منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

الأمن السيبراني

المحتويات

التعريف بالأمن السيبراني

يُعرف بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنية الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج ولا تتحول الأضرار الى خسائر دائمة ، بالإضافة إلى ماذكر في التقرير الصادر عن الاتحاد الدوليّ للاتصالات حول "اتجاهات الإصلاح في الاتصالات للعام 2010-2011": حيث أنه يُعد مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية، ومقاربات لإدارة المخاطر وتدريبات وممارسات فضلى وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين.

الهيئة الوطنية للأمن السيبراني:

عرف تنظيم الهيئة الأمن السيبراني على أنه: "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوها".

ويمكن الاطلاع على اختصاصات الهيئة من خلال موقع الهيئة الرسمي.

الأخطار والتهديدات:

مع الاعتماد المتزايد في حياتنا اليومية على الأنظمة المعلوماتية والأجهزة المتصلة بالشبكة العالمية للمعلومات، وتشعّب طبيعة هذه الأجهزة من هواتف خلوية وأجهزة حوسبة شخصية، يزداد عدد المتصلين بالفضاء السيبراني، وتزداد احتمالات الاعتداءات والجريمة، مع وجود حوادث تعبر عن اختراق الأنظمة وسرقة البيانات وتسربها، كاختراق أنظمة معلومات سوني، التي نتج عنها تسرب بيانات مليون مستخدم، فالمعلومات التي تضخ وتنساب وتحفظ في الفضاء السيبراني وعبره، من أهم الموجودات التي يسعى إليها جميع المعنيين بهذا الفضاء دون استثناء. فالشركات والحكومات ومستخدمو الإنترنت يلاحقون المعلومات كلٌ بحسب أهدافه، وتصدر الأخطار والتهديدات السيبرانية عن أعمال ذات مغزى كالاختراقات والاعتداءات، وأعمال بلا هدف كالإهمال وقلة الوعي والإدراك.

التعريف بالأمن السيبراني

مقارنة بين أمن المعلومات والأمن السيبراني

أمن المعلومات	الأمن السيبراني
القيام بحماية المعلومات التي قد تكون على هيئة وثائق ورقية أو إلكترونية وحمايتها من الوصول غير المُصرح به	يهتم بأمن المعلومات التي يتم نقلها أو تخزينها أو معالجتها في أنظمة الاتصالات وتقنية المعلومات
يهتم بمجالات ضخمة كالتشفير والتخزين والتأمين الفيزيائي والمعايير الأمنية، وإدارة أمن المعلومات والمخاطر وغيرها من المجالات	يهتم بوسائل الحماية والدفاع عن كل أنظمة الحواسيب والشبكات الذكية؛ فهو لا يركز كثيرًا على الوسائل التأسيسية -كوسائل التشفير مثلاً- بقدر تركيزه على الإفادة من هذه الوسائل في الدفاع الرقمي
يهتم بحماية المعلومات بطريقة لاتقل أهمية عن توافر الخدمات الإلكترونية	يعمل على توفير الخدمات وسلامتها من خلال تقديمها عبر الفضاء السيبراني كالطاقة الكهربائية
النسخ الاحتياطي للبيانات	يهتم بنسخ البيانات وتشفيرها
تحديث الأنظمة وزيادة أمنّها	تحديث الأنظمة وحمايتها والتوعية ومحاربة البرمجيات الخبيثة

أمن المعلومات أشمل وأوسع من الأمن السيبراني

محاور الأمن السيبراني

المحور الأول: محور أساسيات الأمان

أولًا: السرية

هي الحفاظ على خصوصية البيانات ومنع الإفصاح عنها للأشخاص غير المصرح لهم، وتتم عن طريق:

1. حماية البيانات والخصوصية

أنواع المعلومات والبيانات:

المعلومات الشخصية Personal information	المعلومات داخل منظمة Organization information	المعلومات الدولية International information
1. معلومات عامة 2. معلومات خاصة 3. معلومات عائلية 4. معلومات محظورة	1. بيانات الموظفين 2. بيانات الملكية الفكرية 3. بيانات مالية	1. بيانات المقيمين والمواطنين 2. بيانات مالية اقتصادية 3. الوثائق العسكرية

2. التحكم بالوصول إلى المعلومات :

ويتم التأكد من هوية المستخدم قبل السماح له بالدخول إلى النظام عن طريق ثلاثة أشياء:

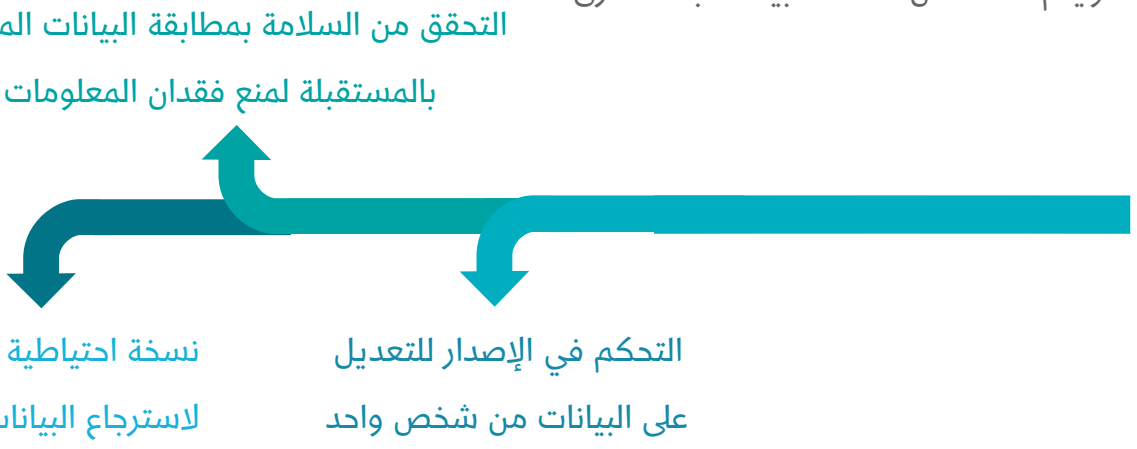
1. شيء فريد بك دون غيرك، مثل بصمة الأصبع أو العين
2. شيء تملكه، مثل البطاقة الشخصية
3. شيء تعرفه، مثل كلمة المرور

محاور الأمن السيبراني

ثانيًا: السلامة

وتعني دقة وتطابق البيانات في كل مراحلها من تخزينٍ واسترجاعٍ ونقلٍ وأن يتم التعديل عليها من قبل الأشخاص المصرح لهم.

ويتم التأكد من سلامة البيانات بعدة طرق:



ثالثاً: توفر البيانات

وتعني ضرورة توفر المعلومات بشكلٍ دقيق، بالإضافة لاكتشاف ضعف وبطء النظام عند حدوثه، وبالتالي العمل على تخفيف الضغط على النظام.

رابعًا: الهوية الشخصية

وهي كل ما يدل على شخص بعينه، حيث هناك نوعين من الهوية الشخصية:

- الهوية الحقيقية: وهي المعلومات الشخصية الحقيقية التي يعرفك بها الناس في الواقع
- الهوية الإلكترونية: هي كل ما اخترت مشاركته ونشره عنك في الفضاء الإلكتروني

خامساً: الأثر الرقمي (Digital Footprint)

وهي البيانات التي تدل على الشخص إما بشكلٍ مباشر أو غير مباشر

مباشر

مثل البيانات التي ينشرها الشخص عن نفسه للحصول على خدماتٍ معينةٍ أو المنشورات على وسائل التواصل الاجتماعي.

غير مباشر

وهي كل ما يتعلق بنشاطه على الشبكة مثل مشترياته والمواقع التي يزورها والمواضيع التي يبحث عنها.

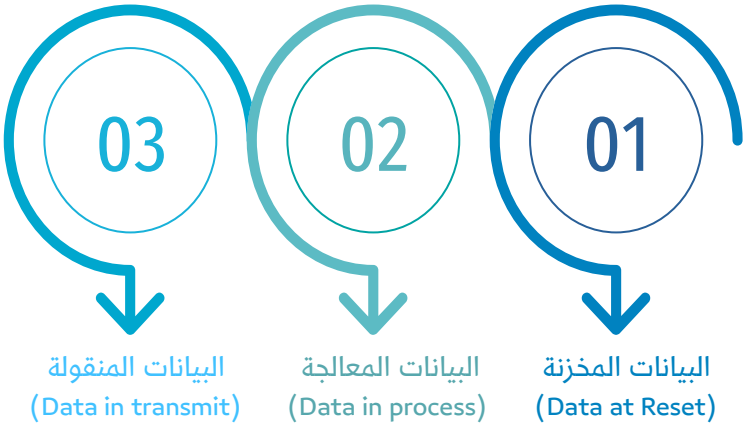
محاور الأمن السيبراني

سادسًا: ملفات الارتباط (Cookies)

هي ملفات برمجية نصية صغيرة جدًا تخزن في جهاز المستخدم عند زيارته لموقع ما بحيث تسهل عملية تصفح المواقع وتعتبر هذه الملفات نصية غير تنفيذية لذلك التصنيف ولا تعامل على أنها برامج خبيثة بالرغم من أنها أول ما يتم سرقته من قبل المخترقين لمعرفة حساباتك وكلمات المرور الخاصة بك.

المحور الثاني: حالات المعلومات

حالات المعلومات (Data Statuses)



المحور الثالث: الاحتياطات

01 التوعية والمعرفة بأساليب الاختراق والحروب السيبرانية

02 عمل نسخ اختياطية بشكل دائم وحفظها في مكان آمن

03 تحديث البرامج ونظام التشغيل بشكل مستمر

04 فحص الأجهزة والبرامج قبل استخدامها

الفيروسات

يعتبر التعرض لهجمات فيروسيّة هجمات سيبرانيّة تؤدي إلى تعطّل المنظمات لذا يجب الحماية منها.

تعريف الفيروسات:

هو برنامج تخريبيّ تتم برمجته على أيدي محترفين، بحيث يُحدث هذا البرنامج خللاً في خصائص الملفات التي يستهدفها ليجعلها تحت سيطرة المبرمج من خلال حذف جميع مستندات هذا الملف أو تخريبها أو التعديل عليها، وتكون الغاية من هذه البرامج تخريب أجهزة الحاسوب الخاصة بالمستخدمين، وكما قد يكون الهدف منه الحصول على ملفاتٍ وبياناتٍ مهمةٍ من جهازٍ مستخدمٍ ما.

تمتاز فيروسات الحاسوب بعدّة صفات، منها:

- التلقائيّة في القدرة على التناسخ والانتشار
- الرّبط الذّاتي للفيروس مع برنامج يطلق عليه الحاضن (Host)
- غير قابلة للنشوء من تلقاء ذاتها
- فيروس الحاسوب مرضٌ حاسوبيٌّ معدٍ

تصنف مكونات برنامج فيروس الحاسوب إلى أربعة مكونات رئيسية وهي:

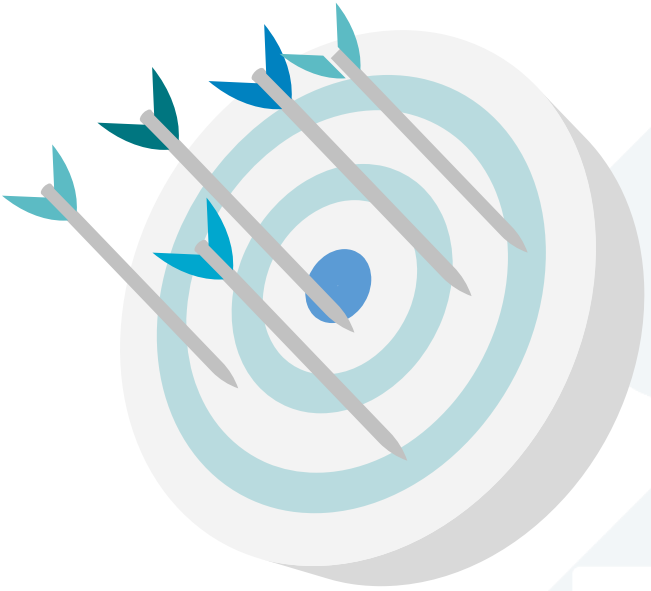
التّناسخ (Replication)	هو أحد أجزاء برنامج الفيروس الذي يمنحه خاصية التناسخ والانتشار
التّخفّي (Protection)	يضفي هذا الجزء خاصية السرية وعدم القدرة على الكشف عن وجوده بسهولة
التّنشيط (The Trigger)	يعطي هذا الجزء خاصية القدرة على الانتشار قبل اكتشافه ويكون غالبًا ضمن توقيت معين
التّنفيذ (The Payload)	المهمة المنّاطة بالفيروس لتنفيذها عند بدء النشاط وانتشاره

الفيروسات

تنتقل الفيروسات في الحاسوب بطريقتين رئيسيتين، وهما:

- العدوى المباشرة (Direct Infector): يغزو الفيروس ملفات الحاسوب وعندما يتم تشغيل أو استخدام أحد هذه الملفات فإن الفيروس يبدأ بنشاطه وانتشاره وينتقل بين الملفات الموجودة على جهاز الحاسوب، وفور انتقال العدوى لأيّ ملف فإنه يتم تحميله ونقله إلى الذاكرة تلقائيًا ومن ثم تشغيله.
- العدوى غير المباشرة (Indirect Infector): ينقل البرنامج المصاب بالفيروس إلى ذاكرة جهاز الحاسوب فور بدء تشغيل الملف المصاب وينفذ الحاسوب أوامر الملف الأصليّ، وبعد ذلك تنتقل الإصابة بالفيروس لأيّ ملفٍ يتم تحميله إلى الذاكرة، ويتوقف هذا النوع من الانتشار في حال فصل التيّار الكهربائيّ عن جهاز الحاسوب أو إعادة التشغيل، مثل ملف وورد مصاب.

ينصح المستخدم عادةً بحماية جهازه من الفيروسات والوقاية منها وذلك باتباع الخطوات التالية:



01 عدم تحميل أي برنامج بدون إجراء الفحص الكامل

02 تحميل البرامج الخاصة للكشف عن وجود الفيروسات، وعدم تشغيل ملفات مجهولة المصدر

03 الاحتفاظ بنسخ احتياطية للملفات والبرامج

04 الاعتماد على برامج الجدار الناري

05 تنصيب أنظمة تشغيل أكثر أمانًا كنظام جنو/لينكس

حماية حساباتك في مواقع التواصل الاجتماعي:

- حماية حسابك في تطبيق Snapchat
- حماية حسابك في WhatsApp

وللمزيد يمكنك الاطلاع على المواد التوعوية المنشورة على موقع المركز الوطني الإرشادي للأمن السيبراني.

المركز الوطني الإرشادي للأمن السيبراني
SAUDI CERT

الجريمة السيبرانية

تتعدّد التّعريفات لمصطلح الجرائم السيبرانية تبعًا لتعدّد اختلاف وجهات نظر الباحثين، ومن أبرزها ما يلي:

- الدخول بغير وجه حق إلى جهاز حاسب مستقل أو مرتبط بآخر بواسطة شبكة محلية بغرض ارتكاب فعّل يحرمه الشرع والقانون.
- استخدام الأجهزة التقنية الحديثة مثل الحاسب الآلي في تنفيذ أغراض مشبوهة وأمور غير أخلاقية لايرتضيها المجتمع لأنها منافية للأخلاق العامة.
- فعل غير مشروع ناتج عن إرادة يقرر لها القانون عقوبة، بحيث يتم ارتكابها بواسطة نظام حاسوبي ويُقصد بها أي جريمة يتم ارتكابها في البيئة المعلوماتية.

أنواع الجرائم السيبرانية

تصنف الجرائم السيبرانية لأربعة أقسام رئيسية وذلك تبعًا لـ:

01 لمرتكبها ودوافعه وطرق التنفيذ

مثل المخترقين كالهاكر المتطفل والحاقدين والمحترفين

02 لمساسها بالأشخاص والأموال

المساس بالأشخاص: كانتحال الشخصية أو التشهير
المساس بالأموال: كالتزوير والسرقة

03 المساس بأجهزة الحاسب والنظم والبيانات

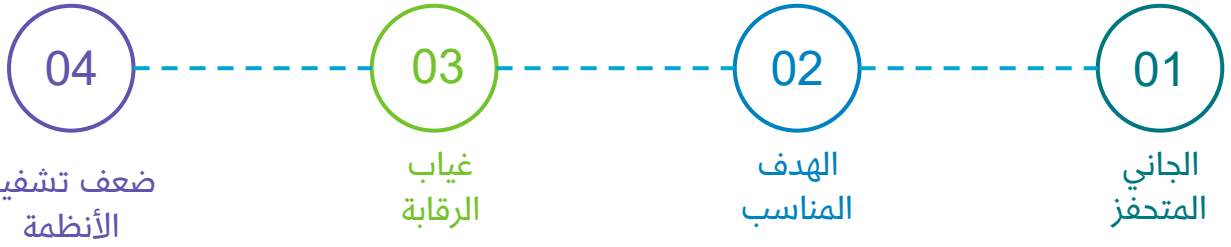
المساس بالبيانات والمعلومات: مثل التزوير في المعلومات أو الاعتداء على البيانات
المساس بالحاسب والنظم: كالاختراق

04 المساس بالنظام العام والآداب

كالجرائم السيبرانية لتجارة المخدرات ونشر الإباحية أو لقرصنة الخصوصية

الجريمة السيبرانية

تحدث الجريمة السيبرانية بعد تحقق عناصرها الأربعة :



تطبيق كلنا أمن للتّبليغ عن أيّ جريمة تحصل لك من تهديدٍ أو ابتزازٍ أو مضايقةٍ في برامج التواصل الاجتماعي؛ وذلك بتصوير الحدث وإرفاق صورةٍ مع موضوع الطلب وإرسالها إلى قسم الجرائم المعلوماتية في الدّوريات الأمنية، حيث يتم علاج الجريمة وتطبيق القانون بحقّ مرتكبها.

قانون ونظام الجرائم السيبرانية في المملكة العربية السعودية

إدراكاً من المملكة العربية السعودية بأهمية مواكبة تطورات التقنية الحديثة مع تحقيق الأمن المعلوماتيّ للفرد والمجتمع وللحدّ من إساءة استخدام النظم المعلوماتية وسدًّا للفراغ النظاميّ في هذا الجانب فقد صدر المرسوم الملكيّ الكريم رقم (م/17) وتاريخ 8/ 3/ 1428هـ بالموافقة على نظام مكافحة الجرائم المعلوماتية من خلال تحديد تلك الجرائم والعقوبات المقررة لها وجهات الاختصاص.

وقد اشتمل النظام على (16) مادّة تضمّنت التعريفات بالألفاظ والعبارات التي تخص النظام، والهدف من النظام وعقوبات مرتكب الجرائم المعلوماتية ومسؤولية هيئة الاتصالات وتقنية المعلومات.

منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority