الخليج

أخبار الدار, تحقيقات وحوارات

14 أغسطس 2023 01:21 صباحا

«رسائل احتيالية تهاجم هواتف المتعاملين بـ «صفة رسمية

تحقيق: محمد الماحي

رسائل احتيالية خادعة استقبلها الآلاف من المتعاملين عبر الهاتف وتطبيق واتساب، بعد أن طوَّر محتالون إلكترونيون وسائلهم بانتحال صفات دوائر ومؤسسات رسمية، من خلال إنشاء مواقع إلكترونية مشابهة لها، بغرض النصب على الشركات والأفراد بعد أن تنوّعت أساليبهم وأنشطتهم الإجرامية وطرق الاحتيال الإلكتروني التي تنطوي على محاولة الحصول على المعلومات البنكية والمالية للعديد من الشركات والأفراد، والوصول إلى بيانات الحسابات والبطاقات الائتمانية الخاصة بهم، عبر رسائل احتيالية تحمل الشعار الرسمي لمؤسسات الدولة.

بحسب ضحايا وقعوا في هذا الفخ، فإن تلقي الرسالة أثار ارتباكهم، وجعلهم يعتقدون أن المرسل يتبع لجهة رسمية خصوصا أنها تتضمن الشعار والأسلوب الرسمي، ما يُضفي نوعاً من المصداقية على حديث المحتال.

عبدالله الكعبي

حيلة جديدة

وشكا متعاملو بنوك تداول رسائل احتيالية بشكل موسع، أخيراً، عبر تطبيقات مواقع التواصل الاجتماعي، مستغلة اسم وشعار المصرف المركزي، بهدف الحصول على بيانات المتعاملين المصرفية، من خلال التواصل مع أرقام هواتف مرفقة مع الرسائل، مؤكدين ل«الخليج» أن الرسائل تطلب من المتعاملين تجميد حساباتهم المصرفية، أو بطاقات الائتمان.

وتلقى عدد من المواطنين والمقيمين في الفترة الأخيرة، رسالة إلكترونية مُزيّفة استهدفت اصطيادهم إلكترونياً، للاحتيال على حساباتهم البنكية باستخدام حيلة جديدة، عن طريق اختراق هواتفهم الذكية، لإخطارهم بأنه تقرر فصلهم من العمل، وأنه يجب عليهم الضغط على رابط أسفل الرسالة لمعرفة أسباب الفصل، وإجمالي مستحقاتهم المالية. وبعد أن قاموا بمراجعة إدارات الموارد البشرية تأكدوا أن الرابط وهمي، يستهدف سرقة الأموال من الحسابات البنكية، بينما استجاب آخرون لرابط الرسالة حتى تبيّن لهم أنها احتيالية، ما يؤكد أن عمليات الاحتيال باتت تتقرّب إلى الضحايا من خلال مطالبتهم بتقديم معلومات شخصية أو مهنية عنهم، بعد طمأنتهم وإشعارهم بصدق ومأمونية الجهة المرسلة.

خالد محمد الشبلي

كشفت وزارة الموارد البشرية والتوطين أنها رصدت رسالة وهمية مرسلة من خلال قنوات رقمية وإلكترونية متضمنة الشعار الرسمي للوزارة وجهات حكومية أخرى، يدّعي مرسلوها تجميد الحسابات البنكية ما لم يتم تزويدهم ببيانات المتعاملين، وطلب الاتصال على أرقام معينة، وأهابت الوزارة عدم التجاوب مع هذه الرسالة وتجاهلها حال تلقيها، والتواصل فوراً مع الجهات الأمنية المعنية للإبلاغ عنها.

وحذرت هيئة تنظيم الاتصالات والحكومة الرقمية من عمليات النصب والاحتيال عبر وسائل التواصل الاجتماعي، وقالت على موقعها الرسمي إن الآونة الأخيرة شهدت ظهور أساليب وطرق جديدة للنصب والاحتيال، موضحة أنها بادرت بإطلاق حملات للتوعية بتلك العمليات الاحتيالية عبر موقعها الرسمي وحسابات التواصل الاجتماعي، لتفادي وقوع ضحايا للنصب والاحتيال والابتزاز الإلكتروني.

ونصحت بعدم الضغط على الروابط الغريبة أو فتح مرفقات من مصادر لم يتم التحقق منها، والتأكد من صحة الرسائل النصية، وتحديث أجهزة المشتركين الإلكترونية، وتجنّب استخدام برامج مقرصنة أو الحصول عليها من مواقع غير موثوقة.

أبلغ عدد من المستخدمين عن الأنشطة الاحتيالية في الأسابيع الأخيرة، بما في ذلك أفراد يتلقون رسائل نصية «إس إم إس» واستطلاعات رأي تزعم أنها من «بريد الإمارات»، وتخدع عمليات الاحتيال هذه المتلقّين، لتقديم معلومات شخصية، وإجراء مدفوعات لمصادر غير مصرح بها.

وحث بريد الإمارات، على «إكس» ووسائل التواصل الاجتماعي الأخرى، السكان على توخي الحيطة والحذر، واتخاذ

الاحتياطات اللازمة لحماية أنفسهم من الوقوع ضحية لمثل هذه الحيل. وقالت المؤسسة على موقعها على الإنترنت: ««نحن نرسل فقط الرسائل القصيرة من خلال حساب بريد الإمارات المسجل لدينا».

خطورة الانجرار

وشدد مسؤولون وقانونيون على خطورة الانجرار خلف المجرمين، الذين يترصدون ضحاياهم عبر الرسائل الوهمية بانتحال صفة رسمية لتحقيق مآربهم، مؤكدين أن الجهات الحكومية تبذل جهوداً متواصلة للحد من عمليات النصب والاحتيال على الإنترنت أو من خلال رسائل مضللة عبر الهواتف، مشيرين إلى أن الجهات الأمنية المختصة تقوم بتتبع مصدر الرسائل والإيقاع بمرتكبيها وتقديمهم للعدالة، وفقاً لقانون مكافحة جرائم تقنية المعلومات ومواده القانونية التي تتضمن الغرامات المالية والحبس.

قال رئيس نيابة أول بنيابة ديرة، الخبير بالجرائم الإلكترونية، المستشار الدكتور خالد الجنيبي، إن هناك حقيقة واحدة يجب أن يدركها جميع أفراد المجتمع، وهي أنه لن تطلب جهة رسمية أو حتى البنك نفسه بيانات سرية من العميل عبر الهاتف، لذا يجب عدم الانقياد وراء هذه الأساليب الاحتيالية.

وأضاف أن الاحتيال الإلكتروني واحد، لكن الكذبة تتغير، مؤكداً أن هذه الجريمة تحديداً لا يمكن أن تقع دون مشاركة المجني عليه، سواء بالإفصاح عن بياناته السرية، أو الضغط على رابط مشبوه ورد في رسالة نصية أو عبر البريد الإلكتروني.

قالت الخبيرة المصرفية، عواطف الهرمودي: «يجب الحذر من الاستجابة لتلك الرسائل والتأكد من زيفها عبر مظاهر عدة، أبرزها أن المصرف المركزي لا يتواصل بشكل مباشر مع المتعاملين، ولا يضع أرقام هواتف شخصية للتواصل، كما أنه لن يطلب من المتعاملين بيانات خاصة بأرقام بطاقتهم، أو الأرقام السرية لها، أو أرقام الخدمات الإلكترونية المصرفية».

وأكدت أنه يجب على المتعامل أن يتجنب التواصل مع أي أرقام مرفقة بالرسائل، أو الضغط على الروابط الإلكترونية المرفقة، مشددة على أهمية التواصل مع البنك الخاص بالمتعامل، عند الشك في أي رسائل تتعلق بحسابه.

وأكدت أن الجهات الحكومية تبذل جهوداً متواصلة للحد من عمليات النصب والاحتيال على الإنترنت أو من خلال رسائل مضللة عبر الهواتف، مشيرة إلى أن الجهات الأمنية المختصة تقوم بتتبع مصدر الرسائل والإيقاع بمرتكبيها وتقديمهم للعدالة، وفقاً لقانون مكافحة جرائم تقنية المعلومات ومواده القانونية التي تتضمن الغرامات المالية والحبس.

الصفحات الشخصية

وأكد أخصائي أمن المعلومات في مركز الإمارات للدراسات والبحوث الاستراتيجية، خالد محمد الشبلي، أن رسائل الاحتيال الإلكتروني باتت تعتمد على تقديم بعض المعلومات الشخصية أو المهنية عن الشخص الذي يتم إرسال الرسالة إليه، بهدف طمأنته وإشعاره بصدق ومأمونية الجهة المرسلة، لافتاً إلى أن أغلب المعلومات التي يعتمد عليها المحتالون في تلك الرسائل تكون موجودة بالفعل على الصفحات الشخصية في وسائل التواصل الاجتماعي.

وتابع: إن التأني والتدقيق في المعلومات الواردة في مثل هذه الرسائل يكشفان زيف الجهة المرسلة، ولكن يبقى الخطر

الحقيقي في عدم السيطرة على المشاعر والصدمة التي قد تدفع البعض للتجاوب مع المحتال وإعطائه ما يريد من أرقام حسابات بنكية، أو وثائق ثبوتية يمكن بيعها لأغراض وجهات متنوعة.

تقنية معلومات

وقال المحامي والمستشار القانوني عبد الله الكعبي إن القانون الأخير الصادر وفق المرسوم رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية تناول الأساليب الإجرامية للاحتيال الإلكتروني في أكثر من مادة، ما يعكس حرص المشرع على ردعها بالسبل كافة.

وقال إن المادة الثانية من القانون تناولت جرائم الاختراق الإلكتروني، ونصّت على أنه يعاقب بالحبس وغرامة لا تقل عن 100 ألف درهم ولا تزيد على 300 ألف درهم، أو بإحدى هاتين العقوبتين، كل من اخترق موقعاً أو نظام معلومات إلكترونياً أو شبكة معلومات، أو وسيلة تقنية معلومات.

وأضاف أن المادة السادسة تطرقت بشكل مفصل لجريمة الاعتداء على البيانات والمعلومات الشخصية، ونصت على أنه يعاقب بالحبس مدة لا تقل عن ستة أشهر، وغرامة لا تقل عن 20 ألف درهم، ولا تزيد على 100 ألف درهم، أو بإحدى هاتين العقوبتين، لافتاً إلى أن البند الثاني من هذه المادة اعتبر اختراق الحسابات المصرفية أو بيانات ومعلومات وسائل الدفع الإلكترونية ظرفاً مشدداً.

وأشار إلى أن القانون الجديد الذي بدأ سريانه مطلع العام الجاري دمج مادتين في القانون السابق متعلقتين بالاستيلاء على بيانات البطاقات والحسابات البنكية وتزويرها في مادة واحدة رقم 15، وتنص على أنه يعاقب بالحبس والغرامة التي لا تقل عن 200 ألف درهم ولا تزيد على مليوني درهم، أو بإحدى هاتين العقوبتين، كل من زوّر أو قلد أو نسخ بطاقة ائتمانية أو بطاقة مدينة أو أي وسيلة من وسائل الدفع الإلكتروني، أو استولى على بياناتها أو معلوماتها باستخدام وسائل تقنية المعلومات أو نظام معلوماتي.

شرطة أبوظبي تحذر من الأساليب المتجددة

«أبوظبي: «الخليج

حذرت شرطة أبوظبي من تجدد أساليب المحتالين والنصابين المخادعة، واستدراج الضحايا بطرق مضللة، من مكالمات احتيالية وروابط مواقع نصب إلكترونية مزورة عبر رسائل نصية قصيرة تحاكي مؤسسات حكومية، وتتصيد الجمهور، وتقدم لهم خدمات وإغراءات وهمية.

ونبّهت من مواقع الإنترنت المزيفة التي تحمل أسماء مطاعم ومحال مشهورة، وتقوم بتقديم عروض مميزة للجمهور، مقابل دفع رسوم يتم من خلالها سحب الرصيد بعد إتمام عملية الدفع من البطاقة الائتمانية في الموقع المزيف.

ودعت شرطة أبوظبي، الجمهور إلى عدم التعامل مع الإعلانات الإلكترونية المزيفة التي تعرض حيوانات أليفة للبيع أو التبني، مقابل تحمل تكاليف الشحن والتأمين من خارج الدولة، ويتم الإعلان عنها عبر مواقع التواصل الاجتماعي

وبعض تطبيقات البيع والشراء على الهواتف الذكية؛ حيث يُطلب من الضحايا إرسال أموال إلى حسابات بنكية، فُتحت لغرض السرقة والاحتيال أو طلب تحويل الأموال عبر شركات الصرافة المحلية والعالمية المرخصة بالدولة.

كما حذرت الباحثين عن عمل من التوظيف الوهمي، ومن تصديق أكاذيب المحتالين والذين يقومون حالياً باستغلال فرصة إقامة المناسبات والفعاليات الرسمية للاحتيال عليهم؛ وذلك بإنشاء صفحات لشركات وهمية عبر الإنترنت على أنها شركات توظيف معتمدة، وتطلب دفع مبالغ مالية رسوماً لتلك الوظائف الوهمية، ليكتشف المتقدمون بطلباتهم في آخر المطاف أنهم وقعوا ضحية للنصب والاحتيال.

وناشدت الجمهور بعدم مشاركة معلوماتهم السرية مع أي شخص سواء معلومات الحساب الشخصي أو البطاقة البنكية، أو كلمات المرور الخاصة بالخدمات المصرفية عبر الإنترنت أو أرقام التعريف الشخصية الخاصة بأجهزة الصراف الآلي أو رقم الأمان (CCV) أو كلمة المرور وأن موظفي البنوك والمصارف لن يطلبوا هذه المعلومات من أي شخص بتاتاً.

ودعت شرطة أبوظبي الجمهور في حالة الاحتيال التوجه إلى أقرب مركز شرطة، وسرعة الإبلاغ عن أي اتصالات تردهم من قبل مجهولين يطالبونهم بتحديث بياناتهم المصرفية، بالتواصل مع خدمة أمان رقم 8002626 أو عن طريق إرسال رسالة نصية 2828 تعزيزاً لجهود الشرطة في مواجهة هذه الأساليب الاحتيالية، ووقاية المجتمع من مخاطرها، وطالبت بتفعيل برامج الحماية، لضمان كفاءة التخلص من المواقع الضارة التي تحتوي على شيفرات إلكترونية، تستهدف سلب مدخراتهم، وعدم الانسياق وراء الإغراءات الوهمية.