ISSUE 04 DECEMBER 2019

إشارات
Esharat

Dedicated to a safer cyberspace

THE FUTURE OF CYBERSECURITY

DESC POLICIES ENSURE PROTECTION

5G PROMISES UNPRECEDENTED SPEED

TIPS FOR HEALTHIER TECH HABITS

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

www.desc.dubai.ae

التحرير والتصميم

سفن جي ميديا للاستشارات

هيئة التحرير
أماني أبوسيدو
ماري جين بوثا
أحمد مرسال
نيكول رهبان

التصميم الفني
سري إي إس
ياسمين المنير

الرسم
أكيلا شيكار

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

هل فعّلت خاصية التّحقّق بخطوتين على حساباتك الإلكترونية؟

تتيح خاصية التحقّق بخطوتين طبقة حماية إضافية لحسابك الإلكتروني، وتحد من خطر الاختراق حتى وإن تم الكشف عن كلمة المرور الخاصة بك. يمكنك تفعيل خاصية التحقق بخطوتين لكافة حساباتك الإلكترونية بخطوات سريعة وبسيطة من خلال الإعدادات. وفي كل مرة تقوم فيها بالدخول إلى حسابك، سيُطلب منك تأكيد الدخول عبر خطوتين:

الخطوة الأولى - سيطلب منك إدخال كلمة المرور

الخطوة الثانية - سيطلب منك إدخال رمز التحقق الذي يتم إرساله قبيل الدخول إلى الحساب إلى رقم هاتفك المتحرك أو بريدك الإلكتروني، وستستخدمه لمرة واحدة فقط.

هاتان الخطوتان توفران لحساباتك حماية أمنية مضاعفة وتؤمن حماية مضاعفة لحسابك الإلكتروني.

مزايا خاصية التحقق بخطوتين

- تحدّ من مخاطر سرقة الهوية
- تخفض من احتمالات اختراق حسابك الإلكتروني
- تحمي بياناتك
- تضيف طبقة حماية إضافية لكلمات المرور

#الوعي_أمان

مركز دبي للأمن الإلكتروني يؤسس شراكات استراتيجية لتأمين فضائنا الإلكتروني

عام آخر يشرف على نهايته.. وقد كان عاماً زاخراً بالإنجازات المتميزة والخطط الرائدة التي اتخذها مركز دبي للأمن الإلكتروني نحو تنفيذ خطة دبي الاستراتيجية للأمن الإلكتروني ضمن مسيرتنا لتحقيق رؤية صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، الرامية إلى جعل مدينة دبي الأكثر أماناً في الفضاء الإلكتروني، وقد دفعت موجة التطوّر التكنولوجي الفائقة في العام 2019 مبادرات مركز دبي للأمن الإلكتروني إلى الأمام بشكل حثيث.

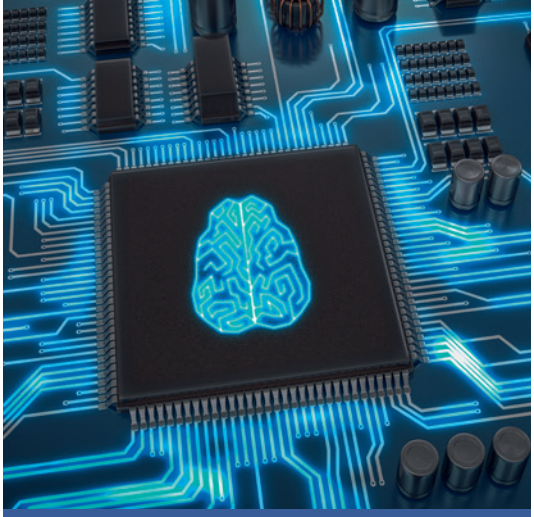
يقوم مركز دبي للأمن الإلكتروني، من خلال شراكاته الاستراتيجية بتوفير فرص ريادية في مجال الأبحاث المتقدمة والتطوير وإطلاق ابتكارات استشرافية بما يضمن فضاء آمن لإمارة دبي. وترتكز مهمتنا على دعم الجهات الحكومية وشبه الحكومية ورواد الأعمال وتمكينهم من تسريع نمو مشاريعهم في بيئة إلكترونية آمنة بما يدعم رؤية دبي لتحقيق التنمية الاجتماعية والازدهار الاقتصادي والعلمي في المستقبل القريب.

لقد قام مركز دبي للأمن الإلكتروني بإطلاق "مبادرة دبي للأبحاث والدراسات السيبرانية" التي تُعدّ الأولى من نوعها في منطقة الشرق الأوسط، وتقوم هذه المبادرة على الخطة الاستراتيجية الأساسية للمركز التي تتضمن بناء شراكات رفيعة المستوى تعمل على تطوير منصة تفاعلية للعصف الذهني تهدف إلى وضع حلول لمواجهة الهجمات الإلكترونية الحالية والمستقبلية. وتشكل الشراكات الاستراتيجية الأخرى التي يعقدها المركز مثل "قمة معهد مهندسي الكهرباء والإلكترونيات للذكاء الإلكتروني" و"مؤتمر Hack In The Box للأمن الإلكتروني"، وافتتاح مختبرات لأبحاث الأمن الإلكتروني في الجامعات الوطنية الرائدة في الدولة مثالاً جلياً على تبني المركز للتقدّم التكنولوجي الذي يستهدف تطوير حلول مبتكرة لتأمين فضاء دبي الرقمي.

ويحرص المركز على الاستفادة من الفرص المستقبلية التي توفرها التقنيات المُتقدمة مثل الذكاء الاصطناعي الذي يقوم على استخدام التعلّم العميق ومعالجة اللغات الطبيعية لتعزيز الإمكانيات البشرية. وفي هذا السياق، يعمل فريق الاستجابة للأزمات في مركز دبي للأمن الإلكتروني على إجراء اختبارات الاختراق من خلال محاكاة النهج الذي يسلكه المخترقون لتنفيذ عمليات الاختراق، ومن ثم تحديد مواطن الضعف فيها ومعالجتها، على الرغم من أن أنظمة الحواسيب الحكومية تحظى بحماية متكاملة من قِبل سياسات الأمن الإلكتروني التي يطبقها المركز والتي تشمل سياسة أمن الإنترنت والمعايير الأمنية لمقدمي الخدمات السحابية.

لا شك أن التوعية بشأن أمن المعلومات أمر حتمي لإنجاح استراتيجية الأمن الإلكتروني، إذ أن المجتمع الواعي يشكّل مجتمعاً آمناً مستعداً لمواجهة أي مخاطر تهدد فضاءه الرقمي. وتدعم مجلة "إشارات" أهداف مركز دبي للأمن الإلكتروني من خلال مشاركة المعرفة معكم، قراءنا الأعزاء، وإطلاعكم على أحدث ما وصلت إليه تكنولوجيا المعلومات وأحدث مستجدات العالم الافتراضي سريع الخطى الذي يعمل المركز على تأمينه وحراسته طوال الوقت. إن مواكبة هذا العصر الرقمي الجديد تعتمد بشكل كبير على النهج الذي نتبعه وكيفية استخدام هذه الابتكارات التقنية المتطورة بصورة آمنة من أجل بناء مستقبل مشرق يسوده الاستقرار والازدهار في إمارة دبي ودولة الإمارات.

يوسف حمد الشيباني
المدير العام
مركز دبي للأمن الإلكتروني



اقرأ في هذا العدد

مركز دبي للأمن الإلكتروني يدعم **مبادئ دبي الاستراتيجية الثمانية** التي أطلقها صاحب السمو الشيخ محمد بن راشد آل مكتوم

يعمل مركز دبي للأمن الإلكتروني على إدارة التخطيط الاستراتيجي والأنشطة المركزية وفقاً لمبادئ دبي الاستراتيجية للحكم والحكومة في دبي، كما أعلن عنها صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، في يناير من هذا العام.

جاء هذا الإعلان التاريخي تزامناً مع مرور خمسين عاماً من القيادة الحكيمة لصاحب السمو في خدمة دولة الإمارات، وقال صاحب السمو إن المبادئ الثمانية هي المبادئ التي قامت عليها دبي ومضى عليها الحكم سابقاً.

وأعلن صاحب السمو أن هذه المبادئ "هي مبادئ حكم وحكومة.. ضماناً لرفاه شعبنا وتفوق بلدنا وخير أجيالنا التي لم تأت بعد"، ودعا الأجيال المستقبلية إلى الحفاظ على هذه المبادئ، كما دعا كل من يتولى مسؤولية في إمارة دبي إلى الالتزام بها والتمسك بما جاء فيها وضمان تطبيقها.

وقد ارتكزت استراتيجية الأمن الإلكتروني التي أطلقها مركز دبي للأمن الإلكتروني على أسس رؤية صاحب السمو الشيخ محمد بن راشد، وتستهدف هذه الاستراتيجية حماية دبي من المخاطر ودعم نمو الإمارة وتضمن ازدهار اقتصادها.

ومن منطلق التزامه بتأمين الفضاء الرقمي في دبي، يتبع مركز دبي للأمن الإلكتروني إرشادات صاحب السمو الشيخ محمد بن راشد آل مكتوم ومبادئه الاستراتيجية، فالفضاء الرقمي المفتوح الموثوق يضيف قيمة لكافة الأفراد والقطاعات العامة والخاصة، حيث يقلص الحواجز في عالم الأعمال والحواجز بين الدول والمجتمعات والأفراد، ويسمح بمشاركة المعلومات الآمنة على نطاق عالمي.

مبادئ دبي الاستراتيجية الثمانية التي أرساها صاحب السمو الشيخ محمد بن راشد

1. الاتحاد هو الأساس

دبي جزء أساسي من دولة الإمارات وركن في الاتحاد، ومصيرها مصير دولة الإمارات، وخيرها لكل الإمارات، وشعبها فداء لكل ذرة في دولة الإمارات.

مصلحة الاتحاد فوق مصلحتنا، وقوانين الاتحاد فوق قوانيننا وتشريعاتنا، وسياسة الاتحاد هي سياستنا، وأولويات حكومة الاتحاد هي أولويات حكومتنا.

2. لا أحد فوق القانون

العدل دولة وقوة وعزة وضمان ازدهار واستقرار. لا أحد فوق القانون في دبي، بدءاً من الأسرة الحاكمة، ولا يفرق القانون بين مواطن ومقيم، أو غني وفقير، أو ذكر وأنثى، أو مسلم وغير مسلم، والتأخير في تنفيذ العدالة ظلم، والظلم في أي مكان هو تهديد للعدالة في كل مكان.

3. نحن عاصمة للاقتصاد

هدف حكومة دبي وغايتها تحسين حياة شعبها بتحسين اقتصادها. دبي لا تستثمر في السياسة أو تشارك فيها، ولا تعول على السياسة لضمان تفوقها. دبي صديقة لكل من يحمل لها ولدولة الإمارات الخير، وصديقة للمال والأعمال ومحطة عالمية لخلق الفرص الاقتصادية.

4. النمو له محركات ثلاثة

نمو دبي تقوده محركات ثلاثة هي: حكومة ذات مصداقية ومرونة وتميز، وقطاع خاص نشط وعادل ومفتوح للجميع، وشركات عامة وحكومية تنافس عالمياً وتدر دخلاً للحكومة ووظائف للمواطنين وأصولاً لأجيال المستقبل.

5. مجتمعنا له شخصية مُتفردة

مجتمعنا يسوده الاحترام، ويربط كافة مكوناته التسامح، ويبتعد عن العنصرية والتمييز.. هو مجتمع يتميز بكثرة العمل وقلة الجدل، مجتمع يتميز بالانضباط والالتزام في وعوده ومواعيده وعهوده؛ متواضعون عند النجاح، مثابرون عند التحديات، ناشرون للخير، منفتحون على الجميع.

6. لا نعتمد على مصدر واحد للحياة

تنويع الاقتصاد قاعدة في دستور دبي غير المكتوب منذ عام 1833. وتغير الزمن وسرعة التطورات يفرض الالتزام بهذا المبدأ دائماً وأبداً. وهدفنا الجديد استحداث قطاع اقتصادي جديد على الأقل كل ثلاثة أعوام.. قطاع منتج ومساهم في ناتجنا المحلي وموفر للوظائف وقادر على الاستمرار بقوة دفعه الذاتية.

7. أرض للمواهب

دبي قامت على الموهوبين من التجار والإداريين والمهندسين والمبدعين والحالمين. وبقاء دبي متفوقة مرهون ببقائها قبلة للمتفوقين، واستمرار تنافسيتها مرهون باستمرار استقطابها لأصحاب العقول والأفكار. ولا بد من تجديد سياساتنا وإجراءاتنا بشكل مستمر لتجديد جاذبيتنا للمواهب، ولا بد من بناء الحياة الأفضل في دبي لأصحاب العقول والأفكار الأفضل.

8. نفكر بالأجيال

لا نترك مصير الأجيال القادمة مرهوناً بتقلبات السياسة الإقليمية ودورات الاقتصاد العالمية، بل نستثمر لهم، ونخلق أصولاً استثمارية من أجلهم. وقاعدتنا في ذلك أن تمتلك الحكومة في كل الأحوال أصولاً تعادل عشرين ضعف ميزانيتها السنوية على الأقل.

نسعى لضمان المستقبل ونفكر من اليوم في رخاء أجيالنا القادمة.

مركز دبي للأمن الإلكتروني يضع معايير الأمن الرقمي للمواقع الإلكترونية الحكومية

قامت مجلة "إشارات" في إجراء مقابلة صحفية مع الدكتورة بشرى البلوشي، رئيس قسم الأبحاث والابتكار في مركز دبي للأمن الإلكتروني، للتعرف على سياسة أمن الإنترنت التي أطلقها المركز في العام 2019 بهدف حماية المواقع الإلكترونية للجهات الحكومية من مخاطر الفضاء الرقمي والهجمات الإلكترونية من خلال تزويدها بالضوابط التي يجب تطبيقها والتي يمكن للمطورين من خلالها وضع أسس أمن الأنظمة والتصميمات الرقمية لبنية المواقع الإلكترونية الحكومية.

أوضحت الدكتورة بشرى البلوشي، أنه في عالمنا الرقمي دائم التطوّر، أصبح حتمياً على الجهات الحكومية تبنّي نهج استباقي لحماية قواعد بياناتها وأصولها الرقمية، وتطوير المواقع الإلكترونية الحديثة بحيث يمكن تزويدها بأحدث التقنيات الرقمية وأدوات الرقابة الأخرى، وأصبح على جهات الأمن الإلكتروني وضع شبكة أمنية واقية على نطاق واسع لحماية المنتجات والخدمات المتعلقة بالإنترنت. وقد انضمت تطبيقات الهواتف الذكية وتطبيقات الإنترنت وواجهات برمجة التطبيقات ومعايير الترميز الآمن وآليات اختبار الأمان ونطاقات المعلومات العامة إلى المواقع الإلكترونية لتحقيق المرونة اللازمة تجاه الهجمات الإلكترونية.

وقالت الدكتورة بشرى البلوشي إن المركز قام بإعداد "سياسة أمن المواقع الإلكترونية" لدعم الجهات الحكومية في إمارة دبي ومساعدتها على تحقيق أعلى مستويات الأمن الإلكتروني الشمولي. كما توفر السياسة دليلاً لتحديد مبادئ أمن المعلومات التي يجب على أي مؤسسة أو مُطوّر اتباعها بمسؤولية.

الدكتورة بشرى البلوشي، رئيس قسم الأبحاث والابتكار في مركز دبي للأمن الإلكتروني

وتشير البلوشي إلى أن "الهدف الأساسي من سياسة أمن المواقع الإلكترونية يتمثل في الحد من نقاط الضعف الرقمي في قنوات التواصل الرقمية التي توفرها الجهات الحكومية لخدمة المستخدمين."

وتوضح أنه "بدلاً من البحث عن نقاط الضعف في المنتجات المعتمدة على شبكة الإنترنت، قام المركز بوضع مجموعة من الضوابط الأمنية الأساسية التي يمكن للمطورين - أكانوا تابعين للمؤسسة أم تم إسناد المشاريع إليهم - تنفيذها بدءاً من مراحل التطوير الأولى."

يتم تطبيق العديد من مبادئ أمان شبكة الإنترنت داخل نطاق المواصفة، أكان المنتج مُطوراً داخل الشركة أم من قبل مزود خارجي، أم إذا كان قد تم شراؤه أو قائماً على أحد الحلول الموجودة (في هذه الحالة يتم إجراء عملية تقييم للمخاطر وتهيئة الضوابط المطبّقة).

تضافر الجهود لضمان أمن دبي

إن مواصفة أمن المواقع الإلكترونية ليست إلزامية لغاية الآن، ولكن الامتثال للتشريعات يُعدّ جزءاً أساسياً في أنظمة التقييم التي يعتمدها مركز دبي للأمن الإلكتروني.

وقالت البلوشي: "تم منح الهيئات الحكومية مهلة لمدة عام كامل لتنفيذ المواصفة؛ إذ أن معظمها تمتلك مواقع إلكترونية. ويفضّل المركز دائماً تقديم الحوافز لعملائه لتشجيعهم على الاستفادة من المبادئ التوجيهية والسياسات الخاصة بالمعلومات والأمن الإلكتروني بدلاً من إلزامهم بالامتثال للقوانين."

إن اعتماد السياسات التي يفرضها مركز دبي للأمن الإلكتروني يُعدّ من بين مؤشرات الأداء الرئيسة ضمن برنامج دبي للأداء الحكومي المتميز، وتقوم إدارة جوائز البرنامج بمكافأة وتكريم موظفي الجهات الحكومية المتميزين والإدارات والمبادرات المبتكرة، وهي جوائز رفيعة المستوى.

وتهدف "استراتيجية دبي للأمن الإلكتروني" إلى توفير الحماية المتكاملة من التحديات والمخاطر التي تصاحب التقدم التكنولوجي ومسار التحول الذكي الذي تسلكه إمارة دبي، كما يعمل الدعم الشامل للابتكار في مجال الفضاء الرقمي على تعزيز التنمية المستدامة والازدهار الاقتصادي.

محاور خطة دبي الاستراتيجية للأمن الإلكتروني

تستند خطة دبي الاستراتيجية للأمن الإلكتروني إلى تنفيذ خمسة محاور رئيسية لتوفير فضاء رقمي آمن:

- **مجتمع واعٍ بمخاطر الأمن الإلكتروني -** بناء الوعي والمهارات والقدرات اللازمة لإدارة مخاطر الأمن الإلكتروني في المؤسسات العامة والخاصة ولدى الأفراد.
- **أمن الفضاء الرقمي -** وضع ضوابط لحماية سرية البيانات ومصداقيتها وتوفّرها وخصوصيتها.
- **الابتكار -** تشجيع الابتكار والبحث العلمي في مجال الأمن الإلكتروني، وإنشاء فضاء إلكتروني يتّسم بالحرية والعدل والأمن ويشجع الابتكار.
- **الحفاظ على مرونة الفضاء الرقمي -** العمل على ضمان استمرارية وتوفّر أنظمة تكنولوجيا المعلومات.
- **التعاون المحلي والدولي -** بناء شراكات مع القطاعات المختلفة المحلية والعالمية لإدارة مخاطر الفضاء الرقمي.

يشكّل تنفيذ مواصفة أمن المواقع الإلكترونية ومبادئها التوجيهية الداعمة جزءاً جوهرياً من استراتيجية دبي للأمن الإلكتروني التي يعتمدها مركز دبي للأمن الإلكتروني، كما أنها تساهم في تحقيق رؤية صاحب السمو الشيخ محمد بن راشد آل مكتوم حاكم دبي، رعاه الله، الرامية إلى جعل إمارة دبي واحة للابتكار والأمن والأمان على مستوى العالم.

التطبيقات والمتطلبات

تُطبّق السياسة على العناصر الأساسية الأربعة التالية لأمن الفضاء الرقمي:

- أمن المواقع الإلكترونية
- أمن تطبيقات الإنترنت
- أمن تطبيقات الهواتف المتحركة
- أمن واجهات برمجة التطبيقات

ومن بين المتطلبات الأخرى الموضحة في السياسة، تأتي تلك المتطلبات التي تشرف على المصادقة وإدارة الهوية، والتفويض / والتحكم بإمكانية الوصول، وتكوين الموقع، وتخزين البيانات، والتشفير، والتسجيل ومعالجة الأخطاء، وخادم الاستضافة، وقواعد بيانات العملاء وبرمجيات الأطراف الثالثة من بين عناصر أخرى من أمن الإنترنت المتكامل.

> "الهدف الأساسي لسياسة أمن الإنترنت يتمثل في الحد من نقاط الضعف الرقمية في قنوات التواصل الرقمية التي توفرها الجهات الحكومية لخدمة المستخدمين"

مركز دبي للأمن الإلكتروني **قوة محركة للابتكار** في قطاع الأمن الإلكتروني

الاكتشافات والاختراعات ترى النور بفضل لقاء العقول المبتكرة والكوادر الخبيرة في المجتمعات العلمية التي يرعاها الدعم والتمويل، وتعتبر مختبرات أبحاث الأمن الإلكتروني التي يمولها مركز دبي للأمن الإلكتروني في مجموعة من الجامعات الرائدة في دولة الإمارات مثالاً يحتذى لدعم الابتكارات والأبحاث العلمية.

يشكل الابتكار وتشجيع البحث العلمي في مجال الأمن الإلكتروني محوراً رئيسياً في خطة دبي الاستراتيجية للأمن الإلكتروني لتأسيس فضاء رقمي آمن، ويوفر المركز الدعم المالي للمجتمع العلمي الوطني من خلال تقديم المنح لدعم الأبحاث وقنوات التمويل الأخرى لتعزيز مساعيها لتطوير ابتكارات متقدمة تقنياً تهدف لجعل فضاء دبي الرقمي الأكثر أماناً على مستوى العالم. وانطلاقاً من هذه الرؤية، فقد تم إطلاق مختبرين للأمن الإلكتروني - في كل من جامعة دبي وجامعة الشارقة - في وقت سابق من هذا العام، وحالياً يجري العمل فيهما ومن المخطط إطلاق مختبر آخر في جامعة خليفة في المستقبل القريب.

وأكدت الدكتورة بشرى البلوشي، رئيس قسم الأبحاث والابتكار في مركز دبي للأمن الإلكتروني، هذا التوجه العلمي للمركز، موضحة أن المركز يأتي في صدارة المؤسسات الحكومية في مجال التعاون العلمي والبحثي وبما يتناسب مع مبادئه الاستراتيجية الرئيسة لتحقيق الأمن الإلكتروني.

وأضافت الدكتورة بشرى إن العديد من الجهات الحكومية المحلية والاتحادية تقوم بزيارتنا للتعرف على مسيرتنا الناجحة في مجال البحث العلمي وكيف نقوم بتطوير شراكات مع المؤسسات التعليمية العريقة.

وقالت: "لقد قمنا في البداية بإطلاق مسابقة للمشاريع البحثية المبتكرة في مجال الأمن الإلكتروني وكانت الاستجابة ممتازة من داخل الدولة وخارجها، وقد تلقينا أفكاراً بحثية رفيعة المستوى، مما شجعنا على تمديد فترة المسابقة ومنحها صفة رسمية". وأشارت البلوشي إلى أن "المسابقة تُرحب بالأبحاث المقترحة من الجامعات وقطاع الأمن الإلكتروني والجهات الأخرى شرط أن تكون نتائج الأبحاث عملية وليست نظرية، وأن ينعكس تأثيرها إيجاباً في مجال الأمن الإلكتروني بدبي، الأمر الذي يؤدي إلى دفع عجلة النمو الاقتصادي الوطني في المستقبل."

وأضافت: "حرصاً من مركز دبي للأمن الإلكتروني على حماية كافة البيانات في المركز، فقد تقرر منح الباحثين فرصة لإجراء أبحاثهم في مختبرات متخصصة داخل الجامعات."

وتؤكد البلوشي أن مركز دبي للأمن الإلكتروني يعقد اجتماعات منتظمة مع فرق عمل مختبرات أبحاث الأمن الإلكتروني لمتابعة مخرجات الأبحاث وضمان تطورها للحصول على نتائج ثابتة، فيما تعرض نتائج ومخرجات الأبحاث على جهتين حكوميتين قبل النظر في تطبيقها.

DESC CYBER INTELLIGENCE LAB

الدكتورة سميرة الملا أحد أعضاء الفريق القيادي لمختبر أبحاث الأمن الإلكتروني والباحث المساعد كارل بيرون والباحثان محمد وائل وعمر أحمد

مختبر "بايت" بالشراكة بين مركز دبي للأمن الإلكتروني وجامعة الشارقة

أقامت جامعة الشارقة بالتعاون مع مركز دبي للأمن الإلكتروني في يناير الماضي "مختبر بايت" الذي يُعنى بالتحقق من عمليات الفحص الأمني للأعداد المتزايدة من أجهزة إنترنت الأشياء إضافة إلى الأبحاث التي تقام في مجال البلوك تشين والذكاء الاصطناعي والمجالات الأخرى المتعلقة بالفضاء الرقمي.

افتتح المختبر سعادة يوسف الشيباني، مدير عام مركز دبي للأمن الإلكتروني، والأستاذ الدكتور حميد مجول النعيمي مدير جامعة الشارقة. وأثناء كلمته الافتتاحية، أكّد سعادة يوسف الشيباني على دعم المركز المتواصل لهذا المختبر، وصرّح بأن نتائج أبحاثه العلمية سوف تنعكس قريباً على واقع حياتنا، وذلك في إطار سعي مدينة دبي لأن تكون سبّاقة في مجال التطور الرقمي وتنفيذ المبادرات النموذجية المتعلقة بإنترنت الأشياء.

ويتكون فريق عمل المختبر من الأستاذ الدكتور قاسم ناصر والدكتورة منار أبو طالب والدكتورة بشرى البلوشي، إضافة إلى فرق من الباحثين من طلبة الماجستير والدكتوراه ضمن برامج علمية وهندسية متخصصة. ومن جانبها أكدت الدكتورة بشرى البلوشي على أهمية دعم المجتمع العلمي وتمويل الأبحاث التطبيقية التي تخدم المؤسسات الحكومية وتسهم في توفير ابتكارات بحثية جديدة.

وتشكّل المنصة التفاعلية لاختبار أمن إنترنت الأشياء، التي يعمل على تطويرها الأستاذ الدكتور ناصر والدكتورة منار أبو طالب منذ العام 2016، واحدة من المشاريع البحثية الرئيسة للمختبر، حيث يوضح ملخص البحث كيف تقوم عملية تصديق الأجهزة الذكية وبناء الثقة بالبنية التحتية الأساسية بدور حيوي في تحقيق أهداف إنترنت الأشياء. فمن خلال منصة الاختبار، يستطيع الفريق فحص وسائل الأمان والخصوصية في إعدادات أجهزة إنترنت الأشياء عن طريق تجارب متخصصة مثل اختبار الاختراق والبحث عن نقاط الضعف.

وتسهم أعمال المختبر بدرجة كبيرة في تحقيق السلامة الشاملة لشبكة إنترنت الأشياء في دبي، التي من المقرر أن تشهد نمواً سريعاً لاسيما مع تطبيق تكنولوجيا الجيل الخامس في المستقبل القريب.

سعادة يوسف الشيباني، مدير عام مركز دبي للأمن الإلكتروني، ومعالي الأستاذ الدكتور حميد النعيمي، رئيس جامعة الشارقة، يفتتحان مختبر "بايت"، أحدث المختبرات في مجال أبحاث إنترنت الأشياء والذكاء الاصطناعي

مختبر أبحاث الأمن الإلكتروني في جامعة دبي

دشّن مركز دبي للأمن الإلكتروني بالتعاون مع جامعة دبي مختبراً لأبحاث الأمن الإلكتروني في أكتوبر 2018، ويختص المختبر بتوفير اختبارات بحثية غير مسبوقة بهدف تأمين كافة أنظمة التحكم التي تدير جميع الأجهزة المتصلة بالإنترنت في كل أنحاء المدينة.

وفي لقاء مع الأستاذة الدكتورة سميرة الملا، أحد أعضاء الفريق القيادي للمختبر، عن مهام فريق العمل، أوضحت أن الفريق قام بتحليل كافة البيانات الواردة من شبكة الإنترنت إلى شبكاته الخاصة ومن ثم عمل على توليد بيانات مفيدة تتضمن تقارير عن عناوين بروتوكول الإنترنت ذات المصادر المشبوهة.

وأشارت إلى أن الفريق يقوم بتحليل كافة البرامج الخبيثة كالفيروسات، إضافة إلى الكشف عن مصادر البرامج التي تحاول استهداف البنية التحتية الأساسية في المدينة. كما يعمل الفريق على دمج تقنية الذكاء الاصطناعي بالعمليات من خلال تقنية تعليم الآلة التي لديها القدرة على تحديد التهديدات في حركة البيانات على الشبكة.

> مركز دبي للأمن الإلكتروني يأتي في صدارة المؤسسات الحكومية بدولة الإمارات في مجال التعاون العلمي والبحثي

يُعد مختبر أبحاث الأمن الإلكتروني الأول من نوعه في المنطقة، وهو مختبر رائد في تطبيق تقنيات الذكاء الاصطناعي بإمكانيات مُعزّزة بهدف الكشف عن الأنشطة المشبوهة على الإنترنت وتقييمها، بما يسهم في حماية دبي من الهجمات التي تستهدف البنية التحتية للمدينة. ويغطي هذا المشروع الطموح عدة مجالات تشمل الشبكة المظلمة والبيانات الضخمة وتعلّم الآلة.

كما أكدت الملّا التزام مركز دبي للأمن الإلكتروني في إتاحة فرص تدريبية لطلاب الجامعات داخل المختبر، قائلة: "يحظى الطلاب بفرصة المساهمة بفعالية في المشاريع البحثية والمشاركة في تجارب علمية تتيح لهم التعلم والمساعدة في مثل هذه المشاريع وتوفير الدعم اللازم."

وأوضحت أن مركز دبي للأمن الإلكتروني يبحث دائماً عن خريجي الجامعات الموهوبين من أبناء الدولة، إذ يعد البرنامج التدريبي الخاص بالمختبر فرصة مثالية لاكتشاف قدرات الطلاب وإثراء معرفتهم وتعزيز مسيرتهم العلمية."

واختتمت الملا: "لقد أبدى الطلاب حماساً وشغفاً كبيرين بالانضمام إلى جامعة دبي بفضل مختبراتها المتطورة. فما يقوم به مركز دبي للأمن الإلكتروني هو مهمة فريدة من نوعها، ويحرص على بذل جهود حثيثة لتشجيع الجهات الحكومية على الاستثمار في الأبحاث العلمية التي تشكل خطوة مهمة من أجل تنمية قطاع حيوي في الدولة."

> يشجع مركز دبي للأمن الإلكتروني الجهات الحكومية على الاستثمار في أبحاث الأمن الإلكتروني وتشهد جامعة دبي إقبالاً كبيراً من الطلاب بفضل مختبرات الأمن الإلكتروني المتطورة التي تمتلكها

مختبر الأبحاث الأمنية المبتكر لمركز دبي للأمن الإلكتروني وجامعة دبي - الأستاذة الدكتورة سميرة الملا تشرف على أعمال الباحث محمد وائل. تم افتتاح المختبر في أكتوبر 2018.

تسديد المدفوعات بشكل آمن وذكي عبر الهاتف المتحرك

قطعت خدمات تسديد المدفوعات شوطاً كبيراً منذ أن كنا نسدد مدفوعاتنا باستخدام حزم من النقود.. حتى أصبحنا اليوم نقوم بدفع ثمن مشترياتنا إلكترونياً وبلمسة زر ولغاية التسوق عبر الإنترنت وتحويل الأموال والودائع وغير ذلك الكثير بمجرد النقر أو الضغط على هاتفنا الذكي. وتتيح تكنولوجيا الخدمات المالية التي يطلق عليها مصطلح "فينتك" تقنية سهلة للغاية، ولكنها في ذات الوقت تأتي بتحديات أمنية، لذا دعنا نساعدك على تنفيذ معاملاتك المصرفية وتسديد مدفوعاتك عبر الهاتف الذكي بشكل آمن من خلال هذه النصائح البسيطة:

استخدم منصات الدفع الآمنة

إن منصات الدفع الإلكتروني الموثوقة لا تحتفظ بتفاصيل بطاقتك الائتمانية بعد المعاملة. أما تطبيقات الدفع الاحتيالية فهي عادةً ما تكون مصممة لجمع معلوماتك المالية واستخدامها، لذا توخَ الحذر الزائد بشأن استخدام تطبيقات الطرف الثالث.

أغلق هاتفك المفقود أو المسروق عن بُعد

احرص على تفعيل خدمة "العثور على الآيفون" لهواتف آيفون أو "العثور على الجهاز" لهواتف الأندرويد، للعثور على جهازك ومسحه عن بعد إذا فُقد أو سُرق. حتى إذا لم تسترد هاتفك أبداً فعلى الأقل ستبقى معلوماتك في أمان.

اجعل كلمة السر قوية فهي درعك الآمن

اضبط هاتفك على وضعية الإغلاق التلقائي واختر كلمة سر قوية لحماية هاتفك والمعلومات المخزنة بداخله. احرص على استخدام كل مزايا الأمان المتقدمة تقنياً التي يوفرها هاتفك الذكي، كنظام بصمة الإصبع أو التعرف على الوجه.

احذر من شبكات الـ"واي فاي" العامة

لا ترسل أي معلومات حساسة عبر شبكات الـ"واي فاي" العامة أبداً، فشبكات الإنترنت المفتوحة في مراكز التسوق والمقاهي وغيرها من الأماكن العامة متاحة لكل من يتصل بها، أي أن بياناتك تصبح أكثر عرضة للاستغلال عند إجراء عمليات الشراء أو تحويل الأموال إلكترونياً عبر شبكات الـ"واي فاي" العامة.

لا تنقر على رسائل إلكترونية للوصول إلى حساباتك المصرفية

الضغط على روابط البريد الإلكتروني أو الرسائل النصية ليس آمناً، فرسائل التصيّد الاحتيالي مصممة لتبدو كأنها قادمة مباشرة من مصرفك، لكن النقر عليها سيأخذك إلى موقع وهمي يسرق معلومات الدخول التي توفرها أنت بحسن نية. عليك أيضاً ألا تكشف عن أرقامك أو كلمات السر الخاصة بك أبداً عند الرد على رسالة إلكترونية أو رسالة نصية قصيرة، فمصرفك الحقيقي لن يطلب مثل هذه البيانات منك أبداً.

قم بتنزيل التطبيق الخاص بمصرفك

إن تنزيل التطبيق الذي صممه مصرفك خصيصاً للهواتف الذكية هو في الواقع أكثر أماناً من استخدام المتصفّح. احرص على تحديث البرمجيات على هاتفك بانتظام، فهذا سيحمي نظامك من أي برمجيات خبيثة جديدة أو أعطال برمجية.

استخدم خاصية التحكم بخطوتين

ينبغي أن تمنح معاملاتك المصرفية حماية مزدوجة عن طريق الجمع بين كلمة السر وإدخال رقم تعريف شخصي يتم استخدامه لمرة واحدة حيث يقوم النظام بإرساله إلى رقم هاتفك المسجل، بحيث إنه حتى إذا عرف أحدهم كلمة السر فلن تتم الموافقة على عملية الدفع من دون رقم التعريف الشخصي.

حافظ على سلامة هاتفك!

بالطبع ليس هناك من يهمل هاتفه عمداً، ولكن بعد أن أصبحت هواتفنا أكثر بكثير من مجرد أجهزة "لاسلكية" ذكية أصبح ضرورياً أن نوليها مزيداً من العناية. احتفظ بهاتفك مغلقاً وأبقه معك طوال الوقت ولا تعره لمن لا تعرفه أو تثق به.

مركز دبي للأمن الإلكتروني يقدم منحة الابتكار في مجال أبحاث الأمن الإلكتروني

أعلن مركز دبي للأمن الإلكتروني في فبراير الماضي عن الفائزين بجائزة "الابتكار البحثي للأمن الإلكتروني"، وتم تكريم الفريقين الفائزين، وهما "جامعة خليفة" و"جامعة الشارقة"، بالجائزة التي تبلغ قيمتها الإجمالية 700 ألف درهم وتهدف لدعم المعرفة والابتكار.

وحضر حفل توزيع الجائزة المرموقة نخبة من رؤساء الجامعات والباحثين والخبراء في مجال الأمن الإلكتروني، وألقى الدكتور مروان الزرعوني، مدير إدارة خدمات المعلومات في مركز دبي للأمن الإلكتروني كلمة ترحيبية أكد فيها على أهمية الابتكار، مشيراً إلى أنه يُعد البنية الأساسية للتطوّر الاجتماعي والاقتصادي لإمارة دبي، ودولة الإمارات العربية المتحدة، كما تطرق إلى آليات تنفيذ استراتيجيات الابتكار وأطر العمل في مركز دبي للأمن الإلكتروني على وجه التحديد.

أشار الزرعوني إلى "استراتيجية دبي للأمن الإلكتروني" التي أطلقها صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة، رئيس مجلس الوزراء، حاكم دبي، رعاه الله، في العام 2017، ضمن رؤية سموه في أن تكون دبي رائدة عالمياً في مجالات الابتكار والسلامة والأمن، معتبراً أن للبحث والتطوير دوراً حيوياً في دفع عجلة الابتكار. وعبّر الزرعوني عن أمله في أن يكون هذا التكريم حافزاً ووسيلة لتوسيع أفق الباحثين فيما يتعلق بمجال الأمن الإلكتروني وبأن هذه الجائزة تأتي كمبادرة تهدف إلى جعل المركز ركناً استراتيجياً حاضناً للابتكار.

يذكر أن أكثر من 70 باحثاً وطالباً من أكثر من 20 جامعة وطنية ودولية تنافسوا على جوائز المنحة، واجتاز المرحلة الأولى 14 مشروعاً بحثياً ممتازاً.

وفي سياق حديثه عن جائزة "الابتكار البحثي للأمن الإلكتروني" أعرب الدكتور مروان الزرعوني عن تقديره لجميع الباحثين والطلبة المشاركين قائلاً: "يقدر مركز دبي للأمن الإلكتروني الجهود الهائلة التي كرسها الباحثون للمسابقة، ويسرنا تهنئة الفريقين الفائزين، وكلنا ثقة بأن تساهم هذه الجائزة بصفتها مبادرة أولية من مركز دبي للأمن الإلكتروني في حماية ثروة دبي الرقمية، وهذا بدوره يعزز رؤية قيادتنا الحكيمة بجعل دبي أكثر المدن أماناً في العالم."

مشروعات بحثية غير مسبوقة

فتحت المنحة أبوابها أمام مشروعات كافة الباحثين في مؤسسات التعليم العالي المعتمدة في دولة الإمارات العربية المتحدة والمؤسسات الدولية، ومن أبرزها التحديات في مجال الأمن الإلكتروني والتحديات الإلكترونية.

وبحث الفريق البحثي الفائز من جامعة خليفة موضوع "أجهزة إنترنت الأشياء الآمنة بتكنولوجيا كفاءة الطاقة للمدن الذكية"، أما المشروع البحثي الخاص بالفريق الفائز الآخر وهو جامعة الشارقة فيهدف إلى تصميم "مُولّد بت" (Bit Generator) عشوائي حقيقي فائق السرعة قائم على البلازما الميكرونية للتشفير في الوقت الحقيقي."

إضافة إلى ذلك شملت المشروعات الأخرى مجالات متنوعة مرتبطة بالأمن الإلكتروني كالعلوم الجنائية الرقمية واستخبارات التهديدات الرقمية وأمن الهاتف المتحرك والبيانات الضخمة والبلوك تشين وأمن المركبات ذاتية القيادة.

تبنّي الابتكارات في مجال الأمن الإلكتروني خلال مؤتمر أوبسدي

شارك مركز دبي للأمن الإلكتروني في تنظيم مؤتمر OPCDE التقني رفيع المستوى بحضور نخبة من أبرز الخبراء والباحثين في مجال الأمن الإلكتروني على مستوى العالم، وذلك التزاماً منه بكبح تهديدات الأمن الإلكتروني.

تم تنظيم نسخة العام 2019 بالتعاون مع شركة "كوم أي للتكنولوجيا"، وشملت قائمة المتحدثين خبراء من شركات "غوغل" و"مايكروسوفت" و"فاير آي"، الذين شاركوا بخبراتهم حول الأبحاث والتهديدات الرقمية والتوجهات في مجال تأمين العالم الرقمي، ويشير اسم "OPCDE" إلى مصطلح "شفرة العملية" الذي يُستخدم ضمن أوامر الحاسوب.

وفي كلمته الافتتاحية خلال المؤتمر، قال الدكتور مروان الزرعوني، مدير إدارة خدمات المعلومات في مركز دبي للأمن الإلكتروني: "إن هذا المؤتمر يدعم جهود التوعية بالمخاطر وبالدور المهم للأمن في العصر الرقمي في ظل الطلب المتزايد على التعليم والتدريب في مجال الفضاء الرقمي."

ومن جانبه قال مات سويش مؤسس مؤتمر OPCDE إن المؤتمر يشكّل إضافة مميزة وناجحة في بيئة دبي المحلية، ويعزز نمو المواهب المحلية بما يجعل دبي مركزاً عالمياً للابتكارات في مجال الأمن الإلكتروني.

وشدد الزرعوني على أهمية تمكين الكوادر الشابة في مجال الأمن الرقمي.. إن مشاركة مركز دبي للأمن الإلكتروني في فعاليات من هذا النوع تدعم جهود حكومة دبي وتسهم في تحقيق مبادراتنا التي تستهدف التغلب على تحديات الأمن الإلكتروني وبناء فضاء رقمي آمن.

أحدث التطورات في مجال الأمن الإلكتروني في معرض ومؤتمر الخليج لأمن المعلومات " جيسيك" 2019

للعام الثاني على التوالي شارك مركز دبي للأمن الإلكتروني في معرض ومؤتمر الخليج لأمن المعلومات "جيسيك" 2019، الذي أقيم في مركز دبي التجاري العالمي في أبريل الماضي.

ويعد معرض "جيسيك" أكبر الفعاليات السنوية في مجال أمن المعلومات في الشرق الأوسط، حيث يستقطب خبراء عالميين في مجال الأمن الإلكتروني و170 جهة عارضة من 86 دولة وأكثر من 12 ألف زائر. وفي هذا العام ألقى مركز دبي للأمن الإلكتروني الضوء على أحدث التطورات والممارسات في مجال الأمن الإلكتروني، إضافة إلى المبادرات المسخرة لجعل فضاء دبي الرقمي الأكثر أمناً على مستوى العالم.

وضمن مساهمات مركز دبي للأمن الإلكتروني في الفعالية، عرض المركز شاشة تفاعلية بكلمة مرور سرية بهدف اختبار مناعة الأمن الإلكتروني للأفراد من خلال الإشارة إلى المدة المتوقعة لقيام برنامج الحاسوب باختراق كلمة السر، والتي تراوحت من ثوان معدودة إلى بضعة آلاف عام.

وبالحديث عن الهجمات الإلكترونية، قال عامر شرف مدير إدارة التعاون ودعم التحديات الإلكترونية في مركز دبي للأمن الإلكتروني: "إن الهجمات تزداد تعقيداً وتخريباً، وبالتالي تمثل خطراً على نمو الاقتصاد الرقمي والبنى التحتية الذكية، وفي كل عام في معرض "جيسيك" نلقي الضوء على أحدث الممارسات في مجال الأمن الإلكتروني، ونربط بينها وبين التقنيات الناشئة لزيادة الأمان وبالتالي ترسيخ الثقة بفضائنا الإلكتروني، وأولويتنا الرئيسة هي حماية دبي من التحديات الإلكترونية من خلال تأمين الخصوصية والبيانات، وحماية ثروة دبي الرقمية."

إطلاق مبادرة دبي للأبحاث والدراسات السيبرانية

أطلق مركز دبي للأمن الإلكتروني مبادرة دبي للأبحاث والدراسات السيبرانية التي تُعدّ الأولى من نوعها في منطقة الشرق الأوسط كمنصة تفاعلية للعصف الذهني والمناقشات بين المركز وكافة الهيئات والمؤسسات المشاركة لوضع حلول فعّالة لمواجهة الهجمات الإلكترونية الحالية والمستقبلية.

تم تدشين هذه المنصة الرائدة في دورتها الأولى في أكتوبر 2019 لتكون بمثابة نقطة انطلاق للاجتماعات الدورية والمناقشات الجماعية رفيعة المستوى بالتعاون مع المؤسسات والدوائر الحكومية في إمارة دبي. وأوضح جاسم محمد، رئيس قسم العمليات الأمنية في مركز دبي للأمن الإلكتروني: "تشمل أولويات المنصة مواجهة المخاطر والتحديات الإلكترونية الحالية والمستقبلية، والمساهمة في تطوير أطر وسياسات استباقية للأمن الرقمي لمدينة دبي."

وستقوم المنصة في نهاية كل دورة بإعداد تقرير شامل ومفصّل عن نتائج كافة البحوث والدراسات العلمية التي من شأنها تطوير استراتيجيات ووسائل الأمن الإلكتروني للهيئات الحكومية والخاصة على حد سواء، وذلك بناءً على تقارير التوصيات المُجمّعة من نتائج الأبحاث والدراسات.

وأكّد جاسم محمد أن مبادرة دبي للأبحاث والدراسات السيبرانية تندرج ضمن تفعيل أهم المحاور الاستراتيجية لمركز دبي للأمن الإلكتروني التي تشتمل على تأسيس شراكات فعّالة مع كافة الهيئات والمؤسسات المحلية في دبي لمواجهة التهديدات والمخاطر في مجال الفضاء الرقمي.

وأضاف جاسم أن مثل هذه المبادرات تسهم في تحقيق رؤية حكومة دبي في تطوير وتنفيذ السياسات والمبادرات الهادفة إلى التعامل مع تحديات الأمن الإلكتروني وبناء فضاء رقمي آمن ومرن لمدينة دبي ودولة الإمارات العربية المتحدة بكافة قطاعاتها الحكومية والخاصة.

تقنيات الذكاء الاصطناعي تعيد تعريف الأمن الإلكتروني

الذكاء الاصطناعي يعزز إمكانيات وضوابط خبراء الأمن الإلكتروني بطرق احترافية مبتكرة ومذهلة

يضع مركز دبي للأمن الإلكتروني الابتكار والتطوير على قائمة أولوياته لترسيخ مكانة إمارة دبي كمدينة رائدة عالمياً في مجال الأمن الرقمي، وتحقيق رؤية صاحب السمو الشيخ محمد بن راشد آل مكتوم وضمان توفير فضاء رقمي آمن والارتقاء بمستويات الابتكار إلى آفاق جديدة.

وفي حديث سعادة يوسف الشيباني المدير العام لمركز دبي للأمن الإلكتروني عن أهمية تعزيز قدرات الابتكار في مجال الأمن الإلكتروني لمجلة "إشارات" قال: "إن رؤية قيادتنا الرشيدة لا تستشرف المستقبل القريب فحسب، بل تحرص على تطوير خطط استراتيجية تلبي احتياجات دبي وترسخ مكانتها بين مدن العالم."

وأضاف: "حقّقت تقنيات الذكاء الاصطناعي قفزات هائلة حتى وصل تأثيرها إلى قطاع الأمن الإلكتروني الذي أصبح أكثر اعتماداً على تطبيقات تعلم الآلة والحوسبة المعرفية وابتكارات الذكاء الاصطناعي الأخرى وتوظيفها بما يدعم قدرة عمليات الأمن البشري وتمكينهم من الاستجابة للتهديدات بشكل أسرع وأكثر كفاءة من أي وقت مضى."

التعلم – تستمد تقنية الذكاء الاصطناعي قوّتها من تريليونات الوحدات من البيانات التي تنشأ من مجموعة واسعة من المصادر، وتكتسب قوة أكبر مع كل تجربة جديدة. إذ تعتمد تقنية الذكاء الاصطناعي على تطبيقات تعلم الآلة والتعلم العميق لبناء قاعدة معرفية هائلة حول التهديدات الإلكترونية ومن ثم تطوير استجابات فعالة بسرعة فائقة لمثل هذه التهديدات.

الاستدلال – بعد توظيف المعارف والمعلومات التي تم جمعها، يتمكن الذكاء الاصطناعي من تحليل التهديدات التي تأتي في صورة برامج خبيثة أو ملفات ضارة أو أي نشاط مشبوه والتعرّف عليه في غضون ثوانٍ. تشكّل هذه السرعة والاتقان أحد العوامل الحيوية لضمان الحماية في عالم يقوم فيه المخترقون بتوظيف أحدث التقنيات لشن هجماتهم الإلكترونية.

تعزيز الأداء – توفر الآلات المعرفية دعماً مهماً لفرق الأمن الإلكتروني وتعزيز أدوارهم من خلال إجراء البحث المتواصل وتحليل مليارات سجلات البيانات. ومن خلال التصنيف المستمر والكشف عن الأنماط والتنبؤ بالهجمات قبل حدوثها وتزويد الأفراد بمعلومات دقيقة، يعمل الذكاء الاصطناعي على اختزال الوقت الذي يحتاجه المتخصصون لاتخاذ قرارات حاسمة والاستجابة لظروف التهديدات.

الذكاء الاصطناعي يُعزّز الذكاء البشري للحد من التهديدات الأمنية

تقنية تعلم الآلة تعمل على تمكين الأنظمة الحاسوبية من إنشاء خوارزميات بناءً على البيانات التي تتلقاها، حتى تتمكن من التعرّف على الأنماط سريعاً وكذلك التجاوزات التي قد تشير إلى وجود مشكلة. وتقوم الحوسبة المعرفية بوصف تعلم الآلة الذي يوظف البيانات لبناء أنظمة تحاكي أنماط التفكير البشري. وبدلاً من برمجته بالمدخلات والمخرجات، يكتسب هذا الذكاء الاصطناعي "فهماً" أفضل مع كل تجربة تفاعلية جديدة في بيئته.

ويشكل الأمن المعرفي قفزة كبيرة في مجال الأمن الإلكتروني نظراً لأنه يجمع بين أفضل ما يقدمه الذكاء الاصطناعي والذكاء البشري؛ حيث تعتمد الآلات على قاعدتها المعرفية الهائلة من خلال توظيف تقنية التعلم العميق، ومن ثم تزداد ذكاءً وكفاءة في اكتشاف وتحليل التهديدات الإلكترونية بشكل استباقي، مما يسهل على محللي الأمن الإلكتروني اتخاذ القرارات والإجراءات. لذلك، يمكن استخدام الذكاء الاصطناعي لأداء مهام رتيبة للغاية ومستهلكة للوقت بسرعة ودقة تفوق إمكانيات البشر.

في الحقيقة، هذا النوع من المهام هو الأنسب لتقنيات الذكاء الاصطناعي، فالحواسيب لا تكل ولا تمل، إذ إن قدرتها المذهلة على تحليل البيانات على نطاق واسع ومهاراتها في اكتشاف الحالات المشبوهة هي قدرات قابلة للتطور المستمر بما يعزز من الجهود البشرية وتحسين الأمن الإلكتروني للمؤسسات.

سعادة يوسف الشيباني، مدير عام مركز دبي للأمن الإلكتروني والرئيس الشرفي لقمة معهد مهندسي الكهرباء والإلكترونيات للذكاء الإلكتروني

تطبيقات الذكاء الاصطناعي

يعتبر البحث عن التهديدات الإلكترونية أحد المجالات التي يتم توظيف الذكاء الاصطناعي فيها بشكل فعال، لأنه يتضمن البحث عن كميات هائلة من البيانات لتحديد أي نقاط ضعف أو مخاطر أو تهديدات تواجه البنية التحتية لتكنولوجيا المعلومات في المؤسسات. ويكاد يكون من المستحيل أن يقوم الإنسان بتنفيذ خدمة الأمن الإلكتروني الوقائي بنفس التركيز والسرعة والدقة والتناسق كالآلة المعرفية.

وبالإضافة إلى هذه التطبيقات، يتم توظيف تقنيات الذكاء الاصطناعي وتعلم الآلة لتطوير إمكانيات الأمن الإلكتروني بطرق مبتكرة أخرى أيضاً ومنها ما يلي:

الحماية البيومترية

تم استخدام المصادقة البيومترية أو الحيوية، كالتعرّف على بصمة الوجه أو الإصبع، كبديل عصري للمصادقة بكلمة المرور التقليدية بعد أن أثبتت تعرّضها المستمر للاختراق. وأوضحت مجلة "فوربس" والخبراء في مجال الذكاء الاصطناعي أنه بما أن الأنظمة ليست مؤمّنة كلياً، تم تطوير برنامج بيومتري لتسجيل الدخول إلى هذه الأنظمة لضمان حمايتها. وتعمل هذه التقنية على معالجة ملامح الوجه من خلال التعرّف على الأنماط والارتباطات التي غالباً ما يكون تزييفها شبه مستحيل. كما تعمل التقنية في ظروف إضاءة مختلفة.

الحماية من رسائل التصيّد الاحتيالي

أصبحت رسائل التصيّد الاحتيالي من الأساليب الأكثر شيوعاً للهجمات الإلكترونية، حيث نجد أن من بين كل مئة رسالة عادية هناك رسالة تصيد احتيالي واحدة (zdnet.com). وباستخدام تقنية الذكاء الاصطناعي يُمكن مسح الشبكات واكتشاف آلاف الرسائل الاحتيالية النشطة وحظرها في غضون دقائق. كما يمكن لنظام تعلم الآلة التمييز بين المواقع الإلكترونية الأصلية والمزيفة ليوفر بذلك الحماية السريعة على كافة المستويات. وهناك أنظمة مضادة للتصيد الاحتيالي تقوم بعملية "فحص الارتباطات العميقة" من خلال محاكاة النقرات على كافة الارتباطات في رسالة بريد إلكتروني وفحص الصفحات المنشأة بحثاً عن أي أنشطة خبيثة.

التحليل السلوكي

تستطيع خوارزميات تعلم الآلة دراسة الأنماط في سلوكك كمستخدم من خلال تحليل طريقتك المعتادة في استخدام جهازك، وأوقات تسجيل الدخول المعتادة والمواقع الإلكترونية التي تقوم بزيارتها، وحتى أنماط الكتابة أو التمرير على الشاشة. وإذا كشف نظام الذكاء الاصطناعي عن أي سلوك مختلف عن الأنماط القياسية الخاصة بك، كالكتابة السريعة أو الارتفاع المفاجئ في تنزيل الوثائق، سيقوم بتنبيهك على الفور أو قد يحظر المستخدم إذا كان السلوك المتبع يشير بوضوح إلى عملية قرصنة.

تعلُّم اللغات الطبيعية

تشكل "معالجة اللغات الطبيعية" إحدى أبرز التطورات المعززة بالذكاء الاصطناعي، فمن خلالها تستطيع الأنظمة جمع البيانات عن طريق مسح المقالات والمحادثات وأخبار شبكة الإنترنت المظلمة لبناء قاعدة معرفية، ما يمكنها من التنبؤ بالهجمات الإلكترونية وحظرها. هذه المعالجة تمكّن عمليات الأمن الإلكتروني من تصدي المخاطر ومواكبة أحدث

التقنيات المستخدمة في الجرائم الإلكترونية ومن ثم إعداد خطط استراتيجية أمنية فعالة. كما تُستخدم معالجة اللغات الطبيعية في حماية البريد الإلكتروني من خلال التحقق من اختيار الكلمات وقواعد اللغة والهجاء وما إذا كانت مصدراً مشتبهاً به أم لا.

التحليل الآلي للشبكات

تتدفق البيانات عبر الشبكات بكميات هائلة وبسرعة تفوق قدرة الإنسان على تحليلها ومراقبتها، وبما أن معظم البرمجيات الخبيثة والهجمات الإلكترونية تشن ضد الشبكات، أصبح حتمياً تأمين هذه الشبكات من خلال عمليات التحليل المستمرة والسريعة والدقيقة. تستخدم أنظمة الذكاء الاصطناعي الخوارزميات لمطابقة الكلمات الرئيسة والكشف عن البيانات التي تسجل اختلافاً حتى ولو كان طفيفاً عن البيانات الطبيعية. هذه الخدمة تمنح محللي الأمن الإلكتروني الوقت الكافي لتوجيه استجابات سريعة عندما تُحذر أنظمة الذكاء الاصطناعي بوجود أي تهديدات.

القيود وفرص التقدّم

تتطلب الآلات المعززة بالذكاء الاصطناعي موارد ضخمة مثل أداء الحاسوب ومجموعات البيانات الدقيقة. كما يتطلب تصميم وصيانة مثل هذه الأنظمة ودمجها في التطبيقات الرئيسية بعض الوقت، وهناك بالفعل قائمة من التحديات والقيود التي يعمل خبراء الأمن الإلكتروني على حلّها، لكنها مسألة وقت فقط حتى يصبح الذكاء الاصطناعي حلاً مستقلاً لحماية المعلومات الرقمية. وأوضح الشيباني أن الذكاء الاصطناعي الآن يعمل على دعم وتحسين أداء المهنيين التقليديين، ويحقق تطوراً فائق السرعة من خلال عمليات البحث والتطوير. كما يتم دمج الذكاء الاصطناعي مع التقنيات المتطوّرة الأخرى، كتقنية البلوك تشين، لضمان بناء بروتوكولات أمنية بإمكانيات متفوقة تجعلها أداة الحماية الحيوية في عالم الأمن الإلكتروني.

مركز دبي للأمن الإلكتروني يدعم الأبحاث والشراكات في مجال الذكاء الاصطناعي

يضع مركز دبي للأمن الإلكتروني التقنيات المبتكرة والتطوير في مقدمة أولوياته لترسيخ مكانة دبي كمدينة رائدة عالمياً في مجال الأمن الرقمي، وأكد الشيباني حرص المركز على تحقيق هذه الرسالة من خلال بناء الشراكات المثمرة مع المؤسسات العلمية والأكاديمية على المستوى المحلي والدولي من أجل المساهمة في أعمال البحث والتطوير في هذا المجال بما يدعم أهداف استراتيجية دبي للأمن الإلكتروني ومحاور الريادة التكنولوجية الأخرى.

وهذا العام كان "الذكاء الاصطناعي ومستقبل الأمن الإلكتروني" عنواناً لقمة معهد مهندسي الكهرباء والإلكترونيات (فرع الإمارات) للذكاء الإلكتروني التي نظمها مركز دبي للأمن الإلكتروني بالشراكة مع هيئة تنظيم الاتصالات (TRA) ومعهد مهندسي الكهرباء والإلكترونيات (فرع الإمارات) للمرة الثالثة على التوالي يوم 14 نوفمبر في دبي.

يعتبر معهد مهندسي الكهرباء والإلكترونيات أكبر منظمة تجمع المهنيين التقنيين في مجال التطوير التكنولوجي على مستوى العالم، وهي تتألف من نخبة من المهندسين والعلماء ومطوري البرمجيات وخبراء تكنولوجيا المعلومات وغيرهم من الكوادر المهنية. ويُعد معهد مهندسي الكهرباء والإلكترونيات (فرع الإمارات) الذي تأسس في العام 1987 ممثل المعهد في دولة الإمارات.

وأوضح سعادة يوسف الشيباني الرئيس الشرفي لقمة معهد مهندسي الكهرباء والإلكترونيات (فرع الإمارات) للذكاء الإلكتروني أن القمة تمثل خطوة مهمة نحو تحقيق خطة دبي الاستراتيجية للأمن الإلكتروني التي تهدف إلى تشجيع الابتكار والبحث والتطوير في مجال الأمن الرقمي وبناء فضاء رقمي يتسم بالحرية والعدالة والأمان في دبي، وتطبيق هذه الرؤية على المستوى العالمي.

وأضاف: "نحن في مركز دبي للأمن الإلكتروني يسرّنا عقد هذه الشراكة مع معهد مهندسي الكهرباء والإلكترونيات (فرع الإمارات) الذي يعد واحداً من أكبر المؤسسات المهنية التقنية على مستوى العالم. وهدفنا هو توفير منصة تتيح للخبراء والباحثين في مجال الأمن الإلكتروني التواصل من خلال مناقشات مثمرة وتبادل الأفكار وبحث أهم تطبيقات تقنية الذكاء الاصطناعي في مجال أمن المعلومات."

> "هدفنا توفير منصة تتيح للخبراء والباحثين في مجال الأمن الإلكتروني التواصل وتبادل الأفكار وبحث أهم تطبيقات تقنية الذكاء الاصطناعي في مجال أمن المعلومات"

اختبارات الاختراق..
لحماية فضاء دبي الرقمي

تسلك إدارة الاستجابة للأزمات في مركز دبي للأمن الإلكتروني نهجاً استراتيجياً ذكياً يستهدف تجنب الهجمات الإلكترونية الإجرامية على أنظمة حواسيب الحكومة، وذلك من خلال القيام بعملية تجربة قابلية الاختراق مصرّح بها على الأنظمة.

إن هذا النظام يُعرف باختبار قابلية الاختراق، ويستطيع من خلاله خبراء مركز دبي للأمن الإلكتروني الكشف عن نقاط الضعف في أنظمة الحواسيب وإصلاحها.

تخيل أنك تُعرّض نفسك للفيروسات عمداً، فقط للتحقق من قوة حصانتك في وجه المرض، أو في حال مرضك، للتأكد من أسرع الطرق لاستعادة صحتك! ببساطة هذا هو ما تشمله اختبارات الاختراق، غير أن الفيروسات هنا رقمية، ويتم إطلاقها ضد أنظمة وشبكات الحواسيب.

اختبار الاختراق ويعرف في مجال الأمن الإلكتروني بمصطلح (penetration testing) هو نوع من الهجوم المحاكي المتعمّد على نظام حاسوب بهدف تقييم مستواه الأمني، ومن خلال الاختبار يستطيع خبراء الأمن الإلكتروني إجراء تقييم كامل للخطر يحدد نقاط الضعف المحتملة في النظام، كما يسلّط الضوء أيضاً على مواضع القوة فيه.

أحمد الحسين، نائب مدير إدارة الاستجابة للأزمات في مركز دبي للأمن الإلكتروني

حراسة احترافية للبنية التحتية الإلكترونية للحكومة

صرّح أحمد الحسين نائب مدير إدارة الاستجابة للأزمات في مركز دبي للأمن الإلكتروني بأن هدف تشكيل الفريق هو تقييم وضمان الأمن المستمر لكافة الأنظمة الحكومية المتصلة بالتقنية الرقمية الإلكترونية المتشابكة.

وأضاف قائلاً إنه: "من خلال عمل فريق الاستجابة للأزمات، يقدّم مركز دبي للأمن الإلكتروني خدمة تشمل اختبارات الاختراق لتطبيقات الهاتف المتحرك والإنترنت والبنى التحتية للشبكات الداخلية."

وأوضح: "مع تزايد عدد الأنظمة الرقمية في الحكومة نشأت حاجة ماسة إلى خدمة توفر اختبارات الاختراق، وتقوم تلك الخدمة بقياس فاعلية الإجراءات الأمنية المطبقة في الأنظمة المذكورة، ويوفر مركز دبي للأمن الإلكتروني، من خلال إدارة الاستجابة للأزمات، هذه الخدمة الحيوية إلى كافة الهيئات الحكومية، وذلك للتأكد من أن أنظمتها الحاسوبية وشبكاتها وتطبيقاتها عبر الإنترنت والهاتف المتحرك تتمتع كلها بمستوى تأمين احترافي." وأشار الحسين إلى أن إدارته تساعد هذه الهيئات الحكومية على تأمين بنيتها التحتية الحيوية، بما يعزز من رؤية المركز بجعل دبي المدينة الأكثر أماناً إلكترونياً في العالم.

وأضاف الحسين: "إن عملية اختبار الاختراق تتضمن تقييم الإجراءات والآليات الأمنية في الأنظمة المستهدفة، ويتم ذلك على يد فريق الاستجابة للأزمات المدرّب تدريباً فائقاً والمزوّد بمعرفة عميقة حول اكتشاف وتقييم أية نقاط ضعف وإدارة تطبيقات برامج الهندسة العكسية ومراجعة الشفرة المصدرية الخاصة بالتطبيق."

الاختراق الأخلاقي

لعلك تتساءل الآن عن الأساس الذي يقوم عليه اختبار الاختراق، والواقع أن هذا النهج الأمني يُعرف أحياناً بالاختراق الأخلاقي، لأنه اختراق يتم التصريح به لأغراض هادفة، حيث يلعب المُختبِر

تتألف عملية اختبار الاختراق من خطوات دقيقة تشمل الاستطلاع، المسح، الاستغلال، التحليل والتقرير:

1. **الاستطلاع**
يتم تحديد نطاق التقييم، ويجمع المُختبِر المعلومات عن النظام المستهدف.

2. **المسح**
تُستخدم أدوات مسح متخصصة

3. **الاستغلال**
عند اكتشاف أي عيوب أو مواطن ضعف يتم استغلالها واختراقها لتحديد مدى الاختراق الممكن.

4. **التحليل**
يحلل المُختبِر العيب ويحصل على البيانات، أو يُدخل تغييرات معينة على النظام يتم استخدامها كدليل على الاختراق.

5. **التقرير**
يتم تقديم تقرير شامل يحتوي على نتائج الاختبار الكاملة وعلى الأدلة الداعمة لها، إضافة إلى الحلول، أكانت حلولاً موصى بها أم معالجة متكاملة.

دور المخترق ويحاكي الهجمة الحقيقية، يبحث فيها عن طرق يخترق بها الطبقات الأمنية ويغزو الشبكة أو الموقع أو التطبيق، وإذا نجح في ذلك فهذا يعني أن المخترقين الحقيقيين قد ينجحون أيضاً.

وإذا نجح المُختبِر في الاختراق، فسيوفر ذلك صورة واضحة عن أماكن العيوب والضعف في الأمن الإلكتروني للنظام في وقت الاختبار، وبهذه المعرفة يمكن تقوية نقاط الضعف الأمنية التي تم اكتشافها، مما يؤدي إلى تعزيز أمن النظام.

وأوضح فيصل عبد العزيز، نائب مدير إدارة عمليات أنظمة الأمن في مركز دبي للأمن الإلكتروني، أن المخترقين لا يزالون يكتشفون طرقاً جديدة لاختراق أنظمة الحكومات والشركات والأفراد وجميعها متشابكة إلكترونياً، مما يلزم القيام بإجراء اختبارات الاختراق بانتظام من قِبل كوادر متخصصة وخبراء الأمن الإلكتروني الذين حصلوا على تدريبات خاصة في اليقظة المستمرة لأية تقنيات جديدة يستغلها القراصنة، وبذلك يمكنهم التدخل بسرعة لتحديث دفاعات الشبكة إذا لزم الأمر.

فيصل عبد العزيز، نائب مدير إدارة عمليات أنظمة الأمن في مركز دبي للأمن الإلكتروني

وبوجه عام، فإن اختبار الاختراق يتألف من عمليات تسير خطوة بخطوة بدءاً من الاستطلاع فالمسح ثم الاستغلال والتحليل وأخيراً تقديم التقارير.

نهج متعدد الجوانب

هناك طرق ومناهج مختلفة لاختبار الاختراق يمكن تطبيقها لضمان التقييم المتكامل للمخاطر:

اختبار الصندوق الأبيض

يمتلك مُختبِر الاختراق في هذا الاختبار المعرفة الكاملة للبنية الأساسية لتكنولوجيا المعلومات بما في ذلك عناوين بروتوكول الإنترنت وتكوين النظام وإجراءات الاعتماد الأخرى. ويشمل اختبار الصندوق الأبيض المكثف تحليلاً متعمقاً للعمليات والأنظمة لتقييم أمن جميع التقنيات الأساسية.

اختبار الصندوق الأسود

يتضمن هذا الاختبار تقمص المُختبِر لدور المخترق الحقيقي للتحقق من البنية الأساسية لتكنولوجيا المعلومات باستخدام الحد الأدنى من المعرفة المسبقة، حيث يستخدم كل وسائل تقنيات الاختراق الحديثة لمحاولة الوصول إلى الشبكة والأنظمة، حتى يستطيع توفير تقييم أمني كامل واتخاذ خطوات محددة لتصحيح نقاط الضعف ومنع إمكانية حدوث اختراقات عدائية.

اختبار الصندوق الرمادي

اختبار الصندوق الرمادي هو مزيج من الاختبارين السابقين، ويتضمن مشاركة معرفة محددة حول البنية الأساسية والأنظمة مع المُختبِر.

الهندسة الاجتماعية

ربما تعرّض الكثيرون منا لنوع واحد على الأقل من محاولات اختراق الهندسة الاجتماعية - ونأمل ألا يكون قد وقع أحد ضحية لهذا النوع من الاستغلال - إذ إن هذا النهج يتضمن مراسلات احتيالية لمحاولة اختراق الأنظمة. وتُعدّ رسائل التصيّد الاحتيالي وسيلة شائعة لهذا الاحتيال، وتتضمن استخدام رسائل البريد الإلكتروني أو الرسائل النصية القصيرة ذات المحتوى المزيف الذي يشجع الضحايا على الضغط على روابط مشبوهة. وبمجرد الضغط عليها يقوم المستخدم بتنزيل برنامج خبيث أو يكشف عن بيانات شخصية قيّمة أو بيانات الشركة، ليفتح بذلك الباب أمام عمليات الابتزاز والاستغلال. ويقرر فريق اختبار الاختراق اتباع هذه المناهج بالضبط، وذلك من خلال التواصل المباشر مع الموظفين الجاهلين في محاولة لاختراق البنية الأساسية لتكنولوجيا المعلومات الخاصة بالمؤسسة، ما يساعد فريق تكنولوجيا المعلومات على إجراء فحوصات وعمليات مضادة لتجنب أي مواطن ضعف بشرية.

اختبار اختراق الشبكات

اختبار تقييم الشبكة هو أحد أشكال الاختبار الأكثر تعقيداً وشيوعاً ضمن اختبارات الاختراق. حيث يقوم المُختبِر بمحاولة اختراق شبكة المؤسسة من خلال شن هجمات على البنية الأساسية التي تشمل تكوينات جدار الحماية واحتماليات التجاوز، وتجنب نظام منع التسلل (IPS)، وهجمات نظام أسماء الحقول (DNS)، بالإضافة إلى الهجمات على البرمجيات التي تعمل داخل الشبكة، مثل بروتوكول نقل البريد البسيط (SMTP) وبروتوكول نقل الملفات (FTP) وصفحات تسجيل الدخول بالبريد الإلكتروني.

اختبار تطبيقات الإنترنت

عند وجود بيانات شخصية حساسة مثل البيانات المالية أو المتعلقة بالصحة، داخل موقع إلكتروني أو تطبيق الويب، يتعين على عملية اختبار الاختراق معالجة مواطن الضعف في هذه الأنظمة. حيث يقوم المُختبِر بفحص مكونات وبرامج وترميز موقع الإنترنت أو التطبيق وفقاً لتصميم كلٍ منها.

الوقاية الاستباقية من جرائم الفضاء الرقمي

قد يتباين نطاق اختبار الاختراق بصورة كبيرة من حيث الوقت والتكلفة والموارد، بناءً على نطاق التدقيق وحجم البنية الأساسية وعدد الأجهزة والخوادم التي تتواصل مع بعضها بعضاً والفضاء الرقمي الأكبر. وفي ظل الآثار المدمرة للجريمة الإلكترونية في الاقتصاد العالمي، يأتي هذا الأسلوب الاستباقي كإحدى الطرق المتقدّمة لمقاومة الهجمات الإلكترونية بكفاءة عالية وحماية سلامة الثروة الرقمية للقطاعين الحكومي والخاص في إمارة دبي.

الجيل الخامس..

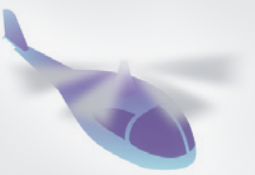
الجيل الأحدث في تقنيات الاتصال..

استعد للسرعة الفائقة!

نشهد الآن وصول شبكة الجيل الخامس إلى أيدي المستخدمين وتعدنا بإحداث ثورة كبرى تغير وجه الاتصال الهاتفي بشكل كبير وتسرع كل أنماط حياتنا، إذ توفر تكنولوجيا الجيل الخامس من شبكات الاتصال الخلوي تقنية متطورة بسرعة اتصال وتحميل مذهلتين تصل إلى 1 جيجابايت في الثانية الواحدة.

ولكن ما تأثير هذه التكنولوجيا المتقدمة في طبيعة الحياة وإدارة القطاع الحكومي والأعمال في دبي؟ وماذا سيكون تأثيرها في الأمن الإلكتروني؟ قامت "إشارات" باستكشاف هذا التطور التكنولوجي ودراسة تأثيره وتطبيقاته.

تكنولوجيا الجيل الخامس (5G)



تكنولوجيا الجيل الخامس هي ببساطة الجيل الخامس من الشبكات اللاسلكية للاتصال بالإنترنت، وكل جيل من التكنولوجيات أحدث نقلة تقنية في طبيعة الاتصال اللاسلكي. وبات العالم يشهد إطلاق جيل جديد كل 10 سنوات تقريباً، وفي حين أن تقنية الجيل الثاني أخرجتنا من عصر إنترنت الطلب الهاتفي (dial-up) في العام 1991، فإن تقنية الجيل الثالث أخذتنا إلى عصر وصول الهاتف المتحرك إلى شبكة الإنترنت مباشرة وذلك في العام 1998 إضافة إلى تمكين تطبيقات محددة مثل تطبيق نظام تحديد المواقع العالمي (GPS). وبعد ذلك بعشر سنوات بدأ عصر الجيل الرابع، وتحديداً في العام 2008، حيث أصبح الإنترنت في الهواتف المتحركة يمنحنا نطاق تغطية أوسع واتصالاً فائق السرعة وتطورت سرعة نقل البيانات والبث المباشر عبر الإنترنت بشكل فائق.

أما شبكة تكنولوجيا الجيل الخامس - وهي الجيل الأحدث من شبكة الاتصالات الهاتفية المتحركة والتي بدأنا نشهد بدايات انتشارها الآن - فإنها ستكون أسرع من الجيل الرابع بعشرين ضعفاً. على سبيل المثال، الملف العالي الدقة والذي يستغرق عدة ساعات في التحميل والنقل فإنه لن يستغرق سوى بضع ثوانٍ مع الجيل الخامس.

كيف تعمل هذه التقنية؟

من المتوقع أن تنتشر شبكة الجيل الخامس في العالم بحلول العام 2020، لتوفر قدرة اتصال فائقة السرعة غير متقطّعة في أي مكان. وعلى عكس تكنولوجيا الجيل الرابع التي تطورت بصورة جذرية من حيث سرعة الاتصال ومن دون تحميل المستخدمين أي نفقات، فإن شبكة الجيل الخامس لن تتطلب تحديث الهواتف الذكية أو الأجهزة الأخرى الحالية، بل ستتطلب شراء وتثبيت أنظمة جديدة كلياً بما في ذلك البرمجيات. وسوف تعمل شبكة الجيل الخامس بمجرد توفرها جنباً إلى جنب مع الجيلين الثالث والرابع الحاليين.

إن تكنولوجيا الجيل الخامس سوف تؤثر كلياً في طريقة عمل الإنترنت من خلال التحول إلى "الاتصال اللاسلكي الثابت." فبدلاً من الاتصال بالشبكة عبر جهاز توجيه (راوتر)، كما تعمل بنية الاتصال اللاسلكي الآن، فإن شبكة "الواي فاي" في منزلك أو مكتبك سوف تتصل لاسلكياً بشبكة اتصال أكبر.

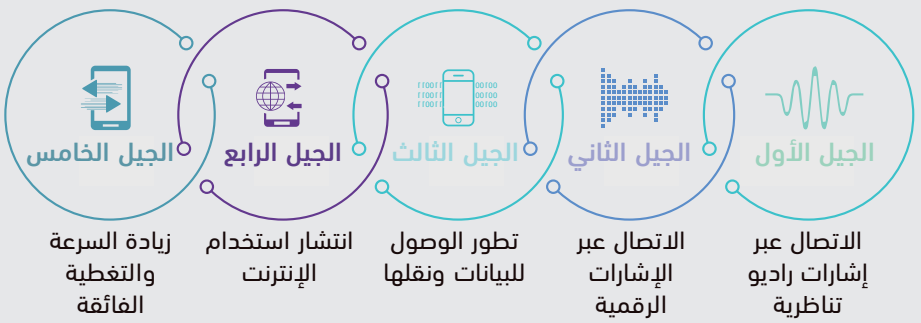
البيانات التي تتطلبها الأجهزة دائمة التشغيل، كتلك الأجهزة التي توجد في السيارة ذاتية التشغيل، سيتم تخزينها بجوار هذه الشبكات اللاسلكية لضمان اتصال أسرع.

تقوم جميع الاتصالات اللاسلكية بإرسال واستقبال البيانات عبر الإشارات المحمولة على الطيف الراديوي (الكهرومغناطيسي)، بينما تستخدم شبكة الجيل الخامس ترددات الراديو العالية (الموجات المليمترية) لتحقيق سرعتها وقدرتها. إن الترددات العالية أقصر وتتعرض للمزيد من التداخل، لذلك ستكون هناك حاجة إلى توزيع أعداد كبيرة من أبراج الإرسال في أماكن استراتيجية لضمان التغطية المثالية.

ما هي مزايا شبكة الجيل الخامس؟

نلخصها بكلمة واحدة: السرعة الفائقة! تتميز شبكة الجيل الخامس بسرعة اتصال فائقة تضاهي سرعة البرق، وهذا التطور هو ما سيؤثر في علاقاتنا بالإنترنت بشكل يفوق قدرتنا على تنزيل الأفلام. فسوف تكون تقنية الجيل الخامس

مراحل تطور الهاتف المتحرك:



محركاً رئيساً لتطوير كافة التقنيات الناشئة مثل إنترنت الأشياء والمركبات ذاتية القيادة وتعلم الآلة وغيرها.

كما يمكن لشبكة الجيل الخامس أن تدعم عدداً هائلاً من الأجهزة - مليون جهاز على الأقل في كل كيلومتر واحد. وقد يضم ذلك كافة الأجهزة بدءاً من الهواتف الذكية وصولاً إلى الساعات الذكية وأي أجهزة أخرى في المنطقة المحيطة، وكذلك جميع أجهزة إنترنت الأشياء التي تتطلب الاتصال المتزامن.

من المتوقع أن تحدث تقنية الجيل الخامس طفرة كبيرة في تطبيقات الاتصال، بدءاً من التطبيقات الطبية مثل الجراحة عن بُعد، حيث يمكن لجراح متخصص في أحد المستشفيات، على سبيل المثال، إنقاذ حياة طفل داخل عيادة في قرية إفريقية نائية وذلك من خلال البث المباشر وإرسال التعليمات الآنية إلى الطبيب المباشر.

وقد تغدو الازدحامات المرورية شيئاً من الماضي، حيث ستتمكن المركبات ذاتية القيادة من التواصل فيما بينها والتوفيق بين سرعاتها أو مساراتها ومن ثم تحافظ على سلاسة الحركة المرورية.

وكان سليم البلوشي، الرئيس التنفيذي للبنية التحتية في شركة الإمارات للاتصالات المتكاملة "دو" قد صرح للصحافة المحلية أن أحد المحركات الرئيسة لتقنية الجيل الخامس هو تطوير تقنية الفيديو. وأضاف: "إن تقنية الجيل الخامس سوف تعزز تجربة مشاهدة الفيديو عالي الوضوح مثل تقنية 4K وHD. ونتوقع أن يحدث الجيل الخامس طفرة كبيرة في تطبيقات الواقع الافتراضي والمعزّز، نظراً لكم البيانات الكبير والسرعة الفائقة التي تحتاجها وتتعامل معها هذه التطبيقات." تحتاج هذه الأجهزة إلى موجات ترددية أوسع وقدرة اتصال أسرع لتمكينها من تحقيق التجربة "الواقعية" للمستخدمين.

إليكم بعضاً من المزايا التي ستغمرنا بها تكنولوجيا الجيل الخامس:

- اتصال فوري بمحتوى البيانات على شبكة الإنترنت
- عدم حدوث أي تأخر في زمن البث - وهذه أخبار سارة لهواة ألعاب الفيديو
- ثورة في المنتجات المبتكرة التي تتطلب سرعات فائقة
- اتصال غير متقطّع وموثوق في كل مكان

> إطلاق الجيل الخامس من خدمات اتصالات الهاتف يتماشى مع رؤية الإمارات 2021 وسيُعزّز من مكانة الدولة الريادية في تطوير تقنية الجيل الخامس

- تطوير مدن ومواصلات ومصانع وبنية تحتية ذكية ذات فضاء رقمي آمن
- سيارات متصلة بالفضاء الرقمي وضوابط مرورية ذكية
- تطوير مراكز رعاية صحية ذكية معززة بالذكاء الاصطناعي
- إنتاج معدات زراعية أذكى وذات كفاءة عالية لإنتاج محاصيل أفضل وأكثر بتكلفة أقل
- تطور اتصالات الواقع المُعزّز مثل المكالمات الجماعية المجسّمة ورسائل البريد الإلكتروني أو الوثائق التي تتفاعل مع الفضاء المحيط وكذلك شاشات التلفاز الذكية.

متى ستتوفر تكنولوجيا الجيل الخامس في دبي؟

لقد أصبحنا معتادين على السرعة الفائقة لوتيرة التطور التكنولوجي في حياتنا وتقنية الجيل الخامس لن تكون استثناء.

من المتوقع أن يكون تطبيق تكنولوجيا الجيل الخامس مكلفاً للغاية ويجب استخدامها بعد اتخاذ الإجراءات الأمنية اللازمة. وهناك عوامل كثيرة تؤثر في زمن وصولها مثل موافقات الجهات التنظيمية وبناء الشبكات - بما في ذلك أبراج الإرسال والهوائيات والأسلاك وغيرها - وكذلك توفر الأجهزة المعززة بتقنية الجيل الخامس.

تتوفر خدمة الجيل الخامس في مواقع عدة وأماكن محدودة من حول العالم، لكن من المرجح أن تكون دولة الإمارات واحدة من أوائل الدول في المنطقة بل في العالم التي ستستخدم هذه التقنية. وقد أعلنت الهيئة العامة لتنظيم الاتصالات في وقت سابق أن إطلاق الجيل الخامس من خدمات اتصالات الهاتف يأتي تماشياً مع رؤية الإمارات 2021 وسوف يُعزّز من مكانة الدولة الريادية في تطوير تقنية الجيل الخامس.

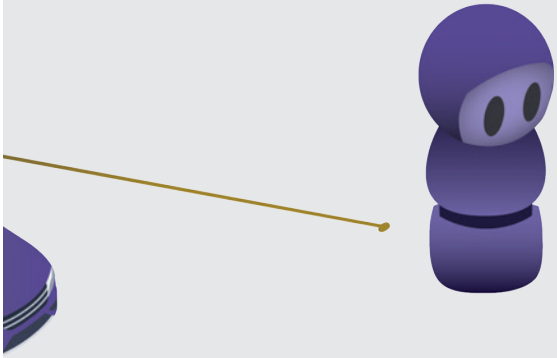
كشفت رائدتا تقديم خدمات الاتصالات في الدولة، "اتصالات" و"دو"، عن جاهزية بنيتهما التحتية لإطلاق خدمات التقنية الجديدة، لكن سيكون على العملاء الانتظار حتى يتم طرح المنتجات المُعزّزة بتقنية الجيل الخامس في السوق.

وفي السياق نفسه أكّد سليم البلوشي على أن ثورة الشبكات الحالية في شركة "دو" على حد قوله على أتم الاستعداد لتقديم خدمة الجيل الخامس، مشيراً إلى أن هذه التقنية ستسجل سرعة قصوى غير مسبوقة وزمن انتظار أقل بكثير وسعة تخزين هائلة.

كشف تقرير إريكسون للاتصالات المتنقلة لعام 2019 أن نمو اشتراكات خدمة الجيل الخامس سيكون أسرع في الشرق الأوسط، ومن المتوقع أن يصل إلى ثمانية أضعاف سرعته بحلول العام 2024 مقارنة بنموه بمقدار خمسة أضعاف على مستوى العالم. ويعود هذا في المقام الأول إلى معدلات المشاهدة العالية للفيديو إضافة إلى الثورة الصناعية سعياً لمضاعفة الكفاءات، فضلاً عن استراتيجيات التنوع الاقتصادي التي تشهدها المنطقة.

ماذا سيكون تأثير تقنية الجيل الخامس في الأمن الإلكتروني؟

على غرار التقدم في كافة التطبيقات التكنولوجية، فإن الأدوات التي تحسّن نوعية



الحياة تساعد قراصنة الفضاء الرقمي أيضاً على تطوير جرائمهم، ما يعني أن على خبراء الأمن الإلكتروني مواصلة إحداث التطور على مستوى الإجراءات الأمنية حتى يكونوا متقدمين عنهم دائماً بخطوة، وذلك في ظل التزايد المستمر لما يُعرف بـ"المساحات المعرّضة للهجمات"، مما يزيد من تعرضنا للمخاطر الإلكترونية.

يقول آرمين فازيسك، الخبير المتخصص في تقنية الجيل الخامس في شركة "إيه في جي لأمن الإنترنت AVG Internet Security": إن أعظم التحديات الأمنية التي ستواجه الجيل الخامس تأتي مع تطور "إنترنت الأشياء"، أي أنه كلما زادت الأجهزة المتصلة بالإنترنت زادت احتمالية التعرض للهجمات الإلكترونية. وحتى قبل ظهور تقنية الجيل الخامس، كان المخترقون يواصلون تخريب التطبيقات، إلا أن فرص اختراقهم للشبكات أصبحت أكبر الآن وذلك باستخدام برمجيات خبيثة مُدمّرة قد تسبب أضراراً باهظة التكلفة. وبما أن التهديدات الأمنية ستكون غير مسبوقة يواصل خبراء الأمن الإلكتروني إجراء الأبحاث المكثفة بمساعدة المخترقين الأخلاقيين للبحث عن الثغرات في النظام ومعالجتها.

تتمتع تقنية الجيل الخامس أيضاً بالقدرة على تحفيز قطاعات وخدمات جديدة كلياً، وجميعها تتطلب مستويات جديدة من الأمان. فقد يظهر نوع جديد من الهجمات الإلكترونية الموجهة إلى المركبات مع انتشار المركبات ذاتية القيادة. وقد وضع مركز دبي للأمن الإلكتروني هذه الاحتمالية في حساباته وحرص على تأسيس درع حماية إلكترونية متعددة الطبقات وذلك من خلال وضع معايير أمنية لتشغيل المركبات ذاتية القيادة في دبي والتي سيتم تطبيقها في المستقبل القريب بالتعاون مع هيئة الطرق والمواصلات.

وفي قطاع الصحة، فإن المخاطر التي تهدد الرعاية الصحية مثل سرقة الهوية أو تخريب البيانات سوف تتطلب أيضاً إجراءات أمنية أكثر صرامة. ومن حسن الحظ فقد توقع المركز هذه التحديات غير المسبوقة وقام بتطوير معايير أمنية تستهدف خدمات "إنترنت الأشياء" وأمن المعدات الطبية بهدف توفير مستويات أعلى من التحكم. وبوجه عام، فإن الأجهزة المعززة بإنترنت الأشياء وأجهزة الاستشعار كالتي تستخدم في المنازل والمؤسسات العامة والخاصة، تحتاج إلى عمليات تصديق معقّدة لمنع الوصول غير المصرح إليها. وقد يصبح التوثيق البيومتري باستخدام الصوت، مثل تطبيق أيريس (Iris) والقفل ببصمة الأصابع، معايير قياسية يجب تطبيقها وسوف تحتاج الشركات إلى مراقبة استراتيجيتها الأمنية بصفة مستمرة.

كيف تتقدم تكنولوجيا الهواتف المحمولة نحو المستقبل؟

لقد تخطينا مرحلة الاتصال البطيء بالإنترنت، لكن مع تزايد الأجهزة المتصلة بالإنترنت سيكون هناك حاجة لمواصلة تطوير البنية التحتية لمعالجة البيانات بسرعة وموثوقية. ويشير التطور الطبيعي لتكنولوجيا الهواتف إلى احتمالية مواصلة تعزيز شبكات الاتصال لتصبح أسرع وأكثر كفاءة.

وحتى قبل أن يتم تجربة خدمة الجيل الخامس، يعمل الخبراء الآن على تقنية الجيل السادس التي يتوقع لها أن ترى النور بحلول العام 2030 تقريباً.

ومن المتوقع أن تكون الاتصالات - والارتباط - فوريين ومستدامين في كافة أنحاء الكرة الأرضية لبناء توافق بين الطبيعة والذكاء الاصطناعي كما وصفها ماركوس ويلدون رئيس مختبرات بيل التابعة لشركة نوكيا العالمية (Nokia Bell Labs)، قائلاً "ستكون تكنولوجيا الاتصالات بمثابة الحاسة السادسة للبشر والآلات على حد سواء."

مركز دبي للأمن الإلكتروني يحمي البيانات الحكومية في السحابة الإلكترونية

كان مصطلح "الحوسبة السحابية" بمثابة لغز غامض عندما تم استخدامه في بداية عهده، إلا أنه سرعان ما أصبح مصطلحاً مألوفاً لدى معظمنا وبات مرتبطاً ارتباطاً مباشراً بشبكة المعلومات والإنترنت.. الشبكة التي تربط بين المستخدمين من كل أنحاء العالم.

توفر السحابة الإلكترونية منصة مبتكرة ومرنة ومنخفضة التكلفة للوصول إلى المعلومات والموارد الرقمية والبرمجيات وغيرها، إلا أنها تحمل طيفاً من التحديات التي تمس ثروة البيانات الخاصة بالحكومة. وهنا يأتي دور مركز دبي للأمن الإلكتروني كدرع واقية للبيانات السحابية الخاصة بكافة الجهات الحكومية وشبه الحكومية في دبي. وذلك من خلال اعتماده مجموعة من المعايير الأمنية لمقدمي الخدمات السحابية. تحدد هذه المعايير المتطلبات والمبادئ التوجيهية التي يجب على المؤسسات المستخدمة للخدمات السحابية تطبيقها، ويعد الامتثال بها إلزامياً لجميع من يرغب من الشركات التي تقدم الخدمات المتعلقة بالحوسبة السحابية للجهات الحكومية في دبي.

دعنا أولاً نوضح كيفية عمل الحوسبة السحابية:

هل تعلم أنك قد تكون بالفعل من أحد مستخدمي الخدمة السحابية؟ إذا كان لديك حساب على مواقع التواصل الاجتماعي مثل "فيسبوك" أو "لينكد إن" أو "جي ميل" أو إذا كنت تشاهد مقاطع الفيديو عبر يوتيوب، فأنت بذلك تستخدم الخدمة السحابية. تُعد الخدمة السحابية مخزناً هائلاً للبيانات مقارنة بالبيانات المُخزّنة على الأجهزة الفردية مثل الحاسوب والهواتف الذكية. وقد توقعت "مؤسسة البيانات الدولية" في أحدث تقرير لها أنه بحلول العام 2025 سوف تنمو البيانات المولّدة على مستوى العالم من 33 زيتابايت (عام 2018) إلى 175 زيتابيت، وسوف تُخزّن نصف هذه البيانات في بيئات سحابية عامة. كم يعني هذا؟ حسناً، الزيتابايت بأبسط معانيه هو وحدة قياس سعة تخزين تعادل تريليون جيجابايت.. فتخيل مساحة مهولة دائمة النمو!

يتم تخزين البيانات على خوادم فعلية أو افتراضية تخضع لإدارة وتحكّم شركات تقديم خدمات الحوسبة السحابية، وهي الجهات المنوطة بتوفير البيانات وإتاحتها وحماية بيئة تخزينها المادية. ويمكنك بصفتك فرداً أو مؤسسة الوصول إلى البيانات المخزّنة على الخدمة السحابية عبر الإنترنت.

هناك ثلاث استراتيجيات رئيسة لتوظيف الخدمات السحابية وخاصة للمؤسسات وهي:

• الخدمة السحابية العامة - حيث يتم تخزين كافة البيانات على البنية التحتية الخاصة بمزود الخدمة فيما يتم مشاركة الموارد مع العملاء الآخرين.

• الخدمة السحابية الخاصة - وهي شبكة خاصة بموارد مخصصة لعميل واحد؛ وهي تحظى بمستويات عالية من الأمن والتحكم.

• الخدمة السحابية الهجينة - وهي مزيج من السحابة العامة والخاصة ويتم توفيرها اعتماداً على متطلبات العميل.

استخدامات دولة الإمارات للسحابة الإلكترونية

تحتل دولة الإمارات العربية المتحدة المركز الأول في اعتماد خدمات الحوسبة السحابية على مستوى الشرق الأوسط ويأتي ذلك تماشياً مع رؤية الحكومة الرامية إلى بناء اقتصاد يستند إلى التكنولوجيا الرقمية ودعم التنوع الاقتصادي غير القائم على النفط.

وقد أسهمت هذه الرؤية في تبني نظام مزدهر اقتصادياً يضم مؤسسات حكومية وخاصة في قطاعات حيوية مثل القطاعات المالية والتجزئة والنقل وغيرها.

وفيما يتعلق بدبي ومركز دبي للأمن الإلكتروني، قالت الدكتورة بشرى البلوشي، رئيس قسم الأبحاث والابتكار في مركز دبي للأمن الإلكتروني: "إن المركز يسعى دائماً لتشجيع الشركات المبتكرة الناشئة وتوظيف التقنيات الجديدة، مما يسهم بشكل كبير في ازدهار الاقتصاد الوطني. غير أن المسؤولية الأولى للمركز تتمثّل في حماية سلامة الفضاء الرقمي لإمارة دبي لاسيما ثروة البيانات الهائلة التي تمتلكها الجهات الحكومية في دبي."

وأشارت إلى أن "نهجنا الموصى به في التعامل مع الخدمة السحابية يعتمد على مدى أهمية البيانات؛ فإذا كان الغرض من البيانات هو توفيرها للجميع، فإن الخدمة السحابية العامة ستكون مناسبة لمثل هذه البيانات، لكننا ننصح الجهات الحكومية دائماً بدراسة أهدافها والغرض من البيانات أولاً إذا كانت ترغب بالاستفادة من خدماتها السحابية؛ إذ يجب إبقاء البيانات السرية والحساسة في بيئة سحابية آمنة ومعتمدة في دولة الإمارات."

عامر شرف الدين شرف، مدير إدارة التعاون ودعم الامتثال في مركز دبي للأمن الإلكتروني، وتيونس كوتزي، المدير الإداري والإقليمي في المعهد البريطاني للمعايير يوقعان مذكرة تفاهم في المقر الرئيسي للمركز في دبي

المعايير الأمنية لمقدمي الخدمات السحابية

تهدف المعايير الأمنية التي وضعها مركز دبي للأمن الإلكتروني إلى تحديد المعايير التي يجب على مزودي الخدمات السحابية الامتثال بها للحصول على شهادة الاعتماد. وتقول البلوشي إن مركز دبي للأمن الإلكتروني هو أول مؤسسة حكومية تقوم بتقديم أفضل الممارسات الموثقة لإدارة المعلومات. وقد تم تطوير المعايير استناداً إلى نظام إدارة المعلومات المعتمد دولياً والمستخدم في المواصفة الدولية آيزو/ آي إي سي 27001.

ويهدف مركز دبي للأمن الإلكتروني إلى جعل عملية الاعتماد سلسة بقدر المستطاع وقد قام بتطبيق معايير أفضل الممارسات العالمية، بحيث يمكن تطبيق مجموعة محددة من الضوابط المحلية وعمليات التدقيق البسيطة لاعتماد المؤسسات الرائدة في تقديم الخدمة.

ويُعتبر مزودو الخدمات السحابية - بمجرد اعتمادهم - ممتثلين للمعايير ومن ثم يمكنهم ممارسة أنشطتهم التجارية مع الجهات الحكومية. ويتم إجراء عمليات التدقيق والمراقبة سنوياً بواسطة هيئات منح الشهادات المعتمدة، ويخضع الموردون للتدقيق كل ثلاث سنوات لتجديد الاعتماد.

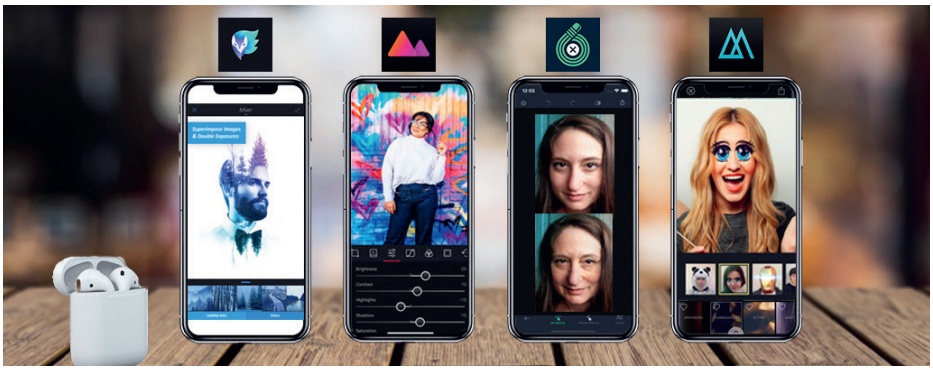
وعقد مركز دبي للأمن الإلكتروني شراكة مع المعهد البريطاني للمعايير (BSI)، وهي شركة رائدة عالمياً في تأسيس إنترنت الأشياء وممارسات الأمن الإلكتروني، وذلك لإجراء عمليات التدقيق الخاصة بالمعايير الأمنية لمقدمي الخدمات السحابية وإدارة عملية الاعتماد وإصدار الشهادات للموردين.

وتعليقاً على هذه الشراكة، قال عامر شرف، مدير إدارة التعاون ودعم الامتثال في مركز دبي للأمن الإلكتروني: "هذه الشراكة مع المعهد البريطاني للمعايير تعزز جهودنا في حماية المستقبل الرقمي لإمارة دبي وتساعدنا على تطبيق أفضل الممارسات في مجال الأمن الإلكتروني بالإمارة."

ومن جانبه أشار المدير الإقليمي للمعهد البريطاني للمعايير في منطقة الشرق الأوسط وإفريقيا تيونس كوتزي إلى أن الشركة تشيد بالدور الجوهري الذي يقوم به مركز دبي للأمن الإلكتروني في ترسيخ مكانة دبي كمدينة رائدة عالمياً في مجالات الابتكار والسلامة والأمن. وقال كوتز: "يسعدنا التعاون عن كثب مع مركز دبي للأمن الإلكتروني والمساهمة في دعم استراتيجية دبي للأمن الإلكتروني."

مايكروسوفت.. تتخذ الخطوة الأولى

"مايكروسوفت" هي أول شركة تحصل على اعتماد مركز دبي للأمن الإلكتروني في يونيو 2019 من خلال حصولها على شهادة المعايير الأمنية لمجموعة مختارة من الخدمات السحابية. وأسست أول مناطق للخدمات السحابية في الإمارات، في دبي وأبوظبي، لتزويد المؤسسات المحلية والأفراد والمطورين بخدمات سحابية آمنة كلياً، مع الحفاظ على مرونة وأمن وامتثال البيانات. وتشهد منطقة الشرق الأوسط نمواً متزايداً في عدد الشركات التقنية المتخصصة بإطلاق مراكز للبيانات في المنطقة.



تطبيقات تعديل الصور مسلية ومفيدة ولكن هل تعرّض خصوصيتك للخطر؟

على الرغم من إطلاق تطبيق الهاتف الذكي "فيس آب" (FaceApp) في العام 2017 إلا أنه لم يحقق شهرة كبيرة على مواقع التواصل الاجتماعي سوى في الآونة الأخيرة، بعد أن بدأ المشاهير بنشر صور منقّحة لهم تظهرهم في عمر متقدم، ولكن التطبيق تعرض لهجوم نبع من مخاوف انتهاك الخصوصية.

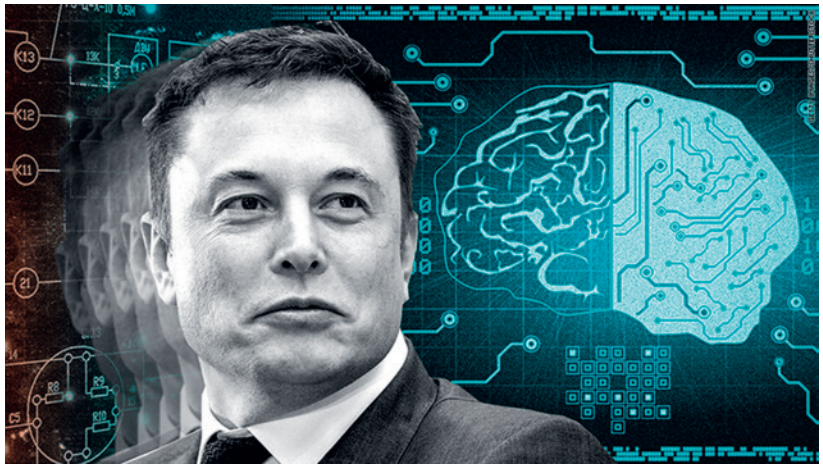
تطبيق "فيس آب" هو أحدث تطبيقات تنقيح الصور التي تعتمد على تقنية الذكاء الاصطناعي، ويستخدمه أكثر من 150 مليون مستخدم نشط، كما حاز جوائز عديدة من بينها لقب أفضل تطبيقات العام 2017 من متجر "آب ستور" و"غوغل بلاي." ويوفر التطبيق أكثر من 20 فلتراً تتيح للمستخدم إنتاج صور رقمية تظهرهم أكبر أو أصغر سناً أو بشكل أكثر جاذبية على نحو واقعي.

وكغيره من التطبيقات الحديثة، وقع تطبيق "فيس آب" تحت مجهر الجهات الأمنية، والسبب الرئيسي هو أنه شأنه شأن العديد من التطبيقات ومنصات التواصل الاجتماعي يقوم بجمع بيانات معينة من المستخدمين، وإذا تم الكشف عن تلك البيانات فقد يُعرّض ذلك أصحابها للهجمات الإجرامية.

لا يستخدم "فيس آب" سوى الصور التي يوفرها المستخدمون لتغيير ملامح وجوههم، ولا يقوم التطبيق بتحميل أي بيانات أخرى، غير أن ملفات هذه الصور تُرسل إلى السحابة الإلكترونية لمعالجتها، حيث توجد حاجة مستمرة إلى ضوابط مشددة لتأمين هذه البيانات. وتحث شركات وسائل التواصل الاجتماعي المستخدمين على حماية بياناتهم الرقمية واستخدام هذا التطبيق بحذر.

وقامت الشركة الصينية "تينسنت" بابتكار نظام ذكاء اصطناعي مشابه استُخدم مؤخراً في لمّ شمل عائلة اختفى طفلها الرضيع منذ 18 عاماً، بعد أن تمكنت الشرطة من اقتفاء أثره باستخدام التطبيق لتغيير ملامح وجهه ليصبح متقدماً في العمر، وذلك للتنبؤ بشكل وملامح وجه الطفل اليوم. تعرض ذلك الطفل المفقود الذي يبلغ 21 سنة اليوم للاختطاف في صغره، وأكدت فحوصات الحمض النووي مطابقته لوالديه البيولوجيين.

«إيلون ماسك» يكشف عن خططه لربط العقل البشري بأجهزة الكمبيوتر



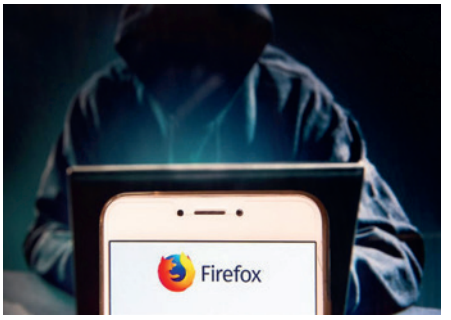
أعلن رائد الأعمال التكنولوجية المتطورة "إيلون ماسك" عن قيامه بتطوير واجهات دماغية حاسوبية (BMIs) قابلة للزرع، وهي أجهزة تربط العقل البشري بأجهزة الكمبيوتر. ويهدف المشروع إلى إيجاد طرق تحفّز عقول المرضى ذوي الإصابات العصبية الحادة، وتمكينهم من التحكم بأجهزة الكمبيوتر وبالتالي تحسين نوعية حياتهم.

تقود الأبحاث شركة "نيورالينك"، إحدى شركات "ماسك"، بينما تبحث شركات تكنولوجية أخرى طرقاً مشابهة لتعزيز قدرات العقل البشري بالاعتماد على تعلم الآلة المُعزز بالذكاء الاصطناعي. وقد تم بالفعل اختبار أحد أنظمته على قرد، وأثبت القرد قدرة الحيوان على التحكم في جهاز كمبيوتر بعقله. والآن يريد "ماسك" اختبار الجهاز على البشر.

يتضمن النظام مسباراً صغيراً يحتوي على أكثر من 3000 قطب كهربائي متصل بخيوط مرنة أرق من سمك الشعرة البشرية، مما يسمح للمسبار بمراقبة مناطق محددة من الدماغ، وتحليل تسجيلاته باستخدام الذكاء الاصطناعي، والذي سيحدد حينئذ نوع التحفيز الذي يحتاجه المريض.

يحتاج النظام سنوات من التطوير العلمي والتكنولوجي والأخلاقي ليصبح جاهزاً، لكنه نال استحسان الكثيرين لقدرته المحتملة على التخفيف من الحالات الصحية الحادة كالسكتة الدماغية والصرع ومرض "باركنسون."

«موزيلا فايرفوكس» يخطط لإبلاغ مستخدميه في حالة اختراق كلمة المرور



يخطط متصفح "موزيلا فايرفوكس" لطرح تحديث أمني يتيح إمكانية تحذير مستخدميه في حالة تم اختراق بيانات الدخول الخاصة بهم.

وتتعاون الشركة مع متتبع لاختراق البيانات في تطوير مبادرتها والاعتماد على قاعدة بيانات مكونة من أكثر من ثمانية مليارات حساب تعرضت للاختراق لتحذير مستخدميها، حيث ستقوم بمسح بيانات الدخول المحفوظة بحثاً عن نتائج مطابقة، كما ستصدر تحذيراً بشأن كلمات المرور لأصحاب تلك الحسابات وستحث مستخدميها على تغيير كلمات المرور الخاصة بهم.

سيتم دمج الخاصية الأمنية الجديدة في متصفح "فايرفوكس 70"، مما سيفيد أكثر من 800 مليون شخص يتصفحون عبر أجهزة الكمبيوتر المكتبية، والذين قاموا بحفظ بيانات دخولهم قبل حدوث الاختراق، حيث سيتم إصدار التحذير آلياً وسيتضمن الرسالة التالية: "تعرضت بعض كلمات المرور للتسريب أو السرقة من هذا الموقع منذ آخر مرة قمت فيها بتحديث بيانات الدخول الخاصة بك."

وتنوي الشركة الإفصاح عن المزيد من المعلومات بشكل أكثر تفصيلاً، بما في ذلك تأثير الاختراق في حساب المستخدم؛ هذا وقد حثت "موزيلا" مستخدميها على مواصلة تطبيق التدابير الأمنية الأساسية الخاصة بكلمة المرور، كالحرص على تكوين كلمات مرور متفردة يصعب اختراقها وتفعيل خاصية التحقق بخطوتين.

لا رادع أمام مخترقي الأقمار الصناعية

تدور آلاف الأقمار الصناعية حول الأرض وتمثل مرتعاً جديداً للمجرمين الإلكترونيين، ويخشى الخبراء ألا يأخذ مهندسو الأقمار الصناعية حول العالم هذه المخاطر في الحسبان بما يكفي في تصميماتهم المستقبلية.

وقد ذكر الباحثون في مؤتمر 2019 RSA لأمن المعلومات أنه في حين تركز هياكل اتصالات الأقمار الصناعية على السلامة فقد أصبح أمن المعلومات مهماً بالقدر ذاته.. والجدير بالذكر أن مؤتمرات RSA تستقطب آلاف المشاركين سنوياً وتقام في دولة الإمارات العربية المتحدة والولايات المتحدة الأمريكية وأوروبا وآسيا.

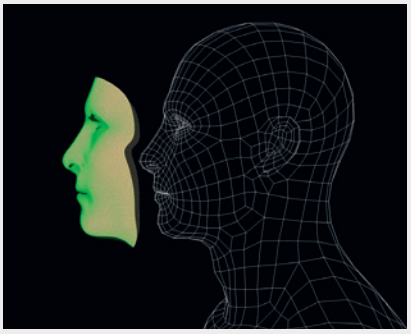
كان "سبوتنك 1" الذي أطلق في العام 1957 أول قمر صناعي يتم إطلاقه في التاريخ، ومنذ ذلك الحين تم إطلاق أكثر من 8900 قمر صناعي ما زالت أغلبيتها تعمل حتى الآن. وتوفر هذه الآلات شديدة التعقيد معلومات جوهرية تخدم مجموعة واسعة من التطبيقات، بدءاً من نظام تحديد المواقع العالمي (GPS) ومراقبة الطقس وتتبع الكوارث الطبيعية وصولاً إلى استكشاف الفضاء.

وفي العقود الأخيرة، وقعت عدة هجمات خبيثة كان الهدف منها الإخلال ببعض الأقمار الصناعية أو تدميرها، ويُزعم أن مرصداً فضائياً تابعاً لكل من الولايات المتحدة الأمريكية وألمانيا تعرض للاختراق في العام 1998 عبر الاختراق الإلكتروني، وتم توجيهه نحو الشمس، مما نجم عن تدميره بفعل حرارتها.

غير أنه من المتوقع أن تزداد عمليات اختراق الأقمار الصناعية، وذلك مع انخفاض تكلفة الهوائيات والنمو الذي يشهده مجال الأقمار الصناعية والقدرات الفضائية. كما يستطيع المخترقون التشويش على إشارات نظام تحديد المواقع العالمي، ويمكنهم أيضاً اعتراض البيانات الحيوية أو التلاعب بها، كما أنهم قادرون على اختطاف أحد الأقمار الصناعية والمطالبة بفدية، وغيرها الكثير من الأنشطة الإجرامية.

وينصح خبراء الأمن الإلكتروني بضرورة تفعيل عدة طبقات من الإجراءات الأمنية من بينها التدابير التكنولوجية وسياسات الأمان.

الذكاء الاصطناعي المحرك الرئيسي لخطر التزييف العميق



حيثما تكون هناك تقنيات مبتكرة، تكون هناك فرصة للاختراق. ومن بين هذه التقنيات، ظهرت تقنية الذكاء الاصطناعي الخبيثة التي تقود تطوير "التزييف العميق"، الذي يستخدم مزيجاً من المقاطع الصوتية والمرئية الحقيقية ومعالجتها لإنتاج صور ومقاطع فيديو مزيفة تبدو حقيقية تماماً لشخص يفعل أو يصرح بشيء لم يقم به.

وتتخطى تقنية التزييف العميق فكرة المعالجة الرقمية للصور بكثير، حيث يقوم المخادعون باستخدام الذكاء الاصطناعي بطرق غير قانونية لخداع الناس وإقناعهم بأنهم يشاهدون صوراً حقيقية لمشاهير أو شخصيات تم تصويرهم في مواقف مثيرة للشبهة أو نقل تصريحات صادمة لهم وما إلى ذلك. وتستطيع برمجيات التعلم الآلي المعتمدة على الذكاء الاصطناعي نسخ صوت الشخص لصياغة خطاب جديد له، كما تم تطوير سلسلة من الخوارزميات لابتكار وجوه مزيفة بالاعتماد على مجموعات هائلة من البيانات.

يقوم المخترقون والإرهابيون بإنتاج مقاطع الفيديو المزيفة لأغراض الابتزاز وطلب الفدية أو لزعزعة استقرار الأسواق المالية، أو حتى لإثارة الذعر، أو لأي أغراض تحقق رغباتهم الخبيثة. وبغضون دقائق قد تنتشر هذه الصور والمقاطع المزيفة بشكل هائل في كافة أنحاء العالم بمجرد نشرها على صفحات التواصل الاجتماعي.

وفي حين أن المحللين المحترفين يستطيعون اكتشاف هذه المواد المزيفة باستخدام برمجيات متخصصة، فإننا ما زلنا بحاجة إلى الوثوق في غرائزنا والتفكير ملياً عند سماع أو مشاهدة مواد تبدو غير حقيقية.

أنظمة المناعة وتخزين البيانات في الحمض النووي رقمياً لحماية مستقبل دبي!

هل سمعت من قبل عن المناعة الرقمية وتخزين البيانات داخل الشفرة الجينية واعتقدت أنك تقرأ عن أحد أفلام الخيال العلمي.. فأهلاً بك في المستقبل!

الدكتور روكي ترمانيني

تعمل الدكتورة بشرى البلوشي، رئيس قسم الأبحاث والابتكار في مركز دبي للأمن الإلكتروني، مع الدكتور عيسى البستكي، رئيس جامعة دبي، على تطوير نموذج نظام مناعة رقمي ومختبر أحماض نووية لأرشفة البيانات، بالتعاون مع الخبير العالمي الدكتور روكي ترمانيني، الرئيس التنفيذي في شركة ميريت لاستشارات الأمن الإلكتروني وسيتم عرضه في إكسبو 2020.

في هذا المقال يشرح الدكتور ترمانيني هذه المفاهيم التقنية المعقدة وكيف يمكنها المساهمة في حماية دبي من التحديات الإلكترونية المستقبلية.

إننا نعيش في عصر الابتكار، ونلتزم بتأدية دورنا بما يحقق الرؤية الاستراتيجية الثاقبة لصاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، التي تستهدف بناء المستقبل الذكي لدولة الإمارات ولإمارة دبي من خلال تطبيق وابتكار التقنيات المستقبلية والذكاء البشري والموارد الطبيعية للارتقاء بمستوى جودة الحياة وتحقيق نمو اقتصادي مستدام.

وحالياً تُجرى الأبحاث حول مبادرتين استراتيجيتين يمكنهما تحقيق هذه الرؤية وذلك بالتعاون مع مركز دبي للأمن الإلكتروني وتحت إشراف مباشر من سعادة يوسف الشيباني المدير العام بالمركز وإدارة الأبحاث والابتكار:

1. **نظام المناعة الرقمية** - النظام الذي سيوفر الجيل الجديد من الحماية المستقلة للأمن الإلكتروني على مدار العشرين عاماً المقبلة، حيث تم دمج الذكاء الاصطناعي مع منصة النظام القائمة على التكنولوجيا النانوية لتصميم نسخة طبق الأصل من الجهاز المناعي البشري. إنه الحل التكنولوجي القادر على إبادة البرمجيات الخبيثة إذا تم إطلاقها ضد نظم المدن الذكية.

2. **تخزين البيانات في الحمض النووي** – رحلة مذهلة إلى أصل الحياة، أو الحمض النووي الريبوزي منقوص الأكسجين. ستكون مدينة دبي من أوائل المدن التي ستقوم بتخزين بيانات الحمض النووي، والتي ستمثل عنصراً جوهرياً في نظام المناعة الرقمية.

كيف يمكن تطبيق هاتين التقنيتين الحديثتين تطبيقاً ناجحاً لتتصدر دبي مجال الأمن الإلكتروني للمدن الذكية؟

نظام المناعة الرقمية

لطالما كانت التكنولوجيا سلاحاً ذا حدين، وقد قامت الجرائم الإلكترونية والإرهاب الإلكتروني مؤخراً بالعبث بنسيجنا المجتمعي محاولة تفكيكه من الناحية الفكرية والخلقية، لكن نظام المناعة الرقمية مصمم لتوفير شبكة معقدة تحمي المدن الذكية من الهجمات الإلكترونية.

إن مفهوم تكنولوجيا الذكاء الاصطناعي يعد نسخة مطابقة للذكاء البشري ويمثل تحدياً وإلهاماً

على حد سواء، فنظام المناعة الرقمية عبارة عن هجين يتشكل من الذكاء البشري، الخبرة، الذكاء الاصطناعي وعناصر التكنولوجيا النانوية.

تسمح مكونات الذكاء الاصطناعي للنظام ببرمجة وتشغيل نفسه والتعلم من أخطائه السابقة بل وإصلاح نفسه، لكن صنع نسخة طبق الأصل من الجهاز المناعي البشري يتطلب مكوناً حيوياً آخر على المستوى الذري، وهو دور التكنولوجيا النانوية، التي ستوفر لنظام المناعة الرقمية تحكماً أفضل ومرونة أكثر وكفاءة أعلى وسرعة وقدرة على توقع الهجمات الإلكترونية بدقة تامة.

• **نظام الإنذار المبكر -** يوفر قدرة تنبيهية ذكية قادرة على اكتشاف الهجمات قبل وصولها إلى المدينة وأنظمة البنية التحتية الحيوية فيها.

• **ذاكرة الهجوم الإدراكي -** محرّك يتعلم الهجوم بحيث يتذكر الهجمات السابقة ويتنبأ بالهجمات المستقبلية.

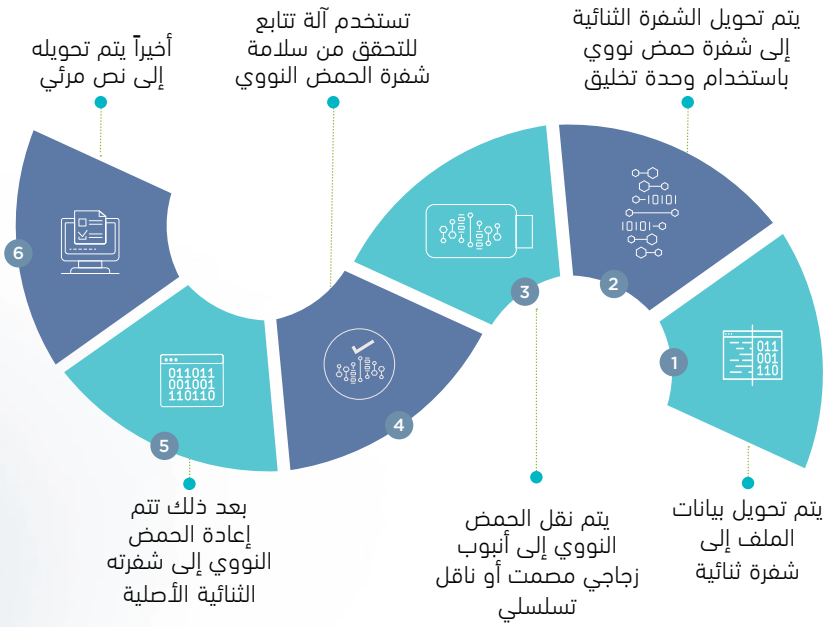
• **دفاع لقاح النانو الذكي -** يقوي مناعة كافة الأنظمة ضد الهجمات المفاجئة.

• **الشبكة المستقلة -** توفر ذكاءً اصطناعياً فائق الاستجابة وهندسة نانوية، مما يتيح الحماية المستمرة لكافة أجهزة المدينة وأنظمتها الحيوية.

يعد نظام المناعة الرقمية شبيهاً بتكنولوجيا مضادات الفيروسات، لكن كل منهما ينتمي إلى جيل مختلف، والمقارنة بينهما تشبه المقارنة بين قطار الطلقة والقطارات البخارية، حيث إن نظام المناعة الرقمي مصنوع باستخدام مكونات الذكاء الاصطناعي على المستوى الجزيئي، وخلافاً لتكنولوجيا مضادات الفيروسات الموجودة على الإنترنت فإن نظام المناعة الرقمية يسكن شبكة نانوية ذكية تمثل جهازه العصبي، ويتواصل مع الأقمار الاصطناعية والتكنولوجيا السحابية.

وبعد أن تبدأ الشبكة النانوية الذكية التي تحتوي على نظام المناعة الرقمية بالعمل، ستكون مدينة دبي يقظة وعلى أهبة الاستعداد لرد أية هجمات إلكترونية، حيث إن كافة الأنظمة الحيوية ومنها إنترنت الأشياء وأنظمة البلوك تشين في دبي ستكون متصلة بالشبكة وسيتم تحصينها دورياً حفاظاً على مناعتها ضد الهجمات المفاجئة.

عملية تشفير الحمض النووي رقمياً



بالرغم من الحجم متناهي الصغر للجزيء الوراثي فإن تقنية التشفير الرقمي هذه تتيح الفرصة لتخزين 213 بيتابت (أو 215 مليون غيغابت) من البيانات الرقمية في غرام واحد من الحمض النووي، وهو تقريباً حجم البيانات المخزنة حالياً على الإنترنت!

تخزين البيانات في الحمض النووي

في العام 2012 وصف الدكتور جورج ماكدونالد تشرش عالم الوراثيات الأمريكي في جامعة هارفارد كيف أضاف المعلومات الرقمية المشفرة إلى الحمض النووي، حيث نشر كتاباً يتألف من 53,400 كلمة إضافة إلى عدة صور وبرامج. وقد استطاع تخزين 5.5 بيتابت في ملليمتر مكعب واحد من الحمض النووي. [ملاحظة: البيتابت من أكبر أدوات قياس البيانات، حيث يساوي البيتابت الواحد مليون غيغابت من البيانات].

واليوم يعمل مصممو الحواسيب وعلماء علم الأحياء التركيبي على تصميم أنظمة لأتمتة عملية التخزين في الحمض النووي، حيث سيتم استخدام شفرة الحمض النووي مستقبلاً لتخزين البيانات التشغيلية الخاصة بكل الأنظمة الحيوية وبيانات عمليات المناعة الرقمية في نظام المناعة الرقمية.

[ملاحظة: تم تنقيح المقالة الأصلية وحذف بعضها ليكون حجمها ملائماً]

ابدأ مسيرتك المهنية الواعدة في قطاع الأمن الإلكتروني

شارك مركز دبي للأمن الإلكتروني في معرض الإمارات للوظائف الذي أقيم في مركز دبي التجاري العالمي في مارس 2019 وعرض مجموعة من الفرص الوظيفية الواعدة المتاحة في قطاع الأمن الإلكتروني أمام الشباب الإماراتي.

في عصر البيانات الضخمة تعاظمت أهمية الوظائف التي تستهدف حماية المعلومات وأمن الفضاء الرقمي، وأصبح عليها طلباً غير مسبوق خاصة بعد أن أصبحت قيمة البيانات تتجاوز أثمن الموارد في العالم. والجيل الحالي يملك الحماس والألفة مع التكنولوجيا، وكيف لا؟ وقد كبر وترعرع في ظلالها.. ومركز دبي للأمن الإلكتروني يشجع الشباب على التخصص في هذا القطاع، ويتطلع لأن يصبح لدينا جيل من الخريجين المؤهلين لحراسة فضائنا الرقمي.

معرض الإمارات للوظائف 2019

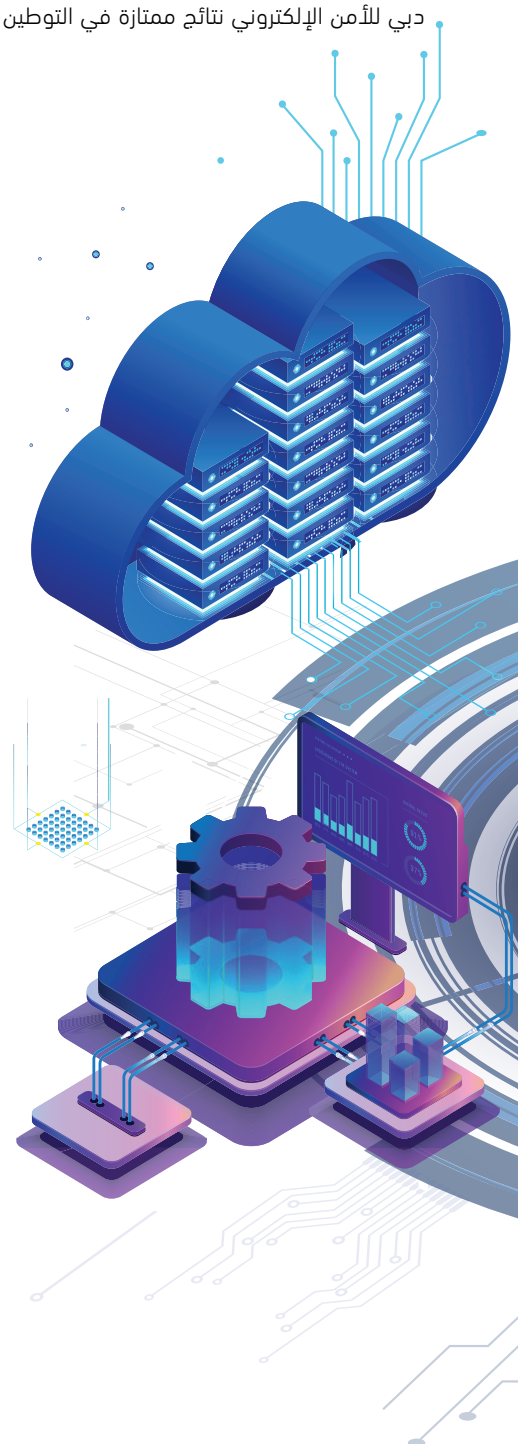
شارك مركز دبي للأمن الإلكتروني في معرض الإمارات للوظائف 2019 ضمن خطته لتمكين الكوادر الإماراتية الاحترافية من الحصول على وظائف مستقبلية واعدة، ودعماً لرؤية قيادتنا الحكيمة الرامية لجعل مدينة دبي الأكثر أماناً في الفضاء الإلكتروني في العالم. ويشهد قطاع الأمن الإلكتروني ارتفاع الطلب على الخبراء في قطاع تكنولوجيا المعلومات وأمن المعلومات، وتتيح الوظائف المتنوعة التي يقدمها مركز دبي للأمن الإلكتروني فرصاً واعدة للخريجين.

وفي سياق البحث عن الكوادر الوطنية المتميزة، قال سعادة يوسف حمد الشيباني، مدير عام مركز دبي للأمن الإلكتروني: "يضطلع مركز دبي للأمن الإلكتروني بدور نشط في توظيف أفضل الكفاءات الوطنية على نحو حيوي مبتكر، كي نحسن قدراتنا الرقمية باستمرار ونطور تقنيات

جديدة ونتطور مع الاتجاهات والتحديات دائمة التغير في العالم الإلكتروني."

"نحن حريصون على تنفيذ رؤية المركز المنبثقة من توجيهات قيادتنا الرشيدة والتي تعكسها استراتيجيتنا للأمن الإلكتروني. لقد حقق مركز دبي للأمن الإلكتروني نتائج ممتازة في التوطين حيث أصبح المركز يدار من قبل المواطنين بالكامل."

"ومثّلت مشاركتنا هذا العام فرصة مواتية لنواصل استقطاب الكوادر الوطنية المبدعة التي ستكون جزءاً من فريق عمل المركز لتحقيق رؤيته. يستقطب معرض الإمارات للوظائف قاعدة عريضة من الكوادر والقادة والإداريين الأكفاء في مختلف التخصصات، ونحن ملتزمون بالمشاركة في معارض التوظيف المماثلة لاستهداف وتمكين المواطنين الإماراتيين الذين يريدون التفوق في مجال الأمن الإلكتروني، فنحن دوماً نتطلع لتعزيز فريقنا."



مشاركة مبتكرة

طرح مركز دبي للأمن الإلكتروني نظاماً جديداً للتسجيل التفاعلي في منصته بمعرض الإمارات للوظائف هذا العام، حيث طُلب من المتقدمين تعبئة نموذج تسجيل رقمي إضافة إلى اختبار لتقييم الشخصية، وقد وفّر هذا الابتكار مقياساً لمدى ملاءمة المتقدم لشريحة العمل التي أبدى رغبته فيها، كما طابق بين صفاته واستعداداته الشخصية، وأوضح المعايير التي تتطلبها الوظائف في مركز دبي للأمن الإلكتروني، حيث استطاع الزوار تفقّد مجموعة من الوظائف الشاغرة وتسجيل اهتمامهم بها إلكترونياً.

وقد استعرض المركز أيضاً أقسامه وإنجازاته الجديدة في خدمة مختلف القطاعات، إضافة إلى أحدث المشروعات والمبادرات التي يشارك فيها المركز.

فرص وظيفية في دولة الإمارات

أظهرت أبحاث أجرتها مؤخراً شركة سانز العالمية للتدريب على أمن المعلومات أن الوعي بالأمن الإلكتروني وتفضيل هذا المجال كخيار مهني بين الشباب في دولة الإمارات والمملكة العربية السعودية هما من الأعلى في العالم.

استهدف الاستبيان أربعة آلاف شخص بين الرابعة عشرة والثامنة عشرة عبر سبع دول في الشرق الأوسط وأوروبا، وأوضحت نتيجة الاستبيان أن اختيار تكنولوجيا المعلومات (شاملاً الأمن الإلكتروني) بلغ أعلى مستوياته في المملكة العربية السعودية (47 في المئة) ودولة الإمارات (46 في المئة). ومن بين هؤلاء، أعرب

الوظائف التي يطلبها مركز دبي للأمن الإلكتروني

- مهندس شبكات
- مسؤول مركز بيانات
- مسؤول أنظمة أمنية
- باحث
- مطوّر برمجيات
- مسؤول مركز عمليات أمن المعلومات
- مسؤول لوائح أمن المعلومات
- مسؤول دعم تكنولوجيا المعلومات

63 في المئة من الطلاب في المملكة العربية السعودية عن رغبتهم في الأمن الإلكتروني تحديداً وكذلك فعل 58 في المئة في دولة الإمارات. أما الدول الأوروبية التي شملها الاستبيان فهي بريطانيا وفرنسا وألمانيا وهولندا وبلجيكا.

وفيما يخص الوعي الإلكتروني، قال 85 في المئة من الطلاب في دولة الإمارات إنهم قد سمعوا بالأمن الإلكتروني، تبعهم 82 في المئة في بريطانيا، وأشارت سانز إلى أن الدول التي أظهر جيلها الشاب مستويات أعلى من الوعي قد تمتلك ميزة تنافسية فيما يتعلق بتنمية الكوادر لتلبية الحاجات المستقبلية.

الدعم التعليمي لتكنولوجيا المعلومات

من المؤكد أن المدارس والجامعات في دولة الإمارات تساهم بتعزيز امتلاك المهارات التكنولوجية على المستوى العالمي، ودعماً لرؤية الإمارات 2021 ومع ارتفاع أعداد الطلاب في الدولة، خصصت الحكومة الإماراتية 10 مليارات درهم هذا العام (17% من الميزانية الوطنية) لتنمية نظام تعليمي من الطراز الأول.

الأمن الإلكتروني خيار لمهنة المستقبل


%47


%46

الطلاب المهتمون بالأمن الإلكتروني

السعودية %63

الإمارات %58

الوعي الإلكتروني

الإمارات

%85

يُعد الابتكار الرقمي والتكنولوجي من المعايير الرئيسة لنظام التفتيش المدرسي في دولة الإمارات، إذ إن الميزات مثل أدوات التعاون الرقمي ومختبرات الأبحاث والتطوير عالية الأداء والتقنيات المشابهة تسهم في تحول تجارب التعلم.

سد الفجوة العملاقة في المهارات

بحلول 2020 سيبلغ عدد الأجهزة المتصلة بالإنترنت نحو 24 مليار جهاز حول العالم، وهو

ما يعتبره السيد " ند بلطه جي" المدير الإداري لمعهد سانز في الشرق الأوسط تحدياً في مجال الأمن الإلكتروني، يتمثل في نقص عالمي فادح في عدد المحترفين المطلوبين لتأمين كافة تلك الأجهزة والأنظمة المتصلة بالإنترنت.

ونصح بلطه جي قائلاً: "في ظل حماس جيل الآيفون للتقنيات الرقمية وبراعته الفطرية في استخدامها، قد يكمن الحل في تعليم الأجيال الجديدة الأمن الإلكتروني الآن لتعزيز قوتنا العاملة المستقبلية."

هذا وقد شملت النتائج الرئيسة الأخرى من البحث ما يلي:

- احتلت تكنولوجيا المعلومات 32 في المئة من أول خمسة خيارات مهنية لدى أغلب المستجيبين، لتتقدم بذلك على المهن الأكثر تقليدية كالطبيب/الممرض(21%) والمعلم (19%) ووظائف القطاع المالي (16%).
- وصلت تكنولوجيا المعلومات إلى مرتبة أعلى كخيار من أول خمسة خيارات مهنية، وذلك حسب تصويت طلاب المدارس في الإمارات (46%) والمملكة العربية السعودية (47%).
- تربّعت تطوير التطبيقات والبرمجيات على عرش القائمة الإجمالية (61%) بين المهتمين بالمهن في مجال تكنولوجيا المعلومات، تلاه تصميم أنظمة تكنولوجيا المعلومات (52%) ثم الأمن الإلكتروني (49%)، أما في السعودية والإمارات فقد كان الأمن الإلكتروني هو الخيار الأول بنسبة 63% و58% على التوالي.
- أجاب كافة الطلاب تقريباً (81%) أنهم يتوقون إلى تعلّم المزيد عن الموضوع في المدرسة، حيث أثبت المستجيبون من السعودية (93%) والإمارات (91%) مجدداً أنهم الأكثر اهتماماً بالأمن الإلكتروني.

تريد أن تصبح مدافعاً عن فضائنا الإلكتروني..

مع تزايد عدد مؤسسات التعليم العالي المعتمدة عالمياً في دبي، أصبح لدى الخريجين خيارات لا حصر لها فيما يخص التعليم الجامعي. إذا كنت تملك الشغف للتخصص والعمل في إحدى وظائف الأمن الإلكتروني، فعليك الانضمام إلى إحدى الأكاديميات الجامعية، وإجراء بحث شامل حول التعليم والتدريب لتضمن الوصول إلى المسيرة المهنية المناسبة لك.

قم بزيارة بعض معارض التوظيف المميزة التي تقام في الإمارات سنوياً، وتحدث إلى المرشد المهني في مدرستك، وابحث عبر الإنترنت لتكوّن فكرة جيدة عن الخيارات المتاحة. وبعد أن تضع قائمة بأفضل الجامعات أو الكليات أو غيرها من الخيارات، حاول أن تقوم بزيارتها أثناء الأيام المفتوحة التي تقيمها للالتقاء بالطلاب المستقبليين لتعريفهم بالتخصصات المختلفة، أو حدد موعداً لزيارة الأقسام المناسبة لك.

عادة ما يحمل العاملون في قطاع الأمن الإلكتروني شهادات محددة، ولكن ذلك ليس إلزامياً، ويحمل الاختصاصيون درجة البكالوريوس في علوم الحاسوب أو علم نظم المعلومات أو البرمجة أو الهندسة، وعادة ما يكون مستوى مواد الرياضيات والإحصاء في هذه التخصصات أعلى تركيزاً من التخصصات الأخرى، كما يلعب محللو السياسات وأصحاب الخبرات في مجال القانون وإدارة الأعمال أدواراً مهمة في الحفاظ على أمن فضاءنا الرقمي.

إذاً كيف تعرف فيما إذا كان الأمن الإلكتروني هو المجال المناسب لك؟

يحمل الكثيرون من الناجحين في هذا القطاع

سريع النمو، من المحللين إلى المبرمجين وغيرهم، صفات شخصية معينة مشتركة، وقد تكون أنت المرشح المثالي للعمل في مجال الأمن الإلكتروني إذا:

- مواد العلوم والتكنولوجيا والهندسة والرياضيات هي المفضلة لديك
- كنت شغوفاً بالحواسيب وألعاب الفيديو والأجهزة الإلكترونية
- تحب برمجة الحواسيب وكتابة الرموز الرقمية
- تحب تحدي حل الأحجيات والمسائل
- تنتبه لأدق التفاصيل
- تحب إطلاق العنان لخيالك وتفكيرك المبدع
- تجد ممارسة مهام متعددة في آن واحد أمراً مُحفزاً ولا تراه يفوق طاقتك
- تحب أن تبقى في الطليعة ولا تكفّ عن التعلّم أبداً
- أنت فخور بوطنك وتريد أن تقوم بدور مهم في الحفاظ على أمنه
- تشعر بالسعادة حين تشارك في العمل لتحقيق قضية نبيلة وعادلة

الوظائف في مجال الأمن الإلكتروني

ليست كل الوظائف المتاحة في قطاع الأمن الإلكتروني مرتبطة ارتباطاً مباشراً بالتكنولوجيا الرقمية، بل إن الطلب على مهارات التواصل يفوق الطلب على مهارات البرمجة والترميز، ففي مركز دبي للأمن الإلكتروني على سبيل المثال، أحد العناصر الحيوية في مهامه هو صياغة السياسات الإلكترونية وتطبيقها لتأمين تبادل المعلومات وتخزين البيانات.

التحقيقات الجنائية الرقمية تمثل بُعداً جوهرياً آخر للأمن الإلكتروني، ويشمل التحقيق الرقمي عند حدوث الجرائم التعرف على الجريمة وزمانها ومكانها والجاني وكيفية وقوعها وهو الموضوع الأهم، كي يمكن الحؤول دون تكرارها في المستقبل. العمل الجماعي ومهارات حل المشاكل وامتلاك عقل متفتح تحليلي صفات ثمينة في هذه الوظيفة.

فيما يلي بعض أبرز المسميات الوظيفية التي يحملها خريجو تكنولوجيا المعلومات والأمن الإلكتروني:

- محلل نقاط الضعف/مختبر اختراقات
- مهندس شبكات
- خبير أمن المعلومات/محلل مخاطر سيبرانية
- محلل جرائم سيبرانية
- محلل أدلة جنائية في الجرائم المعلوماتية
- مطوّر برمجيات
- إداري أنظمة
- إداري أمن سيبراني
- مهندس ضمان المعلومات
- اختصاصي أمن تكنولوجيا المعلومات
- تقني دعم الشبكات
- مدير تدقيق تكنولوجيا المعلومات
- المخترق الأخلاقي (المخترق الأبيض)

اتّبع ممارسات تكنولوجية صحية لأسلوب حياة صحي

حقائق ونصائح عن التحكّم الفعّال باستخداماتنا المتزايدة للتكنولوجيا

مع دخول العقد الثالث من القرن الحادي والعشرين أصبحنا أكثر خضوعاً لشريك شديد التحكّم في حياتنا.. إنها التكنولوجيا الرقمية! لقد نمت هذه العلاقة حتى أصبح لا مفرّ منها، ولكن يتعين علينا تحديد مسافة صحية بيننا وبين هذا العالم الافتراضي.

أصبحت مخاطر الاستخدام المفرط للتكنولوجيا أكثر وضوحاً في العصر الحديث، وتتجلى مظاهرها السلبية في قصور الانتباه وتحديات التعلم والسمنة والانسحاب الاجتماعي والإدمان وحتى التشوهات الجسدية بين الأطفال الصغار مثل انحناء العنق أو ما يسمى "عنق الهاتف المتحرك."

ولكن كيف نتوقف عن هذا الإدمان؟

"رهاب فقدان الهاتف المحمول" أو "النوموفوبيا" هو الخوف من عدم وجود هاتفك المحمول بحوذتك أو عدم القدرة على استخدام هاتفك لسبب ما، مثل عدم وجود إشارة الاتصال بالإنترنت أو نفاد البطارية. هذا صحيح، هناك مصطلح رسمي لإدمان الهاتف الذكي!

وتبحث مجلة "إشارات" في هذا الموضوع الصحفي إدمان التكنولوجيا الرقمية لاسيما هوس الهواتف الذكية، وتقدم بعض النصائح العملية للتحكّم بالاستخدام اليومي للتكنولوجيا التي توغلت إلى عقولنا وأصبحت جزءاً مكملاً لأسلوب حياتنا في لمح البصر. يمكننا إصلاح الخلل في ميزان القوة بهذه العلاقة بيننا وبين التكنولوجيا من خلال إدخال بعض القواعد البسيطة إلى حياتنا.

أغلق الهاتف أثناء القيادة

نعرف جيداً أنه لا ينبغي علينا كتابة رسائل نصية أو التحدث عبر الهاتف أثناء القيادة وهناك قواعد صارمة تحظر استخدام الهواتف أثناء القيادة. وبرغم ذلك إلا أن الكثيرين منا لا يزالون يشعرون بأنهم مجبرون على الإجابة عن الهاتف بمجرد سماع الرنين أثناء القيادة على الطرق السريعة.. وبالفعل، كثيرون منا يجدون صعوبة في مقاومة ذلك، لذا كل ما عليك فعله هو إغلاق هاتفك أو وضعه في حقيبتك أو بعيداً عن متناول يدك.

تجاهل التنبيهات والإشعارات

رنات التنبيهات والإشعارات مزعجة للغاية وتزيد من مستوى توترنا حيث إنها مصممة خصيصاً لجذب انتباهنا. إنها تؤرق حياتنا بحسب الدراسات التي أثبتت أن الإشعارات تُعدّ ضمن العوامل الرئيسة لانخفاض مستوى الإنتاجية والتركيز والصحة النفسية. لذلك احرص على اختيار الإشعارات والتنبيهات التي تحتاج إليها فقط - كإشعارات رسائل البريد الإلكتروني أثناء يوم العمل - وأوقف أيضاً جميع تنبيهات مواقع التواصل الاجتماعي والتطبيقات الأخرى، التي يمكنك الاطلاع عليها لاحقاً متى شئت.

لا تأخذ الهاتف الذكي إلى غرفة النوم

الكثير من الأشخاص يدمنون تصفح مواقع التواصل الاجتماعي والتطبيقات الأخرى قبل النوم مباشرةً، مما يؤثر بشكل كبير في جودة النوم، وفي الصباح أول ما يقومون به هو تصفح هواتفهم قبل النهوض من على الفراش، ناهيك عن الضوء الأزرق وأصوات الإشعارات الصادرة من الأجهزة الرقمية ليلاً التي تؤثر بدورها في جودة النوم.. اترك هاتفك في غرفة أخرى قبل النوم واستخدم ساعة المنبه التقليدية للاستيقاظ، وإذا كنت مضطراً لترك هاتفك إلى جانبك فعلى الأقل قم بتفعيل خاصية الوضعية الليلية لتقليل الإشعارات وإزالة انبعاثات الضوء الأزرق.

عش حياة واقعية

اجعل المحادثات وجهاً لوجه ومقابلة الأصدقاء على قائمة أولوياتك؛ فهذه اللقاءات المباشرة مع الآخرين هي المحفّز الأول لصحة الإنسان وسعادته. ولأن التكنولوجيا الرقمية ووسائل التواصل الاجتماعي لن تزيدك إلا عزلة وشعوراً بالوحدة، فليس هناك حاجة لها على الإطلاق عندما تكون برفقة الأصدقاء والعائلة. ولتفادي استخدامها يمكنك ضبط هاتفك على الوضعية الصامتة أو وضعه في مكان آمن بعيداً عنك.

استمتع بالتنزه في الهواء الطلق

جميعنا نعمل بلا كلل في هذه الحياة السريعة الوتيرة، فكيف نستغل أوقات فراغنا ونستمتع ببعض الهدوء والسكينة؟ عادةً ما نستخدم هواتفنا لتصفح التطبيقات والرسائل، وهذه ليست سوى عادة سيئة نلجأ إليها خوفاً من الشعور بالوحدة والملل، لكنها في النهاية تمنحنا بعضاً من الراحة المزيفة. إذا توقفت عن الانغماس في الحياة الافتراضية التي تفرضها عليك التكنولوجيا الرقمية، فسوف تكتشف أن لديك الكثير من الوقت يومياً للاستمتاع بأجواء مفعمة بالهدوء والاسترخاء والسكينة في الحياة الواقعية.

تخلّص من مصادر الإلهاء

جميعنا، من دون استثناء، لدينا حياة واحدة فقط علينا الاستفادة من كل لحظاتها في العمل والترفيه وتطوير الذات ومساعدة الآخرين والمساهمة في تقدم المجتمع.. لذلك يجب علينا أن نقلل من استخدام هواتفنا قدر الإمكان ونمضي مزيداً من الوقت مع الأصدقاء والعائلة أو ممارسة الرياضة لأنها الحل الوحيد للتمتع بصحة نفسية جيدة وحياة اجتماعية مثالية. بالرغم من أن التكنولوجيا تثري حياتنا إلا أنها قد تجرّد الحياة من معناها الحقيقي إذا تركناها تتحكم بنا.

استمتع بيوم كامل من دون هاتف

تذكر أن الناس في الماضي كانوا يمضون حياتهم ويمارسون أعمالهم ويستمتعون بأوقاتهم من دون هواتف ذكية وكانت حياتهم الاجتماعية أفضل بكثير من الآن.. قد يبدو الأمر مستحيلاً بالنسبة إليك، ولكن إذا تعمدت ترك هاتفك في المنزل ليوم واحد في الأسبوع وخرجت من دونه، فسوف تتمكن من التخلص من شعور "الخوف من أن يفوتك شيء" وسوف تحظى بالوقت الكافي لملء حياتك بنشاطات اجتماعية مختلفة.

رتّب خزانتك الرقمية

إذا كنت ترغب في أخذ خطوة جدية والتخلص من مصادر الإلهاء الرقمية، فعليك التخلص من التطبيقات المستنزفة للوقت وتخفيف الحمل على أجهزتك قدر المستطاع. هل يمنعك خوفك من فعل ذلك؟ حاول محو تطبيق واحد في كل مرة كلما واتتك الشجاعة أو إذا شعرت بالملل، وسرعان ما ستشعر أنك في الحقيقة لا تفتقد هذه التطبيقات والألعاب وصفحات التواصل الاجتماعي التي تمنعك من الاستمتاع بحياتك الطبيعية.. إن أفضل حلّ للاستمتاع بحياة صحية هو التحول إلى الأنشطة الأقل اعتماداً على التكنولوجيا.

بعض الإحصاءات الصادمة حول الهاتف الذكي

أفادت دراسات بحثية حول الصحة الرقمية أجريت خلال عامي 2018 و2019
بالإحصاءات الحديثة التالية حول استخدامات الهواتف الذكية بمختلف أنظمتها:

%68 نسبة الأشخاص الذين يتصفحون هواتفهم قبل مرور 5 دقائق من استيقاظهم في الصباح

63 متوسط عدد المرات التي يفحص فيها مستخدم الهاتف الذكي هاتفه

%54 نسبة الأشخاص الذين يقاطعون محادثاتهم المباشرة مع الآخرين لإجراء مكالمة أو التحقق من الإشعارات

76 دقيقة متوسط الوقت الذي يمضيه المستخدمون في استخدام تطبيقات التواصل الاجتماعي الخمسة الشهيرة

%86 نسبة الأشخاص الذين يتصفحون هواتفهم أثناء محادثاتهم مع الأصدقاء أو أفراد العائلة

2,617 متوسط عدد المرات التي يقوم فيها المستخدمون بالنقر أو فتح هواتفهم يومياً

تأثير التكنولوجيا المتقدمة في جسم الإنسان

بالإضافة إلى تعلّقنا الشديد بالهاتف الذكي، يقضي معظمنا أكثر من نصف يومه على كرسي العمل محدقين في شاشات الكمبيوتر. إليك بعض الآثار السلبية للجلوس لفترات طويلة أمام الشاشات:

- ألم في الظهر
- صداع مزمن
- رؤية مشوشة وإرهاق العينين
- زيادة الوزن (أو نقصان الوزن لدى مستخدمي ألعاب الفيديو على سبيل المثال)
- متلازمة النفق الرسغي (تلف الأعصاب التي تؤثر في الذراع والمعصم واليد)
- الوذمة (تورم الساقين والقدمين)
- اضطرابات النوم

قد يكون من الصعب تجنب التكنولوجيا إذا كانت حياتك اليومية أو وظيفتك تتضمن استخدام أجهزة الكمبيوتر والأجهزة التقنية الأخرى. لذلك، دعنا نلقي نظرة على بعض الطرق التي يوصي بها الخبراء للحد من الآثار السلبية للتكنولوجيا في أجسامنا.

اجلس بوضعية مستقيمة

تحقق من وضعية جلوسك؛ إذا كانت أذناك لا توازي كتفيك، فهذا يعني أنك تنحني للأمام. سوف يعمل تراخي الجسم على إضعاف عضلات بطنك وظهرك بمرور الوقت، لذلك تأكد من الجلوس بشكل مستقيم.

قم بتهيئة مكتب عملك

يجب أن تكون شاشة الكمبيوتر أمامك مباشرة وبمستوى العينين.

احرص على إرخاء عضلاتك

يجب أن يكون معصمك مستقيماً ومسترخياً أثناء الكتابة حتى لا تصبح عضلاتك مشدودة، وتصاب رقبتك بالإجهاد.

أرح عينيك

هل تعلم أن أعيننا تغمض بدرجة أقل أثناء التحديق في الشاشات؟ كما أن التركيز المستمر أمام الشاشة يضعف عضلات العين. لذا احرص على النظر عبر النافذة أو إلى اتجاه آخر داخل المكتب لإراحة عينيك قليلاً.