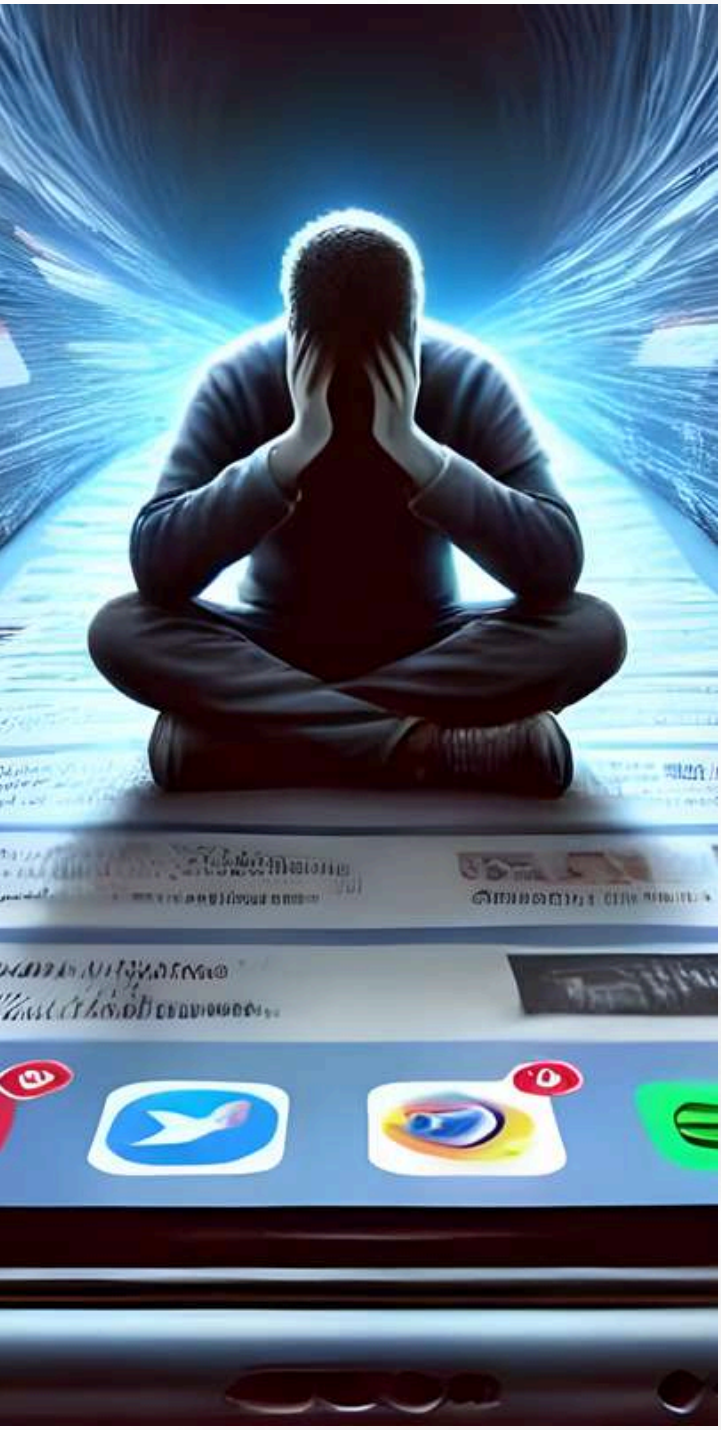
الاحتيال عبر وسائل التواصل الاجتماعي : كيف نحمي مدخراتنا؟

أ.محمد محمود البنا
أخصائي نظم ومعلومات
الإدارة العامة لنظم المعلومات والتحول الرقمي



في العصر الحديث، لم تعد وسائل التواصل الاجتماعي تقتصر على كونها منصات للترفيه أو للتواصل بين الأصدقاء، بل تحوّلت إلى فضاء رقمي متكامل يشمل مجالات متعددة مثل الأعمال، والعلاقات الاجتماعية، والتوظيف، والتسويق. فقد أصبحت منصات مثل "فيسبوك"، و"إنستغرام"، و"واتساب"، و"تيليغرام" جزءًا لا يتجزأ من الحياة اليومية، حيث تسللت إلى المنازل وبيئات العمل، وامتد تأثيرها إلى تفاصيل دقيقة لم يكن من المتصوَّر أن تبلغها قبل عقدٍ من الزمن.

لكن هذا التوسع في الاستخدام الرقمي صاحبه توسع مقلق في الأساليب الإجرامية الإلكترونية، وعلى رأسها عمليات الاحتيال عبر وسائل التواصل الاجتماعي، والتي باتت تهدد الأفراد والمؤسسات على حد سواء. فلم يعد المحتالون بحاجة إلى مهارات تقنية متقدمة، بل يعتمدون على الذكاء الاجتماعي والنفسي للتلاعب بثقة الضحايا، وسرقة أموالهم أو بياناتهم الحساسة بكل دهاء.

والمشكلة لا تقتصر على الأفراد فحسب، بل تمتد لتشمل المؤسسات أيضًا، خاصةً عندما يكون المستهدفون من الاحتيال هم الموظفون أو الشركاء أو العملاء التابعون لتلك المؤسسات.لذلك، تكتسب هذه المقالة أهميتها من تسليطها الضوء على طبيعة هذه التهديدات، وشرح أبرز أساليب الاحتيال المستخدمة، وبيان أثرها على المدخرات، إلى جانب تقديم نصائح عملية تساعد الأفراد والمؤسسات على الوقاية منها والتعامل معها بفعالية.

ما المقصود بالاحتيال الرقمي عبر وسائل التواصل؟

يُعد الاحتيال الرقمي شكلًا من أشكال الخداع المنسق، يهدف إلى دفع شخصٍ ما ، دون علم أو وعي، إلى تقديم معلومات شخصية أو مالية، أو اتخاذ قرارات تلحق به ضررًا ماديًا أو معنويًا.

وفي سياق الحديث عن وسائل التواصل الاجتماعي، فإنها تمثل بيئة رقمية مفتوحة تتيح لمختلف المستخدمين، بمن فيهم المحتالون، الوصول إلى جمهور واسع يوميًا، مما يجعلها منصة مثالية لتنفيذ هذا النوع من الجرائم الإلكترونية.

وجدير بالذكر أن ما يميز الاحتيال عبر "وسائل التواصل الاجتماعي" هو سهولة تنفيذه، وانخفاض تكلفته، وصعوبة تتبعه قانونيًا. فالمحتال قد يكون في دولة أخرى تمامًا، يستخدم هوية مزيفة، ويتواصل مع الضحية وكأنه شخص حقيقي أو جهة موثوقة.

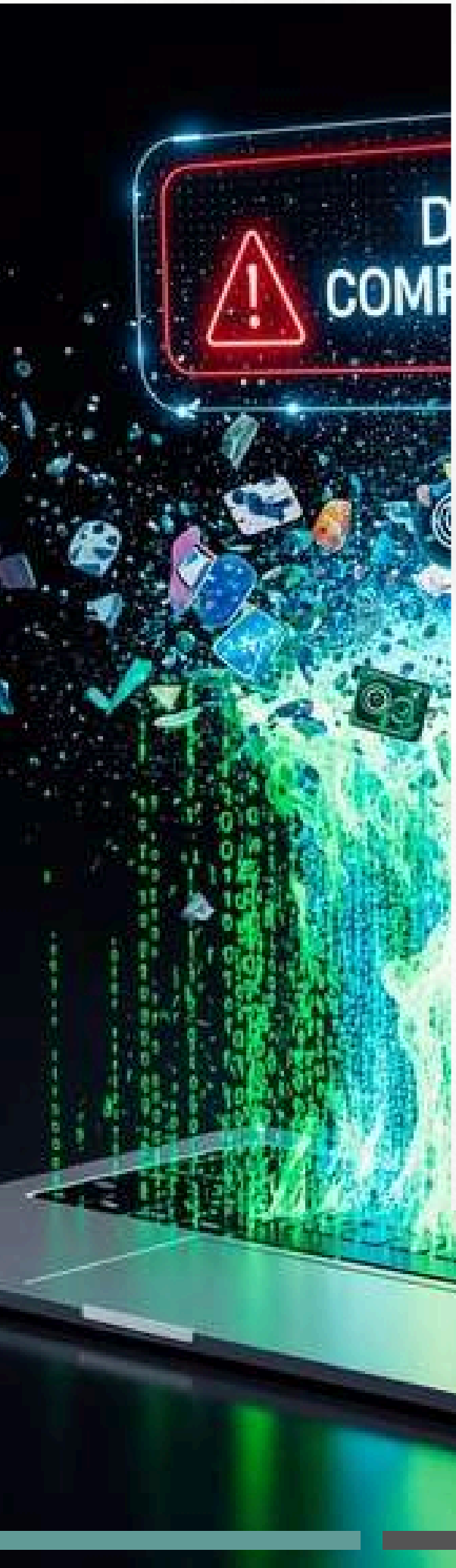
أبرز أساليب الاحتيال الشائعة حاليًا

في ظل تطور أساليب الجريمة الإلكترونية، ابتكر المحتالون طرقًا متعددة للإيقاع بالضحايا عبر الإنترنت، مستغلين ضعف كلمات المرور وسهولة الوصول إلى المعلومات الشخصية، خاصة على مواقع التواصل الاجتماعي. ومن أبرز هذه الأساليب المنتشرة حاليًا:

الصفحات المزيفة التي تنتحل صفة جهات رسمية:
حيث يقوم المحتال بإنشاء صفحة تشبه تمامًا صفحة بنك معروف أو جهة حكومية، مستخدمًا نفس الشعار ونفس أسلوب النشر؛ ثم يبدأ في إرسال رسائل للمتابعين تطلب منهم تحديث بياناتهم أو إدخال رقم الحساب وكلمة السر عبر رابط وهمي.

رسائل "خدمة العملاء" المزيفة:
في هذا النوع من الاحتيال تصل رسالة إلى المستخدم عبر تطبيق ماسنجر أو واتساب تخبره بأن هناك مشكلة في حسابه البنكي أو أنه فاز بجائزة. وقد تطلب منه مشاركة بيانات أو إدخال كود أمان تم إرساله على هاتفه.

الإعلانات الاستثمارية الوهمية:
انتشرت في الآونة الأخيرة إعلانات عن مشاريع استثمارية تدّعي أنها تابعة لشركات عالمية؛ وتعد المستخدم بعائد شهري كبير مقابل مبلغ صغير من المال. وبمجرد تحويل الأموال، تختفي الصفحة، ولا يستطيع الضحية استرجاع شيء.



عروض التوظيف المزيفة:
يقوم البعض بنشر وظائف مغرية على مجموعات الفيسبوك أو تيليجرام، مدعين أنها وظائف حكومية أو تابعة لمؤسسات كبرى. ثم يطلبون من المتقدمين إرسال صورة بطاقتهم أو تحويل مبلغ مالي رمزي "لفتح ملف التوظيف"، ثم لا يتواصلون مرة أخرى

الاحتيال العاطفي:
يقوم أحدهم بإنشاء حساب مزيف بشخصية جذابة، ويتواصل مع الضحية بشكل ودي حتى يكوّن علاقة ثقة، ثم يبدأ في طلب الأموال بحجج متعددة: مرض، حادث، حاجة للسفر... إلخ.

روابط التصيّد الاحتيالي:
يتم إرسال روابط شبيهة بمواقع معروفة، يضغط عليها المستخدم فيجد واجهة تطلب إدخال بيانات الدخول، لكنها في الواقع تسجل المعلومات وترسلها للمحتال.

بيع سلع وهمية:
تنتشر إعلانات على منصات مثل فيسبوك وإنستجرام عن سلع بسعر مغرٍ جدًا، وبعد الدفع إما لا تصل السلعة أبدًا، أو تصل بشكل مختلف تمامًا عن الإعلان.

كيف يؤثر الاحتيال الرقمي على مدخرات الأفراد؟

قد يظن البعض أن الخسائر الناتجة عن هذه العمليات بسيطة أو محدودة، لكن الواقع يثبت أن التأثير قد يكون كبيرًا جدًا، سواء من الناحية المالية أو النفسية، وأحيانًا يمتد لأبعاد قانونية أو اجتماعية. نوضح فيما يلي أبرز الآثار.

الخسارة المالية المباشرة:

أبسط شكل للخسارة هو عندما يُطلب من الضحية تحويل مبلغ مالي صغير "كرسوم إدارية" أو "فتح ملف توظيف"، ثم لا يسمع شيئًا بعدها.أما الأشكال الأخطر فهي عند استخدام بيانات الضحية لسحب أموال من حسابه البنكي، أو شراء منتجات عبر الإنترنت باستخدام بطاقته دون إذنه.

فتح حسابات وهمية باسم الضحية:

أحيانًا يتم استخدام بطاقة الرقم القومي أو بيانات الهوية الخاصة بالشخص لإنشاء حسابات على منصات دفع أو مواقع تجارية، ثم تُستخدم في عمليات مشبوهة، مما يضع الضحية في دائرة الاتهام دون أن يعلم.

استغلال البيانات لاحقًا:

حتى لو لم تحدث خسارة فورية، يمكن أن تُباع بيانات الشخص (مثل البريد الإلكتروني، رقم الهاتف، العنوان) على مواقع السوق السوداء، وتُستخدم لاحقًا في حملات احتيالية متقدمة أو للاحتيال على أشخاص آخرين من المحيط القريب للضحية.

الأثر النفسي والمهني:

الوقوع ضحية لعملية نصب يشعر الشخص بالحرج أو الإحباط أو الذنب. وقد يمتنع عن استخدام وسائل رقمية مرة أخرى. وإذا كان موظفًا - خاصة في جهة حكومية- فقد يضر ذلك بسمعة المؤسسة أو يفتح ثغرة أمنية فيها.

كيف يمكن للمؤسسات الإسهام في الحماية؟

إن مسؤولية الوقاية من الاحتيال لا تقع على الفرد فحسب؛ بل إن الجهات الحكومية والخاصة تتحمل مسؤولية كبيرة في رفع الوعيوحماية موظفيها من هذه التهديدات. ومن أهم ما يمكن أن تقوم به المؤسسات:

تعيين مسؤولين لأمن المعلومات

يجب أن تمتلك كل جهة أو مؤسسة وحدة متخصصة لمتابعة أمن المعلومات والتعامل مع الحوادث الرقمية، والاستجابة بسرعة لأي محاولة احتيال.

تحديث السياسات الأمنية:

من الضروري تحديث سياسات "الاستخدام الآمن للبريد الإلكتروني"، و"أمن البيانات"، و"التعامل مع الأطراف الخارجية"، مع إلزام الموظفين بتطبيقها بشكل واضح.

نشر التوعية الدورية:

إن كل مؤسسة يجب أن تضع ضمن أولوياتها برامج توعية إلكترونية؛ تشمل نشرات شهرية أو دورات تدريبية مبسطة، توضح أساليب الاحتيال المتجددة، وتشرح للموظف كيف يتصرف إذا واجه موقفًا مشبوهًا.

التعاون مع الجهات الرسمية:

يجب أن تبادر المؤسسة بإبلاغ الأجهزة الأمنية المختصة مثل مباحث الإنترنت أو الجهاز القومي لتنظيم الاتصالات في حالة رصد أي سلوك احتيالي؛ وذلك لتفادي تكرار الاستهداف أو توسّعه.

تعزيز ثقافة التبليغ:

ينبغي تشجيع الموظف على التبليغ الفوري دون خوف أو تردد، مع ضمان عدم تحميله المسؤولية كاملة إذا وقع ضحية لعملية احتيال رغم حسن نيته.

خطوات عملية لحماية نفسك من الاحتيال الرقمي

إن التهديدات الإلكترونية لا تعرف حدودًا؛ ولذلك فإن تعزيز الوعي بالتصرفات الآمنة على الإنترنت أصبح ضرورة لا غنى عنها. فيما يلي مجموعة من النصائح الوقائية التي يمكن أن تشكّل خط الدفاع الأول ضد محاولات الاحتيال عبر وسائل التواصل الاجتماعي:

لا تفترض حسن النية دائمًا:

في بيئة الإنترنت؛ من السهل تزييف الهويات. قد تصلك رسالة من حساب يبدو رسميًّا أو من شخص ينتحل صفة موظف في بنك أو شركة معروفة؛ لا تنخدع بالشعارات أو الصور أو اللغة المنمقة، فالمحتالون بارعون في تقليد الرسائل الرسمية وتزوير التفاصيل، لذلك ينبغي دائمًا التشكيك في أي عرض أو طلب غير متوقع.

مثال: كثيرًا ما يتلقى المستخدمون رسائل مثل "مبروك! ربحت جائزة بقيمة ١٠ آلاف جنيه"، ويُطلب منهم إرسال بياناتهم البنكية أو دفع "رسوم تحويل بسيطة". هذه رسائل احتيالية شائعة تهدف إلى سرقة الأموال أو البيانات.لا تشارك بياناتك بسهولة؛ رقمك القومي، صورتك الشخصية، عنوانك، أرقام الحسابات... كل هذه معلومات حساسة. لا تعطها لأي جهة غير موثوقة، حتى لو بدا الأمر وكأنه "إجراء روتيني".

احمِ خصوصيتك... بياناتك ليست للجميع:

من القواعد الذهبية في الأمن السيبراني أن أي جهة موثوقة لن تطلب منك أبدًا مشاركة معلومات حساسة مثل الرقم القومي، أو كلمة السر، أو رمز التحقق عبر الرسائل. إذا طُلب منك ذلك، فاعلم أنك أمام محاولة احتيال صريحة. المعلومات التي تقدمها للمحتالين يمكن أن تُستخدم في سرقة هويتك، أو فتح حسابات وهمية باسمك، أو الوصول إلى حساباتك البنكية.

وفقًا لتقرير شركة Kaspersky) 2024)، فإن أكثر من ٧٥٪ من عمليات الاحتيال عبر الإنترنت تبدأ بجمع معلومات شخصية من الضحية، مثل البريد الإلكتروني ورقم الهاتف، لتُستخدم لاحقًا في تنفيذ هجمات أكثر تعقيدًا.

احذر من الروابط المزيفة والمواقع الاحتيالية:

غالبًا ما يستخدم المحتالون روابط إلكترونية مزيفة تُشبه الروابط الرسمية، مثل إضافة نقطة أو حرف مختلف داخل عنوان الموقع الإلكتروني، وعند الضغط على هذه الروابط، يتم تحويلك إلى صفحة احتيالية تطلب منك إدخال معلوماتك.

- لا تضغط على أي رابط يصلك من جهة غير معروفة.افحص عنوان الرابط جيدًا قبل فتحه.
- استخدم إضافات المتصفح التي تحذرك من المواقع غير الآمنة (مثل McAfee WebAdvisor أو Bitdefender TrafficLight).
- أي رابط يصلك في رسالة غير متوقعة، تجاهله. وإن كنت مضطرًا لفتحه، افتحه من متصفح آمن وتأكد من أنه يبدأ بـ"https".

فعّل التحقق بخطوتين (Two-Factor Authentication):

توفر خاصية التحقق بخطوتين حماية إضافية لحساباتك. حتى لو تمكن أحدهم من سرقة كلمة المرور، فلن يستطيع الدخول إلى الحساب دون رمز التحقق الإضافي المرسل إلى هاتفك أو بريدك الإلكتروني. ينصح بتفعيل هذه الخاصية في جميع الحسابات الأساسية مثل فيسبوك، واتساب، إنستجرام، والبريد الإلكتروني.

لا تتسرع في الرد على رسائل التهديد أو العروض المغرية:
أسلوب "الضغط الزمني" هو أحد أبرز أسلحة المحتالين. مثلًا: "عرض لفترة محدودة"، أو "يجب تحويل المبلغ خلال ٣٠ دقيقة حتى لا تُلغى الجائزة". هذا النوع من الضغط هدفه دفعك لاتخاذ قرار دون تفكير لذلك، من المهم أن تمنح نفسك وقتًا كافيًا قبل القيام بأي إجراء، وأن تستشير صديقًا موثوقًا أو تتواصل مباشرة مع الجهة الرسمية عبر رقمها المعتمد.

راقب نشاطاتك الرقمية:
ينبغي عليك التحقق من سجل الدخول لحساباتك بشكل دوري، ومتابعة ظهور أي رسائل لم تقم بإرسالها بنفسك، بالإضافة إلى حذف أي تطبيقات مشبوهة من هاتفك فورًا للحفاظ على أمان بياناتك.

تابع الصفحات الرسمية فقط:
إذا كنت تتعامل مع مؤسسة مثل بنك أو شركة، تأكد أن الحساب الذي تتفاعل معه موثّق بعلامة زرقاء أو أنه مذكور في الموقع الرسمي للشركة، وتجنّب التفاعل مع الحسابات التي تحمل أسماء قريبة للحسابات الأصلية لكن مع اختلاف بسيط، لأنها قد تكون حسابات انتحالية.

احتفظ بإثباتات التراسل
إذا حدث تواصل مشبوه من أحد المستخدمين، لا تمسح المحادثة فورًا، بل احتفظ بها كمستند يمكن تقديمه عند التبليغ، وسجّل كل التفاصيل (الاسم، الرابط، وقت الرسالة....)

لا تُجري أي تحويل مالي قبل التأكد التام:
قبل القيام بأي عملية تحويل مالي، خاصةً إذا جاءك الطلب عبر وسائل التواصل الاجتماعي، توقّف وفكّر جيدًا. لا تعتمد على الرسائل أو المحادثات المكتوبة فقط، حتى لو بدا الشخص مألوفًا. فالمحتالون قد يسرقون حسابات الأصدقاء أو يقلدون أسلوبهم ببراعة.

اطلب وسيلة تواصل إضافية للتحقق، مثل مكالمة فيديو، أو التأكد من بعض التفاصيل التي لا يعرفها إلا الشخص الحقيقي. والأفضل دائمًا أن تتواصل مع الشخص عبر وسيلة مستقلة عن المحادثة الأصلية (مثل رقم هاتف موثوق أو لقاء شخصي عند الإمكان). وتذكّر: لا يوجد ما يستدعي التسرّع في إرسال أموال دون التحقق التام من هوية الطرف الآخر.

حجم الخسائر الناجمة عن الاحتيال الرقمي

تشير الإحصائيات إلى تصاعد مقلق في عمليات الاحتيال الإلكتروني، سواء عالميًا أو داخل مصر:

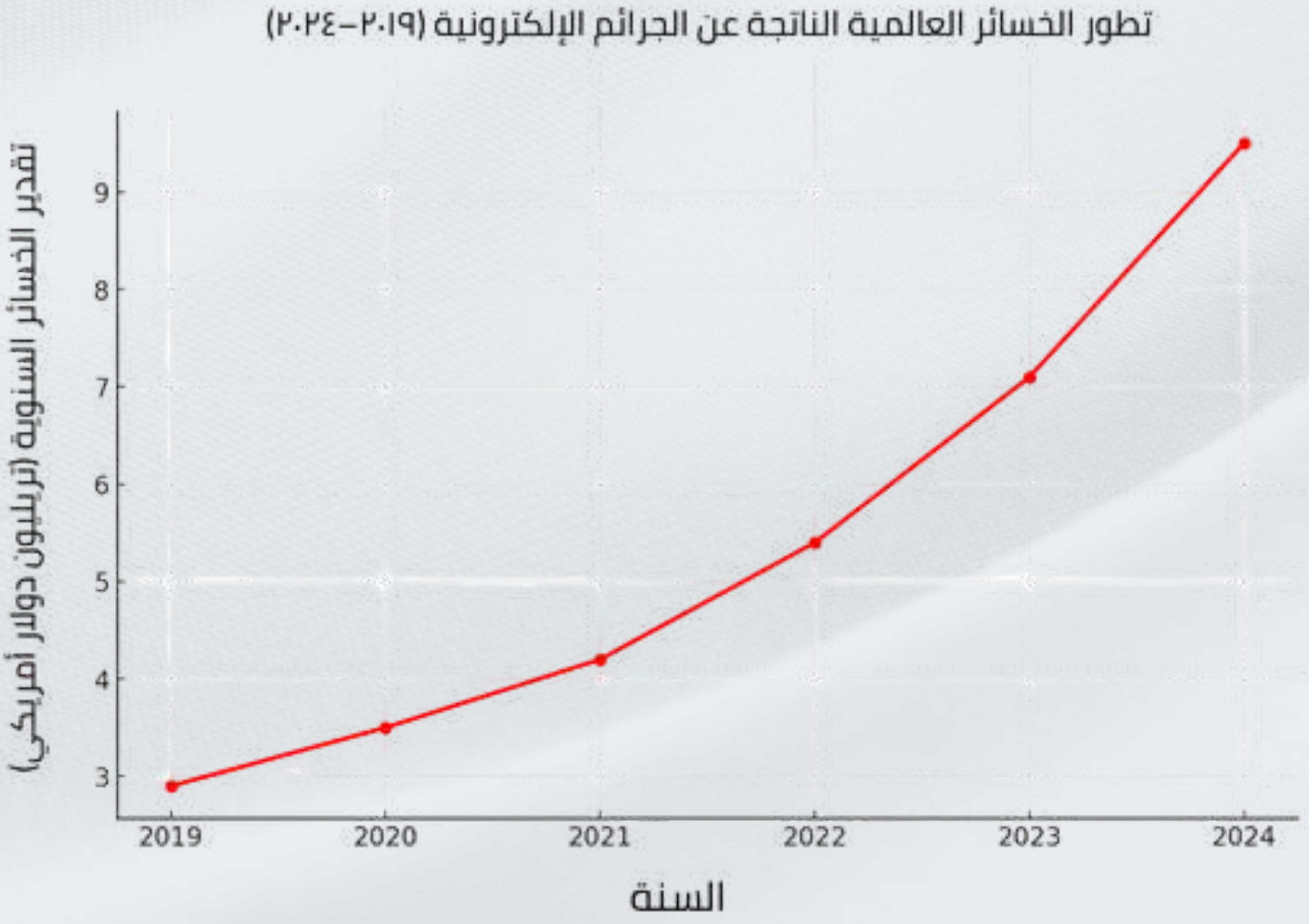
عالميًا:

تكشف الإحصائيات العالمية عن أرقام صادمة تعكس حجم التهديدات. فقد أظهرت لجنة التجارة الفيدرالية الأمريكية (FTC) في تقريرها لعام ٢٠٢٤ أن أكثر من ٧٠٪ من حالات الاحتيال بدأت من خلال منصات التواصل الاجتماعي، وأدت إلى خسائر مالية تجاوزت ١.٩ مليار دولار أمريكي خلال عام واحد فقط.

وفي هذا السياق أعلنت شركة كاسبرسكي (Kaspersky) عن إحباطها لأكثر من ٨٩٣ مليون محاولة تصيّد احتيالي خلال عام ٢٠٢٤، في حين سجلت مصر زيادة بنسبة ٤٩٪ في هذه الهجمات مقارنةً بالعام السابق.

من ناحية أخرى، كشف تقرير لموقع "إرم نيوز" عن واحدة من أكبر قضايا الاحتيال الإلكتروني، والتي قُدِّم فيها بلاغات من أكثر من مليون ضحية، وبلغت فيها الخسائر نحو ٦ مليارات دولار.

ولم تقتصر الأمور على ذلك، بل إن الاحتيال عبر عروض التوظيف الوهمية سجّل ارتفاعًا كبيرًا، حيث قفز إجمالي الخسائر من ٩٠ مليون دولار في عام ٢٠٢٠ إلى أكثر من ٥٠٠ مليون دولار في عام ٢٠٢٤، وهو ما يدل على تطور وتنوع أساليب المحتالين.



محليًا في مصر:

تلقى قطاع مكافحة جرائم المعلومات نحو ٧٠٠٠ بلاغ خلال عام ٢٠٢٣ ، تتعلق بالنصب الإلكتروني، كما ذكر جهاز حماية المستهلك في عدة تقارير أن عدد الشكاوى المتعلقة بالتجارة الإلكترونية – التي تتضمن بلاغات عن الاحتيال الإلكتروني، النصب، وعدم تسليم السلع طبقًا للمواصفات - وصل إلى ما يُقارب ٣٢,٠٠٠ شكوى خلال عام ٢٠٢٤ ، وقد تم التحقق وحل حوالي ٣٠,٠٠٠ حالة منها، بما يُعادل نسبة إنجاز حوالي ٩٥ %

كما أوضح جهاز حماية المستهلك في تقاريره الرسمية لعام ٢٠٢٤ أن عدد الشكاوى المتعلقة بالتجارة الإلكترونية- والتي تشمل بلاغات عن الاحتيال، النصب، أو عدم استلام السلع طبقًا للمواصفات – بلغ نحو ٣٢,٠٠٠ شكوى، وقد تم التحقق من ٣٠,٠٠٠ شكوى منها، أي بنسبة إنجاز تقارب ٩٥٪.

كما تشير البيانات العامة للجهاز إلى أنه تلقى ما مجموعه ٢٠٦,٠٧٣ الاف شكوى من المستهلكين في مختلف القطاعات خلال عام ٢٠٢٤، من بينها ٦٥٣,٣١ شكوى تتعلق بالتجارة الإلكترونية فقط، وقد تم حل ٣٠,١٠٥ شكوى منها بشكل نهائي.

ومع أن هذه الأرقام لا تُحدّد بدقة الحالات التي تخص الاحتيال الرقمي فقط، إلا أنها تمثّل مؤشرًا قويًا على التحدي الكبير الذي تمثّله التعاملات الافتراضية غير الموثوقة في مصر.

ويُظهر هذا التصاعد في عدد البلاغات مدى تفاقم جرائم الاحتيال الإلكتروني في مصر، مما يستدعي تكثيف جهود الرقابة، وتحسين آليات الحماية، لضمان بيئة رقمية أكثر أمانًا للمستهلك المصري.

في الختام
الوعي هو خط الدفاع الأول

أصبح الاحتيال الرقمي أكثر تعقيدًا وصعوبة في الاكتشاف. ورغم ذلك، يظل الوعي الفردي والمؤسسي خط الدفاع الأول ضد هذه التهديدات.

فكل موظف مدرّب أو فرد واعٍ يشكّل حاجزًا أمام محاولات الاختراق، لأن المواجهة لا تقتصر على الجانب التقني فقط، بل تبدأ من الانتباه إلى أبسط المؤشرات مثل رسالة مشبوهة أو رابط غير مألوف.

لذلك، من المهم التعامل بحذر مع أي رسالة أو عرض غير متوقع، ومع تكامل وعي الأفراد مع إجراءات المؤسسات يمكن الحد من الاحتيال وحماية البيانات والأصول وضمان مستقبل رقمي آمن.

المصادر :

1- kaspersky (me.kaspersky.com)
https://www.kaspersky.com/resource-center/threats/top-scams-how-to-avoid-becoming-a-victim

2- Microsoft (www.microsoft.com)
https://support.microsoft.com/en-us/office/protect-yourself-from-online-scams-and-attacks-0109ae3f-fe61-4262-8dce-2ee3cd43bac7

3- Eset (www. eset.com)
https://help.eset.com/ems/9/ar-EG/antiphishing.html

4- Mcafee (www.mcafee.com)
https://www.mcafee.com/learn/what-is-phishing/