العدد 1 يوليو 2017

إشارات
Esharat

لفضـــاء إلكـــتروني آمـــن

صاحب السمو الشيخ محمد بن راشد ينشئ مركز دبي للأمن الإلكتروني لجعل دبي أأمن مدن العالم إلكترونياً

المبتكر أحمد الحمادي الأول عربياً

10 نصائح للحماية من الهجمات الإلكترونية

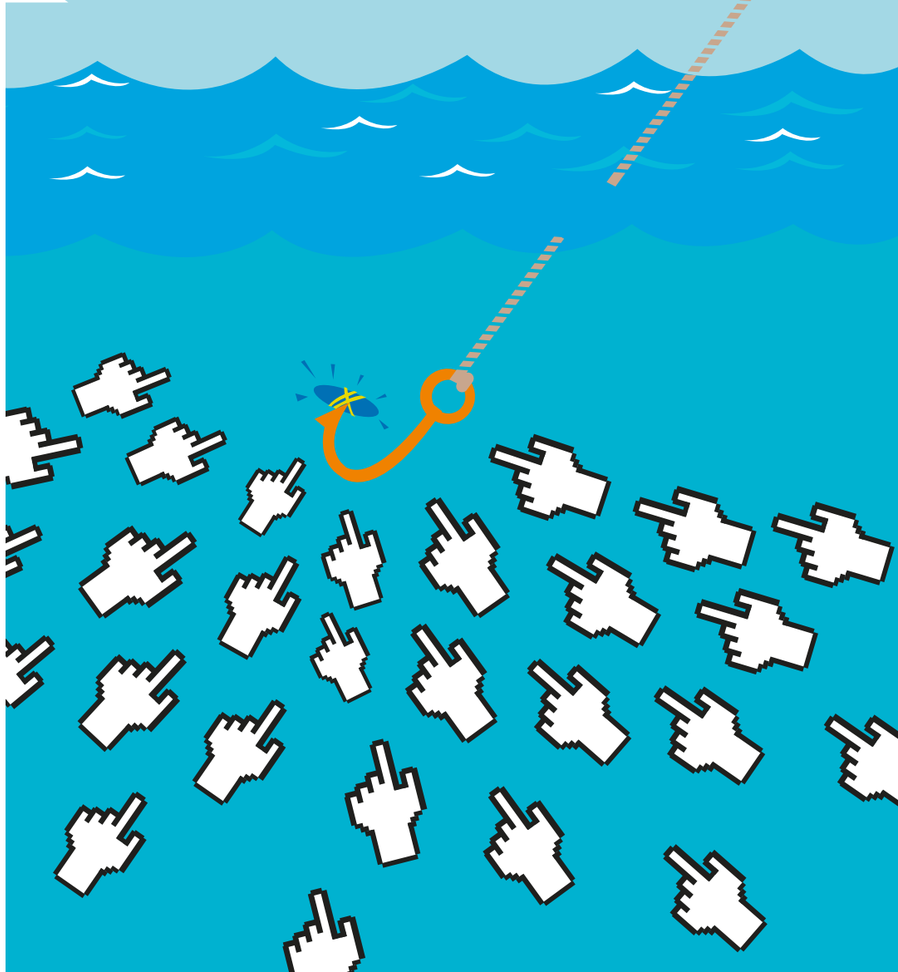
عامر شرف: "هدفنا أن تتمتع دبي بفضاء إلكتروني حصين"

كيفين ميتنيك "ليس هناك شيئ لا يمكن اختراقه!"

احتيال ثم نقرة فاختراق!

قراصنة الفضاء الإلكتروني يسعون للحصول على بياناتك الشخصية ويجربون كل الحيل للوصول إلى معلوماتك السرية كأرقام الحسابات المصرفية وبطاقات الائتمان والصور والمستندات الخاصة. وكثير من أشكال الاحتيال قد تكون على شكل رابط إلكتروني، لذلك لا تنقر إلا على الروابط الموثوقة فالحاسوب المخترق يشكل تهديداً لك وللآخرين!

كن حذراً، فكر ثم انقر!



مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

مجلة متخصصة بالأمن الإلكتروني والتكنولوجيا، نصف سنوية، تصدر عن مركز دبي للأمن الإلكتروني

المشرف العام
يوسف حمد الشيباني

مدير التحرير
عامر شرف

سكرتيرة التحرير:
شيخة عيسى

التحرير والتصميم

سفن جي ميديا للاستشارات

هيئة التحرير
أماني أبوسيدو
دان شارتر
أحمد مرسال

التصميم الفني
سري إي إس
أوس رحال

الرسم
برايِن رايس

للاتصال بالمجلة
مركز دبي للأمن الإلكتروني: 2538 251 4 971+
سفن جي ميديا للاستشارات: 5427 449 4 971+
info@desc.gov.ae
info@7gmedia.com

جميع المعلومات المنشورة في مجلة "إشارات" هي لأهداف إعلامية فقط. وبالرغم من كل الجهود المبذولة لتحري الصحة والدقة، إلا أن "إشارات" لا تتحمل المسؤولية عن أي خطأ أو إغفال ورد في المجلة.

جميع حقوق الطبع محفوظة 2017.

تقرأ في هذا العدد

الإشارة الأولى.. نحو فضاء إلكتروني آمن!

خلال السنوات الثلاثين الماضية، تقلص حجم العالم مرتين، فأصبح في المرة الأولى "قرية صغيرة" كما كان يقول خبراء التكنولوجيا والاتصال، ثم أصبح في المرة الثانية جهازاً إلكترونياً صغيراً بحجم قبضة اليد. فقد أصبح العالم الإلكتروني متداخلاً ومترابطاً ووثيق الصلة بالعالم الحقيقي، نطل عليه من خلال شاشة صغيرة هي شاشة الهاتف الذكي، كما أصبحت التعاملات الإلكترونية ذات أهمية جوهرية بالنسبة إلى الخدمات الحكومية والخاصة. فأي معاملة أو وثيقة نحتاج إليها صرنا نطلبها عن طريق الخدمات الذكية، كما أصبحنا نجري حجوزات السفر والطيران والفنادق عبر الهاتف الذكي، ونشتري من خلاله أيضاً السلع ونحصل على الخدمات. وبالتالي، أصبح الدفع عبر الشبكة مسألة اعتيادية، وأصبحت التجارة الإلكترونية وإنجاز الأعمال وطلب الخدمات إلكترونياً من حقائق عالمنا الجديد. وباتت المواقع الاجتماعية هي مفتاح علاقاتنا وسلوكياتنا.

إن هذا التحول جعل حياتنا أسهل، لكنه حمل معه تحديات جديدة. فمع المدن الذكية، والحوسبة السحابية، وإنترنت الأشياء، حمل إلينا هذا العالم الاحتيال الإلكتروني، وعصابات الإجرام المنظم، وبرامج التجسس، وانتحال الشخصية. وعلى الرغم من الطابع الافتراضي لهذه المخاطر حيث تجري وراء شاشة الحاسوب أو الهاتف الذكي، ولكن وقع تأثيرها حقيقي، وتحمل تهديدات جدية قد تطال حياتنا الاجتماعية وحساباتنا المصرفية وأمننا الشخصي، وتهدد عائلاتنا وأطفالنا وكل من نحب.

إن إقامة حيز إلكتروني آمن وموثوق هو سبيلنا الوحيد للإبحار بأمان في هذا العالم الجديد. ويتولى مركز دبي للأمن الإلكتروني التأكد من إقامة جدار يحمي مؤسساتنا وشركاتنا ومدينتنا، إلا أن تعاظم التحديات المطروحة في دبي، المدينة التي تتطلع لأن تصبح الأكثر ذكاء وابتكاراً في العالم، بات يستلزم تعاوناً وتضافراً ما بين القطاع الحكومي وبين المؤسسات والشركات ومراكز القرار والجامعات والأفراد، بغية تشكيل درع موثوق لا ينفذ منه الاحتيال الإلكتروني ولا الجريمة المنظمة. بناء على ذلك، يأتي إصدار مجلة "إشارات"، بهدف رفع وعي الأفراد والشركات وكل المعنيين بأساسيات التعامل التجاري والاجتماعي عبر الإنترنت، وإقامة شبكة أمان يكون فيها كل فرد مدركاً لحقوقه ولواجباته في الدفاع عن أمنه الشخصي الإلكتروني، بما يحصن أمن المدينة بأسرها.

لقد أطلقنا أولى إشاراتنا نحو فضاء إلكتروني آمن.

يوسف الشيباني
المدير التنفيذي
مركز دبي للأمن الإلكتروني

صاحب السمو الشيخ محمد بن راشد آل مكتوم ينشئ مركز دبي للأمن الإلكتروني لتعزيز مكانة دبي كمدينة عالمية رائدة في الأمان والسلامة والابتكار

أصدر صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، قانوناً بإنشاء مركز دبي للأمن الإلكتروني في عام 2014. بهدف جعل دبي أأمن مدن العالم إلكترونياً وتطوير استخدام الوسائل اللازمة في مجال أمن المعلومات ووضع المعايير الكفيلة بتوفير الأمن الإلكتروني في الإمارة والإشراف على تنفيذها وإعداد خطة استراتيجية لمواجهة أي مخاطر أو تهديدات أو اعتداءات على المعلومات.

تعدّ خطة دبي 2021 ترجمةً لرؤية صاحب السمو الشيخ محمد بن راشد، وهي الخطة التي تتبناها الحكومة لتحقيق أهداف الإمارة على مدى السنوات الخمس القادمة، وتشمل الخطة محورين أساسيين يتمثلان في جعل دبي المدينة الأكثر أمناً للعيش والإقامة والعمل، وبناء مدينة ذكية ومتكاملة ومتصلة؛ ومن هذا المنطلق يتبنى مركز دبي للأمن الإلكتروني خطة استراتيجية للمساهمة في تحقيق هذين الهدفين، بالإضافة إلى مكافحة تهديدات الأمن الإلكتروني ومواجهة الاعتداء على المعلومات وكافة أشكال الجرائم الإلكترونية.

وتهدف الخطة الاستراتيجية التي أطلقها المركز إلى توفير الحماية المتكاملة ضد كافة مخاطر الأمن الإلكتروني في دبي، ودعم الابتكار في الفضاء الإلكتروني ونمو الإمارة وازدهارها الاقتصادي، وقد تمّ تحديد مدّة خمس سنوات كجدول زمني لتحقيق أهداف هذه الاستراتيجية.

ويتعاون مركز دبي للأمن الإلكتروني مع كافة الجهات الحكومية في الإمارة لضمان رفع مستوى الوعي بالأمن الإلكتروني، واتخاذ التدابير الاحتياطية اللازمة، وموائمة أنظمة أمن المعلومات مع المعايير المتبعة دولياً، ويتطلع المركز إلى مبدأ التعاون من كافة الجهات الحكومية لتحقيق مختلف الأهداف التي حددتها الخطة الاستراتيجية تحقيقاً للهدف الأسمى ألا وهو تعزيز مكانة دبي كمدينة عالمية رائدة في مجال الأمن الإلكتروني، وتستند الخطة على تنفيذ خمسة محاور رئيسية تتمثل في ما يلي:

مجتمع واعٍ بمخاطر الأمن الإلكتروني

يهدف المركز من خلال هذا المحور إلى ضمان وجود كادر يتمتع بالمعرفة الكافية بالأمن الإلكتروني لتدريب الأفراد والموظفين داخل المؤسسات العامة والخاصة بهدف ترسيخ معرفتهم بالأمن الإلكتروني، وتوفير الدعم الكامل لهم. إن بناء مجتمع يعي ويدرك مخاطر الأمن الإلكتروني يسهم في تعزيز من مكانة دبي كمدينة رائدة في مجال الأمن الإلكتروني، إذ إن معرفة أحدث أنواع التهديدات الإلكترونية وتعلم طرق مواجهتها يعدّ عاملاً أساسياً لتحقيق أعلى مستويات الأمن الإلكتروني في المدينة.

الابتكار

يعمل المركز على تعزيز مشاريع البحث العلمي والتطوير في مجال الأمن الإلكتروني بهدف إنشاء فضاء إلكتروني يتّسم بالحريّة والعدل والأمن ويشجّع الابتكار في دبي.

أمن الفضاء الإلكتروني

يضع المركز مجموعة من الضوابط الأمنية لحماية سرية البيانات ومصداقيّتها للأفراد والمؤسسات العامة والخاصة في دبي، ويقوم بتطبيق وتطوير معايير نظام إدارة أمن المعلومات (ISMS)، والتأكد من أن الإدارات التنفيذية العليا تدرك أهمية الأمن الإلكتروني.

المرونة في الفضاء الإلكتروني

يعدّ مركز دبي للأمن الإلكتروني الجهة الأولى المسؤولة عن مواجهة أي تهديدات أو هجمات إلكترونية داخل المؤسسات الحكومية، حيث يعمل على ضمان استمرارية الأعمال وأنظمة تكنولوجيا المعلومات وتوفّرها داخل المؤسسات في حالة حدوث أي هجمات إلكترونية أو مشاكل ذات صلة، بالإضافة إلى توفير منصّة لتبادل المعلومات والدعم في إدارة الحوادث الخاصّة بالأمن الإلكتروني والآليات المتطورة لمكافحة التهديدات.

التعاون الدولي والإقليمي والوطني

يهدف مركز دبي للأمن الإلكتروني إلى قيادة إمارة دبي نحو تأسيس شراكات وطنية وعالمية بهدف ترسيخ أطر التعاون مع القطاعات المختلفة على المستويين العالمي والمحلي لمواجهة التهديدات والمخاطر في مجال الفضاء الإلكتروني، ويخطط المركز إلى اعتماد نظام أمن المعلومات بناءً على منهجيات وتجارب دولية رائدة.

ويعد التعاون الوطني واحداً من المحاور الرئيسية لرؤية صاحب السمو الشيخ محمد بن راشد آل مكتوم، التي تقر بأن العنصر الأساسي لبناء دولة ومدينة قادرة على التنافس مع البلدان الرائدة حول العالم يعتمد كلياً على الكفاءات ومنهج العمل الذي يتبعه العاملون داخل المؤسسات الحكومية.

> استراتيجية مركز دبي للأمن الإلكتروني تهدف إلى توفير الحماية المتكاملة ضد مخاطر الأمن الإلكتروني، ودعم الابتكار.. وأن تتحقق في 5 سنوات

صاحب السمو الشيخ محمد بن راشد يطلق خطة دبي الاستراتيجية للأمن الإلكتروني

> الأمن المعلوماتي بات يمثل مطلباً مُلحاً في وقتنا الحالي الذي أضحى فيه العالم أكثر ترابطاً إلكترونياً

صاحب السمو الشيخ
محمد بن راشد آل مكتوم

أطلق صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، "خطة دبي الاستراتيجية للأمن الإلكتروني" تعزيزاً لمكانة دبي كمدينة عالمية رائدة في الابتكار والسلامة والأمن.

حضر إطلاق "خطة دبي الاستراتيجية للأمن الالكتروني" سمو الشيخ حمدان بن محمد بن راشد آل مكتوم، ولي عهد دبي رئيس المجلس التنفيذي، وسمو الشيخ أحمد بن محمد آل مكتوم، رئيس مؤسسة محمد بن راشد للمعرفة، وسمو الشيخ منصور بن محمد بن راشد آل مكتوم، ومعالي محمد عبدالله القرقاوي، وزير شؤون مجلس الوزراء والمستقبل، ومعالي الفريق ضاحي خلفان تميم، نائب رئيس الشرطة والأمن العام في دبي، وسعادة اللواء طلال بالهول الفلاسي، وعدد من القيادات الحكومية في دبي.

وأكد صاحب السمو الشيخ محمد بن راشد آل مكتوم أن دولة الإمارات حققت مكانة متقدمة في مجال الأمن والأمان إقليمياً وعالمياً بشهادة التقارير الدولية، في ضوء الجهود الحثيثة التي تبذلها الحكومة على الصعيدين الاتحادي والمحلي، لاستكمال كافة الركائز التي تكفل أمن وسلامة المجتمع، بما يضمن نجاح أهداف التنمية.

وشدد سموه على أن الأمن المعلوماتي بات يمثل مطلباً مُلحاً في وقتنا الحالي الذي أضحى فيه العالم أكثر ترابطاً إلكترونياً مع الانتشار الكبير للتقنيات الذكية والتي باتت تمثل ركيزة مهمة من ركائز العمل في مختلف الميادين والتخصصات، ما يوجب الاستعداد وبقوة لكل ما تحمله التكنولوجيا من تحديات إلى جانب ما توفره من فرص.

وقال سموه: "اختارت دولة الإمارات ومنذ قيامها طريق التميز والابداع لتسلكه في سبيل تحقيق رفعة شعبها وازدهار مستقبله، واليوم نطلق خطة دبي الاستراتيجية للأمن الالكتروني لنضيف إنجازاً جديداً إلى سلسلة الانجازات الحكومية لنثبت للعالم أن التحديات مهما كان حجمها لم تثنينا يوماً عن استكمال مسيرة التميز"، وأكد سموه على أهمية توحيد جهود المؤسسات الحكومية والخاصة والأفراد من أجل توفير فضاء إلكتروني آمن يرسخ من مكانة دبي بين أكثر مدن العالم أماناً في الفضاء الإلكتروني.

وتهدف الخطة الاستراتيجية للأمن الالكتروني إلى توفير الحماية المتكاملة ضد مخاطر الأمن الالكتروني، ودعم الابتكار في الفضاء الالكتروني مما يعزز نمو الامارة وازدهارها الاقتصادي.

ترتكز خطة دبي 2021 على محورين أساسيين يهدفان إلى جعل دبي المدينة الأكثر أمناً للإقامة والعمل، وبناء مدينة ذكية ومتكاملة ومتصلة؛ ومن هذا المنطلق تهدف الخطة الاستراتيجية للأمن الإلكتروني إلى المساهمة في تحقيق هذين الهدفين، بالإضافة إلى مكافحة تهديدات الأمن الإلكتروني ومواجهة الاعتداء على المعلومات وكافة أشكال الجرائم الإلكترونية. وتستند خطة دبي الاستراتيجية للأمن الالكتروني على تنفيذ خمسة محاور رئيسية هي:

مجتمع واعٍ بمخاطر الأمن الإلكتروني: زيادة وعي المجتمع بأهمية الأمن الإلكتروني ومخاطر الجرائم الإلكترونية ومساعدته في تطبيق الوسائل المناسبة لتقليل مخاطر التعرض لهذا النوع من الجرائم.

الابتكار: تحفيز الابتكار والبحث العلمي في مجال الأمن الإلكتروني.

أمن الفضاء الالكتروني: بناء فضاء إلكتروني آمن بوضع ضوابط لحماية سرية البيانات ومصداقيّتها وتوافرها وخصوصيتها.

المرونة في الفضاء الالكتروني: ضمان استمرارية أنظمة تكنولوجيا المعلومات وتوفرها في حالة حدوث أي هجمات إلكترونية.

التعاون المحلي والدولي: تأسيس شراكات محلية وعالمية بهدف ترسيخ أطر التعاون لمواجهة التهديدات والمخاطر في مجال الفضاء الالكتروني.

عامر شرف: "هدفنا أن تتمتع دبي بفضاء إلكتروني حصين أكثر أماناً وبدأنا رفع وعي المؤسسات والأفراد"

عامر شرف مدير إدارة التعاون ودعم الامتثال في مركز دبي للأمن الإلكتروني. يحمل درجة البكالوريوس في علوم الحاسوب والماجستير في أنظمة المعلومات الإلكترونية من جامعة بوسطن في الولايات المتحدة، قبل أن ينتقل شرف إلى وظيفته الحالية، عمل في شرطة دبي في إدارة تكنولوجيا المعلومات. ويتطلع حالياً من خلال مهامه الوظيفية إلى أن تتخذ كل المؤسسات الحكومية والشركات الخاصة في دبي أعلى درجات الحرص والتدابير الأمنية لحماية أنظمتها الإلكترونية لتكون في مأمن حصين من أي خطر إلكتروني، وأن يتحلى الأفراد في دبي بالوعي الأمني الإلكتروني العالي.

يتولى فريق إدارة التعاون ودعم الامتثال في مركز دبي للأمن الإلكتروني مسؤولية وضع سياسات أمن المعلومات، التي ستصبح إجراءات وقائية تنظيمية أساسية تلتزم بها المنشآت الحكومية في إمارة دبي، ويرتكز دور الإدارة على تحقيق رؤية مركز دبي للأمن الإلكتروني، الرامية إلى جعل دبي أكثر مدن العالم أماناً على الصعيد الإلكتروني. مجلة "إشارات" في عددها الأول حظيت بفرصة لقاء المهندس عامر شرف الذي ألقى الضوء على مهام المركز، وأوضح الأسباب التي جعلت من أمن الفضاء الإلكتروني مسألة أساسية وعلى قائمة الأولويات في دولة الإمارات، وفي ما يلي نص المقابلة.

إشارات: حدثنا عن مركز دبي للأمن الإلكتروني وأهدافه الاستراتيجية؟

شرف: "تأسّس مركز دبي للأمن الإلكتروني في العام 2014 عندما أصدر صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة، رئيس مجلس الوزراء رعاه الله بصفته حاكم دبي، القانون رقم 11 لسنة 2014 بإنشاء "مركز دبي للأمن الإلكتروني"، وتتركز مهام المركز حول جعل دبي من المدن الأكثر أماناً في العالم على الصعيد الإلكتروني. فدورنا يقوم على حماية المعلومات وأنظمة المعلومات الحكومية، وطرق حفظ وتبادل المعلومات وتشاركها بين الجهات الحكومية، كما يتولى المركز العديد من المهام من أجل تحقيق هذا الهدف نفسه. كذلك، يسعى المركز إلى تطوير الإجراءات الضرورية لتوفير أعلى مستويات الأمن الإلكتروني. كما نقوم في المركز بتطوير الوسائل والحلول بهدف تعزيز الأمن الإلكتروني في دبي، ومن بينها الأدوات التي تعزز أمن الشبكات. إن أدوات مثل Security Incident Event Management وتعرف اختصاراً باسم (SIEM) تعتبر مثالاً جيداً على ذلك، حيث تستخدم في قياس معدل حركة البيانات ورصد أي حالات غير طبيعية لتدفقها، لتكشف بالتالي عن أي هجمات محتملة".

إشارات: كيف يحمي المركز شبكات المعلومات الحكومية؟

شرف: "هناك طرق مختلفة نحمي من خلالها شبكات المعلومات الحكومية، منها مساعدة الدوائر الحكومية على تأسيس مركز لعمليات الأمن الإلكتروني، وهي خطوة ضرورية تكفل للجهة المعنية متابعة الأنشطة على الشبكة وتتبع أي نشاط أو سلوك غير طبيعي في حركة البيانات. المركز يقدم أيضاً النصائح لكافة الدوائر الحكومية من خلال تشارك البيانات ذات الصلة معها، لتعزيز قدرتها على حماية نفسها من التهديدات الآنية. ويسعى المركز إلى تقديم التدريب للكوادر الرئيسية في كل دائرة حكومية، على أن تتولى تلك الكوادر تدريب باقي الموظفين في الدائرة".

> يتطلع مركز دبي للأمن الإلكتروني إلى تطوير كافة الوسائل الضرورية لتأمين أعلى مستويات الأمان الإلكتروني

نعمل في المركز بموجب سياسة أمن المعلومات الملزمة لكافة المؤسسات الحكومية

إشارات: ما الإجراءات التي تتخذونها في حال بروز تهديد إلكتروني لجهة حكومية ما؟

شرف: "إذا لاحظنا، أو لاحظت المؤسسة الحكومية، بروز تهديد محدد، فإن أول ما ينبغي فعله هو عزل المشكلة، واتخاذ تدابير احترازية للسيطرة على أي اختراق يحدث. الخطوة التالية هي دراسة السبب الذي سهل الاختراق، والتأكد من ضمان عدم حدوثه في مكان آخر.

"من المهم في هذا المجال إبلاغ الإدارة ومركز دبي للأمن الإلكتروني بالأمر. بعدها نقوم بتقييم طبيعة التهديد الذي واجهناه، ونتشارك الدروس والخلاصات والتجارب التي تعلمناها مع بقية الدوائر، بهدف مساعدتها على حماية نفسها إذا واجهت تهديداً مماثلاً.

"بالرغم من علمنا أن تحقيق مستوى أمان بنسبة مئة بالمئة أمر غير ممكن في عالم الأمن الإلكتروني، يجب علينا أن نعمل دائماً لرصد أي أنشطة مبهمة داخل شبكاتنا، وإيقافها قبل أن تنتشر، وهناك عدة تقنيات تتيح لنا مراقبة الأنشطة المشتبه بها لحظة بلحظة، واتخاذ الإجراءات اللازمة سريعاً لعزل التهديدات".

إشارات: ما نوع المعلومات التي يحاول المخترق الوصول إليها داخل المؤسّسة الحكومية؟

شرف: "المعلومات الحساسة والشخصية والخاصة يجب تصنيفها على هذا الأساس، وضمان حمايتها من أي اختراق أو وصول غير مرخص إليها. بالنسبة إلى الشبكات الحكومية، يستهدف القراصنة قوائم الموظفين والعناوين، والرسائل الإلكترونية، وكلمات المرور، وأرقام بطاقات الهوية على سبيل المثال لا الحصر، وهذه المعلومات قد تجعل الموظفين عرضة للسرقة أو أي جرائم خطيرة أخرى. في حالات عدة يستهدف القراصنة التأثير سلباً في سمعة الجهة المستهدفة.

"يتحقق ذلك عبر الكشف عن بيانات شخصية أو تعطيل مواقع إلكترونية بالشكل الذي يتسبب بخسائر مالية. وقد تكون منطلقات القراصنة عدوانية وتخريبية أحياناً، عن طريق شل الخدمات التي تقدمها الجهة المستهدفة، من خلال محو البيانات، كما رأينا في هجوم فيروس "شامون".

إشارات: ما هي مهام عملك بالتحديد؟

شرف: "مهامي تنقسم إلى جزءين. الأول يتلخص في مراقبة ممارسات الامتثال، وهذا يعني أننا نعمل جنباً إلى جنب مع المؤسسات الحكومية المختلفة لمساعدتها على الالتزام بقواعد الامتثال والتوافق مع الإجراءات الصادرة عن المركز.

"ودعني أبدأ بالسياسات وهو موضوع الساعة: "سياسة أمن المعلومات"، هي قواعد ملزمة لكافة المؤسسات الحكومية في دبي منذ العام 2012. دورنا هو الإشراف على الالتزام بتطبيق اللوائح التي تضمها هذه السياسة، كما نقوم بتعزيز وتحديث وتطوير اللوائح حتى تواكب أحدث التطورات في مجال الأمن الإلكتروني، نقوم بعدها بتوزيعها على كافة الدوائر والمؤسسات الحكومية كي تعمل بموجبها وتتبناها.

"كذلك نضع سياسات جديدة للإشراف والحفاظ على سلامة أمن المعلومات، وبعد أن يتم توزيعها على المؤسسات الحكومية، يبدأ فريق المراجعة في مركزنا بالتحقق من مقدار امتثال المؤسسات لهذه القوانين.

"أما الهدف الأساسي من ذلك فهو التأكد من أن الجميع يضع أمن المعلومات على رأس أولوياته. ونقوم بزيارات منتظمة لكل الجهات الحكومية للتأكد من أنها تطبق كل الضوابط التي يبلغ عددها 388 والواردة ضمن سياسة أمن المعلومات".

إشارات: هل تقومون بزيارات يومية إلى المؤسسات الحكومية لمراجعة تطبيق الإجراءات المطلوبة؟

شرف: "بقدراتنا ومواردنا الحالية نقوم بزيارة إلى زيارتين أسبوعياً، ويعتمد ذلك على حجم الجهة الحكومية. وكلما ارتفع عدد أفراد فريقنا، تمكنا من زيادة عدد زيارات المراجعة والتحقق التي نستطيع القيام بها أسبوعياً. فهناك أكثر من ١٤٠ هيئة حكومية وشبه حكومية في دبي تتفاوت من حيث عدد الموظفين وعدد المراكز التي تضمها.

"وتغطي المراجعة التي يجريها فريقنا 12 قطاعاً من قطاعات نظام أمن المعلومات، التي تتألف من 388 ضابطاً. ويهدف هذا النظام إلى تمكين الهيئات والمنظمات الحكومية في دبي من الالتزام بمعايير تضمن استمرارية الأعمال، وتحد من الأضرار والأخطار المرتبطة بأمن المعلومات.

إشارات: مسؤوليتك تشمل أيضاً إدارة التعاون، فما طبيعة هذه الإدارة؟

شرف: "إنه جزء مبني على التنسيق مع الشركاء، إذ أن عمل مركز دبي للأمن الإلكتروني يقوم أساساً على التنسيق، كالتعاون مع المؤسسات والهيئات الوطنية والعالمية التي تعمل في المجال ذاته بهدف توثيق العلاقات وتشكيل الصلات والروابط التي تمكننا من تشارك المعلومات حول أي تهديدات أمنية إلكترونية عامة أو محددة. فبالتعاون وحده يمكن محاربة هذه التهديدات. كذلك يشمل عملي إدارة العلاقات العامة والتغطيات الإعلامية تحت مظلة إدارة التعاون".

إشارات: جعل دبي المدينة الإلكترونية الأكثر أماناً في العالم ليس بالمهمة السهلة. أين وصلتم في مسيرتكم نحو تحقيق هذه الرؤية؟

شرف: "هذه المهمة لا تنتهي أبداً، لا سيما علينا أن نواصل العمل باستمرار لاستباق أي تهديدات أو تحديات قد تواجه مدينة دبي، والتأقلم مع التغيرات، والتعلم من كافة التيارات الحديثة التي تواصل الظهور من حولنا، وهذه هي نقطة الانطلاق التي نستطيع من خلالها تحسين وتعزيز خدماتنا. إنها مسيرة أشبه بالدائرة، لا تتوقف أبداً".

إشارات: ما تقييمك لمستوى الأمن الإلكتروني والوعي بالمخاطر في دبي؟

شرف: "سؤال جيد، يمكن ربطه ببعض المبادرات التي نعمل على إطلاقها في المركز. فبهدف بلوغ المستوى المناسب والمقبول من الأمن الإلكتروني، علينا اتخاذ إجراءات محددة تعتمد على تطبيق إجراءات أمن المعلومات من جهة، وعلى رفع الوعي الأمني لدى المؤسسات والأفراد من جهة أخرى.

"ولدينا في هذا المجال استراتيجية للأمن الإلكتروني في دبي، نستعد لإطلاقها قريباً بعد اكتمال العمل عليها، وقد عقدنا حولها ورش عمل عدة مع شركائنا الاستراتيجيين (الهيئات الحكومية).

"يتمثل أحد واجباتنا في وضع استراتيجية للأمن الإلكتروني لإمارة دبي. وتقوم الاستراتيجية على رؤية محددة هي ترسيخ مكانة دبي كمدينة رائدة في مجال الأمن والسلامة والابتكار. يتحقق ذلك عن طريق خمسة محاور تغطي كافة أوجه الأمن الإلكتروني.

رؤية مركز دبي للأمن الإلكتروني هي جعل مدينة دبي أأمن مدن العالم إلكترونياً

وحرصنا أن تلبي استراتيجيتنا للأمن الإلكتروني المعايير الدولية وأن تتواءم مع الممارسات المتبعة دولياً في هذا المجال. وتتركز الخطة على توفير بنية إلكترونية آمنة ضد التحديات الإلكترونية؛ وبناء مجتمع واعٍ بمخاطر الأمن الإلكتروني، وذلك من خلال رفع الوعي بين المواطنين والمقيمين والزوار في إمارة دبي؛ وتعزيز الامتثال الإلكتروني، من خلال ضمان إتاحة الأنظمة والحلول واستمرارية الأعمال؛ والابتكار، من خلال مبادرات الابتكار في مجال الأمن الإلكتروني، وتعزيز الأبحاث، والتواصل مع مراكز البحث في الجامعات المختصة؛ إضافة إلى المحور الأخير وهو التنسيق المحلي والدولي. إنها استراتيجية محكمة ستسهم في تعزيز أمن إمارة دبي بحلول العام 2021".

إشارات: يقال إن الموظفين هم الخطر الرئيسي على أمن الجهات الحكومية. فالعديد من هجمات الاختراق الشهيرة تمت بسبب نقرة من أحد الموظفين على رابط خبيث، أو كما حدث في هجوم "شامون". كيف نواجه هذا التهديد؟

شرف: "أنت محق، فالأمر في النهاية يعتمد على وعي الموظفين أنفسهم، لا سيما أنّ الإجراءات التنظيمية لا تتحقق من تلقاء ذاتها، ومن الضروري أن يلتزم بها الموظف والفرد العادي على حد سواء. من خلال خطتنا الاستراتيجية، نعمل على الوصول إلى كافة أفراد المجتمع، وليس المؤسسات الحكومية وحدها.

"إنّ نطاق عملنا يرتكز على حكومة دبي، لذلك نعمل على التنسيق مع الجهات المسؤولة عن توعية السكان بهدف زيادة مستوى الوعي، حيث تقوم كل جهة حكومية بدور أساسي في تحقيق الاستراتيجية والمساعدة في رفع مستوى الوعي لدى الجميع في دبي. إن الوعي هو العامل الأساسي لتحقيق هذه الاستراتيجية، ويجب تعزيزه باستمرار، ومسؤوليتنا تتمثل في التأكد من تحقيق ذلك من خلال التقييم المستمر والمنظم. ونطالب دائماً بالاطلاع على النتائج لنتأكد من أن الجهة المعنية تتبنى هذا النهج. فالمتابعة المستمرة والتقييم الدقيق يعدان شرطاً أساسياً من شروط نجاحنا في عملنا".

إشارات: ما أسباب الهجمات الإلكترونية بشكل عام؟ فقد شهدنا مؤخراً اتهامات بهجمات إلكترونية ذات دوافع سياسية، أو هذا ما أشيع وقيل. هل مثل هذه الأمور واردة الحدوث؟

شرف: "احتمال شن هجمات إلكترونية لأغراض سياسية هو احتمال قائم، وهو ما يبدو واضحاً على المستوى العالمي حالياً. ولا يمكن فصل هذه الهجمات عن السياق العام للأحداث، ولا عن الظروف التي تحدث فيها. لكن الهجمات الأكثر رواجاً حالياً تتم باستخدام برامج الفدية (رانسوم وير) لتحقيق أغراض مالية لا سياسية، وهذه التهديدات في ازدياد مستمر، فبمجرد أن تخترق هذه البرامج جهازك، تقوم بتشفيره، ومن ثم يكون عليك دفع فدية لاستعادة نظامك. برامج الفدية تعد مثالاً جلياً على تغير طبيعة الجرائم الإلكترونية، إذ أصبح المجرمون يمتلكون الوسائل التي تمكنهم من ابتزازك من دون أن يغادروا منازلهم".

إشارات: كيف يمكن جعل الجميع آمنين إلكترونياً؟

شرف: "الحل بسيط في الواقع، ويبدأ من الفرد نفسه، وهذا ما تدلنا عليه الأحداث ودروس التاريخ. فإذا امتلك الفرد مستويات الوعي اللازمة، وأبدى الحرص المطلوب، تتغير الأمور بصورة ملحوظة. إن وضع السياسات والتشدد في الإجراءات وامتلاك أحدث البرمجيات وأنظمة الحماية المتقدمة كلها عوامل مهمة، لكن الأهم منها هو التركيز على رفع مستوى الوعي لدى الأفراد أولاً".

القراصنة قد يكتشفون كلمة المرور من وضعية الإمساك بالهاتف

أثبتت دراسة حديثة أجراها خبراء في جامعة نيوكاسل الإنجليزية أن قراصنة الفضاء الإلكتروني يستطيعون معرفة أرقام المرور الخاصَّة بمستخدمي الهواتف الذكية من خلال مراقبة درجة انحناء الهاتف أثناء قيام المستخدم بكتابتها على شاشة الهاتف، فضلاً عن مراقبة حركة عينيه ويديه. تتألف أرقام المرور كما هو معروف من أربعة أرقام، وقد تمكن الباحثون من تخمينها بدقة نسبتها 70 بالمئة بعد أن أخضعوا المستخدمين للمراقبة وجمعوا بيانات استخرجوها من هواتفهم، كما تمكنوا من تخمين الأرقام ذاتها بدقة تصل إلى مئة بالمئة من المحاولة الخامسة.

ويقول الخبراء في الجامعة الإنجليزية إن المخترقين يستهدفون المعلومات المخزنة في تطبيقات الهاتف، وفيها يتولى المستخدم مشاركة معلومات حساسة حين يقوم بتفعيل خاصية تحديد موقع الهاتف الذكي مثلاً أو حين يسمح أيضاً لبعض التطبيقات والمواقع بالنفاذ إلى هاتفه، ظناً منه أن هذه المعلومات غير حساسة وأن تسريبها ليس ضاراً، لكنها في الحقيقة تشكل فرصة لأي موقع خبيث لمعرفة موقع الهاتف بسهولة، وتالياً اختراقه.

بالرغم من ذلك، ليست مهمة قراصنة الفضاء الإلكتروني سهلة بحسب تأكيد الخبراء في جامعة نيوكاسل، إذ سيكون من الصعب أن ينجحوا في برمجة نظام قادر على تحديد أرقام المرور الخاصة بالهواتف الذكية بالاعتماد على مراقبة حركة يد أو عين المستخدم أثناء كتابتها للولوج إلى هاتفه. وقد أشارت الدراسة إلى أن الخبراء تمكنوا من معرفة أرقام المرور الخاصة بالهواتف بعد أن حصلوا من المستخدمين أنفسهم على قائمة من خمسين توليفة أرقام مختلفة، بينها التوليفة الصحيحة. ومن دون هذه القائمة، فإن اختراق كلمة المرور سيظل أمراً عسيراً. لكن الخبراء يحذرون في المقابل من احتمال أن يخترق القراصنة المواقع التي تسجل بيانات خاصة بمستخدمي الهواتف الذكية، مثل المواقع الإلكترونية الخاصة بتحديد موقع الهاتف وتفعيل الاتصال بالكاميرا، فيلجأون إلى مراقبة حركة عيني المستخدم بدقة حين يعمد إلى وضع أرقام المرور على شاشة هاتفه، ومن ثم سينجحون في اختراق الهاتف بعد محاولات قد يفشل بعضها، لكن إحداها ربما تنجح في نهاية المطاف. وقد تمثل هذه الممارسات خطراً في عالم يلجأ فيه القراصنة إلى خدع احتيالية ومعقّدة من أجل الحصول على أكبر قدر من المكاسب.

وقالت الدكتورة المشرفة على الدراسة مريم مهرنزاد من جامعة نيوكاسل إن "معظم الهواتف والحواسيب والأجهزة الأخرى أصبحت مزودة بالعديد من أجهزة الاستشعار، وبالرغم من أن التطبيقات والمواقع الإلكترونية لا تطلب إذناً لدخول الكثير منها، إلا أن هناك برامج خبيثة يمكنها التجسس على البيانات واستخدامها لكشف المعلومات الحساسة، مثل تواريخ المكالمات والأنشطة اليومية وحتى رمز التعريف الشخصي للمستخدم وكلمات المرور".

توفير فرص عمل في معرض الإمارات للوظائف 2017 للخريجين الإماراتيين من أصحاب الكفاءات العالية

شارك مركز دبي للأمن الإلكتروني للسنة الثانية على التوالي في معرض الإمارات للوظائف 2017، الذي انطلقت فعالياته في 9 أبريل واستمر ثلاثة أيام في مركز دبي التجاري العالمي.

تأتي المشاركة بهدف استقطاب كوادر واعدة من أبناء الدولة وكفاءات وطنية قادرة على المساهمة في تحقيق الإنجازات وفق خطة يتم تطويرها بشكل مستمر، كما توفر فرصاً للارتقاء في شتى المجالات. يقدم المركز فرص عمل في مختلف المجالات، بما في ذلك التخصصات التقنية والفنية والإدارية.

يوفر المركز بيئة عمل تتسم بالإبداع والابتكار، تماشياً مع رؤية صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، بأهمية استباق التغييرات المتسارعة في العالم مع ثورة الابتكارات التكنولوجية وتطورها. ويعزز ذلك تحقيق أهداف وغايات المركز، الرامية إلى ابتكار أحدث التقنيات والحلول في مجال حماية المعلومات وشبكة الاتصالات وأنظمة المعلومات الحكومية في الإمارة.

ويتبع المركز خططاً واضحة لتعزيز الموارد البشرية وإعداد الكوادر الوطنية، إيماناً منه بأن الوطن يبنى بسواعد أبنائه، عملاً بمقولة صاحب السمو الشيخ محمد بن راشد آل مكتوم: "إن بناء الإنسان هو الأساس، ولا يكتمل بناء الأوطان إلا ببناء المواطن، الذي هو الثروة البشرية الدائمة العطاء".

ومثلت الهيئات الحكومية نحو سبعين بالمئة من العارضين المشاركين في المعرض الذي ينظمه مركز دبي التجاري العالمي، ويتيح لمواطني الدولة التقدم للوظائف والحصول على فرص التدريب والتعرف على أفضل طرق كتابة السير الذاتية بشكل يعبر عن مهارات المتقدمين ويقدمهم بأفضل صورة إلى الشركات ومسؤولي التوظيف.

وقد شهدت قاعات المعرض حضوراً لافتاً من الشبان والشابات من الخريجين الجدد القادمين للاطلاع على الفرص الوظيفية التي توفرها المؤسسات العامة والخاصة في أكثر من عشرين قطاعاً وتقديم أوراق التحاقهم بها.

مركز دبي للأمن الإلكتروني يشارك في مؤتمر آسيا لأمن الحاسب الآلي والشبكات

نظم مركز دبي للأمن الإلكتروني بالتعاون مع جامعة نيويورك أبوظبي مؤتمر آسيا لأمن الحاسب الآلي والشبكات، الذي يعتبر أحد أهم الأحداث في مجال الأمن الإلكتروني في المنطقة، إذ يشمل عدداً كبيراً من المواضيع التقنية حول آخر التهديدات والتحديات المتعلقة بالأمن الإلكتروني في مجالات الحاسب الآلي والاتصالات والاستدامة الأمنية.

ألقى المؤتمر الضوء على أهمية بناء علاقات تعاون بحثي بين الجهات الصناعية والحكومية والأكاديمية على مستوى دولة الإمارات لتحفيز بيئة ديناميكية في تطوير وبناء حلول أمنية مبتكرة في كافة المجالات.

وأطلع الدكتور مروان الزرعوني، مدير إدارة خدمات المعلومات في مركز دبي للأمن الإلكتروني، الحضور على الأهداف الرئيسية للمركز، والتي تتمثل في حماية كافة المعلومات الحكومية وشبه الحكومية ونظم المعلومات والاتصالات في دبي، لتطوير وتعديل واستخدام الوسائل اللازمة في مجال الأمن الإلكتروني ورفع كفاءة طرق حفظ المعلومات أيضاً.

وأكد سعادة يوسف الشيباني، الرئيس التنفيذي لمركز دبي للأمن الإلكتروني، أهمية الدور الذي تقوم به البحوث والمؤتمرات المحلية في نقل وبناء المعرفة في مجال الأمن الإلكتروني في دولة الإمارات بين الباحثين والخبراء والمهتمين.

وشدد على أن المركز يتعاون بشكل وثيق مع الجامعات ومراكز الأبحاث لرعاية ودعم مشاريع أبحاث أمن المعلومات وتمكين الطلبة بما يحتاجون من وسائل ومعارف، بما يتماشى مع استراتيجية دبي للأمن الإلكتروني التي يديرها المركز.

إطلاق مشروع الشهادات الرقمية لتأمين الاتصال بين الأجهزة وإنترنت الأشياء

أعلن مركز دبي للأمن الإلكتروني عن إطلاق مشروع الشهادات الرقمية الآمنة والذي يهدف إلى تأمين قنوات الاتصال بين الأنظمة والأجهزة وإنترنت الأشياء، والتأكد من موثوقية تلك القنوات بحيث يتم إصدار شهادات موثوق بها ومعتمدة من المركز ليتم تبادلها بين تلك الأجهزة والأنظمة في الإمارة.

يأتي إطلاق هذا المشروع كجزء من استراتيجية الأمن الإلكتروني في دبي، ويدعم رؤية مركز دبي للأمن الإلكتروني في جعل دبي المدينة الأكثر أماناً إلكترونياً في العالم.

يعتبر المشروع مصدراً موثوقاً ومعتمداً لإصدار الشهادات الرقمية الآمنة للجهات الحكومية في دبي. ويرتكز دور المشروع على ضمان تحديد صحة وهوية حامل الشهادة، مما يسهم في تسهيل تأدية العديد من المهام مثل تشفير الملفات، وتوفير قنوات اتصال آمنة لتبادل البيانات.

وقال سعادة يوسف الشيباني المدير التنفيذي لمركز دبي للأمن الإلكتروني: "في ظل التوجه نحو إنترنت الأشياء، أصبح من المهم جداً التأكد من موثوقية الأجهزة لضمان توفير قنوات اتصال آمنة في ما بينها. ويعمل المركز حالياً على تبني حلول البنية التحتية الرئيسية العامة لأجهزة إنترنت الأشياء وأجهزة الحاسوب والتقنيات التشغيلية المتصلة. وسيسهم المشروع في بناء بنية تحتية آمنة في الإمارة والذي بدوره سيحد من مخاطر الأمن الإلكتروني".

من المخطط الانتهاء من المشروع في منتصف العام 2017 حيث سيتيح للدوائر الحكومية في دبي إمكانية طلب وتلقي الشهادات الرقمية الآمنة.

مركز دبي للأمن الإلكتروني يستضيف ورشة مبادرات خطة دبي الاستراتيجية للأمن الإلكتروني

نظم مركز دبي للأمن الإلكتروني ورشة العمل الثانية بعنوان "مبادرات خطة دبي الاستراتيجية للأمن الإلكتروني"، التي تأتي في إطار سلسلة ورش العمل الهادفة إلى الإطلاع على احتياجات واقتراحات المؤسسات الحكومية لدعم الإطار الأولي لخطة دبي الاستراتيجية للأمن الإلكتروني.

تهدف الورشة إلى تحقيق الأهداف الاستراتيجية التي تم وضعها من أجل درء المخاطر والتحديات الإلكترونية المحتملة على الأنظمة والمعلومات الحكومية. ويعمل مركز دبي للأمن الإلكتروني بالتنسيق مع الجهات والقطاعات الحكومية المختلفة على توفير بنية إلكترونية آمنة ضد التحديات الإلكترونية وبناء مجتمع واعٍ بمخاطر الأمن الإلكتروني، لتمتلك إمارة دبي بنية تحتية هي الأكثر أماناً في العالم للخدمات الإلكترونية، تشمل جميع القطاعات الحكومية والشركات العامة والخاصة، بما في ذلك الأفراد في جميع القطاعات المتوفرة من مواطنين ومقيمين وزوار.

وخلال ورشة العمل، تم شرح الخطة التنفيذية التي سيتم من خلالها متابعة تنفيذ الأهداف ومؤشرات الأداء المعنية بكل جهة مشاركة في الخطة.

وقد تخللت الورشة حلقات نقاشية بين مختلف الهيئات والمؤسسات، إذ اعتمدت على طريقة التفكير الإبداعي وذلك لحصر كافة التحديات التي تواجهها هيئاتهم خصوصاً وإمارة دبي عموماً، ومن ثم طرح الأفكار والحلول المبتكرة التي من شأنها التغلب على تلك المخاطر ووضع الإطار الزمني لتنفيذ الخطط.

وأكد سعادة يوسف الشيباني، المدير التنفيذي لمركز دبي للأمن الإلكتروني أهمية التعاون مع المؤسسات والقطاعات المختلفة، معتبراً أن حماية الأمن الإلكتروني والوقاية من أي مخاطر محتملة هي مسؤولية مشتركة بيننا كجهة مسؤولة عن إعداد خطة استراتيجية لمواجهة أي أخطار أو تهديدات أو اعتداءات، وبين الجهات المعنية المختلفة، وذلك عبر معرفة الاحتياجات الرامية الى تحقيق الأهداف العليا المشتركة والتنفيذ العملي لمتطلبات الأمن الإلكتروني".

وأضاف: "نعمل مع جميع المؤسسات والجهات لوضع الخطط الرادعة للمخاطر والتحديات الأمنية الإلكترونية، بمعايير عالية على أن يجري تنفيذها بالتنسيق والتعاون بين جميع الأطراف، بما يتماشى مع الرؤية السديدة لصاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي".

أكبر هجوم قرصنة إلكتروني في التاريخ يضرب 100 دولة

تسبب هجوم إلكتروني واسع النطاق حمل اسم " WannaCry" في حالة من الاضطراب الشديد بين المؤسسات والأفراد حول العالم، في ما وصفه الخبراء بأنه هجوم غير مسبوق من حيث الحجم. وكانت خدمات الصحة العامة في بريطانيا الضحية الرئيسية للهجوم، حيث تم إلغاء آلاف مواعيد العلاج للمرضى في أعقاب الهجوم الإلكتروني. طال الهجوم الخبيث عشرات الآلاف من أجهزة الحاسوب مستغلاً ثغرة في أنظمة التشغيل "ويندوز"، ومن ثم تشفيرها وتعطيلها والمطالبة بفدية مالية قدرها 300 دولار مقابل فك تشفير واستعادة أنظمة تشغيل كمبيوتر واحد.

وذكر خبراء في الأمن الإلكتروني أن مجموعة من القراصنة تحمل اسم "شادو بروكرز" قامت بإنشاء الفيروس ويطلق عليه اسم "برنامج الفدية" وتم طرحه في السوق السوداء قبل شهر من الهجوم الإلكتروني، في حين أفاد المسؤولون في شركة مايكروسوفت أنهم كانوا على دراية بنقاط الضعف في نظام التشغيل "ويندوز" وقاموا بإصدار حل تصحيحي لإغلاق الثغرة الأمنية، لكن نظراً لعدم وجود وعي المستخدمين بأهمية تحديث الأنظمة والبرامج الحاسوبية بشكل دوري، أصيب أكثر من 200 ألف نظام في 100 دولة، إذ يبدو أن الغالبية العظمى من المؤسسات الكبرى تتجاهل عمل التحديثات التلقائية لأنظمتها، خاصة التابعة لمايكروسوفت، زعماً منها أن مثل هذه التحديثات تؤثر سلباً على برامج فعّالة أخرى. واستهدف الهجوم الإلكتروني عدداً من المؤسسات العملاقة من بينها "فيديكس" و"نيسان" و"دويتشه بان" وهيئة الصحة العامة في بريطانيا، إضافة إلى العديد من الوكالات والشركات الروسية، إلا أن الهجوم الذي تعرضت له هيئة الصحة العامة في بريطانيا كان الأكثر إثارة للقلق كونه يجسّد خطورة كبيرة على حياة الناس، حيث عجز آلاف المرضى عن تلقي علاجهم وأصيبت حركة سيارات الإسعاف بالاضطراب والشلل التام.

ولحسن الحظ توقف الفيروس عن الانتشار بعد أن أعلنت مختلف القنوات الإخبارية الرئيسية من حول العالم حالة الطوارئ وأوصت المستخدمين بعدم فتح أي روابط من مصادر غير موثوقة، لكن يبدو أن آلاف الأنظمة كانت قد تضررت بالفعل، ولا تزال هوية منفذي الهجوم مجهولة، ويرجح خبراء الأمن الإلكتروني أن منفذي الهجوم هم مجموعة من الهواة.

ونجح باحث بريطاني مختص بالهجمات الإلكترونية يبلغ من العمر 22 عاماً في التوصل إلى برنامج "كيل سويتش" يعمل على وقف انتشار الفيروس باستخدام عملية بسيطة، لكنه لم يتمكن من إصلاح الأضرار التي طالت آلاف الأجهزة التي تمكن القراصنة الهواة من تشفيرها وجني أكثر من 50 ألف دولار قبل إيقاف الفيروس. وتعليقاً على هجوم فيروس " WannaCry" ووقف انتشاره، صرح المسؤول عن الأمن الإلكتروني في الحكومة البريطانية بأن "الطريقة التي يعمل بها هذا الفيروس تعني أن الأضرار التي أصابت الأجهزة والشبكات ربما لم تُكتشف بعد، ويمكنها الكمون والانتشار في أي لحظة داخل الشبكات". ويُنصح الخبراء المستخدمين من حول العالم بإجراء التحديثات الفورية على أنظمتهم وبرامجهم، في حال توفرها، وتوخي الحذر التام قبل فتح أي روابط من مصادر غير موثوق بها عبر البريد الإلكتروني أو فيسبوك أو تويتر أو أي قناة اتصال أخرى على الإنترنت.

نظام أمن إلكتروني أسرع 100 مرة في اكتشاف الهجمات

صممت مختبرات لويس رودز بالتعاون مع مختبرات ساندیا الدولية رقاقة حوسبة عصبية قادرة على البحث عن الأنماط المعقدة والكشف عن التهديدات الأمنية باستخدام طاقة منخفضة تقل عما يستهلكه مصباح صغير.

تم تصميم معظم أنظمة الأمن الإلكتروني التقليدية بهدف البحث والكشف عن مؤشرات الهجمات العامة، ولكنها لا تمتلك القدرة على استهداف أنماط محددة، ما يترك المجال مفتوحاً أمام هجمات متقدمة صممت لتخطي الاحتياطات الأمنية الحديثة والولوج عبر الأبواب الخلفية.

تتخطى الرقاقة الجديدة هذه القيود، وتكشف مباشرة عن تهديدات محددة، مما يتيح لمتخصصي الأمن الإلكتروني التعامل معها فوراً.

يتمثل العامل المشترك بين الدماغ ورقاقة الحوسبة العصبية في المسح الدائم للتهديدات. فدماغ الإنسان قادر على استدعاء البيانات السابقة ومقارنتها بالموقف الحالي لمعرفة ما إذا كانت هناك هجمات وشيكة، واتخاذ الإجراءات الفورية لردعها. ويتبع النظام الحاسوبي العصبي نفس الطريقة، فهو يقارن البيانات المتدفقة بالأنماط المشتبه بها بصورة منتظمة.

مختبرات ساندیا اختبرت الرقاقة وقارنتها بنظام الأمن الإلكتروني التقليدي، وأظهرت النتائج تفوّق النظام الجديد، كما أثبتت أن النظام الجديد الذي لا يزال في المراحل الأولى من التطوير يعمل أسرع من أنظمة الأمن الإلكتروني التقليدية بحوالي 100 مرة، ويمتلك كفاءة طاقة أكثر بحوالي 1000 مرة أيضاً.

مستخدمو الهواتف الذكية يفتقرون إلى الوعي الأمني

أظهر تقرير عن مركز بيو للأبحاث في الولايات المتحدة أن مستخدمي الهواتف الذكية يفتقرون إلى الوعي الأمني على نحو يدعو للقلق. وأوضح التقرير أن إجراءات الأمن الأساسية تتطلب استخدام رمز مرور وتحديث التطبيقات ونظام التشغيل بصورة منتظمة، إلا أن معظم المستخدمين لا يلتزمون بهذه الإجراءات.

أشار التقرير إلى أن 28 بالمئة من المستخدمين لا يستخدمون رمز مرور لهواتفهم، بينما قال 40 بالمئة منهم إنهم لا يحدثون التطبيقات وأنظمة التشغيل إلا في أوقات تناسبهم، وقد لا تناسب بالضرورة الإجراءات الأمنية. وأوضح الاستطلاع أن 40 بالمئة لم يحدّثوا أنظمة التشغيل الخاصة بهواتفهم على الإطلاق، بينما يفضل 10 بالمئة عدم تحديث تطبيقاتهم.

قال التقرير إن 22 بالمئة فقط يستخدمون رموز مرور ويحدّثون تطبيقات الهاتف، بينما يمتنع 3 بالمئة عن فعل ذلك. ويقع أغلبية المستخدمين (75 بالمئة) في الفئة المتوسطة بحسب مقاييس أمن الهواتف الذكية، إذ تستخدم هذه الفئة "قفل الشاشة"، لكنهم لا يحدثون التطبيقات أو أنظمة التشغيل إلا في الأوقات المناسبة لهم.

من حيث الفئات العمرية، فإن المستخدمين الذين تخطوا 65 سنة هم أقل استخداماً لقفل الشاشة، وأوضحت النتائج أن عدد من تخطوا 65 سنة يزيد بأكثر من الضعفين من حيث عدم اتباع أفضل الممارسات المقترحة لتأمين هواتفهم.

تعتبر إجراءات الحماية على الهواتف الذكية مصدر قلق أيضاً، حيث أوضح التقرير أن 54 بالمئة يستخدمون شبكات الواي فاي العامة، بينما يقر 20 بالمئة أنهم يجرون معاملات بنكية أو يتسوقون عبر الإنترنت باستخدام هذه الشبكات. ومن المعروف أن استخدام شبكات الإنترنت العامة في المراكز التجارية أو المطارات أو المقاهي والمطاعم يعد أبرز المخاطر التي تعرض البيانات الشخصية للاختراق.

إيلون ماسك يخطط لزرع أجهزة في المخ لتزويد العقل البشري بذكاء خارق

كشف إيلون ماسك أنه سيقوم بتأسيس شركة باسم "نيورالينك"، هدفها ربط العقول البشرية بالحواسيب. يرى ماسك أن الذكاء الاصطناعي يتقدم بسرعة، ولا شيء سيمنعه قريباً من التفوق على البشر والاستيلاء على العالم. يقول: "لا يمكننا تحديد متى سيحدث ذلك، لكن الخطر الوجودي المحدق بنا يجبرنا على إيجاد حلول".

ستبتكر "نيورالينك" أجهزة يتم زرعها في المخّ لتزود العقل البشري بذكاء فائق وبمستويات معالجة قادرة على إيقاف صحوة الماكينات. وقد ألقى إيلون الضوء على هذا المفهوم خلال قمة الحكومات العالمية التي أقيمت في دبي.

يتصدر مشروع ماسك صدارة الأخبار حالياً، وهناك جهات أخرى تعمل على مفهوم مشابه، وعلى رأسها جناح الأبحاث التابع لوزارة الدفاع الأمريكية، إلا أن معظم أبحاثه سرية. ومن المتوقع أن تنجح مساعي ماسك، بالرغم من أن رائد التقنية يواجه تحدي إيجاد الوقت الكافي لمشروعه الجديد في ظل انشغاله بتسيير "سبيس إكس" و"تيسلا" ومشاريع أخرى.

الجدير بالذكر أن فيسبوك تختبر تقنية مشابهة بشكل غير معلن، حيث تطور تقنية واجهة دماغ حاسوبية ستتيح للبشر التواصل مع الأجهزة الخارجية. كما أن باحثين في جامعات مثل جامعة كاليفورنيا وديوك في الولايات المتحدة يطورون أيضاً تقنية واجهة دماغ حاسوبية ستتيح للمصابين بالشلل النصفي المشي مرة أخرى.

شرطة دبي.. عقوبات رادعة لمرتكبي الجرائم الإلكترونية في الإمارات

مع اتساع مساحة شبكات التواصل الاجتماعي على شبكة الإنترنت وتعددها، أصبحت الجريمة الإلكترونية أكثر تنوعاً وبأساليب ونوايا مختلفة، وأصبح الفضاء الرقمي ساحة صيد واحتيال للمخترقين والمتطفلين الذين يرتكبون جرائم الاختراق لغايات متعددة، ومنها انتهاك الخصوصية وسرقة البيانات والحسابات، وانتحال شخصية المستخدمين. وهذه الاختراقات تتم عبر روابط احتيالية وصفحات وهمية. فما الذي يجب معرفته عن هذا العالم، وكيف نحمي أنفسنا من الجرائم؟ للإجابة عن هذه الأسئلة الهامة، قامت مجلة "إشارات" بإجراء لقاءات مع أصحاب الاختصاص، نعرض في ما يلي إجاباتهم.

يقول مساعد القائد العام لشؤون البحث الجنائي بشرطة دبي سعادة اللواء خبير خليل إبراهيم المنصوري، إن الإنترنت وسيلة تجمع بين الخطر والفائدة، وبوجود برامج التواصل الاجتماعي وانتقالها إلى الهواتف، ازداد الأمر تعقيداً، خصوصاً مع ازدياد عدد القراصنة الذين يمارسون إجرامهم من خلال اختراق الحسابات الشخصية، وما يتبعه من استغلال مادي وابتزاز وتخريب.

يوضح المنصوري أن الأطفال دون سن 18 عاماً، هم الأكثر عرضةً لاختراق الحسابات الشخصية عبر البريد الإلكتروني ومواقع التواصل الاجتماعي، إذ لا يمتلكون المعرفة والثقافة الكافية لحمايتها، فهم يفتحون حساب البريد الإلكتروني باستخدام بيانات وهمية، وبعد فترة يستقبلون رسائل "تحديث البيانات" التي تنقلهم إلى صفحة أخرى "مقرصنة" تطلب منهم إعادة كتابة بريدهم الإلكتروني وكودهم السري، وبهذا يصل القرصان الإلكتروني إلى جميع بيانات المستخدم.

القرصان الإلكتروني أنواع

يشير المنصوري إلى وجود قرصان إلكتروني متخصص بابتزاز الفتيات، وآخر يمارس النصب والاحتيال. وهناك أيضاً القرصان الإلكتروني العشوائي والقرصان الإلكتروني المستهدف، الذي يستغل المستخدم ويجمع المعلومات عنه لغايات منها الابتزاز أو المال، عدا عن القرصان الإلكتروني المنتمي إلى عصابات متخصصة بالجريمة.

يوضح المنصوري أن القرصان الإلكتروني العشوائي يتبع أسلوب إرسال روابط مخترقة

متضمنة رسائل تحتوي على عروض مغرية، ومنها خصومات في الفنادق وغيرها، قد تجذب المستخدم للنقر على الرابط، ومنها يتم سحب جميع بياناته ومعلوماته الشخصية المخزنة.

أنواع الاختراقات

كثيرة هي الطرق التي يعتمدها القرصان الإلكتروني لاختراق الحاسوب والهاتف. يقول المنصوري: "أساليبهم متعددة، يتم تصنيفها تبعاً لأهدافها، ومنها استخدام أدوات التجسس على أجهزة المستخدم والإطلاع على بياناته المحفوظة في الحاسوب، واستخدام الروابط التي تمكنه من الوصول إلى صور المستخدم ورسائله، بهدف الاستغلال والابتزاز". ويحذر من فتح برامج تُروَّج عبر مجموعات الواتساب، الغاية منها التجسس.

يوضح المنصوري أن طالبات الجامعات والمدارس هن الأكثر عرضة للابتزاز الإلكتروني، لقلة خبرتهن بالتعامل مع مواقع التواصل الاجتماعي، وعدم الإلمام بأهمية حماية وتحديث أجهزتهن، فنجد أغلبيتهن يلتقطن الصور ويخزّنها في البريد الإلكتروني ومواقع التواصل الاجتماعي، من دون تفعيل خدمة الرقم السري وخدمة البحث عن الهاتف، ما يجعل الهاتف عرضة للاختراق، أو ربما السرقة، وبالتالي يعرض الفتاه للوقوع ضحية الابتزاز والاستغلال.

يقول المنصوري إن لدى إدارة المباحث الإلكترونية فريق شرطة نسائية يستقبل البلاغات ويدون بحضور ولي الأمر إفادات الضحايا بسرية تامة.

توعية وحماية

لأن حماية البريد الإلكتروني أمر مهم لحماية المستخدمين من الاختراق وما يتبعه من ابتزاز واستدراج، يقدم نائب مدير إدارة المباحث الإلكترونية بالإدارة العامة للتحريات والمباحث الجنائية بشرطة دبي المقدم سالم بن سالمين مجموعة من النصائح بهذا الخصوص، هي: التأكد من وجود برامج حماية خاصة، وتحديثها دائماً، وتجنب فتح الروابط غير المعروفة، والاطلاع على سياسات الأنظمة والحماية في كل موقع تواصل اجتماعي، وربطها برقم الهاتف وبريد إلكتروني آخر.

> الاحتيال الإلكتروني أنواع، منه العشوائي، ومنه الذي يتم بقصد الاستغلال والابتزاز، وبعضه يتبع لعصابات إجرامية
>
> **سعادة اللواء الخبير خليل المنصوري**

تقوم شرطة دبي بنشر الوعي بمخاطر الجرائم الإلكترونية

المقدم سالم بن سالمين

وأضاف: "أطلقت إدارة المباحث الإلكترونية في شرطة دبي عدداً من المحاضرات وبرامج توعية الجمهور، استهدفت بها طلاب المدارس والجامعات باعتبارهم الأكثر استخداماً لمواقع التواصل الاجتماعي، عبر تخصيص حملات توعوية بالعربية والإنجليزية، وتقديم النصائح عبر حساب القيادة العامة لشرطة دبي على تويتر، كما تقيم شرطة دبي في مجالس الأحياء محاضرات توعوية حول مخاطر الجرائم الإلكترونية". ويدعو سالمين كل من تعرض لأذى من الغير عبر الأجهزة المتصلة بالإنترنت، التبليغ عن الإساءة عبر قنوات التواصل الخاصة بالقيادة العامة لشرطة دبي، والاتصال على الرقم: 800CID أو 800243.

سيكولوجية القراصنة

يحدد الاختصاصي في علم النفس محمد النحاس سيكولوجية قراصنة الإنترنت، بالقول: "نسبة ذكائهم عالية، يوظفونها في الاعتداء على خصوصية الغير من باب التطفل أو الابتزاز أو سعياً وراء المال، مشيراً إلى ضرورة التبليغ عنهم، كون أعمالهم تتنافى مع الأخلاق والتقاليد وتعاليم الدين.

يرى النحاس أن المخترق الذي يؤذي الأطفال بتوزيع صورهم أو بابتزازهم، هو صاحب شخصية "مريضة" تستمتع بإيقاع الأذى بالآخرين، وقد يكون تعرض للتحرش في طفولته، فيختار الجريمة كوسيلة للانتقام من المجتمع.

ويبدأ الطفل بالوصول إلى الإنترنت والتعرض إلى مختلف محتوياته في سن الثالثة، وبشكل خاص إذا كان الأهل لا يراقبون أطفالهم ويتركون لهم الحرية في استخدام الإنترنت.

ويستخدم الأطفال شبكة الإنترنت دون أن يدركوا ما يترتب على هذا الاستخدام من أضرار أو فوائد، حيث تختلف تصورات الأطفال للإنترنت بحسب استخداماتهم ووفقاً للطريقة التي يرسم بها الأهل مفهوم الإنترنت في ذهنهم.

كما أن كثيراً من الأطفال يتعرضون إلى محتوياتٍ غير لائقةٍ مثل: المشاهد العنيفة والعدوانية والإباحية، ما يؤكد عدم متابعة الأهل لنشاط طفلهم على الإنترنت وذلك يقود إلى العديد من التأثيرات السلبية على الطفل.ينصح النحاس أولياء الأمور بأن يدركوا أن الرقابة على الأطفال، مهما كانت مشددة، قد يخترقها الطفل، لأن الإنترنت شبكة مفتوحة ومن الصعب تحديدها ومراقبتها.

ويشدد على أهمية أن يدرك أولياء الأمور وجوب تعزيز ثقة طفلهم بنفسه، من خلال بناء شعور الرقابة الذاتية، ويتحقق ذلك عن طريق المعلومات الصحيحة التي يتم تزويده بها.

العقوبة مليون درهم

يؤكد المحامي يوسف البحر أن المُشرع في دولة الإمارات العربية المتحدة تصدى بقوة لمسألة اختراق الحسابات الشخصية على الإنترنت، لما لهذا الأمر من أثر سلبي كبير على حقوق الأشخاص، وإمكانية استغلال البيانات الشخصية في التهديد أو الابتزاز أو ارتكاب جرائم تضر بصاحب الملفات أو المواد.

ردعاً لمن يفكر في اختراق ملفات الآخرين، جاءت العقوبة مشددة وفقاً لقانون مكافحة جرائم تقنية المعلومات، وذلك في المادة رقم (2) البند أولاً، وتنص على التالي: "يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد على ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكترونياً أو شبكة معلومات أو وسيلة تقنية معلومات بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة".

إذن، فعقوبة "الدخول إلى أي موقع دون تصريح" هي الحبس وغرامة تتراوح بين 100 ألف درهم ولا تزيد على 300 ألف درهم، والقاضي هو من يحدد قيمة الغرامة ومدة الحكم استناداً إلى وقائع وتفاصيل كل قضية، لذلك فهذه العقوبة رادعة، وتأتي إيماناً من المشرع الإماراتي بأهمية حفظ الخصوصية.

في حالة استخدام "البيانات الشخصية" من خلال حذفها أو تدميرها أو نشرها من دون إذن، فإنَّ البند الثالث من المادة ذاتها (2) يشدد العقوبة لتصل إلى الحبس مدة لا تقل عن سنة واحدة، والغرامة التي لا تقل عن 250 ألف درهم، ولا تتجاوز مليون درهم أو بإحدى هاتين العقوبتين.

أما في حالة اختراق مواقع إلكترونية تحتوي على بيانات حكومية أو معلومات سرية خاصة بمنشآت مالية أو تجارية أو اقتصادية، فإن قانون تقنية المعلومات يشدد العقوبة على هذه الأفعال في المادة (٤) لتصل إلى السجن المؤقت، و"المقصود بالسجن المؤقت هو السجن من 3 إلى 15 عاماً وفقاً لما تقدره الهيئة القضائية في منطوق حكمها"، إضافة إلى غرامة مالية لا تقل عن 250 ألف درهم ولا تتجاوز مليوناً و500 ألف درهم.

أدرك المُشرِّع الإماراتي أهمية حفظ الخصوصية في الفضاء الإلكتروني، وحدّد عقوبات مشدّدة للمخالفين

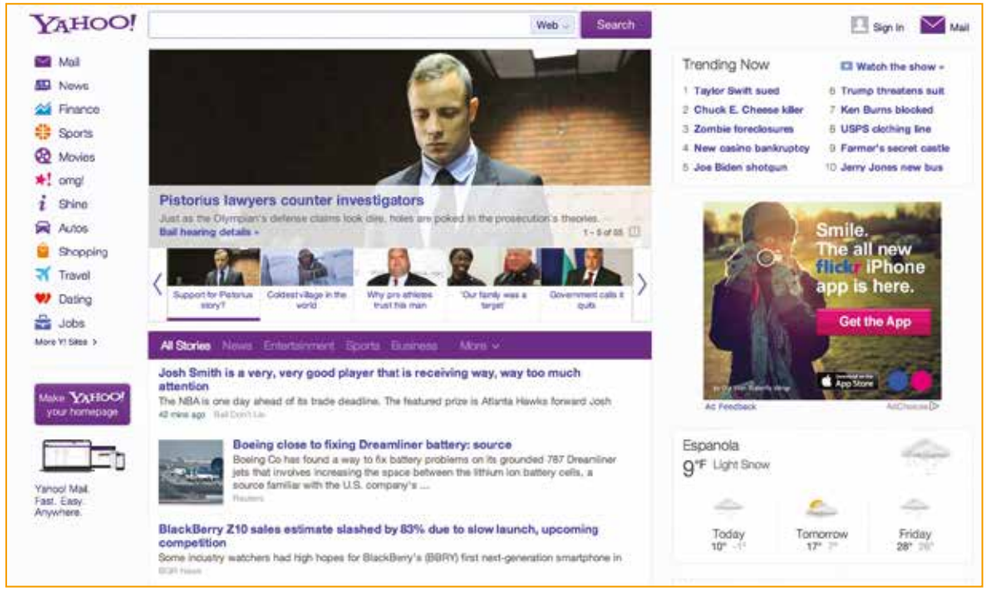
المحامي يوسف البحر

الرقابة على الطفل مهما كانت مشددة قد يخترقها، والحل بتزويده بالمعلومات الصحيحة

الاختصاصي في علم النفس محمد النحاس

هكذا اختُرقت ياهو... بنقرة!

تنشر "إشارات" القصة الكاملة لإحدى أضخم عمليات القرصنة الإلكترونية في التاريخ، والتي ظلت سراً مخفياً عن الجمهور وعن عملاء ياهو لمدة عامين، خوفاً من انكماش قاعدة المستخدمين لدى هذه الشركة العملاقة التي تعتبر إحدى أكبر الشركات العاملة في ميدان محركات البحث على مستوى العالم.



كان يكفي أن يهمل موظف واحد في "ياهو" "Yahoo" تطبيق شروط الأمان حتى يدخل القراصنة إلى بيانات إحدى أكبر شركات التقنية في العالم، من خلال التسلل إلى شبكة "ياهو" الداخلية، مستخدمين رسالة تصيّد احتيالية بسيطة للغاية.

هذا النوع من الهجمات صار أكثر تعقيداً في السنوات الأخيرة، ويستخدم القراصنة طرقاً أكثر احترافية لزرع روابط الاختراق في مواقع التواصل الاجتماعي، ويقومون بإنشاء مواقع إلكترونية مزيفة تشبه في عناوينها عناوين المواقع الحقيقية.

إلّا أن الهجوم الذي استهدف "ياهو" قبل سنتين تم تنفيذه باستخدام وسائل أقل تعقيداً، من خلال عناوين إلكترونية بنت حلقة وصل مع أحد الروابط، ولم يتبق أمام المخترق سوى نقرة واحدة فقط لكي يسطو على قاعدة بيانات هائلة، وينجح في اختراقها. وبالفعل مثلت تلك النقرة أكبر اختراق إلكتروني في التاريخ، وإليكم كيفية حصوله.

كشف تقرير مكتب التحقيقات الفيدرالي الأمريكي أن الهجوم الواسع النطاق عائد إلى العام 2014، حيث أُدين أربعة قراصنة ووجهت إليهم تهمة سرقة بيانات ومعلومات خاصّة بنصف مليار حساب إلكتروني تديرها "ياهو".

وقد أظهرت التحقيقات المعمقة اللاحقة معلومات جديدة عن الهجوم الذي بدأ برسالة أرسلها القراصنة إلى عددٍ من الموظفين العاديين في "ياهو"، ولم تستهدف أي إداري. وفيما تغيب أي بيانات مؤكدة عن عدد الموظفين الذين تلقوا الرسالة، لكن المؤكّد أن موظفاً واحداً على الأقل نقر على رابط الاختراق، فكانت النقرة كافية للحصول على حق الوصول إلى قاعدة هائلة من البيانات.

كان ألكسي بيلان أحد القراصنة الذين تمت إدانتهم، وهو مدرج على قائمة القراصنة المطلوبين لدى مكتب التحقيقات الفيدرالي. وهدف بيلان من النفاذ إلى شبكة "ياهو" هو الوصول إلى قاعدة بيانات الشركة التي تتضمن المعلومات الخاصة بالمستخدمين، والوصول إلى أداة إدارة الحسابات، التي تُستخدم في تعديل قاعدة البيانات.

وقد استخدم بيلان بروتوكول نقل الملفات لتنزيل قاعدة البيانات في ياهو بأكملها. وبمجرد وصوله إلى قاعدة البيانات، وضع يده على كنز من المعلومات، مثل أسماء المستخدمين وأرقام هواتفهم والأسئلة الأمنية الخاصة بدخول حساباتهم والإجابات عنها، إضافة إلى رسائل استعادة كلمات المرور الضائعة والرموز التشفيرية لكل حساب.

بهدف اقتحام العناوين البريدية التي كانوا مكلفين باختراقها، قضت خطة بيلان وشريكه باراتوف باستخدام ملفات "كوكيز" حتى يتمكنوا من النفاذ إلى حسابات البريد الإلكتروني من دون الحاجة إلى كلمات مرور. وقد كشف التقرير أن المخترقين قاموا بإنتاج ملفات "كوكيز" هذه أكثر من مرة خلال الفترة الممتدة بين 2015 و2016، حيث تم انتقاء 6500 حساب في "ياهو" من بين الحسابات التي تم اختراقها والتي بلغ عددها نصف مليار حساب. ينتمي بعض هذه الحسابات إلى سياسيين ومسؤولين رفيعي المستوى وصحفيين وموظفين في شركات طيران وغيرهم.

أفاد تقرير مكتب التحقيقات الفيدرالي أن "ياهو" أطلعت ضحايا الهجوم على تفاصيل الحادث لأول مرة في 2014، مشيراً إلى أن الشركة لم تستطع إخفاء الأمر وقتاً أطول، لكنها لم تسمح بالإعلان عن الاختراق إعلامياً حتى ديسمبر 2016، عندما نصحت الشركة مئات الملايين من المستخدمين بتغيير كلمات المرور الخاصة بهم. وقد تم القبض على أحد الأربعة المتورطين، واسمه باراتوف، في كندا.

وهكذا فقد كان الهجوم الإلكتروني يستهدف أفراداً لديهم معلومات مهمة للقراصنة، إلا أن الاختراق طال نصف مليار حساب تديرها "ياهو"، تتضمن أسماء المستخدمين وكلمات المرور ومعلومات شخصيّة أخرى عرضها المخترقون للبيع على عصابات تمارس الابتزاز. وتنصح "ياهو" المستخدمين بالمزيد من الحرص، وتغيير كلمات المرور تفادياً للمزيد من الخسائر التي أدت إلى خسارة أسهم "ياهو" في البورصة حوالي 200 مليون دولار، وهو الخطأ المكلف للغاية تسبب به موظف واحد في "ياهو".

(من اليمين في الأعلى) إيغور سوشين وديمتري دوكشييف (في الأسفل) ألكسي بيلان وكريم باراتوف

المبتكر أحمد الحمادي يرتقي إلى المركز التقني الأول عربياً

هل ترغب بزيارة متحف والتجول في أرجائه من دون أن تغادر منزلك؟ هل تريد أن تتدرب على قيادة طائرة حربية من دون الاستعانة بمدرب؟ يتيح لك المبتكر الإماراتي الشاب أحمد الحمادي تحقيق ذلك من خلال سلسلة ابتكاراته المميزة، والتي تدلّ على أن الشباب الإماراتي قادر على تحقيق أفضل النتائج في كل حقول الابتكار والإبداع.

رفع الحمادي اسم الإمارات عالياً بتفوقه على 56 مشاركاً من 19 بلداً عربياً في "مسابقة الألكسو الكبرى للتطبيقات الجوالة العربية في العام 2016". وانتزع الحمادي الجائزة الأولى عن تطبيق "المتحف الذكي"، الذي يعرض المتاحف ومقتنياتها بطريقة تقنية مبتكرة.

إنجاز آخر حققه الحمادي حين دخل عالم الصناعات الدفاعية بابتكار عرضه في معرض الدفاع الدولي "آيدكس"، ويستخدم لأغراض التدريب.

كذلك، يستعد الحمادي لدخول عالم النفط قريباً بتطبيق يتيح التجول افتراضياً في حقول النفط. للحديث عن كل هذه الابتكارات وغيرها، التقينا الحمادي الذي يدرس الماجستير في تكنولوجيا المعلومات في جامعة أبوظبي، ولمعرفة المزيد عن رحلة الحمادي وانجازاته ومشاريعه، اجرينا معه هذة المقابلة وفيما يلي نصها:

إشارات: ما طبيعة الابتكار الجديد الذي عرضته في الدورة الأخيرة من معرض الدفاع الدولي "آيدكس"، في العاصمة أبوظبي؟

الحمادي: أنجزت تطبيقاً يخدم مجالات التعليم والتدريب المهني في المجال العسكري باستخدام نظارة (مايكروسوفت هولولنس) الحديثة، والتي تتميز عن باقي النظارات المشابهة بأنها تمكن المستخدم من رؤية المجسم الافتراضي مدمجاً في واقعه الفعلي، فيستطيع رؤية المجسم والدوران حوله.

في التطبيق طائرة حربية افتراضية وقنابل وأسلحة يدوية، تظهر للمستخدم حين يرتدي النظارة، فيستطيع أن يدور حول الطائرة مستكشفاً دونما عائق، باعتباره يشاهد كل ما حوله في الوقت نفسه، ويستطيع استعراض الأسلحة باستخدام الأوامر الصوتية.

إشارات: ما أهمية مشاركتك في هذا المعرض؟

الحمادي: "آيدكس" من أكبر المعارض المتخصّصة بالأنظمة العسكرية، وفيه تُستعرض أحدث التقنيات. وشاركت بتقنية تعرض لأول مرة، وكل من اختبر النظارة أبدى رغبة باستخدامها وإدخالها في برامجه التدريبية.

هذه التقنية تزيد من استيعاب المتدرب للمعلومات، حيث يستطيع مشاهدة المكونات الداخلية للأسلحة التي تعرض أمامه، في حين تعفي المدرب من عرض المعدات بصورة فعلية أمام المتدربين.

إشارات: فاز تطبيقك "المتحف الذكي" بالمركز الأول في فئة العلوم ضمن "مسابقة ألكسو الكبرى للتطبيقات الجوالة 2016". ماذا عنى لك هذا الفوز؟

الحمادي: إنه إنجاز لدولة الإمارات قبل أن يكون إنجازاً لي، لأنني مثلت بلادي في المسابقة، وزادني فخراً أن الفوز يأتي للسنة الثانية على التوالي.

وسبق لي أن مثلت دولة الإمارات في فئة التربية في الدورة الأولى من المسابقة بتطبيق "دروسي"، ويهدف إلى مساعدة الطلاب على التحصيل وإدارة المواد الدراسية.

إشارات: حدثنا عن تطبيق "المتحف الذكي"، وما الهدف منه؟

الحمادي: يتيح هذا التطبيق زيارة المتاحف وعرض مقتنياتها بتقنية 360 درجة وتقنية الواقع المعزز.

يغني التطبيق عن تكبد مشقات السفر لمشاهدة المتاحف، ويقدم فرصة الاطلاع على عالم المتاحف والآثار، وتسمح تقنية الواقع المعزز بتوجيه الكاميرا نحو أي قطعة أثرية، فتعرض على الشاشة كل المعلومات عنها.

الهدف من التطبيق حفظ الذاكرة العربية بما تضمه من آثار ومتاحف، باستخدام تقنيات حديثة تواكب التطور السريع للتكنولوجيا وتعمق معرفة المستخدمين بالآثار والمتاحف العالمية.

إشارات: أي متاحف إماراتية يغطيها التطبيق؟

الحمادي: يغطي 19 متحفاً هي: متحف الخيل، متحف العمارة التقليدية، متحف نايف، متحف الشاعر العقيلي، متحف دبي (حصن الفهيدي)، متحف المسكوكات، متحف الإبل، قصر الموجعي، قصر الحصن، حصن الجاهلي، حصن السلطان، بيت الشيخ سعيد آل مكتوم، مجلس غرفة أم الشيف، قرية الغوص، بيت جمعة وعبيد الثاني، قرية التراث، بيت التراث، حي الفهيدي التاريخي والمدرسة الأحمدية.

في حين يغطي بتقنية الواقع المعزز "متحف الشيخ زايد العدل" في منطقة البطين في أبوظبي، وبالتحديد في قسم شركة "أدكو".

إشارات: هل يتوافق تطبيق المتحف الذكي مع كل أنواع الهواتف؟

الحمادي: يتوافق التطبيق مع أجهزة مستخدمي النظام أندرويد، وأعمل على تطويره في الوقت الحالي لكي يتوافق مع منصة أجهزة أيفون. بهذا نغطي كل الهواتف الشائعة الاستخدام عالمياً.

إشارات: برنامج "حياك" الخاص بهيئة الأوراق المالية والسلع أول ابتكار تعمل عليه، وكنت طالباً في كلية التقنية العليا. ما هو "حياك"؟

الحمادي: إنه نظام تعريف إلكتروني خاص بالموظفين الجدد في هيئة الأوراق المالية والسلع، أنجزته حين كنت طالباً، ومن خلاله يتم التعريف بالهيئة بطريقة مبتكرة وتفاعلية باستخدام الفيديو.

يطرح التطبيق على الموظف حديث الانتساب إلى الهيئة أسئلة تخص إدارة محددة، فيجيب عليها كي ينتقل إلى الإدارة التي تليها، حتى ينتهي من جميع الإدارات، بعدها يستطيع مباشرة العمل في غضون ساعة تقريباً.

"حياك" استطاع توفير الكثير من الوقت على الهيئة، إذ أن الجولة التعريفية الميدانية كانت تستغرق في السابق أسبوعاً.

إشارات: ما النصيحة التي توجهها للشباب الإماراتي؟

الحمادي: أنصح محبي التقنية بمتابعة أحدث التقنيات، وتجربتها، والمشاركة في المعارض والمؤتمرات ذات الصلة بالتكنولوجيا، ما يسمح لهم بالتعرف على خبرات من جميع أنحاء العالم، والتعرف على أحدث ما وصل إليه العلم.

أما بالنسبة إلى الشباب بشكل عام، فأنصح بأن يكون الإبداع والابتكار أسلوب حياة وفرضاً على كل شخص، حتى تستمر مسيرة النجاح والتقدم لدولة الإمارات.

إشارات: أهناك اختراعات او ابتكارات جديدة تعمل عليها؟

الحمادي: أواصل تطوير تطبيق خاص بنظارة "مايكروسوفت هولولنس"، يعرض حقلاً نفطياً بكل مكوناته، والغرض منه تدريبي وتعليمي دونما حاجة لدخول المتدرب إلى حقل النفط.

يعتبر التطبيق جزءاً من رسالة الماجستير التي أعدها عن التعليم الافتراضي. وأطور تطبيقاً يعرض أبرز معالم أبوظبي لصالح هيئة أبوظبي للسياحة والثقافة، الغرض منه دعم السياحة في دولة الإمارات.

إشارات: هل تفكر بطرح نسخة ثانية من تطبيق "المتحف الذكي" قد يشمل معالم أخرى؟

الحمادي: أعمل على تطبيق جديد بالتقنية نفسها لحساب متحف الشارقة للحضارة الإسلامية.

وبدأت التعاون مع الجهات المعنية بالتراث ليصبح التطبيق قاعدة معلومات متكاملة عن جميع المتاحف الوطنية.

وأستعد هذة السنة أيضاً للمشاركة في الدورة الثالثة من جائزة "ألكسو" للتطبيقات الجوالة على مستوى العالم العربي، وتقام في تونس.

إشارات: ما الذي تتطلع إلى إنجازه مستقبلاً؟

الحمادي: أتطلع إلى أن أكون كادراً إماراتياً يجلب قيمة إلى قطاع تقنية المعلومات، وأن أسخر كل ما تعلمته لخدمة وطني.

كيفين ميتنيك
"ليس هناك شيئ لا يمكن اختراقه!"

كيفين ميتنيك أحد أشهر مخترقي أنظمة الحاسوب في العالم، ومستشار في أمن الحاسوب ومؤلف أميركي. اعتقل في 1995 بعد تورطه بأعمال قرصنة إلكترونية، وسجن خمس سنوات لإدانته بتُهم تتعلق باختراق الأنظمة.

أثارت محاكمته الكثير من الجدل، وحظيت مطاردات الشرطة له بتغطية إعلامية واسعة، لكنه وضع هذا الفصل الأسود من حياته وراء ظهره، وبدأ بكتابة فصل جديد للصالح العام، حتى أصبح الآن أحد أشهر وأنجح الرموز في مجال الأمن الإلكتروني.

> محترفي الخداع الاجتماعي يستخدمون التلاعب لإخضاع الضحية المستهدفة

يدير ميتنيك شركة "ميتنيك سيكيوريتي" للاستشارات الأمنية، ويساعد المؤسسات الكبرى على كشف الثغرات المحتملة ونقاط الضعف في إجراءاتها الأمنية الخاصَّة. يعمل أيضاً مستشاراً لمؤسسات حكومية اعتبرته في الماضي مصدر خطر على الأمن القومي، لكنه يسخّر قدراته من أجل الصالح العام، بدلاً من استخدامها في الجريمة.

كان من الممكن أن يتجنب السجن الانفرادي لو كان تعاون مع الحكومة قبل عقدين، خصوصاً أن الإعلام بالغ في تقدير قدرته على اختراق الأنظمة، بحسب قوله.

وقال ميتنيك: "عندما مثلت أمام المحكمة قبل 20 عاماً، قال المدعي العام الفيدرالي للقاضي إنني أمثل خطراً عظيماً على الأمن القومي، ونصح سلطة تنفيذ الأحكام بمنعي من الوصول إلى أي هاتف في السجن، زاعماً أنني أستطيع الاتصال بقيادة الدفاع الجوي لأمريكا الشمالية، والنفاذ إلى المودم الخاص بهم وإطلاق سلاح نووي! بصراحة، أثار هذا الكلام سخريتي، لأنني لم
أسمع أمراً ساذجاً كهذا من قبل، لكن القاضي اقتنع بما قال المدعي العام، وأمر بحبسي في سجن انفرادي لمدة عام كامل"، حسب ما يؤكد ميتنيك.

تغير العالم منذ ذلك الوقت. بالرغم من أن فكرة الاتصال بمؤسسة عسكرية والوصول إلى شيفرات إطلاق أسلحة نووية عبر هاتف من السجن لا تزال فكرة خيالية.

يقول ميتنيك: "يمكن تنفيذ أفعال مماثلة عن طريق الاحتيال والخداع الاجتماعي لكي تقنع الهدف بالموافقة على الطلب؛ يمكنني على سبيل المثال أن أخاطبك برسالة نصيّة فأجعلها تبدو كأنها مُرسلة من طرف ثالث، أي أنني أستطيع بصفتي مخترقاً أو خصماً أن أسرق بيانات مالية من شركة محددة، من خلال إرسال رسالة إلى المساعد التنفيذي للمدير المالي للشركة، أتظاهر فيها بأنني أتصل من مكتب المدير المالي، فأكتب في الرسالة: "يرجى تحرير التقارير المالية للربع الثالث عندما يتصل كيفين، وأرجو عدم إرسال رسائل نصية أو الاتصال لأنني في اجتماع مهم".

ثم يتساءل ميتنيك: "ما فرص اقتناع المساعد بالخدعة، وإعطائي حق الوصول للتقارير؟". يضيف: "الحظوظ مرتفعة، وهناك مخططات مماثلة تُنفذ بصورة ناجحة يومياً، إذ يبدو أن الأنظمة الحاسوبية ليست عرضة للخطأ وحدها، إنما الموظفون أيضاً الذين يتبنون طرق أمان واهنة، ويفتقرون إلى الوعي الأمني، وهم نقطة الضعف التي ينفذ منها المخترقون".

ليس هناك وفقاً لميتنيك نظام أو جهاز ذكي أو عنوان بريدي أو حتى شخص منيع ضد الاختراق، لكن "إذا كنت ترغب بألا يطلع أي طرف خارجي على اتصالاتك التي تجريها عبر الهاتف أو الحاسوب، فإن الحل الوحيد أمامك هو التشفير".

ويضيف: "أثيرت ضجة حديثاً بعد الإعلان أن الحكومات تستطيع مراقبة الإرهابيين واقتفاء أثرهم إذا ما وافق "واتساب"، وهو أشهر تطبيق للرسائل النصية في العالم، على فك تشفير الاتصالات التي تنتقل عبر الشبكة، ومن ثم إعطاء الحكومات حق الوصول الكامل إليها.

هذا الأمر ولد حالة من القلق بين مستخدمي "واتساب"، في حين لا تزال شركة "فيسبوك"، مالكة "واتساب"، مصرّة على عدم الامتثال لهذه المطالب".

ويتابع ميتنيك أن "التشفير يكون تاماً بين طرفي المحادثة، وهناك تطبيقات للهواتف الذكية توفر خاصية الأمان هذه، أي أنك والطرف الآخر تمتلكان وحدكما مفتاح تشفير الرسائل وقراءتها، غير أن بعض مقدمي الخدمة لا يسمحون بهذا النوع من التشفير".

يضيف: "إذا أراد أحد المخترقين أو الهيئات القانونية اعتراض رسائلك، فلا يمكنهم فعل ذلك إلا بإرسال برنامج خبيث إلى جهازك، لكنهم لا يستطيعون مراقبة الاتصالات وتشفيرها، وهذا ينطبق أيضاً على تطبيق "واتساب".

يسخّر ميتنيك معرفته ومهاراته الآن لخدمة الصالح العام، حتى أصبح يعرف باسم "قرصان القبعة البيضاء"، كمقابل لـ"قراصنة القبعات السوداء" الذين يستهدفون الأنظمة بهدف تدميرها أو كسب مبالغ مالية أو للتسلية ليس إلا، أما مهمته فهي تمكين عملائه من أن يكونوا على أهبة الاستعداد لأي هجمات خبيثة تستهدفهم، وهو يمارس هذه الوظيفة لصالح مؤسسات حكومية وجهات خاصة عالمياً، وتعتمد طبيعة عمله على ظروف كل مؤسسة.

يقول: "ما زلنا نمارس أعمال حماية الأنظمة، ونتجنب كل ما يترك آثاراً عكسية على المؤسسات أو يضر بعملها، من أجل الاختبارات الأمنية، لذلك تسعى الشركات من كل أنحاء العالم لاستئجار خدمات شركتي بهدف مساعدتها على الدخول إلى قطاعات تجارية محددة، إما من خلال استغلال نقاط الخلل التقنية، أو من خلال التلاعب بالموظفين، أو من خلال الاختراق الشخصي، أو حتى باختراق الهواتف المتحركة".

إلى أي مدى تدرك الحكومات ضرورة مواجهة خطر الهجمات الإلكترونية؟
يقول ميتنيك إنها تعي هذا الخطر، حيث تتصل الكثير من المؤسسات الدولية بشركته يومياً طلباً لدعمه وخدماته.

يضيف: "اتصل بي حديثاً وسيط يطلب استغلال نقاط ضعف في برمجيات وثغرات أمنية لم يكتشفها أو يصلحها المطورون. وتواصلت معنا بعض الجهات لمحاولة شراء أسلحة إلكترونية واستخدامها في أغراض خاصة، لكننا لا نقدم كل الخدمات للمؤسسات الأجنبية، ونعتبر هذا القرار غير قابل للنقاش".

لم تسلم انتخابات الرئاسة الأمريكية الأخيرة من هجمات الاختراق أيضاً، إذ زعم البعض أن عدداً من القراصنة اخترقوا قاعدة بيانات المصوتين وتسببوا بخسارة هيلاري كلينتون أمام دونالد ترامب، وهي ليست المرة الأولى التي تُستهدف فيها الانتخابات الأمريكية إلكترونياً بهدف التأثير في النتائج.

> الموظفون هم أبرز نقاط الضعف في الشركات والمؤسسات ومنها ينفذ المخترقون

يقول ميتنيك: "صارت هذه عادة، لكن خلال الاختراقات الإلكترونية الأخيرة وجهة الحكومة أصابع الاتهام إلى جهة محددة وهي اللجنة الوطنية الديمقراطية".

يضيف ميتنيك: "على كل المؤسسات العامة والشركات الخاصة أن تتسلح بإجراءات أمنية أقوى فلا يوجد هناك شيئ لا يمكن اختراقه".

ويقول ميتنيك: "لا ننكر أن أغلبية الشركات تتعرض للاختراق الذي يبدأ عادةً ببريد إلكتروني بسيط، ثم يفرض المخترق كامل سيطرته على أنظمة الشركة، وعندها يستطيع التحرك بسهولة داخل شبكة الشركة. ويبدأ الأمر بإرسال ملف عادي إلى الشركة بمجرد فتحه يحظى المخترق بالسيطرة الكاملة على الحاسوب، لذلك نتطلع إلى رفع مستوى الوعي لدى الأشخاص والمؤسسات وحثهم على إعادة التفكير في آلياتهم الدفاعية واتخاذ إجراءات استباقية حتى لا يقعوا ضحايا هجمات مماثلة في المستقبل".

ما الذي يجب أن تفعله المؤسسات والأفراد في غياب أي نظام منيع ضد الاختراق؟ يقول ميتنيك: "يجب على الأفراد والمؤسسات أن يتولوا الأمور بأنفسهم، وأن يطبقوا الإجراءات الوقائية؛ أي أن يستخدموا الهجوم بدلاً من الدفاع، وأن يقسّموا آليات الدفاع إلى طبقات، حتى تشكل حائلاً أمام أي مخترق أو خصم يحاول النفاذ إلى شبكاتهم. هذه هي الخطوات الأكثر أهمية لتجنب مثل هذه المخاطر".

إطلاق "إعلان دبي" لتعزيز الأمن الإلكتروني للطيران

سجلت دولة الإمارات سبقاً جديداً في عالم الأمن الإلكتروني، بإطلاق "إعلان دبي" الذي يتناول الأمن الإلكتروني في قطاع الطيران المدني. يؤكد الإعلان على ضرورة تحصين أنظمة البنية التحتية الحسّاسة للطيران المدني، وحماية المعلومات من التهديدات الإلكترونية المتزايدة في عصرنا الحاضر، وقد تبنته المنظمة الدولية للطيران المدني (ايكاو)، وجرى إطلاقه خلال قمة ومعرض الإيكاو الخاصّة بالأمن الإلكتروني، التي استضافتها دبي تحت رعاية صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، وبحضور ممثلين عن أكثر من ثمانين دولة.

وأكد معالي المهندس سلطان بن سعيد المنصوري وزير الاقتصاد، رئيس مجلس إدارة الهيئة العامة للطيران المدني، أن دولة الإمارات تلعب "دوراً فاعلاً في تعزيز منظومة أمن وسلامة الطيران المدني على المستوى الإقليمي والدولي"، وأضاف أن اهتمام دولة الإمارات بقطاع الطيران المدني يأتي من حقيقة أن هذا القطاع يعد "أحد أهم المكونات التي ستسهم في ازدهار الدولة وتحويلها إلى مركز عالمي للتجارة والسياحة يكون قادراً على الدخول بثقة في مرحلة ما بعد النفط". ووصف مدير عام الهيئة العامة للطيران المدني سيف السويدي "إعلان دبي" بالتاريخي، حيث يؤسّس لمرحلة جديدة من الالتزام والتعاون الدولي في مكافحة التهديدات الأمنية الإلكترونية. وقال "إن ضمان التعاون بين الجهات الحكومية والشركاء الدوليين في قطاع الطيران والعديد من الجهات المعنية بمكافحة تهديدات الأمن الإلكتروني هو أمر بالغ الأهمية"، مضيفاً أن يوم إصدار إعلان دبي خلال قمة الأمن الإلكتروني "هو يوم نفخر فيه بقطاع الطيران وقدرته على زيادة مستوى التعاون بين الدول عبر الحدود". وقال السويدي إن الهيئة بصدد إنشاء مركز عمليات لمراقبة الهجمات والتهديدات الإلكترونية في قطاع الطيران المدني، وذلك كخطوة مبكرة لمواجهة مخاطر القرصنة الإلكترونية في ظل تزايد ارتباط القطاع بالإنترنت وحفظ البيانات على السحابة.

ويعكس "إعلان دبي" الجهود التي تقوم بها دولة الإمارات بالتعاون مع باقي الجهات المختصة في التحذير من خطر التهديدات الإلكترونية على قطاع الطيران. وينصّ على تقليل الخطر الذي تشكله التهديدات الأمنية على المستوى الإلكتروني بهدف تعزيز القدرة على التصدي لمثل هذه التهديدات في مجال الطيران المدني، والتأكد من تأسيس الإطار التشريعي بشكل مناسب، والتعاون وتبادل المعلومات بين الدول والشركاء الآخرين، وتأكيد التزام الجميع على تطوير نظام قوي، فعال ومستدام للطيران المدني.

الأمن الإلكتروني
10 نصائح للحماية من الهجمات الإلكترونية

يسعى القراصنة إلى الحصول على بيانات المستخدمين الشخصيَّة، واستعمالها لانتزاع مكاسب مادية وغير مادية من الضحية. ومع التطور التكنولوجي والتشدد في إجراءات الوقاية الإلكترونية، يطوِّر القراصنة طرقهم وأساليبهم باستمرار.

إنها معركة لا يمكن حسمها، لكن يمكن التقليل من مخاطرها وتفادي الإصابة بالبرمجيات الخبيثة. هذه بعض النصائح للوقاية والحماية.

1 كن أكثر حرصاً عند استخدام مواقع التواصل الاجتماعي

شبكات التواصل الاجتماعي بيئة خصبة للقراصنة، وازدادت الاختراقات عبرها بنسبة كبيرة خلال السنوات الماضية، خصوصاً أن غالبية المستخدمين يشاركون البيانات الشخصية بصورة غير مسؤولة. ابدأ بحماية نفسك بحجب عنوانك ورقم هاتفك وتاريخ ميلادك، وأي معلومات أخرى تُستخدم لتزييف هويتك. لا بأس أيضاً لو أخفيت "المجموعات" التي تنتمي إليها و"قوائم الأصدقاء" عن المتربصين، فكلما جمع القراصنة معلومات أكثر عنك، بدت خططهم للإيقاع بك أكثر إقناعاً. اضبط إعدادات الخصوصية على أقصى درجات الأمان، واجعل الوصول إلى بياناتك وصورك مقتصراً فقط على العائلة والأصدقاء، ولا تتشارك أي بيانات شخصية مع غرباء.

2 استخدم بطاقات الائتمان لا بطاقات الدفع

استخدام بطاقات الائتمان على الإنترنت أكثر أماناً، لأنه يؤمن مستوى إضافياً من الحماية لا توفره البنوك أو بطاقات الخصم. فعند استخدام بطاقة الخصم، تُسحب الرسوم فوراً من حسابك المصرفي، فلا سبيل لمعرفة إذا كان هذا الاستخدام مصرحاً به أم لا. وحتى إذا بلغت عن الاختراق، فإن استرداد الأموال المسروقة قد يستغرق أسابيع، هذا إذا استرددتها أساساً. لهذا، استخدم بطاقات الائتمان دائماً لمشترياتك الإلكترونية. وتعد «فيزا» إحدى الشركات الرائدة في وسائل الدفع الآمن، وتمتلك برامج متطورة تتيح اكتشاف التعاملات المشتبه بها، من دون الحاجة للاتصال بالعميل. وهناك ممارسات يجب تجنبها في الدفع على الإنترنت، ومنها عدم تخزين بيانات البطاقة للاستخدام المستقبلي، فإذا تعرضت المؤسسة التي تخزّن بياناتك فيها للاختراق، قد تتكبد خسائر فادحة. وقد يبدو هذا الاحتمال مستبعداً، إلا أنه وارد، فتفادى الوقوع ضحية مثل هذه الاختراقات، وتذكر أن إدخال البيانات لا يستغرق سوى دقيقة واحدة، لكنه يعفيك من المخاطرة.

3 استخدم ميزة التحقق بخطوتين

لا يستطيع القراصنة النفاذ إلى حسابك إذا كنت تستخدم هذه الميزة، حتى لو امتلكوا كلمة المرور. فرموز التحقق سترُسل إلى هاتفك كلما حاول أحدهم النفاذ إلى حسابك من جهاز آخر. هذه الميزة متوافرة في البريد الإلكتروني وفي الخدمات السحابية. استخدم هذه الميزة أثناء تسجيل الدخول، فتضيف إلى حسابك طبقة أمان إضافية. يمتلك فيسبوك وتويتر هذه الميزة أيضاً.

4 كن على علم أن أجهزة "ماك" ليست منيعة مثلها مثل أجهزة الحاسب الآلي الشخصي

ستيف جوبز بكل عبقريته لم يستطع ابتكار نظام تشغيل منيع ومقاوم للاختراق. وإذا نجت منتجات أبل من الوقوع ضحية للبرامج الخبيثة، فهذا يعود إلى أن القراصنة رأوا في اختراقها مضيعة للوقت، بسبب قلة مستخدميها. لكن عدداً لا بأس به من القراصنة يستهدفون أجهزة "ماك"، لذا كن حذراً دائماً، بغض النظر عن نظام التشغيل الذي تستخدمه.

5 استخدم برنامجاً مضاداً للفيروسات

على الجميع استخدام برامج حماية من الفيروسات وبرامج حماية من التجسس. احرص على تحديث هذه البرامج بانتظام، وضبطها على وضعية التحديث التلقائي. بعض المبرمجين لا يستخدمون برامج الحماية بزعم أنها تتسبب في إبطاء نظام التشغيل، لكن الأنظمة المصابة أبطأ من السليمة. لنتذكر أن الوقاية خير من العلاج.

6 دقق في عناوين المواقع الإلكترونية

يجب التدقيق في كل رابط تنوي النقر عليه وفي كل بريد تتلقاه. بعض القراصنة يعمد إلى إنشاء موقع إلكتروني مطابق للموقع الأصلي للمصرف الذي تتعامل معه أو الشركة التي تطلب خدماتها، ودخولك إلى الموقع المزيف يعرض حاسوبك للاختراق وفقدان البيانات الشخصية. يمكنك كشف هذه الخدعة بسهولة: فعادة ما تكون هناك أخطاء إملائية في اسم الموقع المزيف، أو ربما تجد مثلاً الرابط www.bank.money.com بدلاً من www.bank.com. وليست هناك بالطبع بنوك تستخدم عناوين إلكترونية مماثلة.

7 تجاهل الرسائل الإلكترونية التي تطلب بيانات شخصية

مخططات التصيد الاحتيالي أصبحت أكثر تطوراً من السابق، وانتهت فترة الرسائل التي تخدعك بعبارات مثل "مبروك! فزت بمبلغ 4,500,000 دولار في اليانصيب، ويرجى إرسال بياناتك المصرفية لاستلام المبلغ". هذه المخططات استبدلت ببريد مزيف يبدو كأنه مرسل من البنك الذي تتعامل معه، أو بطلب لتحديث معلومات شخصية من موقع يبدو صحيحاً، لكن ليس هناك أي بنك أو مؤسسة ستطلب إرسال بيانات شخصية عبر البريد الإلكتروني. تأكد دائماً من صحة عنوان البريد الإلكتروني للمُرسل، وقد تكتشف أنه ليس بريداً رسمياً يشير إلى أنه مُرسل من قِبل موظف أو مؤسسة، لذلك عليك تجنّبه.

8 احذر شبكات الواي فاي العامة

تعتبر هذه الشبكات كنزاً للقراصنة، لأنها غالباً غير مشفرة وغير محمية. عندما تغادر البيانات جهازك وتتجه نحو وجهة محددة، يتم اعتراضها واختراقها غالباً. الخبراء ينصحون بعدم إجراء أي معاملات مالية أو مصرفية على شبكة عامة.

9 استخدم أكثر من بريد إلكتروني واحد

البعض يستخدم كلمة المرور نفسها لكل حساباتهم، والبعض يستخدم بريداً إلكترونياً واحداً لكل شؤونهم، بدءاً من الصرافة الإلكترونية وصولاً إلى شبكات التواصل الاجتماعي، وهذا خطأ.

ننصحك بأن تمتلك أكثر من بريد واحد، تخصص أحدها لمعاملاتك المصرفية، وآخر لحياتك الاجتماعية، وثالث للتسوق عبر الإنترنت، ما يبقي شؤونك منفصلة، فإذا تعرض بريد واحد للاختراق، تبقى الحسابات الأخرى بأمان. تخصيص بريد واحد لكل مجالات الحياة يتيح للقراصنة إذا اخترقوه للحصول على كنز من معلوماتك الشخصية، كالبيانات المالية وبيانات جواز السفر والعناوين وأرقام الهواتف وغيرها.

10 لا تنقر على روابط غير موثوقة

استخدامك للإنترنت مراقب دائماً بفعل خوارزميات متقدمة، ترصد كل ما تفعله. هذه المعلومات متاحة للشركات التي ترسل عروضاً بناء على توجهاتك وميولك. إذا كنت من عشاق التسوق عبر الإنترنت، توقع أن تكون هدفاً لإعلانات تحاول إقناعك بشراء شيء مشابه لما اشتريته أو تبحث عنه.

هذه المعلومات متاحة للقراصنة أيضاً، وتحتوي رسائلهم إليك على برمجيات خبيثة هدفها انتزاع بيانات خاصة، لذا تجاهل كل الرسائل التي تطلب رأيك في مواقع التسوق الإلكتروني على سبيل المثال، لأن هذه المواقع موطن للرموز الضارة. يستهدف القراصنة الحاسوب ببرمجيات خبيثة بعد إقناع المستخدمين بالنقر على رابط معين أو فتح رسالة مرفقة، لأنهم يعرفون ما سيجذب انتباهك، ومن ثم يرسلون إليك رسائل معدة خصوصاً لك، تقنعك بالنقر على ما يبدو جذاباً في الظاهر، لكنه فخ خبيث.

7 معتقدات خاطئة عن فيروسات الحاسوب

الأفكار الشائعة عن فيروسات الحاسوب والبرامج الخبيثة كثيرة، سواء لجهة أسبابها أو الأضرار التي تتسبب بها وآثارها الطويلة المدى. تعرّف على قائمة "إشارات" لأشهر هذه المعتقدات والمفاهيم الخاطئة.

1 جدار الحماية يقي الحاسوب من الفيروسات

لا يحمي جدار الحماية الحاسوب من برامج التجسس أو فيروس "تروجان" أو أي فيروس آخر، لكنه قادر على حماية الجهاز من نفاذ بعض البرامج الخبيثة مثل ديدان الإنترنت، وتستخدم الشبكة كوسيلة للتنقل. ميزة جدار الحماية أنه يحذر المستخدم إذا بدأ برنامج خبيث بإرسال بيانات إلى النظام.

2 الفيروسات تتلف جهاز الحاسب الآلي

الفيروسات لا تتلف جهاز الحاسب الآلي على الإطلاق بل تتلف البرامج وأنظمة التشغيل فقط، وفي أسوأ الأحوال قد يضطر المستخدم إلى محو محتوى نظام المدخلات/المخرجات في جدار الحماية نتيجة لفيروس خطير، لكن الحاسب الآلي يظل سليماً.

3 الإشعارات المتكررة تعني وجود فيروس

هذا الافتراض غير صحيح. فالملف لا يتعرض للتلف بسبب الفيروسات، بل بسبب خطأ ينتج عن إعادة تشغيل مفاجئة أو تلف القرص الصلب أو وجود برمجيات غير سليمة، والقائمة تطول.

4 إعادة تثبيت الويندوز ونسخ الملفات يحلان المشكلة

إذا أصيب الحاسوب بفيروس، فإن إعادة تثبيت نظام التشغيل "ويندوز" وإعادة تحميل كل الملفات سيصيب الجهاز بالفيروس مرة أخرى. يجب مسح الملفات وإزالة التالفة من بينها قبل إعادة تحميلها.

5 برامج الحماية فعالة مئة بالمئة

بعض برامج مكافحة الفيروسات تحظر تنزيل ملفات قد تكون سليمة، فقط لأنها تشتبه باحتوائها على فيروس. الطريقة المثلى للتأكد من سلامة الملفات هي مسحها على موقع VirusTotal، وليس الاعتماد على برامج مكافحة الفيروسات فقط.

6 شاشة الموت الزرقاء (BSOD) تعني وجود فيروس

شاشة الموت الزرقاء هي أسوأ عطل قد يصيب الحاسوب، لكنها لا تعني وجود فيروس دائماً. إن السبب الأول لظهورها هو غالباً تعرض القرص الصلب للتلف، وأفضل طريقة لحل المشكلة هي العثور على رمز الخطأ والبحث عن طرق تصحيحه على الإنترنت.

7 الهواتف الذكية لا تصاب بفيروسات

إذا صح أن أغلبية الفيروسات قد جرى تصميمها لكي تستهدف أجهزة الحاسوب بالذات، باعتبار أن تلك كانت الأجهزة الوحيدة المستخدمة حتى فترة قريبة، فإن شعبية الهواتف الذكية تزداد بسرعة، وأضحت تتفوق على أجهزة الحاسوب عدداً. ويتصل معظم المستخدمين اليوم بشبكة الإنترنت عن طريق هواتفهم الذكية، ما يجعلهم عرضة أكثر فأكثر للفيروسات على أنواعها. ليست هناك إذاً منصات مضمونة كلياً، ما يوجب الحذر الدائم.

انتحال الشخصية إلكترونياً... هل ستكون أنت الضحية التالية؟

شهدت السنوات العشر الماضية أكثر من 50 مليون حالة انتحال شخصية بحسب "دراسة انتحال الشخصية ٢١٠٧" الصادرة عن دار أبحاث "جافلين استراتيجي آند ريسريش"، ولفتت إلى أن هذا النوع من الجرائم صار يمثل تهديداً حقيقياً، بعدما أضحى سمة خاصة من سمات العالم الافتراضي. وتزداد جرائم انتحال الشخصية بصورة منتظمة، فيتكبد الضحايا بسببها خسائر مادية كبيرة، ويدخلون أحياناً في تعقيدات قانونية متعددة. وبالرغم من الطابع الجدي لهذا التهديد، إلا أن الكثيرين لا يأخذون هذا الأمر على محمل الجد، حيث يسود الاعتقاد أننا قد نكون بمأمن من الوقوع ضحية لمثل هذه الجرائم، فنتساءل في سرنا: "لمَ قد يرغب أحدهم بانتحال هويتي؟".

يمثل انتحال الهوية مشكلة جدية وخطيرة في آن واحد. فحين يتمكّن القرصان الإلكتروني من انتحال هويتك والوصول إلى بياناتك الشخصية، فإن النتيجة ستكون كارثية، حيث تتعدد المشكلات التي يمكنه توريطك فيها، من إفراغ حسابك المصرفي واستخدام الحد الأقصى من رصيد بطاقاتك الائتمانية، إلى إقحام اسمك في قضايا جنائية، أو التنقل والسفر مستخدماً هويتك وجواز سفر باسمك.

ما الإشارات التي تدل على انتحال هويتك؟

كثيرة هي الإشارات التي تدل على أن هويتك قد تعرضت للسرقة أو لسوء استخدام، وعليك أن تبادر إلى التصرف بسرعة وإبلاغ المعنيين بالأمر إذا صادفت واحدة أو أكثر من هذه الإشارات:

- حسابك المصرفي يُظهر عمليات سحب أو تحويلات مالية من رصيدك لم تقم بها أو تمت من دون علمك.
- عدم تسلم الفواتير المصرفية الخاصة بمشترياتك التي قمت بها عبر بطاقات الائتمان.
- ارتجاع أحد الشيكات التي أصدرتها بسبب عدم وجود رصيد كافٍ في حسابك المصرفي.
- شركة التأمين الصحي تزودك بكشوفات تظهر أن أحدهم انتحل شخصيتك واستخدم بطاقتك.
- تتلقى معلومات بأن اختراقاً حدث داخل مؤسسة تحفظ فيها بياناتك الشخصية.

ما الذي ينبغي عليك فعله؟

حين تكتشف أن طرفاً ما قد انتحل شخصيتك وأساء استخدام هويتك، فعليك المسارعة فوراً إلى إبلاغ الجهات المعنية بالأمر. وعليك أن تذكر أن طرق انتحال الشخصية تتعدد وتتنوع، حيث تتراوح بين استعمال بطاقاتك الائتمانية أو بطاقات التسوق الخاصة بك، أو محاولة فتح حسابات مصرفية باسمك، أو الحصول على قرض عليه توقيعك. إن كل ما تقدم جرائم يعاقب عليها القانون، وعليك الاتصال فوراً بالشرطة، وكذلك الجهات المعنية، لإبلاغها بالوقائع وبالتفاصيل.

وفي حين تستغرق عملية إعادة الأمور إلى طبيعتها وقتاً، فإن عدم اتخاذ إجراءات فورية يزيد المشكلة تعقيداً، وقد تزداد خسائرك المادية وغير المادية على المدى الطويل. من هنا، ينبغي أن تبقى على يقظة دوماً، وأن تتحقق من عدم ظهور أي أنشطة غير طبيعية باسمك، والأهم من ذلك هو أن تحمي مستنداتك وبياناتك وبطاقاتك الشخصية بحرص بالغ.