العدد 02 فبراير 2018

إشارات
Esharat

لفضـــاء إلكـــتروني ـــي آمـــن

حمدان بن محمد يعتمد خطط ومشاريع مؤسسة دبي للمستقبل لعام 2018

دليلك لتصفّح آمن على الإنترنت

مشروع شهادات دبي الرقمية مع المهندسة عفراء بن فارس

كيف ستغير تقنية البلوك تشين مستقبل دبي

إنجاز على مسار التحول الذكي

تعتبر مذكرة التفاهم التي وقعها "مركز دبي للأمن الإلكتروني" مع "مكتب دبي الذكية" إنجازاً رفيع المستوى في مسيرة تحول مدينة دبي إلى المدينة الأكثر ذكاءً على مستوى العالم، وشهد توقيعها صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، وسمو الشيخ حمدان بن محمد بن راشد آل مكتوم، ولي عهد دبي رئيس المجلس التنفيذي، وسمو الشيخ مكتوم بن محمد بن راشد آل مكتوم نائب حاكم دبي. وإذا كان هذا يدل على شيء فإنه يدل على مدى أهمية هذه الشراكة لمستقبل دبي.

تهدف هذه الاتفاقية التي تشرفت بتوقيعها مع سعادة الدكتورة عائشة بن بطي بن بشر، المديرة العامة لدبي الذكية، في المقام الأول إلى حماية ثروة دبي الرقمية وتفعيل الشهادات الرقمية وتحقيق أعلى درجات الأمان لبيانات المدينة، وذلك من خلال إدارة المنظومة الرقمية بأكملها، بما في ذلك البيانات وتخزين البيانات ومعالجتها مثل تقنية الحوسبة السحابية، والإجراءات والأجهزة والبرامج المصممة لجمع ومعالجة المعلومات، والتحول إلى التكنولوجيا الذكية، إلى جانب سياسات وأنظمة المعاملات غير الورقية ، والتوقيع الرقمي والهوية الرقمية، بالإضافة إلى محاور العيش الذكي ومكونات أخرى.

وستساعد مبادرة ثروة دبي الرقمية على دعم أكثر من 1100 خدمة ذكية، و 121 مبادرة ذكية ومن المتوقع أن تحقق نتائج اقتصادية واعدة في ثلاث سنوات تصل قيمتها إلى 33.8 مليار درهم. وتنص مذكرة التفاهم كذلك على تعاون الطرفين في حماية الثروة الرقمية وإصدار الشهادات الرقمية للمشاريع الحيوية التي ستقود دبي إلى المستقبل.

مع إطلاق إشارة البدء في تدشين البنية التحتية الرقمية المستقبلية سنشهد ارتفاعاً في مستوى الأمن الإلكتروني لكافة الخدمات الرقمية في دبي وتقدم هذه الشراكة الفرصة للقطاعات الحكومية والخاصة لتوفير أفضل الحلول التي تتميز بالسهولة والسرعة إلى جانب المصداقية والأمان، الأمر الذي سيسهم حتماً بقدر كبير في تحويل دبي إلى المدينة الأكثر ذكاءً وأماناً في العالم ويحقق أهداف مركز دبي للأمن الإلكتروني كما نصت عليه استراتيجيته.

وتعتبر هذه الاتفاقية جزءاً جوهرياً ضمن مبادرة الثروة الرقمية واستراتيجية إنترنت الأشياء، وسوف تلبي الأهداف التي أرساها صاحب السمو الشيخ محمد بن راشد آل مكتوم لتفعيل الشهادات الرقمية، والتي ستكون عاملاً رئيسياً في الحفاظ على أمن وسلامة بياناتنا وثروتنا الرقمية. وتأتي هذه الشراكة الآن لتوحد أهدافنا وتدفعنا نحو تحويل دبي إلى المدينة الأذكى والأكثر أماناً على مستوى العالم.

يوسف حمد الشيباني
المدير العام
مركز دبي للأمن الإلكتروني

اقرأ في هذا العدد

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

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

المدير العام
يوسف حمد الشيباني

مدير التحرير
عامر شرف

سكرتيرة التحرير
شيخة عيسى
ميثاء خالد

التحرير والتصميم
7g media
سفن جي ميديا للاستشارات

هيئة التحرير
أماني أبوسيدو
دان شارتر
أحمد مرسال
نيكول رهبان

التصميم الفني
سري إي إس
أوس رحال

الرسم
براين رايس
جوزيف كارتانو

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

خذ حذرك.. فليس كل ما يلمع ذهباً!

معظم ضحايا الجرائم الإلكترونية يقعون فريسة سهلة للقراصنة بسبب تصديقهم الرسائل التي تعدهم بمكافآت أو جوائز مجزية ولكنها ليست إلا مجرد طُعم لاصطيادهم. فإذا تلقيت مثل هذه الرسائل فلا تنقر على الرابط الموجود فيها، وتذكر ما يلي:

- إغداق المكافآت بلا سبب! يرتبط في أغلب الأحيان بخديعة تُحاك ضدك.
- إذا وعدتك الرسالة الإلكترونية بشيء غير واقعي فالزم الحذر.
- أخبر كل من حولك بشأن هذه الرسالة.

كن يقظاً وحافظ على أمنك الإلكتروني

محمد بن راشد آل مكتوم يشهد توقيع مذكرة تفاهم بين "مركز دبي للأمن الإلكتروني" و"دبي الذكية" لحماية ثروة دبي الرقمية

> صناعة المستقبل في دولة الإمارات أثمرت بناء منظومة رقمية أصبحت جزءاً استراتيجياً من ثرواتنا الوطنية
>
> **محمد بن راشد آل مكتوم**

شهد صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، وسمو الشيخ حمدان بن محمد بن راشد آل مكتوم، ولي عهد دبي رئيس المجلس التنفيذي، وسمو الشيخ مكتوم بن محمد بن راشد نائب حاكم دبي، توقيع مذكرة تفاهم بين "مركز دبي للأمن الإلكتروني" و"دبي الذكية" لحماية ثروة دبي الرقمية. قام بتوقيع الاتفاقية سعادة يوسف الشيباني، المدير العام لمركز دبي للأمن الإلكتروني وسعادة الدكتورة عائشة بن بطي بن بشر، المديرة العامة لدبي الذكية، وتضمنت المذكرة تنفيذ الشهادات الرقمية لإماراة دبي للمشاريع الحيوية التابعة للمدينة الذكية.

وتم التوقيع على مذكرة التفاهم والمصادقة عليها إلكترونياً، باستخدام البنية التحتية للشهادات الرقمية. وتعد المرة الأولى التي يجري فيها اعتماد التوقيع الإلكتروني الرقمي في مذكرة تفاهم في الإمارات.

وجاء توقيع الاتفاقية على هامش إطلاق مبادرة الثروة الرقمية واستراتيجية إنترنت الأشياء، التي تأذن ببداية تحول دبي إلى مدينة ذكية، حيث سيتم إتاحة وتخزين ومعالجة البيانات والتحول إلى التكنولوجيا الذكية بما يحقق الراحة والسعادة للمتعاملين.

وقال صاحب السمو الشيخ محمد بن راشد: "صناعة المستقبل أثمرت بناء منظومة رقمية أصبحت جزءاً استراتيجياً من ثرواتنا الوطنية في عصر الثورة الصناعية الرابعة، وهذه المنظومة الرقمية من بنية تحتية ذكية وبيانات هي ثروة على الجميع الحفاظ عليها".

وأضاف سموه: "نريد أن تكون شهادات دبي الرقمية أساساً تستند عليه كافة الخدمات الذكية للحفاظ على ثروة دبي الرقمية وبإطلاق تلك الشهادات واستراتيجية إنترنت الأشياء... نعلن اكتمال الحياة الذكية في دبي بكافة أبعادها وقد وجهنا جميع المؤسسات الحكومية في الإمارة للتعاون في تحقيقها بنسبة 100% بحلول 2021".

وأوضح سعادة يوسف الشيباني، المدير العام لمركز دبي للأمن الإلكتروني: "من خلال التعاون مع دبي الذكية، سنتمكن من مواجهة التحديات الإلكترونية لجعل مدينة دبي الأذكى والأكثر أماناً إلكترونياً على مستوى العالم"، مؤكداً أهمية تبادل المعرفة والخبرات في كل المشاريع المشتركة، لتمكين الجهات المعنية من تأمين أنظمتها، إضافة إلى ضرورة الامتثال بأفضل المعايير الدولية ومعايير نظام أمن المعلومات الخاص بإمارة دبي.

وتتضمن المذكرة جوانب الشراكة في مجالات تبادل المعلومات ذات الاهتمام المشترك عن المشاريع، سواء في مراحل التخطيط والتنفيذ والمتابعة واستخدام المعلومات المنشورة وإعادة استخدامها، مثل المعايير المعتمدة لأمن المعلومات، والممارسات والخبرات في مجال المدن الذكية والأمن الإلكتروني، وكذلك الاستفادة من الأبحاث والدراسات المعنية في مجالات التقنيات الحديثة، مثل البلوك تشين والذكاء الاصطناعي والبيانات الضخمة وغيرها من التقنيات.

وتتولى سعادة الدكتورة عائشة بن بطي بن بشر مسؤولية التحول إلى التكنولوجيا الذكية في دبي، إضافة إلى إطلاق نظام إدارة الحشود في دبي كأول مشروع تقني ضمن استراتيجية إنترنت الأشياء، حيث يتم من خلاله تنظيم الحشود في دبي في المواسم الأكثر ازدحاماً بالتجمعات لزيادة الأمان والسلامة، إذ تعد دبي واحدة من أشهر المدن العالمية التي تشهد ازدحامات بشرية في المواسم والمناسبات مثل الاحتفال بالعام الجديد. إذ يعمل نظام إدارة الحشود على تحليل البيانات اللحظية وتوفير التصورات الضرورية لصناعة القرارات الذكية.

وقالت سعادتها: "عندما أطلق صاحب السمو الشيخ محمد بن راشد آل مكتوم استراتيجية دبي الذكية، قبل نحو ثلاث سنوات، حرصنا على أن تكون بنيتنا التحتية متوافقة مع احتياجات الحياة المستقبلية التي نريدها للناس، وقادرة على استثمار الكم الهائل من البيانات الناتجة عن الحياة في أكثر مدن العالم ازدحاماً. وبإطلاق استراتيجية إنترنت الأشياء، سنقدم للناس في دبي تجارب معيشية لم يعهدوها من قبل."

ويرتكز إنترنت الأشياء على الربط بين مختلف الأجهزة الذكية التي نستخدمها يومياً، بما في ذلك إشارات المرور ومستشعرات الطقس، ومستشعرات المرور، والعدادات الذكية، والحافلات، والقطارات وغيرها. وتشكل البيانات التي يتم جمعها مع كل هذه الأجهزة جزءاً كبيراً من ثروة دبي الرقمية، لذلك ستشمل الشراكة بين "مركز دبي للأمن الإلكتروني" و"دبي الذكية" تأمين هذه البيانات إضافة إلى إصدار شهادة رقمية للمشاريع الحيوية بالمدينة الذكية. وبموجب هذه المذكرة يحق لمركز دبي للأمن الإلكتروني الإشراف على الأمن الإلكتروني لكافة الأجهزة الإلكترونية والبيانات، إضافة إلى تنظيم عملية إصدار الشهادات الرقمية.

> نريد أن تكون شهادات دبي الرقمية أساساً تستند إليه كافة الخدمات الذكية بحلول عام 2021 للحفاظ على ثروة دبي الرقمية
>
> **محمد بن راشد آل مكتوم**

وأضافت الدكتورة عائشة بن بشر: "دخلت دبي الذكية مرحلة جديدة في مسيرتها، بإطلاق صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، مبادرة المحافظة على الثروة الرقمية لإمارة دبي. وتعتبر هذه المذكرة من الدعائم الاستراتيجية لتنفيذ توجيهات سموه بجعل شهادات دبي الرقمية الأداة الأولى في الحفاظ على أمان البيانات والثروة الرقمية في دبي".

وأشارت: "الأمان الإلكتروني وسهولة تدفق المعلومات هما حجر الأساس لتمكين عمليات التحول الذكي"، موضحةً أن عملية التحول الذكي لإمارة دبي تتطلب تعاون وجهود كل الجهات الحكومية والخاصة وتضافرها، لضمان تطبيق أفضل المعايير لمستوى جودة الخدمات الذكية المقدمة وشفافيتها، وتتيح الشراكة مع مركز دبي للأمن الإلكتروني آفاقاً أكثر رحابة لتطبيق أفضل الممارسات في مجال الأمان الإلكتروني، وتوفر الفرصة للتعرف إلى التحديات ومعالجتها ووضع الحلول.

حمدان بن محمد يعتمد خطط ومشاريع مؤسسة دبي للمستقبل لعام 2018

اعتمد سمو الشيخ حمدان بن محمد بن راشد آل مكتوم، ولي عهد دبي رئيس مجلس أمناء مؤسسة دبي للمستقبل، خطط ومشاريع مؤسسة دبي للمستقبل للعام 2018.

حمدان بن محمد: دبي بوابة للعلوم ومركز لصناعة المستقبل

أكد سمو الشيخ حمدان بن محمد بن راشد آل مكتوم، أن دبي بما تحققه من إنجازات، بسرعة فائقة، وضمن خطط محددة، لم تعد تقود الركب إلى المستقبل فحسب، وإنما أصبحت تُصدّر المستقبل وأدواته إلى العالم.

وشدد سموه على أهمية مواصلة هذا النهج بمضاعفة الجهود وتوظيف الطاقات وبلورة أحدث أساليب العمل الحكومي القائمة على الابتكار وسرعة الإنجاز وتوسيع الخطى لتحقيق المستهدفات، تنفيذاً لتوجيهات صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، بتحويل دبي إلى مدينة مستقبلية وبوابة عالمية للعلوم والتقنيات المتقدمة، ومركز دولي لصناعة المستقبل.

واعتمد سموه لدى ترؤسه اجتماع اللجنة التنفيذية لمؤسسة دبي للمستقبل بمقر المؤسسة في أبراج الإمارات، بحضور سمو الشيخ مكتوم بن محمد بن راشد آل مكتوم، نائب حاكم دبي، ومعالي محمد عبدالله القرقاوي، نائب رئيس مجلس أمناء مؤسسة دبي للمستقبل والعضو المنتدب، خطط المؤسسة ومشاريعها للعام 2018.

حمدان بن محمد يشهد ختام الدورة الثالثة من برنامج مسرعات دبي المستقبل

أكد سمو الشيخ حمدان بن محمد بن راشد آل مكتوم أن الرؤية الحكيمة لصاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، تقود دبي بخطى متسارعة وثابتة نحو تشكيل نموذج عالمي لمدن المستقبل بأساليب عمل استثنائية تطور حلولاً مبتكرة للتحديات.

جاء ذلك، لدى زيارة سموه مقر برنامج مسرعات دبي المستقبل، حيث شهد فعاليات اختتام الدورة الثالثة من البرنامج وتوقيع عدد من الاتفاقيات ومذكرات التفاهم بين الجهات الحكومية في الإمارة ونخبة من أبرز الشركات العالمية المشاركة في فعاليات الدورة الثالثة من مسرعات دبي المستقبل.

وقال سموه: "إن ما تحقق من نتائج خلال ثلاث دورات لمسرعات دبي المستقبل يؤكد أن دبي ماضية بثقة نحو المستقبل وقد هيأت البيئة الحاضنة والمحفزة لتسريع المسار نحو تحقيق الأهداف، وعملت على تطوير خدمات مبتكرة وفعالة في القطاعات التي تمس حياة أفراد المجتمع، وتسهم في تعزيز سعادتهم".

وأشاد سموه بالدور الفاعل لمؤسسة دبي للمستقبل التي طورت فكرة المسرعات لتمكين الجهات من تنفيذ توجيهات القيادة بتسريع وتيرة الإنجاز من خلال تشكيل فرق عمل مشتركة فاعلة تتبنى منظوراً علمياً وتطبق ممارسات مستقبلية، لتقدم للعالم إنجازات مبتكرة وحلولاً إبداعية لصناعة مستقبل أفضل للأجيال القادمة.

حمدان بن محمد يلتقي الشريك المؤسس لشركة "جوجل" العالمية

التقى سمو الشيخ حمدان بن محمد بن راشد آل مكتوم ولي عهد دبي رئيس المجلس التنفيذي لإمارة دبي، سيرجي برين الشريك المؤسس لشركة "جوجل" العالمية ورئيس "ألفابت" الشركة الأم لـ "جوجل".

وأثنى سمو الشيخ حمدان بن محمد بن راشد آل مكتوم على تجربة برين ومسيرته العلمية التي تكللت بنجاح عالمي، وأشاد بقصة سيرجي الملهمة الذي بدأ مسيرته وهو على مقاعد الدراسة الجامعية إلى أن تمكن مع صديقه لاري بيج من تأسيس شركة جوجل التي تتجاوز قيمتها اليوم 600 مليار دولار.

مضيفاً سموه: "قصة سيرجي ولاري ملهمة، وقصة دبي أيضا ملهمة.. نشترك معاً في الشغف بمحاولة صنع المستقبل.. لقد صنعنا مستقبل المعرفة البشرية، وصنعنا نحن للعالم مدينة تمثل المستقبل العمراني والخدمي لمدن العالم".

وقال سموه: "الهدف من شركة جوجل ملهم وإنساني .. تنظيم المعرفة البشرية، وجعلها متاحة للجميع". مؤكداً سموه بقوله: "بالشراكة والتعاون معها يمكننا عمل شيء مختلف للبشرية خلال العقود المقبلة".

واستعرض سمو الشيخ حمدان بن محمد بن راشد آل مكتوم مع برين بحضور معالي محمد بن عبدالله القرقاوي وزير شؤون مجلس الوزراء والمستقبل نائب رئيس مجلس الأمناء العضو المنتدب لمؤسسة دبي للمستقبل آفاق التعاون المستقبلي مع "جوجل" من خلال مشاريع مشتركة تسعى إلى تسخير أحدث التقنيات المعلوماتية وتطوير الفضاء الإلكتروني المعلوماتي في سبيل خدمة البشرية في كافة المجالات، قائلا سموه "نسعى لأن تكون دبي المختبر الأكبر عالمياً لتجربة تكنولوجيا المستقبل".

وأكد سموه أن "دبي قطعت مسافة كبيرة نحو المستقبل بفضل رؤية صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، الذي أدرك أهمية بناء مجتمع قائم على اقتصاد المعرفة والاستثمار البنّاء في العلم والعلماء، وربط التنمية الحديثة بالتقنيات المتقدمة".

وقد نوه سموه بأهمية بناء علاقات استراتيجية مع الشركات العالمية، حيث قال: "إن تطوير العلاقات مع الشركات العالمية الكبرى يوازي في أهميته تطوير العلاقات مع الدول الكبرى".

”الشهادات الرقمية“ عنصر جوهري في مسيرة إمارة دبي نحو تحقيق رؤيتها بأن تصبح المدينة الأكثر أمناً في الفضاء الإلكتروني على مستوى العالم

عفراء بن فارس

تحولت في عصرنا الحالي المعاملات الحكومية من ورقية إلى إلكترونية، والحكومات من تقليدية إلى ذكية، وطبقاً لآخر الإحصائيات بلغ متوسط نسبة استخدام الخدمات الحكومية الإلكترونية والذكية في دبي نحو 80% من إجمالي حجم المعاملات التي تقدمها الجهات الحكومية؛ ومؤخراً أطلقت حكومة دبي الشهادات الرقمية بهدف حماية تلك المعاملات الإلكترونية من المخاطر والتحديات الأمنية التي ترافقها.

عفراء بن فارس إحدى الكوادر الشابة التي تعمل في قطاع متخصص وهو الأمن الإلكتروني، وهي باحثة في مركز دبي للأمن الإلكتروني، وتمتلك طموحاً وشغفاً كبيرين

في هذا القطاع، أجرت مجلة ”إشارات“ مقابلة معها للتعرف على مشروع الشهادات الرقمية والمفاهيم المنبثقة عنه وانعكاساته الإيجابية على إمارة دبي.

تتولى عفراء مسؤولية إدارة مشروع الشهادات الرقمية (PKI)، وتقود العمل مع فريق متخصص منذ مايو 2016، من أجل تنفيذ وتفعيل هذا المشروع لدى الجهات الحكومية في إمارة دبي كافة.

وأوضحت لمجلة ”إشارات“: ”أود في البداية التعريف بالشهادات الرقمية وأهميتها ودورها في العالم الرقمي، إنها بالأساس تهدف للتحقق من هوية المستخدمين في العالم الرقمي، فعلى سبيل المثال؛ في العالم الواقعي يمكن التحقق من شخصية الفرد بالاطلاع على بطاقة الهوية الخاصة به والتي تثبت أنه لا ينتحل شخصية أحد آخر“.

”وفي العالم الرقمي، تقوم الشهادات الرقمية بهذا الدور، حيث تتحقق وتصادق على هوية المتعاملين على الشبكة، فإذا صادقت على هوية مؤسسة أو شركة، فإنها بذلك تمنح الثقة للمتعاملين إلكترونياً مع هذا الطرف. فالهدف من الشهادات الرقمية هو تمكين المؤسسات والهيئات والجهات الحكومية وشبه الحكومية من تقديم خدماتها أو منتجاتها وإيصالها إلى المستخدمين بأمان تام“.

وقالت عفراء بن فارس: ”إن مشروع الشهادات الرقمية يأتي تنفيذاً لتوجيهات صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، وسمو ولي عهد دبي، الشيخ حمدان بن محمد بن راشد آل مكتوم، التي دعت كافة المؤسسات الحكومية في الإمارة بالتعاون للحفاظ على ثروة دبي الرقمية، وشددت على التطبيق الأمثل لهذه المبادرة، سعياً نحو حكومة مستقبلية، بلا اورق بحلول عام 2021“.

فقد أكد الشيخ حمدان أن الشهادات الرقمية وانترنت الأشياء تدعم جاهزيتنا الكاملة لحكومة بلا اوراق بحلول2021.

كذلك وجه سموه الجهات الحكومية في دبي إلى جعل الشهادات الرقمية جزءاً أصيلاً من آليات عملها، بما يحقق أهداف التحول

> الشهادات الرقمية تقوم بتشفير الرسائل والبيانات والمعلومات الإلكترونية من أجل ضمان أعلى مستويات الأمن والسرية

> البنية التحتية الخاصة بإمارة دبي تضيف طبقة حماية إضافية تمنع انتحال الشخصية

الرقمي وجعل دبي المدينة الأذكى عالمياً، وأوضح سموه أن هذه المبادرات ستعزز مستويات رضا الناس وسعادتهم.. وستفتح آفاقاً جديدة للارتقاء بالكفاءة والإنتاجية في مختلف قطاعات العمل في دبي.

أمن المعلومات

واستفسرت مجلة "إشارات" من عفراء بن فارس عما إذا كانت شهادات دبي الرقمية تضمن أمن المعلومات إلى جانب كونها تثبت هوية المستخدمين، فأجابت عفراء: "بالتأكيد تضمن منظومة الشهادات الرقمية أيضاً أمن كافة البيانات التي يتم تبادلها بين الأطراف التي تستخدم شهادات دبي الرقمية حيث تقوم بتشفير الرسائل والبيانات والمعلومات الإلكترونية، فهذه الشهادات تضمن السرية أيضاً".

البنية التحتية

وأضافت عفراء: "تتألف البنية التحتية للشهادات الرقمية من الأجهزة والبرمجيات، وسلسلة من السياسات والمعايير لضمان تشغيلها بفاعلية وفقاً لأفضل الممارسات العالمية. وقد قمنا خلال تنفيذ المنظومة باعتماد مجموعة مختارة من البنى التحتية الدولية كمعيار لنا في مركز دبي للأمن الإلكتروني، واتبعنا مبادئ ومعايير Web trust التي تم وضعها بهدف تعزيز مستوى الثقة والمصداقية بين المتعاملين والشركات التي تدير أعمالها عبر الإنترنت.

حرصنا على الاستفادة من الخبرات الواسعة لعدد من الدول المتقدمة في هذا المجال، لإعداد نسخة أكثر تطوراً من الشهادات الرقمية تنسجم مع متطلبات إمارة دبي وتلبي احتياجات المشاريع التي نقوم بتنفيذها".

وقالت عفراء: "إننا في مركز دبي للأمن الإلكتروني على ثقة تامة أن هذا المشروع سيكون له إنعكاسات كبيرة على إمارة دبي، ودور هام في تلبية احتياجات المشروعات الحكومية المستقبلية، وتعتبر الشهادات الرقمية جزءاً أساسياً من آلية عمل الهيئات الحكومية في المستقبل المنظور، للحفاظ على ثروة دبي الرقمية وحمايتها، ومواكبة متطلبات العصر الرقمي والتحديات التي تفرضها التطورات المتسارعة".

حصن منيع ضد القرصنة الإلكترونية

وأكدت عفراء: "لقد تم تصميم الشهادات الرقمية بهدف التصدي لمخاطر القرصنة الإلكترونية التي تهدد الجهات الحكومية، وتمتلك البنية التحتية الإلكترونية بإمارة دبي طبقة حماية إضافية الأمر الذي يحول دون انتحال القراصنة شخصيات أخرى بأي حال من الأحوال".

وأوضحت: "وفيما تخطط مدينة دبي لإطلاق مشاريع رائدة لتحقيق مفهوم المدينة الذكية والتحرك قدماً باتجاه المستقبل، أصبحت الشهادات الرقمية ضرورة حتمية كي تتحرك الخطط الأخرى على أرضية راسخة من الأمان والتكامل الإلكتروني".

وأضافت: "إن تفعيل الشهادات الرقمية سيقوم بتحقيق مستوى الحماية الذي تطمح له إمارة دبي في القطاع التكنولوجي".

مشيرة أن: "جميع المشاريع التي تتطلع الجهات الحكومية في دبي لإطلاقها تعتمد إلى حد كبير على تنفيذ الشهادات الرقمية. كما أن معظم المشاريع التي يعمل عليها مكتب دبي الذكية حالياً على سبيل المثال، مثل تقنية بلوك تشين، وإنترنت الأشياء، تعتمد كلياً على الشهادات الرقمية".

الحلول الذكية تتحقق بأعلى مستويات الأمان

وأكدت: "سيتم تنفيذ هذه المنظومة في وقت قريب، فقد بدأنا العمل على الشهادات الرقمية على وجه التحديد في مايو 2016 وحالياً شارفنا على إنجاز مرحلة تأسيس البنية التحتية، وهي مرحلة متقدمة من المشروع، ومن المخطط أن تكتمل في بدايات العام 2018. حيث سنقوم في مركز دبي للأمن الإلكتروني بتقديمه لحكومة دبي حتى تتبناه كافة الجهات الحكومية".

> صممت الشهادات الرقمية في دبي للتصدي لخطر القراصنة الإلكترونيين الذين يهددون الجهات الحكومية

وأضافت: "تشكل الشهادات الرقمية خطوة أساسية في مسيرة مركز دبي للأمن الإلكتروني باتجاه تحقيق استراتيجية المركز ومهمته الرئيسية التي تتمثل في جعل مدينة دبي أأمن مدن العالم إلكترونياً. وأتطلع للمساهمة مع فريق العمل في تحقيق رؤية إمارة دبي التي أرساها صاحب السمو الشيخ محمد بن راشد آل مكتوم، رعاه الله، وتنفيذ توجيهات سموه بشأن التحول الرقمي وجعل دبي المدينة الأذكى عالمياً".

واختتمت: "على الرغم من أن مشروع شهادات دبي الرقمية مشروعاً مليئاً بالتحديات التقنية إلا أننا بحمد الله تمكنا من إنجازه خلال فترة زمنية قياسية، ولا زال بانتظارنا الكثير من التحديات في مسار استكماله فالتقنية التي نعرفها اليوم قد تتغير كلياً غداً، وهذا ما تفرضه علينا الوتيرة السريعة التي يسير بها قطاع التكنولوجيا من حول العالم. ونحن في دبي نتبنى المنهج الاستباقي من أجل مواكبة التقنيات الرائدة بدلاً من انتظار ما سيجلبه لنا الغد".

مركز دبي للأمن الإلكتروني يوقع مذكرة تفاهم مع معهد مهندسي الإلكترونيات

وقّع مركز دبي للأمن الإلكتروني مذكرة تفاهم مع معهد مهندسي الكهرباء والإلكترونيات (فرع الإمارات) بشأن التعاون المشترك في نشر العلم والمعرفة في الإمارة، ووقع المذكرة سعادة يوسف حمد الشيباني، المدير العام لمركز دبي للأمن الإلكتروني، والدكتور عيسى باسعيد، رئيس فرع الإمارات لمعهد المهندسين الكهربائيين والإلكترونيين، بحضور عدد من ممثلي الجهتين، وجاء توقيع مذكرة التفاهم كإحدى مبادرات المركز التي تدعم خطة دبي الاستراتيجية للأمن الإلكتروني في الابتكار ونشر المعرفة وتعزيز ثقافة البحث والاستقصاء.

وأكد الطرفان أن توقيع هذه المذكرة بداية انطلاق العديد من المشاريع والمبادرات التي من شأنها أن تسهم في رفع مستوى الوعي بالأمن الإلكتروني، من خلال استضافة الفعاليات الدولية، وتبني مشاريع المسؤولية المجتمعية، وعقد الورش والدورات التدريبية والمؤتمرات العلمية.

وتعزز المذكرة سبل التعاون المشترك بين الطرفين في مجال تطوير المواد والبرامج التثقيفية في مجال أمن المعلومات لتحقيق الوعي بين أفراد المجتمع، كما تسهم في نشر المعارف والخبرات والأبحاث، ودعم الأنشطة والمشاريع الطلابية.

وقال سعادة يوسف حمد الشيباني: "إن بناء فضاء إلكتروني يتسم بالحرية والابتكار لن يتحقق إلا بدعم المشاريع البحثية وعقد المؤتمرات العلمية".

من جهته، قال الدكتور عيسى باسعيد رئيس فرع الإمارات: "يعد معهد مهندسي الكهرباء والإلكترونيات أكبر الجمعيات المهنية في العالم التي تتخصص في تطوير وتسخير العلم والتكنولوجيا لخدمة البشرية".

وأضاف: "إن تعاوننا مع مركز دبي للأمن الإلكتروني في تنظيم الأنشطة والفعاليات المختلفة التي تسهم في تعزيز الأمن الإلكتروني لهو خطوة تعكس واجبنا - في فرع دولة الإمارات - تجاه خدمة الوطن والمقيمين على أرضه".

إطلاق موقع استراتيجية دبي للأمن الإلكتروني

تزامناً مع إطلاق صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة، رئيس مجلس الوزراء، حاكم دبي، استراتيجية دبي للأمن الإلكتروني في عام 2017، أطلق مركز دبي للأمن الإلكتروني الموقع الخاص باستراتيجية دبي للأمن الإلكتروني الذي يتميز بسلاسة التصفح ويزخر بمحتوى إعلامي وتثقيفي معزز برسوم الإنفوجرافيك والتصميمات الفريدة التي تحاكي تطور مدينة دبي.

وقد اشتمل الموقع الإلكتروني على مبادئ الاستراتيجية التي تتضمن الامتثال للتشريعات، والتبادل الآمن للمعلومات، والتعاون، وتقييم المخاطر. وعلاوة على ذلك، قد ضمن الموقع محاور الاستراتيجية الخمسة التي تتضمن مجتمعاً واعياً بمخاطر الأمن الإلكتروني، أمن الفضاء الإلكتروني، والابتكار، المرونة في الفضاء الإلكتروني، التعاون المحلي والدولي، إضافة إلى الإطار العام للخطة الاستراتيجية.

يمكنك تصفح الموقع الإلكتروني الجديد عبر هذا الرابط: *desc.dubai.ae*.

"مركز دبي للأمن الإلكتروني" ينظم ورشة "مؤشرات أداء استراتيجية دبي للأمن الإلكتروني" للجهات الحكومية

نظم مركز دبي للأمن الإلكتروني الورشة الثالثة لدعم تطبيق استراتيجية دبي للأمن الإلكتروني، وذلك يوم 24 أغسطس 2017، وركزت الورشة على مناقشة مؤشرات أداء استراتيجية دبي للأمن الإلكتروني والمبادرات المقترحة من قبل الجهات الحكومية والشبه حكومية والورش التوعوية التي قام المركز بتنسيقها مع الجهات المعنية. وقد حضر الورشة عدد من مدراء وممثلي الجهات الحكومية وشبه الحكومية.

تضمنت الورشة عرض المبادرات الاستراتيجية التي ستدعم الأهداف الاستراتيجية للخطة والتي أطلقها صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة، رئيس مجلس الوزراء، حاكم دبي، مؤخراً. وتأتي هذه الورشة تماشياً مع توجيهات صاحب السمو بأهمية توحيد جهود المؤسسات الحكومية والخاصة والأفراد من أجل توفير فضاء إلكتروني آمن. ومن جانبه أكد السيد عامر شرف، مدير إدارة التعاون ودعم الامتثال، ضرورة التعاون مع الجهات الحكومية والشبه حكومية وذلك سعياً لتحقيق رؤية الخطة الاستراتيجية لتعزيز مكانة دبي كمدينة عالمية رائدة في الابتكار والسلامة والأمن والتي تعم كافة شرائح المجتمع بما فيه القطاع الخاص.

"طرق دبي" تستعرض استراتيجية "الأمن الإلكتروني"

نظمت هيئة الطرق والمواصلات في دبي بالتنسيق مع مركز دبي للأمن الإلكتروني، ورشة توعوية لقادة وموظفي الهيئة عن أهداف ومحاور استراتيجية دبي للأمن الإلكتروني التي أطلقتها حكومة دبي الرشيدة في شهر مايو من عام 2017، انطلاقاً من حرص الهيئة على العمل والتعاون مع الجهات الحكومية لتكون دبي أأمن مدن العالم إلكترونياً.

يأتي ذلك في إطار سلسلة ورش العمل الهادفة الى إطلاع الجهات الحكومية في دبي على المخاطر والتحديات الإلكترونية، ومتابعة تنفيذ الأهداف ومؤشرات الأداء المعنية بكل جهة مشاركة في الخطة.

ومن خلال التعاون مع القطاعات الحكومية الرئيسية يعلن المركز عن استراتيجيته للحماية من المخاطر من الجرائم الإلكترونية وإرساء درع منيع ضد الهجمات التي تستهدف بيانات حكومة دبي والتي تعتبر بمثابة كنز ثمين.

وقال عبد الله البستكي، مدير إدارة استراتيجية وحوكمة التقنيات بقطاع خدمات الدعم التقني المؤسسي في الهيئة: إن الهدف الرئيسي لهذه الاستراتيجية يتمثل في الحد من مخاطر الشبكة الإلكترونية ومكافحة أي اختراقات لها، وتمكين المستخدمين من الوصول إلى تقنيات المعلومات المختلفة. وذلك من خلال خمسة مجالات رئيسية هي: مجتمع واع بمخاطر الأمن الإلكتروني، والابتكار، وأمن الفضاء الإلكتروني، والحفاظ على مرونة الفضاء الإلكتروني، والتعاون المحلي والدولي، لافتاً إلى أن الهيئة تعمل على التأكد من التزام جميع قطاعاتها ومؤسساتها بالمعايير المعتمدة من مركز دبي للأمن الإلكتروني، وذلك بشكل دوري.

من جانبه أكد عامر شرف، مدير إدارة التعاون ودعم الامتثال في مركز دبي للأمن الإلكتروني، على ضرورة التعاون مع الجهات الحكومية وشبه الحكومية، لتحقيق الخطة الاستراتيجية لتعزيز مكانة دبي كمدينة عالمية رائدة في الابتكار والسلامة والأمن.

كيف ستغير تقنية "البلوك تشين" مستقبل دبي

تشهد مدينة دبي نقلة مذهلة في تطبيقات تقنية "البلوك تشين"؛ وما تزال المدينة الذكية تتطلع إلى استخدام التعاملات الرقمية في المزيد من التطبيقات ضمن استراتيجية دبي للتعاملات الرقمية "البلوك تشين"؛ تلقي "إشارات" الضوء على تأثير تقنية "البلوك تشين" على مستقبل دبي، وتبحث إمكانية تطوير تطبيقاتها لتحقيق الاستفادة المثلى منها في بعض المجالات الحيوية الجديدة.

تعتبر "البلوك تشين" الشبكة الأساسية لتبادل العملات الرقمية فهي ترتكز بالأساس على تداول هذه العملات، ولكن شهرتها تراجعت في البداية لصالح العملات الرقمية، وعادت إليها الأضواء بعد أن تم التأكد الكامل من إمكانيات اعتماد تقنية "البلوك تشين" في كل جوانب الحكومات الحديثة وأبرزها القطاعات المالية.

وتحقيقاً لتوجيهات سمو الشيخ حمدان بن محمد آل مكتوم ولي عهد دبي قام "مكتب دبي الذكية" بإطلاق استراتيجية دبي للتعاملات الرقمية "البلوك تشين" في ديسمبر 2016، وتهدف هذه الاستراتيجية إلى جعل دبي أول حكومة في العالم تطبق جميع تعاملاتها من خلال هذه الشبكة الرقمية وذلك بحلول عام 2020.

وتنص الاستراتيجية على أن يستمر "مكتب دبي الذكية"، بالتعاون مع "مؤسسة دبي للمستقبل"، في تقييم ودراسة كافة إمكانيات تطبيق تقنية "البلوك تشين" في دبي، للمساهمة في تحقيق رؤية دبي الرامية إلى جعل دبي الوجهة الأكثر ابتكاراً وتقدماً وأمناً وشفافية وكفاءة في العالم. ولتسريع عملية تنفيذ هذه التقنية في كل أنحاء المدينة تتعاون الحكومة مع الشريك الاستراتيجي "أي بي إم" وشركة "كونسينسس" كمستشار لتقنية "البلوك تشين".

> تواصل إمارة دبي تقييم ودراسة كافة إمكانيات تطبيق واعتماد تقنية "البلوك تشين"

إن درجة الشفافية العالية التي تتمتع بها تقنية "البلوك تشين" سيكون لها أثر إيجابي بالغ على قطاع الخدمات المالية وطريقة عمل البنوك في المستقبل.

ومع تعزيز عوامل الأمان والسلامة والاعتمادية في التداول، أصبحت هذه التقنية بمثابة حصن يحمي العالم من حدوث أزمات مالية.

ولا تقتصر تطبيقات "البلوك تشين" على قطاع الخدمات المالية بل يمكن تطبيقها في مختلف القطاعات الأخرى. وتهدف حكومة دبي، من خلال هذه الاستخدامات والتطبيقات، إلى أن تصبح أول حكومة في العالم تطبق تعاملاتها عبر شبكة "البلوك تشين"، مما يحقق الريادة العالمية في المشهد الاقتصادي خلال المستقبل القريب.

ومن المتوقع أن يثمر عن اعتماد تقنية "البلوك تشين" وفورات سنوية تصل إلى 5.5 مليار درهم، وذلك فقط نتيجة"لتبسيط عملية معالجة الوثائق، وسوف تحتفل الإمارة بنهاية عصر المعاملات الورقية الحكومية بإصدار آخر وثيقة حكومية مطبوعة بحلول العام 2021.

يتمثل هدف إمارة دبي الدائم في تحسين الكفاءة الحكومية في كافة القطاعات، وتمتلك تقنية "البلوك تشين" المزايا التي تتيح لها تسريع الإجراءات الحكومية وأن يكون لها تأثير حقيقي على الخدمات العامة مثل التعليم والصحة.

وانطلاقاً من ذلك جاءت تقنية "البلوك تشين" كحل مبتكر يساعد الحكومات على تحقيق الاستفادة المثلى من جوانب الكفاءة والأمان في مختلف مجالات العمل والخدمات.

يعتمد قطاع الرعاية الصحية واحداً من التطبيقات الثورية للبلوك تشين، حيث يوفر برنامج "ميدريك" نظاماً مركزياً لإدارة السجلات. يستخدم تقنية "البلوك تشين" لإدارة البيانات والخصوصية والمساءلة والتوثيق للقطاع بأكمله، وإذا ما تم اعتماد هذا النظام على نطاق واسع فسوف يغير وجه قطاع الرعاية الصحية كلياً على مستوى العالم.

وفيما يتعلق بالدوائر والمؤسسات الحكومية التي سارعت باعتماد هذه التقنية فإن دائرة الأراضي والأملاك في دبي أول دائرة حكومية على مستوى العالم تطبق تقنية "البلوك تشين" في جميع تعاملاتها، وذلك بالتعاون مع "دبي الذكية" وشركاء آخرين.

ويعتمد نظامها على قاعدة بيانات ذكية وآمنة تقوم بتسجيل كل العقود العقارية وربطها مع هيئة كهرباء ومياه دبي، وصولاً إلى نظام الاتصالات، ومختلف الفواتير المتعلقة بالعقار. وتعمل المنصة الإلكترونية على إدراج قواعد البيانات الشخصية للمستأجر، بما في ذلك بطاقة هوية الإمارات وصلاحية إقامته، حيث يكون بمقدوره دفع المبالغ المستحقة عن طريق شيك إلكتروني في غضون دقائق معدودة.

وتتطلع إمارة دبي إلى اتخاذ دائرة الأراضي والأملاك كدليل لتطبيق تقنية "البلوك تشين" في مختلف الجهات الحكومية بحلول العام 2021، وتدرك الحكومة أنه كلما تطورت التقنية انتشرت تطبيقاتها في مختلف القطاعات.

لكن برغم الاهتمام الواسع الذي تحظى به تقنية "البلوك تشين" الآن، فإنها لا تزال غير معروفة وغير مستغلة إلى حد كبير، ولا تزال مرحلة استكشافها في طور الإعداد. لا شك أن هذه التقنية تمتلك العديد من الإمكانيات بالإضافة إلى كونها تسرع وتسهل المعاملات الحكومية وتجعلها أكثر كفاءة، وهناك بالفعل فِرَق متخصصة حول العالم تبحث عن طرق لتطبيقها في المساعدات الإنسانية، ومساعدة بلدان العالم الثالث في إجراء المعاملات، وتمكين العالم من الوصول إلى المعلومات العامة بطريقة ذكية.

يرى المستخدمون أن أكبر مكاسب تقنية "البلوك تشين" تتمثل في الشفافية التي توفرها، والتي تعمل إمارة دبي على ترسيخها في كافة القطاعات ضمن خطتها لتحقيق الريادة العالمية في مجال البيانات المفتوحة.

> دائرة الأراضي والأملاك في دبي أول دائرة حكومية على مستوى العالم تطبق تقنية "البلوك تشين" في جميع تعاملاتها

دليلك لتصفّح آمن
ونصائح مهمة لحماية حاسوبك أثناء الاتصال بالإنترنت

مع التطور في وسائل الاتصال التي تتيح لنا مشاركة البيانات الشخصية بشكل سهل ومكثف أصبحت هناك حاجة ماسة لحماية حاسوبك واتخاذ الإجراءات الوقائية اللازمة في كافة أنشطتك اليومية على شبكة الإنترنت، ومع تسجيلنا للكثير من معلوماتنا الشخصية على الشبكة سيظل السؤال كيف تضمن أنها ستبقى سرية دون أن تطلع عليها أطراف أخرى ؟ وكيف تضمن أنك لن تتخلى عن خصوصيتك بمجرد أن تسجل دخولك لأحد المواقع، فربما يكون هناك قراصنة يتربصون، فكيف تحقق أقصى درجات الأمان لبياناتك. لمعرفة ذلك، أعددنا لك بعض النصائح التي ستساعدك في الحفاظ على سرية بياناتك على الشبكة، وحماية نفسك من العواقب التي تصاحب أنشطتك الشخصية على الإنترنت.

الاتصال بشبكات الواي فاي

ينصح باستخدام شبكات واي فاي عامة موثوقة، وتجنب تلك التي تحمل أسماء مبهمة أو مشبوهة.

إذا استخدمت شبكة واي فاي عامة، فيجب عليك أن تقوم بتسجيل الخروج بمجرد أن تنتهي من أعمالك، وبالطبع يُحظر استخدام مثل هذه الشبكات لإجراء معاملات مصرفية أو التسوق.

تصفح الإنترنت

لاشك في أن الإنترنت مليء بالمعلومات والمحتوى المُلهم، ولكنه يتضمن أيضاً جانباً مظلماً آخر مليئاً بالفيروسات والروابط المضللة والهجمات الخبيثة. لتجنب هذا الجانب الضار، يجب عليك الابتعاد كلياً عن المناطق المظلمة من الإنترنت أثناء تصفحك، ولهذا يفضل بأن تتصفح المواقع الموثوقة.

يشير حرف (S) في البروتوكول (https) على الرابط URL إلى أن هذا الرابط آمن، وإذا كان الموقع الإلكتروني يستخدم بروتوكول طبقة المنافذ الآمنة، اختصاراً SSL، فسوف تظهر حروف https، وستظهر بجانبه صورة القفل؛ تأكد من ظهور هذه العلامات واحرص على أن يكون الموقع الذي تتصفحه آمناً قبل أن تبدأ بإدخال أي بيانات شخصية.

اقرأ سياسات الخصوصية، فهي توضح لك كيف تتعامل مع البيانات التي تقوم بجمعها من المتصفحين وتخبرك بالأجزاء المحمية في بياناتك، وكيف يقوم الموقع بتتبع أنشطتك على الإنترنت.

استخدم أداة حظر الإعلانات المنبثقة، فهي تقوم بمنع ظهور أي إعلانات تحتوي على بريد عشوائي أو روابط لمواقع ضارة في حالة تصفح الإنترنت بطريقة غير لائقة.

استخدام واتساب

رسائل واتساب يتم تشفرها، مما يوفر مستويات عالية من الأمن للمستخدم، غير أن إهمال المستخدم يمكن أن يعرض خصوصية أمن رسائله للخطر.

فمنذ إتاحة تطبيق الواتساب على أجهزة الكمبيوتر ظهرت العديد من الحالات التي قام فيها القراصنة باختراق خصوصية المستخدم والوصول إلى كافة رسائله. ويحدث ذلك عندما يقوم شخص ما بترك هاتفه من دون مراقبة.

ومن ثم يقوم القرصان بربط هاتفه عن طريق رمز الاستجابة السريع الخاص بالواتساب مع حاسوبه في ثوانٍ معدودة فقط، ومن ثم يتمكن القراصنة من قراءة رسائلك، وإذا تُركت الصفحة مفتوحة على الحاسوب فسوف يتمكنون من مراقبة كل رسالة تقوم بإرسالها أو استقبالها باستمرار، وفي جميع الأوقات طالما لم يغلقوا صفحة واتساب الخاصة بك على حاسوبهم، لذا ينصح بتفعيل ميزة التحقق التي يوفرها واتساب وتضمن خطوتين كطبقة حماية إضافية.

مواقع التواصل الاجتماعي

احذر من الإفراط في رسائلك، وتتبع مسار ما تنشره، فقد تعود سلوكياتك الإلكترونية بعواقب وخيمة عليك إذا لم تتبع الطرق الملائمة.

للاستفادة القصوى من شبكة الإنترنت على المتصفحين دوماً تذكّر أن الاستخدام المسؤول والالتزام بقوانين الإنترنت، واحترام القواعد والأعراف الاجتماعية هو السبيل الوحيد لهذا الإبحار الرائع.

احذر من نشر تفاصيل نشاطاتك اليومية على مواقع التواصل الاجتماعي، لأنك بذلك تدعو المتربصين لاستخدام بياناتك لتحقيق الاستفادة والربح المادي.

تحتوي مواقع التواصل الاجتماعي على خاصية تتضمن تسجيل موقع الحدث أثناء النشر. قم بتحديد وإغلاق هذه الخاصية لتحتفظ بخصوصيتك، لأنك بذلك ستعزز من سلامتك الشخصية وسلامة ممتلكاتك، وستمنع أي أشخاص غير مرغوب فيهم من معرفة مكانك ومتى تكون متغيباً عن المنزل.

إرسال/ استقبال الرسائل الإلكترونية

احذر النقر على الروابط التي تبدو مشبوهة من مصادر موثوقة أو غير موثوقة. إذا كنت تتلقى الكثير من الرسائل الإلكترونية العشوائية، سيكون عليك إلغاء اشتراكك من كل المواقع التي ترسل إليك رسائل تسويقية، وهذا سيجنبك مخاطر النقر على روابط ضارة أيضاً.

وكما ترى، فإن حماية نفسك وبياناتك وأجهزتك لا تتطلب منك سوى بضع خطوات بسيطة؛ هذه الإجراءات الوقائية الأساسية ستساعدك على تحقيق الاستفادة المثلى من الفرص والمزايا التي يتيحها الإنترنت للجميع، وتمكّنك من اكتشاف قنوات جديدة للنمو والازدهار في حياتك الشخصية والاجتماعية والأسرية وحتى العمل، من دون المجازفة بسلامتك وراحة بالك. نتمنى لك أن تنعم بتصفح آمن.

لعبة جديدة تقيس مهاراتك في مجال الأمن الإلكتروني

أعلنت شركة "إميرسيف لابس" البريطانية عن إطلاق لعبة إنترنت جديدة تهدف إلى تقييم اللاعبين وقياس المهارات اللازمة لدخول قطاع الأمن الإلكتروني، ولا تهدف اللعبة التي تم إطلاقها في المملكة المتحدة إلى تقييم اللاعبين فقط إنما تهدف أيضاً إلى تثقيف الناس بمجال الأمن الإلكتروني وجذبهم إليه.

شهد عام 2017 ظهور أشكال متطورة من الهجمات الإلكترونية التي تسللت إلى المؤسسات الكبرى من حول العالم، مثل هجمات NotPetya و WannaCry، وأصبح هناك طلب متزايد لخبراء الأمن الإلكتروني من أجل توفير الحماية اللازمة من هذه البرامج الخبيثة والمدمرة.

ويقول جيمس هادلي مبتكر اللعبة إنه ليس هناك ما يكفي من المتخصصين في الكمبيوتر بما يغطي حاجة السوق، مؤكداً أن على الشركات البحث عن طرق أكثر ابتكاراً وأن قطاع الأمن الإلكتروني ككل سوف يستفيد من مشاركة الناس بمختلف خلفياتهم التعليمية.

وأضاف هارلي: "الأشخاص الذين لا ينتمون إلى خلفيات تقنية ربما يأتون بحلول جديدة ومبتكرة للمشاكل الإلكترونية. إذ يمكن للطلبة الذي يمتلكون خبرات أوسع في مجالات الحياة تقديم أفكار جديدة، وكذلك يمكننا الاستفادة من مهارات الأشخاص الذين يجيدون تحليل المواقف وتحديد وحل المشاكل، وحتى أولئك الذين يجتهدون أو يمتلكون حب الفضول".

وتستهدف المنصة الإلكترونية الجديدة طلبة المملكة المتحدة حالياً، وهي توفر سلسلة من الدورات التدريبية للمبتدئين والمستويات المتقدمة، وتضم اللعبة لوحة بأسماء أفضل اللاعبين، ما يتيح للشركات البحث عن المرشحين الذين يمتلكون مستويات عالية من المهارات المطلوبة وتقييمهم من أجل إلحاقهم بوظائف خاصة بالأمن الإلكتروني.

المصدر: *www.newscientist.com*

خبراء يحذرون: برمجية "ريبر بوتنت" تشكل الخطر الأكبر على شبكة الإنترنت

حذر مؤخراً خبراء في مجال الأمن الإلكتروني من أن برمجية "ريبر بوتنت" التي تعدّ نسخة مطورة من البرمجية الخبيثة "ميراي بوتنت" (Mirai Botnet) قد تسبب تعطيلاً بالغاً في شبكة الإنترنت. ونمت "ريبر بوتنت" وتطورت خلال فترة وجيزة لعدة أنواع من البرمجيات لتتفاقم وتنتشر في الكثير من الأجهزة المتصلة بشبكة الإنترنت بما في ذلك انترنت الأشياء، حيث استهدفت نقاط الضعف في الأجهزة والبرامج غير المحدثة وتحكمت بها وأضافتها لمنصة القيادة والتحكم الخاصة بها، مما أدى إلى وقوعها في قبضة قراصنة الإنترنت للقيام بأنشطة الابتزاز حينما رغبوا، مثل هجمات الحرمان من الخدمة أو هجوم حجب الخدمة (Denial of Service Attacks).

وتعتبر برمجية "ريبر بوتنت" قوة مدمرة غير مسبوقة، حيث يمكن أن تصيب كافة أنظمة تكنولوجيا المعلومات، وتتضاعف إلى حد تعطيل الخدمات وإعاقة الوصول إلى الموارد على شبكة الإنترنت. ويشمل ذلك شبكة واسعة من الأجهزة التي يتم اختراقها، بما في ذلك أجهزة "راوتر" "واي فاي"، وكاميرات الويب الذكية، والكمبيوترات، وترسل هذه البرمجية كميات هائلة من البيانات الضخمة تؤدي إلى ازدحام الخوادم بهدف تعطيلها، وفي أسواء الاحتمالات قد يصل الأمر الى تعطيل موضعي لشبكة الإنترنت بشكل عام.

يشار إلى أنه يمكن لهذه الهجمات الإلكترونية الانتشار على نطاق واسع وبطابع عدواني، إضافةً إلى أن الشبكات الأكبر حجماً قد تتعرض إلى مزيد من الخطر، حيث من الصعوبة البالغة التصدي لانتشار برمجية "ريبر بوتنت" على كافة الجبهات في نفس الوقت، وإصلاح الأعطال الناتجة عنها.

والجدير بالذكر أن هجوماً إلكترونياً واسع النطاق حدث سابقاً في عدة مناطق من الولايات المتحدة، عندما تسببت البرمجية الخبيثة "ميراي بوتنت" بحدوث اضطرابات كبيرة على شبكة الإنترنت.

وعلى الرغم من قيام المؤسسات والشركات باتخاذ تدابير وقائية من الهجمات الإلكترونية، وتشغيل أحدث الإصدارات من البرمجيات الأساسية التي توفر التحديثات الأمنية المطلوبة للتعامل مع هذه البرمجيات، إلا أن شريحة كبيرة من الأفراد (تصل إلى 80%) لا يقومون بتركيب برامج تشتمل على تحديثات البرامج التي توفر الحماية من البرمجيات الضارة وغير المرغوب بها على الأجهزة التي لديهم، الأمر الذي يعرض أجهزتهم وبياناتهم لمخاطر كبيرة.

ولتحقيق الأمن على شبكة الإنترنت وتوفير الحماية اللازمة لمعلومات وبيانات الأفراد والشركات، خاصة مع ارتفاع الهجمات الإلكترونية وتزايد أعداد الأجهزة المتصلة بالإنترنت، ينصح خبراء الأمن الإلكتروني بضرورة تركيب تحديثات البرامج التي تضمن عدم تعرض الأجهزة المتصلة بالإنترنت في المكتب والمنزل إلى أي أعطال واضطرابات قد تسببها برمجية "ريبر بوتنت".

المصدر: *www.sott.net*

اتخاذ إجراءات وقائية لحماية شبكات الكهرباء من هجمات واختراقات إلكترونية

أعلنت وزارة الطاقة الأمريكية أنها تخطط لاتخاذ إجراءات وقائية بغرض حماية شبكة الكهرباء من مخاطر البرامج الخبيثة التي قد تنتقل إليها عبر الأجهزة الكهربائية.

وأعلنت لجنة تنظيم الطاقة الفيدرالية أن الهدف الرئيسي لمثل هذه الإجراءات هو القضاء على تهديدات الهجمات الإلكترونية التي قد تؤثر على الشبكة بأكملها.

وتخطط الهيئة التنظيمية للحصول على معايير إنشاء وحدات تحكم إلكترونية للوصول إلى أنظمة الشبكة، قبل البحث عن حلول لتقليل تهديدات الهجمات الخبيثة.

كانت وزارة الطاقة الأمريكية أعلنت في بداية عام 2017 أن منظومة الكهرباء تواجه "خطراً داهماً" من الهجمات الإلكترونية.

وقد أسهمت الهجمات الإلكترونية التي وقعت سابقاً في تعزيز هذه التكهنات.

لكن إذا تم اختراق الشبكة بنجاح فسوف ينتج عن ذلك قطع الكهرباء على نطاق واسع، وقد يقوض ذلك أنظمة الدفاع الوطنية ويدمر اقتصاد الدولة بحسب تصريح الوزارة.

المصدر: *www.bloomberg.com*

اختراق "اكويفاكس" وتداعياته الخطيرة على خدمات التصنيف الائتماني

كشفت شركة اكويفاكس العملاقة للتقارير الائتمانية أن معلومات شخصية عن 145 مليون عميل سُرقت إثر واحدة من أكبر عمليات القرصنة الإلكترونية في تاريخ الولايات المتحدة.

من ناحية أخرى، قال أعضاء في الكونغرس الأميركي إن اختراق كومبيوترات اكويفاكس يعرض المتعاملين معها إلى خطر سرقة هوياتهم وأشكال أخرى من الاحتيال. كما سُرقت معلومات شخصية عن عملاء في كندا وبريطانيا، وقال مكتب مفوّض المعلومات البريطاني إنه يخشى أن تكون معلومات 44 مليون عميل بريطاني سُرقت في عملية القرصنة. وبدأ المكتب تحقيقاً في الحادث مطالباً اكويفاكس بإبلاغ العملاء بأسرع وقت ممكن.

وقالت الشركة إنها وجدت دلائل على الوصول بطريقة غير قانونية إلى بيانات بينها أسماء وعناوين وأرقام الضمان الاجتماعي نتيجة عملية اختراق نُفذت خلال الفترة الواقعة بين منتصف مايو وأواخر يوليو 2017 ولكن لم تكشف الشركة عنها إلا الآن. وهاجم أعضاء في الكونغرس الأميركي شركة اكويفاكس بشدة بعد الكشف عن عملية الاختراق. وقال رؤساء اللجان إنهم سيعقدون جلسات استماع بشأن الحادث فيما أكّد الادعاء العام في عدة ولايات أميركية فتح تحقيقات.

وصرّح رئيس لجنة الخدمات المالية في مجلس النواب الاميركي جيب هينسارلنغ قائلاً: "إن أي اختراق يترك العملاء معرضين ومكشوفين لسرقة هوياتهم والاحتيال عليهم ولطائفة من الجرائم الأخرى وأن هؤلاء يستحقون إجابات". وستعقد هذه اللجنة ولجنة التجارة في المجلس جلسات استماع من المتوقع أن يُستدعى إليها مسؤولون من الشركة.

وأطلقت شركة اكويفاكس موقعاً إلكترونياً ليعرف العملاء إن كانوا من الذين سُرقت معلوماتهم. وأثارت الشركة موجة من ردود الأفعال الغاضبة باشتراطها على مستخدمي الموقع أن يتنازلوا عن حق مقاضاتها. وأوضحت الشركة لاحقاً أن هذا الشرط لا يسري إلا على المشتركين في خدمات مراقبة الائتمان وليس على المتضررين من سرقة المعلومات.

وتتولى شركة اكويفاكس معلومات أكثر من 820 مليون عميل و91 مليون شركة في أنحاء العالم ، بحسب موقعها الإلكتروني. وهي تقدم خدمات مثل المراقبة الائتمانية والتحقق الوظيفي ومراقبة سرقة الهويات.

المصدر: *www.chicagotribune.com*

كيف تحسّن مستوى الخصوصية والأمان على مواقع التواصل الاجتماعي؟

مواقع التواصل الاجتماعي أصبحت جزءاً لا يتجزء من أسلوب حياتنا، ووسيلة تواصل أساسية بين أفراد الأسرة والأصدقاء وزملاء العمل، وحتى بين الشركات وعملائها، كما منحت مواقع التواصل بعداً جديداً لحياتنا ووفرت لنا مساحة للتعبير عن أنفسنا وأثرت حياتنا وعززت من مستوى تواصلنا ومشاركتنا لأفكارنا، كما سهلت علينا تبادل أفكارنا أفراداً ومجموعات بشكل كبير.

إيهاب معوض نائب رئيس شركة تريند ميكرو: "تفعيل إعدادات الخصوصية لحساباتك على مواقع التواصل لن يستغرق أكثر من بضع دقائق من وقتك ولكنها تحمي أمنك".

من المخاطر إذا أسيء استخدامها، ويمتلك كل موقع تواصل اجتماعي إعدادات في أنظمته لدرء مخاطر انتهاك الخصوصية وحماية البيانات الشخصية، وللتعرف على ضبط إعدادات الخصوصية والأمان على مواقع التواصل الاجتماعي لتأمين وحماية بياناتنا ومعلوماتنا وصورنا الشخصية، أجرت مجلة إشارات مقابلة مع إيهاب معوض، نائب رئيس شركة "تريند مايكرو".

بدأ إيهاب معوض حديثه بالقول: "إن مواقع التواصل الاجتماعي تتيح أساليب تواصل مرنة، وتعزز من تبادل أفكارنا، وطرق تصفّح الأخبار والأحداث العامة. ولكن بالرغم من كل هذه الإيجابيات إلا أن مواقع التواصل الاجتماعي ليست خالية من المخاطر، إذ يتاح لأي شخص الاطلاع على ما تفعله أو ما تخطط للقيام به أو حتى مكان وجودك.

وظهرت قصص اختراق كبيرة للمعلومات الشخصية واستخدامها في أغراض تنتهك الخصوصية والقانون، وأود هنا التنويه إلى ضرورة وضع مستوى من الحماية والأمان لتأمين صفحاتك الشخصية على مواقع التواصل الاجتماعي".

وشدد معوض: "ينبغي أن تكون الحماية والأمان موضع اهتمامك الأول لأنه من السهل على قراصنة الفضاء الإلكتروني استخدام بياناتك والاستفادة منها لتحقيق الاستفادة والربح المادي.

وأرغب في تقديم بعض النصائح للمستخدمين لتحسين مستويات الخصوصية والأمان في حساباتهم على مواقع التواصل الاجتماعي، كما أود التنبيه إلى أنه يجب مراجعة وضبط الإعدادات في كل مرة يتم إجراء تحديثات في المواقع لتتوافق مع الإصدار الجديد. ولن يأخذ ضبط الإعدادات أكثر من دقائق من وقتك، وكما يقول المثل، فإن الوقاية خيرٌ من العلاج".

ضبط الأمان على فيسبوك

من الممكن أن يكون تعديل إعدادات الخصوصية والأمان لصفحتك على فيسبوك محيراً بعض الشيء، ولكن إذا كنت تعرف مسبقاً مستوى الأمان الذي تريده فسيصبح تطبيق الإعدادات بسيطاً للغاية.

تستطيع البحث عن "إعدادات الخصوصية وأدواتها" في صفحتك على الفيسبوك، فقد جعل موقع الفيسبوك الوصول إلى هذه الإعدادات سهلاً للغاية وذلك باختيار أيقونة القفل التي توجد في الزاوية العليا اليسرى.

حيث تعرض عدة خيارات لضبط الخصوصية في حسابكم وهي: مَن يستطيع مشاهدة معلوماتي وصوري، مَن يستطيع التواصل معي، مَن يستطيع العثور على صفحتي والاتصال بي. ومؤخراً، أنشأ فيسبوك صفحة لإعدادات الخصوصية أكثر سهولة وشمولية، ومن المفيد جداً الاطلاع عليها.

يمكنكم رفع مستوى الحماية في حسابكم باختيار إعدادات "الأمان" من القائمة. حيث تتيح لكم الخيارات ضبط الإشعارات، والموافقات، وكلمات سر التطبيقات بالإضافة إلى أنشطة أخرى متعلقة بالحساب.

يجب مراجعة وضبط إعدادات الخصوصية والأمان لصفحتك على مواقع التواصل الاجتماعي في كل مرة يتم فيها إجراء تحديثات على المواقع لتتوافق مع الإصدار الجديد

ويعتمد الغالبية العظمى من المستخدمين على الإعدادات الافتراضية، لذلك يتوجب مراجعة خيارات "الأمان" لضمان استعادة حساباتكم في حالة قرصنتها أو اختراقها"كي تتمكنوا من الحصول على طريقة لاستعادة الحساب في حالة فقدانه.

ضبط الخصوصية على تويتر

ويتابع معوض: "نظراً لطبيعة موقع تويتر القائم على مشاركة الأفكار فإنه لا يحظى بتدابير حفظ الخصوصية كتلك التي يتمتع بها موقع فيسبوك، لهذا فإنه يتعرض لعمليات قرصنة وتسريب للبيانات أكثر. ولكن أهم أمرين يتوجب وضعهما بعين الاعتبار والتأكد من الحفاظ عليهما بأمان"في حسابكم على تويتر هما: معلومات تسجيل الدخول، وتعيين كلمة المرور".

وعندما يتعلق الأمر بإعادة تعيين كلمة المرور فإن كل ما يطلبه موقع 'تويتر' هو اسم المستخدم. لذلك ارفع مستوى الأمان في كلمة المرور باختيار "طلب معلومات شخصية" (عاملى مصادقة) مثل تعيين إشعارات البريد الإلكتروني والرسائل القصيرة، والتأكد من أن معلوماتكم الشخصية لن يتم مشاركتها على أي صفحة أو أحد حسابات التواصل الاجتماعي العامة.

يبين لنا معوض: "وكما هو الحال في شبكات التواصل الاجتماعي الأخرى، فإذا لم يتم تعيين إعدادات الخصوصية لمشاركاتك. فإن ذلك يعني أن أي شخص، حتى لو لم يكن من المتابعين لك، بإمكانه رؤية تغريداتك".

فإذا كنت من الناشطين على موقع 'تويتر' ولا تنشر معلوماتٍ شخصية، فلا يوجد مانع من أن يكون حسابك متاحاً للجميع، وعليه ليس من الضروري لك القيام بحماية تغريداتك، لأن ذلك سيحدد مشاهدة التغريدات للمتابعين فقط، ولا يتيح للآخرين إمكانية إعادة التغريد الخاصة بكم.

وسيتوجب على المستخدمين عندها إرسال طلب موافقة للمتابعين، كما وأن الردود التي تقومون بها للمستخدمين الذين لم يقوموا بمتابعتكم (مثل المشاهير) لن تكون متاحة لهؤلاء المستخدمي".

لينكد إن

موقع 'لينكد إن' موقع تواصل اجتماعي خاص بالمهنيين من حول العالم، فإذا كنت ترغب بالتعرف على زملاء جدد، أو مشاهدة مقاطع فيديو لها علاقة بطبيعة عملك، أو مشاركة إنجازاتك المهنية فإن موقع' لينكد إن' موقع تواصل اجتماعي يتيح لك ذلك، كما يتيح للباحثين عن عمل استكشاف الفرص الوظيفية، أو التواصل مع زملاء العمل السابقين، وكموقع يضم سيرتك المهنية فإنه يتيح لجميع الأشخاص الذين ترتبط معهم بعلاقات مهنية الاتصال بك والتعرف على مهاراتك.

يخبرنا معوض: "وكما هو الحال في مواقع التواصل الاجتماعي الأخرى، يضم "لينكد إن" إعدادات "الأمان" و"الخصوصية" ويتيح لكم "عناصر التحكم في الخصوصية" مراجعة واختيار كيفية ضبط بث الأنشطة، وتحديد إمكانية رؤية الصفحة وترتيبها، واختيار ما يمكن للآخرين مشاهدته في صفحتك الشخصية. ومن الضروري إعادة تعيين كلمة المرور بشكل دوري لتجنب الوقوع ضحيةً للاختراق أو القرصنة".

"إن مواقع التواصل الاجتماعي الأخرى مثل'بينتريست'"Pinterest, و'فورسكوير' Foursquare, و'جوجل بلاس' Google+"تمتلك إعدادات وأدوات ضبط مفيدة أيضاً تساعدكم في رفع مستويات الحفاظ على خصوصيتكم وأمان حساباتكم. وأخيراً، تذكروا أن الحفاظ على خصوصيتكم لا تقتصر مزاياه على حمايتكم فحسب، بل وحماية عائلاتكم، وأصدقائكم أيضاً".

أسوأ الاختراقات الإلكترونية في عام 2017

شهد العام 2017 زيادة كبيرة"في مستوى الوعي بمخاطر الهجمات الأمنية الإلكترونية لدى الجمهور، وهذا يرجع بالطبع إلى الأعداد الهائلة للهجمات الإلكترونية المدمرة التي اجتاحت بعضاً من المؤسسات العالمية الكبرى، وجعلت ملايين الأفراد فريسة لعصابات من القراصنة عديمي القيم الأخلاقية. وفي هذا المقال نلقي نظرة على أسوأ هذه الهجمات التي هزت العالم خلال 2017.

هجوم "وانا كراي"

هجوم "ونا كراي" عبارة عن سلسلة من برمجيات الفدية الخبيثة التي هاجمت ملايين الكمبيوترات حول العالم واخترقت كمبيوترات المؤسسات العالمية الكبرى، وكانت مؤسسة الصحة العامة في بريطانيا من أكبر ضحايا الهجوم بالإضافة إلى المؤسسات العالمية الأخرى. وقد أطلقت شركة ميكروسوفت تحديثاً عمل على سد الثغرة التي ينفذ من خلالها الفيروس، وذلك قبل شهرين من الهجوم، لكن المؤسسات التي تعمل على نظم تشغيل قديمة وغير محدّثة ظلت عُرضة للهجمات.

فيروس "بتيا"

فوجئ العالم في أعقاب هجوم "وانا كراي" بهجوم برمجيات فدية آخر يحمل اسم "بتيا"، اخترق عدداً كبيراً من الشركات العالمية العملاقة بالرغم من أنه كان يستهدف مؤسسات أوكرانية في البداية، إذ تعرضت بعض شركات البنية التحتية في أوكرانيا لخسائر فادحة جراء هذا الهجوم، ومن بينها شركات الكهرباء، والمطارات، والمواصلات العامة، والبنك المركزي.

تسريب قوائم 200 مليون أمريكي قاموا بالتصويت

في حادث غير مسبوق تم تسريب قاعدة بيانات تحتوي على معلومات شخصية يقال إنها تنتمي لكل من قاموا بالتصويت في الانتخابات الأمريكية على مدار العقد المنصرم، واتضح لاحقاً أن قاعدة البيانات تعرضت لاختراق أمني بسبب ثغرة في نظم التشغيل. وتعتبر هذه أبرز مخاطر الاختراق الإلكتروني التي قد يكون لها تداعيات وخيمة، غير أن المسؤولين أعلنوا أنه لم يستطع أحد من المستخدمين الوصول إلى بيانات قوائم الأشخاص.

اكويفاكس

اكويفاكس واحدة من أكبر الشركات المتخصصة في تقديم التقارير الائتمانية في الولايات المتحدة الأمريكية، وقد أصيبت باختراق خطير طال ما يقرب من 145 مليون عميل، إذ تمت سرقة بيانات شخصية لملايين العملاء من بينها أسماء وعناوين وأرقام الضمان الاجتماعي وأرقام البطاقات الائتمانية، ما يجعلها واحدة من أسوأ هجمات الاختراق الإلكتروني في التاريخ.

برامج الفدية..
فيروسات توقع بآلاف الضحايا في العالم

حلّت دولة الإمارات في المرتبة الثامنة عالمياً والأولى إقليمياً في قائمة الدول الأكثر تعرضاً للهجمات الإلكترونية، بحسب الإصدار 21 الخاص بالتهديدات الأمنية لشركة سيمانتك العالمية المتخصصة في الحلول الأمنية المعلوماتية. ويعزى تزايد هجمات التصيد التي تتعرض لها الشركات في الإمارات كون الدولة بوابة محورية لمنطقة الشرق الأوسط، وتمتعها ببنية تحتية عالمية المستوى لتكنولوجيا المعلومات والاتصال وبيئة عمل جاذبة للاستثمارات، مما يجعل منها مركزاً تجارياً لعدد كبير من الشركات العالمية.

تحرص دبي على تعزيز جاهزيتها لمواجهة مخاطر الأمن الإلكتروني، وحماية البنية التحتية الحيوية ضد التهديدات الإلكترونية المتنامية. وقد أطلق صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي رعاه الله، في العام 2017 خطة دبي الاستراتيجية للأمن الإلكتروني التي تهدف لتعزيز مكانة دبي كمدينة عالمية رائدة في الابتكار والسلامة والأمن. ودعا سموه جميع المؤسسات الحكومية والخاصة والأفراد في الإمارة إلى توحيد الجهود من أجل توفير فضاء إلكتروني آمن ولجعل دبي أآمن مدن العالم إلكترونياً.

ويتنامى خطر قراصنة الإنترنت الذين يستخدمون برامج الفدية في ابتزاز الشركات، بما يعطل وعلى نحو متزايد الشبكات الإلكترونية لكبرى الشركات حيث تعرض العالم في عام 2017 لأكبر موجة قرصنة عرفتها الدول حديثاً مع فيروس الفدية الذي اجتاح أكثر من 150 دولة، وأدى إلى تضرر أكثر من 200 ألف جهاز، معظمها لشركات ومؤسسات تجارية كبرى، كما جاء في العديد من وسائل الأعلام المحلية والعالمية.

وما يزال فيروس الفدية يتسبب بأعطال وخسائر للشبكات الإلكترونية، وحددت شركة "سيمانتك" المتخصصة في بيع برامج الكمبيوتر لا سيما في مجال الأمن وإدارة المعلومات، أكثر من 100 نوع من البرمجيات الخبيثة التي تتزايد بمعدل ينذر بالخطر، وبما يعرض الشركات والأفراد لتهديدات جسيمة.

تعتبر برامج الفدية من الفيروسات الجديدة نسبياً في عالم الهجمات الإلكترونية، وتعتمد على استخدام برنامج معقد يتيح للقراصنة الوصول إلى نظام التشغيل، ويشفر جميع البيانات المخزنة على جهاز الكمبيوتر، ومن ثم يبتز الضحية ويرغمها على دفع مبلغ من المال مقابل إعادة فتح نظام التشغيل، أو محو الملفات في حالة عدم الانصياع لمطالبهم.

وعادة ما تستخدم فيروسات الفدية أسلوباً قديماً يعتمد على إرسال رابط أو رسالة إلكترونية من مصدر مجهول، ولكنها رغم قدمها ما تزال حيلة تنطلي على متصفحي شبكة الإنترنت وتأتي بأفضل النتائج للقراصنة الإلكترونيين، وفي حال لفتت هذه الرسالة انتباه الضحية وقام بفتح الرابط وتحميله، يقع عندئذ في مصيدة القراصنة. وشهدنا في عام 2017 زيادة كبيرة في هجمات الفيروسات التي أدت إلى حدوث اضطرابات لم يسبق لها مثيل على مستوى العالم وإصابة مئات الآلاف من الأجهزة، حيث قام "برنامج الفدية" بتشفير ملفات المستخدمين المستهدفين وإرغامهم على دفع فدية تتراوح بين 300 و600 دولار لكل جهاز. وكان القراصنة يطالبون بدفع الفدية في غضون ثلاثة أيام وإلا فإن المبلغ سيزداد إلى الضعف، أما إذا لم يتم الدفع بعد مهلة سبعة أيام فكانت الملفات تتعرض للمحو.

والجدير بالذكر أن أول حادثة اختراق باستخدام فيروسات الفدية ظهرت في عام 1989 عندما شارك جوزيف بوب وهو أكاديمي من جامعة هارفارد في مؤتمر لمنظمة الصحة العالمية بشأن مرض الإيدز. وخلال الاستعداد للمؤتمر، قام بإعداد 20 ألف قرص مرن لإرسالها إلى المندوبين تحتوي على "معلومات حول الإيدز.

ولكن ما لم يدركه المندوبون هو أن الأقراص المرنة كانت تحتوي في الواقع على فيروس كمبيوتر تم إدخاله من قبل جوزيف بوب، وبعد تشغيل محتويات الأقراص، ظل الفيروس مخفي على كمبيوتر الضحايا لبعض الوقت. وبعد قيام المستخدمين بإعادة تشغيل أجهزة الكمبيوتر 90 مرة، بدأ عمل الفيروس حيث قام بتشفير كافة الملفات وإخفاء الدلائل. وتم عرض رسالة لإعلام المستخدمين بأن نظامهم سيعود إلى وضعه الطبيعي بعد إرسال 189 دولار أمريكي إلى صندوق بريد في بنما.

وقد استغرق الأمر 16 عاماً آخراً قبل استطاعة أي شخص تنفيذ فكرة فيروسات الفدية الخاصة بالدكتور بوب واستخدامها في أوج ازدهار عصر الانترنت، أما سنة الصفر أو سنة البداية لهجمات الفدية فقد كانت في عام 2005، مع فيروس حصان طروادة "GP Coder" الذي أصاب أنظمة وملفات الويندوز، ومنذ ذلك الوقت ما تزال هجمات الفدية تشكل خطراً متزايداً على الفضاء الإلكتروني بأكمله.

ولتجنب الوقوع في فخ فيروس الفدية، تنصح مجلة إشارات قراءها بالحرص على إنشاء نسخة احتياطية من بيانات الأجهزة باستمرار، وتجنب فتح روابط غير معروفة المصدر وتنزيل أي ملفات مرسلة من مجهولين تصل عبر البريد الإلكتروني، كما يفضل استخدام برامج مكافحة الفيروسات الأصلية والمحدثة وتحديث برامجهم باستمرار، وكذلك تجنب الدخول إلى مواقع مشبوهة والتأكد من تنزيل برامج وتطبيقات من مصادرها الرسمية. أما في حال الوقوع في فخ فيروس الفدية، فيجب عدم الانصياع إلى مطالب المخترقين، وإيقاف جميع العمليات في الجهاز أو الشبكة مباشرة واستعادة النسخة الاحتياطية.

برامج الفدية

5 علامات تحذيرية.. تؤكد إصابة حاسوبك بفيروس!

هناك أنواع مختلفة من البرمجيات الخبيثة التي تستهدف الأنظمة غير المدعمة ببرامج حماية لكي تنفذ إلى البيانات الشخصية، ومن الضروري أن نكون قادرين على اكتشاف هذه الهجمات على الفور لحماية حاسباتنا والبحث عن حلول فورية للتخلص من هذه الفيروسات. ولمساعدتك على معرفة ما إذا كان حاسوبك وقع ضحية لمثل هذه الهجمات أم لا، إليك خمسة أعراض رئيسية تشير إلى إصابة حاسوبك بفيروس أو برمجيات خبيثة..

1. تعطل عمل البرامج بشكل مستمر

إذا تعطل عمل أحد البرامج أو نظام التشغيل بشكل مستمر، فهذا يعني أن حاسوبك قد يحتوي على فيروس.

2. نشاط غريب في القرص الصلب

إذا كنت لا تستخدم حاسوبك، ولاحظت أن القرص الصلب يتعرض للتشغيل والإطفاء عدة مرات، يستحسن التحقق من وجود برامج ضارة، وتشغيل برنامج كشف وإزالة الفيروسات، وتنظيف الحاسوب من خلال برنامج مكافحة الفيروسات.

3. الرسائل المنبثقة

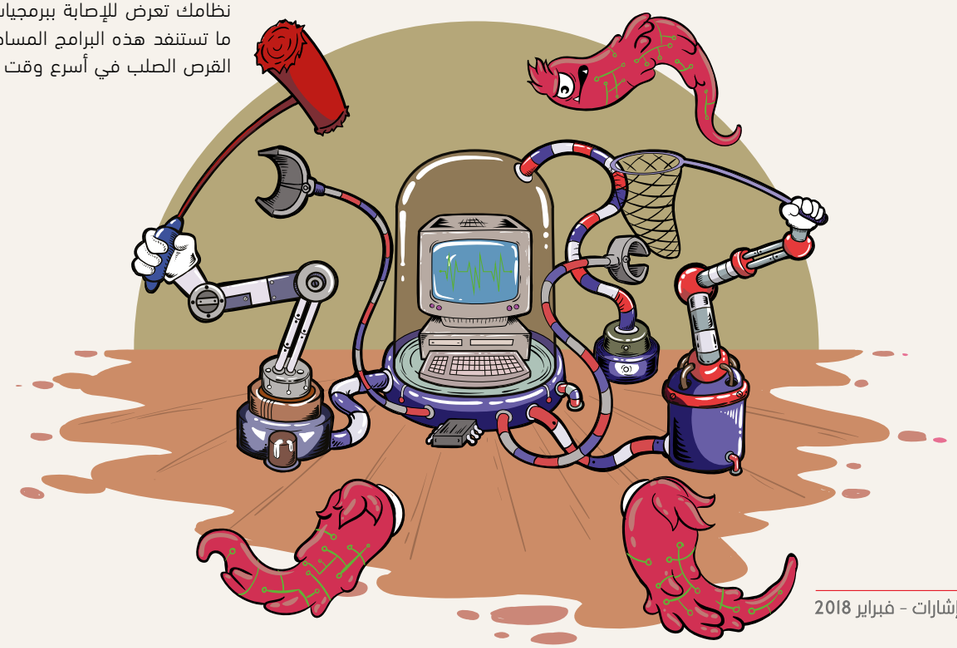
إذا لاحظت أن شاشة حاسوبك أصبحت مزدحمة بالرسائل المنبثقة على الرغم من عدم قيامك بالنقر على أي رابط بصورة متعمدة، هذا يعني أن هناك إحتمالية وجود فيروس في حاسوبك، لذلك ينصح بتشغيل برنامج كشف وإزالة الفيروسات.

4. انخفاض سرعة الجهاز

في أغلب الأحيان تعد برامج التجسس السبب الرئيسي وراء انخفاض سرعة الحاسب الآلي، فإذا كان تشغيل الجهاز أو فتح أي برنامج موجود على جهازك يستغرق وقتاً أطول من المعتاد عند النقر عليه فهذا يعود لسببين؛ إما أن ذاكرة الجهاز أصبحت منخفضة أو أن نظام التشغيل مصاب بفيروس.

5. عدم وجود مساحة على حاسوبك

إذا أصبح القرص الصلب في حاسوبك ممتلئاً فجأة ومن دون سبب وجيه، أو إذا ظهر إشعار تحذيري بأن مساحة الذاكرة أصبحت منخفضة للغاية وتتناقص بصورة مستمرة، فهذا يعني أن نظامك تعرض للإصابة ببرمجيات خبيثة، وعادة ما تستنفد هذه البرامج المساحة المتبقية على القرص الصلب في أسرع وقت ممكن.



ماذا تفعل لو أصيب حاسوبك بفيروس

ماذا تفعل لو نقرت على رابط خبيث وأصيب حاسوبك بفيروس أو برنامج ضار نتيجة لذلك؟ في هذه الحالة سيكون عليك اتخاذ إجراءات فورية لحماية ملفاتك المهمة من التلف، ووقاية حاسوبك وحساباتك الإلكترونية من الاستخدام كوسيلة لمهاجمة الآخرين.

هناك خطوات محددة يجب عليك اتخاذها لإعادة حاسوبك إلى طبيعته في أسرع وقت ممكن بعد التعرض لأي عملية اختراق.

انتقل إلى وضع عدم الاتصال بشبكة الإنترنت

أول خطوة عليك القيام بها هي الانفصال عن شبكة الإنترنت التي يتصل حاسوبك بها. عدم إتاحة الشبكة سيعني أن الاختراق سيكون عديم الفائدة، هذا من وجهة نظر المخترق على الأقل، فلن يستطيع فعل أي شيء إذا كان لا يستطيع الاتصال بحاسوبك.

أغلق الحاسوب وقم بفصل القرص الصلب

أغلق الحاسوب على الفور إذا اكتشفت أن لديك فيروس، وبعد ذلك افصل القرص الصلب وأوصله بحاسوب آخر معزز ببرنامج مكافحة فيروسات متكامل، كل ما عليك هو توصيل القرص الصلب بالحاسوب الآخر عبر فتحة الـ"USB".

قم بفحص القرص الصلب لإزالة الفيروسات

قم بفحص القرص الصلب بعد توصيله بالحاسوب الآخر، تأكد من مسح الفيروسات كلياً من القرص الصلب.

أنشئ نسخة احتياطية

قم بإنشاء نسخة احتياطية لكل البيانات القيّمة على القرص الصلب. خزّن المحتوى على قرص مرن أو على قرص صلب آخر، أو على سحابة على الشبكة وتذكر أننا في عام 2018 فكل شيء يمكن إجراؤه عبر الإنترنت.

أعد القرص الصلب إلى كمبيوترك

عندما تنتهي من إنشاء نسخة احتياطية لملفاتك، يمكنك الاستعانة بخبير لإعادة القرص الصلب إلى الحاسوب وبدء عملية إعادة التشغيل.

احذف الملفات من القرص الصلب

على الرغم من أنك قمت بعمل مسح كامل للملفات لتنظيف القرص من البرامج الخبيثة، إلا أن هذه الخطوة لا تكفي، والطريقة الوحيدة للتأكد من نظافة الحاسوب بنسبة 100% هي حذف كافة الملفات ثم إعادة تثبيت نظام تشغيل جديد، من مصدر موثوق بالطبع.

ثبت التحديثات بشكل كامل

احرص على تنزيل كافة التحديثات وبرامج الإصلاح الخاصة بنظام التشغيل الجديد قبل تثبيت أي برامج أخرى.

ثبت برنامجاً مضاداً للفيروسات، وبرنامجاً مضاداً للتجسس، وأي برامج حماية أخرى

يجب أن تقوم بتثبيت أكبر عدد ممكن من طبقات الحماية قبل أن تبدأ باستخدام الحاسوب، مع الحرص على تثبيت التحديثات وبرامج الإصلاح أولاً، وتذكر أن عدم اتباع هذه الإجراءات سيعرض حاسوبك للتلف مرة أخرى.

تحقق من عدم وجود فيروسات على ملفاتك القديمة قبل تثبيتها على الحاسوب

إذا وصلت إلى هذه الخطوة فهذا يعني أن حاسوبك أصبح خالياً من الفيروسات، ويمكنك إعادة تثبيت ملفاتك القديمة، لكن لمزيد من الحرص عليك دائماً أن تقوم بمسح كامل للملفات التي نقلتها إلى أسطوانة أو قمت بتحميلها على السحابة الإلكترونية من قبل.

اصنع نسخة احتياطية لنظامك

يجب أن تقوم بعمل نسخة احتياطية كاملة لملفاتك حتى لا تضطر لإجراء هذه العملية مرة أخرى في حالة أصيب حاسوبك بفيروس آخر. وتذكّر أن تنشئ نسخة احتياطية بصورة شهرية على الأقل.

كيف تنشئ كلمة سر لا تُخترق لتحمي فضاءك الخاص على الشبكة!

تعتبر كلمات السر المفتاح إلى العالم الخاص بنا ضمن الفضاء الإلكتروني الذي يحيطنا من كل حدب وصوب، فهي تقوم بحماية خصوصيتنا، لذلك أصبح تعلم كيفية إنشاء كلمات سر حصينة، مطلباً ملحاً وأكيداً مع ازدياد عدد الساعات التي نبحر فيها عبر الإنترنت وحجم بياناتنا الكبير على الشبكة، وأي استسهال في إنشاء كلمات السر فإن ذلك يعني وضع هذه البيانات والمعلومات في تصرف القراصنة، الذين سيستخدمونها لصالحهم.

إن آلاف المستخدمين من حول العالم يومياً يقعون ضحايا أعمال قرصنة تكبدهم خسائر مادية ومعنوية كبيرة. وتشير تقديرات وحدة البحوث في مصرف والس فارغو الأميركي إلى أن القرصنة الإلكترونية تكبد الشركات ١٨٠ مليار دولار سنوياً، وتكلف المستخدمين الأفراد ١٢ مليار دولار كخسائر مادية مباشرة، بالإضافة إلى كلفة الوقت المطلوب لاستعادة البيانات.

ولكن كيف يمكننا إنشاء كلمة سر حصينة يصعب اختراقها؟ للإجابة عن هذا السؤال، علينا أولاً أن نتعرف على الأخطاء الشائعة التي نرتكبها في اختيارنا لكلمة السر، وأن نطلع على أساليب عمل القراصنة.

من هم القراصنة؟

إذا كنت تظنّ أن القرصان هو شخص يحاول اختراق حسابك عن طريق تجربة حظه عدة مرات في اكتشاف كلمة السر، وحين يعجز عن ذلك ينتقل إلى حساب آخر، فأنت مخطئ تماماً. فالقراصنة هم في الغالب أشخاص يعتمدون على حواسيب ذات برمجيات متطورة، تهاجم الحساب المستهدف من دون كلل أو ملل، وتكون قادرة على اقتراح ما يصل إلى ألف توليفة لكلمة السر في الدقيقة الواحدة. وبهذه الطريقة، يقوم البرنامج بكشف التوليفة التي قد تكون وضعتها لكلمة السر الخاصة بك.

ما هو الخطأ الشائع في بناء كلمة السر؟

كشفت دراسة عن قطاع الإنترنت أن واحداً من كل عشرة أشخاص يستخدم كلمة سر بسيطة مؤلفة من الأرقام 1234، وأن عشرات الآلاف يستخدمون كلمات سر شائعة يمكن توقعها بسهولة تامة حيث أنها تعتمد في تركيبتها على البيانات الشخصية، مثل تاريخ الميلاد ورقم الهاتف أو العنوان البريدي وأسماء الأبناء.

وتؤكد الدراسة التي أجرتها جامعة لانكستر أيضاً أن السبب الرئيسي الذي لا يزال يدفع الكثير من المستخدمين إلى استخدام كلمات سر سهلة على حساباتهم هو جهلهم بمدى خطورة هذا الأمر. وخلصت الدراسة: إلى أن"السبب الرئيسي الذي يدفع البعض إلى استخدام كلمات سر سهلة هو عدم علمهم بالمخاطر الأمنية على شبكة الإنترنت".

كيف يتم اختراق كلمة السر؟

يتم اختراق كلمات السر بطرق عديدة، أبرزها - كما أشرنا استخدام برامج إلكترونية تحاول الدخول إلى الحساب المستهدف عبر اقتراح آلاف كلمات السر في الدقيقة الواحدة. وهناك طريقة أخرى تدعى Brute Force، حيث يقوم أحد القراصنة بالدخول إلى بيانات إحدى الشركات والحصول على قاعدة بيانات تحتوي عدة ملايين من كلمات السر، فيقوم بفك تشفيرها واستخدامها.

وإذا لم يستطع فك تشفيرها، يقوم بتلقيم الكلمات المشفرة لأحد برامج الاختراق لاستعمالها في تخمين كلمة السر لأحد الحسابات الشخصية واختراقها، وغالباً ما ينجح في ذلك إذا كانت كلمات سهلة.

ولهذا السبب، ينصح الخبراء بأن تكون كلمة السر صعبة لا يمكن تخمينها بسهولة، وأن تكون معقدة من خلال استخدام كلمات ورموز وأرقام، وتبديلها بحد أقصى كل عشرة أسابيع.

المصدر:
www.theguardian.com
securingtomorrow.mcafee.com

نصائح لبناء كلمة سر حصينة

من الضروري جعل كلمة السر قوية جداً، بحيث يصعب التنبؤ بها وتخمينها بسهولة عند أولى محاولات الاختراق من قبل القراصنة. وفيما يلي بعض النصائح المهمة لإنشاء كلمة سر قوية وآمنة يصعب اكتشافها.

- تجنب اختيار الكلمات الشائعة والمتداولة، حتى لو كانت الكلمة التي تختارها عربية لكنها مكتوبة بحروف لاتينية.
- اختر كلمة سر لا تقل عن عشر خانات، بشرط أن تحتوي على حروف وأرقام ورموز، ومن المستحسن أن تستهلك الحد الأقصى من الخانات الذي تسمح به المواقع الإلكترونية.
- تجنب استخدام أسماء الرياضات المفضلة لديك في تركيبة كلمات السر مثل f00tbAll و basketball777، وتجنب استخدام كلمة سرّ تعتمد في تركيبتها على بياناتك الشخصية واحرص على عدم نشر هذه البيانات على مواقع التواصل الاجتماعي (فيسبوك، تويتر وإنستغرام وغيرها)، بحيث يسهل حصول القراصنة عليها واستخدامها لمعرفة كلمة السر الخاصة بك.
- لا تحفظ كلمات السر في جهاز الكمبيوتر أو الهاتف.
- تجنب تكرار الحروف والأرقام والرموز في كلمة السر.
- تجنب استخدام كلمة السر ذاتها في العديد من الحسابات، إذ أن كشفها سيسهل النفاذ إلى جميع حساباتك دفعة واحدة.
- قم بتغيير كلمة السر بصورة منتظمة، مرة في الشهر لحساباتك المصرفية، ومرة كل ثلاثة أشهر للحسابات الأخرى.

كيف تكتشف أن موقعك الإلكتروني تعرض للاختراق؟

المواقع الإلكترونية واحدة من الأهداف المفضلة لدى قراصنة الإنترنت الذين يوجهون لها أنشطتهم الإجرامية لإتلاف كل ما يمكن إتلافه، والسبب الرئيسي لنجاحهم في ذلك هو أن أصحاب المواقع الإلكترونية لا يعيرون بالاً لحماية مواقعهم، حتى إن الكثير من أصحاب المواقع الإلكترونية يعتبرونها أقل أهمية من صفحاتهم على مواقع التواصل الاجتماعي.

وتعتبر المواقع الإلكترونية مفتوحة المصدر مثل مواقع وورد بريس عُرضة لهجمات القراصنة المكثفة، وعلى الرغم من أن "ووردبريس" يعد نظاماً رائداً في اعتماد طرق وأساليب الحماية إلا أنه في بعض الحالات لا ينجح.

لمساعدتك على تجنب وقوع مثل هذه الهجمات الخبيثة على موقعك الإلكتروني، إليك قائمة ببعض الإشارات التي تنبهك إلى أن موقعك الإلكتروني قد تعرض للاختراق:

الرسائل الإلكترونية تبدأ بالارتداد

عادةً ما تبدأ الرسائل الإلكترونية بالارتداد لأن القراصنة يستخدمون حسابك لإرسال آلاف الرسائل العشوائية من عنوان بروتوكول الإنترنت الخاص بك، وفي المقابل يتم تصنيفها على أنها رسائل عشوائية من قِبل آلاف المستخدمين الذين يتلقونها، لذلك فأنت معرض لأن يتم تعليق بريدك الإلكتروني.

محتوى لم تقم بنشره ولكنك تكتشف أنه موجود على الشبكة

إذا كان موقعك الإلكتروني مخترقاً فسوف يستخدمه القراصنة كمنصة سهلة لنشر المحتوى الخاص بك، وقد ينجم عن ذلك عواقب وخيمة تشمل إرسال روابط خبيثة أو نشر محتويات مختلفة.

انخفاض سرعة الموقع الإلكتروني

يعود بطء تحميل الموقع لسببين؛ إما أن المخترق يقوم بإضافة مقدار هائل من الرموز

إلى موقعك، أو أن موقعك الإلكتروني أضيف إلى شبكة تعمل على توجيه حركة البيانات آلياً إلى موقعك من أجل نقلها إلى موقع مستهدف.

اختفاء حركة مرور البيانات

إذا كان موقعك الإلكتروني مخترقاً فإن إدارة محرك البحث "جوجل" ستكون أول من يعلم، وسوف تطلع كافة المستخدمين الآخرين، وربما تدرجك في القائمة السوداء وسيظهر تحذير إلى جانب قائمتك، هذا إذا عثر أحد عليك. الخلاصة، إذا لاحظت تباطؤ حركة مرور البيانات الخاصة بك بدرجة كبيرة فاعلم أن موقعك الإلكتروني مخترق.

زيادة حركة مرور البيانات

إذا كان موقعك على "ووردبريس" يستقبل حركة بيانات من أماكن لا تتوقع أن يهتم المتصفحون فيها بموقعك الإلكتروني، فاعلم أن "روبوتات" تحاول العثور على نقطة ضعف والنفاذ من الباب الخلفي لموقعك الإلكتروني. إذا زادت حركة مرور البيانات القادمة من دولة لا تقع ضمن جمهورك المستهدف، فهناك احتمال كبير بأن أحد الروبوتات وجد نقطة ضعف لديك.

اختفاء موقعك الإلكتروني كلياً

إذا كنت لا تستطيع الولوج إلى موقعك الإلكتروني فالاحتمال الأكبر أنه تعرض للاختراق، وعادة من يعطله النظام المضيف لحماية مستخدمي الشبكة، وفي هذه الحالة يجب عليك إدارة الملفات التالفة وإزالتها يدوياً، أو يمكنك تكليف مدير الموقع أو أحد شركائه بعمل ذلك بالنيابة عنك مقابل مبلغ مالي.

إذا كنت تمتلك أو تدير موقعاً إلكترونياً، فعليك أن تضع في صدارة أولوياتك مراقبة الموقع وتحديثه وعمل نسخ احتياطية بصورة مستمرة. وهذه هي الطريقة المثالية لحمايته من الاختراق الأمر الذي سيعزز من موقفك ويساعدك على سرعة الاستجابة واتخاذ الإجراءات اللازمة إذا تم استهداف موقعك الإلكتروني.

حماية المؤسسات

كيف تحمي مؤسستك من الهجمات الإلكترونية!

الأمر يبدأ بتطبيق أحدث معايير الأمان الإلكترونية العالمية

كلما ارتفع ثراء الدول أصبحت أكثر عرضة للهجمات الإلكترونية، هكذا جاء في نتائج دراسة صادرة عن شركة "ديلويت"؛ وبحسب التقرير جاءت بريطانيا وأمريكا وكوريا الجنوبية واليابان على رأس قائمة أكثر الدول تعرضاً للجرائم الإلكترونية. وتتسبب الجرائم الإلكترونية في تكلفة المؤسسات التجارية عالمياً حوالي ٤٠٠ مليار دولار سنوياً وذلك وفقاً لدراسة صادرة عن مركز الدراسات الاستراتيجية والدولية.

تؤدي الهجمات الإلكترونية إلى إلحاق أضرار جسيمة بالشركات بطرق تفوق سرقة الأموال التقليدية، إذ إن خطرها يتخطى الخسائر المالية ليشمل خطر الإضرار بالسمعة، كما يمكن أن تشكل عائقاً أمام المعاملات التجارية للمؤسسة مما يترتب عليه توقف المشاريع والخدمات.

وتتخذ الهجمات الإلكترونية شكلاً أكثر خطورة في البلدان المتقدمة، لدرجة أن آثارها المدمرة تتسبب في انخفاض معدلات التوظيف بشكل كبير. وإذا كنت تعتقد أن مؤسستك بعيدة عن مثل هذه الهجمات فأنت بذلك ترتكب خطأ سيتسبب في جعلك فريسة سهلة للقراصنة الإلكترونيين، لذلك من الضروري أن تحمي معلوماتك وبياناتك، بل ويجب أن تعامل الأنظمة والشبكات التي تعمل عليها مثل باب بيتك.

السياسة الداخلية

القوى العاملة تعتبر الخطر الأكبر على الأمن الإلكتروني لأي مؤسسة أي الموظفون والعاملون أنفسهم، فهناك أمثلة لا تحصى لقراصنة تمكنوا من اختراق أنظمة وشبكات كبرى بسبب تصرف أحد العاملين بإهمال، مثل قيامه بالنقر على رابط خبيث، أو استخدام كلمة سر متوقعة مثل استخدام التسلسل 123456 التي لا تعتبر كلمة سر بل دعوة للمخترقين، وفي حالات أخرى كثيراً ما يقوم أحد الموظفين بتقديم معلومات سرية عبر الهاتف مع طرف آخر يحمل هوية مزيفة، وهناك أمثلة كثيرة أخرى. فالخطط الاحتيالية تحيط بنا كل يوم وتتخذ أشكالاً متغيرة مع مرور الوقت، لذلك يجب علينا أولاً أن نرفع مستوى الوعي لدى الأفراد حتى نغلق الباب أمام أي هجمات تستهدف أمننا الإلكتروني.

قم بتحديث البرمجيات

عليك أولاً أن تستجيب على الفور لأي طلب تحديث من قِبل نظام التشغيل أو برنامج الحماية الخاص بك، وتذكّر أن تجاهلها سوف يجعلك عُرضة للمزيد من الهجمات الحديثة التي لن يستطيع النظام التعرف عليها نظراً لعدم تحديثه.

تحدّث مع خبير متخصص

معظمنا لا يعرف سوى معلومات أساسية جداً عن أمن الإنترنت؛ إذ يمكننا تغيير كلمات السر بانتظام، لكننا نتجاهل ذلك، ويمكننا أيضاً ابتكار كلمات مرور معقّدة من تركيبات الأرقام والحروف، كما أننا نتجاهل ذلك أيضاً، ويمكننا تنزيل آخر تحديثات برامج جدار الحماية. لكن ليس هناك بديل للاستعانة بخبير لتقديم النصائح ومساعدتنا على تقييم واختبار أنظمتنا وشبكاتنا.

وفي ظل التقنيات المتطورة التي تتيح لقراصنة الإنترنت إمكانية تحديد نقاط الضعف في الأنظمة بسرعة مذهلة، أصبح من الضروري علينا الاستعانة بخبير ليقوم بتحديد هذه النقاط وإصلاحها قبل أن يصل أي مخترق إليها. ربما يكون هذا إجراءً مكلفاً بعض الشيء، لكنه لن يساوي شيئاً إذا قارنته بمدى الدمار الذي سيلحق بأنظمتك إذا تعرضت لإحدى الهجمات الخبيثة.

وإذا كنت لا تتصور خطورة هذه الهجمات، يمكنك أن تبحث عن قصص لضحاياها الكبار أمثال "ياهو" و"آي بي إم" و"لويدز" و"سوني" و"فيسبوك" و"تويتر"، وحتى "آبل"؛ هذه الشركات العملاقة ستوضح لك حجم الأضرار الفادحة التي تعرضت لها جرّاء الهجمات الإلكترونية.

تأكد من تحديث برامج حاسوبك قبل استخدامك لشبكات الواي فاي

كشفت دراسة أجراها الباحث البلجيكي ماثي فانهوف من جامعة "لوفين" في بلجيكا أن القراصنة يستطيعون اختراق بيانات جميع مستخدمي شبكات واي فاي.

وأصدر"فانهوف معلومات حول الثغرة التي أطلق عليها اسم (KRACK) "هجوم مفاتيح التثبيت"، وكشفت المعلومات عن حقائق صادمة، إذ تسمح هذه الثغرة للمخترقين بفك شفرات الأجهزة المحمية والوصول إلى كافة بياناتك عند استخدام أي شبكة واي فاي، سواء كانت خاصة أو عامة.

ووصف فانهوف هذه الثغرة على موقعه الإلكتروني قائلاً "يمكن أن يستخدم القراصنة هذه الثغرة لسرقة معلومات خاصة مثل أرقام البطاقات الائتمانية وكلمات المرور والمحادثات ورسائل البريد الإلكتروني والصور وغيرها، ويمكن لهذا الهجوم استهداف كل شبكات الواي فاي الحديثة المحمية، واستناداً إلى تكوين الشبكة يستطيع القراصنة إدخال البيانات والتلاعب بها، إذ يمكن للقرصان على سبيل المثال إدخال برنامج فدية أو أي برامج خبيثة إلى المواقع الإلكترونية".

وتكمن نقطة الضعف في بروتوكول "WPA2" المسؤول عن حماية شبكات الواي فاي، وهو ما يستخدمه أغلبية مستخدمي شبكات الواي فاي لحماية بياناتهم. وتعمل الثغرة (KRACK) على خداع المستخدم وجعله يقوم بإعادة تثبيت مفتاح تشفير.

إن مفتاح التشفير الذي يمثل الاتفاقية بين راوتر شبكة الواي فاي والجهاز أو الكمبيوتر المتصل به، عادة ما يكون مفتاحاً فريداً ولا يستخدم سوى من قِبل مستخدم واحد فقط. ومع إتمام التنسيق والتوصيل يتم توليد مفاتيح التشفير وينتج عنه رقم واحد. وقد وجد الباحث أن القرصان يستطيع التلاعب بهذا التنسيق الأول عبر بروتوكول "WPA2" حتى يتحول ذلك المفتاح الجديد والفريد إلى مفتاح قديم ومستخدم، وهذا ما يتيح للمخترق التجسس على كافة البيانات الصادرة والواردة عبر الشبكة.

وتعتبر الأجهزة العاملة بنظام تشغيل أندرويد الأكثر عُرضة للاختراق، حيث اكتشف الباحثون خطأً في الترميز يتيح للقراصنة إنشاء المفتاح من خلال إعادة تثبيته، إضافة إلى أنظمة التشغيل التي تستخدم "مفتاح التشفير الصفري" وهي أيضاً أكثر عُرضة للهجمات الخبيثة.

الخلاصة هي أن كافة الأجهزة التي تستخدم شبكات الواي فاي مُعرضة للاختراق بحسب فانهوف الذي يؤكد أن "الثغرات تكمن في معايير شبكات الواي فاي نفسها، وليس في الأجهزة أو أنظمة التشغيل، لذلك يمكن اختراق أي نسخة لبروتوكول "WPA2". ولتجنب هذه الهجمات يجب على المستخدمين تحديث أجهزتهم المصابة بالثغرات بمجرد أن تتاح التحديثات الأمنية. وتذكر أن جهازك سيكون مصاباً بثغرة على الأرجح ما دام يدعم شبكة الواي فاي. فقد اكتشفنا خلال بحثنا المبدئي أن نظم التشغيل "أندرويد" و"لينكس" و"آبل" و"ويندوز" و"أوبن بي إس دي" و"ميديا تك" و"لينكسيس" تعرضت لأشكال مختلفة من الهجمات.

هذا يعني أنه يجب على كل مستخدمي شبكات الواي فاي تحديث أجهزتهم على الفور، بما في ذلك أجهزة الكمبيوتر والأجهزة الذكية والحواسيب اللوحية، وأجهزة تشغيل الألعاب والتلفزيون والراديو وأنظمة السيارات، وغيرها. وتجاهل ذلك قد يعود بعواقب وخيمة قد تصل إلى سرقة كافة المعلومات الشخصية مثل كلمات السر وتفاصيل الحسابات البنكية.

جاءت ثغرة KRACK لتكون بمثابة نداء استغاثة يحذر مجتمع الأمن الإلكتروني حول العالم، بعد أن كنا نعتقد أن شبكات الواي فاي الخاصة هي محيط آمن كلياً. إلاّ أن هذا العيب الجذر ي في بروتوكول الحماية"جعل مليارات المستخدمين فريسة سهلة أمام القراصنة برغم أن مسار الهجمات البعيدة دائماً ما يكون معقداً وغير مضمون نظراً لضرورة تواجد المخترق بالقرب من الجهاز. لكن هذا الاكتشاف أثار معه بعض التساؤلات الهامة حول ما إذا كانت هناك عيوب أخرى في الإعدادات العامة للشبكات والتي كان يعتقد المستخدمون أنها آمنة كلياً! نرجو أن تتمكن الفرق الأخلاقية من اكتشاف تلك الثغرات قبل أن تصل إليها فرق الظلام.

المصدر: *www.forbes.com*