أمن السيبراني للمبتدئين

AMEER. SEC

Rtum4

https://t.me/sec4hack

المقدمة

مرحبًا بك في رحلة تعلمٍ أساسيات الأمن السيبراني! هذا الكتاب مُصمم خصيصًا لك إذا كنت جديدًا على هذا العالم. سنشرح كل شيء بلغة بسيطة، بعيدًا عن التعقيدات التقنية. هدفنا هو مساعدتك على حماية نفسك في العالم الرقمي بثقة وسهولة.

ولن نتوقف عند هذا الحد، ففي نهاية الكتاب ستجد خريطة واضحة لمسارك في الأمن السيبراني

الفصل 1: مقدمة في الأمن السيبراني

ما هو الأمن السيبراني؟

الأمن السيبراني هو ببساطة "الممارسة التي تحمي أجهزتك، وشبكاتك، وبياناتك من الهجمات الرقمية أو السرقة أو التلف."
لكن في الحقيقة، الأمن السيبراني أوسع من مجرد حماية جهازك، فهو يشمل:

التقنيات (مثل مضادات الفيروسات والتشفير).

الأشخاص (وعي المستخدمين وتدريبهم).

العمليات والسياسات (مثل خطط الاستجابة للحوادث، وضوابط حماية الشركات).

يمكن تشبيهه بـ"**نظام المناعة**" الرقمي: مجموعة من الإجراءات التي تعمل على درء الفيروسات والمخترقين تمامًا كما يحميك جسمك من الأمراض.

لماذا هو مهم اليوم؟

لأن حياتنا كلها تقريبًا أصبحت مرتبطة بالإنترنت! من العمل والدراسة إلى التسوق والتواصل مع الأصدقاء، أصبحت بياناتنا الشخصية (صورنا، أرقام بطاقاتنا، محادثاتنا) مخزّنة على الشبكات.
حماية هذه البيانات أصبحت مسؤولية شخصية مثل إقفال باب منزلك عند الخروج.

إضافة لذلك:

الجرائم المالية الإلكترونية (مثل سرقة الحسابات البنكية أو بطاقات الائتمان) أصبحت من أكثر أشكال الجريمة انتشارًا.

حتى الدول أصبحت تعتبر الأمن السيبراني جزءًا من أمنها القومي، لأنه يرتبط بالطاقة، الصحة، والاقتصاد.

Rtum4

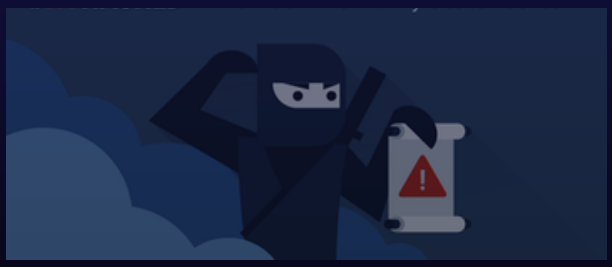
الفصل 1: مقدمة في الأمن السيبراني

قصص بسيطة عن اختراقات مشهورة

اختراق فيسبوك (**2021**): تسربت بيانات أكثر من 500 مليون مستخدم، بما في ذلك أرقام الهواتف وتواريخ الميلاد. لم يتم اختراق كلمات المرور، ولكن هذه المعلومات كافية للمخترقين لاستخدامها في عمليات التصيد أو سرقة الهوية.

هجوم (**2017**) **WannaCry**: فيروس فدية جعل أجهزة الضحايا غير قابلة للاستخدام وطالب بمبالغ مالية مقابل فك التشفير. أصاب أكثر من 200,000 جهاز حول العالم، بما في ذلك أجهزة في المستشفيات، مما أظهر كيف يمكن لهجوم إلكتروني أن يؤثر على حياة الناس مباشرة.

اختراق ياهو (**2013–2014**): أكبر عملية اختراق بيانات في التاريخ، حيث سُرقت معلومات أكثر من 3 مليار حساب.



هجوم (**2021**) **Colonial Pipeline**: هجوم فدية عطّل أكبر خط أنابيب نفطي في الولايات المتحدة، وتسبب بأزمة وقود في عدة ولايات، مما أثبت أن الأمن السيبراني لا يؤثر فقط على الأفراد بل على دول بأكملها.

Rtum4

الفصل 2: التهديدات التي تواجهك يوميًا

الأمن السيبراني يبدأ بفهم طبيعة التهديدات اللي تواجهك كل يوم. ومعظم الهجمات تعتمد على استغلال أخطاء المستخدم أو ثغرات بسيطة في الأجهزة والبرامج.

الفيروسات والبرمجيات الخبيثة (Malware)

هي برامج ضارة تُصمم لإلحاق الضرر بجهازك أو سرقة بياناتك. ومن أبرز أنواعها:

الفيروسات (**Viruses**): تنتشر عبر الملفات المصابة وتُحدث خللًا في النظام.

التروجان (**Trojans**): برنامج يبدو مفيدًا لكنه يخفي وظيفة ضارة (مثل سرقة كلمات المرور).

الديدان (**Worms**): تنتشر تلقائيًا عبر الشبكات بدون تدخل المستخدم.

برامج التجسس (**Spyware**): تراقب أنشطتك وتجمع بياناتك دون علمك.

فيروسات الفدية (**Ransomware**): تحبس ملفاتك عبر التشفير وتطلب مبلغًا ماليًا لفكها.

Rtum4

غالبًا ما تنتقل هذه البرمجيات عند تحميل ملفات من مصادر غير موثوقة، أو عبر مرفقات البريد الإلكتروني المزيفة.

الفصل 2: التهديدات التي تواجهك يوميًا

Rtum4

التصيد (Phishing)

هو انتحال شخصية مؤسسة موثوقة (مثل **البنك** أو **فيسبوك**) لخداعك وإجبارك على الكشف عن معلومات حساسة مثل كلمات المرور أو أرقام البطاقة الائتمانية.

أشكاله الحديثة: لم يعد يقتصر على الإيميل، بل صار يظهر في رسائل **SMS**، **واتساب**، **إنستغرام**، أو حتى إعلانات مزيفة في محركات البحث.

علاماته: رسائل تحتوي على روابط مشبوهة، أخطاء إملائية، أو تهديدات مثل "سيُغلق حسابك إذا لم تدخل بياناتك الآن".

سرقة الهوية وكلمات المرور

تحدث عندما يحصل المجرم على معلوماتك الشخصية (الاسم، العنوان، رقم الهوية، تاريخ الميلاد) وينتحل شخصيتك لفتح حسابات أو القيام بعمليات شراء باسمك.

أحيانًا تكفي صورة بطاقة هوية منشورة على الإنترنت، أو بيانات مسربة من موقع ما.

الخطر الأكبر أن المهاجم قد يستخدم هويتك في أعمال غير قانونية

إعطاء أذونات غير ضرورية للتطبيقات (مثل تطبيق مصباح يطلب الوصول إلى الكاميرا والرسائل).

الفصل 2: التهديدات التي تواجهك يوميًا

wifi-hacker0.blogspot.com
WiFi HACKS

الاختراق عبر الواي فاي العام

شبكات الواي فاي العامة (في المقاهي أو المطارات) غالبًا ما تكون غير آمنة. يمكن للمخترق:

اعتراض البيانات التي ترسلها (مثل كلمات المرور والرسائل).

تنفيذ هجوم يُسمى **Man-in-the-Middle Attack**: أي التسلل بينك وبين الموقع الذي تزوره لقراءة أو تعديل البيانات.

خداعك عبر شبكات وهمية (مثلاً: بدل "**Airport_Free_WiFi**" ينشئ شبكة باسم مشابه).

الهندسة الاجتماعية (Social Engineering)

الهندسة الاجتماعية لا تعتمد على التقنية بقدر ما تعتمد على **التلاعب النفسي واستغلال الثقة.**

مثال: شخص يتصل بك ويدعي أنه من البنك ويطلب بياناتك.

أو موظف مزيف يتواصل معك عبر لينكدإن ليجمع معلومات حساسة.

Rtum4

الفصل 3: حماية أجهزتك

حماية أجهزتك هي خط الدفاع الأول في الأمن السيبراني. كثير من الهجمات تبدأ بثغرة صغيرة أو إهمال بسيط، لذلك الاهتمام بالجهاز نفسه يختصر عليك مشاكل كبيرة.

تحديثات النظام والبرامج

هذه هي أسهل وأهم خطوة للحماية! التحديثات لا تضيف ميزات جديدة فقط، بل تغلق ثغرات أمنية اكتشفها المطورون.

حدّث نظام التشغيل بانتظام (ويندوز، ماك، أندرويد، iOS).

لا تنسَ تحديث التطبيقات المهمة، خصوصًا المتصفحات مثل Chrome و Firefox.

حدّث الراوتر (Firmware)، لأنه جزء أساسي من شبكتك، وكثير من الهجمات تستغل أجهزة الراوتر القديمة.

مضاد الفيروسات وأدوات الحماية

يعمل مضاد الفيروسات كـ"شرطي" يراقب جهازك ويمنع البرمجيات الخبيثة من العمل. تأكد من تفعيله وإجراء فحوصات دورية.

Windows 10/11 يأتي مع Windows Defender، وهو جيد جدًا للمستخدم العادي.

لا تثبّت أكثر من مضاد فيروسات في نفس الجهاز، لأن ذلك يسبب تضاربًا ويبطئ الأداء.

برامج الهاتف لمضاد فايروسات / Dr.web لمراقبة شبكة /Fing

الجدار الناري (Firewall)

يمكن اعتباره "حارس البوابة"، فهو يراقب الاتصالات التي تدخل وتخرج من جهازك ويمنع أي اتصال مشبوه.
مفعّل تلقائيًا في أنظمة ويندوز وماك يُفضّل إبقاؤه دائمًا مفعّلًا

Rtum4

الفصل 3: حماية أجهزتك

النسخ الاحتياطي للملفات المهمة

النسخ الاحتياطي هو شبكة الأمان الأخيرة ضد الفقدان.

أنشئ نسخة من ملفاتك المهمة (الصور، المستندات) على قرص خارجي أو خدمة سحابية (Google Drive, iCloud).

اتبع مبدأ Backup 1-2-3:

3 نسخ من بياناتك.

2 على وسائط مختلفة.

1 خارج جهازك (سحابية أو منفصلة Offline).

حافظ على نسخة مفصولة (قرص خارجي غير متصل دائمًا) حتى لا يصاب بفيروسات الفدية.

Rtum4

الفصل 4: حماية حساباتك

الحسابات الإلكترونية هي مفاتيح حياتك الرقمية، وإذا تعرض واحد منها للاختراق، قد تُفتح بقية الحسابات بسهولة. لذلك حمايتها أولوية قصوى.

اختيار كلمة مرور قوية

اجعلها طويلة (12 حرفًا على الأقل).

استخدم مزيجًا من الأحرف الكبيرة والصغيرة والأرقام والرموز (!@#$%).

لا تستخدم كلمات يمكن تخمينها (مثل اسمك، تاريخ ميلادك، أو 123456).
لا تعيد استخدام نفس كلمة المرور في أكثر من حساب.

استخدم مدير كلمات مرور (Password Manager) مثل Bitwarden أو LastPass لتوليد وحفظ كلمات مرور قوية بدل الاعتماد على ذاكرتك.

لا تعتمد فقط على المتصفحات لحفظ كلمات المرور (مثل Chrome)، فهي أقل أمانًا من البرامج المتخصصة.

التعامل مع الإيميلات والرسائل المشبوهة

افحص عنوان المرسل: هل هو مطابق تمامًا للعنوان الرسمي للشركة؟ (مثل support@paypal.com وليس support@paypa1.com).

مرّر مؤشر الماوس على الرابط قبل الضغط عليه لمعرفة العنوان الحقيقي.

لا تضغط على الروابط أو المرفقات فجأة.

ابحث عن أخطاء إملائية أو نحوية: غالبًا ما تحتوي رسائل التصيد على أخطاء.

الفصل 4: حماية حساباتك

إذا كان فيه تهديد أو عجلة ("حسابك سيُغلق إذا لم...") فهو على الأغلب احتيال.

تذكّر أن التصيّد صار يُستخدم أيضًا في واتساب وتيليجرام، مو بس الإيميل.

يمكنك استخدام مواقع مثل **VirusTotal** لفحص الروابط والملفات المشبوهة قبل فتحها.

التوثيق الثنائي (2FA)

هذه هي الطبقة الثانية من الحماية بعد كلمة المرور. حتى إذا عرف أحدهم كلمة مرورك، لن يتمكن من الدخول إلى حسابك دون هذه الخطوة الإضافية.

1-لما تسوي تسجيل دخول، يوصلك رمز مؤقت برسالة نصية.

هذا الأكثر شيوعًا، لكنه أضعف لأن ممكن المهاجم يسرق خطك (هجوم اسمه SIM Swap).

2. Google Authenticator / Authy

تطبيق مجاني تنزله على الموبايل.

بدل ما تنتظر SMS، التطبيق يولّد لك رموز تتغير كل 30 ثانية.

أقوى من SMS لأنه ما يعتمد على الشبكة أو شريحة الهاتف.

3. Security Keys (مثل YubiKey)

جهاز صغير مثل USB.

توصله بالكمبيوتر (أو الموبايل) وقت تسجيل الدخول حتى يثبت إنك أنت صاحب الحساب.

يُعتبر أقوى طريقة توثيق حاليًا، خصوصًا لحسابات حساسة مثل البنوك أو الإيميل الرئيسي.

Rtum4

الفصل 5: التشفير ببساطة

ما معنى التشفير؟

التشفير هو عملية تحويل المعلومات إلى شفرة سرية حتى لا يتمكن أي شخص من قراءتها إلا من يملك "المفتاح" لفكها. يشبه إرسال رسالة سرية بلغة لا يفهمها سوى أنت والمستقبل.

أنواع التشفير ببساطة

التشفير المتماثل (**Symmetric**): نفس المفتاح يُستخدم للتشفير وفك التشفير. يشبه صندوق له مفتاح واحد فقط.

التشفير غير المتماثل (**Asymmetric**): مفتاح عام للتشفير ومفتاح خاص مختلف لفك التشفير. يشبه صندوق بريد: أي شخص يقدر يضع رسالة داخله (**مفتاح عام**)، لكن فقط صاحب الصندوق يقدر يفتح ويقرأ الرسالة (**مفتاح خاص**).

أمثلة من حياتنا اليومية

WhatsApp و **Signal**: تشفر محادثاتك "من طرف إلى طرف"، مما يعني أن حتى الشركة نفسها لا تستطيع قراءة رسائلك.

VPN: تشفر كل البيانات الخارجة من جهازك إلى الإنترنت، مما يحميك خاصة عند استخدام شبكات الواي فاي العامة.

بطاقات البنوك (Chip & PIN): عند الدفع ببطاقة، يتم تشفير المعلومات حتى البنك فقط هو القادر على قراءتها.

المواقع الآمنة (HTTPS): أي موقع يبدأ بـ https:// يستخدم التشفير لحماية بياناتك (مثل كلمات المرور أو بطاقات الدفع) أثناء انتقالها بينك وبين الموقع.

Rtum4

الفصل 5: التشفير ببساطة

مثال عملي للتشفير (تشفير القيصر)

تخيل عندك رسالة:

HELLO <

باستخدام مفتاح رقم (3)، كل حرف يتحرك 3 خطوات للأمام في الأبجدية:

H → K

E → H

L → O

O → R

فتصير الرسالة المشفرة:

KHOOR <

لفك التشفير، لازم تعرف المفتاح (3) وترجع الحروف 3 خطوات للوراء.

🔑 هذا مثال بسيط، لكن المبدأ نفسه يُستخدم في التشفير الحديث، مع مفاتيح معقدة جدًا تجعل من المستحيل كسرها بالطرق التقليدية.

كيف يحمي بياناتك؟

التشفير يجعل البيانات غير مفهومة للمتطفلين. حتى إذا اعترضها مهاجم أو مزود خدمة الإنترنت، لن يستطيع قراءتها بدون المفتاح الصحيح. النتيجة: بياناتك تبقى آمنة بينك وبين المستقبل فقط.

Rtum4

الفصل 6: أدوات مجانية ونصائح عملية

VPN مجاني/مدفوع

ما هو: خدمة تخفي عنوان IP الخاص بك وتشفر اتصالك بالإنترنت.

المجاني: مثل ProtonVPN – جيد للاستخدام الأساسي، لكنه محدود السرعة والبيانات.

المدفوع: مثل NordVPN أو ExpressVPN – يوفر سرعة أعلى، خوادم أكثر، وموثوقية أكبر.

🔑 **نصائح**:

استخدم VPN فقط من الشركات المعروفة، لأن بعض التطبيقات "المجانية" تجمع بياناتك بدل حمايتك.

لا تعتمد على VPN لوحده كوسيلة حماية، هو مجرد طبقة إضافية.

مواقع لفحص الاختراقات

Have I Been Pwned: أدخل بريدك الإلكتروني لترى إذا كان ضمن بيانات مسربة. إذا ظهر، غيّر كلمة المرور فورًا لذلك الحساب.

Firefox Monitor: خدمة مشابهة تفحص الإيميل وتعطي نصائح للأمان.

🔑 **نصائح**:

إذا اكتشفت أن إيميلك مخترق، غيّر كلمة المرور فورًا وفعل التوثيق الثنائي.

لا تستخدم نفس كلمة المرور لأكثر من حساب.

Rtum4

الفصل 6: أدوات مجانية ونصائح عملية

نصائح عامة لتجنب الاختراقات

لا تضغط على أي رابط قبل التأكد منه:

مرّر المؤشر على الرابط لترى العنوان الحقيقي.

إذا كان الرابط مشبوه، افحصه باستخدام مواقع مثل **VirusTotal** أو **PhishTank** قبل فتحه.

لا تحمّل ملفات من أي موقع عشوائي:

نزّل البرامج فقط من الموقع الرسمي أو المتاجر الموثوقة (مثل **Google Play, App Store**).

إذا اضطررت لتحميل ملف من مصدر غير معروف، افحصه أولًا في **VirusTotal** أو مضاد الفيروسات.

التسوق الآمن: لا تدخل بيانات بطاقتك إلا في مواقع تستخدم https://.

الحذر من USB مجهول: لا توصل أي ذاكرة خارجية بجهازك إلا إذا كنت تعرف مصدرها.

نسخ احتياطي دوري: حافظ على نسخة احتياطية لملفاتك المهمة في مكان منفصل.

تحديث البرامج: أبقِ نظامك وتطبيقاتك محدثة دائمًا لتجنب استغلال الثغرات.

Rtum4

مسار الكامل في امن سيبراني

CompTIA +A

+

لغة python

ثم

CompTIA Network

+

نظام كالي لينيكس

ثم

CompTIA security

تتعلم معها لغة SQL

ثم تتجة لأحد هاتين مسارين وتتعلمه لما تبقى من عمرك
ويمكنك دمج بينهما وهذا يرجع لك

Red team **Blue team**

Rtum4

مسارك في هاتين مجالين

Red team	Blue team
eJPT	BTL1
PenTest	cryptography
CEH	digital forensics
OSCP	CISSP

Rtum4

Cybersecurity Certifications

©Cyber Edition

©Cyber Edition

Blue Team

Beginner

Security+ | CSA | eCDFP | BTL1

Advanced

CASP+ | GCFA

Intermediate

CySA+ | BTL2 | eCTHP | CCD | CDSA | OSDA | GCIH | eCIR

Red Team

Beginner

PNPT | CBBH | eJPT | CRTP | CEH

Advanced

OSMR | OSED | CRTO

Intermediate

OSCP | OSWP | OSWA | OSEP | CPTS

Expert

OSCE3 | OSEE | OSWE

Novice

KLCP

InfoSec

Intermediate

CRISC | CISA | CISM

Advanced

CGEIT | CISSP