الخليج

أخبار الدار ,

6 نوفمبر 2010 01:35 صباحا

تضمين المناهج الجرائم الإلكترونية "حرب ناعمة" ضد مرتكبيها

الجرائم الإلكترونية مصطلح برز حديثاً وأخذ يتسع نطاقه ويتسارع بوتيرة عالية، خلال الفترة الماضية، وهو نتاج التطور الهائل الحاصل في قطاع التكنولوجيا والتقنيات الحديثة، لاسيما الشبكة العنكبوتية التي تشهد زيادة مضطردة في عدد مستخدميها، ولعل مكمن خطورتها، الجهل بأساليب الاحتيال التي يبرع فيها ما يطلق عليهم اسم الهاكرز أو القراصنة من خلال ابتكار الطرق الجهنمية في التحايل، ليجد الشخص نفسه لقمة سائغة وفريسة سهلة في فخ نُصب له بكل إتقان ومهارة، ويظل نقص الثقافة الأمنية المعلوماتية، السبب الأبرز في وقوع المرء ضحية لهذه الجرائم، التي تطال المال أو المعلومات أو تهدف إلى تزييف الحقائق ونشر معلومات مضللة وكاذبة .

بتنا نسمع أخيراً الكثير عن عمليات النصب، وتحديداً الإلكترونية منها، حيث يتعرض أشخاص لعمليات سطو من قبل محتالين على أرصدتهم البنكية، من خلال تحويلها لجهات غير معلومة، خلال دقائق معدودة دون شعور الضحايا بذلك .

ولا يقتصر الأمر عند هذا الحد، بل قد يتعرض الشخص لحالات سرقة معلومات شخصية من خلال الولوج إلى المواقع كما phishing أو البريد الإلكتروني الخاص به، باستخدام أساليب وطرق مختلفة، أبرزها، صيد مستخدمي الحاسوب

. يؤكد الدكتور فادي علول، تخصص هندسة الكمبيوتر في كلية الهندسة في الجامعة الأمريكية بالشارقة

ويقول الدكتور فادي علول: لقد غزت التكنولوجيا عالمنا، وغدت جزءاً من حياتنا لا يمكن الاستغناء عنه، حيث أصبح المرء رهينة لهذا التطور، وباتت المشاريع والأعمال تدار من خلالها، كما أصبح بالإمكان إنجاز المعاملات البنكية والمصرفية، ودفع الفواتير والالتزامات المترتبة على الأشخاص بسهولة مطلقة، وكذلك يسّرت من عملية التواصل مع الآخرين في أي وقت، وفي الوقت ذاته يعد الجهل ونقص الثقافة في كيفية التعامل مع التقنيات الحديثة عنصراً له . خطورته وقد ينقلب إلى الضد ونتائجه لا يحمد عقباها

أصبح هناك تركيز من قبل الهاكرز على الأفراد الذين يعتبرون الحلقة الأضعف، بدلاً من المؤسسات والشركات التي تنبهت إلى ما قد تتسبب به هذه الفئة من أضرار، بعد أن عملوا على استقطاب خبراء في مجال الحاسوب، لتزويد شبكاتهم بالحماية اللازمة لها، والتي تضمن عدم تعرضها للاختراق، بيد أن الفئة المستهدفة حالياً تتمثل في الأفراد الذين . تنقصهم الخبرة ويعدون لقمة سائغة بيد هؤلاء الذين لا يتوانون عن اختراق أجهزتهم بسهولة والعبث بها كيفما شاؤوا

إن الزيادة في عدد مستخدمي الشبكة العنكبوتية ومن جميع الفئات والأعمار في العالم بشكل عام وفي الوطن العربي خصوصاً، شجعت المخربين على تنفيذ هجماتهم الشرسة، حيث أمسينا نسمع ونقرأ عن تعرض مواقع إلكترونية حكومية وخاصة لهجمات القراصنة بشكل متزايد في الآونة الأخيرة، ما يتعين تكثيف الجرعات التثقيفية والتوعوية حول . هذا الموضوع، خاصة الموجهة نحو الأفراد للتصدي بشكل حازم لما قد يتعرضون له من مشاكل

أضف إلى ذلك، أن من أسباب تزايد مخاطر هذه الطريقة سهولة تعلمها والقيام بها، ويمكن أن يتم ممارستها من أي موقع في العالم، إلى جانب سرعة تنفيذ عملية الاحتيال، وتزايد أعداد مرتكبيها، خاصة مع ظهور الأزمة العالمية . وتداعياتها

تجربة عملية

وقال لهذا الغرض حرصت الجامعة الأمريكية في الشارقة على دراسة مدى الوعي لدى الطلاب والموظفين العاملين لديها، حول إمكانية تعرضهم للتحايل، من خلال الطرق التي يتبعها القراصنة، لإيجاد الحلول البديلة، حيث قمنا بتنفيذ أحد أساليب الخدع المستخدمة على أحد صفحات الموقع الإلكتروني للجامعة، والتي تخص الطلاب والموظفين وتتضمن معلومات تهمهم، بعد أخذ الموافقات المسبقة من إدارة الجامعة، وقام بأداء التجربة 3 طلاب يدرسون مادة . أمن المعلومات في الجامعة، وتعتبر هذه التجربة الأولى من نوعها في الإمارات

وقمنا بمراقبة أعداد الطلبة والموظفين، الذين تجاوبوا مع الإيميلات الوهمية التي أرسلناها لهم، وكانوا بصدد تحديث . بياناتهم حسبما طلبنا منهم، دون طلب كلمة السر، بل اقتصر الأمر على تغيير الاسم فقط

وبالفعل تم إرسال الإيميل إلى 5 آلاف طالب وطالبة على مقاعد الدراسة، و5 آخرين تخرجوا، بالإضافة إلى ألف مدرس وموظف يعملون في الجامعة، وتبين أن 950 شخصاً وقعوا في الفخ بنسبة 6 .8% من العدد الإجمالي، وكان 96 % منهم طلاباً، قد تجاوبوا مع طلبنا المزيف، فيما كانت النسبة متساوية تقريباً لكلا الجنسين، وكانت موزعة على جميع . المراحل الدراسية للطلبة

وهذه الخطوة تأتي بالدرجة الأولى لتحصين الطلبة وزيادة وعيهم بالمخاطر التي قد يتعرضون لها، وعدم الانسياق وراء

. مثل هذه الإيميلات وتدعيم أمنهم المعلوماتي، لتلافي الوقوع فريسة سهلة في يد العابثين والمحتالين

وأضاف إنه بعد الانتهاء من أداء التجربة، قمنا بحملة توعية شاملة للطلبة والموظفين عن الموضوع، كما أننا ندرس مادة عن أمن المعلومات للطلبة، إلى جانب إنشاء موقع تعليمي يشرح الخطوات التي يجب على الطالب أن يتنبه إليها قبل إدخال أي بيانات لمعرفة URL عن طرائق الاحتيال المتعددة، من ضمنها التأكد من عنوان الموقع الإلكتروني . مصداقية الموقع من زيفه

كما أن قسم تقنية المعلومات بالجامعة يقوم بصفة دورية بإرسال إيميلات توعوية للطلبة لأخذ الحيطة والحذر عند . التعامل مع الايملات التي ترد إليهم

وفي ذات الإطار أكدت زينب ناصر ـ ربة بيت ـ أنها كانت خلال فترة دراستها في الجامعة، وهي تتصفح بريدها الإلكتروني، تتعرض لإيميلات من قبل أشخاص وجهات غريبة وغامضة بغرض الدعوة للتعارف، ما اضطرني إلى عمل . خصوصية على إيميلي لاستقبال الإيميلات، التي تأتي من قبل أصدقائي والمعروفين لدي فقط

وقالت الطالبة آمنة الأزهر، التي تدرس في كلية الهندسة الكهربائية في الجامعة الأمريكية بالشارقة: إنها سمعت عن الذي يتبعه المخربون للولوج إلى الحواسيب الشخصية وإجراء عمليات التخريب بشتى أشكالها، fishing أسلوب ال . ولكني حينها لم أبد أي اهتمام بها، ولم أكن أعي مدى خطورتها

وقامت الجامعة أخيراً بإجراء تجربة لمعرفة مدى إطلاع الطلاب والموظفين العاملين فيها، في حال تعرضوا لهجمة من قبل المخربين، حيث عمدت الجهة المنفذة إلى إجراء تجربة وهمية عبر استخدام موقع شبيه بصفحة معينة على موقع الجامعة، وبالفعل فوجئنا بوجود طلب من الجامعة على الموقع بتحديث بياناتنا، ولم أكن أدرك أنه عبارة عن فخ، وأن الموقع لم يكن للجامعة بل شبيهاً له، وحينها تتبعت التعليمات المطلوبة مني، ووافقت على تحديث بياناتي دون أن أتأكد . التي من خلالها نستطيع التحقق من أن الموقع صادق وليس وهمياً url من ال

قوانين رادعة

لبنى عبدالوهاب طالبة تدرس تخصص الاتصال في جامعة الشارقة، رأت أن مسألة الجرائم الإلكترونية باتت خطراً يهدد الجميع، سواء كانوا أفراداً أم مؤسسات، وبالتالي أصبح لا بد من وضع مزيد من القوانين الرادعة وآليات الضبط والرقابة على أولئك الذين ينفذونها، خاصة أن عالم الإنترنت آخذ في اتساع مداه، ويزداد عدد مستخدميه يوماً بعد آخر، . وبالتالي زيادة عدد الذين تعرضوا أو سيتعرضو لأحد أنواع الجرائم الإلكترونية

لقد تعرضت شخصياً لإحدى هذه الجرائم، ولكن كانت على نطاق ضيق، من خلال إيميل غير موثوق مصدره، ومعنون باسم شركة أجنبية، يشير إلى أني ربحت مبلغاً من المال، وبالتالي دفعني فضولي إلى اتباع الخطوات المذكورة في الإيميل، وعندها تنبهت إلى أني قد وقعت في شرك مصيدة حبكت لي، من خلال وجود فيروس هاجم جهازي وقام بتعطيله بشكل نهائي، فتوجهت إلى أحد فنيي الحاسوب لمعرفة ما حل به، فأكد لي الفني أنه بحاجة إلى قطعة معينة . باهظة الثمن، نتيجة تعطلها بفعل الفيروس الذي تم إرساله عبر الايميل الغريب

وذكرت رناد الريماوي ـ موظفة ـ أنها تنبهت لهذه القضية ولديها خلفية جيدة نوعاً ما عنها، نتيجة خبرات تراكمية سابقة، مؤكدة انه بامكان الشخص الذي يرسل إيميلاً إلى بريدك الإلكتروني أن يهاجمك لحظة الرد عليه، من خلال

التعرف إلى أرقامك السرية، وبالتالي يتاح له ارتكاب ما يحلو له من جرائم متنوعة، ولذلك كنت أرفض أية إيميلات تأتيني ولا أتعامل معها، كما أن استخدام المواقع المختلفة غير الموثوقة يسهِّل على الهاكرز عملية مهاجمتك .

ويجب على الشخص أخذ الحيطة والحذر من خلال اتباع خطوات معينة منها، تغيير البرنامج المضاد للفيروسات باستمرار، وعدم التعامل وفتح مواقع غير مضمونة، بالإضافة إلى تجنب الاحتفاظ بأشياء شخصية ومعلومات مهمة على الجهاز، وتبقى الثقافة المعلوماتية أهم الأمور للحيلولة دون الوقوع في مصيدة هؤلاء المخربين .

التصيد الإلكتروني

إلى ذلك أكدت هيئة تنظيم الاتصالات في الدولة، أن الجرائم الإلكترونية التي ترد متنوعة، حيث يتم تبليغ الفريق العامل لدينا عن جرائم إلكترونية مختلفة في طبيعتها تشمل التصيد، واختراق الحسابات الإلكترونية وأجهزة الحاسب الآلي، فضلاً عن إصابة الأجهزة بالبرامج الخبيثة، وسرقة المعلومات الحساسة، وتشويه المواقع، وغيرها .

ويقوم الفريق بتوفير الاستشارات والحلول وطرق الوقاية المناسبة للمنتسبين لمعالجة الجرائم الإلكترونية والحماية منها .

وقالت الهيئة، إن نسبة هجمات التصيد الإلكتروني تُعد أعلى نسبة يتم الإبلاغ عنها، وهي في ازدياد بسبب نقص الوعي الأمني الإلكتروني لدى مستخدمي الأجهزة الإلكترونية على شبكة الإنترنت من خدع الهندسة الاجتماعية، حيث يقوم مجرم الإنترنت بانتحال شخصية فرد أو جهة يثق بها المستخدم مثل المصرف الذي يتعامل معه بهدف سرقة معلوماته السرية .

وذكرت، أن مهام فريق العمل يتلخص في تعزيز الوعي الأمني لدى الجمهور عن طريق إطلاق حملات أمنية توعوية إلكترونية مختلفة، وحماية البنية التحتية المعلوماتية في دولة الإمارات، عن طريق خدمات يقدمها الفريق للمنتسبين، مثل كشف الثغرات الأمنية للشبكات، ومراقبة الشبكات، وتوفير أفضل الممارسات في تكوين السياسات والمعايير والإجراءات الأمنية، وتحذير المنتسبين عن أحدث المخاطر الأمنية عن طريق نظم إنذار مبكر، وكذلك يعمل مركز الاستجابة للفريق، كنقطة تنسيق لمعالجة جميع الهجمات الإلكترونية، التي يتم التبليغ عنها .

وأوضحت الهيئة، أن الجرائم الإلكترونية تختلف في طبيعتها، فمدى خطورتها وتأثيرها يعتمد على تواجد الثغرات الأمنية واحتمالية اختراقها، ويمكن تحديد أضرار الهجمة بعد تحليلها، مثل الأضرار المالية، وأضرار سلبية على سمعة الجهة المتأثرة، فعلى سبيل المثال، فإن هجمات التصيد على القطاع المصرفي تتسبب في خسائر مالية وتفشي البرامج الخبيثة، التي قد تؤدي إلى سرقة المعلومات الحساسة، مما قد يسيئ إلى سمعة الجهة المتأثرة، وتؤدي بالتالي إلى فقدان ثقة المتعاملين، فيما يتم متابعة هذه الهجمات بالعمل على توفير الحلول المناسبة وطرق الوقاية ومراقبة الشبكات لتفادي تكرار حدوثها .

أمجد حمدان يعمل مدرساً لمادة الحاسوب في معهد القدس في عجمان، أوضح أنه من خلال الدورات التدريبية التي يعقدها المركز، وجد أن هناك نسبة كبيرة من الطلبة، سواء الذين هم على مقاعد الدراسة أم موظفون يجهلون حقيقة الأخطار والطرق التي بالامكان أن يتعرضوا لها أثناء استخدامهم للتقنيات الحديثة، ومن ضمنها الشبكة العنكبوتية، الأمر الذي يؤكد أنهم يشكلون هدفاً سهلاً للمخربين .

أكثر الأساليب شيوعاً

أكد الدكتور فادي علول، أن طرق الهاكرز في الولوج إلى الحواسيب متعددة، وأبرزها حالياً أسلوب صيد مستخدمي الحاسوب phishing من خلال قيام المخربين بإرسال إيميلات مزيفة بشكل عشوائي إلى مستخدمي الإنترنت، تبلغهم أنه تم اختراق حساباتهم أو يجب تحديث بياناتهم، ويحتوي الإيميل على وصلة يطلب من المستخدم الضغط عليها، فتأخذه إلى موقع شبيه بالموقع الأصلي للمؤسسة المعنية، ولكنه في الحقيقة وهمي ومزيف، استخدمه المخرب ليوهم الضحية بأنه الموقع الأصلي، لكي يدخل إليه باستخدام كلمة السر الأصلية، وبمجرد إدخال البيانات يتم تحويل الضحية إلى الموقع الأصلي، حتى لا يتسنى له اكتشاف أنه وقع ضحية عملية نصب إلكترونية، وبنفس الوقت يكون المخرب قد تمكن من الاستيلاء على كلمة السر الخاصة بالبنك، أو المؤسسة، أو ما شابه ويستخدمها لاحقاً لتنفيذ مآربه الشخصية .

تنامي الإنترنت

يشير أحد المواقع المعروفة على الشبكة العنكبوتية إلى أن إحدى الدراسات عن عدد مستخدمي الشبكة العنكبوتية تؤكد أن العدد قد ارتفع ووصل نحو 63 مليون مستخدم، ويشكل العرب 2 .3% من النسبة الإجمالية، وأنها آخذة في الازدياد، حيث إنه منذ عام 2000 وحتى العام الجاري كانت نسبة النمو في استخدامها في العالم العربي 1825%، في المقابل كانت نسبة الزيادة في باقي دول العالم 432% . وبالتالي فإن الزيادة المضطردة في أعداد المستخدمين باتت تجذب المخربين، الأمر الذي يشكل هاجساً وقلقاً، نظراً لعدم وجود التوعية الأمنية الكافية، وفي المقابل هناك نمو سريع ومتزايد في عدد مستخدمي الشبكة العنكبوتية، ومن مختلف الأعمار والفئات في العالم العربي .

طرق الوقاية

أوضحت هيئة تنظيم الاتصالات، الطرق التي يجب أن يتبعها الجمهور لتفادي وقوعهم في براثن هذه الجرائم، وذلك من خلال، تحديث جميع البرامج وأنظمة التشغيل واستخدام برنامج محدث مضاد للفيروسات، بالإضافة إلى اتباع أفضل الممارسات الأمنية الإلكترونية، مثل استخدام كلمات مرور قوية، ومسح مرفقات البريد الإلكتروني ببرنامج مضاد للفيروسات محدث قبل فتحه، إلى جانب عدم توفير معلوماتهم الشخصية للغرباء على الإنترنت .

وأن العقوبات التي تفرض تستند إلى القانون الاتحادي رقم (2) لسنة 2006، في شأن مكافحة جرائم تقنية المعلومات، وأنه بإمكان الجمهور الاطلاع على برامج التوعية الأمنية للفريق على الرابط التالي:

http://www.aecert.ae/security-ar.php