الاقتصادية
جريدة العرب الاقتصادية الدولية
جريدة الاقتصادية الالكترونية - أسواق المال - الأربعاء، ٢٦ ذو القعدة ١٤٢٦ هـ الموافق ٢٠٠٥/١٢/٢٨ م - العدد ٤٤٦١

التلويح بمقاضاته عبر الإنتربول وجهات حكومية تحذر منسوبيها

هاكرز دولي ينشئ موقعا مزورا لبنك سعودي و"المدينة" تغلقه

محمد عبيد . عبد الله آل غصنة - الرياض . الجبيل الصناعية - ١٤٢٦/١١/٢٦هـ

تمكن هاكرز يقيم خارج المملكة من تصميم موقع لأحد البنوك السعودية وإرسال رسائل باللغتين العربية والإنجليزية إلى عملاء البنك يحثهم فيها على أهمية تحديث البيانات ليكون التعامل عبر الإنترنت أكثر أمنا وسرعة. واستطاع الهاكرز من وضع صور وبيانات تطابق الموقع الأصلي لخدمة (أون لاين) البنك على الإنترنت (تحتفظ الجريدة باسمه) تمهيدا لنقل البيانات المدخلة من قبل العملاء إلى موقعه إلكترونيا مما يتيح له إمكانية التلاعب في الأرصدة أو إجراء عمليات تحويل وهمية.

ولم يثبت إن كان الهاكرز قد استطاع الإضرار بأرصدة العملاء أم تم تداركه قبل ذلك. حيث اعتذر البنك عن التصريح عن ذلك.

وأكد لـ" الاقتصادية" مصدر مطلع في هيئة الاتصالات وتقنية المعلومات، أن الهيئة تلقت معلومات من الجهات المختصة، تفيد بقيام شخص – يقيم في الولايات المتحدة وموقعه مستضاف في تايوان، بتضليل عملاء البنك.

وتابع المصدر أن الهاكرز أنشأ موقعين وهميين على شبكة الإنترنت، ويحويان معلومات مقلدة Phishing، للموقع الأصلي لخدمة البنك، بهدف الحصول على أموالهم بطريقة غير شرعية. بحيث يقوم العميل في البداية بإدخال (اسم المستخدم والرقم السري له)، ثم ينتقل بطريقه لا يمكن ملاحظتها إلى الموقع الرئيسي للبنك، وفي أثناء عملية الانتقال، يكون قد تم الدخول إلى حسابات العميل والتلاعب بها.

وأفاد المصدر، أنه تم على الفور التنسيق مع مدينة الملك عبد العزيز للعلوم والتقنية، بناء على طلب مؤسسة النقد العربي السعودي، وتم على الفور إغلاق الموقعين، لحماية العملاء المتعاملين مع البنك، والحد من التلاعب بأموالهم.

وأشار إلى أن هذه العملية تصنف ضمن جرائم المعلومات التقنية الدولية، مستبعدا أن يكون لبرنامج الحماية الذي يستخدمه البنك، أية علاقة بعملية التزوير الحاصلة، كونها عملية تضليل مشابهة للموقع وليس اختراقا لبرنامج الحماية. ولم يستبعد المصدر أن يلجأ البنك المتضرر إلى اتخاذ إجراءات قانونية عبر القنوات الرسمية من خلال وزارة الداخلية عبر الإنتربول ضد الهاكرز لمقاضاته.

أمام ذلك أرسلت بعض الجهات الحكومية ومن بينها الهيئة الملكية للجبيل وينبع وجامعة الملك سعود تحذيرات لمنسوبيها عبر رسائل إلكترونية تنذرهم من الالتفات إلى الرسالة المزورة إضافة إلى وضعها في البريد غير المرغوب فيه.

يشار إلى أن المؤسسات المالية عرضة دائما إلى الاختراقات حيث تمثل النسبة الأكبر بين تلك العمليات إذ قد تتجاوز٨١ في المائة بمعدل نحو ٣ آلاف موقع شهريا. وتتخذ المؤسسات المالية في السعودية مثلها مثل مختلف المؤسسات على مستوى العالم إجراءات حماية ضد مثل

هذه الاختراقات أو تزوير المواقع لمنع دخول الهاكرز والتلاعب بأرصدة عملائها.

في المقابل أكد الدكتور خالد بن سليمان الغثبر استشاري أمن المعلومات في جامعة الملك سعود أن طرق الاحتيال والخداع أصبحت أكثر تفنناً وإتقاناً ومنها ما يسمى برسائل الاصطياد الخادعة Phishing، وهي رسائل تبدو بالشكل والعنوان البريدي أنها مرسلة من منظمة حقيقية (وغالباً ما تكون المنظمة أحد البنوك) وتفيد بأن هناك تحديث للبيانات أو إجراءات جديدة للحماية والأمن وتطلب منك الدخول لموقع البنك عن طريق الرابط المزود مع الرسالة. وعند الانتقال للموقع الوهمي الذي يبدو بشكله وتصميمه وكذلك عنوانه كالبنك المعني يطلب منك بيانات خاصة ككلمة المرور أو معلومات بطاقة الائتمان ثم بعد الحصول على تلك المعلومات الثمينة يحيلك إلى موقع البنك الحقيقي.

وأفاد الغثبر أن الرسالة التي أرسلت إلى عملاء البنك السعودي من الوهلة الأولى وللشخص البسيط لا تثير الشك كونها تحتوي على شعار البنك وكذلك الموقع الذي يتسمى ويتموه باسم و شعار البنك الأصلي. لكن – والحديث ما زال للغثبر - الشخص المطّلع يدرك أن هناك شبهة في الأمر من خلال أنه ليس من المتعارف عليه (أو هكذا يفترض) أن يطلب البنك هذا الطلب من خلال الرسائل الإلكترونية عديمة الأمان.

وأضاف أن عنوان الموقع المحول إليه ليس هو عنوان موقع البنك، كما أنه لا يوجد قفل صغير في أسفل الشاشة (وهو كناية عن وضع التشفير) مثلما يوجد في موقع البنك الحقيقي.

وأشار الغثبر إلى أن ما لفت انتباه هو ردة الفعل العالية المستوى من قبل مؤسسة النقد ووحدة خدمات الإنترنت في مدينة الملك عبد العزيز للعلوم والتقنية على ما فعلتاه لردم هذا الخطر في فترة وجيزة.

وحذر الغثبر متصفحي الإنترنت من الرسائل التي تطلب بشكل مستعجلاً معلومات شخصية سرية، مشيرا إلى أن رسائل الخداع موجهة للعموم أما الرسائل المرسلة من الجهات الحقيقية فتكون مخصصة باسم العميل.

وأسدى استشاري أمن المعلومات نصائح من بينها في حال وصول مثل هذه الرسالة إلى العميل ألا يستخدم الرابط، قبل محادثة الجهة مباشرة أو كتابة موقع الجهة على برنامج المستكشف مباشرة. كما طالب بعدم تعبئة أي نموذج بالبريد الإلكتروني، حيث تكون تعبئة البيانات عن طريق موقع ومحمي، مشيرا إلى أن تلك المواقع تبدأ بـ https وليس http فقط وشكل القفل الصغير في زاوية المتصفح السفلى.

وطالب أيضا بتحديث برنامج المتصفح ونظام التشغيل بأحدث الترقيات الأمنية، موضحا أن استخدام عنوان (نطاق) مسجلاً سعودياً بامتداد sa قد يساعد في تقليل مخاطر الاصطياد نظراً لتدقيق التسجيل في هذا النطاق.

وطالب في حالة تقديم بيانات سرية بضرورة الإبلاغ في أسرع وقت ممكن للجهة الحقيقية لتغيير رقم الحساب أو كلمة المرور أو اسم المستخدم أو غيرها من الإجراءات اللازمة لتلافي أي خسائر.