جمهورية العراق
وزارة التربية
المديرية العامة للتعليم المهني

أساسيات الأمن السيبراني

فرع الحاسوب وتقنية المعلومات

اختصاص الأمن السيبراني

الصف الثاني

تأليف

أ.د. فائز حسن علي

أ.م. د. أياد غازي ناصر

م.م. وائل وحيد شاتي

م.م.سيف احمد شاكر

الطبعة الاولى

1447هـ – 2025م

المصمم الفني

محمد عامر محمود

المقدمـــــــة

يعلم الجميع أن الأمن السيبراني أصبح ضرورة ملحة في عصرنا الرقمي، وإذ يعتمد العالم بنحو كبير على التكنولوجيا والإنترنت في جميع جوانب الحياة. مع تزايد التهديدات السيبرانية، مثل الاختراقات والبرمجيات الخبيثة، أصبح من الضروري حماية البيانات الحساسة وضمان استمرارية العمليات الرقمية. الأمن السيبراني لا يقتصر فقط على المؤسسات الكبرى، بل يشمل الأفراد أيضًا، إذ يساهم في حماية الخصوصية الشخصية ومنع الاحتيال الإلكتروني. ولتحقيق ذلك، يتم استخدام تقنيات متقدمة مثل الذكاء الاصطناعي وتحليل البيانات، فضلاً عن وضع سياسات أمنية صارمة وتدريب الأفراد على أفضل الممارسات. إن الأمن السيبراني يلعب دورًا حيويًا في تعزيز الثقة في البيئة الرقمية ودعم الابتكار التكنولوجي. تطرقت محتويات هذا الكتاب نظرة عامة عن الاساسيات المهمة في مجال الأمن السيبراني والتوعية من الهجمات السيبرانية والطرائق الكفيلة بردعها وتناول الكتاب التقنيات الأمنية الحديثة في مجال الأمن السيبراني الاخلاقيات والسياسات المتبعة في الحفاظ على أمنية المعلومات والبيانات وتجنب الإساءة في استخدام البرامج والأنظمة .

وعلى فق التوجيهات البناءة المتواصلة والدعم الكامل والملموس من المسؤولين والقيادات التربوية في المديرية العامة للتعليم المهني وبغية إعداد ملاكات فنية مدربة ومتطورة على استيعاب وسائل التقنية الحديثة في إعداد مناهج نظرية وعملية تتوافق مع مواصفات التخصصات الفنية المختلفة وإخراج الكتاب المهني بما يتفق ومستوى الطالب في المدارس المهنية فقد بات لزاما علينا أن نضع نصب أعيننا عند تأليف هذا الكتاب الاستيعاب الذهني للطالب في هذه المرحلة وبأسلوب مُيسر خالٍ من التعقيد من غير الإخلال بالمستوى العلمي، وهنا بات علينا إعداد وتهيئة ملاكات مهنية في هذا المجال لتعزيز ورفد سوق العمل والمؤسسات بطاقات شابة وواعدة للنهوض بالثورة التكنولوجية في بلدنا والالتحاق بركب الدول التي سبقتنا في هذا المجال والله المستعان .

..... ومن الله التوفيق .

المؤلفون

المحتويات

الفصل الاول

مدخل إلى الأمن السيبراني
(Introduction to Cybersecurity)

الأهداف

من المتوقع أن يكون الطالب قادراً على أن :

1. **يتعرف على مفهوم الأمن السيبراني وأهميته لحماية الأفراد والمؤسسات.**
2. **يفهم الفرق بين الأمن السيبراني وامن المعلومات.**
3. **يدرك المبادئ الاساسية للأمن السيبراني (السرية، السلامة، والتوافر).**
4. **تحديد أمثلة من التهديدات الأمنية المحيطة على الانترنت.**
5. **يقوم بتطبيق مهارة تمييز المعلومات التي يجب حمايتها وتقييم المخاطر المرابطة بها.**

حقوق الانسان والأمن السيبراني

الأمن السيبراني هو مجال حيوي في العصر الرقمي، حيث يلعب دورًا هامًا في حماية المعلومات والبيانات من التهديدات السيبرانية. ومع ذلك، فإن الأمن السيبراني يثير أيضًا تحديات حقوقية كبيرة، حيث يمكن أن يؤثر على حقوق الإنسان الأساسية مثل الحق في الخصوصية والحرية في التعبير.

أن حقوق الإنسان في الأمن السيبراني موضوع حيوي يتطلب اهتمامًا كبيرًا. يجب أن نعمل معًا لحماية حقوق الإنسان الأساسية في الأمن السيبراني، مثل الحق في الخصوصية والحرية في التعبير. يمكن أن تساعد التوعية والتثقيف والتقنيات الأمنية والتعاون الدولي على حماية حقوق الإنسان في الأمن السيبراني

1. الحق في الخصوصية.
2. الحرية في التعبير .
3. الحق في الوصول إلى المعلومات.

الفصل الاول

مدخل الى الأمن السيبراني (Introduction to Cybersecurity)

1-1 مفهوم الأمن السيبراني واهدافه

تعريف الأمن السيبراني

هناك الكثير من التعريفات للأمن السيبراني، تختلف باختلاف الزاوية التي يتم النظر من خلالها إلى هذا المجال، ومن أهمها:

- **التعريف الاول:**

هو مجموعة التقنيات والعمليات والممارسات وتدابير الاستجابة المصممة لحماية الأنظمة والشبكات والبرامج والبيانات من الهجمات الرقمية أو الضرر بها أو الوصول غير المصرح لها لضمان سريةٌ المعلومات وسلامتها وتوافرها، سواء أكانت هذه المعلومات مخزونة في أجهزة الحواسيب أم الهواتف الذكية أو المتناقلة بينها.

- **التعريف الثاني:**

هو الدفاع عن أجهزة الكمبيوتر والخوادم والأنظمة الإلكترونية.. إلخ من الهجمات الضارة، سواء أكانت هذه الهجمات من قِبل مهاجمين مستهدفين أم بوساطة برامج ضارة إنتهازية.

- **التعريف الثالث:**

هو توظيف التقنيات من أجل تنفيذ التدابير اللازمة التي تضمن للمستخدم أمنه، وتحمي بياناته، وتحميه من الاستغلال.

1-1-1 مصطلحات ومفاهيم أساسية في الأمن السيبراني

عند الخوض في مجال الأمن السيبراني لابد من التعرف على بعض المفاهيم والمصطلحات الاساسية، ومنها:

1. مختبِر الاختراق

هو شخص لديه خبرة أو على الأقل لديه الأساسيات في أنظمة التشغيل والبرمجة وبرمجة مواقع الويب والتشفير وبعض الأمور الأخرى. وهذا الشخص يقوم بإجراءات اختبار الاختراق على الشبكات والتطبيقات

والأنظمة. وهدفه هو إيجاد الثغرات الأمنية التي تمكن المهاجمين من استغلالها يستعمل أساليبهم نفسها ولكن بنحو قانوني بتصريح من مالك النظام.

2. المهاجم

هو الشخص الذي لديه نفس مهارات مختبر الاختراق ولكن يستخدمها بشكل غير قانوني بهدف التسلية أو إيذاء الآخرين أو بهدف سياسي أو اقتصادي أو ما إلى ذلك.

ويجب أن نعرف بانه يوجد فريق مخصص للدفاع عن أنظمة الشركة إذ ما ذكر سابقا المقصود به مختبر الاختراق يسمى فريق الاختراق (Red Team) وفريق الدفاع (Blue Team).

3. فريق الدفاع

يجب ان يكون على معرفة عميقة بالشبكات وان يكون لد يه مهارات الوصول للمعلومات.

4. الثغرة

هي نقطة ضعف في النظام يمكن للمهاجم استغلالها لسرقة بعض المعلومات او يمكن ان تصل للتحكم الكامل في أنظمة الشركة و يمكن ان يمنع الخدمة عن هذه الشركة ويمكن ان تكون هذه الثغرة خطأ برمجي او اعدادات غير صحيحة او حتى يمكن ان تكون تصاميم ضعيفة واكتشافها يتم عن طريق مختبر الاختراق و هو امر أساس للحفاظ على سلامة وأمان الأنظمة.

2-1-1 انواع الأمن السيبراني (Types of Cybersecurity)

هناك انواع عديدة للأمن السيبراني، يمكن التعرف عليها من خلال النقاط الآتية :

1. أمن الشبكات

إن أغلب الهجمات تتم عبر الشبكة العنكبوتية، وبالتالي تم تأسيس هذا الفرع من الأمن السيبراني لحماية أجهزة الكمبيوتر من الهجمات التي تصيبه من داخل وخارج الشبكة، ومن التقنيات المستخدمة في أمن الشبكات (جدار الحماية من الجيل الثاني Fire wall، ومنع فقدان البيانات) كتقنيات **(IAM، DLP)**.

2. أمن التطبيقات

يتم من خلاله حماية البيانات المرتبطة بالبرامج والتطبيقات مثل كلمات السر وأسئلة الأمان وعمليات المصادقة.

3. الأمن السحابي

يتعلق بحماية البيانات التي يتم تخزينها وحفظها على شبكة الإنترنت.

4. الأمن التشغيلي

يتم فيه إدارة مخاطر عمليات الأمن السيبراني الداخلي، ومحاولة إيجاد خطط بديلة عند تعرض المعلومات والبيانات للخطر، ويتضمن أيضًا توعية وتدريب الموظفين على ممارسات تفادي الخطر.

3-1-1 أهداف الأمن السيبراني

إن اهم اهداف الأمن السيبراني تكمن في ما يسمى **(مثلث الحماية الأمنية)** والذي يتكون من ثلاث أضلاع أو دروع، وهي كما يأتي:

1. **الخصوصية (Confidentiality).**
2. **السلامة او التماسك (Integrity).**
3. **التوافر (Availability).**

ومن هنا أتى الاسم **(CIA)** هي بدايات الكلمات الثلاث باللغة الإنجليزية. وعادة يوجد بوسط مثلث الحماية ما نريد أن نحميه.

الشكل (1-1) يوضح السياسات الخاصة الواجب اتباعها لتحقيق الأمن السيبراني وامن المعلومات، ويرمز لها بالرمز **(CIA).**

الشكل (1-1) يمثل سياسات **(CIA)** لتحقيق الأمن السيبراني وأمن المعلومات

1. الخصوصية (Confidentiality)

ويقصد بها اتخاذ التدابير التي تضمن سرية البيانات ومنع حالات الوصول الى المعلومات غير المصرح بها (المعلومات الحساسة)، مع تحديد صلاحية التعديل والحذف والإضافة. وهذا الدرع يوجد في الشركة لحماية المعلومات الشخصية للأفراد. فمثلا زيد يستطيع فقط الدخول إلى حسابه هو ليرى معلوماته الشخصية أو بياناته في الشركة ولكنه لا يستطيع أن يرى معلومات زميله أحمد. والمبرمج الذي يقوم بعمل برنامج للشركة من الواجب أن لا يصل لكل البيانات داخل الشركة بلا داعي. ويمكن تقسيم البيانات داخل الشركة إلى أقسام حسب حساسيتها وحينها يتم تخصيص البيانات السرية فقط للأشخاص المسموح لهم بعرضها أو تعديلها. ويجب أن يتلقى الموظفون بالشركة التدريب اللازم لزيادة قدرتهم على حماية بياناتهم والبيانات الحساسة للشركة. ومن الجدير بالذكر إن طرائق التأكيد على الخصوصية هي استخدام اسم مستخدم وكلمة سر، أو استخدام توثيق ثنائي المفتاح (مثلا استخدام كلمة سر وبطاقة للولوج للنظام) وحماية المعلومات الشخصية بالتشفير أو تقليل تعرضها للهجمات.

2. السلامة (Integrity)

ويقصد بها اتخاذ الاجراءات التي تضمن عدم تغيير البيانات اثناء النقل او الحفظ من قبل اشخاص غير مصرح لهم. اي الحماية من العبث ببيانات الشركة من التخريب والتعديل المقصود أو غير المقصود من الأشخاص غير المصرح لهم. ويمكن إعطاء صلاحيات على مستوى الملف أو التحكم بالدخول لإعطاء الصلاحيات فقط للأشخاص المصرح لهم بالتعديلات. ومن الجدير بالذكر إن النسخ الاحتياطية مهمة جدا لاسترجاع البيانات المخربة.

3. التوافر (Availability)

ويقصد بها الضمان بأن تكون المعلومات متاحة بشكل مستمر وسهل للمستخدمين المرخص لهم. بالإضافة الى عدم تعطل الاجهزة والبنية التحتية التقنية والانظمة التي تحتفظ بالمعلومات (عدم تعطل وسائل الاتصال).

وتعني القيام بحماية النظام مع توافره للمستخدمين. فلا يعقل أن تحمي أموال البنك بغلق البنك. وفي الشركة فإن إجراءات مثل صيانة المعدات وتوفير نسخ احتياطية وترقية نظم التشغيل إلى احدث الإصدارات لهي إجراءات وقائية من وقوع الشركة في فخ انقطاع الخدمة. يجب إعداد العدة لتجاوز الكوارث التي يتسبب بها الإنسان كالحرق والتخريب المتعمد أو تلك الطبيعية مثل السيول والزلازل. الأجهزة والمعدات الخاصة بحماية الشركة مثل الجدران النارية تزيد من حماية بيانات الشركة من هجمات

مثل "هجمة تعطيل الخدمة" وتتم هذه الهجمة بان يقوم المهاجم بشغل الخوادم بكثير من الطلبات الوهمية حتى إغراقه بالطلبات فحينها لن يستطيع التجاوب مع المستخدمين الأبرياء.

2-1 مفهوم الفضاء السيبراني

ان مصطلح (**السيبراني**) يقصد بها الفضاء الإلكتروني أو فضاء الإنترنيت، ومصطلح الفضاء الالكتروني او الفضاء السيبراني يطلق على عناصر الوسط الذي تتواجد فيه البيانات الرقميةٌ واماكن خزنها والتعامل معها. وتضم هذه العناصر أجهزة الحواسيب والهواتف الذكية وأنظمة الشبكات والبرمجيات، وحوسبة المعلومات ونقل وتخزين البيانات، ومستخدم كل هذه العناصر.

1-2-1 اساسيات الأمن السيبراني

للحفاظ على سلامة وأمان الأنظمة والبيانات الرقمية، لابد من التعرف على بعض أساسيات الأمن السيبراني التي يجب اتباعها، وندرج بعض النصائح والإرشادات لتعزيز الأمان الرقمي، وكما يأتي:

1. التوعية السيبرانية

للدراية بالتهديدات السيبرانية الحالية والنصائح الأمنية المتعلقة بالإنترنت يجب ان نقوم بتحديث معرفتنا باستمرار حول التطورات الأمنية الجديدة والطرق المبتكرة للحماية.

2. استخدام البرمجيات الحديثة والمحدثة

التأكد من تحديث جميع البرامج والتطبيقات المستخدمة على أجهزتنا بانتظام، إذ يعد تحديث البرمجيات جزءاً أساسياً من الأمن السيبراني حيث يقوم بإصلاح الثغرات الأمنية والضعف في النظام.

3. النسخ الاحتياطي المنتظم

الاحتفاظ بنسخ احتياطية من البيانات المهمة على أجهزة تخزين خارجية والذي يساعدنا في استعادة البيانات إذا ما تعرضت للفقدان أو التلف.

4. قوة كلمات المرور

استخدام كلمات مرور قوية ومعقدة لحساباتنا الرقمية والتأكد من استخدام مجموعة متنوعة من الأحرف الكبيرة والصغيرة والأرقام والرموز.

5. الحماية من البريد الاحتيالي

الحذر عند فتح رسائل البريد الإلكتروني غير المعروفة أو المشبوهة، وتجنب النقر على الروابط أو تحميل المرفقات إلا إذا كنا واثقين من مصدرها.

6. استخدام الشبكات الأمنة

تجنب الاتصال بشبكات واي فاي عامة غير آمنة، واستخدام شبكات واي فاي مأمونة ومشفرة عند الاتصال بالإنترنت.

7. مراجعة إعدادات الخصوصية

التأكد من ضبط إعدادات الخصوصية على أجهزتنا وحساباتنا الرقمية بحيث تكون معلوماتنا الشخصية والمحتوى الرقمي خاصة ومحمية.

8. الحماية من الفيروسات والبرامج الضارة

تثبيت برامج مكافحة الفيروسات والبرامج الضارة على أجهزتنا وتحديثها بانتظام.

الشكل (1-2) يوضح اهم اساسيات الأمن السيبراني.

الشكل (1-2) اهم اساسيات الأمن السيبراني

2-2-1 أهمية تعلم أساسيات الأمن السيبراني

مع تزايد التهديدات السيبرانية وتطور التقنيات، أصبح تعلم أساسيات الأمن السيبراني أمراً ضرورياً حيث يعد التعليم السيبراني عملية توعوية تهدف إلى تثقيف الأفراد والجهات حول أمان الأنظمة الرقمية وكيفية حمايتها من التهديدات السيبرانية.

لذا يجب على الجهات الحكومية والشركات والمنظمات التعليمية والأفراد العاملين في مجال التقنيات الإلكترونية أن يكونوا على دراية في أساسيات الأمن السيبراني وأفضل الممارسات للحماية الرقمية يمكن تحقيق ذلك من خلال توفير برامج تدريبية وورش عمل حول أساسيات الأمن السيبراني وتعزيز الوعي والمعرفة بين الموظفين والطلاب.

بالإضافة إلى ذلك، يجب على الأفراد أن يكونوا على دراية بمخاطر الأمان السيبراني وكيفية التصدي لها في حياتهم الشخصية والمهنية كما يمكن للأفراد اتباع إجراءات بسيطة واتباع أفضل الممارسات للأمن السيبراني لحماية أنفسهم ومعلوماتهم الشخصية من التهديدات السيبرانية.

3-2-1 فوائد الأمن السيبراني

ويعد الأمن السيبراني أمرًا بالغ الأهمية. ويتضمن حماية أنظمة تكنولوجيا المعلومات والبيانات من التهديدات السيبرانية مثل الاحتيال أو التجسس أو التخريب.

ويمكن توظيف الأمن السيبراني للحد من هذه الآثار، وتقليل الأضرار الناتجة عن التهديدات المُحتملة.

ومن أهم فوائد الأمن السيبراني:

1. تحسين وحفظ بيانات اعتماد المؤسسات أو الشركات المحسّنة مع وجود ضوابط الأمان الصحيحة المعمول بها عالميا.
2. تحسين ثقة أصحاب العمل في ترتيبات أمن المعلومات الخاصة بالمؤسسات أو الشركات.
3. تقليل أوقات استرداد البيانات والمعلومات في حالة حدوث خروقات للشبكات أو الأنظمة.
4. حماية الشبكات والبيانات من الوصول غير المصرح به.
5. إدارة استمرارية الأعمال.
6. تحسين أمن المعلومات

3-1 أهمية الأمن السيبراني في حماية الأفراد والمؤسسات والمجتمع

في ثمانينيات القرن العشرين، ابتكر روبرت تي موريس أول برنامج فيروس إلكتروني، والذي حاز على تغطية إعلامية هائلة نظرًا لانتشاره بين الأجهزة وتسبّبه بأعطال في الأنظمة، فحُكِم على موريس بالسجن والغرامة، وكان لذلك الحكم دور في تطوير القوانين المتعلقة بالأمن السيبراني.

للأمن السيبراني أهمية كبيرة؛ لأنّه يحمي بيانات المستخدمين من الهجمات الإلكترونية الرامية إلى سرقة المعلومات واستخدامها لإحداث ضرر، فقد تكون هذه بيانات حساسة، أو معلومات حكومية وصناعية، أو معلومات شخصية.

أهمية الأمن السيبراني على المستوى الفردي تتمثل في حماية الشخص من محاولات سرقة الهوية، والابتزاز، وحتى فقدان البيانات المهمة، أما على المستوى العام فالأهميات لا حصر لها، منها: حماية البنية التحتية التقنية للبلاد، مثل: المستشفيات، ومحطات الطاقة، والبنوك، وشركات الخدمات المالية، ومؤسسات الدولة، بنحو يعد الأمن السيبراني ضروريًا للغاية في أثناء الوقت الحالي ومع التقدم الذي يشهده العالم لحماية الشركات والأفراد من مجرمي الإنترنت. وتكمن اهمية الأمن السيبراني عبر معرفة اولا انواع التهديدات، اساسيات الأمن السيبراني، أهمية تعلم أساسيات الأمن السيبراني واخيراً معرفة انجازات الأمن السيبراني لحماية الأفراد والمؤسسات والمجتمع.

1-3-1 أنواع التهديدات السيبرانية

تشمل التهديدات السيبرانية مجموعة متنوعة من الهجمات والأنشطة الخبيثة وندرج في ادناه اهم هذه التهديدات:

1. هجمات الاختراق الالكتروني

إذ يحاول المهاجمون اختراق النظام أو الشبكة للوصول إلى المعلومات الحساسة أو السيطرة على الأنظمة، وقد تكون هناك دوافع سياسية.

2. الفيروسات والبرمجيات الخبيثة

وهي برامج ضارة يتم تنفيذها على الأنظمة دون علم المستخدمين وتستهدف تدمير البيانات أو التجسس عليها.

3. الجرائم والاحتيال الإلكتروني

وتتضمن الرسائل الاحتيالية والاحتيال الهاتفي ومواقع الويب الزائفة للحصول على معلومات شخصية ومالية.

4. هجمات الحرمان من الخدمة

وهي هجمات تستهدف تعطيل الخدمات الرقمية وجعلها غير متاحة للمستخدمين.

5. الإرهاب السيبراني

وهو تقويض الأنظمة لأهداف متعددة منها إثارة الذعر وإضعاف الخصم أو فرض السيطرة.

2-3-1 انجازات الأمن السيبراني لحماية الأفراد والمؤسسات والمجتمع

تكمن أهمية **(الأمن السيبراني)** لحماية الأفراد والمؤسسات والمجتمع في تحقيق الانجازات الآتية:

1. توفيره لبرامج وإجراءات إلكترونية لحماية المعلومات من السرقة من قبل المجرمين الإلكترونيين واستخدامها لإحداث ضرر بالفرد والمجتمع.
2. يحافظ على سمعة المؤسسات وثقة المواطنين بها، وثقة المستهلك في الشركات التي يتعامل معها، وتُحافظ أيضاً على استمرارية القدرة التنافسية للأعمال التجارية.
3. يحمي عمل المجتمع عبر حماية معلوماته الحساسة، والتي يُخزن كميات هائلة منها في أماكن تخزين البيانات، وأجهزة الكمبيوتر الخاصة بالمستشفيات ومؤسسات الرعاية الصحية الأخرى، ومحطات الطاقة، والخدمات المالية، والمنظمات الحكومية.
4. يحمي الفرد من سرقة بياناته وهويته وتعرضه لمحاولات ابتزاز تلحق الضرر به.

3-3-1 تحديات الأمن السيبراني

رغم أهمية الأمن السيبراني والجهود المبذولة لتعزيزه، إلا أن هناك العديد من التحديات التي تواجه مجال الأمن السيبراني وتشكل تحدياً مستمراً في المستقبل، ومن ابرز هذه التحديات:

1. التهديدات المتطورة:

يتطور الهجوم السيبراني بشكل مستمر، حيث يبتكر المهاجمون أدوات وتكتيكات جديدة للوصول إلى البيانات والأنظمة، يتطلب ذلك من الأفراد والمؤسسات تحديث استراتيجيات الأمن السيبراني بانتظام والتعامل مع التهديدات المستجدة.

2. نقص المهارات:

يعاني قطاع الأمن السيبراني من نقص في المهارات والخبرات المتخصصة إذ تحتاج الجهات إلى تدريب محترفين متخصصين في مجال الأمن السيبراني لمواجهة التحديات الحالية والمستقبلية.

3. تعقيد التشريعات:

تختلف التشريعات واللوائح المتعلقة بالأمن السيبراني من دولة إلى أخرى، مما يجعل من الصعب تنسيق جهود الأمن السيبراني على المستوى العالمي لذلك يجب العمل على تحسين التعاون الدولي وتطوير مبادرات ومعايير مشتركة للحماية السيبرانية.

4. انتشار التقنيات الرقمية:

يتزايد اعتمادنا على التقنيات الرقمية والشبكات الذكية في حياتنا اليومية، مما يزيد من الفرص للهجمات السيبرانية لذلك يجب أن نتخذ التدابير اللازمة لحماية هذه التقنيات وتأمينها من الاختراق.

5. الحماية من التهديدات الجديدة:

مع تطور التقنيات، قد تظهر تهديدات سيبرانية جديدة تتطلب إجراءات أمان مبتكرة يجب أن تكون الجهات مستعدة للتعامل مع التهديدات الجديدة والاستجابة بسرعة للحفاظ على أمانها.

1-3-4 مستقبل الأمن السيبراني

تتطلع مجتمعاتنا إلى مستقبل رقمي أكثر تطوراً وابتكاراً، ومع ذلك يتزايد التحدي في حماية أنظمتنا ومعلوماتنا من التهديدات السيبرانية لتحقيق مستقبل آمن وواعد، يجب أن يتم التركيز على التحسين المستمر لأمان الأنظمة الرقمية وتعزيز الوعي في أساسيات الأمن السيبراني بين الأفراد والجهات.

ومن المتوقع أن تستمر التحديات والتهديدات السيبرانية في الزيادة في المستقبل، ولذلك يجب أن يتم تبني نهجاً متعدد الأطراف للأمن السيبراني يشمل التعاون بين القطاعين العام والخاص والجهات الأكاديمية والمجتمع المدني، حيث يمثل مجال الأمن السيبراني فرصة للابتكار والتطوير ومن ثم يمكن للشركات والجهات تقديم حلول وأدوات جديدة لمكافحة التهديدات السيبرانية وتحسين الحماية الرقمية وذلك بالتحول الرقمي والعمل على تعزيز أساسيات الأمن السيبراني في كل جانب من جوانب الحياة.

1-3-5 إجراءات الوقاية من الهجمات السيبرانية

هناك عدد من الإجراءات التقنية المتطورة التي تساعد في اكتشاف أنواع الهجمات قبل حدوث الإضرار أو الوقوع ضحيتها، ومن تلك الإجراءات ما يأتي:

1. تثبيت برامج تقنية تقوم بمكافحة الفيروسات، والبرامج الخبيثة لعدم تسرب أي معلومات.
2. وضع التدابير التنظيمية المضادة، والتي تقوم بتوفير التدريب على الأمن السيبراني.
3. إنشاء نسخ احتياطية للبيانات لتجنب سيناريو فقدان أي بيانات أو معلومات مهمة.

4. العمل على تحديث الأنظمة المستخدمة بالكامل لتصحيح ثغرات البرامج وللحماية من تهديدات الأمان الوارد حدوثها.
5. تأمين شبكات الإنترنيت اللاسلكية.
6. التأكد من تشفير الشبكات وتشفير المعلومات عند التخزين أو إرسالها عن طريق الإنترنت.
7. الاطلاع على أحدث عمليات الاحتيال والمخاطر الأمنية، وذلك للاطلاع على الأساليب التي يتعامل بها المخترقون.

4-1 العلاقة بين امن المعلومات والأمن السيبراني

يهتم **(امن المعلومات)** بحماية المعلومات سواء أكانت في شكلها المادي (مثل المستندات الورقية) او في شكلها الرقمي **(الالكتروني)**. في حين يهتم **(الأمن السيبراني)** بآمن كل ما هو موجود في الفضاء الالكتروني مثل البرامج والاجهزة المتصلة بالإنترنيت فضلاً عن أمن المعلومات، بينما **امن المعلومات** ليس له علاقة بأمن البرامج والاجهزة المتصلة بالإنترنيت.

5-1 المبادئ الأساسية للامن السيبراني

يتكون الأمن السيبراني من (خمسة) مبادئ ومكونات رئيسة ممثلة بالآتي:

1. البنية التحتية:

تشمل أنواع أنظمة الأمن السيبراني في المجتمع جميعاً، بما فيها (الشبكات الكهربائية، والمستشفيات، والاتصالات، وإشارات المرور، ومحطات المياه وغيرها).

2. الأمن السحابي:

يوفر الأمن السحابي مجموعة من الأنظمة والخيارات التي تُساعد على حماية البيانات وتأمينها، إذ يُمكن عمل نسخ احتياطية منها إلى مواقع عديدة.

3. إنترنت الأشياء (IoT):

تعرف بكونها شبكة واسعة تُتيح للأجهزة الاتصال ببعضها بعضاً مثل (أجهزة الكاميرات، والطابعات، وأي أجهزة أخرى متصلة بالإنترنت).

4. أمن الشبكات:

يُعد أمن الشبكات العنصر الأساس للأمن السيبراني في أي مؤسسة ويشمل (جدران الحماية، برامج مكافحة الفيروسات، والبرامج الضارة، التحكم في صلاحيات الوصول للبيانات، التحليلات الخاصة بكشف أي سلوك غير طبيعي في الشبكة).

5. تدريب الموظفين:

يعد تدريب الموظفين وتثقيفهم بما يخص التهديدات الإلكترونية التي تمس بمؤسساتهم عبر الإنترنت وكيفية الاستجابة لها أمرًا مهمًا للغاية، ومن الأمور التي لا بد من تدريبهم عليها وكما يأتي:

1. فهم الهندسة الاجتماعية.
2. فهم التهديدات السيبرانية.
3. تصفح مواقع الويب الأمنة.
4. فهم كيفية استخدام البريد الإلكتروني.
5. فهم كيفية إنشاء كلمات مرور قوية وآمنة.

أسئلة الفصل الأول

س1/ عرّف كلاً مما يأتي:

1. **الأمن السيبراني**
2. **فريق الدفاع**
3. **الأمن السحابي**
4. **التوافر**
5. **انترنت الاشياء**
6. **الفضاء السيبراني**

س2/ عدّد انواع الأمن السيبراني؟ واشرح واحدة منها.

س3/ عدّد اهداف الأمن السيبراني؟ واشرح واحدة منها.

س4/ عدّد خمساً فقط من النصائح والإرشادات لتعزيز الأمان الرقمي؟ مع الشرح المبسط.

س5/ اشرح أهمية تعلم أساسيات الأمن السيبراني.

س6/ عدّد فوائد الأمن السيبراني.

س7/ اشرح أهمية الأمن السيبراني في حماية الأفراد والمؤسسات والمجتمع.

س8/ عدّد أنواع التهديدات السيبرانية؟ واشرح واحدة منها.

س9/ عدّد خمساً فقط من اهم الإجراءات الواجب اتخاذها للوقاية من الهجمات السيبرانية.

س10/ املأ الفراغات بما يناسبها لكل من العبارات الآتية:

أ. يتكون مثلث الحماية الأمنية من ..... و ..... و .....

ب. يهتم الأمن السيبراني بآمن كل ما هو موجود في ..... مثل ..... و .....

ج. الإرهاب السيبراني هو تقويض الأنظمة لأهداف عديدة منها ..... و ..... او .....

د. عند اختيار كلمة مرور لحساباتنا الرقمية يجب ان تكون ..... و .....

الفصل الثاني

التوعية بالأمن السيبراني
(Cybersecurity Awareness)

الأهداف

من المتوقع أن يكون الطالب قادراً على أن :

1. يفهم انواع التهديدات السيبرانية مثل الفيروسات وهجمات التصيد.
2. يتعرف على اهمية كلمات المرور القوية واهمية التحقق الثنائي.
3. إعداد كلمة مرور قوية على وفق المعايير الأمنية.
4. أن يتعلم مهارات اكتشاف الرسائل البريدية المشبوهة والتعامل معها بوعي .

الفصل الثاني

التوعية بالأمن السيبراني (Cyber security Awareness)

التهديدات السيبرانية

إن الكثير من معلوماتنا الشخصية أصبحت اليوم الان مخزونة ومعالجة على حواسيبنا الشخصية وعلى انظمة المعلومات المختلفة وان الهدف من الأمنية السيبرانية هي للحماية والدفاع عن تلك المعلومات من خلال كشف ومنع ورد الفعل الى الهجمات السيبرانية .

في هذه الأيام عنصر هوس التطفل يتزايد لمهاجمة الأنترنت باقل جهد وخطر ممكن للحصول على فوائد كبيرة حيث نظمت العصابات الاجرامية نفسها واصبحت تعمل بنحو اكثر احترافي في عالم الجريمة السيبرانية .

من خلال تزايد النشاط الاجرامي السيبراني وتهديدها للحياة الاجتماعية بجميع انواعها يجب علينا تنظيم انفسنا للدفاع عن مكتسباتنا التقنية ويكون هذا الدفاع بطرق مختلفة عبر وضع الأنظمة والاجهزة التي تحمي معلوماتنا الخاصة بصورة أمنة وتوجب علينا تشخيص الوسائل الإجرامية ووضع الحلول النظرية لها.

الشكل (2-1) التهديدات السيبرانية

التهديد السيبراني يشير الى الأنشطة غير المشروعة التي تستعمل التكنولوجيا الحديثة مثل الحاسوب والانترنت والتي تستهدف الأمن والخصوصية للمستخدمين على الانترنت ، يمكن ان يشمل التهديد

السيبراني البرمجيات الخبيثة والفايروسات التي تستخدم لتدمير البيانات والمعلومات والملفات وكذلك الاختراق الالكتروني وسرقة الهوية والتجسس على الانشطة على الانترنت.

ان التهديد الإلكتروني هو أي نشاط يهدف إلى المساس بأجهزة الكمبيوتر أو الشبكات الإلكترونية أو البيانات المخزنة عليها. يمكن أن يشمل التهديد الإلكتروني الفيروسات وبرامج التجسس والبرمجيات الخبيثة الأخرى، فضلاً عن هجمات الاختراق والاحتيال الإلكتروني واحتيال الهويات والاحتيال البنكي والتهديدات الأمنية الأخرى. يعد التهديد الإلكتروني أحد التحديات الرئيسة التي تواجهها الأفراد والشركات والمؤسسات في العصر الرقمي .

ان هذه التهديدات السيبرانية يمكن أن تأتي من مصادر مختلفة منها:

- البرامج الخبيثة (Malware)
- هجمات الحرمان من الخدمة (DDoS)
- الاحتيال عبر الإنترنت (Phishing)
- برامج التجسس (Spyware)
- برامج الفيروسات (Virus)

عندما يتعرض نظام أو شبكة لتهديد سيبراني، يمكن أن يظهر أعراض مختلفة :

1. تباطؤ الجهاز: تدهور أداء الجهاز أو النظام.
2. رسائل خطأ غريبة: ظهور رسائل خطأ غير متوقعة أو غريبة على الشاشة.
3. فتح نافذات غير متوقعة: فتح نافذات أو تطبيقات غير متوقعة تلقائيًا.
4. سرقة بيانات الحساب: سرقة بيانات حسابات البريد الإلكتروني أو الشبكات الاجتماعية.
5. تغيير إعدادات النظام: تغيير إعدادات النظام أو الشبكة من دون إذن المستخدم.

والشكل (2-2) يمثل التهديد الالكتروني على أجهزة الكمبيوتر

الشكل (2-2) التهديد الالكتروني على أجهزة الكمبيوتر

1-2 الحماية من التهديدات السيبرانية

للحماية من التهديدات السيبرانية، من المهم تحديث البرامج والأمن بانتظام. هذا يضمن أن النظام أو الشبكة محمية ضد الثغرات الأمنية الجديدة التي قد تكتشفها البرامج الخبيثة. يجب أيضًا استخدام برامج حماية ضد الفيروسات والبرامج الخبيثة، والتي يمكنها الكشف عن البرامج الخبيثة وتعطيلها قبل أن تسبب أي ضرر. هذه البرامج تقوم بمراقبة النظام أو الشبكة وتحليل سلوك البرامج لاكتشاف أي نشاط مشبوه.

فضلاً عن تحديث البرامج والأمن واستخدام برامج الحماية، هناك خطوات أخرى يمكن اتخاذها للحماية من التهديدات السيبرانية. على سبيل المثال:

- استخدام التحقق بخطوتين لضمان حماية الحسابات
- استخدام كلمات مرور قوية وفريدة لكل حساب
- مراقبة النشاط المشبوه على النظام أو الشبكة
- تثقيف المستخدمين حول التهديدات السيبرانيةوخطوات الحماية

بإتباع هذه الخطوات، يمكن الحد من مخاطر التهديدات السيبرانية وتحسين أمان الأنظمة والشبكات. التهديدات السيبرانية هي خطر حقيقي، ولكن مع اتخاذ الإجراءات الوقائية الصحيحة، يمكن الحفاظ على أمان الأنظمة والشبكات وتحقيق السلامة للبيانات والمعلومات.

من المهم أيضاً أن ندرك أن التهديدات السيبرانية ليست فقط مشكلة تقنية، ولكنها ايضاً مشكلة أمنية واقتصادية واجتماعية. يمكن أن تسبب التهديدات السيبرانية خسائر مالية كبيرة وخرقًا للخصوصية وتعطيلًا للخدمات الحيوية.

لذلك، يجب على جميع الأفراد والمؤسسات فرض إجراءات وقائية صحيحة لمواجهة التهديدات السيبرانية. هذه الإجراءات تشمل:

- تحديث البرامج والأمن باستمرار
- استخدام برامج الحماية والتحقق بخطوتين
- تثقيف المستخدمين حول التهديدات السيبرانية
- مراقبة النشاط المشبوه على الأنظمة والشبكات
- إنشاء خطط الطوارئ لمواجهة الهجمات السيبرانية

زد على ذلك الإجراءات الوقائية، يجب على المؤسسات والمستخدمين أن يكونوا مستعدين لمواجهة الهجمات السيبرانية. هذا يشمل:

- إنشاء فريق أمن سيبراني متخصص لمواجهة الهجمات
- تطوير خطط الطوارئ لمواجهة الهجمات السيبرانية
- تدريب الموظفين على إجراءات الأمن السيبراني
- إجراء عمليات مسح أمني منتظمة لاكتشاف الثغرات الأمنية
- التعاون مع الجهات المعنية لمواجهة التهديدات السيبرانية المشتركة

من خلال اتخاذ هذه الإجراءات، يمكن للمستخدمين والمؤسسات الحفاظ على أمان الأنظمة والشبكات وحماية البيانات والمعلومات من التهديدات السيبرانية.

يجب أن ندرك أن الأمن السيبراني مسؤولية مشتركة بين جميع الأفراد والمؤسسات. يجب علينا جميعًا العمل معًا لمواجهة التهديدات السيبرانية وحماية البيانات والمعلومات في عالم رقمي آمن.

2-2 الحماية الشخصية عبر الانترنت

1-2-2 الحماية من الهجمات الالكترونية للأمن السيبراني

يتحمل قادة المؤسسات المسؤولية الاولى لحماية المؤسسة من أي مخاطر محدقة بها من بينها الهجمات الالكترونية ولا سيما قادة ومدراء الأمن السيبراني في المؤسسات والذين يعتبرون الحماة الرئيسين للمؤسسة وانظمتها وشبكاتها وبيانتها إذ تقع على عاتقهم تجهيز انظمة المؤسسة لتكون مقاومة لأي هجمات الكترونية وكذلك وضع خطط للتعافي من نتائج تلك الهجمات بحال وقوعها والتي قد تكون كارثية على المؤسسة لذلك سنسرد مجموعة أخرى من أدوات الأمن السيبراني التي يجب على مديرو الأمن السيبراني معرفتها والعمل على تطبيقها ضمن المؤسسات.

أهم أدوات الأمن السيبراني للحماية من الهجمات الالكترونية:

فيما يلي ست أدوات وخدمات حيوية يحتاج كل مدير أمن سيبراني النظر في الاستثمار فيها ضمن المؤسسة لضمان ان يكون أمنها السيبراني قويا قدر الامكان

اولاً- جدار الحماية Firewall

لابد أنك سمعت مسبقاً عن جدار الحماية وتفكر الان بأن هذه الاداة قد عفا عليها الزمن نتيجة التعقيد الكبير الذي وصلت له عمليات القرصنة في يومنا هذا لكن هذا غير صحيح بل أن جدار الحماية يبقى من أهم أدوات الامان حيث يساهم هذا الجدار بشكل رئيس بمنع وصول غير مصرح به الى نظامك الشكل (3-2) يوضح ذلك.

الشكل (3-2) يمثل جدار الحماية

- **تعريف جدار الحماية:**

هو جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب والمواقع المشبوهة، ويكون أداة مخصصة أو برنامج على جهاز حاسوب آخر، الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة ويرفض أو يسمح فقط بمرور برنامج طبقاً لقواعد معينة، يراقب جدار الحماية حركة مرور الشبكة فضلاً عن محاولات الاتصال، ويقرر ما إذا كان يمكنك المرور بحرية إلى شبكتك أو جهاز الكمبيوتر الخاص بك أم لا.

- **انواع جدران الحماية**

يوجد عدة انواع لجدران الحماية وهي كالاتي:

1. **Proxy Firewall (بوابة بروكس – الوكيل):** يعمل كبوابة دخول (**Gateway**) بين شبكة واخرى لتطبيق معين خوادم البروكسي يمكنها تزويد وظائف اضافية كتخزين المحتوى المؤقت **(Content Caching**) وكذلك الأمن عبر منع الاتصالات المباشرة من خارج الشبكة يمكن ان يؤثر هذا النوع على القدرات الانتاجية وعلى التطبيقات التي يدعمها وهو نوع قديم من الجدران النارية

2. **Statefull Inspection Firewall (جدار الفحص الحالي – الحالة):** هذا النوع من الجدران النارية يسمح او يحجب حركة مرور البيانات او الاتصالات مستندا على بعض العوامل وهي : الحالة , الناقل , البروتوكول كما يعمل هذا النوع على مراقبة الانشطة جميعاً منذ اللحظة الاولى لبدء الاتصال وحتى اغلاقه ويتخذ قرارات التصفية بالاستناد على القواعد التي يحددها المدير وكذلك "السياق" ما يعنيه السياق هو : استخدام المعلومات من الاتصالات السابقة والحزم العائدة لنفس الاتصال.

3. **UTM Firewall (Unified Threat Management) (جدار الحماية الموحد لإدارة التهديدات):** يعني الادارة الموحدة للتعامل مع التهديدات عادة ما يجمع جدار **UTM** الناري بين وظائف الجدار الناري وبين برامج مضادات الفيروسات **antivirus** كما يمكن ان يتضمن بعض الخدمات الاضافية مثل ادارة الخدمات السحابية

4. **Next – generation Firewall (NGFW) (جدار الحماية من الجيل الجديد):** هي جدران نارية متطورة ليست فقط لتصفية الحزمات او لتفتيش الحالة توظف اعلب الشركات هذه الانواع المتطورة من الجدران النارية لحجب التهديدات الحديثة كالبرامج الضارة المتطورة والهجمات على التطبيقات

على الرغم من كون جدار الحماية مفيدا الا ان له مشاكل او قيود فهو غير فعال تماما للتصدي لكل الهجمات ففي يومنا هذا لقد تعلم المتسللون المهرة كيفية انشاء البيانات والبرامج التي تخدع جدران الحماية للاعتقاد بأنها موثوقة وهذا يعني ان البرنامج يمكنه المرور عبر جدار الحماية دون أي مشكلات لكن على الرغم من ذلك لا تزال جدران الحماية فعالة للغاية في اكتشاف الغالبية العظمى من الهجمات الالكترونية الضارة .

ثانياً: مكافحة الفايروسات :-

1. برامج مكافحة الفيروسات Antivirus Software

اذا كنت تدير نشاطا تجاريا ولم يكن لديك قدر كبير من الخبرة في مجال الأمن السيبراني فقد تفترض أن المصطلحين "جدار الحماية " و "مكافحة الفيروسات " مترادفان لكنهما ليسا كذلك من الضروري ان يكون لديك جدار حماية قوي وبرنامج مكافحة فيروسات محدث للحفاظ على نظامك أمنا وبحال كنت مسؤولا عن أنظمة المؤسسة فيجب تطبيق ذلك على كل الانظمة الموجودة في المؤسسة ستنبهك برامج مكافحة الفيروسات الى الاصابة بالفيروسات والبرامج الضارة كما سيقدم العديد منها خدمات اضافية مثل فحص رسائل البريد الالكتروني للتأكد من خلوها من المرافقات الضارة أو روابط الويب تقدم برامج مكافحة الفيروسات الحديثة اجراءات وقائية مفيدة مثل عزل التهديدات المحتملة وازالتها هناك مجموعة كبيرة من برامج مكافحة الفيروسات كما في الشكل ادناه ويمكنك بسهولة العثور على حزمة تناسب احتياجات عملك.

2. خدمات البنية التحتية للمفاتيح العمومية PKI Services

البنية التحتية للمفاتيح العامة هي الترتيبات التي يتم بها ربط المفتاح العام مع المستعمل بوساطة مصدر الشهادة **(Certificate Authority CA)** هوية المستخدم يجب ان تكون فريدة لكل مصدر شهادة يتم ذلك عن طريق برمجيات خاصة في مصدر الشهادة من الممكن ان تكون هذه البرمجيات تحت اشراف بشري جنبا الى جنب مع برمجيات منسقة في مواقع مختلفة ومتباعدة يربط العديد من الاشخاص **PKI** فقط ب **SSL** أو **TLS** وهي التقنية التي تقوم بتشفير اتصالات الخادم والمسؤولة عن **HTTPS** والقفل الذي تراه في أشرطة عناوين متصفحك في حين ان **SSL** مهم للغاية بالطبع ليس فقط لمواقع الامان العامة ولكن ايضا لشبكاتك الداخلية يمكن ان يحل **PKI** بالفعل عددا من نقاط الضعف الشائعة في مجال الأمن السيبراني ويستحق الامان لكل مؤسسة

3. خدمات الكشف الاستباقية

نظرا لان مجرمي الانترنت والمتسللين اصبحوا اكثر تعقيدا واصبحت التقنيات والبرامج التي يستخدمونها اكثر تقدما فقد اصبح من الضروري للشركات الاستثمار في اشكال دفاعية اكثر قوة حيث لم يعد مجرد وجود دفاعات تتفاعل مع التهديدات امرا كافيا –بل يجب ان تكون تلك الدفاعات استباقية وقادرة على تحديد الهجمات الالكترونية قبل ان تتسبب في حدوث مشكلات شهد الأمن السيبراني تحولا من الاستثمار في التقنيات التي تحاول منع احتمال وقوع هجوم نحو الخدمات المتقدمة التي تتفاعل مع مشكلات الامان المحتملة وتكشفها وتستجيب لها بأسرع ما يمكن يعد تحديد الهجوم والقضاء عليه قبل انتشاره اقل ضررا بكثير من محاولة التعامل مع هجوم له بالفعل موطئ قدم قوي على شبكة تقنية المعلومات الخاصة بك

4. اختبار الاختراق

يعد اختبار الاختراق طريقة مهمة لاختبار انظمة الامان الخاصة بالمؤسسة اثناء اختبار الاختراق سيستخدم متخصصو الأمن السيبراني نفس الاساليب التي يستخدمها المتسللون للتحقق من نقاط الضعف المحتملة يحاول اختبار **(pen test)** محاكاة نوع الهجوم الذي قد تواجهه الشركة من المتسللين المجرمين بدءا من اختراق كلمة المرور والشفرة وحتى التصيد الاحتيالي بمجرد اجراء الاختبار سيقدم لك المختبرون نتائجهم ويمكنهم ايضا المساعدة من طريق التوصية بالتغييرات المحتملة على النظام.

5. تدريب الموظفين

يعد وجود موظفين على دراية بمخاطر الهجمات الالكترونية ويفهمون دورهم في الأمن السيبراني احد اقوى اشكال الدفاع ضد الهجمات الالكترونية، هناك العديد من ادوات التدريب التي يمكن الاستثمار فيها لتثقيف الموظفين حول افضل ممارسات الأمن السيبراني يمكن ان يحدث شيء بسيط فرقا كبيرا مثل التحديثات المنتظمة على استراتيجيات الأمن السيبراني واتباع العادات الصحيحة لاستخدام كلمات المرور، من المهم ايضا تقديم دورات تدريبية او عمليات محاكاة حول اكتشاف الروابط المشبوهة او رسائل البريد الالكتروني الاحتيالية التي قد تكون جزأً من هجوم التصيد الاحتيالي.

○ بعض الامثلة على المعلومات الرقمية التي يجب حمايتها من التهديدات الرقمية :

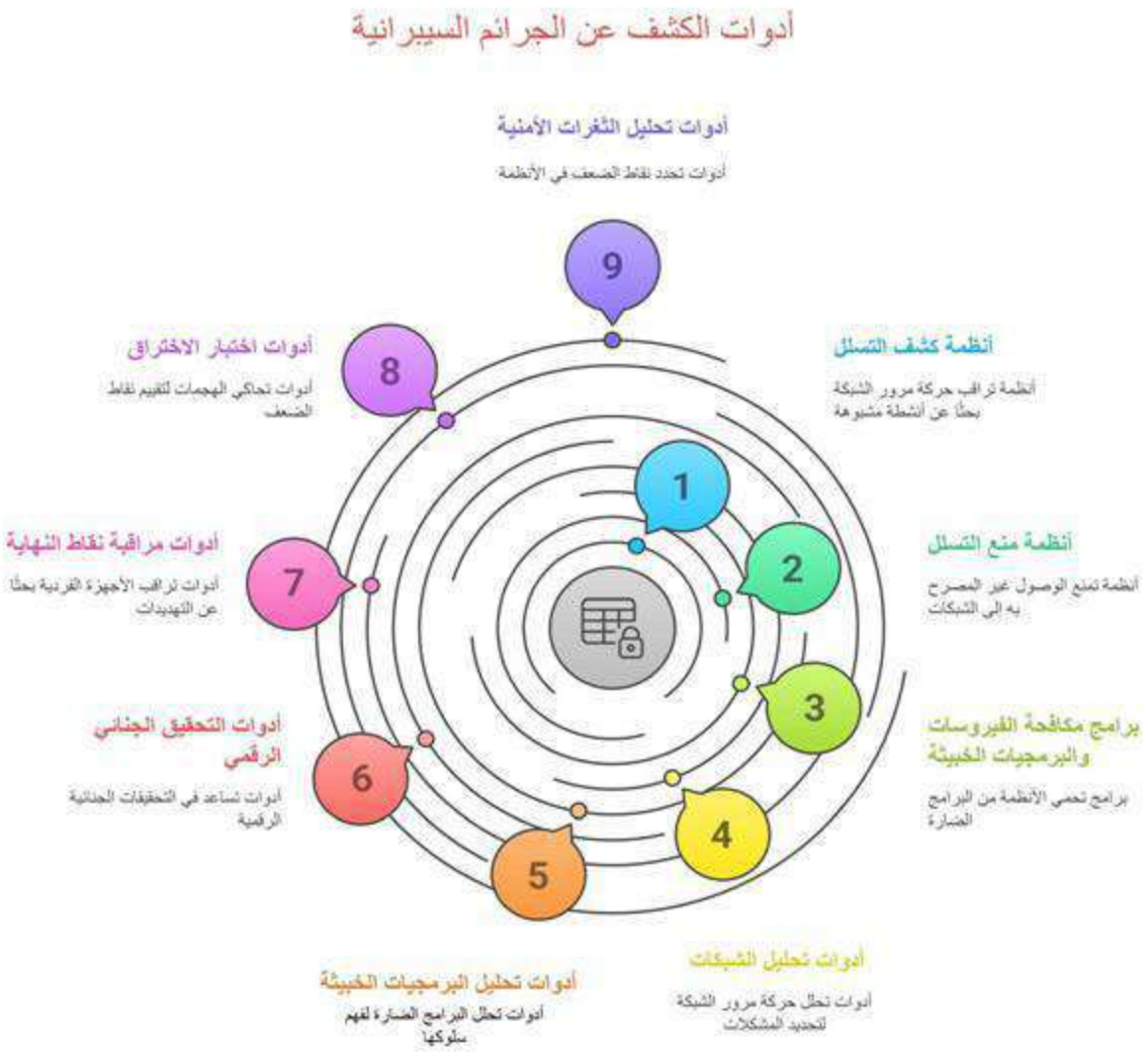
في عصر التحول الرقمي اصبحت المعلومات الرقمية جزءا اساسيا من حياتنا اليومية وعمل المؤسسات ومع ذلك فأن هذه المعلومات معرضة للتهديدات الالكترونية مثل الاختراقات وسرقة البيانات والبرامج الضارة لذلك يجب حماية انواع مختلفة من المعلومات الرقمية الحساسة فيما يلي امثلة عن هذه المعلومات

- البيانات الشخصية
- البيانات المالية
- بيانات العملاء
- البيانات الصحية
- بيانات المؤسسات
- بيانات الاتصالات
- بيانات التعليم
- بيانات الحكومة والقطاع العام
- بيانات الشبكات والانظمة
- بيانات الوسائط الرقمية
- بيانات التطبيقات والبرمجيات
- بيانات الاجهزة الذكية وانترنت الاشياء
- بيانات السحابة
- بيانات وسائل التواصل الاجتماعي
- بيانات البحث والتطوير

○ امثلة على ادوات الكشف عن الجرائم السيبرانية

ادوات الكشف عن الجرائم السيبرانية هي برامج او انظمة تستخدم لتحديد التهديدات الأمنية والانشطة المشبوهة على الشبكات وانظمة الحواسيب وهي:

1. انظمة كشف التسلل **(Systems IDS-Intrusion Detection)**
   - **Snort** نظام مفتوح المصدر يستخدم لمراقبة حركة المرور على الشبكة والكشف عن الهجمات
   - **Suricata** : نظام متقدم لكشف التسلل يدعم المراقبة في الوقت الفعلي
2. انظمة منع التسلل **(Systems IPS –Intrusion Prevention)**
   - **Cisco Firepower**: يجمع بين جدار الحماية ونظام منع التسلل لحماية الشبكات
   - **Pato Alto Networks** : يوفر حماية متقدمة من التهديدات السيبرانية
3. برامج مكافحة الفيروسات والبرمجيات الخبيثة
   - **Kaspersky** : يوفر حماية شاملة من الفيروسات والبرمجيات الخبيثة
   - **Mc Afee:** برنامج متخصص في الكشف عن البرمجيات الضارة وحماية الأجهزة.
4. ادوات تحليل الشبكات
   - **Wireshark** : اداة مفتوحة المصدر لتحليل حركة المرور على الشبكة والكشف عن الانشطة المشبوهة.
   - **Nmap** : اداة مسح شبكات تستخدم لاكتشاف الاجهزة المتصلة والثغرات الأمنية.
     انظمة ادارة المعلومات والاحداث الأمنية **(SIEM)**
   - **Splunk** : يجمع بيانات الامان من مصادر مختلفة لتحليلها والكشف عن التهديدات
   - **IBM QRadar** : يوفر تحليلا متقدما الامان والكشف عن التهديدات في الوقت الفعلي
5. ادوات تحليل البرمجيات الخبيثة
   - **Cuckoo Sandbox** : بيئة افتراضية لتحليل سلوك البرمجيات الخبيثة.
   - **Virus Total** : خدمة عبر الانترنت لفحص الملفات والروابط بحثا عن البرمجيات الضارة
6. ادوات التحقيق الجنائي الرقمي
   - **EnCase** اداة متخصصة في التحقيق الجنائي الرقمي واستخراج الادلة
   - **FTK(Forensic Toolkit)** : يستخدم لتحليل البيانات واستعادة الملفات المحذوفة
7. ادوات مراقبة نقاط النهاية **(Response- EDR Endpoint Detection end)**
   - **Crowd Strike** : يوفر حماية متقدمة لنقاط النهاية والكشف عن التهديدات.
   - **Microsoft Defender for Endpoint** : اداة متكاملة لحماية الأجهزة من التهديدات السيبرانية
8. ادوات اختبار الاختراق **(Penetration Testing Tools)**
   - **Metasploit** : اطار عمل لاختبار الاختراق وتقييم الثغرات الأمنية
   - **Burp Suite** : اداة متخصصة في اختبار امان تطبيقات الويب
9. ادوات تحليل الثغرات الأمنية
   - **Nessus** : اداة مسح للثغرات الأمنية تستعل لتقييم امان الأنظمة.
   - **Open VAS** : نظام مفتوح المصدر لاكتشاف الثغرات الأمنية.



الشكل (2-3) مخطط أدوات الكشف عن الجرائم السيبرانية

3-2 التعامل مع رسائل البريد الإلكتروني المشبوهة

التعامل مع رسائل البريد الإلكتروني المشبوهة أمر بالغ الأهمية لحماية خصوصيتك وأمن معلوماتك. هنا بعض الخطوات التي يجب اتخاذها:

1-3-2 التعرف على رسائل البريد الإلكتروني المشبوهة:

1 . عنوان الرسالة غير معروف : إذا كان عنوان الرسالة غير معروف أو غير متوقع.

2. موضوع الرسالة مشبوه : إذا كان موضوع الرسالة مشبوه أو غير واضح.

3. رسالة تحوي على روابط أو ملفات مرفقة : إذا كانت الرسالة تحوي على روابط أو ملفات مرفقة غير متوقعة.

4. لغة الرسالة غير واضحة أو تحوي على أخطاء : إذا كانت لغة الرسالة غير واضحة أو تحوي على أخطاء إملائية أو نحوية.

- الأجراءات الأولية الواجب اتباعها :-

1. لا افتح الرسالة : لا افتح الرسالة إذا كانت مشبوهة.

2. لا انقر على الروابط : لا انقر على الروابط أو الملفات المرفقة.

3. لا رد على الرسالة : لا رد على الرسالة إذا كانت مشبوهة.

4. احذف الرسالة : احذف الرسالة مباشرة.

5. ابلاغ عن الرسالة : ابلاغ عن الرسالة إلى مزود الخدمة أو صاحب الحساب إذا كانت مشبوهة.

6. استخدم مرشح البريد الإلكتروني : استخدم مرشح البريد الإلكتروني لمنع رسائل البريد الإلكتروني المشبوهة من الوصول إلى صندوق الوارد.

7. تفعيل التحقق بخطوتين : تفعيل التحقق بخطوتين لضمان حماية الحساب.

8. استخدام كلمات مرور قوية : استخدام كلمات مرور قوية وفريدة لكل حساب بريد إلكتروني.

9. تحديث برنامج مكافحة الفيروسات : تحديث برنامج مكافحة الفيروسات بانتظام لحماية الجهاز من البرامج الخبيثة.

10. استخدام متصفح آمن : استخدام متصفح آمن لمنع تتبع النشاط عبر الإنترنت.

11. مراجعة إعدادات الخصوصية : مراجعة إعدادات الخصوصية للحساب بانتظام لضمان حماية البيانات.

2-3-2 أعراض اختراق حساب البريد الإلكتروني:

1. رسائل غير متوقعة في صندوق الصادر
2. تغييرات في إعدادات الحساب : تغييرات في إعدادات الحساب دون موافقة المستخدم.
3. رسائل خطأ عند تسجيل الدخول : رسائل خطأ عند تسجيل الدخول إلى الحساب.
4. نشاط مشبوه في سجل الدخول : نشاط مشبوه في سجل الدخول إلى الحساب.
5. البريد الإلكتروني المفقود أو المحذوف : البريد الإلكتروني المفقود أو المحذوف دون موافقة المستخدم.

3-3-2 إجراءات الاستجابة لاختراق حساب البريد الإلكتروني:

- غيّر كلمة المرور على الفور : غيّر كلمة المرور للحساب البريدي الإلكتروني على الفور.
- احذف الرسائل المشبوهة جميعاً: احذف جميع الرسائل المشبوهة من صندوق الوارد والصادر.
- فحص الحساب بحثًا عن البرامج الخبيثة : فحص الحساب بحثًا عن البرامج الخبيثة أو الفيروسات.
- إعلام مزود الخدمة : إعلام مزود الخدمة البريدي الإلكتروني بالاختراق.
- مراجعة إعدادات الأمان : مراجعة إعدادات الأمان للحساب وتعزيزها إذا لزم الأمر.
- تعزيز أمان حساب البريد الإلكتروني بعد الاختراق:
- تفعيل التحقق بخطوتين دائمًا : تفعيل التحقق بخطوتين دائمًا لحماية الحساب.
- استخدام كلمات مرور طويلة ومعقدة : استخدام كلمات مرور طويلة ومعقدة لكل حساب بريد إلكتروني.
- تحديث برنامج مكافحة الفايروسات
- استخدام متصفح آمن ومحدث : استخدام متصفح آمن ومحدث لمنع تتبع النشاط عبر الإنترنت.
- تفعيل خاصية حظر الرسائل المشبوهة : تفعيل خاصية حظر الرسائل المشبوهة في حساب البريد الإلكتروني.
- استخدام أداة فحص البريد الإلكتروني : استخدام أداة فحص البريد الإلكتروني لاكتشاف البرامج الخبيثة.
- مراجعة سجل الدخول بانتظام : مراجعة سجل الدخول إلى حساب البريد الإلكتروني بانتظام لاكتشاف أي نشاط مشبوه.
- استخدام كلمات مرور مختلفة : استخدام كلمات مرور مختلفة لكل حساب بريد إلكتروني وعلى الأجهزة.
- استخدم كلمات مرور طويلة ومعقدة تتضمن:
  - حروف كبيرة وصغيرة
  - أرقام
  - رموز خاصة **($,#,@,!)**

4-3-2 كيف يتم التعامل مع رسائل البريد الإلكتروني المشبوهة

التعامل مع رسائل البريد الإلكتروني المشبوهة يتطلب الحذر والاحتياط. فيما يلي بعض الخطوات التي يمكن اتخاذها:

1. لا تفتح الرسالة:

إذا كانت الرسالة من مرسل غير معروف أو تحوي على عنوان بريد إلكتروني غريب، لا تفتحها.

2. لا تنقر على الروابط:

أي روابط موجودة في الرسالة المشبوهة قد تكون خبيثة، فلا تنقر عليها.

3. لا تقم بتنزيل الملفات على جهازك:

أي ملفات متصلة بالرسالة المشبوهة قد تحوي على برامج خبيثة، فلا تقم بتنزيلها.

4. فحص عنوان البريد الإلكتروني:

تحقق من عنوان البريد الإلكتروني للمرسل، إذا كان غريبًا أو غير متوقع، فربما يكون مشبوهًا.

5. ابحث عن أخطاء الإملاء والقواعد:

الرسائل المشبوهة غالبًا ما تحوي على أخطاء إملائية وقواعدية، فاحترس منها.

6. لا تقدم معلومات شخصية:

لا تقدم أي معلومات شخصية مثل كلمات المرور أو بيانات البطاقة الإئتمانية في استجابة للرسالة المشبوهة.

7. قم بحذف الرسالة:

إذا كنت متأكداً من أن الرسالة مشبوهة، قم بحذفها على الفور.

8. قم بالإبلاغ عن الرسالة:

- قم بالإبلاغ عن الرسالة المشبوهة إلى مزود خدمة البريد الإلكتروني الخاص بك.
- استخدم خيار "تقرير كبريد مخبث" أو "تقرير كبريد غير مرغوب فيه" في صندوق الوارد.

9. قم بتحديث برامج الحماية:

- قم بتحديث برامج الحماية ضد الفيروسات والبرامج الخبيثة على جهازك.
- تأكد من أن برامج الحماية قادرة على الكشف عن آخر الثغرات الأمنية.

10. كن مستعدًا للهجوم:

- قم بإنشاء نسخة احتياطية من بياناتك الهامة.

- قم بتحديث كلمات المرور الخاصة بك جميعاً إلى كلمات مرور قوية وفريدة.

أعراض رسائل البريد الإلكتروني المشبوهة:

- عنوان بريد إلكتروني غريب أو غير متوقع.
- رسائل تحوي على أخطاء إملائية وقواعدية.
- رسائل تطلب معلومات شخصية أو مالية.
- رسائل تحوي على روابط أو ملفات مشبوهة.
- رسائل تهدد بالتعطيل أو الحذف إذا لم تقم باتخاذ إجراء معين.

أنواع رسائل البريد الإلكتروني المشبوهة:

- الاحتيال عبر البريد الإلكتروني **(Phishing)** : رسائل تطلب معلومات شخصية أو مالية.
- البريد الإلكتروني المزعج **(Spam)** : رسائل غير مرغوب فيها أو مشبوهة.
- البريد الإلكتروني الخبيث **(Malware)** : رسائل تحوي على برامج خبيثة أو فيروسات.

خطوات إضافية لحماية نفسك:

- استخدام مرشح بريد إلكتروني **filtration** الرسائل المشبوهة.
- عدم استخدام نفس كلمة المرور للحسابات جميعاً.
- استخدام التحقق بخطوتين لضمان حماية الحسابات.

أمان الحسابات الإلكترونية:

- استخدام كلمات مرور قوية وفريدة لكل حساب.
- تحديث كلمات المرور كل 60 إلى 90 يومًا.

حماية جهاز الكمبيوتر:

- تثبيت برامج حماية ضد الفيروسات والبرامج الخبيثة.
- تحديث البرامج والأمن بانتظام.
- استخدام جدار حماية لمنع الوصول غير المصرح به.

متابعة نشاط الحسابات:

- مراقبة حساباتك الإلكترونية بانتظام لاكتشاف أي نشاط مشبوه.

- استخدام إشعارات لتتبع نشاط الحسابات.

- الاتصال بالجهات المعنية في حالة اكتشاف أي نشاط مشبوه.

5-3-2 اهمية كلمة المرور واهمية التحقق الثنائي

اهمية كلمة المرور والتحقق الثنائي في حماية الحسابات والأمن السيبراني هي كبيرة.

أهمية كلمة المرور:

1. حماية الحسابات : كلمة المرور هي الخط الدفاعي الأول لحماية حساباتك من الوصول غير المصرح به.
2. صعوبة الاختراق : كلمات المرور القوية تجعل من الصعب على المخترقين اختراق حساباتك.
3. حماية البيانات : كلمة المرور تحمي بياناتك الشخصية والمالية من السرقة أو التدمير.
4. الوصول المصرح به : كلمة المرور تسمح فقط للأشخاص المصرح لهم بالوصول إلى حساباتك.

أهمية التحقق الثنائي (التحقق بخطوتين):

1. ضمان الحماية : التحقق الثنائي يضمن حماية حساباتك حتى إذا تم اختراق كلمة المرور.
2. تأكيد الهوية : التحقق الثنائي يؤكد هويتك قبل السماح بالوصول إلى حساباتك.
3. منع الاختراق : التحقق الثنائي يمنع المخترقين من الوصول إلى حساباتك حتى إذا عرفوا كلمة المرور.
4. زيادة الأمان : التحقق الثنائي يزيد من أمان حساب

6-3-2 مكونات التحقق الثنائي:

1. كلمة المرور : المكون الأول هو كلمة المرور التي تعرفها فقط أنت.
2. رمز التحقق : المكون الثاني هو رمز تحقق يرسل إلى:

- هاتفك المحمول خلال الرسائل القصيرة (SMS)أو الى بريد الكتروني آخر

- تطبيق تحقق على هاتفك مثل (جوجل أو ثنتيكاتور)

- بريد الكتروني آخر

7-3-2 أنواع التحقق الثنائي:

1. تحقق بوساطة رمز **SMS** : رمز يرسل عبر الرسائل القصيرة إلى هاتفك.
2. تحقق بوساطة تطبيق : رمز يظهر في تطبيق تحقق على هاتفك.
3. تحقق بوساطة بريد إلكتروني : رمز يرسل إلى بريد إلكتروني آخر مسجل مع حسابك.

4. تحقق بوساطة بصمة الوجه أو بصمة الإصبع : استخدام تقنيات البصمة الحيوية لالتقاط بصمة وجهك أو إصبعك.

8-3-2 فوائد التحقق الثنائي:

- زيادة أمان حساباتك

- حماية بياناتك الشخصية والمالية

- منع الاختراقات والوصول غير المصرح به

9-3-2 تطبيق التحقق الثنائي في الحياة اليومية:

1. حسابات البنك عبر الإنترنت : يستخدم التحقق الثنائي لحماية حساباتك البنكية عبر الإنترنت.
2. بريد إلكتروني : يستخدم التحقق الثنائي لحماية حسابات البريد الإلكتروني من الاختراق.
3. شبكات التواصل الاجتماعي : يستخدم التحقق الثنائي لحماية حساباتك على منصات التواصل الاجتماعي.
4. تطبيقات المحمول : يستخدم التحقق الثنائي لحماية تطبيقات المحمول مثل تطبيقات البنك والتسوق.
5. نظم الشركات: يستعمل التحقق الثنائي لحماية نظم الشركات وبياناتها الحساسة.

10-3-2 أخطاء شائعة عند استخدام التحقق الثنائي:

1. استخدام رموز تحقق ضعيفة
2. عدم تحديث تطبيقات التحقق
3. استخدام نفس رمز التحقق
4. عدم مراقبة نشاط حساباتك

11-3-2 خطوات لتعزيز أمان التحقق الثنائي:

1. استخدام رموز تحقق قوية : رموز طويلة ومتنوعة الأحرف والارقام.
2. تحديث تطبيقات التحقق بانتظام : لضمان حماية ضد الثغرات الأمنية.
3. استخدام رموز تحقق فريدة لكل حساب : عدم استخدام نفس الرمز لكل حساب.
4. مراقبة نشاط حساباتك بانتظام : لاكتشاف أي نشاط مشبوه.

5. استخدام ميزة "الوصول المسموح به فقط من الأجهزة المعروفة" : لمنع الوصول من أجهزة غير معروفة.

6. تفعيل إشعارات التحقق : لتلقي إشعارات عند حدوث أي نشاط مشبوه.

12-3-2 أفضل تطبيقات التحقق الثنائي:

1. جوجل أوثنتيكاتور **(Google Authenticator)**
2. أوثي **(Authy)**
3. مايكروسوفت أوثنتيكاتور **(Microsoft Authenticator)**
4. لاست باس أوثنتيكاتور **(Last)**

13-3-2 ميزات تطبيقات التحقق الثنائي:

1. جوجل أوثنتيكاتور **(Google Authenticator) :**

- رموز تحقق تلقائية
- دعم متعدد الحسابات
- لا يتطلب اتصال إنترنت

2. أوثي **(Authy)** :

- تحليل سلوك المستخدم لاكتشاف النشاط المشبوه
- دعم متعدد الحسابات
- توفير نسخة احتياطية من رموز التحقق

3. مايكروسوفت أوثنتيكاتور **(Microsoft Authenticator) :**

- دعم متعدد الحسابات
- تحليل سلوك المستخدم لاكتشاف النشاط المشبوه
- توفير نسخة احتياطية من رموز التحقق

4. لاست باس أوثنتيكاتور **(LastPass Authenticator)** :

- دعم متعدد الحسابات
- توفير نسخة احتياطية من رموز التحقق

- تحليل سلوك المستخدم لاكتشاف النشاط المشبوه

2-3-13 تحديثات وأمان تطبيقات التحقق الثنائي:

1. تحديثات دورية : جميع التطبيقات تقوم بتحديثات دورية لأمان النظام والتصحيح الأخطاء.
2. تشفير البيانات : جميع التطبيقات تشفر بيانات التحقق لمنع الوصول غير المصرح به.
3. تحليل سلوك المستخدم : بعض التطبيقات تحلل سلوك المستخدم لاكتشاف النشاط المشبوه.
4. إشعارات التحقق : جميع التطبيقات تقدم إشعارات عند حدوث أي نشاط مشبوه.

اختيار أفضل تطبيق تحقق ثنائي لك:

1. جوجل أوثنتيكاتور : مناسب لمستخدمي جوجل الذين يبحثون عن حل بسيط.
2. أوثي : مناسب للمستخدمين الذين يبحثون عن ميزات إضافية مثل تحليل السلوك.
3. مايكروسوفت أوثنتيكاتور : مناسب لمستخدمي مايكروسوفت الذين يبحثون عن حل متكامل.
4. لاست باس أوثنتيكاتور : مناسب للمستخدمين الذين يبحثون عن حل شامل لجميع حساباتهم.

2-3-14 كيف يتم اختيار وانشاء كلمة مرور قوية

1. اختيار كلمة مرور طويلة : كلمة مرور تتكون من 12 حرفًا على الأقل.
2. استخدام أحرف كبيرة وصغيرة : مزيج من الأحرف الكبيرة والصغيرة لزيادة التعقيد.
3. أرقام ورموز خاصة : إضافة أرقام ورموز خاصة مثل !,@,#,$,% لزيادة التعقيد.
4. كلمات غير متوقعة : استخدام كلمات غير متوقعة أو جمل قصيرة غير منطقية.
5. تجنب المعلومات الشخصية : تجنب استخدام معلومات شخصية مثل اسمك أو تاريخ ميلادك.

توصيات إضافية حول كلمة المرور:

1. استخدام جمل قصيرة : استخدام جمل قصيرة غير منطقية مع أرقام ورموز خاصة.
2. استبدال الأحرف : استبدال الأحرف او أرقام أو رموز خاصة (مثل @ بدلاً من "a").
3. استخدام كلمات غير إنجليزية : استخدام كلمات غير إنجليزية لزيادة التعقيد.
4. تجنب استخدام نفس كلمة المرور : استخدام كلمات مرور فريدة لكل حساب.
5. تحديث كلمة المرور : تحديث كلمة المرور كل 60 إلى 90 يوماً.

والشكل (2-4)يوضح ذلك.

الشكل (2-4) كيف يتم اختيار وانشاء كلمة مرور قوية

4-2 أمن الأجهزة والتطبيقات:

يتم تامين جميع الاجهزة والتطبيقات وتامين الشبكة عن طريق اتباع الخطوات الآتية:

1. تحديث نظام التشغيل : تحديث نظام التشغيل بانتظام لضمان حماية ضد الثغرات الأمنية.
2. تثبيت برنامج حماية ضد الفيروسات : تثبيت برنامج حماية ضد الفيروسات موثوق به لحماية الجهاز من البرامج الخبيثة.
3. استخدام كلمات مرور قوية : استخدام كلمات مرور قوية وفريدة لكل حساب على الجهاز.
4. تفعيل التحقق بخطوتين : تفعيل التحقق بخطوتين لضمان حماية الجهاز من الوصول غير المصرح به.
5. مراقبة النشاط المشبوه : مراقبة النشاط المشبوه على الجهاز واعتراض أي نشاط غير عادي.
6. استخدام شبكة افتراضية خاصة **(VPN) :** استخدام شبكة افتراضية خاصة لتحسين أمان الاتصال بالإنترنت.
7. تفعيل تشفير الشبكة : تفعيل تشفير الشبكة لحماية بياناتك أثناء النقل.
8. مراقبة نشاط الشبكة : مراقبة نشاط الشبكة واكتشاف أي نشاط مشبوه.

9. استخدام كلمات مرور قوية للروتر : استخدام كلمات مرور قوية للروتر لحماية شبكتك المحلية.
10. تحديث برامج الروتر : تحديث برامج الروتر بانتظام لضمان حماية ضد الثغرات الأمنية.

1-4-2 أمن البيانات:

1. استخدام تشفير البيانات : استخدام تشفير البيانات لحماية معلوماتك الشخصية والمهنية.
2. إنشاء نسخ احتياطية : إنشاء نسخ احتياطية من بياناتك بانتظام لمنع فقدانها.
3. مراجعة إعدادات خصوصية التطبيقات : مراجعة إعدادات خصوصية التطبيقات
4. استخدام مدير كلمات المرور : استخدام مدير كلمات المرور لتخزين كلمات المرور بشكل آمن.
5. مراجعة سياسات حفظ البيانات : مراجعة سياسات حفظ البيانات لمواقع الإنترنت وتطبيقاتك.
6. استخدام بروتوكول **HTTPS** : استخدام بروتوكول **HTTPS** عند تصفح مواقع الإنترنت لحماية بياناتك.
7. مراقبة نشاط الحساب : مراقبة نشاط حسابك على مواقع الإنترنت وتطبيقاتك لاكتشاف أي نشاط مشبوه.
8. استخدام تقنيات التشفير المتقدمة : استخدام تقنيات التشفير المتقدمة مثل التشفير الثنائي لحماية بياناتك

5-2 الحفاظ على الخصوصية

ان الحفاظ على الخصوصية أمر بالغ الأهمية في عالم رقمي يتطور باستمرار. هنا بعض الطرق التي يمكن من خلالها الحفاظ على الخصوصية:

1-5-2 حماية البيانات الشخصية:

1. استخدام كلمات مرور قوية: استخدام كلمات مرور فريدة وطويلة لكل حساب.
2. تفعيل التحقق بخطوتين: تفعيل التحقق بخطوتين لضمان الحماية الإضافية.
3. تحديث البرامج والأمن: تحديث البرامج والأمن بانتظام لسد الثغرات الأمنية.

2-5-2 حماية خصوصية الإنترنت:

1. استخدام شبكة افتراضية خاصة **(VPN):** استخدام **VPN** لحماية بيانات الإنترنت من المراقبة.
2. تفعيل خاصية حذف سجل التصفح: تفعيل خاصية حذف سجل التصفح لمنع تتبع النشاط عبر الإنترنت.

3. استخدام متصفحات خاصة: استخدام متصفحات خاصة مثل تور أو برافزي لتحسين الخصوصية.

3-5-2 حماية خصوصية الهاتف المحمول:

1. استخدام قفل الشاشة: استخدام قفل الشاشة بكلمة مرور أو بصمة الإصبع.
2. تفعيل خاصية تحديد الموقع: تفعيل خاصية تحديد الموقع فقط.
3. تحديث نظام التشغيل: تحديث نظام التشغيل بانتظام لسد الثغرات الأمنية.
4. استخدام تطبيقات موثوقة: استخدام تطبيقات موثوقة من متاجر التطبيقات الرسمية.
5. تفعيل خاصية حذف البيانات تلقائياً تفعيل خاصية حذف البيانات تلقائيًا في حالة فقدان أو سرقة الهاتف.
6. استخدام برنامج حماية الهاتف: استخدام برنامج حماية الهاتف لمراقبة النشاط المشبوه وحماية البيانات.

4-5-2 حماية الخصوصية على وسائل التواصل الاجتماعي:

1. تعديل إعدادات الخصوصية: تعديل إعدادات الخصوصية على منصات التواصل الاجتماعي لتحكم في من يمكنه رؤية المحتوى.
2. استخدام كلمات مرور قوية: استخدام كلمات مرور فريدة وطويلة لكل منصة تواصل اجتماعي.
3. تفعيل التحقق بخطوتين: تفعيل التحقق بخطوتين لضمان الحماية على وسائل التواصل الاجتماعي وتتم عن طريق :
   - الخطوة الأولى: كلمة المرور: المستخدم يدخل كلمة مروره.
   - الخطوة الثانية: رمز التحقق: المستخدم يتلقى رمز تحقق عبر:
     - الرسائل القصيرة (SMS)
     - تطبيق تحقق على الهاتف
     - بريد إلكتروني آخر
4. مراقبة طلبات الصداقة: مراقبة طلبات الصداقة والاتصال على منصات التواصل الاجتماعي.
5. إخفاء المعلومات الشخصية: إخفاء المعلومات الشخصية مثل العنوان ورقم الهاتف.
6. استخدام خاصية التحكم في المنشورات: استخدام خاصية التحكم في المنشورات لتحديد من يمكنه رؤية المنشورات.
7. تفعيل إشعارات الأمان: تفعيل إشعارات الأمان لتحذيرات حول النشاط المشبوه على حسابك.

5-5-2 أفضل الممارسات لحماية الخصوصية على الإنترنت:

- تحديثات الأمان: كن مستعدًا لتحديثات الأمان والبرامج بانتظام.
- استخدام أدوات حماية الخصوصية: استخدام أدوات حماية الخصوصية مثل **VPN** وبرامج حماية البيانات.

- ❖ اليقظة من رسائل البريد الإلكتروني المشبوهة: كن متيقظًا من رسائل البريد الإلكتروني المشبوهة والروابط غير الأمنة.
- ❖ حفظ كلمات المرور بأمان: احفظ كلمات المرور بأمان وعدم مشاركتها مع الآخرين.
- ❖ استخدام متصفحات خاصة: استخدام متصفحات خاصة مثل تور أو برافزي لتحسين الخصوصية.
- ❖ تفعيل خاصية حذف سجل التصفح: تفعيل خاصية حذف سجل التصفح لمنع تتبع النشاط عبر الإنترنت.
- ❖ قراءة سياسات الخصوصية: كن مستعدًا لقراءة سياسات الخصوصية لمواقع الإنترنت قبل تقديم البيانات الشخصية.
- ❖ استخدام أدوات حماية الهوية: استخدام أدوات حماية الهوية مثل Authenticator لتعزيز الأمن.

2- 6 امن الشبكات

امن الشبكة هو مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية شبكة الحاسوب والبيانات الموجودة عليها من التهديدات والهجمات الأمنية.

2-6-1 أهداف أمن الشبكة:

1. حماية البيانات: حماية البيانات من الوصول غير المصرح به أو السرقة أو التدمير.
2. حماية الشبكة: حماية الشبكة من الهجمات والاختراقات التي قد تسبب ضررًا أو تعطيلًا.
3. ضمان الخصوصية: ضمان خصوصية البيانات والمعلومات على الشبكة.
4. ضمان السلامة: ضمان سلامة البيانات والمعلومات على الشبكة.

2-6-2 أنواع أمن الشبكة:

1. أمن الشبكة المحلية **(LAN)**: حماية شبكات المحلية من الهجمات والاختراقات.
2. أمن الشبكة الواسعة **(WAN)**: حماية شبكات الواسعة من الهجمات والاختراقات.
3. أمن الإنترنت: حماية الاتصالات عبر الإنترنت من الهجمات والاختراقات.
4. أمن اللاسلكية: حماية الشبكات اللاسلكية من الهجمات والاختراقات.

2-6-3 مكونات أمن الشبكة:

1. جدار الحماية **(Firewall):** برنامج أو جهاز يتحكم في حركة البيانات بين الشبكات.
2. برامج حماية ضد الفيروسات: برامج تقوم بفحص الشبكة والجهاز بحثًا عن الفيروسات والبرامج الخبيثة.
3. تشفير البيانات: تقنية لتشفير البيانات أثناء نقلها عبر الشبكة.

4. التحقق بخطوتين: عملية تأكيد هوية المستخدمين قبل السماح لهم بالوصول إلى الشبكة.

5. مراقبة الشبكة: عملية مراقبة نشاط الشبكة لاكتشاف أي تهديدات أمنية.

4-6-2 أهمية أمن الشبكة:

1. حماية البيانات الحساسة: حماية البيانات الحساسة من الوصول غير المصرح به أو السرقة.

2. منع الهجمات السيبرانية: منع الهجمات السيبرانية التي قد تسبب ضررًا أو تعطيلًا للشبكة.

3. ضمان الاستمرارية: ضمان استمرارية عمل الشبكة والأنظمة المتصلة بها.

4. الحفاظ على الخصوصية: الحفاظ على خصوصية البيانات والمعلومات على الشبكة.

5-6-2 تهديدات أمن الشبكة:

1. الفيروسات والبرامج الخبيثة

2. الهجمات الدوارة **(DDoS)**

3. الاختراقات غير المصرح بها

4. سرقة البيانات الحساسة

5. التعطيلات السيبرانية

6. البريد الإلكتروني المزعج **(Spam)** والبريد الإلكتروني الخبيث **(Phishing):** رسائل بريد إلكتروني غير مرغوب فيها أو خبيثة.

7. التحكم عن بُعد غير المصرح به **(RATs)**: برامج خبيثة تسمح للمخترقين بالتحكم في جهازك عن بُعد.

8. البرامج الخبيثة المضمنة في الإعلانات **(Malvertising):** إعلانات خبيثة تحوي على برامج خبيثة.

9. الهجمات على نقاط الضعف **(Zero-Day Exploits)**: هجمات تستغل نقاط ضعف غير معروفة في البرامج.

10. البرامج الخبيثة التي تنتشر عبر الشبكات الاجتماعية: برامج خبيثة تنشر عبر منصات التواصل الاجتماعي.

6-6-2 طرق الوقاية من تهديدات أمن الشبكة:

1. تحديث البرامج والأمن بانتظام

2. استخدام برامج حماية ضد الفيروسات

3. تفعيل جدار الحماية

4. استخدام كلمات مرور قوية

5. مراقبة الشبكة بانتظام

7-6-2 أدوات الوقاية من تهديدات أمن الشبكة:

1. برامج حماية ضد الفيروسات

2. أجهزة جدار الحماية

3. أنظمة الكشف عن التهديدات

4. برامج فحص الشبكة

7-2 التصدي للهجمات والرد عليها

تصدي الهجمات والرد عليها يتطلب استراتيجية شاملة تتضمن خطوات عديدة :

1. اكتشاف الهجوم: الكشف عن الهجوم في أقرب وقت ممكن باستخدام أنظمة الكشف عن التهديدات.

2. تحليل الهجوم: تحليل الهجوم لتحديد نوعه ومدى تأثيره.

3. إزالة الهجوم ويكون عن طريق :

- عزل الشبكة أو الجهاز المتأثر
- حذف البرامج الخبيثة
- إعادة تشغيل الأنظمة

4. الرد على الهجوم: الرد على الهجوم عن طريق :

- إرسال إشعارات إلى المستخدمين المتأثرين
- تحديث البرامج والأمن
- تعزيز أمن الشبكة

5. متابعة الهجوم: متابعة الهجوم لضمان إزالته الكاملة ومنع تكراره.

1-7-2 استراتيجيات الرد على الهجمات:

1. الرد السريع: هو استراتيجيةردود فعل سريعة وفاعلة على الهجمات.

2. الرد الموحد: تنسيق جهود الرد بين جميع الأطراف المعنية لضمان ردود فعل موحدة وفاعلة.

3. الرد المتكامل: دمج جميع العناصر الأمنية لضمان ردود فعل شاملة على الهجمات.

4. الرد المتعلم: استخدام البيانات والخبرات السابقة لتعزيز ردود الفعل على الهجمات وتحسين استراتيجيات الرد.

5. الرد المنسق مع الجهات الخارجية: التعاون مع الجهات الخارجية مثل الشرطة والجهات الأمنية الأخرى لضمان ردود فعل على الهجمات.

2-7-2 أدوات الرد على الهجمات:

1. أنظمة الكشف عن التهديدات **(IDS/IPS)**
2. برامج حماية ضد الفيروسات
3. أجهزة جدار الحماية
4. أنظمة الرد السريع على الهجمات **(IRMS)**
5. برامج تحليل السلوك المشبوه

3-7-2 مبادئ الرد على الهجمات:

1. السرعة: الرد السريع على الهجمات لمنع الأضرار.
2. الدقة: ضمان دقة ردود الفعل لمنع الأضرار غير المقصودة.
3. الشفافية: تنفيذ ردود الفعل بشفافية لضمان ثقة جميع الأطراف.
4. التعاون: التعاون بين جميع الأطراف لضمان ردود فعل موحدة وفعالة.
5. التعلم المستمر: التعلم من الهجمات السابقة وتحديث استراتيجيات الرد لتحسين فاعليتها.
6. المراقبة المستمرة: مراقبة الشبكة والأنظمة بانتظام لاكتشاف أي تهديدات أمنية جديدة.
7. التحديث المستمر: تحديث البرامج والأمن بانتظام لسد الثغرات الأمنية وتحسين أمن الشبكة.
8. التواصل الفعال: التواصل الفعال مع جميع الأطراف المعنية لضمان فهم الوضع وتحقيق ردود فعل موحدة.

8-2 التدريب المستمر والتوعية الدورية

التدريب المستمر والتوعية الدورية ضروريان لتعزيز أمن المعلومات والرد على الهجمات، وتشمل الخطوات التالية:

1-8-2 التدريب المستمر:

1. دورات تدريبية منتظمة: تقديم دورات تدريبية منتظمة للموظفين حول أمن المعلومات والرد على الهجمات.

2. برامج تدريبية عبر الإنترنت: تقديم برامج تدريبية عبر الإنترنت للموظفين لتعزيز مهاراتهم في أمن المعلومات.

3. تمارين محاكاة: إجراء تمارين محاكاة للهجمات لتدريب الموظفين على الرد السريع والفعال.

4. برامج شهادات: تقديم برامج شهادات للموظفين في أمن المعلومات والرد على الهجمات.

2-8-2 التوعية الدورية:

1. حملات توعية: إطلاق حملات توعية دورية للموظفين حول أهمية أمن المعلومات والرد على الهجمات.

2. رسائل بريدية: إرسال رسائل بريدية دورية للموظفين حول آخر التحديثات والأخبار في مجال أمن المعلومات.

3. لقاءات دورية: عقده لقاءات دورية مع الموظفين لمناقشة قضايا أمن المعلومات والرد على الهجمات.

4. مواد توعية: توزيع مواد توعية مثل الكتب والملصقات والبوسترات حول أمن المعلومات والرد على الهجمات.

5. ألعاب التدريب الأمني: ألعاب تعليمية تقليدية وتفاعلية لتدريب الموظفين على أمن المعلومات والرد على الهجمات.

6. أنظمة إدارة التعلم: أنظمة إلكترونية لإدارة برامج التدريب وتقديم محتوى تعليمي للموظفين.

7. منتديات النقاش: منتديات إلكترونية للموظفين لمناقشة قضايا أمن المعلومات والرد على الهجمات.

3-8-2 مراحل تنفيذ برنامج التوعية والتدريب:

1. التخطيط: تخطيط برنامج التوعية والتدريب وتحديد الأهداف والمحتوى.

2. التطوير: تطوير محتوى التدريب واختيار الأدوات المناسبة.

3. التنفيذ: تنفيذ برنامج التوعية والتدريب وتقديم الدورات التدريبية.

4. التقويم: تقويم برنامج التوعية والتدريب وتحديثه حسب الحاجة.

5. المتابعة: متابعة الموظفين بعد التدريب لضمان تطبيق المعرفة المكتسبة.

اسئلة الفصل الثاني

س1 : ماهي التهديدات السيبرانية اذكر مصادر هذه التهديدات ؟

س2: كيف يتم التعرف على رسائل البريد الإلكتروني المشبوهة وكيف يتم التعامل معها ؟

س3: عدد مكونات التحقق الثنائي وما هي انواعه ؟

س4 : كيف يتم اختيار وانشاء كلمة مرور قوية ؟

س5 : كيف تتم حماية خصوصية الهاتف المحمول ؟

س6 : ما هي أفضل الممارسات لحماية الخصوصية على الإنترنت ؟

س7 : ما المقصود بأمن الشبكة وما هي مكوناتها ؟

س8 : اذكر خطوات التصدي للهجمات وما هي الاستراتيجيات المتبعة للرد عليها ؟

الفصل الثالث

الهندسة الاجتماعية (Social Engineering)

الأهداف

من المتوقع أن يكون الطالب قادراً على أن :

1. يتعرف على مفهوم الهندسة الاجتماعية واساليبها.
2. يتعرف الى امثلة مختلفة من هجمات الهندسة الاجتماعية وكيفية حدوثها.
3. يتمكن من تقييم الرسائل والاتصالات للكشف عن محاولات الهندسة الاجتماعية.
4. يستخدم استراتيجيات لتجنب الافصاح عن المعلومات الشخصية في الاتصالات غير الموثوقة .

الهندسة الاجتماعية

في عالمنا المعاصر الذي يعتمد بشكل كبير على التكنولوجيا، أصبحت معلوماتنا الشخصية والمهنية قيمة لا تقدر بثمن. ومن هذا المنطلق، ظهرت تهديدات جديدة لأمن هذه المعلومات، ومن أبرزها ما يُعرف بـ "هجمات الهندسة الاجتماعية".

الهندسة الاجتماعية هي مجموعة من الأساليب والتقنيات التي يستخدمها المهاجمون لخداع الأفراد أو المؤسسات للحصول على معلومات حساسة بطريقة غير مباشرة، دون الحاجة إلى اختراق الأنظمة التكنولوجية. وتختلف أساليب الهندسة الاجتماعية وتتنوع لتشمل العديد من الطرق التي قد تكون غير متوقعة أو قد تظهر كأنها طلبات عادية.

يتناول هذا الفصل في البداية تعريف هجمات الهندسة الاجتماعية وأنواعها المختلفة مثل "التحايل الهاتفي" و"الهجمات عبر البريد الإلكتروني" (مثل التصيد الإلكتروني)، مرورًا بأساليب وتقنيات استخدامها مثل التلاعب النفسي، واستغلال الثقة، ثم يسلط الضوء على الأمثلة الواقعية لهذه الهجمات.

كما سيتناول الفصل الآثار والخطر الذي يترتب على هذه الهجمات، سواء كان على مستوى الأفراد أو المؤسسات، وتأثيراتها طويلة الأمد على الأمان الشخصي والتنظيمي. وفي نهاية الفصل، سنتعرف على طرق الحماية من هذه الهجمات، بما في ذلك الأساليب الوقائية والتقنيات الحديثة التي تساعد في الكشف عن محاولات الهندسة الاجتماعية، بالإضافة إلى دور الأفراد والمؤسسات في الوقاية منها. كما سنتعرف على دور التكنولوجيا في مكافحة هذه الهجمات وكيفية تطوير الأدوات والأنظمة التي تسهم في تعزيز الأمان الرقمي وحماية المعلومات الحساسة.

إن فهم هجمات الهندسة الاجتماعية وكيفية الوقاية منها يعد أمرًا بالغ الأهمية في العصر الرقمي، حيث تزداد الهجمات الإلكترونية يومًا بعد يوم. لذلك، يعتبر هذا الموضوع من المواضيع الحيوية التي يجب على الجميع الإلمام بها.

1-3 مفهوم الهندسة الاجتماعية (Social Engineering Concept)

الهندسة الإجتماعية هي فن التلاعب بالأشخاص لأداء أفعال أو الإقرار بمعلومات حساسة. مثل بناء الثقة او اثارة عواطف الخوف والطمع بين المخترق **(Hacker)** والأشخاص المستهدفين وجعلهم يتصرفون بطريقة سريعة بدون تفكير. وجمع اكبر قدر من المعلومات ثم البدء بالإبتزاز او الإختراق وغيرها وتعتبر هذه الطرق من أسهل واكثر الطرق شيوعاً والمسببة بكوارث من ناحية الإختراقات والابتزاز على مستوى الافراد والشركات وغيرها. يوجد طرق كثيرة للهندسة الإجتماعية مثل التمثيل، الدخول الغير مصرح به للأماكن الخاصة بعد انتحال الجهة المصرح بها للدخول وغيرها الكثير من الأمثلة، والشكل (3-1) يوضح رسم توضيحي عن كيفية التلاعب بالأشخاص في الهندسة الاجتماعية.

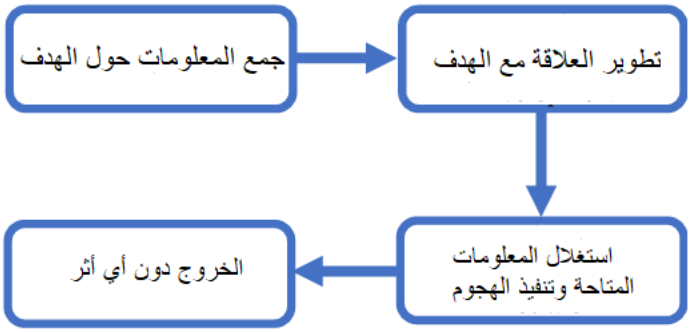
شكل (3-1) التلاعب بالاشخاص في الهندسة الاجتماعية

تتزايد هجمات الهندسة الاجتماعية بسرعة في شبكات اليوم. وتهدف إلى التلاعب بالأفراد والمؤسسات لإفشاء بيانات قيمة وحساسة لصالح مجرمي الإنترنت. وتتحدى الهندسة الاجتماعية أمن جميع الشبكات بغض النظر عن قوة أنظمة اكتشاف التسلل وأنظمة برامج مكافحة الفيروسات. ومن المرجح أن يثق البشر في البشر الآخرين مقارنة بأجهزة الكمبيوتر أو التقنيات. وبالتالي، فهم الحلقة الأضعف في سلسلة الأمن. تؤثر الأنشطة الخبيثة التي تتم من خلال التفاعلات البشرية على الشخص نفسياً لإفشاء معلومات سرية أو كسر إجراءات الأمان. وبسبب هذه التفاعلات البشرية، تعد هجمات الهندسة الاجتماعية أقوى الهجمات لأنها تهدد جميع الأنظمة والشبكات. ولا يمكن منعها باستخدام حلول البرامج أو الأجهزة طالما لم يتم تدريب الأشخاص على منع هذه الهجمات. يختار مجرمو الإنترنت هذه الهجمات عندما لا توجد طريقة لاختراق نظام بدون ثغرات تقنية.

على الرغم من أن هجمات الهندسة الاجتماعية تختلف عن بعضها البعض، إلا أنها تتمتع بنمط مشترك مع مراحل مماثلة. يتضمن النمط المشترك أربع مراحل:

1) جمع المعلومات حول الهدف.
2) تطوير العلاقة مع الهدف.
3) استغلال المعلومات المتاحة وتنفيذ الهجوم.
4) الخروج دون أي أثر.

الشكل (3-2) يوضح مراحل هجمات الهندسة الاجتماعية



الشكل (3-2) يوضح مراحل هجمات الهندسة الاجتماعية

و يمكن تصنيف هجمات الهندسة الاجتماعية إلى فئتين: هجمات بشرية و هجمات معتمدة على البرمجيات كما هو موضح في الشكل (3-3).

الشكل (3-3) تصنيف الهجمات الاجتماعية

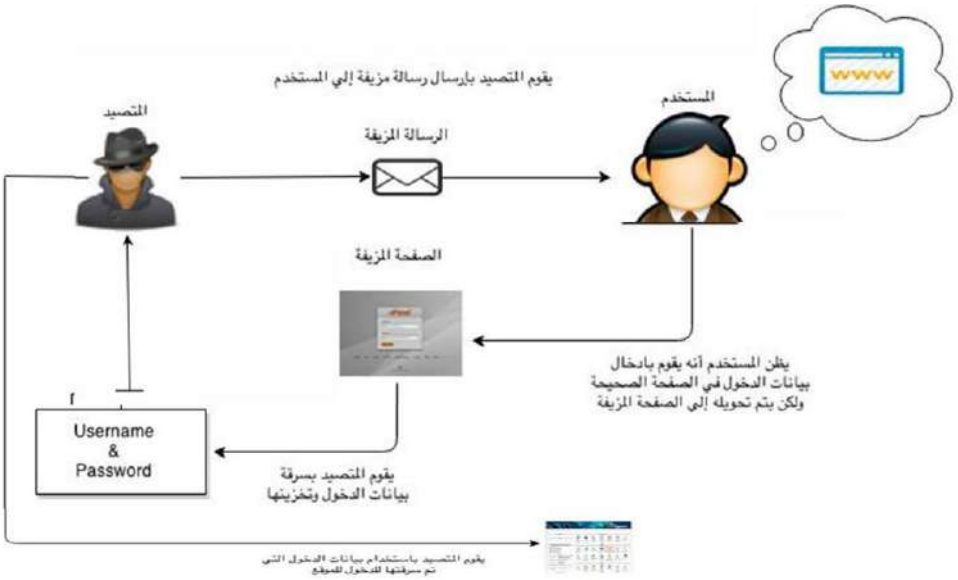
في الهجمات القائمة على الانسان، ينفذ المهاجم الهجوم شخصيًا من خلال التفاعل مع الهدف لجمع المعلومات المطلوبة. وبالتالي، يمكنهم التأثير على عدد محدود من الضحايا. بينما الهجمات القائمة على البرامج باستخدام أجهزة مثل أجهزة الكمبيوتر أو الهواتف المحمولة للحصول على معلومات من الضحايا يمكنهم مهاجمة العديد من الضحايا في بضع ثوانٍ. ويمكننا أيضًا تصنيف هذه الهجمات إلى فئتين رئيسيتين: مباشرة وغير مباشرة. تستخدم الهجمات المباشرة اتصالا مباشر بين المهاجم والضحية لتنفيذ الهجوم. تشير إلى الهجمات التي يتم تنفيذها عبر الاتصال الجسدي أو المكالمات الصوتية. قد تتطلب أيضًا وجود المهاجم في منطقة عمل الضحية لتنفيذ الهجوم. لا تتطلب الهجمات المصنفة ضمن الفئة غير المباشرة وجود المهاجم لشن هجوم. يمكن شن الهجوم عن بُعد عبر برنامج ضار محمول بواسطة مرفقات البريد الإلكتروني أو رسائل **SMS**.

2-3 أنواع هجمات الهندسة الاجتماعية

1. التصيد الالكتروني (Phishing)

وهو من أشهر أنواع هجمات الهندسة الاجتماعية شيوعا يتضمن إرسال رسائل بريد إلكتروني أو رسائل مزيفة تبدو كأنها من مصدر موثوق، مثل البنوك أو الشركات الكبرى، بهدف خداع الضحية لإعطائها معلومات حساسة مثل كلمات المرور أو تفاصيل الحسابات.

- ✓ **مثال :**رسالة مزيفة من بريد الإلكتروني تدعي أنها من بنك او من شركة معروفة تطلب من الضحية تحديث بيانات الحساب عبر رابط مزيف والشكل (3-4) يوضح ذلك.



شكل (3-4) يوضح التصيد الاحتيالي

2. التصيد عبر الهاتف (Vishing)

هذا النوع من الهجوم يعتمد على الاتصال الهاتفي، حيث يتظاهر المهاجم بأنه موظف في مؤسسة معروفة ويطلب من الضحية تقديم بيانات حساسة.

- ✓ **المثال** اتصال هاتفي من موظف بنك او شركة معينة يطلب من الضحية تقديم تفاصيل حسابه بسبب أنشطة مشبوهة حدثت للحساب.

3. التصيد عبر الرسائل النصية (Smishing)

يعتمد هذا النوع من الهجوم على إرسال رسائل نصية الى الجهة المستهدفة تحوي على روابط مزيفة او تطلب منه تثبيت برامج وبالحقيقة تكون هذه البرامج ضارة تهدف إلى سرقة بيانات شخصية.

- **مثال** رسالة نصية تطلب من الضحية إدخال بياناتها على صفحة مزيفة تبدو مطابقة للصفحة الحقيقية لتحديث حسابها البنكي او حسابات شخصية أخرى وعند ادخال المعلومات للتحديث يقوم المهاجم بسرقة معلومات الحساب.

4. الاحتيال باستخدام انتحال الهوية (Impersonation)

في هذا النوع من الهجوم ينتحل المهاجم شخصية اخرى يتظاهر بشخص آخر (مثل موظف حكومي، مدير، أو زميل في العمل) عائد للجهة المستهدفة للحصول على معلومات أو موارد حساسة ويعتمد على كسب ثقة الضحية.

- **مثال** مهاجم يتظاهر بأنه المدير ويطلب من الموظف المستهدف إرسال معلومات حساسة أو تنفيذ مهام مالية، الشكل (3-5) يوضح كيفية استخدام أسلوب انتحال الشخصية.

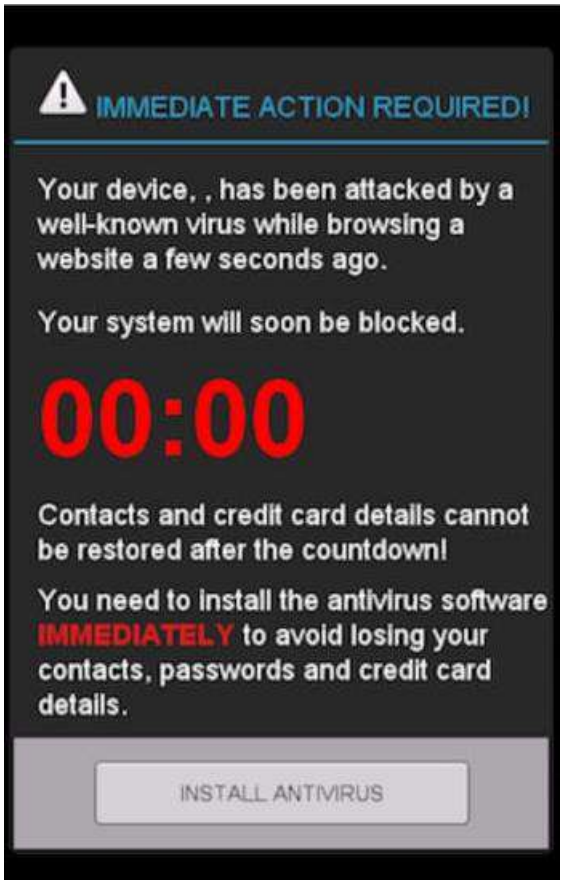
الشكل (3-5) استخدام أسلوب انتحال الشخصية

5. التلاعب العاطفي (Emotional Manipulation)

يتم استخدام هذا النوع من الأساليب في هجمات الهندسة الاجتماعية لتحقيق أهداف المهاجم من خلال الضغط النفسي على الضحية عن طريق استغلال المشاعر الإنسانية مثل الخوف، الرحمة، الطمع لإقناع الضحية بالكشف عن معلومات حساسة أو اتخاذ إجراءات سريعة وبدون تفكير.

انواع التلاعب العاطفي:

1. **الخوف :** عن طريق اثارة مشاعر الخوف لدى الضحية ليجعلها تتصرف بشكل سريع أو تحت ضغط الوقت بإرسال رسالة بريد الكتروني مزيف او مكالمة هاتفية تخبر الضحية بان حسابه يتعرض للاختراق ويطلب منه معلومات الحساب لتجنب الاختراق، الشكل (3-6) يوضح للضحية بان حسابه تم اختراقه ويجب عليه ان يقوم بتحميل البرنامج في الصفحة بشكل فوري لتجنب فقدان الحساب وادخال معلومات حسابه.



الشكل (3-6) رسالة تخبر الضحية باختراق حسابه

2. **الرحمة :** ي قوم المهاجم باختلاق مشكلة أو حالة طارئة تستدعي مساعدة مالية أو شخصية عاجلة مثل تلقي رسالة بريد إلكتروني من شخص يدعي أنه أحد أفراد العائلة، يروي فيها قصة عن حادث أو مرض مفاجئ، ويطلب منك إرسال أموال أو بيانات حساسة بشكل عاجل.
3. **الطمع :** يتم تحفيز الضحية باستخدام مغريات مالية أو مكافآت تجعلها تسعى للحصول على شيء مغري دون التفكير في العواقب بإرسال روابط مزيفة للضحية للاشتراك بمسابقة او التقديم على وظيفة مرموقة بمرتب عالي، الشكل (3-7) يوضح صفحات مزيفة لفرص عمل.

الشكل (3-7) صفحات مزيفة لفرص عمل

يقوم المهاجم بإرسال روابط للضحية يخبره عن الفوز بجوائز مالية كبيرة او الحصول على فرص عمل بمرتب مغري، ومن أبرز انواع الهجمات في الهندسة الاجتماعية :

1. الهجوم عبر الشبكات الاجتماعية (Social Media Attacks)

الهجوم عبر شبكات التواصل الاجتماعي هو استخدام المعلومات المتاحة على منصات التواصل الاجتماعي مثل فيسبوك، تويتر، أو الانستغرام لتنفيذ هجوم يقوم المهاجمون في هذا النوع بجمع وتحليل الملفات الشخصية للمستخدمين واستخدام المعلومات الشخصية أو المهنية في الهجوم.

هناك العديد من أنواع الهجمات عبر الشبكات الاجتماعية منها:

- **تحليل البيانات:** المهاجمون يقومون بجمع معلومات من حسابات الضحايا على وسائل التواصل الاجتماعي مثل الأماكن التي يزورونها، الأصدقاء، أماكن العمل، الهوايات، والعلاقات الشخصية لاستخدامها في الهجمات.
- **استغلال الثقة :** المهاجم يستخدم حسابات حقيقية ليتظاهر بأنهم أشخاص موثوقين، مثل الأصدقاء أو الزملاء، لطلب معلومات أو أموال.

- **الاستهداف المباشر :** المهاجم يرسل رسائل مباشرة لشخص معين مستغلاً المعلومات المتاحة من حساباتهم.

مثال هجوم عبر فيسبوك (استغلال الثقة) :مهاجم يرسل رسالة مباشرة عبر فيسبوك يتظاهر بأنه صديق قديم، ويطلب منك المساعدة المالية بشكل عاجل. يمكن أن يتظاهر بأنه في مشكلة خطيرة مثل حادث سيارة أو مشاكل صحية، الشكل (3-8) يوضح التصيد في مواقع التواصل الاجتماعي.

الشكل (3-8) التصيد في مواقع التواصل الاجتماعي

2. هجوم المغازلة (Baiting)

يعتمد هذا الاسلوب على تقديم عروض مغرية للضحية مثل تنزيل ملفات مجانية، أو تقديم هدايا، أو شيء مغرٍ آخر، وفي الحقيقة، يؤدي هذا العرض إلى تحميل برامج ضارة على الجهاز لسرقة المعلومات الحساسة مثل ارسال رابط عبر رسالة بريد الكتروني يحتوي على برنامج مشاهدة أفلام وفي الحقيقة يحتوي على برامج تجسس وسرقة للمعلومات من جهاز الضحية الشكل (3-9) يوضح التصيد عبر الملفات المرفقة.

الشكل (3-9) التصيد عبر الملفات المرفقة

3. التهديدات المباشرة (Pretexting)

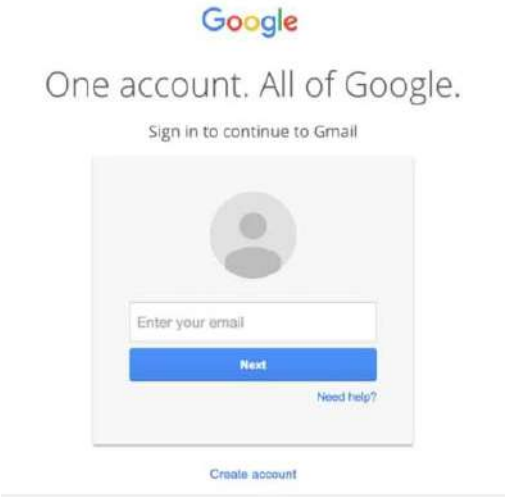
يقوم المهاجم بابتكار قصة كاذبة لإقناع الضحية بالكشف عن معلومات حساسة يقوم المهاجم بالاتصال بالضحية مدعيًا أنه محقق أو موظف حكومي ويطلب تفاصيل حساسة.

3-3 أساليب وتقنيات الهندسة الاجتماعية:

الهندسة الاجتماعية تستغل جوانب نفسية وسلوكية لدى الأفراد، بهدف التأثير عليهم بشكل يتيح للمهاجم الوصول إلى معلومات أو أنظمة محمية. وفيما يلي توضيح لكل من أساليب وتقنيات الهندسة الاجتماعية التي قد يتبعها المهاجمون لتحقيق أهدافهم.

1- انشاء الثقة (Trust Building)

هو أسلوب شائع في الهندسة الاجتماعية حيث يقوم المهاجم باستخدام الثقة المفرطة التي قد يمتلكها الضحية في أشخاص آخرين، سواء كانوا زملاء أو جهات موثوقة. الهدف هو جعل الضحية تشعر بالراحة في تقديم معلومات حساسة. المهاجم يتظاهر بأنه شخص موثوق أو جهة معروفة (مثل موظف في الشركة أو صفحات رسمية) كما في الشكل (3-10). يسعى المهاجم لكسب ثقة الضحية عن طريق التفاعل المريح معها، مما يجعلها تشعر بالأمان. بمجرد أن يشعر المهاجم أن الضحية وثق به بما يكفي، يطلب منها معلومات حساسة مثل كلمات المرور أو تفاصيل حسابات.مثلا المهاجم يتظاهر بأنه موظف الدعم الفني في الشركة ويطلب من الضحية إعطاءه كلمة مرور الحساب للوصول لحل مشكلة مزعومة والشكل (3-10) يوضح صفحة مزيفة تشبه الصفحة الرسمية تخبر الضحية بإدخال الايميل والرقم السري.



الشكل (3-10) صفحة مزيفة تشبه الصفحة الرسمية

2- استغلال الطوارئ (Emergency Exploiting)

استغلال الطوارئ تعتمد على خلق ضغط نفسي على الضحية مثل تقديم تهديدات او استخدام أسلوب يخلق شعورا بالعجلة مثل ان حسابك معرض للحظر اذا لم تقم بتغيير كلمة المرور ويتم ذلك بإرسال روابط مزيفة لصفحات تشبه الصفحات الرسمية. يشعر الضحية ان عليه اتخاذ اجراء سريع مما يجعله اكثر عرضة للاستجابة.

3- استغلال الفضول (Curiosity Exploitation)

تستخدم هذه التقنية الفضول البشري. عن طريق ارسال رسالة بريد الكتروني الى الضحية يتم تقديم روابط صفحات مثير للاهتمام وتشبه صفحات رسمية مثل لقد فزت بجائزة كبرى كما في الشكل (3-11) او روابط تقديم عروض وخصومات او معلومات هامة تتعلق بحسابك. مما يدفع الضحية لفتح تلك الروابط والتفاعل معها.

الشكل (3-11) ارسال روابط تقديم جوائز.

4- التكرار (Repetition Technique)

يقوم المهاجم في هذه التقنية بإعادة ارسال رسائل البريد الالكتروني او الرسائل النصية الى الضحية عدة مرات لزيادة احتمالية الاستجابة.

5- التخفي (Impersonation)

في هذه التقنية يستخدم المهاجم رسالة بريد الإلكتروني او رقم هاتف مموه ليتظاهر للضحية انه شخص موثوق ومن جهة رسمية مثل موظف بنك او شخص يعمل في قسم تكنلوجيا المعلومات لكسب ثقة الضحية حيث يطلب من الضحية تقديم معلومات حساسة.

6- استخدام الذكاء الاجتماعي (Social Intelligence)

المهاجم في هذه التقنية يقوم بتتبع ودراسة شخصية الضحية في مواقع التواصل الاجتماعي وجمع معلومات خاصة عن الضحية مثل تاريخ الميلاد والأماكن التي قد زارها والأنشطة والتفاعلات والأصدقاء وعلى ضوء تلك الاهتمامات يقوم بتنفيذ الهجمات.

7- الهجوم عبر القنوات المتعددة (Multi-Chanel Attack)

في هذه التقنية يقوم المهاجم بإرسال عدة رسائل للضحية في وقت واحد عبر قنوات متعددة مثل البريد الالكتروني، مكالمات هاتفية، عبر وسائل التواصل الاجتماعي. لإعطاء الانطباع بان المهاجم هو شخص موثوق به.

4-3 أمثلة على هجمات الهندسة الاجتماعية

1. الهجوم على موظف البنك عبر البريد الإلكتروني (Phishing Attack)

- تلقت موظفة في أحد البنوك رسالة بريد إلكتروني تبدو من البنك نفسه، تطلب منها تحديث بيانات حسابها عبر رابط مزيف. في الواقع، كان الرابط يقود إلى موقع مزيف سرق بيانات بطاقة الائتمان الخاصة بها.

2. الهجوم عبر الهاتف (Vishing)

- اتصل شخص يُدعي أنه من خدمة العملاء في البنك بالضحية وأخبره بوجود مشكلة في حسابه، وطلب منه تأكيد بياناته الشخصية. الضحية قدمت البيانات المطلوبة، مما أدى إلى سرقة الأموال من حسابه.

3. هجوم التمويه (Pretexting)

- أرسل مهاجم خطابًا مزيفاً يدعي فيه أنه من إدارة الموارد البشرية في إحدى الشركات ويطلب من الموظفين تقديم تحديثات على بياناتهم الشخصية. بفضل خداعه، تمكّن المهاجم من جمع معلومات حساسة حول موظفي الشركة.

4. **التصيد عبر وسائل التواصل الاجتماعي (Social Media Phishing)**

❖ أنشأ مهاجم حسابًا مزيفًا على إنستغرام يشبه حساب شركة كبيرة، وطلب من المتابعين تقديم بيانات شخصية لإرسال هدايا مجانية. الضحايا الذين صدقوا القصة، كشفوا عن معلومات حساسة.

5. **الهجوم عبر الأجهزة المحمولة(USB Dropping)**

❖ قام المهاجم بزرع عدة أجهزة USB ملوثة في أماكن مكتظة مثل المكتبات أو المكاتب، وقام أحد الموظفين بالعثور عليها وتوصيلها بجهاز الكمبيوتر، مما أدى إلى تحميل فيروس على النظام.

6. الهجوم بالترغيب عبر موقع تنزيل برامج:

❖ استخدم المهاجمون موقعًا مزيفًا يقدم برنامجًا مجانيًا لتحميل ملفات موسيقية، وعندما قام الضحية بتنزيله، تم تثبيت برامج تجسس على جهازه.

كيف تحمي نفسك من هجمات الهندسة الاجتماعية:

- **التوعية والتدريب :**قم بتعليم الموظفين أو الأفراد كيفية التعرف على أساليب الهندسة الاجتماعية الشائعة وكيفية التعامل مع الحالات المشبوهة.
- **التحقق من الهوية :**لا تقدم أية معلومات حساسة عبر الهاتف أو الإنترنت ما لم تكن متأكدًا تمامًا من هوية الشخص الذي يطلب منك ذلك.
- **استخدام الحماية التقنية :**تأكد من استخدام برامج مكافحة الفيروسات وأدوات الكشف عن الهجمات التي قد تساعد في الحماية ضد البرمجيات الضارة.
- **تحديث الأنظمة :**حافظ على تحديث كافة الأنظمة والبرامج لضمان حماية جهازك من الثغرات الأمنية.

الهندسة الاجتماعية هي تهديد يتطلب الحذر واليقظة المستمرة، وتعلم كيفية الوقاية منها هو السبيل للبقاء آمنًا في بيئة رقمية متزايدة التعقيد.

تُعدّ هجمات الهندسة الاجتماعية من أبرز التهديدات الأمنية التي تستهدف الأفراد والمؤسسات على حد سواء. تعتمد هذه الهجمات على استغلال الثغرات البشرية بدلاً من الثغرات التقنية، مما يجعلها أكثر تعقيدًا في الكشف والوقاية.

5-3 الآثار والمخاطر الناتجة عن هجمات الهندسة الاجتماعية

1. **الخسائر المالية :**قد تؤدي هجمات الهندسة الاجتماعية إلى سرقة أموال من الحسابات المصرفية أو إجراء معاملات مالية غير مصرح بها، مما يسبب خسائر مالية كبيرة .

2. **انتهاك الخصوصية :**قد يتسبب المهاجمون في تسريب معلومات شخصية وحساسة، مما يعرض الأفراد لانتهاكات للخصوصية ويزيد من خطر التعرض للاحتيال أو الابتزاز.
3. **تضرر السمعة :**قد تؤدي هذه الهجمات إلى تضرر سمعة الأفراد أو المؤسسات، خاصة إذا تم استغلال المعلومات المسروقة في أنشطة غير قانونية أو ضارة.
4. **تسريب البيانات الحساسة :**قد يؤدي تسريب البيانات الحساسة إلى تآكل الثقة بين أصحاب المصلحة، مما يؤثر سلبًا على العلاقات التجارية والشخصية .
5. **الضرر النفسي :**قد يتسبب التعرض لهذه الهجمات في تأثيرات نفسية سلبية على الأفراد، مثل القلق والتوتر، نتيجة لفقدان الثقة في الأمان الرقمي.

6-3 كيفية الحماية من هجمات الهندسة الاجتماعية

1. **التوعية والتدريب :**يجب تنظيم دورات تدريبية دورية للموظفين والأفراد لتوعيتهم بمخاطر الهندسة الاجتماعية وأساليبها، وتعريفهم بكيفية التعرف على محاولات الاحتيال .
2. **التحقق من الهوية :**يجب التحقق من هوية الأشخاص الذين يطلبون معلومات حساسة، سواء عبر الهاتف أو البريد الإلكتروني، وعدم تقديم أي معلومات شخصية أو مالية إلا بعد التأكد من مصداقية الطلب.
3. **استخدام برامج مكافحة الفيروسات وجدران الحماية :**تساعد برامج مكافحة الفيروسات وجدران الحماية في الوقاية من الفيروسات والبرمجيات الخبيثة المرافقة لهجوم الهندسة الاجتماعية .
4. **تحديث الأنظمة والبرامج :**يجب تحديث الأنظمة والبرامج بانتظام لسد الثغرات الأمنية التي قد يستغلها المهاجمون.
5. **تجنب نشر المعلومات الشخصية :**يجب الحد من نشر المعلومات الشخصية على وسائل التواصل الاجتماعي ومراجعة إعدادات الخصوصية بانتظام لتقليل وصول الغرباء إلى بياناتك .

7-3 تقنيات الكشف عن محاولات الهندسة الاجتماعية

1. **مراقبة الأنشطة المشبوهة :**يجب مراقبة الأنشطة غير المعتادة على الشبكة أو في النظام، مثل محاولات الدخول المتكررة أو الوصول إلى معلومات حساسة دون تصريح.
2. **استخدام أدوات الكشف عن التصيد الاحتيالي :**تتوفر أدوات وبرامج متخصصة للكشف عن رسائل البريد الإلكتروني أو المواقع المزيفة التي تهدف إلى سرقة المعلومات.
3. **تحليل السلوك :**يمكن استخدام تقنيات تحليل السلوك للكشف عن الأنماط غير الطبيعية في استخدام النظام، مما يساعد في التعرف على محاولات الهندسة الاجتماعية.

8-3 دور الأفراد والمؤسسات في الوقاية من الهندسة الاجتماعية

- **الأفراد:**
  - تعلم كيفية التعرف على رسائل التصيد الاحتيالي وروابط الاحتيال.

- فهم أساليب الهندسة الاجتماعية الشائعة مثل انتحال الهوية.
- تجنب تقديم معلومات شخصية أو مالية عبر الهاتف أو البريد الإلكتروني إلا بعد التحقق من هوية الشخص.

- **المؤسسات:**
  - تنظيم دورات تدريبية دورية للموظفين لتوعيتهم بمخاطر الهندسة الاجتماعية.
  - محاكاة هجمات الهندسة الاجتماعية كجزء من تدريبات الأمان.
  - تطبيق سياسات صارمة للتحقق من الهوية قبل تقديم أي معلومات حساسة.

9-3 التكنولوجيا ومكافحة الهندسة الاجتماعية

تساهم التكنولوجيا في مكافحة الهندسة الاجتماعية من خلال تطوير أدوات وبرامج متخصصة للكشف عن محاولات الاحتيال مثل:

1- التدريب والتوعية

- **التعليم المستمر** :تستخدم التكنولوجيا لتوفير برامج تدريبية عبر الإنترنت لتحسين الوعي حول الهجمات الهندسية الاجتماعية. يمكن أن تتضمن هذه الدورات التوعوية محاكاة لهجمات الهندسة الاجتماعية مثل التصيد الاحتيالي (Phishing) لتدريب الأفراد على كيفية التعرف على هذه الأنماط.
- **اختبارات المحاكاة** :يمكن أن تقوم المؤسسات باستخدام أدوات محاكاة لتقديم تجارب حية للهجمات على الموظفين وتحليل استجاباتهم، مما يساعد في تحسين مهاراتهم في التعامل مع المواقف الحقيقية.

2- التحقق متعدد العوامل (Multi-Factor Authentication)

- **تعزيز الأمان** :من خلال استخدام نظام التحقق متعدد العوامل **(MFA)** ، يمكن تعزيز أمان الحسابات الرقمية. حيث يتطلب هذا النظام من المستخدم تقديم أكثر من عامل واحد لتوثيق هويته، مثل كلمة مرور بالإضافة إلى رمز يتم إرساله عبر الهاتف المحمول أو البريد الإلكتروني.
- **الحد من التأثير** :حتى لو تم خداع المستخدم وإعطائه بياناته الشخصية (مثل كلمة المرور)، فإن وجود التحقق المتعدد يقلل من احتمالية تمكن المهاجمين من الوصول إلى الأنظمة.

3- الذكاء الاصطناعي وتحليل البيانات

- **كشف الأنماط المشبوهة** : تستخدم أدوات الذكاء الاصطناعي والتعلم الآلي لتحليل أنماط السلوك عبر الإنترنت واكتشاف التصرفات غير الطبيعية أو المريبة. على سبيل المثال، يمكن للذكاء

الاصطناعي تحديد رسائل البريد الإلكتروني التي تحوي على روابط مشبوهة أو التي تشير إلى هجمات تصيد احتيالي.

- **التحليل السلوكي :**يمكن للأدوات المتقدمة أن تحلل سلوك المستخدمين على الأنظمة والشبكات وتكتشف أي محاولات غير مألوفة للوصول إلى البيانات الحساسة.

4- الحماية من التصيد الاحتيالي (Phishing Protection)

- **أدوات تصفية البريد الإلكتروني** :تعتمد الأنظمة الحديثة على تقنيات متقدمة لاكتشاف الرسائل الاحتيالية **(Phishing emails)** وحظرها قبل وصولها إلى صندوق الوارد. تستخدم هذه الأدوات خوارزميات التعرف على النمط والتعلم الآلي لتحليل الرسائل الإلكترونية واكتشاف تلك التي تحوي على روابط أو مرفقات مشبوهة.
- **علامات التصيد :**بعض الأدوات تستخدم العلامات البصرية أو التحذيرات ضمن البريد الإلكتروني لتوجيه المستخدمين إلى احتمالية أن البريد الإلكتروني قد يكون هجومًا.

5- تقنيات تشفير البيانات

- **حماية البيانات الحساسة** :عبر تقنيات التشفير، يمكن تأمين البيانات أثناء انتقالها عبر الشبكات. فحتى إذا تمكن المهاجم من الوصول إلى البيانات، سيكون من الصعب عليه فك تشفيرها واستخدامها.
- **التشفير الشامل** :يستخدم هذا النوع من التشفير لضمان أمان جميع البيانات المخزنة في الأنظمة أو أثناء التنقل، بما في ذلك كلمات المرور والمعلومات الشخصية.

6- إدارة الهوية والوصول (Identity and Access Management)

- **تحديد صلاحيات الوصول** :تستخدم تقنيات إدارة الهوية لضمان أن الأشخاص الذين يمتلكون الوصول إلى الأنظمة يتم التحقق من هويتهم بشكل صحيح ويُمنح لهم فقط الصلاحيات اللازمة. هذه الأنظمة تعتمد على المصادقة متعددة العوامل وتتبع الأنشطة المشبوهة.
- **الحد من حقوق الوصول :**تعتمد سياسات "أقل حقوق وصول" التي تمنح الأفراد فقط الصلاحيات الضرورية لأداء مهامهم.

7- أنظمة الكشف المبكر والاستجابة (Endpoint Detection and Response)

- **رصد النشاطات غير الطبيعية** :تقدم أنظمة الكشف المبكر والاستجابة **(EDR)** أدوات لرصد الهجمات أو الأنشطة المشبوهة في الوقت الفعلي عبر الشبكات والأجهزة. هذه الأنظمة يمكن أن تكتشف محاولات الهجوم باستخدام تقنيات مثل الهندسة الاجتماعية وتتخذ إجراءات فورية لحماية الأنظمة.

- **الاستجابة التلقائية** :في حال تم الكشف عن هجوم، يمكن للنظام التفاعل بشكل تلقائي، مثل فصل الجهاز المهاجم عن الشبكة أو حظر الوصول إلى النظام.

8- الحماية من الهجمات عبر وسائل التواصل الاجتماعي

- **الرصد والتحليل** :العديد من المؤسسات تستخدم أدوات لحماية معلوماتها على وسائل التواصل الاجتماعي، حيث تُستخدم الذكاء الاصطناعي لتحليل المحادثات وتحديد الأنشطة المشبوهة أو محاولات الاحتيال.
- **التحقق من الهوية :**يمكن للأنظمة التكنولوجية أيضًا استخدام تقنيات للتحقق من هوية المستخدمين عبر الإنترنت لمنع انتحال الشخصيات أو إنشاء حسابات مزيفة تستخدم في الهجمات الهندسية.

9- استخدام أدوات إدارة كلمات المرور

- **التخزين الأمن لكلمات المرور** :استخدام أدوات إدارة كلمات المرور يتيح للمستخدمين تخزين كلمات المرور بأمان وتوليد كلمات مرور قوية. هذه الأدوات تساعد في ضمان عدم إعادة استخدام كلمات المرور عبر حسابات مختلفة، مما يقلل من احتمالية الاستهداف عبر أساليب مثل الهجوم بالقاموس أو التجربة والخطأ.

من خلال تبني هذه الاستراتيجيات والتقنيات، يمكن للأفراد والمؤسسات تقليل مخاطر هجمات الهندسة الاجتماعية والحفاظ على أمان المعلومات.

أسئلة الفصل الثالث

السؤال الأول: ماهي الهندسة الاجتماعية وماهي تصنيفاتها؟

السؤال الثاني: عدد أنواع هجمات الهندسة الاجتماعية واشرح واحدة منها؟

السؤال الثالث: ما هو الفرق بين الاحتيال بالتصيد واحتيال انتحال الشخصية؟

السؤال الرابع: ماهي أساليب وتقنيات الهندسة الاجتماعية؟

السؤال الخامس: اذكر مخاطر واضرار هجمات الهندسة الاجتماعية؟

السؤال السادس: ما هو دور الافراد والمؤسسات في الوقاية من هجمات الهندسة الاجتماعية؟

السؤال السابع: ماهي التكنلوجيا المستخدمة في مكافحة الهندسة الاجتماعية؟

الفصل الرابع

الهجمات السيبرانية (Cyber Attacks)

الأهداف

من المتوقع أن يكون الطالب قادراً على أن :

1. يتعرف الى أنواع الهجمات السيبرانية المختلفة وأهدافها.
2. يفهم تقنيات التلاعب في البيانات وأشكال البرمجيات الخبيثة.
3. يقوم بتحديد نوع الهجوم السيبراني بناء على الأنماط والأعراض.
4. يتخذ خطوات وقائية لحماية أجهزته من البرمجيات الضارة.

الهجمات السيبرانية (Cyber Attacks)

1-4 تمهيد

مع تزايد الاعتماد على التكنولوجيا الرقمية في مختلف مجالات الحياة، أصبحت الهجمات السيبرانية تشكل تهديداً خطيراً على الأفراد والمؤسسات والدول. تتنوع هذه الهجمات من حيث الأساليب والأهداف، حيث يتم استخدامها لأغراض متعددة مثل سرقة المعلومات، التجسس، التخريب، أو حتى الحرب السيبرانية. تعتمد الهجمات السيبرانية على استغلال نقاط الضعف في الأنظمة الإلكترونية والشبكات، وتشمل مجموعة متنوعة من الأنماط مثل البرمجيات الخبيثة، هجمات التصيد الاحتيالي، وهجمات منع الوصول الى الخدمة.

في هذا الفصل، سنستعرض الأنماط والأساليب المختلفة للهجمات السيبرانية، بما في ذلك كيفية تنفيذها والتعرف عليها. سنناقش تصنيف الأنماط الهجومية المستخدمة في الهجمات السيبرانية، مع تقديم أمثلة على كل منها. بالإضافة إلى ذلك، سنستعرض الفرق بين الهجمات الإلكترونية والهجمات السيبرانية المتقدمة، ونتناول مخاطر هذه الهجمات وكيفية الوقاية منها. سنختتم الفصل بمناقشة استراتيجيات مكافحة الهجمات السيبرانية وطرق الحماية منها في الحروب الإلكترونية.

سيكتسب الطلاب في نهاية هذا الفصل فهمًا شاملاً لمفهوم الهجمات السيبرانية، وأسس الدفاع ضدها، وأفضل الممارسات لحماية الأنظمة والبيانات في العالم الرقمي المعقد. القراءة المتأنية لهذه المواضيع ستساعد في بناء حصانة معرفية قوية تمكن الطلاب من التصدي للهجمات السيبرانية بفعالية وكفاءة.

2-4 مفهوم الهجمات السيبرانية

الهجمات السيبرانية هي أي محاولة متعمدة لاختراق أو تعطيل أنظمة الحاسوب والشبكات عن بعد بهدف تحقيق أهداف غير مشروعة. يمكن لهذه الأهداف أن تشمل سرقة المعلومات، التخريب، أو حتى شن هجمات على دول أخرى في إطار الحرب السيبرانية. تعتمد هذه الهجمات على تقنيات متطورة تتطور باستمرار، مما يجعل من الضروري التعرف على آليات الدفاع والحماية منها.

3-4 أساليب وأنواع الهجمات السيبرانية

1-3-4 الأساليب المستخدمة في الهجمات السيبرانية

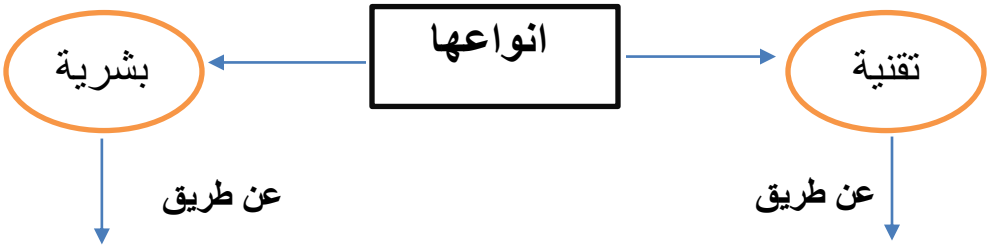
الهجمات السيبرانية تعتمد على عدة أساليب وتقنيات للوصول إلى الأنظمة المستهدفة أو تعطيلها، ومن أبرز هذه الأساليب:

1. الهندسة الاجتماعية (Social Engineering) :

هي فن التلاعب بالبشر وخداعهم بهدف الحصول على البيانات لكشف معلوماتهم او حساباتهم السرية دون علمهم وذلك باستهداف نقاط الضعف البشرية .

اهدافها :

1. **التظليل.**
2. **اصابة جهاز الضحية .**
3. **الحصول على كلمات السر .**
4. **الاحتيال بهدف الحصول على المال .**
5. **دفع المستخدم لزيارة مواقع خبيثة .**



- الاتصال المباشر
- رسائل نصية
- رسائل شبكات التواصل الاجتماعي : (روابط WhatsApp – صداقات Facebook – الخ)

- برامج مهمة
- الاتصال الصوتي
- الرسائل الاقتحامية المزعجة (Spam)

الاساليب المتبعة في الهندسة الاجتماعية :

1. **الاقناع عن طريق استغلال عواطف الضحية .**
2. **استغلال الشائعات (الرسائل الكاذبة).**
3. **المكالمات من مجهولين لتسجيل المكالمات .**
4. **استغلال ضعف الخبرة التقنية للضحية (فتح الملفات غير الأمنة).**
5. **انتحال الشخصية .**
6. **اصطياد كلمات السر .**
7. **البحث في المهملات.**

طرق الوقاية من هجمات الهندسة الاجتماعية :

1. **عدم مشاركة المعلومات الشخصية .**
2. **عدم فتح رسائل البريد من المجهولين .**
3. **تفعيل التحقق بخطوتين في برامج التوصل الاجتماعي .**
4. **التحقق من هوية الذين نتعامل معهم .**
5. **تأمين الاجهزة واستخدام برامج الحماية .**

2. التصيد الاحتيالي (Phishing) :

- **هجوم يُستخدم لخداع المستخدمين عبر البريد الإلكتروني أو الرسائل النصية لإدخال بيانات حساسة.**
- **يتم تصميم مواقع مزيفة تبدو كأنها مواقع حقيقية لجمع بيانات تسجيل الدخول.**
- **الانتحال (Pretexting) : انشاء سيناريوهات وهمية لخداع الضحايا.**
- **استغلال الثقة (Baiting) : استخدام وعود كاذبة لجذب الضحايا.**
- **يمكن أن يكون التصيد موجهاً (Spear Phishing) لاستهداف أفراد معينين أو واسع النطاق (Mass Phishing).**

3. استغلال الثغرات الأمنية (Exploitation of Vulnerabilities) :

- **يحدث عند استغلال نقاط الضعف في البرمجيات أو الأنظمة للوصول غير المصرح به.**
- **يمكن أن تشمل الثغرات في أنظمة التشغيل، التطبيقات، أو الشبكات.**
- **تُستخدم أدوات مثل "Metasploit" لاختبار الثغرات واستغلالها.**

4. الذكاء الاصطناعي (AI)

مع تطور الذكاء الاصطناعي، أصبح يُستخدم في العديد من المجالات الإيجابية مثل الطب والتعليم والنقل، لكنه للأسف يُستخدم أيضًا من قبل المهاجمين السيبرانيين لتطوير هجماتهم وجعلها أكثر دقة وفعالية. في هذا الفصل، سنتعرف على أبرز الطرق التي يُستغل بها الذكاء الاصطناعي لتنفيذ الهجمات السيبرانية:

أولاً: تحليل السلوك والتعلم الآلي لتنفيذ الهجمات

يعتمد المهاجمون على خوارزميات التعلم الآلي (Machine Learning) لتحليل سلوك المستخدمين واكتشاف نقاط الضعف.

كيف يعمل؟

يتم تدريب أنظمة الذكاء الاصطناعي على تحليل البيانات الضخمة الخاصة بالمستخدمين (مثل أوقات الاستخدام، المواقع التي يزورونها، طريقة الكتابة)، ثم استخدامها لتحديد اللحظة المناسبة للهجوم.

ثانياً: التزييف العميق (Deep fake)

الذكاء الاصطناعي يستطيع إنشاء مقاطع فيديو أو تسجيلات صوتية مزيفة لأشخاص حقيقيين.

كيف يستخدم في الهجوم؟

يقوم المهاجم بتوليد مقطع صوتي مزيف بصوت مدير شركة يطلب فيه تحويل مبلغ مالي إلى حساب معين. يصعب تمييز المحتوى الحقيقي عن المزيف، مما يزيد من فرصة نجاح الهجوم.

ثالثاً: روبوتات المحادثة الذكية (AI Chatbots) في الهندسة الاجتماعية

يُستخدم الذكاء الاصطناعي لتصميم روبوتات محادثة تحاكي البشر بطريقة ذكية جدًا.

كيف يستخدم؟

يرسل المهاجم رابطًا لموقع مزيف يديره روبوت دردشة يحاول إقناع الضحية بإدخال معلوماته السرية (كلمات مرور، بيانات بنكية).

رابعاً: التهديدات التلقائية والهجمات واسعة النطاق

الذكاء الاصطناعي يمكنه تنفيذ هجمات سيبرانية تلقائية ضد آلاف الأهداف في وقت قصير.ويتم برمجة الخوارزميات للبحث عن ثغرات أمنية عبر الإنترنت بشكل آلي، وتنفيذ الهجوم مباشرة عند العثور عليها ومثال على ذلك :

استخدام AI لمسح الإنترنت بحثًا عن أجهزة غير محمية، ثم اختراقها تلقائيًا.

خامساً: تجاوز أنظمة الحماية الذكية

كيف يستخدم الذكاء الاصطناعي؟

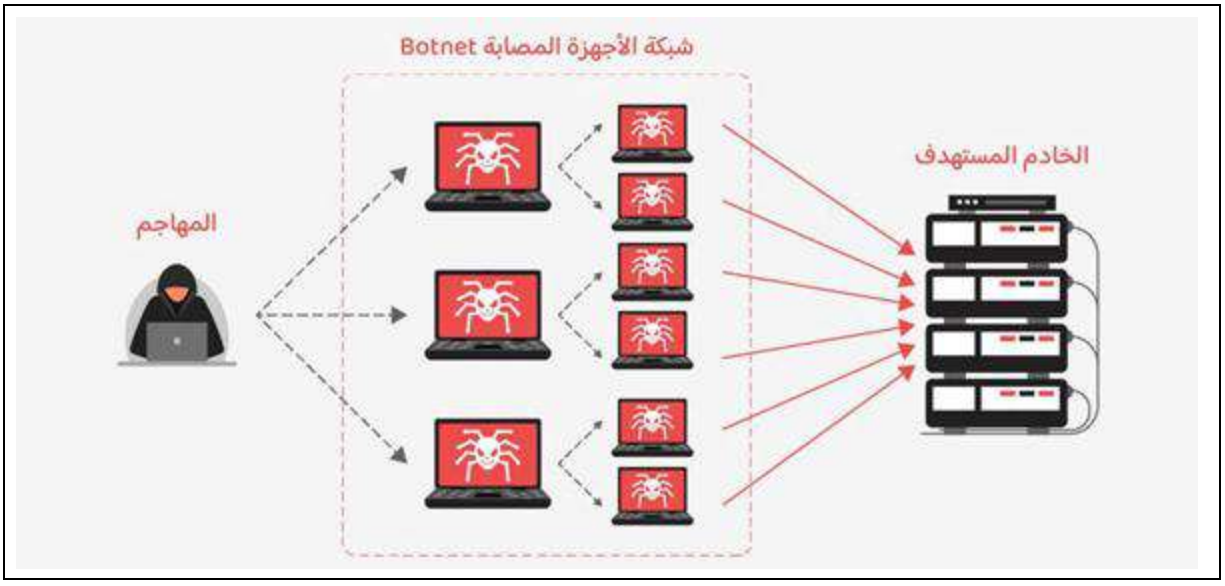
يتم تدريب AI على تحليل أنظمة الحماية والتعرف على طريقة عملها، ثم تصميم هجمات تتجاوزها دون اكتشاف.

5. البرمجيات الضارة (Malware) :

- تشمل أنواعًا مختلفة مثل الفيروسات، الديدان، وأحصنة طروادة.
- يمكن أن تعمل على سرقة البيانات، تعطيل الأنظمة، أو التجسس على الضحايا.
- تنتشر عبر مرافقات البريد الإلكتروني، التنزيلات من الإنترنت، أو الثغرات الأمنية.

6. هجمات حجب الخدمة (DDoS Attacks) :

- تهدف إلى إغراق الخوادم بالطلبات لجعلها غير قادرة على العمل.
- تُنفذ باستخدام شبكات "بوت نت" التي تضم أجهزة مخترقة.
- تُستخدم أحيانًا كوسيلة للابتزاز أو لإضعاف المنافسين.



الشكل (4-1) هجمات حجب الخدمة

2-3-4 أنواع الهجمات السيبرانية

الهجمات السيبرانية تصنف إلى أنواع متعددة بناءً على أهدافها وأساليب تنفيذها:

1. **الهجمات الموجهة (Targeted Attacks) :**
   - يتم التخطيط لها مسبقًا ضد أهداف محددة مثل الشركات أو الحكومات.
   - تتطلب دراسة معمقة للضحية قبل تنفيذ الهجوم.
   - من أمثلتها الهجمات المستمرة المتقدمة (APT) .

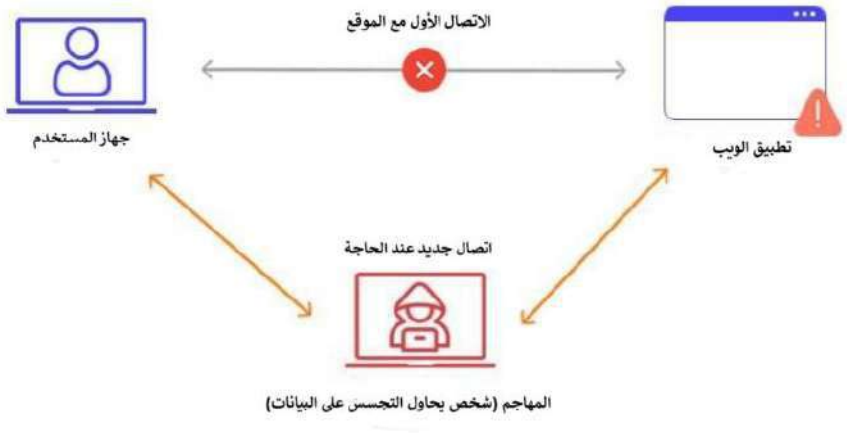
2. **الهجمات غير الموجهة (Untargeted Attacks) :**
   - تُنفذ بشكل عشوائي ضد عدد كبير من الضحايا دون استهداف محدد.
   - تشمل التصيد الاحتيالي الجماعي وهجمات البرمجيات الضارة المنتشرة عبر الإنترنت.

3. **هجمات حجب الخدمة الموزعة (Distributed Denial of Service) (DDoS) و (Denial of Service) (DOS) :**
   - تهدف إلى تعطيل الخدمات الإلكترونية من خلال إرسال كميات هائلة من الطلبات.
   - تُستخدم لإسقاط مواقع إلكترونية أو تعطيل شبكات الاتصالات.

4. **هجمات البرمجيات الضارة (Malware Attacks) :**
   - تشمل الفيروسات وأحصنة طروادة التي تصيب الأجهزة والأنظمة.
   - فيروسات الفدية (Ransomware) تقوم بتشفير البيانات وتطلب فدية مقابل فك التشفير.

5. **هجمات الاعتراض والتنصت (Man-in-the-Middle Attacks -MITM) :**
   - يتم فيها اعتراض الاتصالات بين طرفين للحصول على معلومات حساسة.يمكن أن تحدث عبر الشبكات غير الأمنة مثل شبكات Wi-Fi العامة.

الشكل (2-4) يوضح هجمات MITM



الشكل (4-2) يوضح هجمات MITM

6. هجمات سلسلة التوريد:

استهداف نقاط هي نوع من الهجمات السيبرانية التي تستهدف نقاط الضعف في سلسلة التوريد الخاصة بالشركات أو المؤسسات، بهدف الوصول إلى الأنظمة أو البيانات الحساسة عن طريق التلاعب بأحد المكونات أو المزودين المرتبطين بها.

أهدافها:

1. **التجسس وسرقة البيانات الحساسة مثل البيانات المالية أو بيانات العملاء.**
2. **نشر البرمجيات الخبيثة داخل شبكات آمنة عن طريق تحديثات مزيفة أو أدوات موثوقة تم التلاعب بها.**
3. **التخريب أو تعطيل الخدمات في مؤسسات حساسة (مثل الطاقة، الصحة، الاتصالات).**

طرق تنفيذ الهجوم:

1. **حقن برمجيات خبيثة في تحديثات البرمجيات أو الأدوات المعتمدة من قبل الشركات.**
2. **استغلال ضعف الأمان لدى أحد الموردين للحصول على صلاحية دخول إلى الشبكة الرئيسة.**
3. **استهداف أنظمة سلسلة التوزيع (مثل أنظمة النقل أو اللوجستيات) لتعطيل العمليات أو جمع معلومات.**

7. هجمات إنترنت الأشياء Internet of Things (IoT):

إنترنت الأشياء (IoT) : هي شبكة من الأجهزة الذكية المتصلة بالإنترنت والتي تتبادل البيانات فيما بينها أو مع المستخدم، مثل:(الأجهزة المنزلية الذكية، أنظمة المراقبة والأمن، الأجهزة الطبية، السيارات الذكية، أنظمة المدن الذكية).

هجمات إنترنت الأشياء

هي محاولات لاختراق أو استغلال أجهزة إنترنت الأشياء لتنفيذ أنشطة خبيثة مثل سرقة البيانات، التجسس، التحكم بالجهاز عن بعد، أو استخدامه في هجمات أوسع (مثل هجمات الحرمان من الخدمة - DDoS).

أهداف الهجوم:

1. **التجسس على المستخدمين (صوت/صورة/موقع).**
2. **اختراق الشبكة المنزلية أو المؤسسية من خلال جهاز ضعيف.**
3. **استخدام الجهاز كجزء من شبكة بوت نت (Botnet) لتنفيذ هجمات ضخمة.**
4. **سرقة بيانات المستخدمين أو التحكم في الأجهزة عن بعد.**

طرق تنفيذ الهجوم:

1. **استغلال كلمات مرور ضعيفة أو افتراضية.**
2. **ثغرات في البرمجيات بسبب عدم تحديث الجهاز.**
3. **الهجوم عبر الشبكة اللاسلكية Wi-Fi غير المؤمنة.**
4. **التصيد الإلكتروني لاستدراج المستخدم إلى تحميل برمجية خبيثة على الجهاز.**

4-4 تصنيف الانماط الهجومية المستخدمة في الهجمات السيبرانية :

1. البرمجيات الخبيثة (Malware): هي برامج أو ملفات يتم إنشاؤها بغرض إلحاق الضرر بالأنظمة أو الأجهزة أو سرقة المعلومات أو التحكم في الحاسوب دون علم المستخدم. وأنواع البرمجيات الخبيثة هي :

- **الفيروسات: برامج ضارة تنتشر عن طريق إلحاق نفسها ببرامج أو ملفات أخرى. عندما يتم تنفيذ البرنامج أو الملف المصاب، يتم تفعيل الفيروس وينتشر إلى برامج أو ملفات أخرى.**
- **الديدان: برمجيات تنتشر عبر الشبكات دون الحاجة إلى التفاعل البشري. يمكن للديدان استخدام نقاط ضعف الشبكة للانتشار.**
- **أحصنة طروادة: برامج تبدو مشروعة لكنها تحمل برمجيات ضارة. يمكن أن تتيح للمهاجمين الوصول إلى النظام المصاب والتحكم فيه.**
- **برامج الفدية: برمجيات تحتجز بيانات المستخدم رهينة وتطلب فدية لإعادة الوصول إليها. يمكنها تشفير الملفات أو منع الوصول إلى النظام بالكامل.**
- **برامج التجسس: برامج تراقب نشاط المستخدم وتنقل المعلومات إلى المهاجم. يمكنها سرقة كلمات المرور، والتفاصيل المالية، والمزيد.**

2.هجمات حجب الخدمة (DoS و DDoS):

هجمات رفض الخدمة تهدف إلى جعل النظام أو الشبكة غير قادرين على تلبية الطلبات المشروعة من خلال إغراقهما بكمية كبيرة من الطلبات وأنواع هجمات رفض الخدمة هي :

- **DoS (Denial of Service): هجوم يتم شنه من جهاز واحد أو شبكة واحدة لإغراق النظام بالطلبات.**
- **DDoS (Distributed Denial of Service) : هجوم موزع يتم شنه من عدة أجهزة في مواقع مختلفة لإغراق النظام بالطلبات. عادة ما تكون هذه الأجهزة مصابة ببرامج ضارة تجعلها جزءًا من شبكة بوتنت.**

3. التصيد الاحتيالي (Phishing):

هو عملية خداع المستخدمين للكشف عن معلوماتهم الشخصية أو المالية عن طريق البريد الإلكتروني أو المواقع الزائفة وأساليب التصيد الاحتيالي هي :

- **البريد الإلكتروني الاحتيالي: إرسال رسائل بريد إلكتروني تبدو وكأنها من مصدر موثوق (مثل البنوك أو الشبكات الاجتماعية) تطلب من المستخدمين تقديم معلومات حساسة.**

- **المواقع الزائفة: إنشاء مواقع تبدو مشابهة للمواقع الرسمية وتطلب من المستخدمين إدخال بياناتهم الشخصية.**

4. هجوم الرجل في المنتصف (MITM):

هو هجوم يعترض فيه المهاجم الاتصال بين طرفين دون معرفتهما، مما يسمح له بقراءة البيانات وتعديلها وسرقتها و أساليب هجوم الرجل في المنتصف هي :

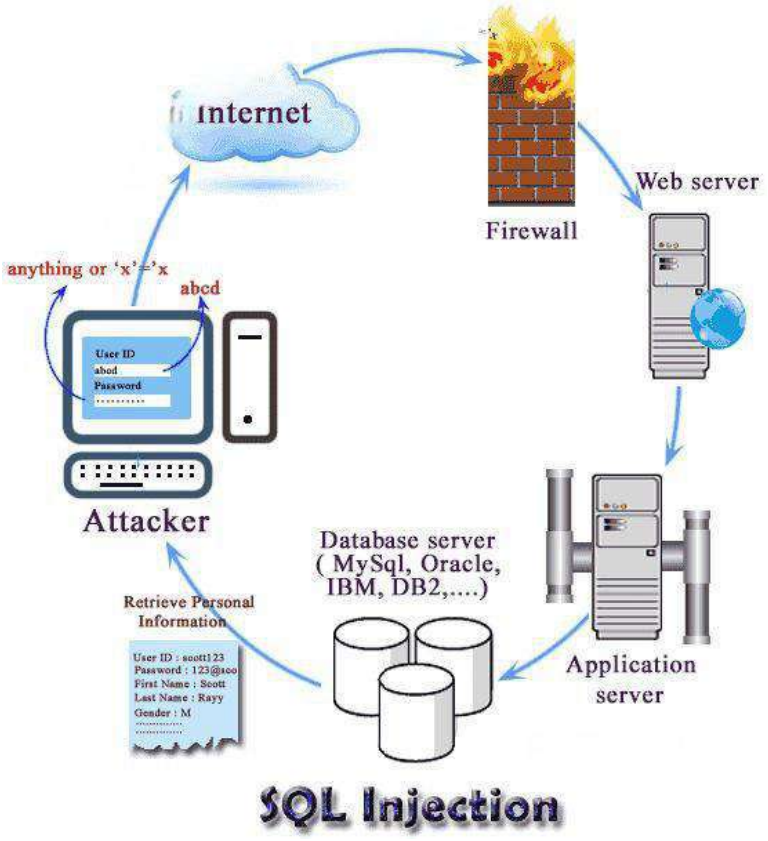
- **اعتراض الاتصالات غير المشفرة: حيث يقوم المهاجم باعتراض الرسائل بين الطرفين.**
- **تزوير الشهادات الأمنية: حيث ينشئ المهاجم شهادة أمان مزيفة لخداع المستخدمين للاعتقاد بأنهم يتواصلون مع موقع آمن.**

5.هجمات الحقن (Injection Attacks) :

تتضمن إدخال تعليمات برمجية ضارة في تطبيقات الويب بهدف الحصول على بيانات غير مصرح بها أو تنفيذ أوامر غير مشروعة وأنواع هجمات الحقن هي :

- **حقن SQL: إدخال تعليمات SQL ضارة في استعلامات قاعدة البيانات للوصول إلى البيانات الحساسة.**

الشكل (4-3) يوضح هجمات الحقن SQL



- **حقن الأوامر: إدخال أوامر برمجية ضارة في تطبيقات الويب لتنفيذ أوامر على الخادم.**
- **حقن العابر للمواقع (XSS): إدخال تعليمات برمجية ضارة في موقع ويب لسرقة بيانات المستخدمين أو التحكم في المتصفح.**

5-4 الفرق بين الهجمات الالكترونية والهجمات السيبرانية المتقدمة

1-5-4 الهجمات الإلكترونية (Electronic Attacks):

هي محاولات تهدف إلى اختراق الأنظمة أو الأجهزة باستخدام الوسائل الرقمية بهدف الوصول إلى البيانات أو تعطيل الأنظمة. قد تشمل هذه الهجمات مجموعة واسعة من الأساليب مثل البرمجيات الخبيثة (الفيروسات، الديدان)، أو هجمات الهندسة الاجتماعية (التصيد الاحتيالي)، أو هجمات رفض الخدمة (DoS) التي تهدف إلى إغراق الأنظمة بالطلبات.

أمثلة على الهجمات الإلكترونية:

- **الفيروسات :برامج ضارة تنقل نفسها عبر الأنظمة وتسبب أضرارًا.**
- **التصيد الاحتيالي :رسائل بريد إلكتروني مزيفة تهدف إلى سرقة المعلومات الشخصية.**
- **هجمات DDoS : هجمات موجهة لغرض تعطيل خوادم الإنترنت عبر إرسال كمية هائلة من البيانات.**

2-5-4 الهجمات السيبرانية المتقدمة (Advanced Cyber Attacks) :

هي هجمات معقدة وذات تصميم دقيق تستهدف الأنظمة والبيانات الحساسة على نطاق أكبر باستخدام تقنيات متقدمة للغاية. تتسم هذه الهجمات بالاستهداف المباشر لمنظمات أو كيانات محددة، وغالبًا ما تكون مدعومة من قبل جماعات ذات قدرات فنية عالية أو حتى دول. تختلف هذه الهجمات عن الهجمات الإلكترونية العادية في أنها تتطلب موارد وتقنيات متطورة، مثل استخدام البرمجيات الخبيثة المتطورة، أو استغلال الثغرات الأمنية الدقيقة التي قد لا تكون معروفة للعديد من فرق الأمان.

أمثلة على الهجمات السيبرانية المتقدمة:

- **الهجمات المدعومة من الدولة (State-Sponsored Attacks) :هجمات تستخدمها الحكومات لتحقيق أهداف سياسية أو اقتصادية ضد أهداف محددة.**
- **البرمجيات الخبيثة المستهدفة (Targeted Malware) : إنشاء برمجيات خبيثة متقدمة لاستهداف أنظمة محددة مثل برامج التجسس أو الفيروسات المصممة خصيصًا.**
- **هجمات الاختراق المتقدمة (Advanced Persistent Threats - APTs) : هجمات معقدة مستمرة تهدف إلى التسلل إلى الأنظمة والبقاء فيها لفترة طويلة للحصول على معلومات حساسة.**

الفرق بين الهجمات الإلكترونية والهجمات السيبرانية المتقدمة:

1. التعقيد:

- **الهجمات الإلكترونية قد تكون بسيطة أو تعتمد على أساليب معروفة مثل الفيروسات أو التصيد الاحتيالي.**
- **الهجمات السيبرانية المتقدمة تتسم بالتعقيد الكبير، باستخدام تقنيات متطورة وأدوات متخصصة لتحقيق أهداف دقيقة.**

2. الاستهداف:

- **الهجمات الإلكترونية عادة ما تكون عشوائية أو تستهدف مجموعات واسعة من الأفراد أو الأنظمة.**
- **الهجمات السيبرانية المتقدمة تستهدف أهدافًا محددة مثل الشركات الكبرى، الحكومات، أو المؤسسات الأمنية.**

3. الموارد المطلوبة:

- **الهجمات الإلكترونية يمكن تنفيذها باستخدام أدوات متوفرة بسهولة على الإنترنت.**
- **الهجمات السيبرانية المتقدمة غالبًا ما تتطلب دعماً متطوراً ومصادر أكبر، مثل فرق من الهاكرز المتخصصين أو دعم دولي.**

4. الهدف النهائي:

- الهجمات الإلكترونية قد تكون بهدف تدمير أو سرقة البيانات على مستوى منخفض.
- الهجمات السيبرانية المتقدمة غالبًا ما تهدف إلى الوصول إلى بيانات حساسة أو السيطرة على الأنظمة لأغراض سياسية أو اقتصادية.

6-4 مخاطر الهجمات السيبرانية :

- سرقة الهوية والبيانات الشخصية مما قد يؤدي إلى الاحتيال المالي وانتحال الشخصية.
- تعطيل البنية التحتية الحيوية مثل شبكات الكهرباء والمياه والاتصالات.
- خسائر مالية ضخمة بسبب الاحتيال أو الابتزاز بفيروسات الفدية.
- انهيار الشركات بسبب تسرب البيانات التجارية أو فقدان الثقة.
- تعزيز النشاطات الإجرامية والإرهابية من خلال استخدام المعلومات المسروقة.

7-4 طرق الوقاية من الهجمات السيبرانية

- استخدام برامج الحماية الموثوقة مثل مضادات الفيروسات وجدران الحماية.
- تحديث الأنظمة والتطبيقات باستمرار لسد الثغرات الأمنية.
- التوعية الأمنية للمستخدمين حول أساليب الهجوم المختلفة وكيفية تجنبها.
- استخدام كلمات مرور قوية وتفعيل المصادقة الثنائية لمنع الاختراق.
- تشفير البيانات لضمان عدم قراءتها في حال اعتراضها.

8-4 استراتيجيات مكافحة الهجمات السيبرانية الهجومية

- الاستخبارات السيبرانية :(Cyber Intelligence) تتبع وتحليل التهديدات قبل وقوعها.
- الردع السيبراني :(Cyber Deterrence) تطوير تقنيات هجومية لحماية الأنظمة.

- **الهجوم الاستباقي (Preemptive Strike): اتخاذ إجراءات ضد المهاجمين قبل تنفيذ الهجمات.**
- **الشراكات الأمنية بين المؤسسات والحكومات لتبادل المعلومات حول التهديدات.**

9-4 الحماية من الهجمات السيبرانية في الحرب الإلكترونية

- **تطوير أنظمة دفاع إلكتروني تعتمد على الذكاء الاصطناعي للكشف المبكر عن الهجمات.**
- **استخدام تقنيات التشفير المتقدمة لحماية الاتصالات العسكرية والحكومية.**
- **إنشاء وحدات متخصصة في الأمن السيبراني ضمن الجيوش والمنظمات الأمنية.**
- **تعزيز التعاون الدولي لمواجهة التهديدات السيبرانية المشتركة عبر تبادل المعلومات والخبرات.**

اسئلة الفصل الرابع

1. ما الفرق بين الهجمات الإلكترونية والهجمات السيبرانية المتقدمة؟
2. اذكر ثلاثة أنواع من الهجمات السيبرانية ووضح كيفية عمل كل منها.
3. كيف يمكن الوقاية من هجمات التصيد الاحتيالي؟
4. ما أهمية الاستخبارات السيبرانية في مكافحة الهجمات؟
5. قم بتحليل دراسة حالة لهجوم سيبراني شهير واذكر الدروس المستفادة منه.

الفصل الخامس

البصمة الرقمية
(Digital Footprint)

الأهداف

من المتوقع أن يكون الطالب قادراً على أن :

1. يعرف مفهوم البصمة الرقمية واهمية التحكم بها.
2. يميز بين انواع البيانات التي يمكن تتبعها على الانترنت.
3. يتقن اعدادات الخصوصية على وسائل التواصل الاجتماعي
4. يتعلم كيفية ازالة البيانات الحساسة من حساباته على الانترنت.

البصمة الرقمية (Digital Footprint)

تعد البصمة الرقمية من المفاهيم الحديثة التي ظهرت نتيجة للتطورات التكنولوجية السريعة في عصر الإنترنت، حيث أصبحت جزءاً لا يتجزأ من حياتنا الرقمية اليومية. ومع ازدياد تفاعل الأفراد مع مختلف المنصات الرقمية، تتولد كميات ضخمة من البيانات التي تكوّن البصمة الرقمية الخاصة بكل فرد. هذه البيانات يمكن أن تشمل كل شيء بدءاً من الأنشطة اليومية على الإنترنت إلى التفاعلات مع وسائل التواصل الاجتماعي، والبحث عبر محركات البحث، وحتى المشتريات عبر الإنترنت. تتبع هذه الأنشطة يساهم في بناء صورة شاملة عن الشخص، ما يتيح للمؤسسات والشركات تحليل سلوكيات الأفراد واحتياجاتهم.

تتكون البصمة الرقمية من أنواع متعددة من البيانات المتعقبة، مثل المعلومات الشخصية (كالاسم، والعمر، والموقع الجغرافي)، وسلوكيات المستخدم عبر الإنترنت، مثل صفحات الويب التي يزورها، محركات البحث التي يستخدمها، والتفاعلات على وسائل التواصل الاجتماعي. يتم جمع هذه البيانات من قبل الشركات والحكومات من أجل تحسين تجربة المستخدم، وتوجيه الإعلانات، وتعزيز الأمان، وحتى المراقبة.

لكن مع تزايد الاهتمام بالبيانات الشخصية على الإنترنت، تزداد المخاوف المتعلقة بخصوصية وسائل التواصل الاجتماعي وأدوات التتبع التي تُستخدم من قبل هذه المنصات. في هذا السياق، تتطلب إعدادات الخصوصية في المتصفح والأجهزة اهتماماً خاصاً لضمان حماية بيانات الأفراد. يمكن أن توفر هذه الإعدادات تحكماً أكبر في المعلومات التي يتم جمعها من قبل المواقع المختلفة، مما يتيح للمستخدمين تخصيص مستوى الحماية الذي يحتاجونه.

ومع تزايد العمليات التي تقوم بها الشركات والحكومات لمراقبة الأنشطة الرقمية، يبقى السؤال مطروحاً حول كيفية التأكد من استخدام هذه البيانات بشكل آمن وغير متجاوز لحدود الخصوصية. بينما يمكن أن تساعد هذه العمليات في تحسين الخدمات وتوفير تجارب مخصصة، فإنها أيضًا تفتح المجال لتهديدات الإلكترونية خطيرة مثل الاحتيال، وسرقة الهوية، والتهديدات السيبرانية الأخرى.

لحماية هذه البيانات، تصبح ممارسات الأمن السيبراني جزءاً أساسياً في حماية وحذف البصمة الرقمية .تتنوع هذه الممارسات بين أدوات التشفير، وبرامج مكافحة الفيروسات، والتحقق الثنائي، إلى جانب تقنيات أخرى تساعد في الحفاظ على أمان البيانات الشخصية.

وأخيراً، في ظل التطورات المستقبلية، توفر البصمة الرقمية فرصاً جديدة تتجاوز مجرد حماية البيانات إلى استخدام هذه المعلومات في مجالات أخرى مثل تحسين تجربة المستخدم، التسويق الموجه، وتحسين الأمان السيبراني .هذه الفرص قد تكون محورية في إحداث تغييرات إيجابية في عالم الإنترنت، مما يؤدي إلى زيادة الكفاءة وتقديم خدمات أفضل، لكنها تتطلب ضمانات قوية لحماية الخصوصية.

إن فهم البصمة الرقمية وأبعادها المتنوعة يمثل أداة حيوية لمواكبة التحديات والفرص في عصر المعلومات الرقمية.

1-5 مفهوم البصمة الرقمية

البصمة الرقمية هي مجموعة من البيانات والمعلومات التي يتم جمعها في قاعدة بيانات عن الشخص أثناء استخدامه للإنترنت. تتكون هذه البصمة من جميع الأنشطة التي يقوم بها الشخص على الشبكة العنكبوتية، مثل التصفح (أي المواقع الإلكترونية التي يتم زيارتها)، التفاعل مع مواقع التواصل الاجتماعي مثل (Facebook, Instagram) من التعليقات والاعجاب والمشاركات، وتطبيقات المحادثات وحتى تحميل الملفات ومشاركتها. بشكل عام، كلما زادت الأنشطة التي يقوم بها الشخص على الإنترنت، كلما كانت بصمته الرقمية أكبر وأكثر تنوعًا. بكلام اخر البصمة الرقمية تشبه آثار أقدامك على الرمال أو الأسطح الصلبة في العالم الحقيقي، ولكنها ليست بصمة أصابعك. فالمصطلح يشير إلى الأماكن والأنشطة التي تمر بها على الإنترنت خلال زياراتك لمواقع مختلفة. مثل بصمة الإصبع، تكون البصمة الرقمية فريدة ولا يمكن أن تتشابه مع أي شخص آخر على الإنترنت، وهي غالبًا صعبة التغيير أو الإزالة. ببساطة، يمكن تعريف البصمة الرقمية على أنها سلوك الفرد على الإنترنت، الذي يتم تتبعه أثناء قيامه بالأنشطة المختلفة مثل زيارة المواقع، نشر المحتوى، أو إرسال واستقبال الرسائل الإلكترونية. وبالتالي، هي تعبير عن "أثر" الشخص الذي يظل موجودًا على الإنترنت حتى بعد مرور وقت طويل، وقد يصعب إزالته تمامًا.

نظرًا لأن البصمة الرقمية تظل مرئية أو قابلة للتتبع، فإنها قد تحد من خصوصيتك الشخصية، وقد تكون عرضة للاطلاع من قبل الآخرين. في بعض الحالات، حتى وإن كانت المعلومات الخاصة محمية، يمكن أن تظل هناك بعض الآثار التي يمكن تتبعها، مما يقلل من قدرتك على التحكم الكامل في خصوصيتك في الشكل (5-1) يوضح الأثر الذي يتركه شخص ما عند مروره على رمل او على غيرها من الاسطح التي تترك اثر والتي يمكن ان يتم تتبعه. كذلك في العالم الرقمي أي نشاط من تصفح او تفاعلات على التواصل الاجتماعي او مراسلات يتم حفظها في قاعدة بيانات خاصة لكل شخص ويتم تتبع نشاطه وتوجهاته وعلى ضوئه يتم ارسال الإعلانات الترويجية او معرفة الحالة الاجتماعية لمجتمع.

2-5 أنواع البيانات المتعقبة

أنواع البيانات التي يتم تتبعها وجمعها من قبل المواقع والتطبيقات للأشخاص على الإنترنت متنوعة ويمكن تصنيفها إلى عدة فئات حسب نوع البيانات والغرض من جمعها. فيما يلي أبرز أنواع البيانات التي يتم تتبعها، استنادًا إلى مصادر أكاديمية ومتخصصة:

1- البيانات السلوكية (Behavioral Data)

هي البيانات التي يتم جمعها عن المستخدم في الإنترنت من خلال سلوكه. مثل الصفحات التي يتم زيارتها، الوقت الذي يقضيه في كل صفحة، وحركاته داخل الموقع.

2- بيانات الموقع الجغرافي (Geolocation Data)

هي بيانات الموقع الجغرافي الفعلي للمستخدم عند تصفحه للإنترنت. يعتمد جمع هذه البيانات على معلومات الـ IP (Internet Protocol) وهو عنوان موقع المستخدم في الانترنت

حيث يتم التعرف على موقع الشخص من خلاله. ويشبه عنوان موقع السكن للشخص أو تقنية GPSفي الأجهزة المحمولة.

3- البيانات الشخصية (Personal Data)

وهي المعلومات الشخصية التي يقدمها المستخدم عند التسجيل الدخول في المواقع مثل اسم المستخدم, العمر, الجنس, تاريخ الميلاد, مكان العمل, كلمات المرور.

4- بيانات الأنشطة الاجتماعية (Social Activity Data)

تتضمن البيانات التي يتم جمعها من التفاعلات على مواقع التواصل الاجتماعية مثل المنشورات, التعليقات ,المشاركات و الإجابات على منصات مثل فيسبوك، اكس، وإنستغرام.

5- البيانات المالية (Financial Data)

تشمل بيانات الدفع والتعاملات المالية التي يتم جمعها عند إجراء عمليات شراء عبر الإنترنت أو عند استخدام خدمات مالية.

6- البيانات التقنية (Technical Data)

وهي معلومات التي تتعلق بتفاصيل الجهاز والتطبيقات التي يستخدمها المستخدم مثل

- نوع المتصفح المستخدم (جوجل كروم، فايرفوكس)
- نوع الجهاز (هاتف محمول, حاسبة)
- نظام التشغيل المستخدم في الجهاز (الاندرويد, ويندوز)

7- البيانات المتعلقة بالصحة (Health Data)

تشمل البيانات التي يتم جمعها من التطبيقات الصحية مثل تطبيقات عدد الخطوات، معدل ضربات القلب أو الأجهزة القابلة للارتداء (مثل الساعات الذكية) اوالمواقع التي تعتني بالحالة الصحية والتي تتعقب الحالة الصحية للمستخدم.

8- بيانات التفاعل مع الإعلانات (Ad Interaction Data)

وتشمل الإعلانات التي يتم مشاهدتها من قبل المستخدم والبضائع التي يتم شراءها من قبله بعد مشاهدة الإعلان.

3-5 خصوصية وسائل التواصل الاجتماعي

تعد الخصوصية في وسائل التواصل الاجتماعي من الموضوعات المهمة للمستخدمين في العصر الرقمي الحالي، حيث يمكن أن تكون المعلومات الشخصية والمعطيات التي يتم مشاركتها على هذه الشبكات عرضة للاستخدام بطرق قد تؤثر على خصوصية الأفراد.

أهم النقاط المتعلقة بخصوصية وسائل التواصل الاجتماعي:

- الإعدادات الخاصة لمشاركة المنشورات تمنح معظم منصات التواصل الاجتماعي مثل فيسبوك، تويتر، وإنستغرام المستخدمين القدرة على تحديد من يستطيع رؤية منشوراتهم.

يمكنك تخصيص هذه الإعدادات بحيث يمكن ان يراه العامة , الأصدقاء, انا فقط. والشكل (2-5) يوضح تعديل الخصوصية الى الأصدقاء.

الشكل (5-2) تعديل الخصوصية الى الاصدقاء من يستطيع ان يرى المنشور في الفيسبوك.

- إعدادات الخصوصية الشخصية يمكن تحديد المعلومات الشخصية يمكن مشاركتها عبر حسابك، مثل أماكن الاقامة، مستوى التعليم، العمل، أو تاريخ الميلاد. وتوفر منصات مثل فيسبوك اكس خيارات لتحديد من يمكنه إرسال طلبات صداقة أو متابعة حسابك، الشكل (5-3) يوضح إخفاء المعلومات الشخصية وتحديد الخصوصية

الشكل (5-3) يوضح إخفاء المعلومات الشخصية وتحديد الخصوصية لمن يستطيع ان يرسل طلب صداقة في تطبيق الفيسبوك.

حيث يمكن إزالة جميع المعلومات الشخصية من مستوى التعليم، والعمل، الإقامة وغيرها. وكذلك تحديد من يمكنه ارسال طلب صداقة حيث يمكن جعل الجميع او تعطيل الخيار بحيث لا يستطيع أحد ارسال طلب صداقة من ضمن خصوصية وسائل التواصل الاجتماعي.

- **التحكم في الموقع الجغرافي:- العديد من وسائل التواصل الاجتماعية مثل سناب شات وإنستغرام تقدم خيارًا لمشاركة الموقع الجغرافي عند تحميل الصور أو الفيديوهات. يُفضل إيقاف هذه الميزة إذا كنت ترغب في الحفاظ على خصوصيتك، الشكل (4-5) يوضح يمكن إيقاف ميزة الموقع الجغرافي.**

الشكل (4-5) يمكن إيقاف ميزة الموقع الجغرافي للحفاظ على الخصوصية.

- **إعدادات الأمان تقدم معظم وسائل التواصل الاجتماعية خيارات المصادقة الثنائية، وهي إضافة طبقة أمان اخرى لحسابك بحيث يتطلب الدخول الى الحساب من خلال كلمة مرور بالإضافة إلى رمز يتم إرساله إلى هاتفك أو بريدك الإلكتروني. وإذا كنت تستخدم حسابك على أكثر من جهاز، يمكنك من خلال الإعدادات الخاصة بالحساب تسجيل الخروج من الأجهزة الأخرى التي لم تعد تستخدمها.**

4-5 اعدادات الخصوصية في المتصفح والأجهزة

هناك مجموعة من الاعدادات للمتصفح والأجهزة التي تقلل لحد كبير من التتبع للشخص, المؤسسات, الشركات عبر الانترنت منها:

1- أهم الإعدادات التي يمكن تخصيصها في المتصفح
يمكن ضبط اكثر من خاصية في اعدادات المتصفح منها:

- **إيقاف تتبع المواقع (Tracking Prevention)**

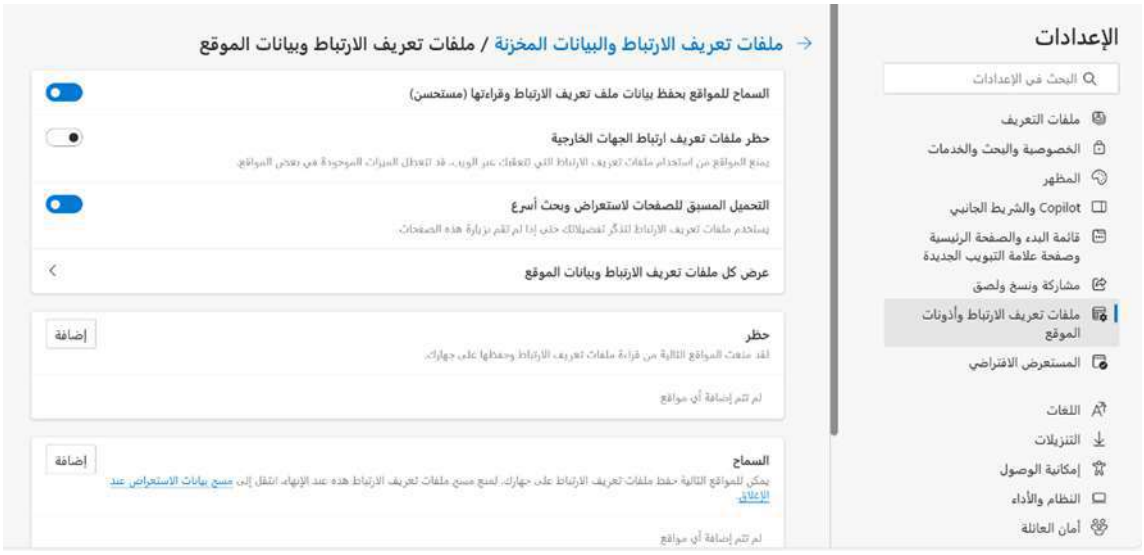
توفر معظم المتصفحات مثل كروم، فايرفوكس، خيار إيقاف تتبع المواقع، مما يمنع المواقع من جمع بياناتك أثناء التصفح. على سبيل المثال، يمكنك تفعيل وضع الحماية ضد التعقب في فايرفوكس أو جوجل كروم لضمان ألا تتمكن المواقع من تتبع سلوكك عبر الإنترنت، الشكل (5-5) يوضح إيقاف

التتبع حيث من النقاط الثلاثة (مزيد) في اعلى المتصفح نختار منها اعدادات ومن الاعدادات نختار الخصوصية ومنها نقوم بضبط التتبع كما موضح بالشكل في الاعلى.

الشكل (5-5) إيقاف تتبع المواقع.

- **إيقاف ملفات تعريف الارتباط (Cookies)**

الكوكيز تعني ملفات تعريف الارتباط ويعرف بسجل التتبع أو سجل المتصفح وهي معلومات يتم تخزينها من قبل متصفح الويب الخاص بك عن الإجراءات التي قمت بها سابقا على موقع ما على الانترنت.
وهذه المعلومات يمكنك ان تكون أي اجراء، مشترياتك ومقتنياتك على الانترنت او معلومات تسجيل الدخول الخاصة بك والصفحات التي قمت بزيارتها والازرار التي نقرت عليها والقائمة تطول وتطول. ومن فوائد ملفات تعريف الارتباط (الكوكيز) تقوم بحفظ تسجيل الدخول الى المواقع التي قمت بزيارتها فلا داعي لإعادة كتابتها في كل مرة، وكذلك عند كتابة الموقع الذي تريده يقوم بتكملة اسم الموقع كما في البحث في (Google) ومن اضراره تتلخص في حماية الخصوصية فتلك الملفات تقوم بحفظ معلوماتك عبر تلك الملفات وتتضمن تلك الملفات موقعك الجغرافي ونوع جهازك واهتماماتك وعنوان بريدك الإلكتروني والعديد من تلك المعلومات والتي تستخدمها بعض المواقع الأخرى.
تتيح لك العديد من المتصفحات مثل كروم وفايرفوكس إمكانية إدارة الكوكيز بحيث يمكنك إيقافها أو قبولها فقط من المواقع التي تختارها. الشكل (5-6) يوضح إعدادات ملفات تعريف الارتباط حيث من النقاط الثلاثة (مزيد) في اعلى المتصفح نختار منها اعدادات ومن الاعدادات نختار ملفات تعريف الارتباط ومنها نقوم بضبط الاعدادات.

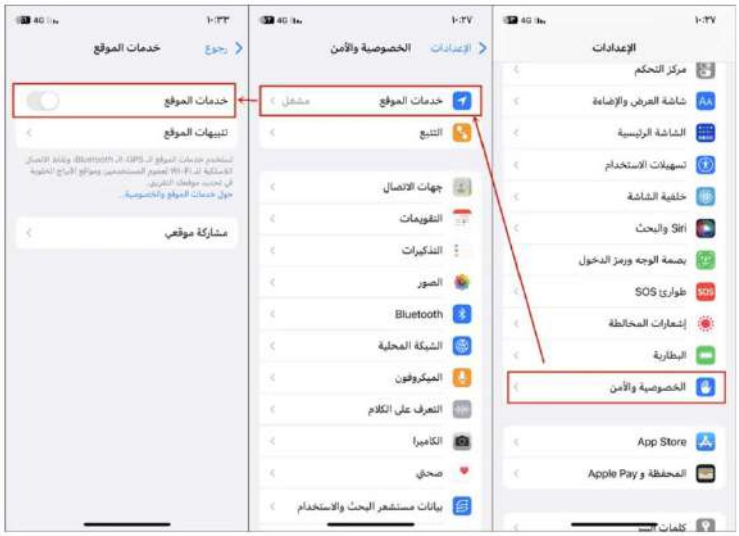


الشكل (5-6) يوضح اعداد ملفات تعريف الارتباط.

2- إعدادات الخصوصية على الهواتف الذكية

يمكن ضبط بعض الخصائص المتعلقة بتتبع الهاتف والتطبيقاته منها:

إيقاف تتبع المواقع على أجهزة آيفون وأندرويد، يمكنك إيقاف تتبع الموقع من خلال إعدادات الخصوصية. بإمكانك تحديد التطبيقات التي يمكنها الوصول إلى موقعك الجغرافي ومنع التطبيقات الأخرى من جمع هذه المعلومات. في الشكل (5-7) تم إيقاف الموقع في الجوال من الدخول الى الاعدادات ومن ثم الى الخصوصية والأمان واختيار خدمات الموقع وتحويلها الى إيقاف.



الشكل (5-7) إيقاف خدمات الموقع في الجوال.

وكذلك يمكن إيقاف تطبيق معين من التطبيقات كما في الشكل (5-8).

الشكل (5-8) إيقاف خدمات الموقع في الجوال لتطبيق معين.

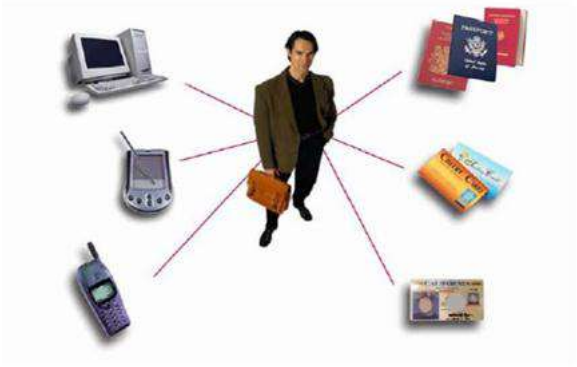
إدارة الأذونات للتطبيقات تأكد من إدارة أذونات التطبيقات بانتظام. على سبيل المثال، يمكنك إيقاف السماح للتطبيقات بالوصول إلى الكاميرا، الميكروفون، أو جهات الاتصال عندما لا تكون بحاجة إليها. في الشكل (5-9) يمكن التحكم في إعطاء او منع الاذن لتطبيق معين من الوصول الى الكاميرا، الميكروفون، أو جهات الاتصال من الدخول الى الاعدادات ومن ثم الى الخصوصية والأمان واختيار الاذونات.

الشكل (5-9) إيقاف او إعطاء الاذن لتطبيق معين من الوصول الى الكاميرا، الميكروفون أو جهات الاتصال.

- المصادقة البايومترية يُفضل تفعيل المصادقة البايومترية مثل البصمة أو التعرف على الوجه لزيادة الأمان وحماية خصوصيتك على الهاتف.
- إيقاف جمع البيانات على المتاجرعلى منصات مثل متجر جوجل ومتجر آبل، يمكنك ضبط إعدادات الخصوصية لتقليل تتبع التطبيقات لتفضيلاتك.

5-5 إدارة الهوية الرقمية وبناء البصمات الرقمية

الهوية الرقمية هي تمثيل شخصي للفرد أو الكيان (منظمة، شركة، مؤسسة) على الإنترنت. تهدف الهوية الرقمية إلى التوثيق والتعريف بالشخص أو المؤسسة في العالم الرقمي، وتسمح له بالوصول إلى الخدمات الإلكترونية بشكل آمن وفعال. تشمل الهوية الرقمية العديد من العناصر مثل الاسم، البريد الإلكتروني، رقم الهاتف، الحسابات على وسائل التواصل الاجتماعي، بيانات الحسابات المصرفية الرقمية، وأي معلومات أخرى تحدد الشخص أو الكيان في الفضاء الإلكتروني. وتشبه الهوية المادية مثل شهادات الميلاد وجوازات السفر ورخص القيادة. قد يكون للمستخدم أشكالًا عديدة من الهويات، تُخزَّن عادةً في أشكال وأماكن مختلفة كما هو موضح في الشكل (5-10).



الشكل (5-10) يوضح اشكال الهويات الشخصية.

5-5-1 إدارة الهوية الرقمية

تتضمن إدارة الهوية الرقمية مجموعة من الأنشطة والإجراءات:

1. إنشاء وتوثيق الهوية الرقمية:

- إنشاء حسابات للأشخاص أو المؤسسات على الإنترنت.
- استخدام التحقق الثنائي، كلمات مرور قوية، التعرف على الوجه أو بصمات الأصابع للتحقق من الهوية.

2. حماية الهوية الرقمية:

- عبر التشفير وأدوات الأمان الحديثة لضمان الأمان في إدارة البيانات الشخصية.
- استخدام تقنيات مثل التوثيق البايومتري (البصمة، التعرف على الوجه) لمنع التلاعب.

3. إدارة البيانات الشخصية:

- حماية الخصوصية من خلال تحديد من يمكنه الوصول إلى المعلومات الشخصية.
- التأكد من أن البيانات يتم تخزينها بشكل آمن، ويجب أن يتم الالتزام بالقوانين المتعلقة بحماية البيانات.

2-5-5 بناء البصمات الرقمية

البصمة الرقمية كما ذكرنا سابقا تشير إلى آثار أو إشارات تتركها الأنشطة الرقمية التي يقوم بها الشخص على الإنترنت. يمكن أن تتكون من:

1. المعلومات الشخصية:
   - مثل الاسم، العمر، البريد الإلكتروني، الموقع الجغرافي، وتفاصيل الحسابات.
2. الأنشطة الرقمية:
   - مثل المواقع التي تم زيارتها، التفاعل على منصات التواصل الاجتماعي، والاشتراكات في الخدمات الرقمية.
3. المحتوى الرقمي الذي يتم إنتاجه:
   - مثل الصور، الفديوات، المقالات، والتعليقات المنشورة على الإنترنت، والتي يمكن أن تساهم في اخذ صورة رقمية عن الشخص أو الكيان.

6-5 آليات التتبع والمراقبة من قبل الشركات والحكومات

يمكن استعمال البيانات التي تم جمعها من خلال نشاط الكيان على الانترنت والتي تساعد الشركات والحكومات على تتبع سلوكيات المستخدمين وتحليلها. وفيما يلي تفصيل لهذه الآليات مع أمثلة:

1- تتبع الأنشطة عبر الإنترنت (ملفات تعريف الارتباط)

تستخدم الشركات هذه البيانات لتحليل سلوك المستخدمين على الإنترنت، وتحسين طريقة الاستخدام الشخصية لهم، كما يمكن استخدامها لتوجيه الإعلانات التي يتفاعلون معها. حيث شركات مثل Google وFacebook تستخدم هذه الملفات لجمع بيانات حول تفاعلات المستخدم وذلك يساعدهم على تحديد اهتمامات المستخدمين بشكل أدق.

2- البصمة الرقمية للأجهزة (Device Fingerprinting)

هي تقنية تستخدم لتحديد هوية جهاز المستخدم بناءً على خصائص فريدة له، مثل نوع المتصفح، نظام التشغيل، إعدادات اللغة، والوقت المستخدم في التصفح. يتم تتبع الأجهزة عبر هذه الخصائص الفريدة حتى في حال مسح ملفات تعريف الارتباط، مما يجعل من الصعب على المستخدمين إخفاء هويتهم.

3- التتبع عبر الشبكات الاجتماعية

شبكات التواصل الاجتماعية مثل Facebook، Twitter، وInstagram تجمع كميات ضخمة من البيانات حول تفاعلات المستخدمين، اهتماماتهم، وموقعهم الجغرافي. تستخدم هذه الشركات تلك البيانات التي تم جمعها لتحديد الإعلانات التي يهتم بها المستخدم، وتحليل الاتجاهات العامة للمستخدمين. قد تقوم الحكومات أحيانًا بالوصول إلى هذه البيانات لأغراض التحقيق أو مراقبة النشاطات الاجتماعية. مثلا الحملات الإعلانية على Facebook تعتمد بشكل كبير على سلوكيات المستخدمين واهتماماتهم لتوجيه الإعلانات المعنية لهم.

4- التتبع عبر الهاتف المحمول

الهواتف المحمولة هي أحد الأدوات الرئيسية التي تستخدمها الشركات والحكومات في تتبع المستخدمين. من خلال تطبيقات الهواتف مثل Google Maps تقوم بتتبع موقع المستخدمين لأغراض تقديم الخدمة في مناطقهم وتحليل الأنماط الجغرافية. تقوم الشركات باستخدام البيانات الجغرافية لتحليل حركات المستخدمين، مثل تحركاتهم اليومية، والوقت الذي يقضونه في أماكن معينة. على سبيل المثال، تستخدم بعض المدن هذه البيانات لتحليل حركة المرور.

5- التعرف على الوجه (Facial Recognition)

تستخدم هذه التقنية لتحليل صور الوجه المخزنة. يمكن استخدامها لمراقبة الأشخاص في الأماكن العامة أو لتحديد الهوية. تستخدم تقنية التعرف على الوجه في هواتف المحمولة لفتح الجهاز وتقديم مزيد من الأمان. تستخدم الحكومة في بعض البلدان تقنية التعرف على الوجه في الأماكن العامة لمراقبة نشاط معين.

6- الاستماع إلى المكالمات وتسجيل البيانات الصوتية

في بعض الحالات، قد تقوم الحكومات أو الشركات باستخدام تقنيات لتحليل البيانات الصوتية التي يتم إرسالها عبر الإنترنت أو من خلال المكالمات الهاتفية. الحكومات قد تستخدم هذه التقنيات في التحقيقات الأمنية، في حين أن الشركات قد تستخدمها لتحليل التفاعلات مع العملاء.

7- تحليل البيانات الكبيرة (Big Data)

الشركات والحكومات يمكنها جمع وتحليل كميات هائلة من البيانات التي تم جمعها من مصادر متعددة مثل الإنترنت، وسائل التواصل الاجتماعي، الهواتف المحمولة، أجهزة الإنترنت يمكن أن تستخدم في اتخاذ قرارات تسويقية أو سياسات عامة.

8- المراقبة الحكومية (Spyware and Surveillance)

بعض الحكومات تستخدم برامج التجسس أو تقنيات المراقبة على الإنترنت لمراقبة النشاطات التي تتم عبر الإنترنت أو عبر الهواتف. تُستخدم هذه التقنيات بشكل متزايد في التحقيقات الأمنية أو للحد من الأنشطة السياسية والاجتماعية.

7-5 التهديدات الالكترونية المتعلقة بالبصمة الرقمية

التهديدات الإلكترونية المتعلقة بالبصمة الرقمية أصبحت واحدة من أكثر القضايا التي تثير القلق في عصرنا الرقمي الحالي. البصمة الرقمية هي جميع البيانات والآثار التي يتركها الأفراد عند استخدامهم للأجهزة والتقنيات الرقمية على الإنترنت. هذه البصمات يمكن أن تكون عرضة للاستغلال من قبل الجهات الخبيثة، سواء كانت شركات تسويقية أو مجرمي الإنترنت أو حتى الحكومات.

1- السرقة والاحتيال الرقمي

مع وجود الكثير من البيانات التي يتم جمعها عبر الإنترنت، يمكن أن تستغل هذه البيانات من قبل المهاجمين من خلال الهجمات الإلكترونية مثل الاحتيال الإلكتروني أو الهويات المزورة باستخدام البيانات التي تم جمعها عبر البصمة الرقمية (مثل بيانات الحسابات، الأنشطة الشرائية، والموقع الجغرافي). مثل هجمات التصيد الإلكتروني (Phishing) التي تعتمد على جمع بيانات المستخدمين لاستغلالها.

2- التجسس والرقابة

يتم استخدام البصمة الرقمية من قبل الحكومات أو المنظمات لمراقبة الأفراد. من خلال تتبع الأنشطة الرقمية عبر الإنترنت، قد تكون هناك انتهاكات لحقوق الخصوصية. مثلا مراقبة وسائل التواصل الاجتماعي أو الرسائل الخاصة.

3- الاستهداف بالإعلانات المضللة

يتم استخدام البيانات التي يتم جمعها من البصمة الرقمية لتوجيه إعلانات. في بعض الحالات، قد تكون هذه الإعلانات مضللة أو حتى ضارة، مثل الإعلانات التي تروج لمنتجات أو خدمات غير قانونية أو ضارة.

4- الهجمات على أنظمة المصادقة

العديد من المواقع والخدمات تستخدم تقنيات مثل المصادقة البايومترية (مثل بصمة الأصبع أو التعرف على الوجه) للتأكد من هوية المستخدم. إذا تم اختراق هذه الأنظمة، يمكن أن يؤدي ذلك إلى سرقة الهوية أو اختراق الحسابات.

8-5 ممارسات الأمن السيبراني لحماية وحذف البصمات الرقمية

حماية وحذف البصمات الرقمية أصبح أمرًا بالغ الأهمية في عصرنا الرقمي، خاصة في ظل تزايد التهديدات الأمنية المتعلقة بالخصوصية .لحماية وحذف البصمات الرقمية، توجد مجموعة من الممارسات الأمنية التي يجب اتباعها:

1- حذف ملفات تعريف الارتباط (الكوكيز) وبيانات التصفح
استخدم إعدادات المتصفح لتمكين الحذف التلقائي للكوكيز عند غلق المتصفح.
2- استخدام محركات بحث تحترم الخصوصية
بعض محركات البحث لا تقوم بتتبع أو تخزين بيانات البحث الشخصية للمستخدم، استخدم محركات البحث التي تركز على الخصوصية بدلاً من المحركات التقليدية مثل Google.

3- استخدام متصفحات معزولة أو وضع التصفح المتخفي (Incognito)
4- يتيح لك وضع التصفح المتخفي أو استخدام متصفحات معزولة مثل Torالتصفح دون تخزين أي بيانات عن المواقع التي تزورها.
5- تقييد الوصول إلى المعلومات الشخصية عبر وسائل التواصل الاجتماعي
من خلال تقليل المعلومات الشخصية المتاحة على الإنترنت، تقل احتمالية استخدامها من قبل الشركات أو المهاجمين.
6- استخدام تقنيات التشفير
تشفير البيانات يعني تحويل البيانات إلى صيغة غير قابلة للقراءة, يساعد التشفير في حماية بياناتك أثناء نقلها أو تخزينها، مما يمنع المهاجمين من الوصول إليها.
7- تقييد جمع البيانات عبر التطبيقات
من خلال تقليل وصول التطبيقات إلى البيانات الشخصية أو إيقاف جمع التطبيقات غير الضرورية، يمكن تقليل البصمة الرقمية.
8- استخدام أدوات الحماية مثل الشبكة الخاصة الافتراضية VPN (Virtual Private Network)
يمكن استخدام VPN لإخفاء موقعك الجغرافي، وعنوان IP، وحركة الإنترنت الخاصة بك، مما يقلل من قدرة الأطراف الخارجية على تتبع سلوكك الرقمي.

9-5 الفرص المستقبلية لاستخدام البصمة الرقمية

تتزايد أهمية البصمة الرقمية (Digital Footprint) في العصر الحديث مع تقدم التكنولوجيا وزيادة الاعتماد على الإنترنت. أصبحت البصمة الرقمية جزءًا لا يتجزأ من حياتنا اليومية، حيث يتم جمع البيانات عن الأفراد من خلال تصفحهم للإنترنت وتفاعلاتهم مع مختلف التطبيقات والمواقع الإلكترونية. هذه البصمة الرقمية توفر فرصًا مستقبلية في العديد من المجالات. في المستقبل، ستزداد أهمية هذه البيانات في تحسين تجربة المستخدم، تعزيز الأمان الرقمي، وفتح أبواب جديدة في مجالات أخرى.

1- تحسين تجربة المستخدم والتخصيص

ممكن للبيانات التي تُجمع من سلوك المستخدمين عبر الإنترنت أن تساهم في تقديم تجربة أكثر تخصيصًا. مثلًا، ستتمكن الشركات من تقديم محتوى، منتجات، أو خدمات تتماشى بشكل أكبر مع اهتمامات المستخدمين.

2- تحسين الخدمات الحكومية والخدمات العامة

من خلال تحليل البيانات التي يتم جمعها من المواطنين، يمكن تحسين تقديم الخدمات، مثل الرعاية الصحية، الرعاية الاجتماعية، والتعليم. يمكن استخدام هذه البيانات لتقديم خدمات مخصصة تعتمد على احتياجات الأفراد.

3- في مجال تعليم

يمكن تحليل بيانات البصمة الرقمية للطلاب في منصات التعليم الإلكتروني لفهم أنماط تعلمهم بشكل أفضل. قد تساعد هذه البيانات في تقديم محتوى تعليمي مخصص لكل طالب بناءً على أسلوبه في التعلم. في المستقبل.

اسئلة الفصل الخامس

س1/ عرف كلا مما يأتي

1- البصمة الرقمية
2- ملفات تعريف الارتباط
3- البيانات المتعقبة
4- الهوية الرقمية

س2/ عدد أنواع البيانات المتعقبة؟

س3/ كيف تؤثر وسائل التواصل الاجتماعي على خصوصية الأفراد؟

س4/ ما هي إعدادات الخصوصية التي يمكن تكوينها في المتصفح لحماية البيانات الشخصية؟

س5/ كيف تقوم الشركات بجمع البيانات من المستخدمين وكيف تستفيد منها؟

س6/ ما هي ممارسات الأمن السيبراني لحماية وحذف البصمات الرقمية؟

س7/ ما هي التهديدات الالكترونية المتعلقة بالبصمة الرقمية؟

الفصل السادس

تقنيات الأمن الحديثة في الأمن السيبراني

الأهداف

من المتوقع أن يكون الطالب قادراً على أن :

1. يتعرف على تقنيات الحماية الحديثة مثل التشفير وانظمة الكشف عن التسلل
2. يفهم اهمية حماية اجهزة انترنت الاشياء
3. يتمكن من اعداد برمجيات مكافحة الفيروسات وتحديثها بانتظام
4. يطبق تقنيات حماية اجهزة الهاتف ضد التطبيقات الخبيثة

1-6 مقدمة في تقنيات الأمن السيبراني الحديثة

مع التوسع في استخدام التكنولوجيا، أصبح الأمن السيبراني ضرورة لحماية البيانات والأنظمة من التهديدات الإلكترونية مثل القرصنة والبرمجيات الخبيثة. تعتمد تقنيات الأمن السيبراني على أدوات مثل التشفير لضمان سرية المعلومات، والجدران النارية لمنع الوصول غير المصرح به، وأنظمة كشف التسلل لمراقبة الأنشطة المشبوهة. كما تشمل المصادقة متعددة المراحل لحماية الحسابات، وبرامج مكافحة الفيروسات للتصدي للهجمات.

إلى جانب الأدوات التقنية، تلعب السياسات والإجراءات دورًا أساسيًا في تعزيز الأمن، من خلال وضع استراتيجيات لحماية البيانات، وتدريب المستخدمين، والاستجابة للطوارئ. ومع تعقيد التهديدات الإلكترونية، تتطور تقنيات الأمن السيبراني باستخدام الذكاء الاصطناعي وتحليل البيانات الضخمة لاكتشاف الهجمات والتصدي لها بفعالية. لذا، فإن تبني أحدث الحلول السيبرانية ورفع الوعي بأهميتها يشكلان حجر الأساس لحماية الأفراد والمؤسسات في العصر الرقمي.

1-1-6 أهمية تقنيات الأمن السيبراني الحديثة

- **حماية البيانات الشخصية**: يزداد خطر سرقة المعلومات مع الاعتماد المتزايد على الخدمات الرقمية.
- **تأمين الأنظمة المؤسسية**: تحتاج الشركات والمؤسسات إلى تقنيات متقدمة لحماية بياناتها الحساسة.
- **التصدي للهجمات الإلكترونية المتطورة**: تعتمد الهجمات الحديثة على أساليب معقدة، مما يتطلب استجابة أمنية متقدمة.

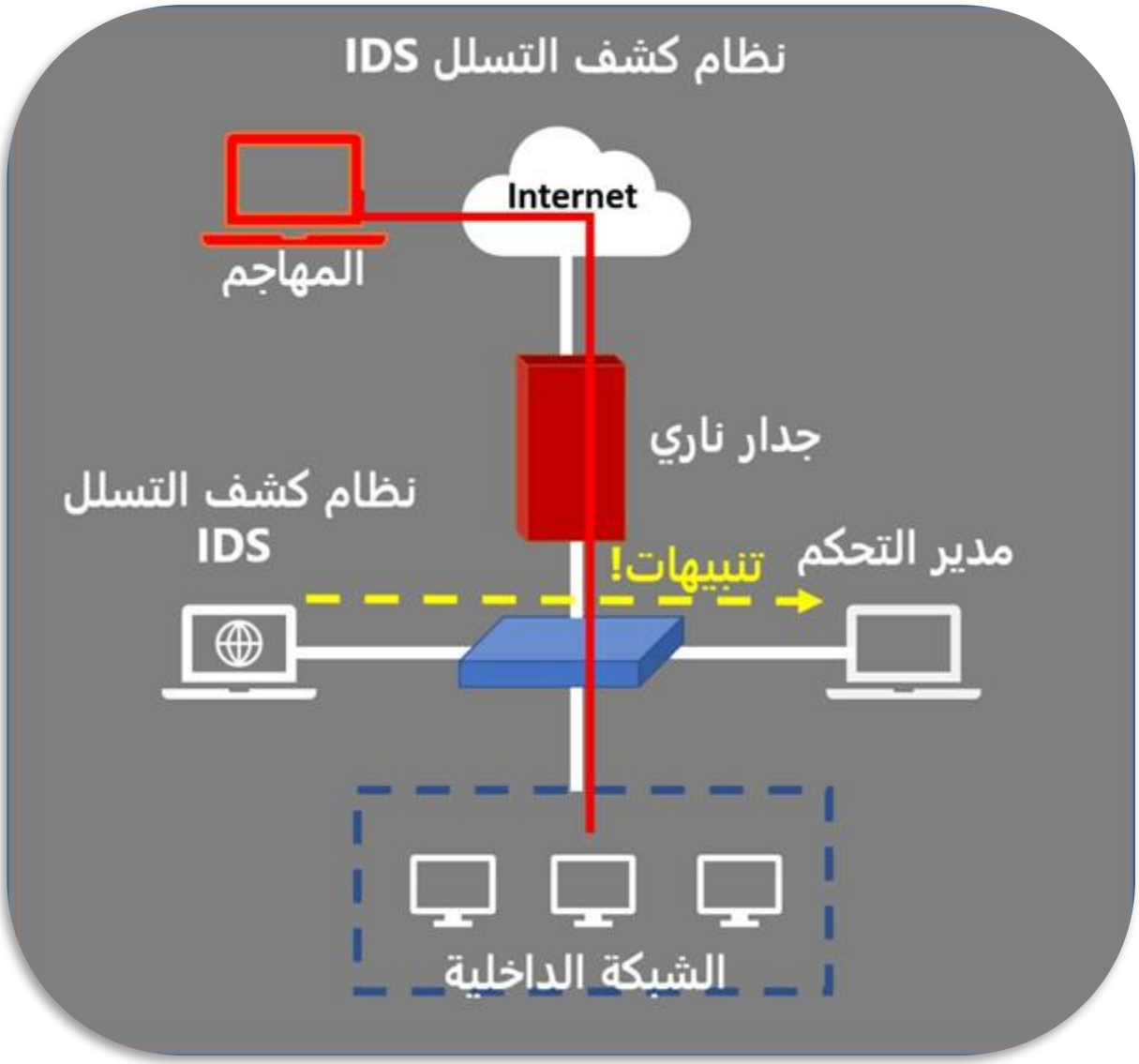
الشكل (6-1) يوضح أهمية تقنيات الأمن السيبراني

الشكل (6-1) أهمية تقنيات الأمن السيبراني

2-1-6 ابرز التقنيات الأمنية الحديثة:

1. أنظمة كشف التسلل (Intrusion Detection Systems - IDS)

هي أنظمة تراقب الشبكات والأنظمة بحثًا عن أنشطة غير طبيعية، مثل محاولات الاختراق أو البرمجيات الخبيثة، تستخدم هذه الأنظمة التحليل السلوكي لاكتشاف الأنشطة المشبوهة وإرسال تنبيهات إلى مسؤولي الأمن.

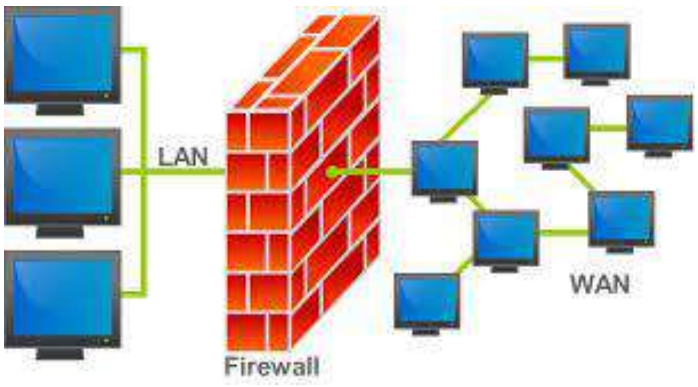


الشكل (2-6) يوضح أنظمة كشف التسلل **IDS**

2. الجدران النارية (Firewalls)

تعمل كحاجز بين الشبكة الداخلية والإنترنت، وتتحكم في تدفق البيانات لمنع التهديدات غير المصرح بها،يمكن أن تكون جدران حماية برمجية أو أجهزة مادية تستخدم في مراكز البيانات الكبيرة.

الشكل (3-6) يوضح عمل الجدار الناري



الشكل (3-6) يوضح عمل الجدار الناري

3. الحماية الاستباقية (Proactive Security Measures)

تُعد الحماية الاستباقية من أبرز الاتجاهات الحديثة في مجال الأمن السيبراني، حيث لا تكتفي بانتظار وقوع الهجمات ثم التعامل معها، بل تعمل على التنبؤ بها ومنعها قبل أن تحدث. تعتمد هذه المنهجية على تقنيات متقدمة مثل الذكاء الاصطناعي (AI) وتحليل البيانات الكبيرة (Big Data Analytics)، ما يجعلها أكثر فاعلية في مواجهة التهديدات المتطورة.

الذكاء الاصطناعي في الحماية الاستباقية

يستخدم الذكاء الاصطناعي خوارزميات قادرة على التعلّم من البيانات وتحليلها للتعرّف على الأنماط التي قد تشير إلى وجود تهديدات. وعند ملاحظة أي سلوك غير طبيعي أو خارج عن المألوف، يمكن للنظام أن يُصدر إنذارًا أو يقوم باتخاذ إجراء تلقائي، مثل حظر اتصال أو إغلاق منفذ شبكي.

من أبرز استخدامات الذكاء الاصطناعي في الحماية الاستباقية:

- **الكشف المبكر عن البرمجيات الخبيثة** من خلال التعرف على سلوكها بدلًا من انتظار توقيعها الرقمي.
- **تحليل سلوك المستخدم (User Behavior Analytics)** لاكتشاف التصرّفات الشاذة، مثل تسجيل الدخول من موقع غير معتاد أو محاولات الوصول إلى ملفات محمية.
- **أتمتة الاستجابة للحوادث** بشكل سريع وفعال، مما يقلل من زمن الاستجابة ويحدّ من الأضرار.
- **تحليل البيانات الكبيرة (Big Data) في التنبؤ بالتهديدات**

يتم جمع كميات ضخمة من البيانات من مصادر مختلفة مثل حركة الشبكة، سجلات الدخول، أنشطة التطبيقات، وأجهزة إنترنت الأشياء. وباستخدام أدوات تحليل متقدمة، يمكن تحديد الاتجاهات غير الطبيعية أو المؤشرات التي قد تدل على هجوم وشيك.

مثال على ذلك:

تحليل آلاف محاولات تسجيل الدخول الفاشلة من أماكن متعددة خلال فترة قصيرة قد يُشير إلى هجوم "تخمين كلمة المرور".

تكرار محاولات الوصول إلى ملف معين من عدة مواقع يمكن أن يدل على محاولة استخراج بيانات حساسة.

أهمية الحماية الاستباقية

- تقلل من احتمالية النجاح في تنفيذ الهجمات.
- تقلل من الخسائر الناتجة عن التهديدات.
- تدعم اتخاذ قرارات أمنية مبنية على معلومات دقيقة وآنية.

2-6 الذكاء الاصطناعي في اكتشاف التهديدات وتحليل البيانات الإلكترونية.

يُعتبر الذكاء الاصطناعي **(AI)** أحد أكثر الأدوات تقدمًا في مجال الأمن السيبراني، حيث يُستخدم لتحليل البيانات الضخمة والتعرف على الأنماط غير الطبيعية التي قد تشير إلى تهديدات سيبرانية محتملة.

6-2-1 كيف يساعد الذكاء الاصطناعي في الأمن السيبراني

يساعد الذكاء الاصطناعي في الأمن السيبراني بعدة طرق فعالة، حيث يستخدم تقنيات التعلم الآلي والتحليل الذكي للكشف عن التهديدات والاستجابة لها بسرعة. إليك أهم الأدوار التي يؤديها:

1. اكتشاف التهديدات بشكل سريع ودقيق:

يستخدم الذكاء الاصطناعي تقنيات مثل التعلم الآلي **(Machine Learning)** لتحليل كميات ضخمة من البيانات والكشف عن التهديدات المحتملة في الوقت الفعلي. يمكن للذكاء الاصطناعي اكتشاف الأنماط غير العادية في حركة المرور الشبكية، مثل محاولات التسلل أو البرمجيات الخبيثة.

2. التنبؤ بالتهديدات المستقبلية:

من خلال تقنيات التعلم العميق **(Deep Learning)** والتعلم الآلي، يمكن للذكاء الاصطناعي التنبؤ بالتهديدات قبل وقوعها بناءً على الأنماط السابقة أو المشبوهة. التنبؤ بالهجمات مثل **Zero-Day attacks** التي تستخدم ثغرات غير مكتشفة بعد.

3. الاستجابة التلقائية للهجمات:

يمكن للذكاء الاصطناعي الاستجابة بشكل تلقائي للهجمات عند اكتشافها، مثل عزل الأنظمة المتأثرة أو تفعيل الدفاعات دون الحاجة لتدخل بشري. تقنيات مثل الاستجابة التلقائية لحوادث الأمان **(SOAR)** تعتمد على الذكاء الاصطناعي لتحسين استجابة الأنظمة.

4. تحسين نظام الدفاعات ضد الهجمات المعقدة:

يساعد الذكاء الاصطناعي في تحليل الهجمات المعقدة مثل الهجمات الموجهة المتقدمة **(APT)**، ويقدم دفاعات ديناميكية تتكيف مع الأساليب الجديدة للهجوم.

باستخدام التعلم الآلي، يمكن أن يتعرف النظام على التكتيكات التي قد تستخدمها الهجمات، مما يجعل الدفاعات أكثر فعالية.

5. تحسين أمان البيانات وحمايتها:

يُستخدم الذكاء الاصطناعي في تقنيات التشفير الذكي لضمان حماية البيانات أثناء النقل أو التخزين. يمكن استخدام الذكاء الاصطناعي لمراقبة حركة البيانات على الشبكة وكشف أي أنشطة مشبوهة.

6. تقليل الإيجابيات الكاذبة (False Positives):

الذكاء الاصطناعي يساعد في تقليل الإيجابيات الكاذبة التي تحدث في أنظمة الأمان التقليدية، مما يسمح للمسؤولين الأمنيين بالتركيز على التهديدات الحقيقية فقط.

7. حماية الهوية والمصادقة:

يمكن استخدام الذكاء الاصطناعي لتحسين المصادقة المتعددة العوامل **(MFA)** و التعرف على الوجه أو البصمة لتوفير حماية قوية ضد الوصول غير المصرح به.

أنظمة الذكاء الاصطناعي يمكنها مراقبة سلوك المستخدمين لاكتشاف أي تغييرات غير معتادة قد تشير إلى اختراق.

8. تعزيز مراقبة الشبكات وأنظمة الأمان:

يعمل الذكاء الاصطناعي على تحسين مراقبة الشبكة عبر تحليل الأنماط السلوكية لاكتشاف الهجمات الجديدة التي قد تستخدم تقنيات غير تقليدية.

يمكن دمج الذكاء الاصطناعي مع أدوات مثل أنظمة الكشف عن التسلل **(IDS)** و الجدران النارية التنبؤية لتعزيز الأمان.

3-6 تقنيات التشفير لحماية البيانات الحساسة أثناء النقل والتخزين

التشفير هو عملية تحويل البيانات إلى صيغة غير مفهومة إلا لمن يملك مفتاح فك التشفير الصحيح.

أهم تقنيات التشفير الحديثة:

1. **التشفير أثناء النقل (Encryption in Transit)**

يحمي البيانات أثناء انتقالها عبر الإنترنت باستخدام بروتوكولات مثل **SSL/TLS**.

مثال: تأمين المعاملات المصرفية عبر الإنترنت.

2. **التشفير أثناء التخزين (Encryption at Rest)**

يُستخدم لحماية البيانات المخزنة على الأقراص الصلبة أو في السحابة الإلكترونية.

مثال: تشفير بيانات المستخدمين في خدمات التخزين السحابي.

3. **التوقيع الرقمي (Digital Signature)**

يُستخدم للتحقق من صحة البيانات والتأكد من عدم التلاعب بها أثناء النقل.

4-6 تقنيات أمنية لإنترنت الأشياء

انترنت الاشياء **Internet Of Things (IOT)** يشير مصطلح إنترنت الأشياء إلى شبكة من الأجهزة الذكية المتصلة بالإنترنت والقادرة على تبادل البيانات ومن الامثلة على اجهزة انترنت الأشياء:

1. **الأجهزة المنزلية الذكية**: مثل الثلاجات الذكية، أنظمة الإضاءة الذكية، وأجهزة التكييف الذكية.
2. **أنظمة المراقبة الأمنية**: مثل كاميرات المراقبة المتصلة بالإنترنت وأجهزة الإنذار الذكية.
3. **أجهزة الرعاية الصحية**: مثل الساعات الذكية التي تراقب معدل ضربات القلب وأجهزة تتبع النشاط البدني.
4. **السيارات الذكية**: أنظمة الملاحة المتصلة بالإنترنت وأنظمة التحكم الذاتي في السيارات.

الشكل (6-5) يمثل انترنت الأشياء

1-4-6 أبرز التهديدات الأمنية لإنترنت الأشياء:

1. **التحكم غير المصرح به في الأجهزة:** مثل اختراق كاميرا مراقبة والتحكم بها عن بُعد.
2. **استغلال الثغرات الأمنية في البرمجيات الثابتة:** وهي البرمجيات المسؤولة عن تشغيل الأجهزة.
3. **التجسس على البيانات المنقولة بين الأجهزة والخوادم:** مثل التنصت على البيانات المرسلة من أجهزة الاستشعار.

2-4-6 تقنيات حماية إنترنت الأشياء

1. **مصادقة الأجهزة (Device Authentication):**

التأكد من هوية الأجهزة المتصلة لمنع دخول أجهزة غير موثوقة.

الشكل (6-4) يوضح **مصادقة الأجهزة (Device Authentication)**

2. **تشفير الاتصالات في انترنت الاشياء (IoT Encryption):**

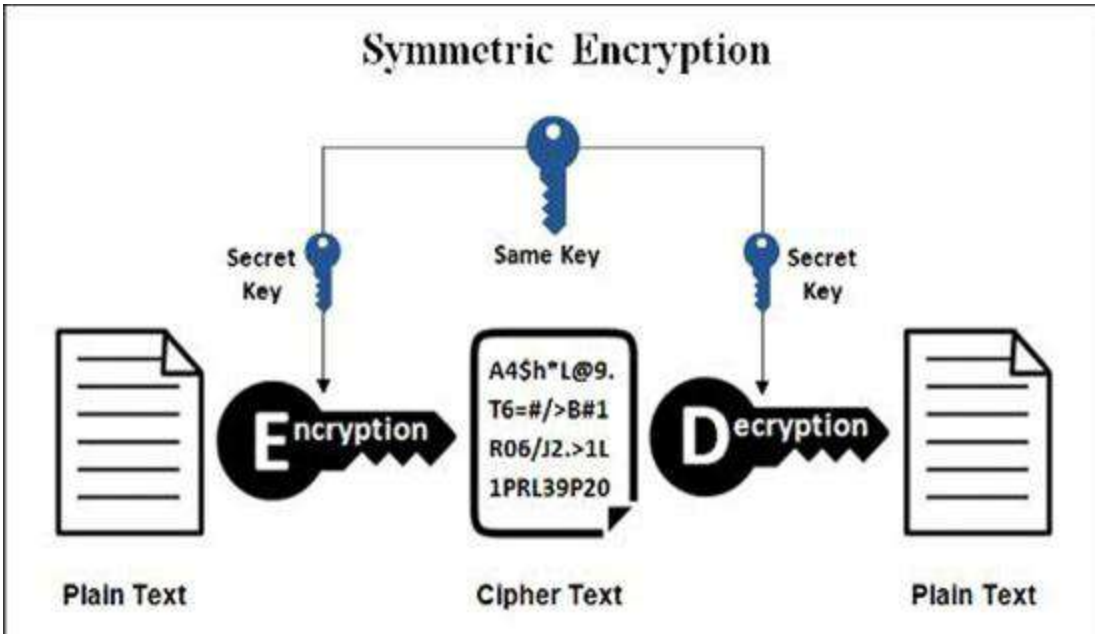
هو عملية تحويل البيانات المتبادلة بين أجهزة إنترنت الأشياء إلى صيغة غير قابلة للقراءة إلا من قبل الأطراف المخوّلة، وذلك لحماية هذه البيانات من التجسس أو التلاعب أثناء النقل.

أنواع التشفير في إنترنت الأشياء:

1. تشفير متماثل (Symmetric Encryption):

مفتاح واحد يُستخدم للتشفير وفك التشفير.سريع وأقل استهلاكًا للطاقة، مناسب للأجهزة ذات الموارد المحدودة.

مثال: خوارزمية AES (Advanced Encryption Standard).

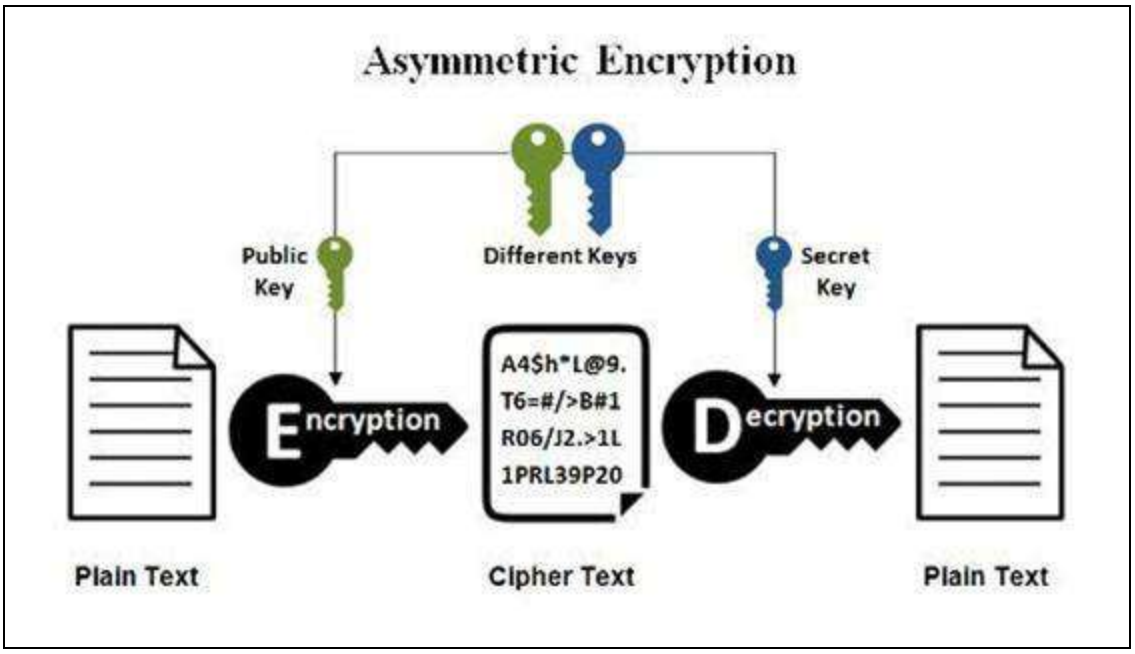


الشكل (6-5) يوضح تشفير متماثل (Symmetric Encryption)

2. تشفير غير متماثل (Asymmetric Encryption):

زوج من المفاتيح: مفتاح عام للتشفير ومفتاح خاص لفك التشفير، أكثر أمانًا لكنه يستهلك طاقة أكثر.

مثال: RSA و ECC (Elliptic Curve Cryptography).



الشكل (6-6) يوضح تشفير غير متماثل (Asymmetric Encryption)

3. تشفير أثناء النقل (Transport Layer Encryption):

مثل TLS/SSL لحماية البيانات المرسلة عبر الإنترنت أو الشبكة المحلية.

SSL هي مختصر لعبارة Secure Socket Layer وبالعربية تعني: طبقة المقابس الأمنة وبالمثل فإن TLS اختصار لـ Transport Layer Security وتعني عربيا أمان طبقة النقل.

علما أن TLS هو الإصدار الأحدث من SSL ولكن بسبب شيوع المصطلح SSL أكثر فإنه هو المستخدم أكثر.

هذا يعني أن المصطلحين مترادفان وهما طبقة تُعنى بأمان وتشفير المعلومات المتبادلة بين السيرفر (الخادم) والعميل (مستخدم الانترنت).

أي أن الاتصال الذي يحدث بين سيرفر الاستضافة المستضاف عليه موقعك الإلكتروني وبرنامج التصفح الذي تستخدمه يصبح آمنا ومشفرا بحيث تكون المعلومات المتبادلة ضمن الاتصال مشفرة.

ويمكن القول أيضا أنها تعمل على تشفير الاتصال بين الأجهزة المتصلة بشبكة الانترنت والتي يحدث بينها اتصال لأجل تبادل ونقل المعلومات بينهم.

وبشكل آخر فإن https أو SSL أو TLS يمنع المخترقين من قراءة أو تعديل المعلومات المنقولة بين الجهازين المتصلين من خلال تشفيرها.

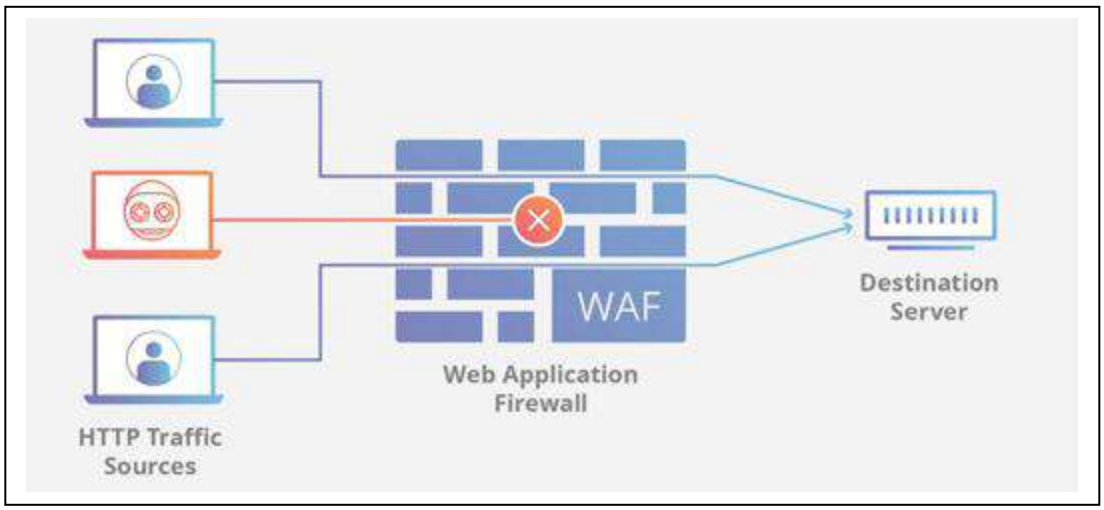
3. **تحديثات الأمان الدورية (Firmware Updates):**

سد الثغرات الأمنية من خلال تحديث البرمجيات الثابتة بانتظام.

5-6 تقنيات حماية التطبيقات والمواقع الإلكترونية:

تعد التطبيقات والمواقع الإلكترونية أهدافًا رئيسية للهجمات الإلكترونية، لذا من الضروري تأمينها من الثغرات الأمنية وأبرز تقنيات الحماية لها هي :

1. **استخدام الجدران النارية لتطبيقات الويب (WAF):** اختبار الاختراق الدوري لاكتشاف الثغرات الأمنية.



الشكل (6-7) يوضح الجدران النارية لتطبيقات الويب (WAF)

2. **اختبار الاختراق الدوري:** إجراء فحوصات أمنية منتظمة لاكتشاف نقاط الضعف ومعالجتها.
3. **إدارة الهوية والتحكم في الوصول (IAM):** تحديد صلاحيات المستخدمين ومنع الدخول غير المصرح به.

6-6 تقنيات أمن الأجهزة المحمولة وتطبيقاتها

أصبحت الهواتف الذكية أداة أساسية في الحياة اليومية، مما يجعلها عرضة للبرمجيات الخبيثة والاختراقات، وأفضل ممارسات الحماية لها هي :

1. **تحديث أنظمة التشغيل بانتظام:** لسد الثغرات الأمنية المكتشفة.
2. **تثبيت برامج مكافحة الفيروسات:** لكشف التهديدات وحذفها.
3. **استخدام المصادقة متعددة العوامل (MFA):** لإضافة طبقة أمان إضافية عند تسجيل الدخول.

الشكل (6-8) يوضح استخدام المصادقة متعددة العوامل (MFA)

اسئلة الفصل السادس

س1 / ناقش في 5 أسطر أهمية حماية أجهزة إنترنت الأشياء من التهديدات السيبرانية، مع ذكر مثال على تقنية لحمايتها.

س2/ اختر الإجابة الصحيحة؟

1- أي من التقنيات التالية تُستخدم لحماية المواقع الإلكترونية؟

أ- **WAF**
ب-**IDS**
ج-**SIEM**
د- جميع ما سبق

2- ما هي فائدة التحديثات الأمنية الدورية لأجهزة إنترنت الأشياء؟
أ) تحسين الأداء فقط
ب) منع استغلال الثغرات الأمنية
ج) تقليل استهلاك الطاقة
د) تحسين سرعة الإنترنت

3- تُستخدم أنظمة كشف التسلل (**IDS**) من أجل:
أ) تحسين أداء الشبكة
ب) مراقبة الأنشطة غير العادية واكتشاف التهديدات
ج) تسريع تحميل المواقع
د) إدارة كلمات المرور

4- يُستخدم بروتوكول **SSL/TLS** في:
أ) حماية الأجهزة المحمولة
ب) تشفير البيانات أثناء النقل
ج) تحليل البيانات الكبيرة
د) مراقبة الكاميرات الذكية

5- من تقنيات الحماية المستخدمة لتأمين أجهزة إنترنت الأشياء:

أ) مضاد الفيروسات
ب) تحليل سلوك المستخدم
ج) مصادقة الأجهزة
د) جميع ما سبق
6- التوقيع الرقمي يُستخدم من أجل:
أ) تسريع نقل البيانات
ب) التأكد من سلامة البيانات وعدم التلاعب بها
ج) التشفير أثناء التخزين
د) تشفير الاتصالات

س3 / علل ما ياتي:

"يُعد الذكاء الاصطناعي أداة قوية في كشف الهجمات الإلكترونية"؟

س4 / املأ الفراغات الاتية :

1. تعمل _____كحاجز أمني يتحكم في تدفق البيانات بين الشبكة الداخلية والإنترنت.
2. يُقصد بعملية تحويل البيانات إلى صيغة غير مفهومة إلا لمن يملك مفتاحًا صحيحًا _____.
3. تُستخدم _____ لاكتشاف الهجمات بناءً على تحليل سلوك المستخدم والبيانات.
4. من الأمثلة على أجهزة إنترنت الأشياء: _____، _____، _____،و._____
5. يُعتبر _____ من أهم التقنيات لحماية البيانات أثناء النقل عبر الإنترنت. من أبرز التهديدات التي تواجه أجهزة إنترنت الأشياء هو _____ والتحكم غير المصرح به بها
6. تُستخدم _____ لتحديد صلاحيات المستخدمين ومنع الدخول غير المصرح به إلى التطبيقات.
7. من أهم خطوات حماية الهاتف الذكي: تثبيت برامج مكافحة الفيروسات وتفعيل_____ .

الفصل السابع

الاخلاقيات والسياسات في الأمن السيبراني
Ethics and Polices in Cybersecurity

الأهداف

من المتوقع أن يكون الطالب قادراً على أن :

1. يتعرف على مفهوم الأخلاقيات في الأمن السيبراني واهميتها.
2. يدرك اهمية السياسات والقوانين لحماية البيانات واحترام الخصوصية.
3. يتدرب على وضع سياسة امان بسيطة للمعلومات الشخصية
4. يمارس الالتزام بأخلاقيات التعامل مع المعلومات مثل السرية وتجنب اساءة الاستخدام.

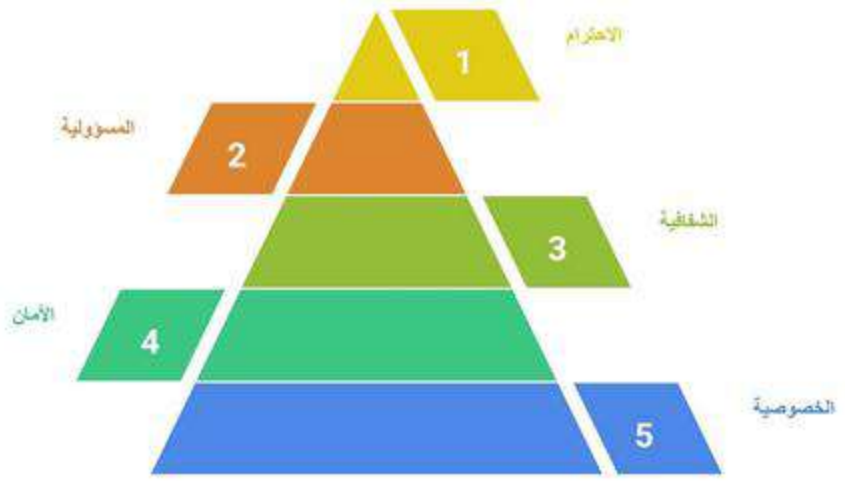
7- 1 مفهوم الاخلاقيات والسياسات في الأمن السيبراني

هي مجموعة من القواعد والمبادئ التي تحكم سلوك الأفراد والمنظمات في استخدام التكنولوجيا والشبكات والبيانات. بشكل عام، الاخلاقيات والسياسات في الأمن السيبراني تلعب دورًا مهماً في حماية البيانات والشبكات والمنظمات من التهديدات السيبرانية. من خلال تطبيق الاخلاقيات والسياسات الأمنية، يمكن للمنظمات والأفراد حماية بياناتهم وشبكاتهم من الهجمات السيبرانية، وبناء الثقة مع المستخدمين، وتقليل المخاطر الأمنية والمالية.

7-1-1الاخلاقيات في الأمن السيبراني

إن من أهم خصائص اخلاقيات الأمن السيبراني هي:

1. **الخصوصية:** حماية المعلومات الشخصية والسرية للأفراد والمنظمات.
2. **الأمان:** حماية البيانات والشبكات من الهجمات والتهديدات السيبرانية.
3. **الشفافية:** الكشف عن المعلومات والسياسات الأمنية بنحو واضح وشفاف.
4. **المسؤولية:** تحمل المسؤولية عن الأفعال والقرارات المتعلقة بالأمن السيبراني.
5. **الاحترام**: احترام حقوق وخصوصية الأفراد والمنظمات.



7-1-2 السياسات في الأمن السيبراني

إن سياسات الأمن السيبراني كثيرة، واهمها:

1. **سياسة الأمان:** مجموعة من القواعد واللوائح التي تحكم استخدام التكنولوجيا والشبكات والبيانات.
2. **سياسة الخصوصية:** مجموعة من القواعد التي تحكم جمع واستخدام المعلومات الشخصية.
3. **سياسة الوصول:** مجموعة من القواعد التي تحكم الوصول إلى البيانات والشبكات.
4. **سياسة النسخ الاحتياطي:** مجموعة من القواعد التي تحكم النسخ الاحتياطي للبيانات.
5. **سياسة الاستجابة للحوادث:** مجموعة من القواعد التي تحكم الاستجابة للحوادث الأمنية.

3-1-7 أهمية واهداف الاخلاقيات والسياسات في الأمن السيبراني

يمكن تلخيص اهمية واهداف الاخلاقيات والسياسات في الأمن السيبراني بالاتي:

1. **حماية البيانات:** حماية البيانات من الهجمات والتهديدات السيبرانية.
2. **بناء الثقة:** بناء الثقة بين الأفراد والمنظمات والمستخدمين.
3. **تقليل المخاطر:** تقليل المخاطر الأمنية والمالية الناجمة عن الهجمات السيبرانية.
4. **الامتثال للقوانين:** الامتثال للقوانين واللوائح الأمنية.
5. **تحسين الأمن:** تحسين الأمن السيبراني والحماية من التهديدات.
6. **حماية الشبكات:** حماية الشبكات من الهجمات والتهديدات السيبرانية.
7. **بناء الثقة:** بناء الثقة بين الأفراد والمنظمات والمستخدمين.
8. **الكشف عن التهديدات:** الكشف عن التهديدات السيبرانية والاستجابة لها.
9. **استعادة البيانات:** استعادة البيانات في حالة حدوث هجوم سيبراني أو كارثة.
10. **حماية الخصوصية:** حماية خصوصية الأفراد والمنظمات.
11. **تطوير المعرفة:** تطوير المعرفة والمهارات في مجال الأمن السيبراني.

ويمكن اعتبار بعض الاهداف قصيرة المدى مثل، الكشف عن التهديدات وحماية واستعادة البيانات. بينما تعتبر تحسين الأمن و بناء الثقة و تطوير المعرفة اهداف بعيدة المدى.

2-7 أهمية السياسات والقوانين في تنظيم الممارسات الأمنية

تلعب السياسات والقوانين دورًا هامًا في تنظيم الممارسات الأمنية، وتوفير إطار عمل واضح ومحدد للتعامل مع التهديدات الأمنية. ويمكن تحديد أهم السياسات والقوانين المهمة لتنظيم الممارسات الأمنية بالاتي:

1. **تحديد الإطار العام:** تحديد الإطار العام للممارسات الأمنية، بما في ذلك الأهداف والمسؤوليات.
2. **توجيه القرارات:** توجيه القرارات الأمنية، وضمان اتخاذ القرارات الصحيحة في الوقت المناسب.
3. **ضمان الاتساق**: ضمان الاتساق في الممارسات الأمنية، وتجنب التباين في تطبيق السياسات.
4. **حماية البيانات:** حماية البيانات من التهديدات الأمنية، وضمان سرية وخصوصية البيانات.
5. **تعزيز الثقة:** تعزيز الثقة بين الأفراد والمنظمات والمستخدمين، وضمان الشفافية في الممارسات الأمنية.

وعليه فان أهمية قوانين تنظيم الممارسات الأمنية تتلخص بالاتي:

1. **تحديد المسؤوليات:** تحديد المسؤوليات القانونية للمنظمات والأفراد، وضمان تحمل المسؤولية عن الأفعال الأمنية.
2. **ضمان الامتثال:** ضمان الامتثال للقوانين واللوائح الأمنية، وتجنب العقوبات القانونية.
3. **حماية الحقوق:** حماية حقوق الأفراد والمنظمات، وضمان احترام الخصوصية والسرية.

4. **توفير الإطار القانوني:** توفير الإطار القانوني للممارسات الأمنية، وضمان تطبيق القوانين واللوائح بشكل عادل.
5. **تعزيز الأمن:** تعزيز الأمن السيبراني، وضمان حماية البيانات والشبكات من التهديدات الأمنية.

3-7 أنواع السياسات المستخدمة في الادارة الإلكترونية

هناك عدة أنواع من السياسات المستخدمة في الإدارة الإلكترونية، وتشمل الاتي:

1. **سياسة الأمان:** سياسة الأمان تحدد الإجراءات والضوابط الأمنية لحماية البيانات والشبكات والأنظمة الإلكترونية من التهديدات الأمنية.
2. **سياسة الخصوصية:** سياسة الخصوصية تحدد كيفية جمع واستخدام وحماية البيانات الشخصية للأفراد والمنظمات.
3. **سياسة الوصول:** سياسة الوصول تحدد من يمكنه الوصول إلى البيانات والشبكات والأنظمة الإلكترونية، وكيفية الوصول إليها.
4. **سياسة النسخ الاحتياطي:** سياسة النسخ الاحتياطي تحدد كيفية عمل نسخ احتياطية للبيانات والأنظمة الإلكترونية، لضمان استعادة البيانات في حالة حدوث كارثة أو هجوم سيبراني.
5. **سياسة الاستجابة للحوادث:** سياسة الاستجابة للحوادث تحدد الإجراءات التي يجب اتخاذها في حالة حدوث هجوم سيبراني أو كارثة، لضمان استعادة النظام والبيانات بسرعة.
6. **سياسة استخدام التكنولوجيا:** سياسة استخدام التكنولوجيا تحدد كيفية استخدام التكنولوجيا في المنظمة، بما في ذلك استخدام الأجهزة والبرمجيات والشبكات.
7. **سياسة حماية البيانات:** سياسة حماية البيانات تحدد كيفية حماية البيانات من التهديدات الأمنية، بما في ذلك حماية البيانات من الوصول غير المصرح به والاستخدام غير المصرح به.
8. **سياسة الشبكات:** سياسة الشبكات تحدد كيفية إدارة الشبكات والأنظمة الإلكترونية، بما في ذلك حماية الشبكات من التهديدات الأمنية.
9. **سياسة البريد الإلكتروني:** سياسة البريد الإلكتروني تحدد كيفية استخدام البريد الإلكتروني في المنظمة، بما في ذلك حماية البريد الإلكتروني من التهديدات الأمنية.
10. **سياسة الاستخدام المقبول:** سياسة الاستخدام المقبول تحدد كيفية استخدام التكنولوجيا والشبكات والأنظمة الإلكترونية بشكل مقبول، بما في ذلك تجنب الاستخدام غير المصرح به أو غير اللائق.
11. **سياسة إدارة الهوية والوصول:** سياسة إدارة الهوية والوصول تحدد كيفية إدارة هويات المستخدمين والوصول إلى البيانات والشبكات والأنظمة الإلكترونية.
12. **سياسة إدارة المخاطر:** سياسة إدارة المخاطر تحدد كيفية تحديد وتقييم وإدارة المخاطر الأمنية في المنظمة.
13. **سياسة التدقيق الأمني:** سياسة التدقيق الأمني تحدد كيفية إجراء التدقيق الأمني للبيانات والشبكات والأنظمة الإلكترونية.
14. **سياسة الاستجابة للتهديدات:** سياسة الاستجابة للتهديدات تحدد كيفية الاستجابة للتهديدات الأمنية، بما في ذلك التهديدات السيبرانية والهجمات الإلكترونية.

15. **سياسة حماية المعلومات:** سياسة حماية المعلومات تحدد كيفية حماية المعلومات من التهديدات الأمنية، بما في ذلك حماية المعلومات من الوصول غير المصرح به والاستخدام غير المصرح به.
16. **سياسة إدارة الشبكات:** سياسة إدارة الشبكات تحدد كيفية إدارة الشبكات والأنظمة الإلكترونية، بما في ذلك حماية الشبكات من التهديدات الأمنية.
17. **سياسة إدارة البرمجيات:** سياسة إدارة البرمجيات تحدد كيفية إدارة البرمجيات والأنظمة الإلكترونية، بما في ذلك تحديث البرمجيات وإدارة الترخيص.
18. **سياسة إدارة الأجهزة:** سياسة إدارة الأجهزة تحدد كيفية إدارة الأجهزة الإلكترونية، بما في ذلك حماية الأجهزة من التهديدات الأمنية.
19. **سياسة إدارة البيانات:** سياسة إدارة البيانات تحدد كيفية إدارة البيانات، بما في ذلك جمع البيانات وتخزينها واستخدامها.
20. **سياسة الامتثال:** سياسة الامتثال تحدد كيفية الامتثال للقوانين واللوائح والسياسات الأمنية في المنظمة.

إن هذه السياسات جميعها تلعب دوراً مهماً في ضمان أمان وفاعلية الإدارة الإلكترونية، وحماية البيانات والشبكات والأنظمة الإلكترونية من التهديدات الأمنية.

4-7 الأدوار والمسؤوليات والمبادئ الأخلاقية المتبعة من قبل المختصين في الأمن السيبراني

1-4-7 الأدوار الأخلاقية المتبعة من قبل المختصين في الأمن السيبراني

الفقرات التالية تتضمن اهم الادوار الأخلاقية المتبعة من قبل المختصين في الأمن السيبراني

1. **حماية البيانات:** حماية البيانات من التهديدات الأمنية والهجمات السيبرانية.
2. **تأمين الشبكات:** تأمين الشبكات والأنظمة الإلكترونية من التهديدات الأمنية.
3. **الكشف عن التهديدات:** الكشف عن التهديدات الأمنية والاستجابة لها.
4. **تطوير السياسات الأمنية:** تطوير السياسات الأمنية والإجراءات الأمنية.
5. **تدريب الموظفين:** تدريب الموظفين على الأمن السيبراني والتهديدات الأمنية.

2-4-7 المسؤوليات الأخلاقية المتبعة من قبل المختصين في الأمن السيبراني

بالطبع هناك الكثير من المسؤوليات الأخلاقية الواجب اتباعها من قبل المختصين في الأمن السيبراني، نورد اهمها:

1. **حماية الخصوصية:** حماية خصوصية الأفراد والمنظمات.
2. **الامتثال للقوانين:** الامتثال للقوانين واللوائح الأمنية.

3. **حماية البيانات:** حماية البيانات من الوصول غير المصرح به والاستخدام غير المصرح به.
4. **الاستجابة للحوادث:** الاستجابة للحوادث الأمنية والتهديدات السيبرانية.
5. **تطوير المعرفة:** تطوير المعرفة والمهارات في مجال الأمن السيبراني.
6. **التعاون:** التعاون مع الأفراد والمنظمات الأخرى لتعزيز الأمن السيبراني.

7-4-3 المبادئ الأخلاقية المتبعة من قبل المختصين في الأمن السيبراني

فيما يلي ادناه اهم المبادئ الأخلاقية الواجب اتباعها من قبل المختصين في الأمن السيبراني:

1. **الصدق:** الصدق في التعامل مع البيانات والتهديدات الأمنية.
2. **الأمانة:** الأمانة في التعامل مع البيانات والتهديدات الأمنية.
3. **الاحترام:** احترام حقوق وخصوصية الأفراد والمنظمات.
4. **المسؤولية:** تحمل المسؤولية عن الأفعال والقرارات الأمنية.
5. **الشفافية:** الشفافية في التعامل مع البيانات والتهديدات الأمنية.

7-5 التحديات الأخلاقية المرتبطة بالمراقبة الإلكترونية

التحديات الأخلاقية المرتبطة بالمراقبة الإلكترونية تشمل:

7-5-1 التحديات الأخلاقية والعملية

التحديات الأخلاقية والعملية والتي لها علاقة وطيدة بالمراقبة الإلكترونية هي:

1. **الخصوصية:** حماية خصوصية الأفراد والمنظمات من المراقبة الإلكترونية غير المصرح بها.
2. **الحرية الفردية:** حماية الحرية الفردية للأفراد من المراقبة الإلكترونية المفرطة.
3. **العدالة:** ضمان عدالة المراقبة الإلكترونية وتجنب التمييز.
4. **المسؤولية:** تحمل المسؤولية عن المراقبة الإلكترونية وضمان استخدامها بشكل مسؤول.
5. **تحديد الحدود:** تحديد الحدود بين المراقبة الإلكترونية المشروعة وغير المشروعة.
6. **تجنب الإفراط:** تجنب الإفراط في المراقبة الإلكترونية وتأثيرها على الحرية الفردية.
7. **ضمان الشفافية:** ضمان الشفافية في المراقبة الإلكترونية وتوضيح الأهداف والأساليب المستخدمة.
8. **حماية البيانات:** حماية البيانات المجمعة من خلال المراقبة الإلكترونية من الوصول غير المصرح به والاستخدام غير المصرح به.
9. **الامتثال للقوانين:** الامتثال للقوانين واللوائح المتعلقة بالمراقبة الإلكترونية.

2-5-7 التحديات التكنولوجية

هناك الكثير من التحديات التكنلوجية والعملية والتي لها علاقة كبيرة بالمراقبة الإلكترونية هي:

1. **تطوير التكنولوجيا:** تطوير التكنولوجيا التي تمكن المراقبة الإلكترونية الفاعلة دون المساس بالخصوصية والحرية الفردية.
2. **حماية البيانات:** حماية البيانات المجمعة من خلال المراقبة الإلكترونية من التهديدات الأمنية.
3. **تأمين الشبكات:** تأمين الشبكات والأنظمة الإلكترونية المستخدمة في المراقبة الإلكترونية.

3-5-7 التحديات الاجتماعية

ان للتحديات الأجتماعية المرتبطة بالمراقبة الإلكترونية دور كبير في تعزيز الأمن السيبراني وهي:

1. **التأثير على المجتمع:** فهم تأثير المراقبة الإلكترونية على المجتمع والحرية الفردية.
2. **الوعي العام:** زيادة الوعي العام بأهمية المراقبة الإلكترونية والتحديات الأخلاقية المرتبطة بها.
3. **التوازن بين الأمن والحرية:** تحقيق التوازن بين الأمن والحرية الفردية في المراقبة الإلكترونية.

6-7 الالتزام بالقوانين والتشريعات المحلية والدولية في مجال الأمن السيبراني

الالتزام بالقوانين والتشريعات المحلية والدولية في مجال الأمن السيبراني يتم من خلال عدة خطوات وإجراءات، تشمل:

1-6-7 الخطوات الأساسية

فيما يلي ادناه اهم الخطوات الأساسية الالتزام بالقوانين والتشريعات المحلية والدولية في مجال الأمن السيبراني:

1. **فهم القوانين والتشريعات:** فهم القوانين والتشريعات المحلية والدولية المتعلقة بالأمن السيبراني.
2. **تطوير السياسات:** تطوير السياسات والإجراءات الأمنية التي تتماشى مع القوانين والتشريعات.
3. **تدريب الموظفين:** تدريب الموظفين على القوانين والتشريعات الأمنية والسياسات والإجراءات الأمنية.
4. **تنفيذ الإجراءات الأمنية:** تنفيذ الإجراءات الأمنية التي تضمن حماية البيانات والشبكات والأنظمة الإلكترونية.
5. **المراجعة والتقييم:** المراجعة والتقييم الدوري للسياسات والإجراءات الأمنية لضمان الامتثال للقوانين والتشريعات.

2-6-7 الإجراءات العملية

..هناك اجراءات عملية لها الدور الكبير في تشريع القوانين الخاصة بالأمن السيبراني، وهي كالاتي:

1. **تحديد المخاطر:** تحديد المخاطر الأمنية والتهديدات السيبرانية التي قد تؤثر على الامتثال للقوانين والتشريعات.
2. **تطوير خطة أمنية:** تطوير خطة أمنية شاملة لضمان الامتثال للقوانين والتشريعات.
3. **تنفيذ الضوابط الأمنية:** تنفيذ الضوابط الأمنية التي تضمن حماية البيانات والشبكات والأنظمة الإلكترونية.
4. **الاستجابة للحوادث:** الاستجابة للحوادث الأمنية والتهديدات السيبرانية بشكل فعال.
5. **التدقيق الأمني:** إجراء التدقيق الأمني الدوري لضمان الامتثال للقوانين والتشريعات.

3-6-7 الأطر القانونية

بالطبع يجب ان يكون هناك اطر قانونية مهمة لوضع القوانين المتعلقة بالأمن السيبراني ومنها:

1. **القوانين المحلية:** الامتثال للقوانين المحلية المتعلقة بالأمن السيبراني، مثل قوانين حماية البيانات والخصوصية.
2. **القوانين الدولية:** الامتثال للقوانين الدولية المتعلقة بالأمن السيبراني، مثل الاتفاقيات والمعاهدات الدولية.
3. **اللوائح التنظيمية:** الامتثال للوائح التنظيمية المتعلقة بالأمن السيبراني، مثل لوائح حماية البيانات والخصوصية.

4-6-7 الأدوات والتقنيات

ان من اهم الأدوات والتقنيات التي نحتاجها في تشريع القوانين الخاصة بالأمن السيبراني، هي الاتي:

1. **أنظمة إدارة الأمن:** استخدام أنظمة إدارة الأمن لضمان الامتثال للقوانين والتشريعات.
2. **أدوات التدقيق الأمني:** استخدام أدوات التدقيق الأمني لضمان الامتثال للقوانين والتشريعات.
3. **أنظمة الكشف عن التهديدات:** استخدام أنظمة الكشف عن التهديدات لضمان الامتثال للقوانين والتشريعات.

جميع هذه الخطوات والإجراءات والأطر القانونية والأدوات والتقنيات تساعد في ضمان الالتزام بالقوانين والتشريعات المحلية والدولية في مجال الأمن السيبراني.

7-7 القرصنة الأخلاقية والقرصنة الخبيثة

القرصنة الأخلاقية والقرصنة الخبيثة هما مصطلحان يُستخدمان لوصف نوعين مختلفين من النشاطات السيبرانية. إليك عزيزي الطالب شرحاً مفصلًا لكل نوع:

1-7-7 القرصنة الأخلاقية

القرصنة الأخلاقية، المعروفة أيضًا **بالاختبار الاختراقي أو القرصنة البيضاء**، هي عملية استخدام تقنيات القرصنة لاختبار أمان الأنظمة والشبكات والبرمجيات. الهدف من القرصنة الأخلاقية هو تحديد الثغرات الأمنية وإصلاحها قبل أن يستغلها القراصنة الخبيثون. ان الغرض النهائي من القرصنة الأخلاقية هو تحسين أمان الأنظمة والشبكات والبرمجيات. وبالطبع فان القرصنة الأخلاقية تتم بترخيص من أصحاب الأنظمة والشبكات.

1-1-7-7 أهداف القرصنة الأخلاقية

هناك عدة اهداف للقرصنة للقرصنة الاخلاقية، اهمها:

1. **تحسين الأمان:** تحسين أمان الأنظمة والشبكات والبرمجيات من خلال تحديد الثغرات الأمنية وإصلاحها.
2. **حماية البيانات:** حماية البيانات من الوصول غير المصرح به والاستخدام غير المصرح به.
3. **تقييم الأمان:** تقييم أمان الأنظمة والشبكات والبرمجيات لتحديد نقاط الضعف.

2-1-7-7 أساليب القرصنة الأخلاقية

تستخدم القرصنة الأخلاقية نفس الأساليب التي يستخدمها القراصنة الخبيثون، ولكن بغرض تحسين الأمان، ومن هذه الاساليب:

1. **اختبار الاختراق:** اختبار الاختراق هو عملية محاكاة هجوم سيبراني لتحديد الثغرات الأمنية.

2. **فحص الثغرات**: فحص الثغرات هو عملية تحديد الثغرات الأمنية في الأنظمة والشبكات والبرمجيات.
3. **اختبار الأمان:** اختبار الأمان هو عملية اختبار أمان الأنظمة والشبكات والبرمجيات لتحديد نقاط الضعف.

2-7-7 القرصنة الخبيثة

القرصنة الخبيثة، المعروفة أيضًا بالقرصنة السوداء، هي عملية استخدام تقنيات القرصنة لاستغلال الثغرات الأمنية في الأنظمة والشبكات والبرمجيات. الهدف من القرصنة الخبيثة هو تحقيق مصالح شخصية أو مالية أو غيرها من المصالح الخبيثة. الغرض من القرصنة الخبيثة هو استغلال الثغرات الأمنية للوصول غير المصرح به إلى البيانات أو الأنظمة.

1-2-7-7 أهداف القرصنة الخبيثة

هناك عدة اهداف للقرصنة الخبيثة، اهمها:

1. **سرقة البيانات:** سرقة البيانات الحساسة، مثل المعلومات المالية أو الشخصية.
2. **تدمير الأنظمة:** تدمير الأنظمة والشبكات والبرمجيات لتحقيق أهداف خبيثة.
3. **ابتزاز الضحايا:** ابتزاز الضحايا من خلال تهديدهم بنشر بياناتهم أو تدمير أنظمتهم.

2-2-7-7 أساليب القرصنة الخبيثة

تستخدم القرصنة الخبيثة أساليب مختلفة، مثل البرمجيات الخبيثة والفيروسات والهجمات السيبرانية، ومنها:

1. **البرمجيات الخبيثة:** استخدام البرمجيات الخبيثة، مثل الفيروسات والديدان والحصان طروادة، لاستغلال الثغرات الأمنية.

2. **الهجمات السيبرانية:** استخدام الهجمات السيبرانية، مثل هجمات الحرمان من الخدمة (**DoS**) وهجمات الوسيط (**Man-in-the-Middle**) لاستغلال الثغرات الأمنية.
3. **التصيد الاحتيالي:** استخدام التصيد الاحتيالي لخداع الضحايا والحصول على بياناتهم الحساسة.

3-7-7 الاختلافات الرئيسية بين القرصنة الاخلاقية والقرصنة الخبيثة

يمكن تلخيص اهم الاختلافات بين القرصنة الاخلاقية والقرصنة الخبيثة من خلال الجدول التالي:

	الوصف	القرصنة الاخلاقية	القرصنة الخبيثة
1	الغرض	تحسين الأمان	استغلال الثغرات الأمنية
2	الترخيص	تتم بترخيص من أصحاب الأنظمة والشبكات	دون ترخيص
3	الأثر	تحسين الأمان	تدمير الأمان

بشكل عام، القرصنة الأخلاقية هي ممارسة أمنية مشروعة وضرورية لتحسين أمان الأنظمة والشبكات، بينما القرصنة الخبيثة هي نشاط غير قانوني وضار.

8-7 المبادئ الاساسية والعملية للقرصنة الأخلاقية

المبادئ الأخلاقية للقرصنة الأخلاقية تشمل:

7-8-1 المبادئ الأساسية للقرصنة الأخلاقية

المبادئ الأخلاقية تلعب دورًا هامًا في ضمان أن تكون القرصنة الأخلاقية ممارسة أمنية مشروعة ومسؤولة، لذلك فان اهم اساسيات المبادئ الأخلاقية:

1. **الاحترام**: احترام خصوصية وحقوق الأفراد والمنظمات.
2. **الشفافية:** الشفافية في التعامل مع البيانات والأنظمة والشبكات.
3. **المسؤولية:** تحمل المسؤولية عن الأفعال والقرارات المتعلقة بالقرصنة الأخلاقية.
4. **الاحترافية:** الاحترافية في التعامل مع البيانات والأنظمة والشبكات.
5. **الالتزام بالقوانين:** الالتزام بالقوانين واللوائح المتعلقة بالقرصنة الأخلاقية.
6. **الصدق والامانة:** الصدق في التعامل مع البيانات والأنظمة والشبكات.
7. **الالتزام بالمعايير الأخلاقية:** الالتزام بالمعايير الأخلاقية والمهنية في مجال القرصنة الأخلاقية.
8. **التعلم المستمر**: التعلم المستمر وتطوير المهارات والمعرفة في مجال القرصنة الأخلاقية.

7-8-2 المبادئ العملية للقرصنة الأخلاقية

ان من اهم المبادئ العملية للقرصنة الأخلاقية هي:

1. **الحصول على الترخيص:** الحصول على الترخيص من أصحاب الأنظمة والشبكات قبل إجراء أي اختبار أمني.
2. **احترام الخصوصية:** احترام خصوصية الأفراد والمنظمات وتجنب الوصول إلى البيانات غير الضرورية.
3. **تجنب الأضرار:** تجنب الأضرار التي قد تنجم عن الاختبارات الأمنية.
4. **الاستخدام المسؤول للبيانات:** استخدام البيانات التي تم الحصول عليها خلال الاختبارات الأمنية بشكل مسؤول وآمن.
5. **التعاون مع الأطراف المعنية:** التعاون مع الأطراف المعنية، مثل أصحاب الأنظمة والشبكات، لضمان نجاح الاختبارات الأمنية.

7-9 حدود الاخلاقيات في عمليات اختبار الاختراق في الأمن السيبراني

هناك حدود اخلاقية وقانونية وفنية في عمليات اختبار الاختراق في الأمن السيبراني وفي التعامل مع البيانات يجب الالتزام بها بشكل دقيق، في هذا البند سنتاول اهم هذه الحدود.

7-9-1 الحدود الأخلاقية في عمليات اختبار الاختراق

هناك حدود الأخلاقية في عمليات اختبار الاختراق يجب الالتزام بها ومنها:

1. **احترام الخصوصية:** احترام خصوصية الأفراد والمنظمات وتجنب الوصول إلى البيانات غير الضرورية.

2. **تجنب الأضرار:** تجنب الأضرار التي قد تنجم عن الاختبارات الأمنية.
3. **الاستخدام المسؤول للبيانات:** استخدام البيانات التي تم الحصول عليها خلال الاختبارات الأمنية بشكل مسؤول وآمن.
4. **الالتزام بالقوانين:** الالتزام بالقوانين واللوائح المتعلقة بالاختبارات الأمنية.
5. **الحصول على الترخيص:** الحصول على الترخيص من أصحاب الأنظمة والشبكات قبل إجراء أي اختبار أمني.

7-9-2 الحدود القانونية في عمليات اختبار الاختراق

يجب ان يكون هناك حدود قانونية في عمليات اختبار الاختراق فمنها على سبيل المثال:

1. **الامتثال للقوانين:** الامتثال للقوانين واللوائح المتعلقة بالاختبارات الأمنية.
2. **تجنب الجرائم السيبرانية:** تجنب ارتكاب الجرائم السيبرانية، مثل القرصنة غير المصرح بها.
3. **الاحترام لحقوق الملكية الفكرية:** احترام حقوق الملكية الفكرية للآخرين.

7-9-3 الحدود الفنية في عمليات اختبار الاختراق

يجب ان لا ننسى ان هناك حدود فنية في عمليات اختبار الاختراق وعليه فاننا نؤكد على الاتي:

1. **تجنب التأثير على الأنظمة:** تجنب التأثير على الأنظمة والشبكات بطريقة قد تؤدي إلى توقفها أو تدهور أدائها.
2. **استخدام الأدوات بشكل مسؤول:** استخدام الأدوات والتقنيات بشكل مسؤول وآمن.
3. **تجنب الوصول غير المصرح به:** تجنب الوصول غير المصرح به إلى البيانات والأنظمة.

7-9-4 الحدود الأخلاقية المتعلقة بالتعامل مع البيانات

ان من هناك الحدود الاخلاقية في عمليات اختبار الاختراق عند التعامل مع البيانات، نورد منها:

1. **حماية البيانات:** حماية البيانات التي تم الحصول عليها خلال الاختبارات الأمنية.
2. **استخدام البيانات بشكل مسؤول:** استخدام البيانات التي تم الحصول عليها خلال الاختبارات الأمنية بشكل مسؤول وآمن.
3. **تجنب نشر البيانات:** تجنب نشر البيانات التي تم الحصول عليها خلال الاختبارات الأمنية دون إذن.

هذه الحدود الأخلاقية والقانونية والفنية تلعب دورًا هامًا في ضمان أن تكون عمليات اختبار الاختراق في الأمن السيبراني ممارسة أمنية مشروعة ومسؤولة.

10-7 التحديات الأخلاقية المستقبلية المرتبطة بالتحول الرقمي والأتمتة

هناك الكثير من التحديات الأخلاقية المستقبلية والتي ترتبط بالتطورات الحديثة مثل التحول الرقمي والذكاء الاصطناعي والأتمتة والحوكمة، في هذ البند سيتم مناقشة تلك التحديات.

1-10-7 التحديات الأخلاقية المتعلقة بالتحول الرقمي

ان من اهم التحديات الاخلاقية المتعلقة بالتحول الرقمي هي:

1. **الخصوصية:** حماية خصوصية الأفراد والمنظمات في ظل التحول الرقمي.
2. **الأمان السيبراني:** ضمان أمان البيانات والأنظمة والشبكات في ظل التهديدات السيبرانية المتزايدة.
3. **العدالة والمساواة:** ضمان العدالة والمساواة في استخدام التكنولوجيا والتحول الرقمي.
4. **الشفافية:** ضمان الشفافية في استخدام التكنولوجيا والتحول الرقمي.
5. **المسؤولية:** تحديد المسؤولية عن الأخطاء والعيوب في أنظمة التحول الرقمي.

2-10-7 التحديات الأخلاقية المتعلقة بالذكاء الاصطناعي

فيما يخص التحديات الاخلاقية المتعلقة بالذكاء الاصطناعي نورد الاتي:

1. **الانحياز:** تجنب الانحياز في الذكاء الاصطناعي والأنظمة الأتمتة.
2. **الشفافية في اتخاذ القرارات:** ضمان الشفافية في اتخاذ القرارات من قبل الذكاء الاصطناعي.
3. **المسؤولية عن الأخطاء:** تحديد المسؤولية عن الأخطاء التي ترتكبها الأنظمة الذكية.
4. **الاستخدام الأخلاقي للبيانات:** استخدام البيانات بشكل أخلاقي في استخدام الذكاء الاصطناعي.

3-10-7 التحديات الأخلاقية المتعلقة بالأتمتة

الأتمتة هي استخدام التكنولوجيا والأنظمة الآلية لتنفيذ المهام والعمليات بشكل تلقائي دون الحاجة إلى تدخل بشري مباشر فلذلك فان الأتمتة يمكن أن تشمل مجموعة واسعة من التطبيقات. ان من اهم التحديات الأخلاقية المتعلقة بالأتمتة هي:

1. **تأثير الأتمتة على العمالة:** تأثير الأتمتة على العمالة والتوظيف.
2. **العدالة في توزيع الفوائد:** ضمان العدالة في توزيع الفوائد الناتجة عن الأتمتة.
3. **المسؤولية عن الأخطاء:** تحديد المسؤولية عن الأخطاء التي ترتكبها الأنظمة الأتمتة.
4. **الاستخدام الأخلاقي للتكنولوجيا:** استخدام التكنولوجيا بشكل أخلاقي في الأتمتة.
5. **الأمان السيبراني:** ضمان أمان الأنظمة الأتمتة من التهديدات السيبرانية.
6. **الاستخدام المستدام للأتمتة:** استخدام الأتمتة بشكل مستدام ومسؤول.

هذه التحديات الأخلاقية المتعلقة بالأتمتة تتطلب من الأفراد والمنظمات والهيئات الحكومية العمل معًا لضمان استخدام الأتمتة بشكل مسؤول وأخلاقي.

7-10-4 التحديات الأخلاقية المتعلقة بالبيانات

ان استخدام البيانات اها خصوصية عالية، وعليه فان اهم التحديات الاخلاقية المتعلقة بالبيانات هي:

1. **حماية البيانات:** حماية البيانات من الوصول غير المصرح به والاستخدام غير المصرح به.
2. **الاستخدام الأخلاقي للبيانات:** استخدام البيانات بشكل أخلاقي ومسؤول.
3. **الشفافية في استخدام البيانات:** ضمان الشفافية والمهنية في استخدام البيانات.
4. **العدالة في توزيع الفوائد:** ضمان العدالة في توزيع الفوائد الناتجة عن استخدام البيانات.

هذه التحديات الأخلاقية المستقبلية المرتبطة بالتحول الرقمي والأتمتة تتطلب من الأفراد والمنظمات والهيئات الحكومية العمل معًا لضمان استخدام التكنولوجيا بشكل مسؤول وأخلاقي.

7-10-5 التحديات الأخلاقية المتعلقة بالحوكمة

ان من اهم التحديات الاخلاقية المتعلقة بالحوكمة هي:

1. **الحوكمة الرقمية:** تطوير الحوكمة الرقمية الفاعلة والشفافة.
2. **الامتثال للقوانين:** الامتثال للقوانين واللوائح المتعلقة بالتحول بالحوكمة.
3. **المسؤولية عن القرارات:** تحديد المسؤولية عن القرارات المتعلقة بالحوكمة.
4. **الشفافية في اتخاذ القرارات:** ضمان الشفافية في اتخاذ القرارات المتعلقة بالحوكمة.

اسئلة الفصل السابع

س1 / ما هو مفهوم الاخلاقيات والسياسات في الأمن السيبراني ؟

س2 / ما هي أهمية الاخلاقيات والسياسات في الأمن السيبراني ؟

س3 / عدد انواع التحديات الأخلاقية المرتبطة بالمراقبة الإلكترونية وأشرح واحدة منها ؟

س4 / ما هو المقصود بالقرصنة الأخلاقية وضح ذلك ؟

س5 / ما هو المقصود بالقرصنة الخبيثة وضح ذلك ؟

س6 / ما هو الفرق بين القرصنة الأخلاقية والقرصنة الخبيثة ؟

س7 / ما هو المقصود بالتحديات الأخلاقية المستقبلية المرتبطة بالتحول الرقمي والأتمتة عددها بالتفصيل ؟

1. National Institute of Standards and Technology (NIST)

2. Cybersecurity and Infrastructure Security Agency (CISA)

3. European Union Agency for Cybersecurity (ENISA)

4. أمن المعلومات – الدكتور ذياب بن عايض القحطاني / المملكة العربية السعودية/ جامعة الملك عبد العزيز للعلوم والتقنية KACST / 2015

5. Audun Jøsang, Identity management and trusted interaction in Internet and mobile computing, IET Inf. Secur., 2014, Vol. 8, Iss. 2, pp. 67–79 doi:10.1049/iet-ifs.2012.0133.

6. Güneş Acar, Brendan Van Alsenoy, Frank Piessens, Claudia Diaz, Bart Preneel, Facebook Tracking Through Social Plug-ins, Technical report prepared for the Belgian Privacy Commission, 24June2015.

7. Smith, D. F., Wiliem, A., & Lovell, B. C. (2015). Face Recognition on Consumer Devices: Reflections on Replay Attacks. IEEE Transactions on Information Forensics and Security, 10(4), 736–745. doi:10.1109/tifs.2015.2398819 .

8. "Computer Security: Principles and Practice" by William Stallings

9. "Artificial Intelligence in Cybersecurity" by Leslie F. Sikos

10. Securing the Internet of Things" by Shancang Li and Li Da Xu