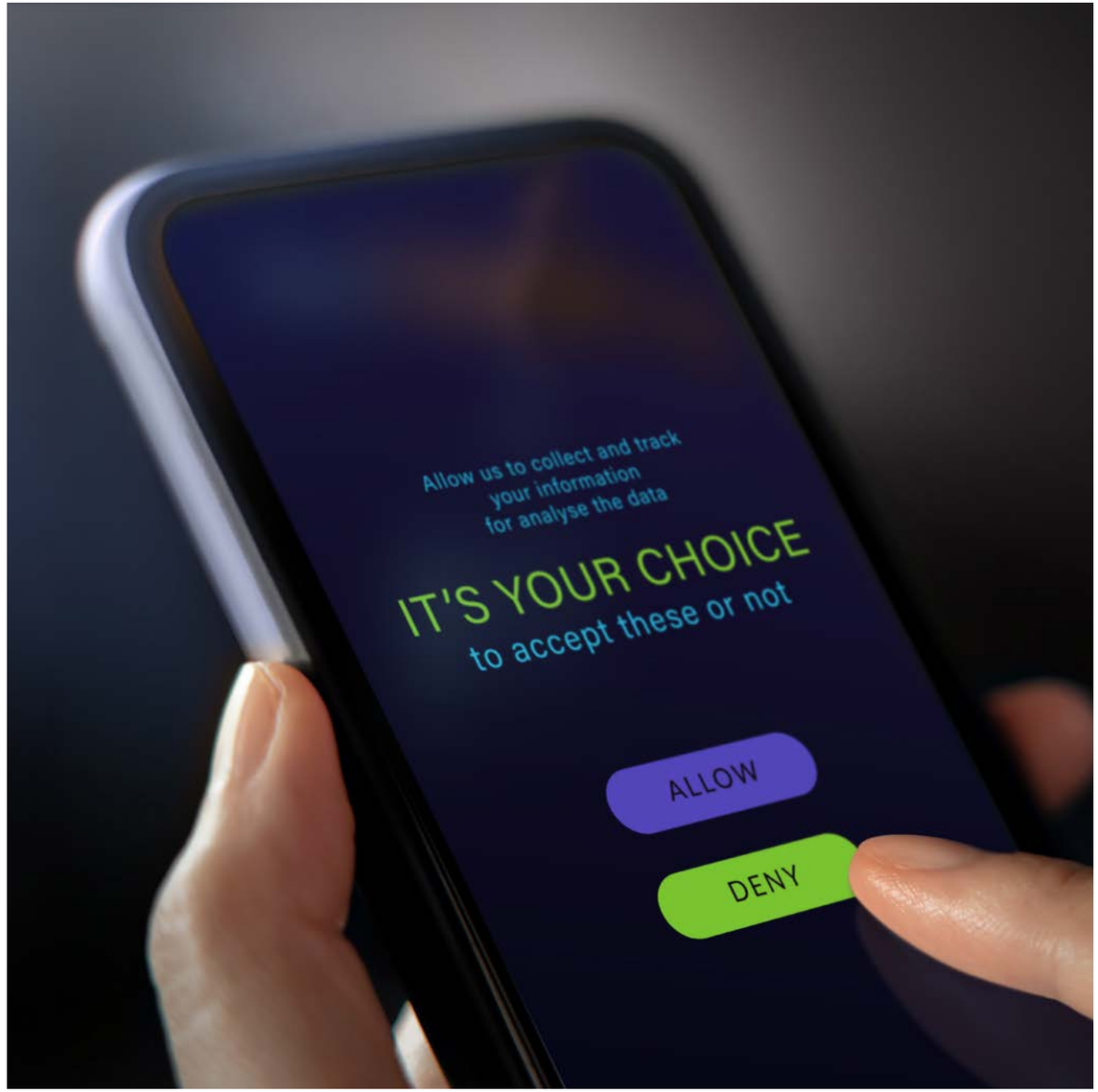
- المواقع الإلكترونية المزيفة: حيث يقوم المحتال بإنشاء موقع إلكتروني مزيف يحاكي فيه منصات التسوق المشهورة، بغرض الحصول على معلومات الحساب المصرفي، والتي تُمكنه بعد ذلك من الاستيلاء على أموال العميل بموجب البيانات التي حصل عليها منه.
- الإعلانات الوهمية: حيث يتم نشر الإعلانات الوهمية التي قد تشمل على سبيل المثال تأجير العقارات أو السيارات أو شراء منتجات على أنها أصلية، وفي الأغلب يكون الثمن المعروض قليل ومُغري بحيث يبادر الضحية بدفع المبلغ كله أو جزء منه كمقدم، ثم يكتشف بعد ذلك بعملية النصب والاحتيال عندما لا يصل إليه شيء مما طلبه أو سعي لتأجيره، أو يصل إليه المنتج ولكن بجودة أقل بكثير من المعروض.

ثانياً: الاحتيال عن طريق الرسائل الإلكترونية

- وهي طريقة من طرق الاحتيال يتم من خلالها إرسال رسائل وهمية ومضللة يُطلب من خلالها أن يقوم العميل بالإفصاح عن رقم الحساب المصرفي أو رقم بطاقة الائتمان، ومن ثمَ يتم استخدام هذه البيانات في سرقة هوية المستخدم أو سرقة معلومات سرية أو أموال، وفي بعض الأحيان يستخدم رصيد الضحية في عمليات شراء أونلاين عن طريق حسابه.
- يقوم أحد المحتالين بالتواصل عبر الرسائل الإلكترونية أو الاتصال المباشر للإعلان عن جوائز وهمية أو الدخول في سحب على هدايا، ويخبر الضحية بأنه قد تم اختيار بريدهم الالكتروني أو رقم الهاتف الخاص للفوز بجائزة كبرى أو بمبلغ مالي كبير، ويتعامل المحتال على أنه مندوب لأحد البنوك أو الشركات المعروفة حتى يقنع الضحية بدفع قيمة شحنها لمكان إقامتهم أو دفع رسوم تحويل المبلغ المالي عبر الحساب البنكي لاستلام الجائزة، ثم يختفي المحتال بالمبالغ المالية أو المعلومات الشخصية أو المصرفية التي أخذها من الضحية.

ثالثاً: الاحتيال عن طريق التداول المالي

- يقوم بعض الأشخاص بالاتصال عن طريق الهاتف أو الرسائل النصية، وغالباً ما يتحدثون باسم شركات تداول مالية وهمية أو حقيقية، ويعدون الضحية المحتملة بالربح السريع في حالة التداول عن طريقهم في بيع وشراء أوراق مالية أو في سوق العملات الرقمية أو سوق الفوركس، وغالباً ما يطلبون منه أن يخوض التجربة بمبلغ صغير في البداية بإشراف أحد الخبراء المجهولين، وقد يحصل الضحية على بعض المكاسب في البداية، ليتم إغرائه بالاستمرار في التداول، ولكن يطلب المحتال منه في مراحل لاحقة أن يتداول بمبالغ أكبر ترغيباً في تضاعف الأرباح، ثم يكتشف الضحية حدوث خسائر متتالية.



4. مخاطر الاحتيال الإلكتروني

لا شك أن الاحتيال الالكتروني يشكل تهديداً كبيراً على مستوى الأفراد والمؤسسات وخاصة المؤسسات المصرفية، ونذكر هنا أهم المخاطر المترتبة على الاحتيال الالكتروني كما يلي:

أولاً: فيما يخص الأفراد

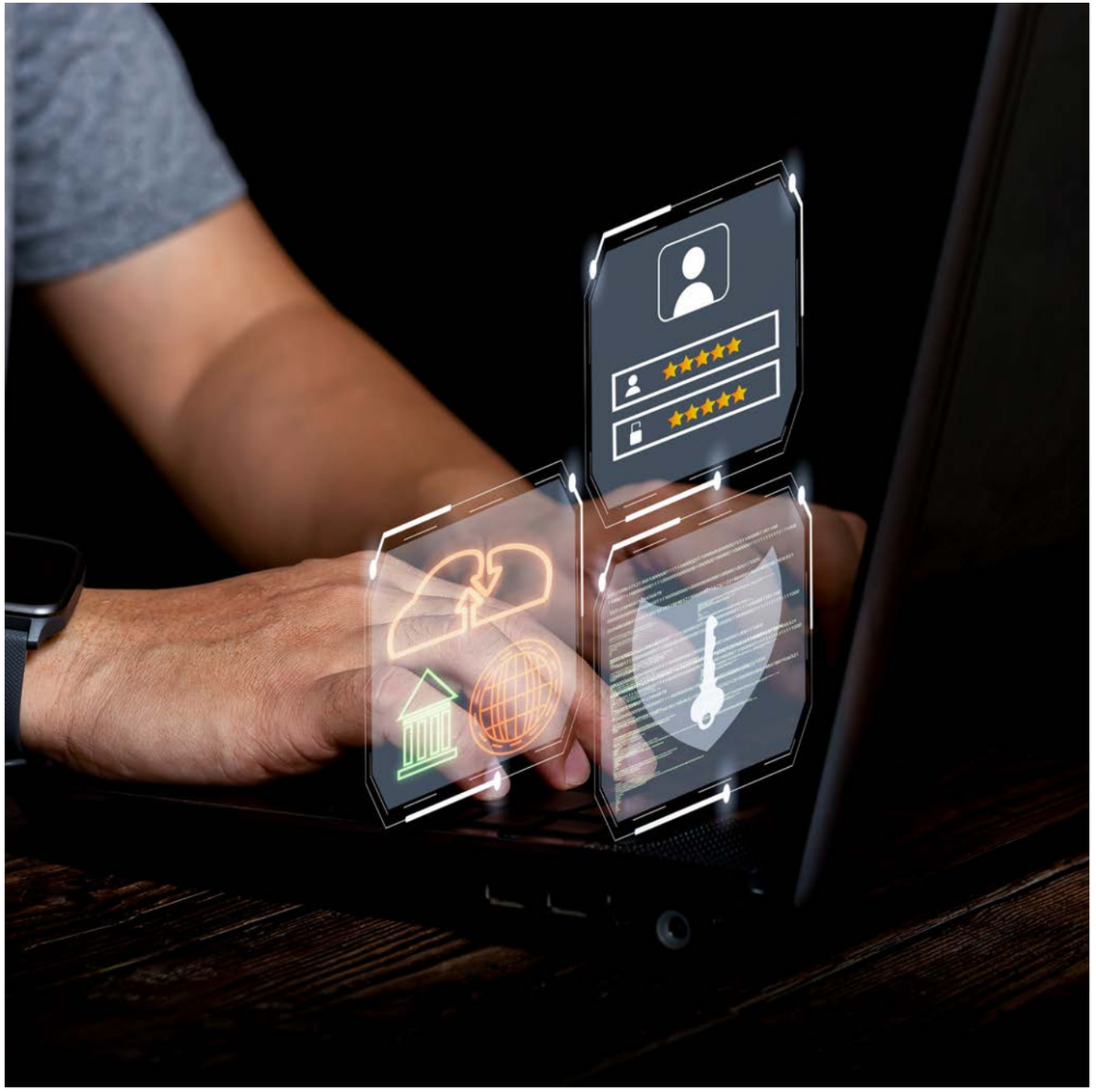
- المخاطر المتعلقة بسرقة البيانات السرية للبطاقات الالكترونية تُسهل من عمليات سرقة وتحويل الأموال من حسابات الأفراد إلى حسابات المحتالين. وفي بعض الأحيان وضع فواتير أو التزامات مالية على الضحية من قِبل الجهة المحتالة.
- يترتب على سرقة البيانات مخاطر تتعلق بالابتزاز الشخصي والتهديد لإجبار الضحية على الامتثال لأمر معين من قِبل الجهة المحتالة.

ثانياً: فيما يخص الشركات

- عمليات الاحتيال قد تشمل سرقة الأموال وتحويلها من حسابات الشركة إلى حسابات أخري خاصة خاضعة للجهات المحتالة وذلك من أجل التأثير السلبي على وضع الشركة من جوانب مختلفة، بالإضافة إلى سرقة البيانات الخاصة من أجل التهديد والابتزاز لمحاولة إجبار الشركة على اتخاذ خطوات معينة تصب في مصلحة الجهات المحتالة.

ثالثاً: فيما يخص المصارف

- وقوع مخاطر تتعلق بالسيولة والائتمان، وذلك من خلال الاستيلاء على أموال كبيرة من أرصدة المصارف بطرق احتيالية بعضها يكون في صورة قروض بضمانات يتم الاكتشاف فيما بعد أنها ضمانات وهمية.



5. إجراءات التحوط لحماية أصحاب الحسابات المصرفية من الاحتيال الإلكتروني

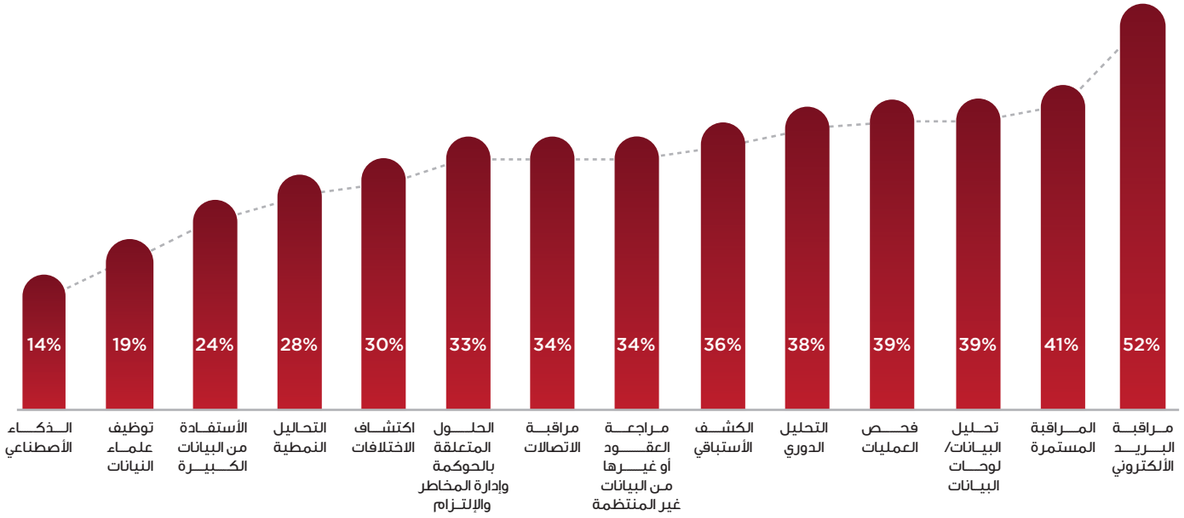
توجد الكثير من أشكال وطرق الاحتيال الالكتروني وتنتشر على نطاق واسع على وجه الخصوص في الوصول لمعلومات عن أصحاب الحسابات المصرفية، وللأسف تتجدد أشكال وأساليب الاحتيال بشكل مستمر للوصول إلى ضحايا أكثر، حيث ناقشت أحد الدراسات الصادرة عن جامعة نايف العربية للعلوم الأمنية «دور المؤسسات المالية في الحد من الجرائم المعلوماتية» ووجدت 24 أسلوبًا إجرامياً يتم استخدامه للوصول إلى ضحايا، وذلك من خلال تحليل 503 إعلاناً احتيالياً، وتوصلت الدراسة إلى أن عدد الزيارات للمواقع الاحتيالية يزيد على 137 ألف زيارة في اليوم من قِبل ضحايا محتملين، وأوضحت الدراسة أن آلية الوصول إلى الضحايا تكون من خلال أسلوب إجرامي مُركَّب صُمم لاستهداف الضحية مرتين وبطريقتين مختلفتين، في المرة الأولي يكون وقوع الضحية عن طريق الإعلانات الاحتيالية الاستثمارية، ثم في المرة الاحتيالية الثانية تكون عبر إعلانات شركات استشارات قانونية تدعي استرداد الأموال.

لذلك تقوم المؤسسات المصرفية بشكل مستمر بأخذ إجراءات تحوطية وعمل توعية ضد أساليب الاحتيال التي تتجدد بشكل مستمر ونتناول هنا أهم هذه الإجراءات التحوطية كما يلي:

- وضع استراتيجية متكاملة لمكافحة الاحتيال: حيث تقوم هذه الاستراتيجية على أساس تحليل كافة الطرق والوسائل التي تُمثل نقاط ضعف قد يتسلل من خلالها المحتالون للوصول لضحايا.
- وضع تدابير مضادة واضحة للجمهور لتفادي الوقوع في العمليات الاحتيالية.
- رفع مستوى الكفاءة بشكل مستمر لدى العاملين في القطاع المصرفي وكذلك رفع مستوى الوعي للعملاء والجمهور من خلال حملات توعوية مستمرة توضح كافة سبل الاحتيال وكيفية التصدي لها.
- التطوير المستمر في أدوات التكنولوجيا الحديثة المستخدمة في كشف عمليات الاحتيال، حيث بالفعل تتنافس المصارف في استخدام أحدث الأجهزة والتقنيات الحديثة التي تمكنها من الكشف عن عمليات الاحتيال بشكل سريع ومستمر، حيث يظهر ذلك في استبيان أعدته شركة برايس ووتر هاوس كوبرز (PWC) حول جرائم الاحتيال عام 2018 في منطقة الشرق الأوسط، حيث يشير الاستبيان إلى أن نسبة الاعتماد على التكنولوجيا الحديثة في كشف الاحتيال تصعد بشكل متسارع، وذلك من خلال تنوع الأدوات والتقنيات المختلفة التي يتم استخدامها لكشف عمليات الاحتيال كما هو موضح في الشكل (1)، كما أكد نحو 82% من المشاركين في الاستبيان من الشرق الأوسط أن المراقبة المؤتمتة المستمرة والآنية تساعدهم في مكافحة الاحتيال.

شكل (1)

استخدام التكنولوجيا للكشف عن عمليات الاحتيال



المصدر: الاستبيان العالمي لشركة برايس ووتر هاوس كوبرز حول الجرائم الاقتصادية والاحتيال في الشرق الأوسط 2018

6. أهم جهود دولة الكويت في توعية الجمهور ضد عمليات الاحتيال

- تقوم دولة الكويت بدور بارز في نشر وتوعية الجمهور ضد عمليات الاحتيال من خلال العديد من الحملات والمبادرات، ومن أبرزها:

- حملة التوعية المصرفية «لنكن على دراية»، التي أطلقها بنك الكويت المركزي بالتعاون مع اتحاد مصارف الكويت وبمشاركة البنوك الكويتية، حيث تهدف إلى نشر الثقافة المالية لدى أوسع شريحة من المجتمع، وزيادة الوعي لدى الجمهور بدور القطاع المصرفي وكيفية الاستفادة من الخدمات المتنوعة التي تقدمها البنوك على الوجه الأمثل وتفادي وتقليل محاولات الاحتيال الإلكتروني ومنها:
  - يحرص بنك الكويت المركزي والبنوك الكويتية على توعية الجمهور بكافة طرق الاحتيال، عن طريق نشر الإعلانات ومشاركة الرسائل النصية عبر قنوات التواصل المختلفة للتصدي لعمليات الاحتيال.
  - تنظيم فعاليات للمساهمة في توعية المجتمع بكافة القضايا المتعلقة بمكافحة الاحتيال والجرائم المالية.
  - التأكيد على أنه لن يُطلب من العميل أي معلومات شخصية أو معلومات تتعلق بالحساب المصرفي أو الرقم السري للبطاقات الائتمانية من خلال البريد الإلكتروني أو الرسائل النصية أو المكالمات الهاتفية.
  - تؤكد الحملة التوعوية على ضرورة عدم حفظ أي معلومات سرية متعلقة برقم التعريف الشخصي أو بطاقة الائتمان أو بطاقة السحب الآلي على الهاتف النقال، إضافة إلى عدم مشاركة الرقم السري مع أي جهة أو كتابته على البطاقة الائتمانية.
  - ضرورة تسجيل الخروج من التطبيق أو الموقع الإلكتروني للبنك فور انتهاء أي معاملة.

- قيام العديد من المصارف الكويتية بعمل مبادرات تهدف لتوعية الجمهور بالجرائم الإلكترونية، منها: قيام أحد المصارف في الكويت بالتعاون مع مؤسسة لوياك التطوعية (يونيو 2021)، لتنفيذ ورشة عمل للشباب لمدة 3 أسابيع لرفع الوعي بالجرائم الإلكترونية والاحتيال مع دعوة عدد من الخبراء والمتخصصين في الجرائم الإلكترونية.
- هناك أيضاً جهود من وزارة الداخلية من خلال إدارة مكافحة الجرائم الإلكترونية في الحد من الاحتيال الإلكتروني: حيث حرصت الوزارة على القيام بالعديد من الأنشطة والإجراءات لمحاربة أشكال الاحتيال الإلكتروني وتوعية المواطنين، من خلال:
  - القيام بتنظيم محاضرات توعوية عن الجرائم الإلكترونية لكافة الفئات العمرية في المدارس الكويتية بالتعاون مع وزارة التربية.
  - المشاركة في حملة (واعي) التي نظمتها جمعية المحامين الكويتية من أجل التوعية بخطورة الجرائم الإلكترونية وكيفية مكافحتها.
  - كما تنشر وزارة الداخلية على صفحاتها بمنصات التواصل الاجتماعي العديد من الرسائل التحذيرية والتوعوية فيما يتعلق بالجرائم الالكترونية وطرق إيقاع العملاء من قِبل المحتالين.
- كما ساهمت الهيئة العامة للاتصالات وتقنية المعلومات (CITRA) بالتوعية ضد عمليات الاحتيال الإلكتروني، حيث قامت الهيئة بنشر العديد من الرسائل التوعوية والتوصيات فيما يخص استخدام مواقع التواصل الاجتماعي والتسويق الالكتروني من خلال الموقع الرسمي للهيئة، والصفحة الرسمية على منصة تويتر. ومن أهم هذه الرسائل:
  - رسائل توعوية متنوعة عن مخاطر التواصل الاجتماعي وكيفية البقاء آمنا أثناء استخدام جميع منصات التواصل الاجتماعي.
  - كما نشرت الهيئة العديد من التوصيات في كيفية الحد من اختراق أجهزة الهاتف المحمول.
  - قامت الهيئة أيضاً بالنشر عن المحاذير اللازمة أثناء التسوق الإلكتروني وكيفية تفادي حيل مجرمي الأمن السيبراني.

- كما تنوعت جهود هيئة أسواق المال (CMA) من خلال تنسيق توعوي مع كلية الدراسات التجارية للتعليم التطبيقي والتدريب، وأيضاً من خلال مجلتها التوعوية الإلكترونية بإصدار عدة إرشادات لمكافحة عمليات الاحتيال الإلكتروني، من أهمها:
  - التحذير من الدخول في الاستثمارات مجهولة المصدر، التي تعطي وعود بالربح السريع دون توفر أي معلومات موثوقة.
  - تجاهل الاتصالات والإعلانات والرسائل النصية مجهولة المصدر، أو التي يرفض مروجها عرض التراخيص المطلوبة.
  - الاطلاع على الأداء التاريخي للجهة المروجة، وطبيعة المخاطر المرتبطة بها، والعوائد المتوقعة منها.
  - التأكيد على الاستعانة بالخبراء المختصين قانونياً ومالياً.

7. الخاتمة

لاشك أن الاحتيال الإلكتروني يعتبر أحد أكبر العقبات التي تواجه الأفراد والمؤسسات، ولكن الجدير بالذكر أن مع تزايد أساليب وطرق الاحتيال الالكتروني يرتفع الوعي بمعدل أكبر لدى الأفراد والمؤسسات للتصدي لأساليب الاحتيال والخداع الإلكتروني، حيث تعمل الحكومات والمؤسسات على محاربة كافة سبل الجرائم الإلكترونية من خلال مبادرات التوعية المستمرة ضد الاحتيال الإلكتروني، ورفع كفاءة العاملين في مختلف القطاعات من أجل العمل على إحباط خداعات المحتالين مبكراً لتقليل المخاطر الناتجة عن الخداع والاحتيال الإلكتروني، وبالتالي تحقيق أكبر استفادة من التقدم التكنولوجي والتقنيات الحديثة التي يشهدها العالم في الآونة الأخيرة.

المراجـــع

المشكلات العملية والقانونية للجرائم الإلكترونية، عبد اللّه دغش، جامعة الشرق الأوسط،2014.

تجريم الاحتيال الإلكتروني في القانون القطري، حمد عبد اللّه حي، جامعة قطر، 2018.

جرائم الاحتيال الإلكتروني/عبد الرحمن محمد قدري حسن/مجلة الفكر الشرطي/العدد 79/المجلد 20/2011.

الاحتيال عبر الإنترنت صوره – أساليبه وحكمه في الإسلام والقوانين المعاصرة، أحمد محمد عبد الرؤوف المنيفي.

دليل مكافحة الاختلاس والاحتيال المالي، صندوق النقد السعودي ص12-23.

الاستبيان العالمي لشركة برايس ووتر هاوس كوبرز حول الجرائم الاقتصادية والاحتيال في الشرق الأوسط 2018، economic-crime-fraud-survey-2018-ar.pdf (pwc.com)

الموقع الرسمي لبنك الكويت المركزي، نصائح أمنية (dirayakw.com)

الموقع الرسمي بنك الكويت الوطني.
https://www.nbk.com/ar/kuwait/news-and-insights/media-relations/news.html?news=al-matrouk--nbk-firmly-supports-the-initiatives-to-raise-the-youth-s-awareness-of-cybercrime-and-protective-measures

الأبعاد الاقتصادية للجريمة الالكترونية، صراع كريمة، دقيش جمال. مجلة الدراسات التسويقية وإدارة الأعمال، م (2) ع(1). 2018.

موقع جامعة نايف العربية للعلوم الأمنية:
https://nauss.edu.sa/ar-sa/news/Pages/2022-1-19.aspx

إدارة مكافحة الجرائم الالكترونية بوزارة الداخلية الكويتية:
Cyber Crime - Ministry of Interior - Kuwait (moi.gov.kw)

الهيئة العامة للاتصالات وتقنية المعلومات (CITRA)
https://citra.gov.kw/sites/Ar/Pages/cybersecurity.aspx

هيئة أسواق المال بالكويت:
https://fliphtml5.com/whptv/tlwq/basic

معهد الدراسات المصرفية

INSTITUTE OF BANKING STUDIES

ص.ب 1080 الصفاة – 13011 الكويت

P.O.Box 1080 Safat 13011 Kuwait | Tel.: +965 22901100 | Fax: +965 22466430

ibs_kuwait | IBSKuwait | www.kibs.edu.kw | cs@kibs.edu.kw