

## الأمن السيبراني خط الدفاع الأول في مواجهة الاحتيال الإلكتروني



دبي: محمد ياسين

طالب المشاركون في مجلس «الخليج» الرمضاني، الذي استضافه المحامي بدر خميس بدبي، بضرورة التعرف إلى أفضل السبل للوقاية من مخاطر الاحتيال الإلكتروني، والاتصال مباشرة بالجهات المعنية، للإبلاغ عن أي هجمات أو محاولات احتيال على الحسابات المصرفية والبطاقات الائتمانية، وأكدوا أن الإمارات كانت سباقة في مواجهة مثل هذه الاختراقات بالأمن السيبراني، حيث وضعت التشريعات وسنت القوانين وغلظت العقوبة على مرتكبي تلك الجرائم، بالحبس وغرامة مالية تصل إلى مليون درهم، مع حظر ولوج المدان إلى الإنترنت.



بدر خميس

في بداية المجلس، شكر بدر عبدالله خميس جريدة «الخليج» على استمرارها في تنظيم المجالس الرمضانية التي تعد

من المظاهر والعادات والتقاليد التراثية لدى المواطنين خلال شهر رمضان المبارك

وقال إن قضية الأمن السيبراني التي يناقشها المجلس، واحدة من أهم القضايا التي يتداولها أفراد المجتمع، لافتاً إلى أن التكنولوجيا أصبحت جزءاً لا يتجزأ من الحياة، وتستخدم بأسلوب مستمر دون توقف، سواء للكبار أو الصغار، لاسيما بعد دخول الأجهزة اللوحية والهواتف والكمبيوتر في كل تفاصيل الحياة

## حماية الشبكات

أوضح بدر خميس، أن تخزين جميع المعلومات والبيانات والصور والأرقام السرية وتنزيل برامج البنوك على الهواتف، أدى إلى توفير وسائل الراحة والرفاهية، حيث سهلت التكنولوجيا الحياة بصورة كبيرة وقصرت المسافات وقللت التكاليف، غير أن ذلك لم يمنع حدوث الاختراقات والاعتداء على البيانات والمعلومات السرية، لافتاً إلى أن الجرائم الإلكترونية امتدت لتكون عابرة للقارات

وأشار إلى أن هذه الهجمات غالباً ما تهدف للوصول إلى المعلومات الحساسة بهدف تغييرها أو إتلافها، لذا تم تصميم تدابير الأمن السيبراني لمكافحة التهديدات للأنظمة المتصلة بالإنترنت مثل الأجهزة والبيانات

وأضاف أن الأمن السيبراني يهدف إلى تقليل مخاطر الهجمات الإلكترونية والحماية من الاستغلال غير المصرح به للأنظمة والشبكات، وسنسخ بالذكر أمن الهاتف وهو يعتمد على الأجهزة المحمولة في كثير من المعاملات ويمنع هذا المجال من الأمن الوصول غير المصرح به إلى المعلومات الشخصية والتنظيمية المخزنة على الأجهزة المحمولة مثل الأجهزة اللوحية والهواتف وأجهزة الكمبيوتر والمعدات المفقودة أو المسروقة والبرامج الضارة والفيروسات وغير ذلك

## تواصل فوري

أكد المحامي سالم الحمادي ضرورة التواصل مع الجهات المعنية فور التعرض للاحتيال الإلكتروني، كون تلك البلاغات التي يقدمها أفراد المجتمع للجهات الأمنية تعرفهم بوسائل الاحتيال الإلكتروني الجديدة التي يعتمد عليها المحتالون في جرائمهم

وأشار إلى أن العصابات الإلكترونية العابرة للقارات لم تتوقف عن ابتكار طرق جديدة للاحتيال واختراق كلمات الأمن السيبراني لأفراد المجتمع، حيث تخدع العصابات أفراد المجتمع وتستغل شغفهم في التسوق من المواقع الإلكترونية الشهيرة، وتصمم صفحات مشابهة يقدم فيها المتسوق بياناته للمحتال بسهولة

وسرد قضية وقع ضحيتها شخص، شاهد عرضاً على وجبة غداء من مطعم شهير بسعر أقل من المتعارف عليه بكثير، فقام الشخص باختيار وجبته ودفع فيمتها التي لا تزيد على 40 درهماً بواسطة بطاقته الائتمانية، ففوجئ بعد ثوانٍ بسحب مبالغ مالية من حسابه تزيد على 20 ألف درهم

## زيادة التوعية

قالت المحامية ميثاء طالب: مع زيادة الاعتماد على تقنيات الذكاء الاصطناعي، أصبح من الضروري زيادة التوعية المجتمعية بتلك المخاطر التي تتنوع وتزيد في العالم الافتراضي وتخرق عالمنا الواقعي

وأشارت إلى أن الجرائم تتطلب زيادة الجهود الدولية ومزيداً من الاتفاقات لملاحقة المحتالين وعدم تركهم يسعون في الأرض فساداً، مشيرةً إلى اتفاقات عقدتها دولة الإمارات مع عدد من الدول لملاحقة المحتالين.

وأضافت أن التوعية ومعرفة الإجراءات اللازمة لحماية الأمن السيبراني، هي الجدار الأول في الحماية من الاحتيال الإلكتروني، والوقوع في فخ العصابات، مشيرة إلى إنشاء كلمة مرور قوية ومعقدة وتثبيت التحديثات للأجهزة المحمولة باستمرار وأجهزة الكمبيوتر والتطبيقات، وعدم فتح رسائل البريد الإلكتروني المجهولة التي قد تحمل فيروسات، تحمي المجتمع من المتربصين في عالم الاحتيال الافتراضي.

## أضرار المستغلين

تحدثت المحامية عائشة الظاهري عن أهمية حماية أنفسنا من أضرار مستغلي الذكاء الاصطناعي في الاحتيال والنصب الإلكتروني، وقالت إن الإمارات وفرت قنوات للإبلاغ عن الجرائم الإلكترونية والمحتالين، الأمر الذي سهل الأمر على الجهات المختصة في ملاحقة تلك الفئة في حال كانوا موجودين داخل الدولة، والتعاون مع جهات في دول أخرى لملاحقتهم.

وأضافت أن أفراد العصابات الإلكترونية لم يتوقفوا عن تحديث طرقهم في الاحتيال والسطو على أموال ضحاياهم، مشيرة إلى قضية، وقعت فتاة ضحيتها، حيث استقبلت رسالة بمرفق صورة، تمكن من خلالها محتال من اختراق حسابها وهاتفها، وأصبحت جميع بياناتها متاحة للمحتال الإلكتروني الذي حاول ابتزازها، فتقدمت ببلاغ وقبض عليه.

وفي ختام المجلس، استعرض المحامي بدر خميس العقوبات التي يتعرض لها المحتال ومخترق خصوصية الآخرين، وقال يجب أن نوضح أن القانون وضع عقوبة أصلية وتدابير جزائية لهذه الجريمة، وقد نصت المادة «40» من قانون مكافحة الشائعات والجرائم الإلكترونية لدولة الإمارات، مرسوم بقانون اتحادي رقم (34) لسنة 2021، على أنه يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (250.000) درهم ولا تزيد على (1.000.000) درهم أو بإحدى هاتين العقوبتين، كل من استولى لنفسه أو لغيره بغير حق على مال منقول أو منفعة أو على سند أو توقيع هذا السند.

أما بالنسبة للتدابير الجزائية، فقد نصت عليها المادة «59» من ذات القانون والتي تضمنت وضع المحكوم عليه تحت الإشراف أو المراقبة الإلكترونية أو حرمانه من استخدام أي شبكة معلوماتية، أو نظام المعلومات الإلكتروني، أو أي وسيلة تقنية معلومات أخرى أو وضعه في مأوى علاجي أو مركز تأهيل للمدة التي تراها المحكمة مناسبة، وإغلاق الموقع المخالف إغلاقاً كلياً أو جزئياً متى أمكن ذلك فنياً، وحجب الموقع المخالف حجباً كلياً أو جزئياً للمدة التي تقررها المحكمة، ويعاقب كل من يخالف هذه التدابير بالحبس مدة لا تزيد على سنة أو بغرامة لا تزيد على (5000) درهم وبالتالي فإن هذه العقوبات رادعة ولا تحتاج إلى تشديد.