

## التطبيقات الذكية.. وسائل احتيال في القرن الـ 21



### تحقيق: محمد الماحي

شهدت التطبيقات الذكية، تزامناً مع انتشار جائحة «كورونا»، نمواً غير مسبوق لتصبح أسرع الآليات لصنع الثروات، ولأن أي شيء مربح يكون هدفاً دائماً للمحتالين، فكان من الطبيعي أن تُسبل هذه التطبيقات الذكية لُعاب المحتالين وقراصنة الإنترنت، حاملةً معها طرقاً جديدة في الاحتيال، فانتشرت مؤخراً على مواقع التواصل الاجتماعي حملات ترويجية لتطبيقات تحتوي على برامج خبيثة وضارة تعمل على اشتراك مستخدمي الهاتف في الخدمات ذات القيمة المضافة المكلفة، ويتم الاحتيال بتسجيل المستخدمين الذين قاموا بتنزيل هذه التطبيقات تلقائياً بمحتوى خاص، دون موافقة أو معرفة مسبقة؛ إذ تستفيد التطبيقات من نقاط ضعف أجهزة أندرويد تمكّن المحتالين من النصب على المستخدمين بأكثر من ألف درهم سنوياً، وهناك تطبيقات أخرى توهم مستخدميها بتحصيل أموال نظير ممارسة رياضة المشي، وتشجع هذه التطبيقات التي تديرها شركات خارج الدولة كل مستخدم على دعوة 5 أصدقاء للحصول على كسب إضافي، في محاولة لزيادة الإقبال عليها، بينما تستغل هذه التطبيقات معلومات المستخدمين للتربح، حيث تباع بيانات كل 25 شخصاً مقابل دولار واحد أمريكي.

مع نائبة «كورونا»، وما رافقها من تدابير احترازية ووقائية، وتوجيهات للجميع بالتزام بيوتهم، خشية الإصابة بالفيروس، أمضى سكان الإمارات 320 مليون ساعة على تطبيقات الهواتف الذكية خلال عام 2020، الذي شهد انتشار جائحة فيروس «كورونا»، وقد بلغت قيمة مدفوعات الصفقات الرقمية في دولة الإمارات 18.50 مليار دولار، بحسب «تقرير العالم الرقمي 2021»، الصادر عن مؤسسة «وي آر سوشال» العالمية، بالتعاون مع «شركة هوت سويت»، هذا الوضع جعل محتالين يلجأون إلى ابتداع أساليب تطبيقات وهمية؛ للحصول على المال، والاستيلاء عليه بطرق ملتوية.

جهود الجهات الأمنية لا تتوقف للحد من الجريمة؛ حيث أظهرت إحصاءات إدارة المباحث الإلكترونية في الإدارة العامة للتحريات والمباحث الجنائية في شرطة دبي أن الإدارة استطاعت الإطاحة بـ 97 متهماً ضمن أخطر العصابات الدولية خلال العام الماضي، كانوا سيتسببون في خسائر تقدر بنحو 11 ملياراً و803 ملايين و728 ألفاً و300 درهم لأفراد المجتمع من خلال عمليات النصب والاحتيال الإلكتروني.

وسجلت إدارة المباحث الإلكترونية 1078 مساعدة تقنية لاستعادة الحسابات المُخترقة في مواقع وبرامج التواصل الاجتماعي خلال العام الماضي، شملت حالات النصب والاحتيال والابتزاز.

وحذر العميد جمال سالم الجلاف، مدير الإدارة العامة للتحريات والمباحث الجنائية، من الانسياق وراء المحتالين على مواقع وبرامج التواصل الاجتماعي، مؤكداً ضرورة الإبلاغ عنهم فور رصد محاولاتهم الاحتيالية، وموضحاً أن الجرائم الإلكترونية بمختلف تصنيفاتها في تسارع عالمي مستمر، نظراً لزيادة الاستخدام العالمي للتقنيات في مجال الخدمات، واستخدام الأنظمة الذكية في المعاملات اليومية، وهو ما يصنع تحديات أمنية مستمرة تتطلب العمل بشكل مستمر في تطوير أنظمة إلكترونية حديثة ومبتكرة للتصدي للمحتالين والعصابات الإلكترونية.

وأطلقت شرطة أبوظبي النسخة الرابعة من الحملة الإعلامية التوعوية «خلك حذر» بهدف تعزيز وعي المجتمع بالأشكال المستجدة للجرائم الإلكترونية.

وأوضح العميد محمد سهيل الراشدي، مدير قطاع الأمن الجنائي أن الحملة في عامها الثالث – والتي تستمر مدة شهر – تركز على زيادة الوعي لدى الجمهور من مستخدمي شبكة الإنترنت والأجهزة الذكية بضرورة المحافظة على بياناتهم ومعلوماتهم الخاصة وعدم الإفصاح عنها، تجنباً للوقوع ضحايا لتنظيمات هدفها زعزعة الاستقرار والأمن وإحداث الفوضى في المجتمع. وأطلقت القيادة العامة لشرطة الشارقة حملة توعية إلكترونية لمدة شهر، تحت عنوان «احذر مخاطر الابتزاز الإلكتروني»، بهدف رفع الوعي لدى أفراد المجتمع حول خطورة الابتزاز الإلكتروني، وتجسيدها لاستراتيجية وزارة الداخلية والقيادة العامة لشرطة الشارقة، الرامية إلى تعزيز الأمن والأمان.

## البيانات الشخصية

اعتبر خبراء تقنيون أن هذه التطبيقات إحدى أسوأ وسائل الاحتيال في القرن الـ 21، محذرين من استخدامها؛ لأن هدفها الاختراق والحصول على معلومات المستخدمين، مؤكداً أن التطبيق يحصل على موافقة ضمنية على شروط الاستخدام ومن ضمنها البيانات الشخصية للمستخدم.

توقعوا حدوث زيادة في الهجمات الإلكترونية التي تستهدف الاحتيال المالي، والحصول على المعلومات والبيانات الشخصية خلال عام 2021، بعد أن كثف مخترقون هجماتهم، العام الماضي، وأصبحوا على دراية واسعة بالثغرات التقنية الموجودة في الأجهزة الذكية وتطبيقات الذكاء الاصطناعي.

كما توقعوا أن يقل تأثير سكان الدولة بعمليات الاحتيال والهجمات الإلكترونية خلال عام 2021؛ لأنهم أصبحوا أكثر وعياً، مشيرين إلى أن كثيراً من المؤسسات والشركات منحت موظفيها أجهزة كمبيوتر مؤمنة، ما أفشل كثيراً من محاولات الاختراق أخيراً.

فيما أكد قانونيون أن مثل هذه التطبيقات مشبوهة، وبداية لعمليات نصب واحتيال لإيهام الناس والإيقاع بهم خصوصاً فئة الشباب، وأن استخدام وسائل تقنية المعلومات أو الشبكة العنكبوتية في النصب عقوبته قانوناً الحبس ستة أشهر على الأقل، والغرامة من 100 ألف إلى 300 ألف درهم.

## الثغرات التقنية

وقال نائب رئيس مجلس إدارة جمعية الإمارات للإنترنت الآمن، عادل الكاف الهاشمي، إنه «من المتوقع حدوث زيادة في الهجمات الإلكترونية التي تستهدف الاحتيال المالي والحصول على المعلومات والبيانات الشخصية خلال عام 2021، بعد أن كثف مخترقون هجماتهم في العام الماضي، وأصبحوا على دراية واسعة بالثغرات التقنية الموجودة في الأجهزة الذكية وتطبيقات الذكاء الاصطناعي»، مشيراً إلى أن مجرمي الإنترنت يقومون بتطوير قدراتهم بشكل مستمر.

وأكد الهاشمي أن سكان الدولة أصبحوا أكثر وعياً بالمخاطر الموجودة في الفضاء الإلكتروني، بعد تصاعد الاحتيال المالي، والهجمات التي تستهدف البيانات الشخصية والبطاقات الائتمانية خلال عام 2020، مطالباً بتطوير برامج الحماية بشكل مستمر؛ لتكون أكثر قدرة على التصدي للهجمات والابتزاز الإلكتروني.

وقال محمد الفقي، خبير الإعلام الرقمي والتسويق الإلكتروني، المحاضر في كلية «الدار الجامعية» في دبي، إنه من المتوقع أن يقل تأثير سكان الدولة بعمليات الاحتيال والهجمات الإلكترونية خلال عام 2021، على الرغم من توقعات بتصاعد المحاولات خلال الفترة المقبلة، موضحاً أن المستخدمين أصبحوا أكثر وعياً، ولا ينساقون وراء رسائل مجهولة عبر ال«واتس آب» أو البريد الإلكتروني، توهمهم بجوائز أو أموال، بعد أن تعرضوا لعمليات نصب من خلال مواقع وروابط مزيفة خلال العام الماضي، واكتسبوا خبرة التعامل مع مثل هذه الرسائل.

ونوه الفقي بأن كثيراً من المؤسسات والشركات منحت موظفيها أجهزة كمبيوتر مؤمنة إلى حد كبير، وتم وضع أنظمة حماية مضادة للفيروس، ما يجعل كثيراً من محاولات الاختراق تفشل خلال الفترة الأخيرة، مشيراً إلى أن عام 2020 شهد تزايد نسبة العمل على الأجهزة الشخصية غير المؤمنة، ما أسهم في تصاعد الهجمات.

وقال سامي عبدالنور، خبير تقنية المعلومات، إن هذه التطبيقات إحدى أذكي وسائل الاحتيال في القرن ال21، وذلك مباشرة بعد احتيال الأسهم والعملات الرقمية المشفرة.

وأوضح أن انتشار التطبيقات المختلفة على مواقع التواصل الاجتماعي ظاهرة تتكرر مرتين إلى ثلاث كل عام، حيث ينتشر أحد التطبيقات ويصبح تريند «موضة»، مبيناً أنها مجهولة الأهداف وغير معلوم مدى الأمان فيها.

كما أوضح أن تسجيل عدد كبير من المستخدمين بهذه التطبيقات يزيد من قدرتها على الاختراق، بهدف الحصول على معلومات المستخدمين، ومن ثم بيعها بالإنترنت المظلم؛ حيث تباع بيانات كل 25 شخصاً مقابل دولار أمريكي واحد، أي أن بيانات الشخص تعادل 4 سنتات، مشيراً إلى أن تطبيق المشي يتطلب الوصول إلى موقع المستخدم، وهذا أحد أنواع اختراق الخصوصية.

## فئة الشباب

من جانبه، أكد المستشار القانوني عبدالله الكعبي، أن مثل هذه التطبيقات غير مرخصة في الدولة وغير معتمدة من قبل الجهات المختصة، حيث تعتبر تطبيقات وهمية قد تكون بداية للنصب والاحتيال؛ لإيهام الناس والإيقاع بهم، خصوصاً فئة الشباب الذين يبحثون عن المكاسب السريعة، مشدداً على ضرورة مكافحة هذه التطبيقات، وإبلاغ النيابة العامة للتحقيق في الأمر وحظر مثل هذه المواقع.

وأوضح أن عقوبة استخدام الشبكة المعلوماتية أو نظام المعلومات الإلكتروني أو وسائل تقنية المعلومات، بهدف الاحتيال و الحصول على أرقام أو بيانات بطاقة ائتمانية أو إلكترونية أو حسابات مصرفية يعاقب بالحبس مدة لا تقل عن ستة أشهر، والغرامة التي لا تقل عن 100 ألف درهم ولا تتجاوز 300 ألف درهم، أو هاتين العقوبتين.

وقال المحامي الدكتور محمد بن حماد: إن هذا النوع من التطبيقات يختلف عن التطبيقات الذكية التي تقدم خدمات وتحصل على مقابل لها من مستخدميها، أما التطبيقات المشبوهة فلا تتحصل على أي مقابل، وإنما تقدم عمالات من أنواع العملات الرقمية، ما يثير الشكوك حول وجه استفادة القائمين على إدارتها، هل هي غسيل أموال، أم نوع من الأغراض التجسسية أو الاستطلاع المشبوه؟

وتابع: إذا ثبت ذلك فإن القانون يتم تطبيقه وفقاً لمعاييره وحسب ما تراه السلطات المختصة، هل المستخدم كان حسناً أم سيئ النية وعلى دراية بمخاطر أو أغراض هذه التطبيقات، وتكون العقوبة وفقاً لأغراض الاستخدام.