# الأمن السيبراني
# CYBER SECURITY

يعيش الانسان في ثورة تكنولوجية هائلة أدت إلى ظهور تحدي جديد يواجه الأفراد والمجتمعات والحكومات، وهو زيادة التهديدات الإلكترونية التي منها السرقة والنصب والاحتيال والابتزاز، الأمر الذي يؤدي إلى عواقب وخيمة تضر بالفرد والمجتمع والحكومات لذا توجب البحث على حل هذه المشكلة عن طريق الأمن السيبراني الذي يعمل على الوقاية من الجرائم الإلكترونية والحد من حدوثها

# مفهوم السيبرانية

السيبرانية: تطلق كلمة (سيبر CYBER)على أي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي فالسيبرانية تعني (فضاء الإنترنت)

# مفهوم الأمن السيبراني

- هو عبارة عن مجموعة من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تامين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية أجهزة الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف أو عبث.

# تاريخ إنشاء الأمن السيبراني

- صدر امر ملكي بإنشاء هيئة باسم (الهيئة الوطنية للأمن السيبراني) في عام ٢٠١٧م ترتبط بمقام خادم الحرمين الشريفين، وهي الجهة المختصة بشؤون الأمن السيبراني في المملكة، وتعد مرجع الدولة لحماية أمنها الوطني، ومصالحها الحيوية، والبنية التحتية الحساسة فيها، وتوفير خدمات تقنية امنة وطرق دفاعية لحماية أنظمة المعلومات والاتصالات ضد الهجمات الإلكترونية، والحفاظ على سرية وسلامة المعلومات.

# أهمية الأمن السيبراني

أن أهمية الأمن السيبراني يقوم في تامين المعلومات الحساسة البالغة لأهمية الدول والأفراد على حد سواء المعرضة للخطر والاختراق والاستيلاء للمحافظة على الأمن الوطني وحفظ وحماية السرية والخصوصية للبيانات الشخصية للمواطنين وأجهزة وأنظمة الدولة.

# أهداف الأمن السيبراني

- -تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
- -التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص
- -توفير بيئة امنة موثوقة للتعاملات في مجتمع المعلومات.
- -صمود البني التحتية الحساسة للهجمات الإلكترونية.
- -توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- -التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
- -سد الثغرات في أنظمة أمن المعلومات.
- -مقاومة البرمجيات الخبيثة، لما تستهدفه من أحداث أضرار بالغة للمستخدمين.

- -تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

- -اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

- -الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

# أنواع الجرائم المعلوماتية

**أولا: جرائم التعدي على البيانات المعلوماتية**

تشمل الجرائم التي يكون موضوعها البيانات أو معلومات، وهي جرائم التعرض للبيانات المعلوماتية، وجرائم اعتراض بيانات معلوماتية، والبيانات هي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها.

**ثانيا: جرائم التعدي على الأنظمة المعلوماتية**

تشمل جرائم الولوج غير المشروع إلى نظام معلوماتي أو المكوث فيه، مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل معلوماتي، ويتمثل النظام المعلوماتي في مجموعة البرامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

## ثالثا: إساءة استعمال الأجهزة أو البرامج المعلوماتية

تتضمن هذه الجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازا أو برنامجا معلوماتيا أو أي بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض ارتكاب أي من الجرائم المنصوص عليها سابقا، ويتضمن البرنامج المعلوماتي مجموعة من التعليمات والأوامر القابلة للتنفيذ باستخدام الحاسب الآلي ومعدة لإنجاز مهمة ما، إما البرامج المعلوماتية هي الكيان المعنوي غير المادي من برامج ومعلومات وما إليها ليكون قادرا على القيام بوظيفة.

## رابعا: الجرائم الواقعة على الأموال

تشمل جرم الاحتيال أو الغش بوسيلة معلوماتية وجرم التزوير المعلوماتي، وجرم الاختلاس أو سرقة أموال بوسيلة معلوماتية، وجرم أعمال التسويق والترويج غير المرغوب فيها، وجرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي، والاستخدام غير المشروع لها، وجرم الاطلاع على معلومات سرية أو حساسة أو إفشائها.

## سادسا: جرائم التعدي على الملكية الفكرية للأعمال الرقمية

تشمل جرام وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات، وجرم بيع أو عرض عمل مقلد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

## خامسا: جرائم الاستغلال الجنسي للقاصرات

تظهرها الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، وتشمل الرسومات أو الصور أو الكتابات أو الأفلام أو الإشارات، أو أي أعمال إباحية يشارك فيها القاصرون، أو تتعلق باستغلال القاصرين في المواد الإباحية، وتشمل أيضا إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.

## ثامنا: الجرائم التي تمس المعلومات الشخصية

تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.

## سابعا: جرائم البطاقات المصرفية والنقود الإلكترونية

تشمل أعمال تقليد بطاقات مصرفية بصورة غير مشروعة واستعمالها عن قصد، وتزوير إلكترونية بصورة غير مشروعة عن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

## تاسعا: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية

تشمل جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية، وجرم تهديد أشخاص أو التعدي عليهم بسبب انتهائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية، وجرم توزيع معلومات بوسيلة إلكترونية من شانها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية، وجرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية.

## عاشراً: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت

تشمل جرم تملك وإدارة مشروع مقامرة، وجرم تسهيل وتشجيع مشروع مقامرة، وجرم ترويج الكحول للقاصرين، وجرم ترويج المواد المخدرة.

## الحادي عشر: الجرائم المعلوماتية ضد الدولة والسلامة العامة

تتضمن الأفعال الإجرامية الناشئة عن المعلوماتية التي تطال الدولة وسلامتها وأمنها واستقرارها ونظامها القانوني، وهي جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية، وتشمل أيضاً جرائم الإخفاق في الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والاطلاع أو الحصول على معلومات سرية تخص الدولة، وذلك من خلال شبكة الإنترنت أو باستعمال وسيلة معلوماتية، بالإضافة إلى فعل العبث بالأدلة القضائية المعلوماتية أو إتلافها أو إخفائها، والأعمال الإرهابية التي ترتكب باستخدام شبكة الإنترنت أو أي وسيلة معلوماتية، وجرائم التحريض على القتل عبر الإنترنت أو أيه وسيلة معلوماتية.

## الثاني عشر: جرائم تشفير المعلومات

تشمل أفعال تسويق أو توزيع أو تصدير أو استيراد وسائل تشفير، بالإضافة إلى أفعال تقديم وسائل تشفير تؤمن السرية دون حيازة تصريح أو ترخيص من قبل المراجع الرسمية المختصة في الدولة، وأيضاً بيع أو تسويق أو تأجير وسائل تشفير ممنوعة.

# أسباب الجرائم المعلوماتية

- الرغبة في جمع المعلومات وتعلمها.
- الاستيلاء على المعلومات والاتجار فيها.
- قهر النظام وإثبات التفوق على تطور وسائل التقنية.
- الحاق الأذى بأشخاص أو جهات.
- تحقيق أرباح ومكاسب مادية.
- تهديد الأمن القومي والعسكري.

# نصائح وإرشادات لمكافحة الجرائم المعلوماتية

- توعية الأفراد بأهمية الأمن السيبراني وتزويدهم بالإرشادات والنصائح اللازمة لاتباعها
- تدريب أفرادها على التعامل مع المخاطر الإلكترونية قدر الإمكان
- التدريب على تفادي الأخطاء ومساعدة أفرادها في الحد من المخاطر الناجمة من اختراق أجهزة وشبكات الحاسب، والتي ترجع لعدم وعيهم بطرق وأساليب الوقاية والحماية
- إعطاء النصائح التي تساهم في تنمية الوعي بالأمن السيبراني لتحقيق درجة عالية من الأمان والحماية في عالم رقمي سهل الاختراق
- العمل على تحقيق الأمن السيبراني وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
- حماية المصلحة العامة والآداب والأخلاق العامة، والاقتصاد الوطني أيضاً

INTRUSION ANALYSIS AND INCIDENT MANAGEMENT
تحليل التسلل وإدارة الحوادث

DIGITAL FORENSIC INVESTIGATION
التحقيق الجنائي الرقمي

NETWORK SECURITY AND PENETRATION TESTING
أمن الشبكات واختبار الاختراق

SECURE SYSTEMS ARCHITECTURES AND MECHANISMS
آليات بناء الأنظمة الآمنة


Cybet
security