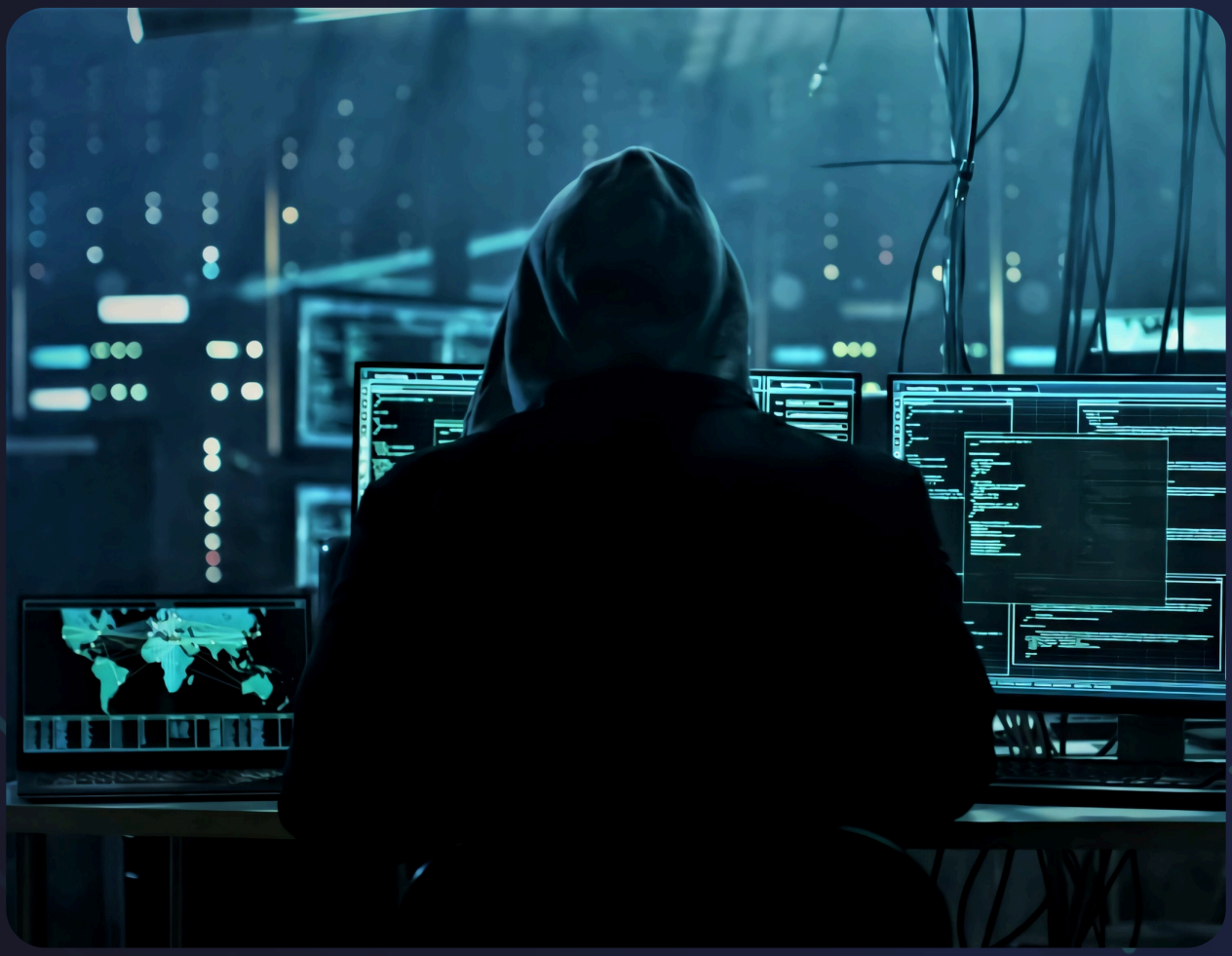
كيف تكون آمنًا في العالم الرقمي؟



إعداد
محمد آل مشوط

الفهرس

كيف تكون آمنًا في العالم الرقمي؟

يُعد الأمن السيبراني من أهم التخصصات الحديثة التي تشكّل حجر الأساس في الحفاظ على استقرار المجتمعات الرقمية. ومع تطور تقنيات المعلومات وتوسع البنية التحتية الرقمية في جميع القطاعات، برزت الحاجة إلى تعزيز الوعي بالأمن السيبراني ليس فقط في الأوساط التقنية، بل أيضًا لدى المستخدم العادي الذي بات جزءًا فعّالًا في سلسلة الأمان المعلوماتي.

تسعى هذه المادة إلى تبسيط مفاهيم الأمن السيبراني، وشرح مبادئه الأساسية بلغة ميسّرة تناسب القارئ العام، دون الإخلال بجوهر المفاهيم العلمية. وقد تم توجيه هذا العمل ليمثّل جسرًا معرفيًا بين الفهم الأكاديمي المتخصص، ومتطلبات التوعية المجتمعية، من خلال ربط المفاهيم النظرية بتطبيقات واقعية، وسيناريوهات يومية تعكس طبيعة التهديدات الرقمية التي قد يتعرض لها أي فرد.

إن بناء ثقافة أمنية رقمية يبدأ من الوعي، ويترسخ بالممارسة. ومن هذا المنطلق، يأتي هذا الكتاب ليكون أداة توعوية قابلة للتطبيق، تفتح باب الفهم، وتدعو إلى التحصين الرقمي.

🛡️ الفصل الأول: ما هو الأمن السيبراني؟

1.1 تعريف الأمن السيبراني

يُعرَّف الأمن السيبراني (Cybersecurity) بأنه مجموعة من العمليات، والممارسات، والتقنيات المصممة لحماية الأنظمة، والشبكات، والبرمجيات، والبيانات من الهجمات الرقمية. وتشمل هذه الحماية كل ما يتعلق باستخدام التقنية، من الأجهزة الشخصية إلى قواعد البيانات المؤسسية، مرورًا بالشبكات والبنية التحتية للإنترنت.

بصورة مبسطة، الأمن السيبراني يعني "الحماية الرقمية"، تمامًا كما تحمي بيتك بأقفال وكاميرات، فإنك تحمي أجهزتك وحساباتك وبرامجك من الاختراقات والتهديدات السيبرانية.

1.2 أهمية الأمن السيبراني

في العصر الحالي، يعتمد الأفراد والمؤسسات بشكل كبير على التقنية في أداء مهامهم اليومية. من التواصل الشخصي إلى المعاملات البنكية، ومن التعليم الإلكتروني إلى إدارة المصانع، أصبحت التقنية جزءًا لا يتجزأ من كل شيء. ومع هذا الاعتماد الكبير، تزداد قيمة وأهمية المعلومات الرقمية، وبالتالي تصبح هدفًا مغريًا للمهاجمين.

تشير التقارير الحديثة إلى أن معظم الهجمات الإلكترونية لا تستهدف فقط الجهات الحكومية أو الشركات الكبرى، بل تمتد إلى الأفراد، والمؤسسات الصغيرة، وحتى الأجهزة المنزلية الذكية. وهذا ما يفرض على الجميع، دون استثناء، الوعي بأساسيات الأمن السيبراني، وفهم طبيعة التهديدات الرقمية.

1.3 ما الذي يحميه الأمن السيبراني؟

يقوم الأمن السيبراني بحماية عدة مستويات، تشمل:

- **البيانات الشخصية :**مثل الصور، المستندات، المعلومات البنكية، والعناوين.
- **الحسابات الرقمية :**كالبريد الإلكتروني، حسابات وسائل التواصل الاجتماعي، والحسابات البنكية.
- **الأجهزة :**مثل الهواتف، الحواسيب، وأجهزة الشبكة من البرمجيات الخبيثة والتطبيقات الضارة.
- **الخصوصية الرقمية :**من التتبع، أو الاستخدام غير المصرح به للمعلومات، أو التسلل عبر تطبيقات التواصل.

1.4 من هم المهاجمون السيبرانيون؟

تتنوع الجهات التي قد تشن هجمات إلكترونية، ويمكن تصنيفها كما يلي:

- **هاكرز أفراد :**وهم أشخاص يمتلكون مهارات تقنية، يقومون بالاختراق إما بدافع الشهرة أو التحدي أو المكاسب المادية.
- **مجرمو الإنترنت (Cybercriminals) :** يعملون ضمن شبكات منظمة، ويهدفون إلى سرقة البيانات، أو الابتزاز، أو النصب المالي.
- **جهات مدعومة من دول :**تقوم ببعض الهجمات لأغراض تجسسية أو سياسية أو اقتصادية.
- **برمجيات خبيثة (Malware) :** قد لا يكون المهاجم بشريًا مباشرًا، بل كود برمجي يعمل في الخلفية بدون علم المستخدم، مصمم لأداء مهمة محددة مثل التجسس أو التدمير أو السرقة.

من المهم إدراك أن التهديد قد لا يبدو دائمًا خطرًا واضحًا. أحيانًا يكون مجرد رسالة بريد إلكتروني مزيفة، أو تطبيق يبدو رسميًا لكنه يحتوي برمجية خبيثة، أو حتى رابط بسيط تم تمريره عبر محادثة.

1.5 هل الأمن السيبراني أمر معقّد؟

الانطباع السائد أن الأمن السيبراني يتطلب معرفة تقنية متقدمة، وهذا صحيح إلى حد ما على المستوى المهني، لكن على المستوى الشخصي، يمكن القول إن **الوعي** و**اتباع بعض الإجراءات البسيطة** كفيل بتوفير حماية فعالة في ٨٠٪ إلى ٩٠٪ من الحالات.

ومن أبرز الممارسات التي تُمكن الفرد من تجنب معظم التهديدات:

- استخدام كلمات مرور قوية وغير مكررة.
- التحقق الثنائي.(Two-Factor Authentication)
- عدم الضغط على الروابط المشبوهة.
- تحديث البرامج بشكل مستمر.
- تحميل التطبيقات من مصادر موثوقة فقط.

1.6 قصة واقعية: "أحمد" والرسالة الوهمية

أحمد موظف بسيط في شركة متوسطة. استلم يومًا ما رسالة بريد إلكتروني تخبره بأن حسابه البنكي سيُغلق خلال ٢٤ ساعة إن لم يحدث بياناته. الرابط في الرسالة

بدا مطابقًا تمامًا لموقع البنك، فدخل عليه وكتب كل شيء. بعد ساعة، تم سحب مبلغ كبير من حسابه.

هذه القصة، التي تحدث بشكل يومي لآلاف المستخدمين، توضح كيف يمكن لثغرة بسيطة في الوعي، أن تؤدي إلى خسائر كبيرة. والمشكلة ليست في أحمد فقط، بل في غياب الثقافة الأمنية الرقمية لدى كثير من الناس.

1.7 خلاصة الفصل الأول

الأمن السيبراني لم يعد رفاهية، ولا تخصصًا محصورًا بالخبراء. بل هو ضرورة يومية لكل من يستخدم جهازًا متصلاً بالإنترنت. فهم أساسياته، واتباع ممارسات بسيطة، كفيلان بتقليل المخاطر بشكل كبير. ومن هنا تنطلق أهمية هذا الكتاب: أن يكون نقطة البداية نحو وعي رقمي حقيقي.

📌 ملخص الفصل الأول (نقاط سريعة)

- الأمن السيبراني يعني حماية الأجهزة والبيانات من الهجمات الرقمية.
- يشمل حماية الحسابات، الملفات، الخصوصية، وأجهزة الاتصال.
- التهديدات السيبرانية قد تأتي من أفراد، أو برمجيات، أو حتى جهات مدعومة.
- المستخدم العادي معرض للاختراق مثل المؤسسات تمامًا.
- الوعي والإجراءات البسيطة مثل كلمات السر القوية وتجنب الروابط المشبوهة تحميك كثيرًا.

✅ أسئلة تقييم ذاتي (اختبر نفسك)

١. ما المقصود بالأمن السيبراني؟ وهل هو مسؤولية المتخصصين فقط؟

٢. اذكر ثلاثة أشياء رئيسية يحميها الأمن السيبراني في حياتك اليومية.

٣. من هم المهاجمون الرقميون؟ وهل يمكن أن يكون التهديد غير ظاهر؟

٤. هل تعتقد أنك قد تتعرض لهجوم سيبراني؟ ولماذا؟

٥. ما الخطوة الأولى التي ستقوم بها اليوم لتحسين أمنك الرقمي؟

⚠️ الفصل الثاني: التهديدات السيبرانية الشائعة

2.1 مقدمة

لفهم الأمن السيبراني بشكل واقعي، لا بد من الإلمام بأنواع التهديدات الرقمية التي قد تواجه المستخدم في حياته اليومية. فالمعرفة المسبقة بالطرق التي يستخدمها المهاجمون تساعد في كشفها مبكرًا واتخاذ الاحتياطات اللازمة.
رغم تنوع التهديدات وتطورها المستمر، إلا أن هناك أنماطًا متكررة تُعد الأكثر شيوعًا، وسنستعرض هنا أبرزها بلغة واضحة وأمثلة واقعية.

2.2 التصيّد الإلكتروني(Phishing)

التصيّد هو أحد أكثر أنواع الهجمات شيوعًا وخطورة، ويعتمد على **خداع المستخدم** لإقناعه بإدخال معلومات حساسة في موقع مزيف أو الرد على رسالة احتيالية.

🧪 كيف يتم؟

- تصل للمستخدم رسالة بريد إلكتروني، أو رسالة واتساب، أو حتى رسالة SMS، تدّعي أنها من جهة موثوقة مثل البنك أو البريد.
- تحتوي الرسالة على تحذير أو إغراء، مثل:

"تم تعليق حسابك البنكي لأسباب أمنية، اضغط هنا لتحديث بياناتك".

- الرابط المرفق يقود إلى صفحة مزيفة تحاكي الموقع الرسمي.

👷 قصة حقيقية:

أحد الموظفين في قطاع حكومي تلقى بريدًا يحمل شعار الجهة الرسمية، وطلب منه تسجيل الدخول للتحقق من معلوماته. بعد الضغط وإدخال بياناته، استُخدمت تلك المعلومات لاحقًا للوصول إلى أنظمة داخلية.

🔑 نصيحة أمنية:

لا تضغط على أي رابط يصلك فجأة، خاصة إذا احتوى على طلب عاجل أو تحذير.
تحقق من عنوان الموقع جيدًا، ويفضّل الدخول للموقع الرسمي يدويًا بدلاً من استخدام الرابط.

2.3 🦠 الفيروسات والبرمجيات الخبيثة(Malware)

تشير البرمجيات الخبيثة إلى أي برنامج ضار يُثبّت على الجهاز دون إذن المستخدم، بهدف التجسس، السرقة، التخريب، أو حتى السيطرة الكاملة.

💻 كيف تنتشر؟

- تحميل برنامج "مجاني" من موقع غير موثوق.
- فتح مرفق في بريد إلكتروني مشبوه.
- زيارة موقع مزيف فيه كود خبيث.

👨‍💻 سيناريو محتمل:

شخص يبحث عن برنامج لتحويل ملفات PDF إلىWord ، فحمّل أداة غير رسمية. دون علمه، احتوت على فيروس راصد للوحة المفاتيح (Keylogger) سجّل بيانات دخوله البنكية.

🔑 نصيحة أمنية:

حمّل البرامج فقط من المواقع الرسمية أو متاجر التطبيقات المعتمدة، ولا تفتح أي ملف مرفق إلا إذا كنت متأكدًا من مصدره.

2.4 الهندسة الاجتماعية(Social Engineering)

الهندسة الاجتماعية تعتمد على خداعك نفسيًا، وليس تقنيًا.
الهاكر لا يحتاج كسر أنظمة حماية معقدة، بل يخدعك لتسلمه أنت المعلومات.

🎭 كيف تحدث؟

- يتصل شخص ويدّعي أنه من الدعم الفني، ويطلب منك مشاركة رمز الدخول.
- يرسل لك شخص رسالة ودية فيها أسئلة شخصية (اسم الأم، أول مدرسة... إلخ)، وقد يستخدمها لاختراق حسابك.

👨‍💻 موقف شائع:

تم اختراق حساب أحد الموظفين بعد أن تواصل معه شخص يدّعي أنه من "قسم تقنية المعلومات"، وأقنعه بإعطائه كود التحقق لإصلاح "مشكلة أمنية."

🔑 **نصيحة أمنية:**
لا تعطِ أي معلومة لأي جهة أو شخص يطلبها بشكل غير رسمي. الجهة الحقيقية لن تطلب منك كلمات السر أو الأكواد بهذه الطريقة.

2.5 كلمات المرور الضعيفة

تشير الإحصائيات إلى أن أكثر من ٨٠٪ من الاختراقات ناتجة عن استخدام كلمات مرور ضعيفة أو مكررة.
كلمة سر مثل 123456، qwerty، أو passwordيمكن تخمينها خلال ثوانٍ.

🚨 **المخاطر:**

- إذا استخدمت نفس الكلمة في أكثر من حساب، فاختراق واحد يكشف البقية.
- كلمات السر القصيرة أو الواضحة يمكن تخمينها ببرمجيات تلقائية (Brute Force).

🔑 **نصيحة أمنية:**
استخدم جملة سرية طويلة ومعقدة تحتوي على حروف كبيرة وصغيرة، أرقام، ورموز، مثلMyC0ffee@Bisha2025 :، وغيّرها دوريًا.

📌 **ملخص الفصل الثاني (نقاط سريعة)**

- التهديدات الرقمية تتنوع، وأبرزها: التصيد، الفيروسات، الهندسة الاجتماعية، وكلمات المرور الضعيفة.
- التصيد يعتمد على الخداع، وغالبًا ما يكون عبر البريد الإلكتروني أو الرسائل.
- البرمجيات الخبيثة تدخل الجهاز غالبًا عبر التحميل أو المرفقات.
- الهندسة الاجتماعية تعتمد على استغلال الثقة للحصول على المعلومات.
- كلمات المرور القوية والمتجددة ضرورة لا خيار.

✅ **أسئلة تقييم ذاتي**

١. ما الفرق بين التصيد الإلكتروني والهندسة الاجتماعية؟

٢. ما هي العلامات التي تجعلك تشك في رسالة بريد إلكتروني؟

٣. ما نوع كلمة المرور التي تستخدمها حاليًا؟ وهل كررتها في أكثر من حساب؟

٤. هل سبق وأن طلب أحد منك معلومة شخصية بشكل مفاجئ؟ كيف تصرّفت؟

٥. ما الإجراءات التي يمكن أن تتخذها اليوم لتقليل فرص الإصابة بالبرمجيات الخبيثة؟

🔐 الفصل الثالث: كيف تحمي نفسك من التهديدات السيبرانية؟

3.1 مقدمة

الوقاية السيبرانية لا تتطلب أن تكون خبيرًا في الحماية الرقمية أو مبرمجًا محترفًا.
بل إن معظم التهديدات الأمنية يمكن تجنّبها عبر **اتباع ممارسات بسيطة** و**التحلي بقدر من الوعي التقني**.
في هذا الفصل، نستعرض الإجراءات الأساسية التي تُعدّ بمثابة "خط الدفاع الأول" لكل مستخدم يريد حماية نفسه وأجهزته ومعلوماته.

3.2 استخدام كلمات مرور قوية

كلمة المرور (Password) هي المفتاح الذي يمنح الوصول إلى حساباتك، وأي ضعف فيها يُعد ثغرة مباشرة.

✅ **خصائص الكلمة القوية:**

- لا تقل عن 12 رمزًا.
- تحتوي على مزيج من الحروف الكبيرة والصغيرة، الأرقام، والرموز.
- لا تعتمد على معلومات شخصية مثل تاريخ الميلاد أو اسم العائلة.
- لا تُستخدم نفسها في أكثر من موقع.

🧪 **مثال:**

كلمة مرور مثل 3bIsha$Coffee2025 أقوى بكثير من كلمة مثل bisha123.

🔑 **نصيحة** : استخدم مدير كلمات مرور (Password Manager) لتوليد كلمات قوية وتخزينها بأمان، مثل Bitwarden أو Password.1

3.3 تفعيل التحقق بخطوتين(Two-Factor Authentication)

التحقق بخطوتين يُضيف طبقة أمان إضافية، بحيث لا يكفي أن يعرف المهاجم كلمة السر فقط، بل يحتاج أيضًا إلى كود مؤقت يصل إلى جهازك.

🧪 **كيف يعمل؟**

1. تسجل دخولك باسم المستخدم وكلمة المرور.
2. تصلك رسالة SMS أو إشعار من تطبيق مصادقة مثل Google Authenticator.
3. تدخل الرمز، فيتم التحقق من هويتك.

✋ **بدون الخطوة الثانية:**

حتى لو تم تسريب كلمة مرورك، يبقى حسابك مؤمن.

🔑 **نصيحة :**فعّل هذه الخاصية في كل حساب يدعمها، خصوصًا البريد الإلكتروني، حسابات السوشال ميديا، والبنوك.

3.4 تحديث الأنظمة والتطبيقات بانتظام

الكثير من التهديدات تعتمد على ثغرات في الأنظمة لم يتم إصلاحها بعد. التحديثات غالبًا ما تحتوي على "تصحيحات أمنية" تسد هذه الثغرات.

🧪 **مثال:**

في 2017، استغل فيروس WannaCry ثغرة في أنظمة ويندوز لم يتم تحديثها، وتسبب بخسائر عالمية رغم وجود تحديث رسمي قبل الهجمة بشهرين.

🔑 **نصيحة:**

- فعّل التحديث التلقائي في نظام التشغيل والتطبيقات.
- لا تؤجل التحديثات تحت أي مبرر.

3.5 الحذر من الروابط والمرفقات

غالبًا ما تبدأ الهجمات برسالة بسيطة فيها رابط مغري أو مرفق ملف، وبمجرد التفاعل معه، يتم تحميل برمجية خبيثة أو سرقة بياناتك.

🧪 **مثال شائع:**

"مبروك! ربحت جوال آيفون. اضغط هنا لاستلام الجائزة".

أو

"نرجو مراجعة الفاتورة المرفقة".

وفي الواقع، الرابط يُوجّهك لموقع مزيف أو المرفق يحتوي على فيروس.

🔑 **نصيحة:**

- لا تفتح أي رابط أو ملف غير متوقع، خصوصًا إذا أتى من جهة غير معروفة.
- تحقق من عنوان الموقع جيدًا — (URL) أحيانًا الفرق يكون حرفًا واحدًا فقط.

3.6 مراجعة التطبيقات المثبتة والصلاحيات

بعض التطبيقات – خصوصًا المجانية وغير الرسمية – تطلب صلاحيات لا علاقة لها بوظيفتها.

🧪 **مثال:**

تطبيق "كشاف ضوء" يطلب إذن الوصول للكاميرا والمايك وجهات الاتصال.
ليش؟ لأنه غالبًا يجمع بياناتك أو يسجل بدون علمك.

🔑 **نصيحة:**

- احذف أي تطبيق لا تستخدمه.
- راجع الصلاحيات الممنوحة لتطبيقاتك من إعدادات الجهاز.
- استخدم التطبيقات الرسمية من المتاجر المعتمدة فقط.

3.7 تعزيز الوعي الأمني

الوعي هو الحصن الأقوى ضد الهجمات الإلكترونية.
معرفة كيف يفكر المهاجم، وكيف يُخدع المستخدمون، يجعلك أكثر يقظة وقدرة على التصرف.

🧪 كيف تطوّر وعيك؟

- تابع الأخبار التقنية.
- اشترك في دورات توعوية مجانية.
- راقب التحديثات الأمنية في المواقع الرسمية للحلول التي تستخدمها.
- تعلم من تجارب الآخرين.

🔑 نصيحة:
أي موقف مشبوه، خذه بجدية. وتذكّر: الوقاية دائمًا أسهل من الاستجابة بعد الاختراق.

📌 ملخص الفصل الثالث (نقاط سريعة)

- استخدم كلمات مرور قوية وفريدة لكل حساب.
- فعّل التحقق الثنائي أينما أمكن.
- لا تؤجل التحديثات — فهي درعك ضد الثغرات.
- لا تثق بالروابط والمرفقات المشبوهة.
- راقب التطبيقات والصلاحيات في جهازك.
- خلك واعي، وتعلم من حولك.

✅ أسئلة تقييم ذاتي

1. هل تعتقد أن كلمة مرورك الحالية قوية كفاية؟ ما الذي يمكنك تحسينه؟
2. كم حساب عندك مفعّل فيه التحقق بخطوتين؟

3. متى كانت آخر مرة حدثت فيها نظام جهازك أو برامجك؟
4. هل فتحت يومًا رابطًا غير متأكد منه؟ كيف تصرفت؟
5. هل تراجع صلاحيات التطبيقات في جوالك؟ ولماذا هو أمر مهم؟

🏢 .الفصل الرابع: الأمن السيبراني في بيئة العمل

4.1 مقدمة

لم تعد بيئة العمل اليوم تعتمد على الملفات الورقية أو المعاملات التقليدية فقط، بل أصبحت **البيئة الرقمية** محورًا رئيسيًا لإدارة الأنشطة المؤسسية اليومية: من البريد الإلكتروني إلى التخزين السحابي، ومن الاجتماعات الافتراضية إلى أنظمة تخطيط الموارد.

هذا الاعتماد الكبير على التكنولوجيا يجعل **أي ضعف بسيط في إجراءات الأمان** مدخلًا محتملاً لهجوم سيبراني قد يؤدي إلى خسائر مالية وتشغيلية وسمعة مؤسسية.

ولهذا، فإن تطبيق ممارسات الأمن السيبراني في بيئة العمل لم يعد خيارًا، بل هو جزء لا يتجزأ من استراتيجيات الحوكمة الحديثة.

4.2 💻 التحقق من الرسائل الإلكترونية والروابط

تشير الدراسات إلى أن أكثر من 90٪ من الهجمات السيبرانية الناجحة تبدأ برسالة بريد إلكتروني احتيالية.(Phishing Email)

🧪 مثال تطبيقي:

أحد موظفي قسم المحاسبة استقبل رسالة تبدو وكأنها من المدير المالي تطلب تحويل مبلغ مستعجل إلى حساب خارجي. المرفق المصاحب احتوى على فايروس سمح للمهاجم بالدخول إلى نظام الفوترة.

🔑 نصيحة مهنية:

- لا تفتح أي رابط أو مرفق قبل التحقق من هوية المرسل.
- استخدم خاصية "عرض العنوان الكامل" للبريد.
- تواصل مباشرة مع صاحب الرسالة إذا كان الطلب غير متوقع.

4.3 📱 حماية الأجهزة المحمولة

أصبح الهاتف المحمول أداة أساسية في أداء المهام المؤسسية، من التوقيع على العقود، إلى الوصول لبيانات العملاء.

مخاطر استخدام الجوال في العمل:

- استخدام شبكات Wi-Fi عامة.
- تثبيت تطبيقات غير مصرح بها.
- فقدان الجهاز بدون حماية.

🔑 توصيات عملية:

- فعّل قفل الشاشة بكلمة سر أو بصمة.
- لا تستخدم الشبكات العامة إلا مع VPN موثوق.
- لا تخزن كلمات السر أو ملفات حساسة في تطبيقات غير مشفرة.

4.4 🔐 مبدأ الحد الأدنى من الصلاحيات(Least Privilege Principle)

واحدة من أبرز أسباب الاختراق الداخلي هو منح صلاحيات مفرطة لموظفين ليسوا بحاجة لها.

🧪 سيناريو حقيقي:

موظف في قسم الدعم الفني كان لديه صلاحية الوصول إلى قاعدة بيانات العملاء، وتم تسريب البيانات بسبب فيروس على جهازه، رغم أنه لم يكن من مهامه استخدام تلك البيانات.

🔑 نصيحة تنظيمية:

- حدد صلاحيات كل موظف بناءً على مهامه الفعلية.
- استخدم أنظمة تحكم في الوصول.(Access Control)
- راجع الصلاحيات بانتظام، وعطّل الحسابات غير النشطة أو المنتهية.

4.5 📚 التوعية الأمنية المستمرة

أغلب الاختراقات المؤسسية سببها "خطأ بشري."
قد تكون المنظمة مجهزة بأفضل الأنظمة، لكن موظفًا غير مدرّب يمكن أن يفتح الباب للمخترق.

برامج التوعية تشمل:

- نشرات أسبوعية.
- دورات إلكترونية.
- اختبارات تصيّد وهمي.
- ورش عمل تطبيقية.

🔑 نصيحة إدارية:
اجعل من الأمن السيبراني ثقافة مؤسسية، وليس مجرد سياسة مكتوبة.

4.6 🗂️ تخزين البيانات بشكل آمن

البيانات هي أحد أعظم أصول المؤسسات.
فقدانها، أو تسريبها، أو التلاعب بها، قد يؤدي إلى تبعات قانونية ومالية كبيرة.

🔐 أساليب الحماية:

- استخدام حلول تخزين سحابية معتمدة وموثوقة) مثل Google Workspace، Microsoft 365).
- تفعيل التشفير (Encryption) لكل البيانات أثناء النقل والتخزين.
- إجراء نسخ احتياطية دورية، وتخزينها في مواقع متعددة.

📌 ملخص الفصل الرابع (نقاط سريعة)

- البريد الإلكتروني هو أكثر وسيلة تُستخدم في الهجمات المؤسسية.
- الهواتف المحمولة المستخدمة للعمل يجب تأمينها جيدًا.

- الصلاحيات يجب أن تُمنح حسب المهام، لا بالأقدمية أو الثقة فقط.
- التدريب والتوعية السيبرانية يجب أن تكون مستمرة.
- حماية البيانات تتطلب تشفيرها، وتخزينها بشكل احترافي، وأخذ نسخ احتياطية.

✅ **أسئلة تقييم ذاتي**

1. هل تتأكد دائمًا من مصدر الرسائل قبل فتح الروابط أو المرفقات؟
2. هل تستخدم جهازك المحمول في العمل؟ وهل قمت بتأمينه بشكل كافٍ؟
3. هل تمتلك صلاحيات في نظام العمل أكثر مما تحتاج؟ لماذا؟
4. متى آخر مرة خضعت فيها لتدريب على الأمن السيبراني؟
5. هل تعلم أين تُخزن بيانات عملك؟ وهل يتم تشفيرها وأخذ نسخ احتياطية لها؟

🧰 .الفصل الخامس: أدوات تساعدك في حماية نفسك

5.1 مقدمة

لا يتطلب الحفاظ على الأمن السيبراني معرفة متقدمة بالتقنية، بل إن توفر بعض **الأدوات البسيطة** قد يحدث فرقًا كبيرًا في حمايتك.
تعمل هذه الأدوات كـ"مساعد ذكي" يوفر الحماية، ويمنحك مستوىً إضافيًا من الأمان عند استخدامك للإنترنت سواء في محيط العمل أو المنزل.

في هذا الفصل نستعرض أهم الأدوات الأساسية التي يجب على كل مستخدم معرفتها وتفعيلها.

5.2 🛡️ برامج مكافحة الفيروسات(Antivirus Software)

تُعد برامج مكافحة الفيروسات خط الدفاع الأول ضد البرمجيات الخبيثة، الفيروسات، برامج التجسس(Spyware) ، وأحصنة طروادة.(Trojans)
تعمل هذه البرامج على فحص الملفات والبرامج والروابط قبل أن تُفتح، وتنبه المستخدم في حال وجود تهديد.

🧪 **ميزاتها:**

- فحص دوري للجهاز.
- اكتشاف التهديدات في الوقت الفعلي.(Real-Time Protection)
- حظر المواقع الضارة.
- إزالة التهديدات تلقائيًا.

🧩 **برامج موصى بها:**

- Windows Defender مدمج ومجاني في نظام ويندوز، ويقدّم حماية جيدة.
- Avast / AVG مجانية وسهلة الاستخدام
- Kaspersky / Bitdefender مدفوعة، لكنها عالية الكفاءة في الحماية المتقدمة.

🔑 **نصيحة** :تأكد أن البرنامج محدث تلقائيًا، ويعمل في الخلفية دون انقطاع.

5.3 🔐 مدير كلمات المرور(Password Manager)

كثرة الحسابات تجعل المستخدمين يميلون لإعادة استخدام نفس كلمة السر، وهذا خطر كبير.
مديرو كلمات المرور يحلون هذه المشكلة بتخزين كلمات المرور وتوليد كلمات قوية لك، دون الحاجة لحفظها كلها.

🧪 **الميزات:**

- توليد كلمات مرور معقدة تلقائيًا.
- تشفير البيانات باستخدام خوارزميات متقدمة.
- تعبئة تلقائية (Auto-fill) للمواقع والتطبيقات.
- مزامنة بين الأجهزة المختلفة.

🧩 **أدوات موصى بها:**

- Bitwarden (مجاني ومفتوح المصدر.)
- 1Password (مدفوع، عالي الأمان.)
- LastPass (سهل الاستخدام، بخطة مجانية ومدفوعة.)

🔑 **نصيحة** :لا تحفظ كلمات مرورك في المتصفح، واستخدم مدير كلمات موثوق وآمن.

5.4 🌐 الشبكة الخاصة الافتراضية(VPN)

الـ VPN يقوم بتشفير اتصالك بالإنترنت، وإخفاء عنوان IP الحقيقي الخاص بك.
يُستخدم لحماية الخصوصية خاصة عند الاتصال بشبكات Wi-Fi عامة أو غير موثوقة.

🧪 **فوائد استخدام VPN :**

- حماية بياناتك من التجسس في الشبكات العامة.
- إخفاء موقعك الحقيقي.
- الوصول الآمن إلى بيانات العمل عن بُعد.
- تقليل تتبع المواقع لك لأغراض الإعلانات.

🧩 **مزوّدو خدمة موثوقون:**

- **NordVPN**
- **ExpressVPN**
- **Surfshark**

🔑 **نصيحة** :تجنب استخدام خدمات VPN مجانية غير معروفة، لأنها قد تبيع بياناتك أو تفتقر للحماية الكافية.

5.5 🔍 أدوات فحص الروابط

في حال وصلك رابط مشبوه، يمكنك التحقق من سلامته قبل الضغط عليه باستخدام أدوات فحص الروابط.

🧪 **طريقة الاستخدام:**

- انسخ الرابط (دون فتحه).
- أدخله في أحد المواقع المتخصصة، وسيُعطيك تقريرًا عن مدى أمانه.

🧩 **أدوات موثوقة:**

- VirusTotal – يفحص الروابط والملفات بأكثر من 70 محرك مكافحة.
- URLVoid – يعطي تقييمًا للموقع، وتاريخه، ومدى موثوقيته.

🔑 **نصيحة** :لا تفتح أي رابط غير متوقع أو من شخص لا تعرفه — حتى لو بدا رسميًا.

5.6 📦 التحديثات التلقائية

رغم أن التحديثات قد تبدو مزعجة للبعض، إلا أنها ضرورية جدًا لحماية النظام من الثغرات الأمنية المكتشفة حديثًا.

🧪 لماذا التحديثات مهمة؟

- تصحح ثغرات أمنية يمكن استغلالها في الهجمات.
- تطوّر أداء النظام وتحسن الكفاءة.
- تسد الطريق على البرمجيات الضارة الحديثة.

أمثلة:

- كثير من البرمجيات الخبيثة تعتمد على ثغرات غير مُحدثة، كما حدث في هجمات WannaCry.

🔑 نصيحة:

- فعّل التحديث التلقائي لنظام التشغيل (Windows / macOS / Android / iOS).
- حدّث المتصفح، برامج الأوفيس، وبرامج الأمان.

📌 ملخص الفصل الخامس (نقاط سريعة)

- برنامج مكافحة الفيروسات ضروري لفحص الجهاز وحمايته من التهديدات.
- مدير كلمات المرور يوفر لك أمانًا وسهولة في إدارة الحسابات.
- VPN يحمي اتصالك ويخفي هويتك على الإنترنت.
- أدوات فحص الروابط تساعدك على التحقق من سلامة الروابط قبل النقر.
- التحديثات المستمرة تسد الثغرات وتحافظ على أمن جهازك.

✅ أسئلة تقييم ذاتي

1. هل تستخدم برنامج مكافحة فيروسات نشط ومحدث على جهازك؟
2. كم كلمة مرور مختلفة عندك؟ وهل تحفظها في ورقة أو المتصفح؟
3. هل سبق لك استخدام VPN أثناء تواجدك في شبكة عامة؟
4. ماذا تفعل عندما يصلك رابط غير متوقع على الإيميل أو الواتساب؟
5. هل تقوم بتحديث جهازك تلقائيًا؟ متى آخر مرة تحققّت من ذلك؟

🆘 .الفصل السادس: ماذا تفعل عند حدوث اختراق؟

6.1 مقدمة

رغم كل الاحتياطات، قد يتعرض أي شخص أو جهة لاختراق أمني.
سواء كان ذلك بسبب رابط خبيث، أو برنامج غير موثوق، أو حتى خطأ بشري بسيط — المهم في هذه الحالة هو **التحرك السريع، لا الذعر**.

هذا الفصل يقدم خطة طوارئ متدرجة وعملية، تساعدك على استعادة السيطرة وتقليل الأضرار، سواء كان الاختراق لحساب شخصي أو لجهازك أو لنظام تابع لجهة عمل.

6.2 🔐 تغيير كلمات المرور فورًا

عند الاشتباه بأي اختراق، أول وأهم خطوة هي تغيير كلمات المرور، خصوصًا للحسابات الأساسية المرتبطة ببريدك الإلكتروني أو بياناتك المالية.

🧩 الحسابات ذات الأولوية:

- البريد الإلكتروني (لأنه مفتاح إعادة تعيين باقي الحسابات).
- حسابات البنوك أو المحافظ الرقمية.
- حسابات التواصل الاجتماعي.
- أي خدمة مرتبطة برقم الهوية أو بيانات رسمية.

🧪 مثال تطبيقي:

إذا تم اختراق بريدك الإلكتروني، فالمهاجم يمكنه استخدامه لإعادة تعيين كلمة مرور حساباتك الأخرى، لذا يجب تغييرها أولًا.

🔑 نصيحة:
لا تعيد استخدام نفس الكلمة، واختر كلمة مرور طويلة ومعقدة، وفعل التحقق بخطوتين فورًا.

6.3 🛑 فصل الإنترنت عن الجهاز

إذا شعرت بأن هناك سلوكًا غريبًا في جهازك (كبطء مفاجئ، أو نوافذ تفتح من نفسها، أو رسائل تنبيه غريبة)، فقد يكون هناك برنامج خبيث نشط.

خطوات سريعة:

- افصل الاتصال بالإنترنت فورًا (Wi-Fi / كابل).
- لا تنقل ملفات أو تشبك فلاش ميموري أو جوالات.
- لا تحاول إغلاق الملفات أو البرامج يدويًا، فذلك قد يُفقدك الأدلة.

🔑 نصيحة:
افصل الجهاز تمامًا عن الشبكة لحين فحصه من قبل مختص أو برنامج حماية موثوق.

6.4 🦠 فحص الجهاز باستخدام برنامج الحماية

قم بإجراء فحص شامل (Full Scan) باستخدام برنامج مكافحة فيروسات محدّث.

إن وُجد تهديد:

- عزل التهديد.(Quarantine)
- حذف الملف الضار.
- إعادة تشغيل الجهاز بعد التنظيف.

🧪 ملاحظة مهمة:

بعض البرمجيات الخبيثة تحاول إخفاء نفسها أو تعطل برامج الحماية، وهنا يفضل تشغيل الفحص من **الوضع الآمن (Safe Mode)** أو استخدام قرص طوارئ لفحص الجهاز خارجيًا.

🔑 نصيحة:
لا تكتفِ بالفحص السريع. قم بفحص شامل لكل الأقراص والمجلدات.

6.5 📞 التواصل مع الجهة المسؤولة

إذا كان الاختراق يخص جهة خارجية (بنك، مزود بريد إلكتروني، شركة تقنية)، فتواصل معهم فورًا عبر القنوات الرسمية.

الأمور التي يجب الإبلاغ عنها:

- وقت الهجوم.
- الأثر المتوقع (سرقة، إيقاف حساب، وصول غير مصرح).
- الخطوات التي اتخذتها.

🧪 مثال:

عند اختراق حسابك البنكي، بلّغ البنك لإيقاف البطاقة مؤقتًا، ومنع أي عمليات شراء أو تحويلات مشبوهة.

🔑 نصيحة:

احتفظ دائمًا بنسخة من أرقام الدعم الفني والمواقع الرسمية للخدمات المهمة.

6.6 📜 مراجعة الأنشطة وتفعيل الحماية

بعد تأمين الحسابات، يجب مراجعة الأنشطة التالية:

ما يجب مراجعته:

- سجل الدخول.(Login Activity)
- الأجهزة المربوطة بالحساب.
- التطبيقات المرتبطة.(Connected Apps)
- إعدادات الاسترداد (البريد، الهاتف، الأسئلة السرية).

إجراءات استباقية:

- تسجيل الخروج من كل الأجهزة.(Log out all sessions)
- حذف أي تطبيق مشبوه.

- تفعيل التحقق بخطوتين إن لم يكن مفعّلًا.

🔑 **نصيحة:**
بعض المواقع تتيح لك تنزيل سجل النشاطات، احتفظ به للمراجعة أو التحقيق لاحقًا.

6.7 🧠 التحليل والتعلّم من التجربة

الاختراق لا يعني بالضرورة أنك مقصّر، لكنه مؤشر واضح على وجود ثغرة ما.

أسئلة للمراجعة:

- كيف حصل الاختراق؟ (رابط؟ تطبيق؟ كلمة سر؟)
- هل كانت أجهزتك محدّثة؟
- هل شاركت بياناتك مع شخص أو موقع غير موثوق؟

هذه الأسئلة تساعدك على بناء "مناعة سيبرانية" أقوى في المستقبل.

🔑 **نصيحة:**
شارك ما حدث مع زملائك أو أسرتك كتجربة تعليمية — قد تنقذهم لاحقًا من نفس الفخ.

6.8 ☂️ تذكير مهم

بعض الهجمات لا تظهر آثارها فورًا، بل تبقى كامنة لأيام أو أسابيع.
لذلك لا تستهين بأي سلوك غريب، وابقَ على يقظة دائمًا.

📌 ملخص الفصل السادس (نقاط سريعة)

- غير كلمات المرور فورًا، وابدأ بالحسابات الحساسة.
- افصل الإنترنت إذا شككت بوجود اختراق.
- استخدم برنامج حماية لإجراء فحص شامل.
- تواصل مع الجهات المعنية لأي حسابات مرتبطة.

- راجع سجلات الدخول والصلاحيات.
- تعلم من التجربة، وطور أسلوبك الرقمي.

✅ أسئلة تقييم ذاتي

1. هل تحتفظ بنسخ احتياطية من بياناتك المهمة في مكان آمن؟
2. ما أول إجراء ستتخذه إذا شعرت باختراق حسابك؟
3. هل تعرف كيف تطّلع على سجل الدخول لحساباتك المختلفة؟
4. هل لديك خطة طوارئ شخصية إذا تم اختراق جهازك؟
5. ما التغيير الذي ستقوم به اليوم لتحسين استعدادك السيبراني؟

🎓 الفصل السابع: مسار أكاديمي ومهني في الأمن السيبراني

7.1 مقدمة

الأمن السيبراني لم يعد مجرد مهارة تقنية تُمارس داخل غرفة السيرفرات، بل أصبح تخصصًا أكاديميًا ومهنيًا يُدرّس في الجامعات العالمية، وركيزة أساسية في سياسات الدول والمؤسسات. هذا الفصل موجه للمهتمين بالتخصص الأكاديمي والمهني، سواء كانوا طلابًا، أو باحثين، أو موظفين يرغبون في التحول الوظيفي نحو هذا المجال.

سنتناول هنا جوانب التخصص الأكاديمية، فرص العمل، المهارات المطلوبة، الشهادات المهنية، وأهم المصادر التعليمية.

7.2 التخصص الأكاديمي في الأمن السيبراني

🌍 التخصص الجامعي:

الأمن السيبراني يُدرّس في عدة مستويات:

- **درجة البكالوريوس** :عادة ما تكون ضمن علوم الحاسوب أو تقنية المعلومات، مع مسار متخصص في الأمن.
- **درجة الماجستير** :أكثر تركيزًا على التهديدات المتقدمة، الحوكمة، التحليل الجنائي الرقمي، والتشفير.
- **درجة الدكتوراه** :تركز على البحث العلمي، ابتكار الحلول، ومحاكاة الهجمات والدفاعات.

🏛️ أمثلة على مواد دراسية:

- مقدمة في أمن المعلومات
- التشفير(Cryptography)
- أمن الشبكات(Network Security)
- التحليل الجنائي الرقمي(Digital Forensics)
- اختبار الاختراق(Penetration Testing)
- حوكمة الأمن السيبراني

7.3 المهارات المطلوبة في المجال

🔧 **مهارات تقنية:**

- فهم بروتوكولات الشبكات(TCP/IP ، DNS، HTTP)
- البرمجة بلغة واحدة على الأقل(Python ، Bash)
- التعامل مع أنظمة التشغيل(Linux ، Windows Server)
- أدوات تحليل الثغرات مثل(Wireshark ، Nmap، Burp Suite

🧠 **مهارات تحليلية:**

- التفكير النقدي
- التحليل المنطقي لسلوك الأنظمة
- ربط الأدلة الرقمية(Log Correlation)

👥 **مهارات ناعمة (Soft Skills) :**

- التواصل الفعّال (خصوصًا في بيئات الطوارئ)
- الكتابة التقنية للتقارير الأمنية
- العمل الجماعي وإدارة الأزمات

7.4 الشهادات المهنية المعترف بها عالميًا

🔰 **للمبتدئين:**

- **CompTIA Security+**
  تغطي أساسيات التهديدات، التشفير، الشبكات، والاستجابة للحوادث.
- **Cisco CCNA CyberOps**
  أساسيات مراقبة الأمن السيبراني وتحليل الحوادث.

🛡️ **للمستوى المتوسط:**

- **Certified Ethical Hacker (CEH)**
  تعلم منهجية اختبار الاختراق وأدوات الهجوم الأخلاقي.
- **CompTIA CySA+**
  متخصصة في التحليل والاستجابة للحوادث.

🎯 **للمحترفين:**

- **Certified Information Systems Security Professional (CISSP)**
  تركيز على الجانب الإداري والحوكمة، معترف بها عالميًا.
- **Certified Information Security Manager (CISM)**
  موجهة للمديرين التنفيذيين والمسؤولين عن السياسات الأمنية.

7.5مجالات التخصص داخل الأمن السيبراني

١. **التحليل الجنائي الرقمي**
كشف وتتبع الهجمات وتحليل الأدلة الرقمية.

٢. **اختبار الاختراق(Pen-testing)**
محاكاة الهجمات لاكتشاف الثغرات قبل أن يستغلها المهاجمون.

٣. **الاستجابة للحوادث(Incident Response)**
التدخل وقت الهجمات واحتواؤها بسرعة.

٤. **أمن الشبكات(Network Security)**
حماية البنية التحتية من التهديدات الخارجية والداخلية.

٥. **تأمين البرمجيات(Application Security)**
فحص البرمجيات والتطبيقات قبل النشر.

٦. **حوكمة الأمن السيبراني(Cybersecurity Governance)**
وضع السياسات والإجراءات والمعايير لحماية البيانات.

7.6 مصادر تعليمية موصى بها

🎓 منصات أكاديمية:

- **Coursera** – شراكات مع جامعات مثل Stanford وIBM
- **edX** – محتوى أكاديمي من Harvard وMIT
- **Cybrary** – منصة أمنية متخصصة

📘 كتب أساسية:

- *Cybersecurity Essentials* – Cisco Press
- *The Web Application Hacker's Handbook* – Dafydd Stuttard
- *Hacking: The Art of Exploitation* – Jon Erickson

🎥 قنوات يوتيوب:

- NetworkChuck
- The Cyber Mentor
- Hak5

7.7 خريطة طريق مقترحة للمبتدئ

🔹 المرحلة الأولى – الأساسيات:

- تعلم الشبكات + أنظمة التشغيل
- قراءة عن أنواع الهجمات
- دورة Security+ أو ما يعادلها

🔹 المرحلة الثانية – التخصص:

- التعرف على أدوات الأمن (Wireshark، Burp Suite)
- ممارسة التحديات في مواقع مثل Hack The Box، TryHackMe
- دورة CEH أو ما يعادلها

🔹 المرحلة الثالثة – الاحتراف:

- بناء مشاريع عملية أو العمل في فرقCTF
- الحصول على شهادة CISSP أوCISM
- الإسهام في أبحاث أو كتابة تقارير فنية

📌 **ملخص الفصل السابع (نقاط سريعة)**

- الأمن السيبراني مجال أكاديمي متكامل من البكالوريوس إلى الدكتوراه.
- يتطلب مزيجًا من المهارات التقنية والتحليلية والتواصلية.
- هناك شهادات عالمية تفتح أبواب التوظيف والاعتراف المهني.
- المجال متنوع ويشمل تخصصات دقيقة، من اختبار الاختراق إلى الحوكمة.
- الموارد التعليمية متوفرة ومجانية في أغلبها — لكن تحتاج التزامًا ومثابرة.

👨‍👩‍👧‍👦الفصل الثامن: حماية الأسرة والأطفال في العالم الرقمي

8.1 مقدمة

في عصرنا الرقمي، لم يعد الأطفال والمراهقون مجرد مستخدمين للتقنية، بل أصبحوا جزءًا أساسيًا من عالم الإنترنت. من مقاطع الفيديو والألعاب، إلى وسائل التواصل والتطبيقات التعليمية — يتعرض الأطفال يوميًا لكم هائل من المحتوى والمخاطر. ولأن الأسرة هي خط الدفاع الأول، فإن التوعية الأسرية بأساسيات الأمن السيبراني أصبحت ضرورة وليست رفاهية.

8.2 لماذا الأطفال أكثر عرضة للخطر؟

- **قلة الخبرة الرقمية** :الأطفال لا يميزون بسهولة بين الآمن والخطر.
- **حب الاستكشاف** :يدفعهم الفضول لتجربة كل ما هو جديد.
- **سهولة الاستدراج** :قد يشاركون معلومات شخصية دون وعي أو يسقطون في فخاخ الدردشة.
- **غياب الرقابة أحيانًا** :يظن بعض الأهالي أن الأجهزة وسيلة للترفيه فقط دون متابعة حقيقية.

8.3 أنواع المخاطر التي تواجه الأسرة

النوع	الوصف
🎧 التصيّد للأطفال	مثل رسائل تدعي الفوز بجوائز أو ألعاب مجانية
💬 الاستدراج الإلكتروني	من خلال تطبيقات الدردشة والألعاب
📱 التطبيقات غير الآمنة	بعض الألعاب تطلب صلاحيات غير مبررة
👀 المحتوى غير اللائق	مشاهد عنف، ألفاظ مسيئة، أو مشاهد غير مناسبة
🕹️ الإدمان الرقمي	ساعات طويلة دون رقابة تؤثر على الصحة النفسية والجسدية

8.4 أساسيات الرقابة الأبوية

🔐 استخدام أدوات الرقابة الأبوية:

- **تطبيقات مثل :** Google Family Link ، Microsoft Family Safety، Qustodio.
- تسمح لك هذه الأدوات بـ:
  - تحديد وقت استخدام الجهاز.
  - مراقبة التطبيقات والمواقع.
  - تحديد الفئة العمرية للمحتوى.

🧠 وضع قواعد منزلية واضحة:

- تحديد ساعات الاستخدام.
- عدم مشاركة أي معلومات شخصية.
- الإبلاغ الفوري عند الشعور بعدم الأمان.

📺 المشاركة لا المراقبة فقط:

- شاهد معهم، اسألهم عما يحبونه.
- ادخل عالمهم الرقمي لا لتقييده، بل لفهمه وتوجيهه.

8.5 سلوكيات رقمية صحية للأسرة

✅ نماذج سلوك إيجابي من الوالدين

الأب أو الأم الذي يتصفح هاتفه طوال اليوم دون تفاعل، يصعب عليه إقناع طفله بترك الجهاز.

✅ التثقيف العائلي الدوري

كل أسبوع، خصص وقتًا للحديث عن موضوع رقمي: "ليش ما نضغط على أي رابط؟" – "كيف نحمي حساباتنا؟"

✅ تحديد مناطق خالية من الأجهزة

مثل غرفة الطعام أو قبل النوم.

✅ **تعزيز بدائل غير رقمية**
قراءة، أنشطة يدوية، لعب جماعي.

8.6 ماذا تفعل لو تم استغلال طفلك رقميًا؟

١. **لا تهاجمه أو تلومه.**
الطفل الضحية يحتاج احتواءً، لا تأنيبًا.

٢. **اجمع الأدلة فورًا.**
صور المحادثات أو الرسائل (بدون تعديل).

٣. **أبلغ الجهات المختصة.**
في السعودية:

- رقم **البلاغات الأمنية الموحدة ٩١١** - بعض المناطق ٩٩٩.
- منصة بلاغات الجرائم المعلوماتية :
https://www.moi.gov.sa

٤. **اطلب الدعم النفسي إن لزم الأمر.**

📌 ملخص الفصل الثامن (نقاط سريعة)

- الأطفال عرضة لهجمات رقمية بسبب قلة الوعي وسهولة التأثر.
- الأسرة مسؤولة عن التوجيه، لا المنع المطلق.
- أدوات الرقابة الأبوية ضرورة في كل منزل.
- التواصل المفتوح مع الأبناء هو الحماية الأقوى.
- ثقافة الاستخدام الآمن تبدأ من القدوة لا من الأوامر.

✅ أسئلة تقييم ذاتي للأسرة

- هل تعرف التطبيقات التي يستخدمها طفلك يوميًا؟
- هل ناقشت معه يومًا مفهوم "الخصوصية الرقمية"؟

- كم عدد الساعات التي يقضيها الطفل أمام الشاشة؟ وهل هي مناسبة لعمره؟
- هل تفعل أدوات الرقابة الأبوية على أجهزته؟
- كيف ستتصرف لو أخبرك أنه تعرّض لموقف رقمي مريب؟

الفصل التاسع: الأمن السيبراني في المملكة – الأنظمة ودور الجهات الوطنية

9.1مقدمة

تسير المملكة العربية السعودية بخطى متسارعة نحو التحول الرقمي في كافة القطاعات، من الحكومة الإلكترونية إلى الذكاء الاصطناعي. ومع هذا التحول، أصبح الأمن السيبراني ركيزة أساسية للحفاظ على سرية البيانات واستمرارية الخدمات. ولهذا أنشأت الدولة جهات متخصصة وسنّت سياسات وتشريعات تهدف إلى تعزيز الأمن الرقمي على مستوى الأفراد والمؤسسات.

9.2الهيئة الوطنية للأمن السيبراني(NCA)

🛡️ من هي الهيئة؟

- جهة حكومية مستقلة أنشئت عام ٢٠١٧.
- ترتبط مباشرة بمقام خادم الحرمين الشريفين.
- تُعد الجهة التنظيمية العليا للأمن السيبراني في المملكة.

🎯 أهدافها:

- **وضع السياسات** الوطنية لحماية الفضاء السيبراني.
- **تعزيز جاهزية الجهات** الحكومية والخاصة ضد الهجمات.
- **تأهيل الكفاءات الوطنية** في مجال الأمن السيبراني.
- **رصد التهديدات** والاستجابة لها على المستوى الوطني.

📄 أبرز الوثائق الصادرة عنها:

- السياسات الوطنية للأمن السيبراني.(NCSP)
- سياسة الحد الأدنى للأمن السيبراني (Minimum Cybersecurity Baseline - MCB).
- الإطار السعودي لحوكمة الأمن السيبراني.(CSF)
- إطار المهارات الوطنية.(NCF)

9.3 سياسة الحد الأدنى للأمن السيبراني(MCB)

ما هي؟

- مجموعة من المتطلبات الفنية والتنظيمية تُلزم بها جميع الجهات الحكومية وشبه الحكومية.

أهم محاورها:

١. **إدارة الهوية والوصول**

٢. **الحماية من البرمجيات الخبيثة**

٣. **تشفير البيانات**

٤. **التحكم في الأجهزة المحمولة**

٥. **النسخ الاحتياطي والتعافي**

٦. **التحديثات الأمنية**

٧. **الاستجابة للحوادث**

الهدف:

ضمان توفر حد أدنى من الحماية لدى جميع الجهات، بغض النظر عن حجمها أو طبيعة خدماتها.

9.4 الجهات الوطنية الأخرى ذات العلاقة

🏛️ **سدايا (الهيئة السعودية للبيانات والذكاء الاصطناعي)**

- معنية بتنظيم **حوكمة البيانات** وضمان خصوصيتها.
- أطلقت سياسة البيانات المفتوحة، وضوابط مشاركة البيانات.

📡 **هيئة الاتصالات والفضاء والتقنية(CST)**

- مسؤولة عن **أمن البنية التحتية الرقمية**.
- تصدر تقارير دورية عن **سرعة الإنترنت والهجمات الرقمية**.
- أطلقت مبادرات توعوية مثل "التشفير حياة."

⚖️ **وزارة الداخلية – الأمن العام**

- تستقبل بلاغات **الجرائم المعلوماتية** عبر:
  - تطبيق كلنا أمن.
  - موقع أبشر.
  - أرقام الطوارئ (٩١١ أو ٩٩٩ حسب المنطقة).

9.5 جهود المملكة عالميًا

- **المملكة ضمن قائمة الدول الأعلى إنفاقًا على الأمن السيبراني في الشرق الأوسط.**
- حلت في **المرتبة الثانية عالميًا** في مؤشر الأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات (ITU) لعام ٢٠٢٠.
- وقّعت اتفاقيات دولية لتعزيز التعاون السيبراني مع:
  - الولايات المتحدة
  - كوريا الجنوبية
  - سنغافورة
  - الاتحاد الأوروبي

9.6 كيف يستفيد المواطن والموظف من هذه السياسات؟

- كمستخدم:
  - حماية معلوماتك محمية قانونيًا.
  - يمكنك الإبلاغ عن أي ابتزاز أو اختراق بسهولة.
- كموظف في جهة حكومية أو خاصة:
  - يجب أن تلتزم مؤسستك بتطبيق سياسات الأمن السيبراني.
  - يحق لك الحصول على تدريب دوري ووعي سيبراني.

- كمطور أو تقني:
  - التزامك بالسياسات الوطنية شرط لأي مشروع رقمي حكومي.

📌 ملخص الفصل التاسع (نقاط سريعة)

- الأمن السيبراني في المملكة تقوده **الهيئة الوطنية للأمن السيبراني**.
- هناك سياسات ملزمة لجميع الجهات، مثل سياسة الحد الأدنى.
- جهات داعمة مثل سدايا وهيئة الاتصالات تكمّل المنظومة.
- المملكة رائدة في مجال الأمن السيبراني عربيًا وعالميًا.
- المواطن والموظف مسؤولان عن الالتزام والوعي بالتشريعات.

✅ أسئلة تقييم ذاتي

- هل سمعت من قبل عن الهيئة الوطنية للأمن السيبراني؟ ما دورها؟
- هل تعرف إن كانت جهتك تطبق سياسة الحد الأدنى؟
- كيف تتصرف لو لاحظت ثغرة أمنية في جهة تعمل بها؟
- هل سبق أن استخدمت "كلنا أمن" أو موقع أبشر للتبليغ عن محتوى مشبوه؟
- كم مرة اطّلعت على سياسات الخصوصية أو شروط الاستخدام في موقع حكومي أو خاص؟

الفصل العاشر: الجانب القانوني – الجرائم الإلكترونية وعقوباتها في المملكة

10.1 مقدمة

مع توسّع استخدام التقنية والاعتماد على الإنترنت، ظهرت تحديات قانونية جديدة تتعلق باستخدام غير مشروع للفضاء السيبراني. ولأن الأمن السيبراني لا يتوقف عند الحماية الفنية، بل يشمل أيضًا **الوعي القانوني**، فإن هذا الفصل يهدف إلى توعية القارئ بالتصرفات التي تُعد جرائم إلكترونية في المملكة، والعقوبات المرتبطة بها، وكيفية التصرف في حال التعرض لها.

10.2 ⚖️ نظام مكافحة الجرائم المعلوماتية في السعودية

صدر هذا النظام بمرسوم ملكي عام ٢٠٠٧، بهدف حماية المصالح العامة والخاصة من جرائم المعلومات، ورفع مستوى الأمان السيبراني.

أبرز الجرائم التي يشملها:

الجريمة	العقوبة	الوصف
الاختراق أو الدخول غير المشروع	السجن حتى سنة، وغرامة حتى ٥٠٠ ألف ريال	دخول أنظمة أو شبكات بدون إذن
التشهير أو انتهاك الخصوصية	السجن سنة، وغرامة تصل ٥٠٠ ألف ريال	نشر صور أو مقاطع أو معلومات شخصية دون إذن
الابتزاز الإلكتروني	السجن سنتين، وغرامة تصل إلى مليون ريال	تهديد شخص بنشر صور أو معلومات للحصول على مال أو خدمة
نشر روابط خبيثة أو ضارة	نفس عقوبة الاختراق أو الابتزاز	إرسال أو نشر روابط تؤدي إلى اختراق أو سرقة بيانات
الاحتيال المالي أو النصب	السجن ٣ سنوات، وغرامة ٢ مليون ريال	انتحال صفة، إنشاء صفحات وهمية، جمع تبرعات كاذبة

10.3 👮 أمثلة واقعية من داخل المملكة

👨‍💻 قصة ١: اختراق سناب ومطالبة بالمال

شاب اخترق حساب فتاة في سناب شات وهددها بنشر صورها ما لم تحوّل له مبلغًا ماليًا. تم القبض عليه من خلال تتبع عنوان الـIP ، وصدر بحقه حكم بالسجن والغرامة.

💸 قصة ٢: حساب وهمي باسم جمعية خيرية

أنشأ شخص صفحة في تويتر تدّعي جمع تبرعات لمرضى السرطان. تبيّن لاحقًا أنها غير مرخصة، وتم تحويل الأموال لحسابه الخاص. أُدين بتهمة الاحتيال المعلوماتي.

10.4 🚨 كيف تتصرف عند التعرض لجريمة إلكترونية؟

✅ الخطوات المقترحة:

١. **توثيق الأدلة فورًا:**

- خذ لقطات شاشة.(Screenshots)
- احتفظ بروابط الحساب أو الرسالة.

٢. **لا تتواصل مع المبتز أو الجهة المشبوهة:**

- لا تدفع، لا ترد، لا تُفاوض.

٣. **الإبلاغ الرسمي الفوري:**

- عبر تطبيق كلنا أمن.
- أو موقع وزارة الداخلية.https://www.moi.gov.sa :
- أو بالاتصال على الرقم ٩١١ (بعض المناطق ٩٩٩).

٤. **طلب دعم نفسي أو اجتماعي عند الحاجة:**

- خصوصًا في حالات الابتزاز أو التأثير النفسي على الأطفال أو النساء.

10.5 🧠 أشياء قد تبدو "عادية" لكنها مخالفة

- تصوير شخص دون إذنه ونشر المقطع.
- مشاركة "نكتة" أو إشاعة تتعلق بشخصية عامة.
- نشر إعلان عن منتج وهمي.
- إرسال رابط فيه كود تتبع أو تجسس.

🔴 حتى وإن لم تكن نيتك سيئة، القانون يُحاسب على الأثر، لا فقط على النية.

📌 ملخص الفصل (نقاط سريعة)

- الجرائم الإلكترونية يعاقب عليها القانون السعودي بشدة.
- يشمل ذلك الاختراق، الابتزاز، التشهير، والاحتيال الرقمي.
- من المهم الإبلاغ وعدم السكوت — حتى لو كان الفاعل قريبًا.
- النيّة الطيبة لا تعفي من المسؤولية القانونية.
- توثيق الأدلة واللجوء للجهات المختصة هو التصرف الصحيح دائمًا.

✅ أسئلة تقييم ذاتي

- هل تعرف الفرق بين المزاح والابتزاز الإلكتروني؟
- هل تعلم أن تصوير شخص دون إذنه ونشر الصورة يُعد جريمة؟
- هل سبق وصلك رابط مشبوه؟ هل قمت بالإبلاغ؟
- ما أول خطوة قانونية يجب اتخاذها في حال تعرضك للابتزاز؟
- كم عدد الأشخاص الذين تعرفهم يجهلون هذه القوانين؟

👥 الفصل الحادي عشر: أمانك الشخصي على شبكات التواصل

11.1 مقدمة

وسائل التواصل الاجتماعي مثل تويتر، إنستغرام، سناب شات، وتيك توك أصبحت جزءًا لا يتجزأ من حياتنا اليومية. نشارك فيها صورنا، أفكارنا، أصدقاءنا، وأحيانًا حتى مواقعنا. لكن هذه المنصات – رغم ما تقدمه من ترفيه وتواصل – قد تكون **بابًا خلفيًا للمخترقين والمحتالين**، إذا لم يتم استخدامها بوعي.

هذا الفصل يقدّم **دليلًا عمليًا ومباشرًا** للاستخدام الآمن لوسائل التواصل، من ضبط الخصوصية إلى الحذر من الروابط المخادعة.

11.2 🔐 لماذا شبكات التواصل هدف رئيسي للمخترقين؟

- تحتوي على **معلوماتك الشخصية**: الاسم، الموقع، الأصدقاء، الصور، البريد، رقم الهاتف.
- يمكن استغلالها في **الهندسة الاجتماعية**: لجمع بياناتك أو انتحال هويتك.
- بعض الحسابات مربوطة بـ **بريدك الإلكتروني أو حسابات أخرى**، ما يجعلها نقطة انطلاق لهجمات أوسع.

11.3 ⚙️ إعدادات الخصوصية: أول خطوة للحماية

🛡️ تويتر (X):

- فعّل "الحساب خاص" إذا كنت لا ترغب في أن يرى غير المتابعين تغريداتك.
- راجع من يمكنه الإشارة لك أو إرسال رسائل خاصة.
- أوقف "الموقع الجغرافي" عند التغريد.

📷 إنستغرام:

- اجعل الحساب خاصًا.
- لا تسمح بالتعليق من الغرباء.
- أوقف خاصية مشاركة الموقع تلقائيًا.

- راقب من يمكنه إعادة مشاركة منشوراتك في القصص.

👻 **سناب شات:**

- فعّل "Ghost Mode" لمنع مشاركة موقعك.
- حدّد من يمكنه إرسال Snaps أو مشاهدة القصص.
- لا تقبل إضافات من غرباء دون التحقق.

🎵 **تيك توك:**

- اجعل الحساب خاصًا.
- امنع الغرباء من تنزيل فيديوهاتك.
- راجع إعدادات من يمكنه التعليق أو التفاعل.
- فعّل ميزة الإشعارات عند تسجيل الدخول من جهاز جديد.

🔑 نصيحة ذهبية:
ادخل على "إعدادات الخصوصية" في كل تطبيق مرة بالشهر على الأقل، وعدّلها حسب تغيّر استخدامك.

11.4 📤 ممارسات آمنة للنشر والمشاركة

✅ افعل:

- فكّر قبل النشر: هل يمكن استخدام هذه الصورة أو التغريدة ضدك لاحقًا؟
- انتبه لما يظهر في خلفية الصور (مستند، رقم لوحة، موقع).
- تجنّب مشاركة موقعك المباشر في الأماكن العامة.
- امسح المنشورات القديمة التي لم تعد مناسبة.

❌ لا تفعل:

- لا تنشر صور أطفالك أو عائلتك بدون وعي، خصوصًا بمواقع محددة.
- لا تُظهر بطاقات هوية، تذاكر سفر، أو أرقام حسابات في الصور.
- لا تضع البريد الإلكتروني الشخصي أو رقم الجوال في النبذة التعريفية.

11.5 🧪 احذر من روابط الاختراق في الرسائل الخاصة

أشهر وسيلة للاختراق في وسائل التواصل هي **روابط ظاهرها عادي، وباطنها تهديد**.

🎣 **السيناريو المتكرر:**

- يصلك رابط من حساب صديقك يقول: "شوف صورتك هنا"!
- أو: "هل هذا أنت في الفيديو؟"
- أو: "تخفيضات خرافية على هذا الموقع"!

تضغط على الرابط، وإذا بك:

- تُحول لصفحة تطلب منك تسجيل دخول وهمي.
- أو يبدأ تحميل ملف خبيث.
- أو يُطلب منك التحقق من هويتك برسالة كاذبة.

💣 **النتائج:**

- سرقة الحساب.
- الدخول لجهات الاتصال، وإرسال نفس الرسائل لهم.
- اختراق بريدك المرتبط بالحساب.
- استخدام حسابك في نشر محتوى مخالف أو محظور.

✅ **ماذا تفعل؟**

- لا تضغط على الروابط المجهولة، حتى لو من صديق.
- تواصل معه خارجيًا واسأله: هل أرسلت لي هذا الرابط؟
- استخدم أدوات فحص الروابط مثل VirusTotal.
- فعّل التحقق الثنائي لمنع الدخول حتى لو تم سرقة كلمة السر.

11.6 🧱 حماية الحساب بخطوتين

تفعيل **التحقق الثنائي (2FA)** يعني أن المخترق لا يستطيع الدخول لحسابك حتى لو عرف كلمة المرور.

في كل منصة:

- ادخل على "إعدادات الأمان."
- اختر "التحقق بخطوتين."
- فعّله برسالة نصية أو تطبيق مصادقة مثل Google Authenticator أو Microsoft Authenticator.

🔑 نصيحة:
كل حساب لا يحتوي على تحقق بخطوتين = حساب في خطر.

11.7 🧠 انتبه من "الهندسة الاجتماعية الرقمية"

المخترق قد لا يستخدم تقنية، بل يستخدم عقلك ضدك:

- يسألك أسئلة عادية (أول مدرسة، اسم الأم...) لجمع إجابات أسئلة الأمان.
- يدعي أنه من الدعم الفني ويطلب منك كود التحقق.
- أو يتقرب منك تدريجيًا ليطلب بياناتك لاحقًا.

✅ خلك واعي: لا تشارك أي معلومة خاصة حتى لو بدا الشخص موثوقًا.

11.8 🧼 راقب نشاط حسابك باستمرار

في كل تطبيق، يوجد قسم اسمه:

- "نشاط الحساب"
- أو "الأجهزة المتصلة"
- أو "الجلسات النشطة"

✅ تأكّد من:

- الأجهزة المتصلة بحسابك: هل هناك جهاز لا تعرفه؟
- مواقع الدخول الجغرافي: هل دخل أحد من مدينة غير منطقتك؟
- ساعات الدخول: هل تم تسجيل دخول وأنت نائم أو مشغول؟

إذا شككت، **سجّل الخروج من كل الجلسات فورًا**، وغيّر كلمة المرور.

📌 ملخص الفصل (نقاط سريعة)

- الخصوصية تبدأ من الإعدادات: عدّلها في تويتر، إنستغرام، سناب، تيك توك.
- لا تنشر كل شيء، وخصوصًا المعلومات الحساسة أو الصور العائلية.
- احذر من الروابط داخل الرسائل الخاصة — حتى لو أرسلها صديق.
- فعّل التحقق الثنائي لحماية الحسابات.
- راقب سجل النشاطات، وكن واعيًا لأي تواصل غير طبيعي.

✅ أسئلة تقييم ذاتي

- هل إعدادات خصوصيتك مفعّلة بشكل كافٍ في جميع حساباتك؟
- متى آخر مرة راجعت من يمكنه رؤية منشوراتك أو التواصل معك؟
- هل سبق وفتحت رابطًا في رسالة خاصة دون أن تتأكد من المصدر؟
- كم حساب لديك مفعّل فيه التحقق الثنائي؟
- هل راقبت يومًا سجل الدخول لحساباتك؟

🧠الفصل الثاني عشر: كيف يؤثر الذكاء الاصطناعي على أمنك السيبراني؟

12.1 مقدمة

الذكاء الاصطناعي (AI) لم يعد مجرد تقنية مستقبلية، بل أصبح جزءًا من واقعنا اليومي — من المساعدات الصوتية، إلى السيارات الذكية، ومحركات التوصية في منصات التواصل. لكن السؤال الأهم اليوم :**هل يمكن أن يكون الذكاء الاصطناعي حليفًا لنا في حماية أنفسنا؟ أم أنه أداة جديدة في يد المهاجمين؟**

هذا الفصل يُلقي الضوء على **الوجهين المتناقضين للذكاء الاصطناعي** في الأمن السيبراني: كيف يُستخدم لحمايتنا، وكيف قد يُستخدم ضدنا.

12.2 🎭كيف يستخدم المهاجمون الذكاء الاصطناعي؟

1. 🧠تصيّد إلكتروني أكثر ذكاءً(Smart Phishing)

- يستخدم المخترق أدوات توليد نصوص) مثل ChatGPT وغيره (لإنشاء رسائل مقنعة جدًا، تخلو من الأخطاء اللغوية، وتبدو وكأنها من جهة رسمية.
- يمكنه أيضًا تخصيص الرسالة حسب الشخص المستهدف (اسمك، وظيفتك، شركتك...) باستخدام بيانات مسرّبة أو متاحة علنًا.

🔎مثال:

"مرحبًا أ. أحمد، تم تعليق حسابك البنكي بسبب عملية مشبوهة. نرجو الدخول عبر الرابط التالي لتأكيد هويتك خلال ١٢ ساعة لتفادي الإيقاف".
التوقيع: البنك الأهلي - قسم المخاطر

🔴رغم أن الرسالة مزيفة، إلا أنها دقيقة واحترافية وتخدع بسهولة.

---

2. 🖼️التزوير العميق(Deepfake)

- تقنية تعتمد على الذكاء الاصطناعي لتوليد **مقاطع فيديو أو صوتيات مزيفة** تبدو حقيقية تمامًا.
- يمكن استخدامها لانتحال شخصية مدير، أو موظف رسمي، أو حتى أحد الوالدين، لطلب تحويل مالي أو معلومات حساسة.

---

3. 📊 تحليل البيانات الضخمة لاستهدافك بدقة

- يستطيع المهاجم استخدام AI لتحليل بياناتك على الإنترنت وتحديد أنسب وقت أو وسيلة لاستهدافك، أو حتى ابتزازك بناءً على اهتماماتك وتفضيلاتك.

12.3 🛡️ كيف يمكن أن يساعدنا الذكاء الاصطناعي في الحماية؟

لحسن الحظ، الذكاء الاصطناعي ليس فقط أداة في يد المهاجم، بل هو **درع قوي في يد المدافع** أيضًا.

1. ✅ تحليل الروابط والملفات

- أدوات مثل VirusTotal تستخدم الذكاء الاصطناعي لتحليل الروابط والملفات والكشف عن التهديدات حتى لو كانت جديدة وغير معروفة.

2. ✅ توليد كلمات مرور قوية

- مواقع مثل Bitwarden Generator تستخدم خوارزميات ذكية لإنشاء كلمات مرور طويلة ومعقدة يصعب اختراقها.

3. ✅ كشف الاختراقات مبكرًا

- بعض برامج مكافحة الفيروسات الحديثة تعتمد على AI لرصد **السلوك غير الطبيعي** في الجهاز أو الشبكة، حتى لو لم يكن هناك فيروس معروف بعد.

4. ✅ أدوات المساعدة الصوتية والكتابية

- يمكن استخدام أدوات مثل ChatGPT لتعلّم طرق الحماية، أو لفحص إعدادات الخصوصية، أو حتى كتابة نموذج بلاغ إلكتروني عن ابتزاز أو اختراق.

12.4 📌 كيف تتصرف بذكاء في زمن الذكاء الاصطناعي؟

🔑 نصائح عملية:

- **لا تثق بأي رسالة لمجرد أن شكلها احترافي** ← تحقق دائمًا من المصدر.

- **تأكد من هوية المتصل أو صاحب المقطع** —خصوصًا في التسجيلات المفاجئة.
- **استخدم أدوات AI الآمنة لمساعدتك، لكن لا تشارك فيها معلوماتك الخاصة.**
- **تابع المستجدات الأمنية** —لأن الهجمات تتطور باستمرار.

📌 ملخص الفصل (نقاط سريعة)

- الذكاء الاصطناعي يُستخدم اليوم في التصيّد، الانتحال، وتحليل البيانات ضد المستخدم.
- في المقابل، يمكن الاستفادة منه في الحماية، توليد كلمات مرور، كشف التهديدات.
- لا تثق بأي شيء لمجرد أنه يبدو "احترافيًا."
- كن على وعي تام بمخاطر التزييف العميق، خاصة مع المقاطع الصوتية والفيديوهات.

✅ أسئلة تقييم ذاتي

- هل سبق ووصلك محتوى بدا حقيقيًا، لكنه اتضح أنه مزيف؟
- هل تستخدم أدوات الذكاء الاصطناعي في حياتك اليومية؟ لأي غرض؟
- ما أول إجراء ستتخذه إذا وصلتك رسالة من مديرك تطلب تحويلًا ماليًا عاجلًا؟
- هل تستطيع التمييز بين مقطع فيديو حقيقي وآخر تم توليده بالذكاء الاصطناعي؟
- هل ترى أن الذكاء الاصطناعي أكثر فائدة أم خطرًا في الأمن السيبراني؟

👁️ الفصل الثالث عشر: خصوصيتك الرقمية – كيف تحمي هويتك وبياناتك على الإنترنت؟

13.1مقدمة

في العالم الرقمي، **خصوصيتك لا تُسرق فقط بالاختراق**، بل أحيانًا **تتخلى عنها دون أن تشعر** —عند التسجيل في تطبيق، مشاركة صورة، أو الضغط على "موافق" دون قراءة.
في هذا الفصل، نتعرف على مفهوم الخصوصية الرقمية، كيف تُجمع بياناتك، وكيف تحمي نفسك من التتبع والاستغلال.

13.2 🔍 ما المقصود بالخصوصية الرقمية؟

هي **حقك في التحكم في معلوماتك الشخصية** (مثل: موقعك، صورك، سجل تصفحك، اهتماماتك، أجهزتك...) وعدم استخدامها أو مشاركتها دون إذنك.

تشمل:

- البيانات التي تقدمها بنفسك (حساب، بريد، صورة).
- البيانات التي تُجمع عنك بدون علمك (كوكيز، موقع جغرافي، سجل تصفح).
- البيانات التي تُستنتج منك (اهتماماتك، ميولك، حالتك النفسية).

13.3 💡 كيف تُجمع بياناتك على الإنترنت؟

الطريقة	أمثلة
تطبيقات التواصل	الاسم، الصور، جهات الاتصال، الموقع
محركات البحث	ما تبحث عنه، متى وأين
تطبيقات الهاتف	صلاحيات غير ضرورية مثل المايك أو الكاميرا
الكوكيز	تتبع المواقع التي تزورها والإعلانات التي تشاهدها
شبكات Wi-Fi العامة	يمكن التنصت على اتصالك وسرقة بياناتك

13.4 🛑 المخاطر المرتبطة بانتهاك الخصوصية

- **الاستهداف الإعلاني المفرط**
- **الابتزاز وسرقة الهوية**
- **انتحال الشخصية**
- **تحليل نفسي وسلوكي دون علمك**
- **بيع بياناتك لجهات مجهولة**

13.5 🛡️ خطوات لحماية خصوصيتك الرقمية

✅ **استخدم متصفحًا يحترم الخصوصية**

- مثل Brave أو Firefox مع إضافات حماية (uBlock Origin ، Privacy Badger)

✅ **راجع صلاحيات التطبيقات**

- هل تطبيق "الآلة الحاسبة" يحتاج الكاميرا أو المايك؟ إذا لا، امنعه.

✅ **لا تشارك معلومات شخصية في ملفات التعريف العامة**

- مثل: رقم الهاتف، البريد الأساسي، المدرسة، الموقع الدقيق.

✅ **استخدم محركات بحث بديلة**

- مثل DuckDuckGo الذي لا يتتبعك.

✅ **راقب إعدادات "الإعلانات المخصصة"**

- في جوجل، فيسبوك، تويتر — وأوقفها من الإعدادات.

✅ **امسح بياناتك الدورية**

- سجل التصفح، ملفات الكوكيز، الأجهزة المرتبطة بالحساب.

✅ **استخدم أدوات لإخفاء هويتك**

- مثل VPN موثوق، وميزة "Private Browsing" عند الحاجة.

13.6 🔁 خصوصيتك ليست "سراً"... بل "حق"

الخطأ الشائع: "ما عندي شي أخاف عليه."
الحقيقة: الخصوصية ليست فقط لحماية الأسرار، بل للحفاظ على كرامتك، قراراتك، حريتك في اختيار ما تشارك، ومع من.

📌 ملخص الفصل (نقاط سريعة)

- خصوصيتك تُنتهك أكثر مما تتخيل، غالبًا دون علمك.
- البيانات تجمع من التطبيقات، البحث، المواقع، وحتى من صورك.
- حماية الخصوصية تبدأ بإدراك الصلاحيات، إعدادات الحسابات، وأدوات الحماية.
- لا تنتظر الاختراق لتبدأ، فكل معلومة تُجمع عنك تبني "بروفايل رقمي" قد يُستخدم ضدك.

✅ أسئلة تقييم ذاتي

- هل تعلم من يملك بياناتك اليوم؟
- هل تراجع صلاحيات التطبيقات على جهازك بشكل دوري؟
- كم مرة تقرأ سياسات الخصوصية قبل الموافقة؟
- هل تستخدم متصفحًا خاصًا عند التصفح الحساس؟
- هل فكرت يومًا في طلب حذف بياناتك من موقع معين؟

🏢 الفصل الرابع عشر: الأمن السيبراني للمنشآت الصغيرة والمتوسطة

14.1 مقدمة

ليست الشركات الكبرى وحدها هدفًا للهجمات السيبرانية.
75٪ من الهجمات الرقمية تستهدف المنشآت الصغيرة والمتوسطة، لأنها غالبًا تفتقر للأنظمة الوقائية، وتعتمد على أدوات بسيطة بدون حماية كافية.
هذا الفصل يقدّم خارطة طريق عملية لحماية منشأتك، حتى لو كنت لا تملك فريقًا تقنيًا.

14.2 💥 لماذا تُستهدف المنشآت الصغيرة؟

- ضعف البنية التحتية التقنية.
- غياب السياسات الأمنية.
- الاعتماد على موظف "واحد لكل شيء."
- استخدام برمجيات مقرصنة أو مجانية غير آمنة.
- عدم وجود نسخ احتياطية أو حماية للبريد.

14.3 🛡️ أهم النقاط التي يجب تأمينها

1. 📧 تأمين البريد الإلكتروني

- استخدم خدمة احترافية (مثل Google Workspace أو Microsoft 365).
- فعّل التحقق بخطوتين.
- امنع إعادة التوجيه التلقائي.(Forwarding)

2. 🖥️ حماية أجهزة الموظفين

- فعّل كلمات مرور قوية لكل جهاز.
- لا تسمح باستخدام أجهزة شخصية في المهام الحساسة.
- استخدم برنامج حماية في كل جهاز.

3. 🔐 إدارة الصلاحيات

- لا تعطي صلاحيات المسؤول Admin إلا لمن يحتاجها.
- امنع الوصول المشترك لحسابات مهمة.
- راجع الصلاحيات شهريًا، خصوصًا للموظفين المنتهية علاقتهم بالمنشأة.

4. 📂 النسخ الاحتياطي

- خزن نسخة من بياناتك المهمة في موقع منفصل + Cloud قرص خارجي.
- افحص النسخ الاحتياطية بشكل دوري.

5. 🌐 الموقع الإلكتروني والمتجر الإلكتروني

- حدّث منصة الموقع أو المتجر دوريًا.
- استخدم شهادة SSL (https)
- راقب محاولات الدخول الفاشلة.
- أزل الإضافات أو القوالب غير المستخدمة.

6. 🔒 التعاقد مع مزود موثوق

- إذا كان لديك فني خارجي أو شركة إدارة أنظمة، اطلب توضيح:
  - من يملك البيانات؟
  - كيف تتم الحماية؟
  - من يملك الوصول؟

14.4 🦸 إجراءات سريعة لحماية منشأتك

١. تغيير كلمات المرور القديمة.

٢. تفعيل التحقق بخطوتين لكل حساب.

٣. تثبيت برنامج حماية لجميع الأجهزة.

٤. تحديث أنظمة التشغيل والبرامج.

٥. تدريب الموظفين على كشف التصيّد.

٦. التحقق من هوية كل مزود خدمة خارجي.

٧. إيقاف حسابات الموظفين السابقين.

٨. مراقبة الوصول للمستندات المشتركة.

٩. تفعيل إشعارات الدخول الغريب.

١٠. إعداد خطة استجابة للحوادث.

14.5 📄 نموذج خطة أمنية مبسطة للمنشآت

المجال	الإجراء المقترح
البريد	خدمة احترافية + تحقق بخطوتين
الأجهزة	كلمة مرور + برنامج حماية
الموظفون	صلاحيات حسب المهام فقط
البيانات	نسخ احتياطي دوري + تشفير
الموقع	SSL + تحديثات منتظمة
التدريب	ورشة شهرية أو نشرة توعوية

14.6 🧠 التوعية داخل المنشأة

- لا تكفِ الأنظمة بدون وعي الموظف.
- اجعل الأمن السيبراني جزءًا من ثقافة العمل.
- خصص ١٠ دقائق أسبوعيًا لاجتماع مصغّر حول الأمن.

📌 ملخص الفصل (نقاط سريعة)

- المنشآت الصغيرة أكثر عرضة للهجمات لأنها تفتقر للأنظمة الوقائية.
- تأمين البريد، الأجهزة، البيانات، والموقع هو الحد الأدنى للحماية.

- إدارة الصلاحيات وتحديث الأنظمة تقلّل المخاطر بنسبة كبيرة.
- التوعية الداخلية لا تقل أهمية عن الحلول التقنية.

✅ **أسئلة تقييم ذاتي (للمنشآت)**

- هل يستخدم كل موظف بريدًا خاصًا أم مشتركًا؟
- هل هناك نسخة احتياطية من بيانات العملاء؟
- هل موقعك محمي بشهادةSSL ؟
- هل لديك قائمة بالمستخدمين وصلاحياتهم؟
- متى آخر مرة دربت فيها موظفيك على الأمن السيبراني؟

الفصل الخامس عشر : الأمن السيبراني من منظور المنشآت والمؤسسات

🏢 التزامات قانونية على المنشآت:

حتى وإن لم تكن جهة حكومية، فإن **أي منشأة تقدم خدمات رقمية أو تتعامل مع بيانات العملاء** تقع تحت طائلة بعض الالتزامات القانونية، مثل:

الالتزام	الوصف
سياسة خصوصية واضحة	لا بد من وجود وثيقة توضح كيف تجمع البيانات، وأين تُخزن، ومن يراها.
حماية بيانات العملاء	يُلزمك القانون بحماية معلومات العملاء من التسريب أو الاستخدام غير المصرح به.
الإبلاغ عن الحوادث	في حال تعرضت للاختراق وسُربت بيانات، قد تُلزم بالإبلاغ الفوري حسب نوع الجهة.
توعية الموظفين	بعض الأنظمة مثل "سياسة الحد الأدنى" تتطلب تدريب الموظفين بشكل دوري.

📋 أمثلة على المخالفات من قبل المؤسسات:

- **نشر بيانات عملاء دون إذن (حتى لو كانت صورة فاتورة).**
- **الاحتفاظ بنسخ من بطاقات الهوية في غير موضعها (مثل الواتساب).**
- **عدم تأمين موقع إلكتروني يحتوي على نموذج تسجيل أو دفع.**
- **عدم حذف بيانات المستخدم عند طلبه** -في بعض الحالات.

⚠️ عقوبات قد تتعرض لها المنشأة:

- غرامات مالية (تصل إلى ملايين الريالات في حال التسريب أو الإهمال المتكرر).
- إغلاق المنصة أو الحجب المؤقت من هيئة الاتصالات.

- مسؤولية قانونية مباشرة على المدير التنفيذي أو مسؤول التقنية.

🔐 أدوات قانونية لحماية منشأتك:

- **اتفاقية سياسة خصوصية** تنشرها على موقعك الإلكتروني.
- **اتفاقية "عدم إفشاء (NDA)"** مع الموظفين والمزودين الخارجيين.
- **سجل حوادث أمني داخلي** توثق فيه أي تهديد أو محاولة اختراق.
- **مراجعة دورية مع محامي أو استشاري تقنية قانونية.**

🧠 نصائح للمسؤولين:

- **لا تنتظر حدوث مشكلة لتتحرك قانونيًا** — استعد دائمًا.
- **احرص على وضوح الصلاحيات والمسؤوليات داخل المنشأة.**
- **لا تعتمد فقط على الطرف التقني** — افهم كيف تُحمى بياناتك.
- **الجهل بالنظام لا يعفي من العقوبة.**

📌 ملخص إضافي للفصل القانوني:

- هناك مسؤولية قانونية ليس فقط على الأفراد، بل على المؤسسات أيضًا.
- حماية بيانات العملاء ليست خيارًا بل التزام قانوني.
- وجود السياسات المكتوبة لا يكفي إن لم تُطبق فعليًا.
- يُستحسن إشراك جهة قانونية في مراجعة الإجراءات الرقمية داخل المنشأة.

✅ أسئلة تقييم ذاتي للمؤسسات:

- هل لدى منشأتك سياسة خصوصية منشورة؟
- كيف يتم التعامل مع طلبات حذف أو تعديل بيانات العملاء؟

- هل توجد اتفاقيات NDA موقعة مع كل من يملك صلاحية على بيانات العملاء؟
- كم عدد الموظفين المدربين على أساسيات حماية البيانات؟
- هل تمت مراجعة نظام الموقع الإلكتروني قانونيًا وتقنيًا؟

📎 الفصل السادس عشر: ملاحق وأدوات جاهزة للطباعة

هذه الملاحق مصممة لتكون أدوات مساعدة جاهزة للاستخدام سواء من قبل الأفراد، أو الأسر، أو المؤسسات الصغيرة. يمكن طباعتها، مشاركتها، أو استخدامها إلكترونيًا بشكل مباشر.

📄 نموذج: خطة استجابة للطوارئ السيبرانية (نسخة مبسطة)

م	الإجراء	المسؤول	الملاحظات
1	فصل الإنترنت فورًا عن الجهاز المصاب	المستخدم	منع انتشار الضرر
2	تغيير كلمات المرور	المستخدم	بدءًا من البريد الإلكتروني
3	فحص الجهاز ببرنامج حماية	الدعم الفني أو المستخدم	Full Scan
4	توثيق الحادث (صور، رسائل، نشاط دخول)	المستخدم	لا تحذف الأدلة
5	إبلاغ الجهة المسؤولة (بنك، مزود خدمة)	المستخدم	عبر القنوات الرسمية
6	مراجعة الصلاحيات والحسابات المرتبطة	المستخدم	وإزالة غير المعروف منها
7	تحليل السبب وتوثيق الدروس المستفادة	الدعم أو الفريق الأمني	للتعلم والتحسين

✅ قائمة مرجعية: تأمين الجهاز والشبكة المنزلية

البند	تم؟(❌ / ✅)
هل تستخدم كلمة مرور قوية لجهازك؟	
هل فعّلت التحقق بخطوتين لكل حساباتك المهمة؟	
هل جهازك محدّث بآخر إصدار؟	
هل فعّلت جدار الحماية(Firewall) ؟	
هل تستخدم برنامج حماية (Antivirus) نشط؟	
هل راجعت صلاحيات التطبيقات في جهازك؟	
هل شبكة الواي فاي محمية بكلمة مرور قوية؟	
هل غيّرت اسم الشبكة الافتراضي(SSID) ؟	
هل قمت بتغيير كلمة مرور جهاز الراوتر؟	
هل تراقب الأجهزة المتصلة بشبكتك؟	

🗓️ جدول متابعة تحديثات البرامج

اسم الجهاز / النظام	آخر تحديث	التحديث التلقائي مفعل؟	ملاحظات
ويندوز / لابتوب شخصي			
iPhone / جوال شخصي			
الراوتر المنزلي			
برنامج مكافحة الفيروسات			
المتصفح(Chrome, Firefox)			

🔄 *يفضل مراجعة هذا الجدول شهريًا.*

🔐 قوالب كلمات مرور قوية وسهلة التذكر

استخدم أحد الأنماط التالية مع تخصيص بسيط لك:

النمط	مثال	التخصيص
[كلمة][رمز][رقم][مدينة]	Coffee@2024Riyadh	كلمة تهمك + رمز + رقم + شيء شخصي
[جملة سرية مختصرة]	!M@Rk2025bE	أول حرف من كل كلمة في جملة مثل "My Account Requires Key 2025 to be Enabled" :
[حيوان][رمز][شهر]	Cat#May2025	تغيير شهري بسيط لتحديث الكلمة

🧠 **نصائح:**

- لا تستخدم اسمك أو تاريخ ميلادك فقط.
- لا تكرر كلمة المرور في أكثر من حساب.
- استخدم مدير كلمات مرور لتوليد وتخزينها.

🌐 **روابط مهمة وأدوات موصى بها**

🔎 **أدوات فحص الروابط والملفات:**

- VirusTotal
- URLVoid

🔐 **برامج مكافحة الفيروسات المجانية:**

- Windows Defender
- Avast Free

🌍 **خدمات VPN موثوقة:**

- NordVPN
- Surfshark
- ProtonVPN

📢 **الإبلاغ عن الجرائم الإلكترونية في السعودية:**

- تطبيق كلنا أمن
- منصة بلاغات الجرائم المعلوماتية - وزارة الداخلية
- الرقم الموحد) **911** :بعض المناطق ٩٩٩(

📌 **ملخص الفصل العاشر (نقاط سريعة)**

- هذه الأدوات تساعدك على الانتقال من الفهم إلى التطبيق.

- يمكنك طباعتها أو استخدامها إلكترونيًا لتأمين نفسك وأسرتك.
- مراجعتها بشكل دوري تساعدك على بناء روتين رقمي آمن.

📚 قائمة المراجع والمصادر الإضافية

📜 مراجع عربية:

١. **الهيئة الوطنية للأمن السيبراني (NCA)** – https://nca.gov.sa
(تشريعات، سياسات، أدلة الأمن السيبراني في المملكة)

٢. **هيئة الاتصالات والفضاء والتقنية (CST)** – https://www.cst.gov.sa
(تقارير التهديدات، التوعية، حوكمة الاتصالات)

٣. **منصة كلنا أمن – وزارة الداخلية**
(للتبليغ عن الجرائم المعلوماتية داخل السعودية)

🌍 مراجع أجنبية:

١. **NIST Cybersecurity Framework** – https://www.nist.gov/cyberframework
إطار شامل من المعهد الوطني الأمريكي للمعايير

٢. **OWASP Top 10** – https://owasp.org
أخطر عشر ثغرات في تطبيقات الويب - محدثة باستمرار

٣. **SANS Institute Reading Room** – https://www.sans.org/white-papers/
مقالات متخصصة وأبحاث قصيرة مجانية في الأمن السيبراني

٤. **ENISA (EU Cybersecurity Agency)** – https://www.enisa.europa.eu
محتوى توعوي من الاتحاد الأوروبي وتحليلات تهديدات

📘 كتب مقترحة:

- *Cybersecurity Essentials* – Cisco Press

- *The Web Application Hacker's Handbook* – Dafydd Stuttard
- *Hacking: The Art of Exploitation* – Jon Erickson
- *Blue Team Handbook: Incident Response Edition* – Don Murdoch

---

🎓 **دورات ومواقع تعليمية:**

- Coursera: Cybersecurity Specialization
- Cybrary – Cybersecurity Courses
- TryHackMe – Hands-on Labs
- Hack The Box – Cybersecurity Challenges

📺 **قنوات يوتيوب موصى بها:**

- **NetworkChuck** – تبسيط التقنية والأمن السيبراني.
- **The Cyber Mentor** – شروحات احترافية لاختبار الاختراق.
- **Hak5** – أدوات واختراقات تقنية عملية.

📌 *تنويه*: هذه المراجع ليست إلزامية، لكنها نقطة انطلاق قوية لمن يريد التعمق أكثر بعد قراءة هذا الكتاب.

الخاتمة

في زمن تتسارع فيه التهديدات الرقمية وتتداخل التقنية مع كل تفاصيل حياتنا، أصبح الأمن السيبراني ضرورة لا خيار. هذا العمل يأتي كخطوة عملية تهدف إلى تمكين الأفراد من فهم أهم المفاهيم والممارسات التي تعزز الأمان الرقمي في بيئتهم اليومية.

هذا الكتاب ليس تأليفًا تقليديًا، بل هو **مبادرة واعية** قمت من خلالها بجمع وتنسيق محتوى متخصص من مصادر موثوقة في مجال الأمن السيبراني، ثم إعادة صياغته وتبسيطه بأسلوب عملي يخاطب القارئ العادي دون الإخلال بجوهر المعلومة.

أردت من خلال هذا الجهد أن أساهم في **ردم الفجوة بين المعلومة والتطبيق**، وبين التخصص والمجتمع. لم أعد إنتاج المحتوى فقط، بل انتقيته بوعي، ورتبته بهدف رفع الوعي وتوفير أداة تعليمية قابلة للنشر والتأثير.

أؤمن أن بناء وعي سيبراني مسؤول يبدأ من مبادرات حقيقية، وأن الأثر لا يُقاس بحجم المؤلفات بل **بمدى وصولها وفائدتها**.

للتواصل، الملاحظات، أو التعاون في مشاريع توعوية:

📧 **البريد الإلكتروني :** m@twal.sa

🔗 **X** : @m7mdatd

مع خالص التقدير،

محمد آل مشوط