#أمنك_مسؤوليتك

أهمية الأمن الرقمي للحفاظ على سلامتنا

ما هي التهديدات الإلكترونية وما عقوبة مرتكبيها؟

أهمية الأمن الرقمي للحفاظ على سلامتنا
ما هي التهديدات الإلكترونية وما عقوبة مرتكبيها؟

المخاطر الأمنية تحيط بنا، بوجود منظومات مراقبة تتعقبنا وتتعدّى على خصوصيتنا، وذلك طبعاً دون علمنا أو اختيارنا.

أينما كنت تتجوّل في ساحات العالم الافتراضي، أنت معرّض للاختراق، فالأجهزة التي تستخدمها والتي تبدو بريئة المظهر، تجمع عنك الكثير من معلوماتك الشخصية، حتى في الأوقات التي تظن أنك قد اتخذت كل التدابير الكفيلة بالحفاظ عليها، وأغلقت جميع الأبواب التي قد تؤدي إلى تجاوزها.

معلوماتك الشخصية وبياناتك اليومية مثل أماكن تواجدك وتوجهاتك السياسية وتاريخك الشرائي، باتت سلعاً تجارية تُباع وتُشترى لتفصيل منتج على مقاس اهتماماتك، يُوجه إليك خصيصاً عبر إعلانات تظهر لك دون مشورتك، أينما كنت تتصفح أو تُطالع، والحقيقة المُرّة أنه ثمة من يجني ملايين الدولارات من عمليات الاختراق الإلكتروني وسرقة المعلومات، فضلاً عما تقوم به الحكومات في بعض الدول من مراقبة لنشاطات الأفراد وتوجهاتهم.

> **"لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمسّ شرفه وسمعته، ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات".**
>
> المادة 12 من الإعلان العالمي لحقوق الإنسان

وهنا تُطرح التساؤلات حول كيفية العمل في بيئة أكثر أمناً بعيداً عن مختلف أنواع التهديدات الإلكترونية التي تواجهنا من جهات عدة، في الوقت الذي أصبح فيه استخدام شبكة الإنترنت ووسائل التواصل الاجتماعي حاجة يومية يستحيل الاستغناء عنها.

ما هو الأمن الرقمي؟

الخصوصية الرقمية وحماية المعلومات الحساسة مواضيع يختصّ بها "الأمن الرقمي"، والذي يمكن تعريفه على أنه "مجموعة الأدوات والتطبيقات التي يتم استخدامها لحماية المعلومات على الحاسوب والإنترنت".

يتيح "الأمن الرقمي" لنا من خلال إجراءات أمنيّة احترازية بسيطة ومتاحة، القدرة على التحكم بالمخاطر والتهديدات الإلكترونية إلى حد كبير، في الوقت الذي قد يؤدي إهمال تلك الإجراءات إلى نتائج كارثية لا تحمد عقباها، قد لا تستثني أياً منّا، فحالات الاختراق والقرصنة والابتزاز وسرقة البيانات والتعدّي على الخصوصية والملكية الفكرية باتت حوادث نسمع عنها بشكل يومي.

ويشهد عالم "الأمن الرقمي" تغييرات مستمرة، يحاول من خلالها خبراء الأمن اكتساب مزيد من المعرفة حول ما يجري، للتخفيف من الآثار المترتبة على الحوادث الإلكترونية، وهو ما يوجب علينا مواكبة هذه المستجدات وتحديث معرفتنا بالممارسات الأمنية وإعادة تقييمها بشكل دوري.

أهمية الأمن الرقمي:

تأتي أهمية الأمن الرقمي لحماية أنفسنا من التهديدات الإلكترونية المتمثلة بـ:

1. **البرمجيات الخبيثة:**

هي برمجيات مصممة للقيام بأفعال غير مرغوب بها على جهاز المستخدم دون علمه أو موافقته بهدف إيذائه، وقد تعمل هذه البرامج على سرقة كلمات السر أو تسجيل أنشطة المستخدم بشكل سري أو حذف بياناته، ويتراوح أذاها من مجرد عرض الإعلانات، إلى تدمير القرص الصلب وعرقلة نظام التشغيل.

ومن أشهرها: الفيروسات، والديدان، وأحصنة طروادة.

توقعت شركة الأبحاث "كاسبرسكي" في تقرير لها أن تصل تكلفة الخسائر التي يتكبدها العالم جراء الهجمات الإلكترونية لنحو 6 تريليون دولار سنوياً بحلول عام 2021.

2. **هجمات الفدية:**

سُمّيت بذلك لأنها تعمل على تشفير حاسوب الضحية مقابل مبلغ من المال يُدفع لمن يقف وراءها "قراصنة الإنترنت"، مقابل فك التشفير مرة أخرى.

من الطرق التي يعتمدها القراصنة للاختراق: رسالة بريد إلكتروني تتضمّن مرفقاً مُلوثاً بالفيروس، الروابط الملغومة، المواقع الوهمية.

3. **برمجيات التجسس:**

وهي البرامج التي تنقل معلومات من جهاز المستخدم إلى مكان آخر عبر شبكة الإنترنت دون علمه، عبر مراقبة الكتابة، أو المواقع الإلكترونية التي يزورها، وتجميع المعلومات الشخصية المتنوعة عنه، وقد يكون ذلك بهدف سرقة المعلومات مثل كلمة المرور، أو التجسس لأغراض تجارية.

وهي ليست برامج نقوم بتنصيبها، وإنما إحدى الإضافات التي قد تكون موجودة مع برنامج آخر، وتكون عادةً مخفيّة عن أنظار المستخدمين ومن الصعب جداً رصدها.

هاجم فيروس الفدية الخبيث "WannaCry" يوم 12 أيار من عام 2017 آلاف الشركات على مستوى 150 دولة حول العالم متسبّباً في خسائر قُدّرت بمليارات الدولارات .

وقام هذا الفيروس بتشفير كل البيانات الموجودة على أجهزة حواسيب الشركات المخترقة، وإعطاء مهلة 6 ساعات لدفع فدية بقيمة 300 $ عن طريق العملة الإلكترونية Bitcoin لاسترداد الملفات المشفرة.

4. انتحال الشخصية:

يعمد منتحل الشخصية إلى استخدام هوية شخص آخر في العالم الافتراضي، وذلك بهدف الحصول على معلومات سرية أو أمنية أو مبالغ مالية مستخدماً اسم الشخص وكلمة المرور الخاصة به، والتي قد يستوحيها من مواليد الشخص أو غيرها من المعلومات التي قد تكون متاحة على مواقع التواصل الاجتماعي، والتي يرى فيها المنتحلون كنزاً معروضاً أمامهم لاستخدامها في عملياتهم الاحتيالية.

أو قد يقوم المنتحل بإرسال رسالة تتضمن روابط صفحات مشابهة تماماً للموقع الأصلي طالباً من المستخدم معلومات معيّنة عنه، كأن يطلب تحديث بياناته البنكية أو معلومات سرّية أخرى.

وفي أحيان أخرى قد يلجأ المنتحل إلى الاتصال المباشر بالشخص المستهدف وطلب معلومات سرية بحجة أنه بحاجة إليها لتحديث النظام كونه يعمل في شركة الاتصالات.

أبلغت شركة الأمن السيبراني الأمريكية "فاير آي" يوم 14 من شهر تشرين الثاني/ نوفمبر 2018، عن انتحال قراصنة إنترنت شخصية مسؤول الشؤون العامة في وزارة الخارجية الأمريكية، مستهدفين وكالات حكومية وشركات ومراكز بحثية، من خلال إرسال رسائل بريد إلكتروني تدّعي أنها قادمة من المسؤول.

واتهمت الشركة مجموعة روسية اسمها "كوزي بير" يُعتقد أنها مرتبطة بالمخابرات الروسية، ولها صلة بعمليات القرصنة التي تمت قبيل انتخابات الرئاسة الأميركية لعام 2016 بالقيام بعملية الانتحال.[1]

5. التصيد:

وهو محاولة للحصول على معلومات شخصية أو مالية للشخص المستهدف، عن طريق إرسال رسائل إلكترونية زائفة قد تحتوي على روابط تقوم بتوجيه المستخدم إلى مواقع الكترونية مُصمّمة خصيصاً لسرقة معلومات المستخدم.

كما قد يقوم المتصيد بتحميل برامج خبيثة على جهاز الضحية تسمح له بالوصول إلى معلوماته، أو قد يستخدم أسلوب "الهندسة الاجتماعية" دون اللجوء إلى أي أدوات، وذلك عبر خداع الضحية واستدراجه للحصول على ما يرغب فيه.

---

[1] "قراصنة إنترنت روس ينتحلون شخصية مسؤول أميركي كبير"، العربية نت، ١٧تشرين الثاني/نوفمبر ٢٠١٨، https://www.alarabiya.net/ar/arab-and-world/american-elections-2016/2018/11/17/%D9%82%D8%B1%D8%A7%D8%B5%D9%86%D8%A9-%D8%A7%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%B1%D9%88%D8%B3-%D9%8A%D9%86%D8%AA%D8%AD%D9%84%D9%88%D9%86-%D8%B4%D8%AE%D8%B5%D9%8A%D8%A9-%D9%85%D8%B3%D8%A4%D9%88%D9%84-%D8%A3%D9%85%D9%8A%D8%B1%D9%83%D9%8A-%D9%83%D8%A8%D9%8A%D8%B1-.html.

هل يعاقب القانون مرتكبي الجرائم الإلكترونية؟

نعم إذ يوجد قسم مختص بهذا النوع من الجرائم في أغلب بلدان العالم.

القوانين المختصة بارتكاب جرائم إلكترونية في سوريا:

وقعت سوريا على اتفاقية محاربة الجريمة الإلكترونية عام 2010، والتي حددت الجرائم المتعلقة بأمن الدولة الخارجي والإرهاب، وتلك المرتكبة بواسطة تقنية المعلومات، والجرائم المتعلقة بالجريمة المنظمة كالإتجار بالأشخاص أو تجارة الأسلحة أو الأعضاء البشرية.

في عام 2012 صدر المرسوم التشريعي رقم (17) المتعلق بتطبيق أحكام قانون التواصل على الشبكة ومكافحة الجريمة المعلوماتية.

المادة (23) المتعلقة بانتهاك حرمة الحياة الخاصة:

يُعاقب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية كل من نشر عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه حتى ولو كانت تلك المعلومات صحيحة.

المادة (15) المتعلقة بالدخول غير المشروع إلى منظومة معلوماتية:

يُعاقب بالغرامة من عشرين ألف إلى مئة ألف ليرة سورية، من يرتكب جريمة "الاختراق" أو "التهكير"، والحبس من ثلاثة أشهر إلى سنتين، وبالغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية إذا قام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل إليها أو ألغاها أو غيرها أو قام بتشويهها أو استخدامها أو إفشائها.

المادة (19) المتعلقة بتصميم البرمجيات الخبيثة واستخدامها:

يُعاقب بالحبس من ثلاث إلى خمس سنوات وبالغرامة من خمسمئة ألف إلى مليونين ونصف المليون ليرة سورية، كل من يقوم بتصميم البرمجيات الخبيثة وترويجها لأغراض إجرامية، كما يعاقب بالحبس من ستة أشهر إلى ثلاث

أظهر تقرير بعنوان: "المخاطر العالمية التي تتهدّد أمن تقنية المعلومات 2018" والذي أعدته شركة "كاسبرسكي لاب" المتخصصة في أمن أجهزة الحواسيب، أن 75 ٪ من الشركات الكبيرة في الشرق الأوسط تعرضت لهجومين إلكترونيين موجهين أو أكثر في عام 2018، وأن نحو ثلث هذه الشركات واجه هجوماً إلكترونياً موجهاً واحداً.

وقد أدت الهجمات على الشركات التجارية إلى خسائر مالية وصلت تكلفتها في المتوسط إلى مليون دولار.

وأشار التقرير إلى أنّ التحديات الثلاثة الأولى الماثلة أمام الشركات في منطقة الشرق الأوسط وتركيا وإفريقيا، عند مواجهة الهجمات الموجهة، تكمن في: الافتقار إلى المعلومات 35 %، ونقص الرؤية في الحوادث التخريبية 26 %، وعدم القدرة على اكتشاف تهديد حقيقي في خضمّ العديد من الإنذارات 23 %.

سنوات والغرامة من مئتي ألف إلى مليون ليرة سورية كل من استخدم البرمجيات الخبيثة أياً كان نوعها وبأي وسيلة بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية.

ولكن هذا المرسوم بقي حبراً على ورق إلى أن تم إصدار القانون رقم (9) في 25 آذار لعام 2018، المتعلق بإحداث محاكم جزائية مختصة بالنظر في الجرائم الإلكترونية، تتألف من قضاة ومساعدين يستعينون في عملهم بمختصين في مجال التقانة للقيام بالمهام الموكلة إليهم.

المؤسسات المشاركة بالحملة:

منظمة سوريون من أجل الحقيقة والعدالة: منظمة سورية مستقلة، تأسست عام 2015، تعمل على توثيق انتهاكات حقوق الإنسان في سوريا، وقضايا المناصرة في المحافل الدولية.

جريدة عنب بلدي: مؤسسة إعلامية سورية مستقلة تأسست عام 2011 في مدينة داريا بريف دمشق، وتصدر مطبوعة أسبوعية، سياسية، اجتماعية، منوعة.

راديو روزنة: إذاعة سورية انطلقت عام 2013، تقدم نشرات ومواجز إخبارية متعددة وبرامج ثقافية وتوعوية وخدمية متنوعة، وتنشط أيضاً عبر موقعها الإلكتروني.

الشبكة السورية للإعلام المطبوع: تأسست عام 2014، وهي تجمّع لصحف ومجلات سورية مستقلة، تعمل على تنسيق الجهود فيما بينها من خلال تبادل الخبرات الصحفية والمهنية.

منظمة آرتا للإعلام والتنمية: وهي منظمة غير حكومية غير ربحية، مقرها في مدينة عامودا بمحافظة الحسكة، تعمل على تطوير مشاريع إعلامية مستقلة وتدريب ودعم صحفيين.

مشروع سلامتك: تأسس عام 2012، يهدف لنشر التوعية والمساعدة حول الأمن الرقمي، عبر تقديم الدعم التقني للمنظمات السورية، والمساعدة التقنية عبر الإنترنت، والتدريب الميداني.

موقع أنا إنسان: يركز على نشر القصص الإنسانية، وبشكل خاص قصص السوريين، بهدف طرح ومعالجة قضايا متعددة، وتوثيق معاناتهم والانتهاكات التي ارتُكبت بحقهم، إلى جانب عرض تجارب نجاحهم وإنجازاتهم.

#أمنك_مسؤوليتك