

IBM Plex Sans Arabic

الجرائم الإلكترونية: التاريخ، التهديدات، ودليل الحماية

من الوعي بالمشكلة إلى استراتيجيات الدفاع النشط Cairo



ما هي الجريمة الإلكترونية؟

هي استخدام الكمبيوتر الآلي للاستيلاء على البيانات أو تغييرها، أو الحصول على خدمات أو استخدام أجهزة بشكل غير قانوني.

Synonyms/Context

تعرف أيضاً بـ •

Cyber Crime, E-crime,

Hi-tech crime

مع الانتشار الواسع للأجهزة التكنولوجية،
شهدت هذه الجرائم زيادة هائلة. •



لماذا تُعد الجرائم الإلكترونية أكثر خطورة؟



سهولة التعلم: من السهل تعلم كيفية ارتكابها.



الموارد مقابل الضرر: تتطلب موارد قليلة جدًا مقارنة بحجم الضرر الهائل الذي تسببه.

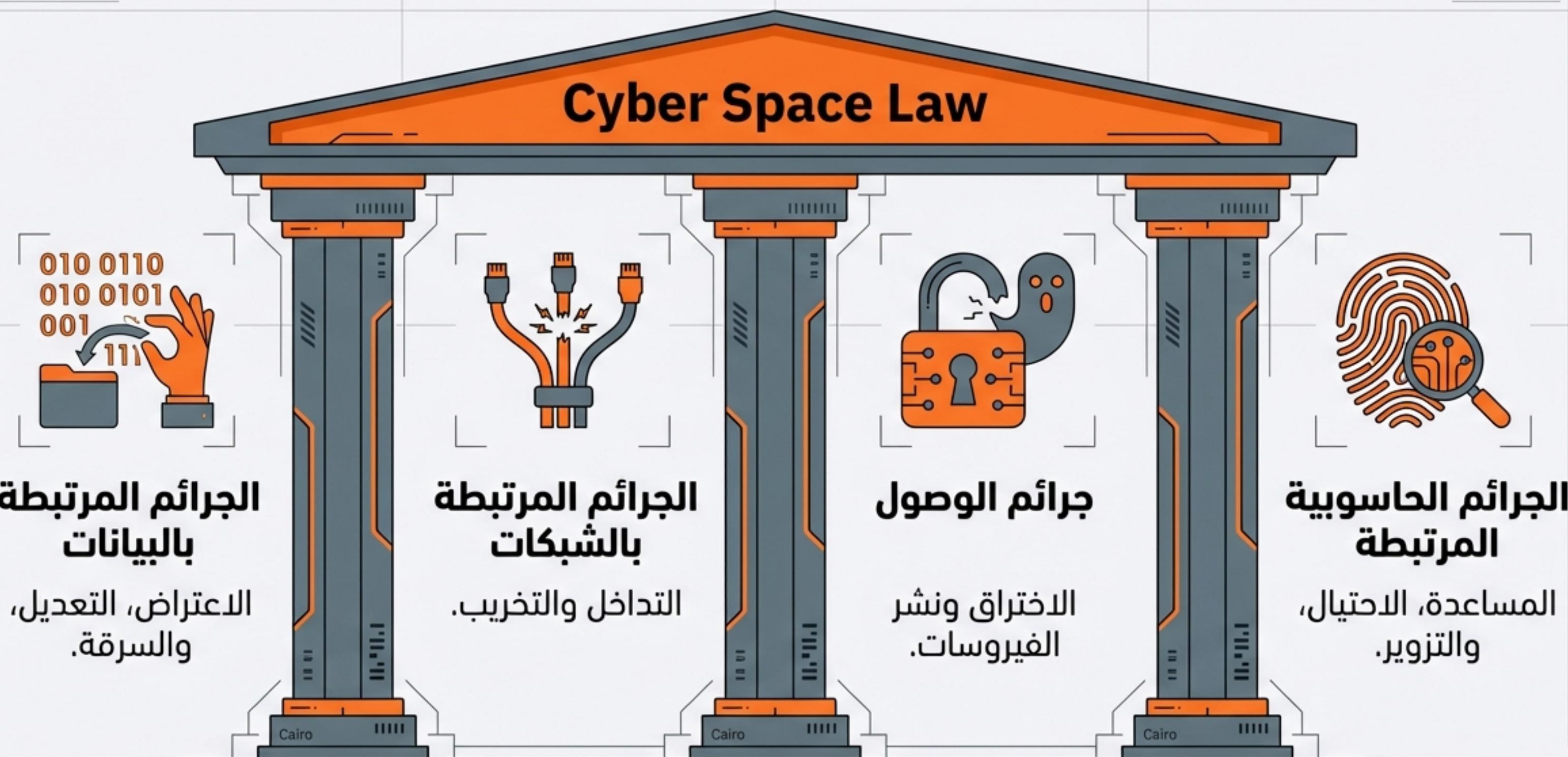


عن بعد: يمكن ارتكابها من أي ولاية قضائية دون الحاجة للتواجد الجسدي.

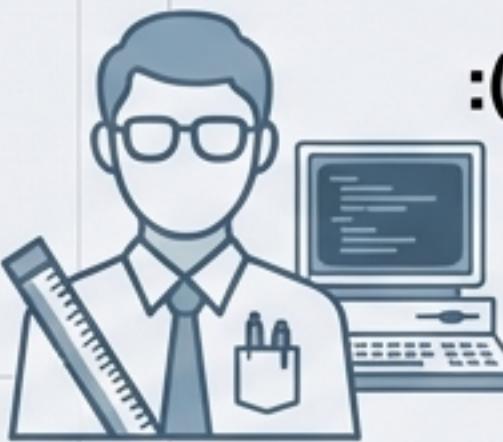


الغموض القانوني: غالباً ما تكون غير مذكورة بوضوح في القوانين التقليدية.

الأركان الأربع للجريمة الإلكترونية



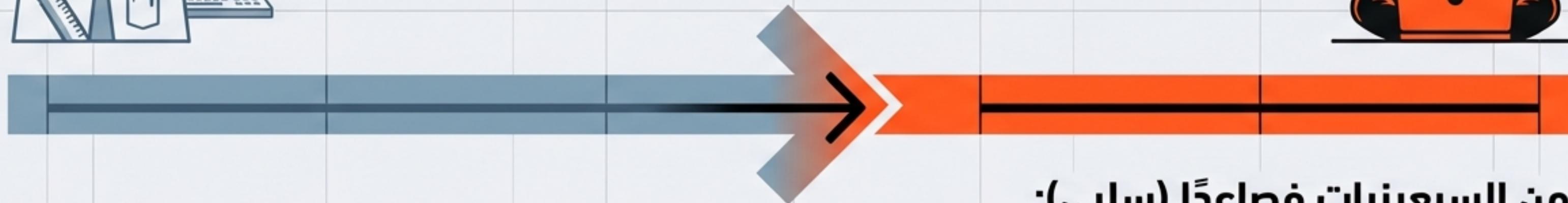
تطور مفهوم "الهاكر": من خبير إلى مجرم



الستينيات والسبعينيات (إيجابي):
خبير يمتلك معرفة عميقة
بالبرمجة وأنظمة التشغيل.



من السبعينيات فصاعداً (سلبي):
شخص يستخدم الحاسب بدون تصريح، أو
يرتكب جرائم.



من يهدد أمنك الرقمي؟



الهاكر (Hacker)

شخص يصل إلى موارد الحاسب بدون تصريح.



الكراكر (Cracker)

هاكر يستخدم مهاراته لارتكاب أعمال غير قانونية أو التخريب المعتمد.



المبتدئون (Script Kiddies)

هاكر يقوم بتحميل 'سكريبتات' جاهزة واستخدامها للتخريب دون فهم حقيقي لكيفية عملها.



المخربون (Vandals)

أشخاص هدفهم تدمير الممتلكات الرقمية.

مدحّات تاريخية في الجريمة الإلكترونية

Case Files



(Morris Worm) 1988: دودة الانترنت

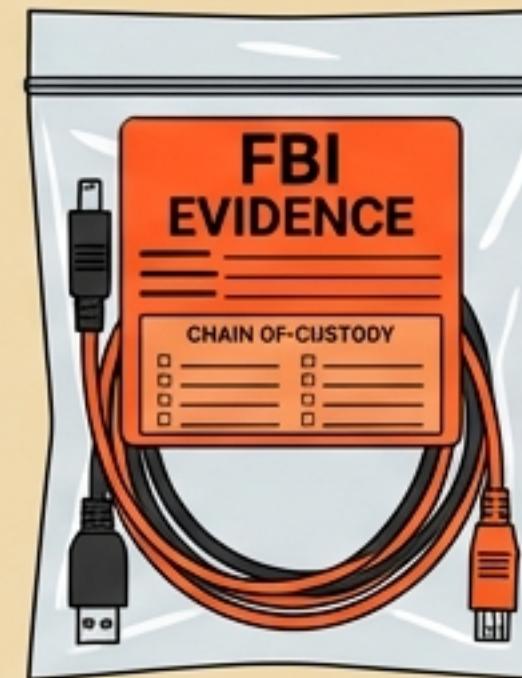


أول هجوم كبير. استغل ثغرة أمنية، نسخ نفسه تلقائياً، وأوقف الانترنت لمدة يومين. تكلفة الإصلاح: 5 ملايين دولار.

Case Files

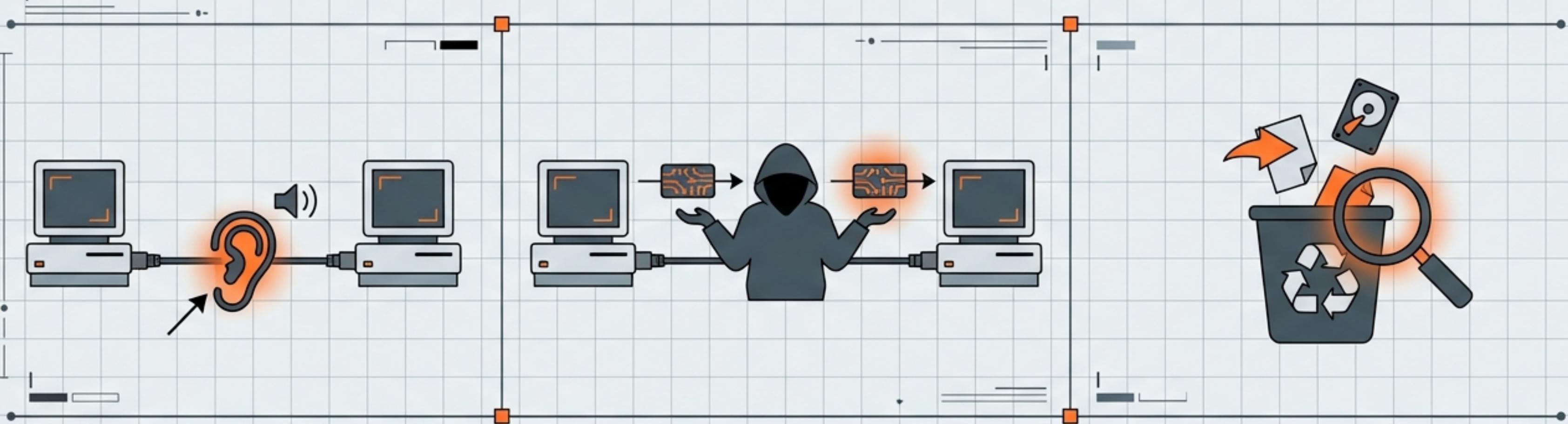


(The First Conviction) 1994: كيفن ميتنيك



استخدمت تكنولوجيا IP Spoofing لسرقة ملفات وبرامج أمان من الخبرير شيمومورا. تم القبض عليه بواسطة الـ FBI.

كيف يحدث الاختراق؟



التنصت (Passive):
مراقبة البيانات بصمت.

هجوم الوسيط:
اعتراض وتعديل الاتصال بين
طرفين بشكل نشط.

البحث في المهملات:
البحث في المخلفات العادية
عن كلمات مرور أو بيانات.

الإنترنت: أحياe غير آمنة



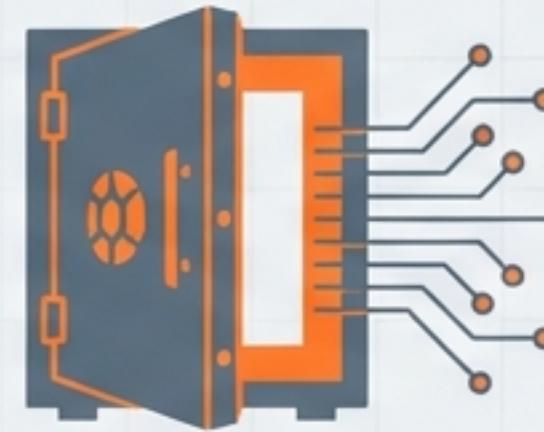
"أصبحت طرقات الإنترنت مثل الأحياء التي لم يعد من الآمن دخولها.
الهاكرز والمحталون يتربصون في الظلال." (Paul Tinnirello.)

رؤية للمستقبل (بروس شناير):
ستزداد الاختراقات لأن البنية التحتية تنتقل للإنترنت، ولأن الأنظمة تزداد تعقيداً.
التكنولوجيا ظورت على أساس "الثقة" وليس الأمان.

الهدف: أموالك و هو يتك

خسائر البنوك

البنوك الكبرى تخصل ملايين الدولارات احتياطياً لتغطية خسائر الاحتيال الإلكتروني.



سرقة الهوية (Identity Fraud) - علامات التحذير



- رفض القروض رغم سجلك الائتماني الجيد.
- ظهور معاملات مالية لا تعرفها.
- اختفاء بريدك المتوقع من المؤسسات المالية.

دليل الحماية (1): النظافة الرقمية



الحماية من الفيروسات

التحديث الدوري لمكافحة الفيروسات ضروري، لا تكتف بالتنزيل فقط.



النسخ الاحتياطي (Backups)

قم به بانتظام لضمان عدم فقدان كل شيء عند الكارثة.

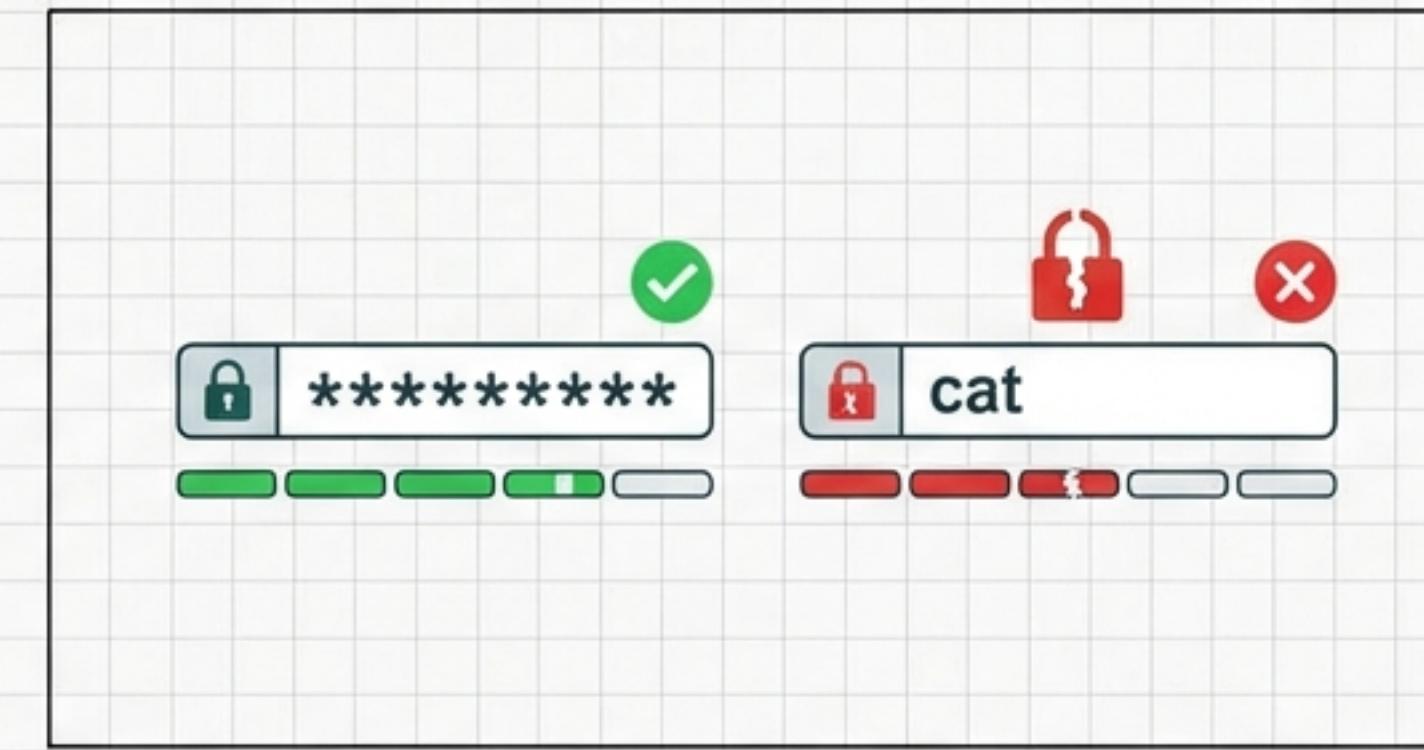
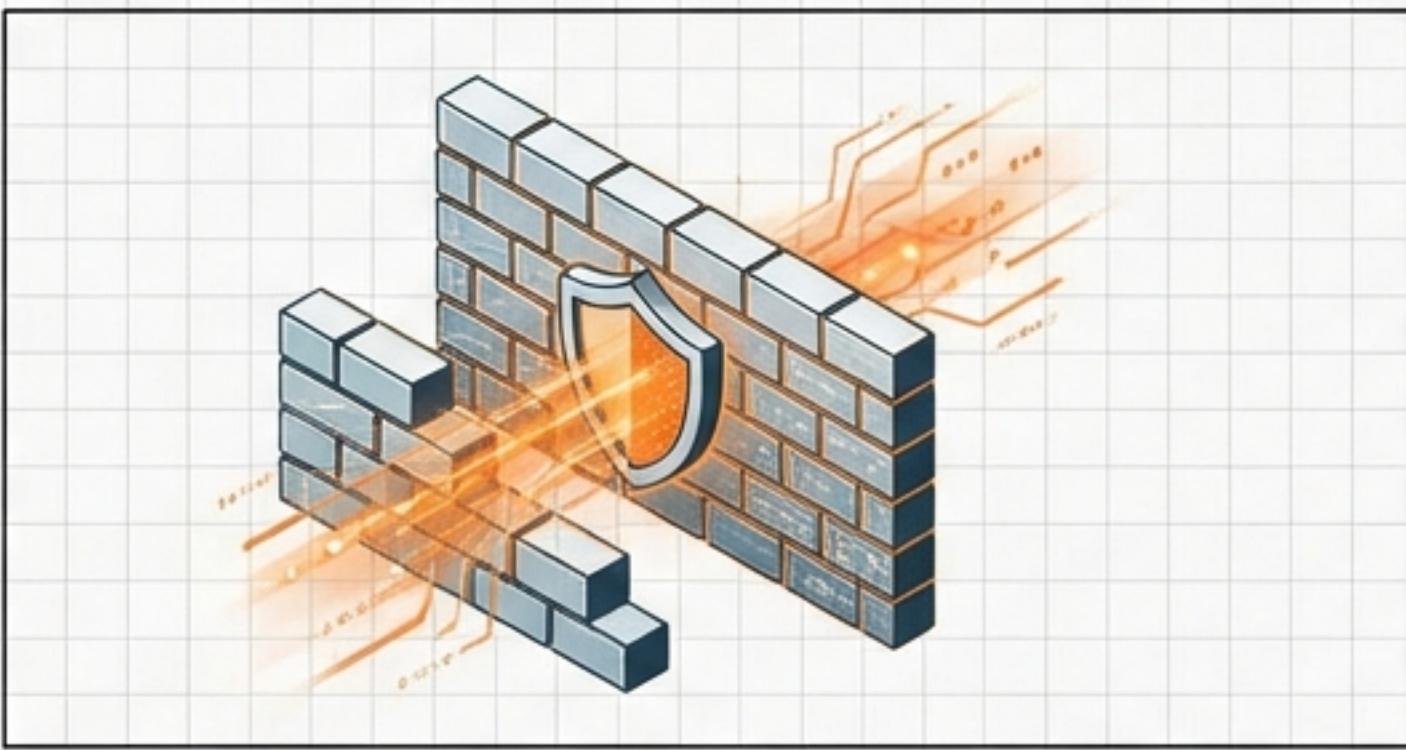


التعامل مع البريد المزعج (Spam)

تأكد من خيارات الموافقة/الرفض في النماذج. احذر من زر "Unsubscribe" في الرسائل المبئث المجهولة.



دليل الدعماية (2): تدريب القلعة



الجدار الناري (Firewall):
تأكد من تفعيل جدار حماية شخصي ولا تتصل
بإنترنت بدونه.

كلمات المرور:

- اجعلها طويلة قدر الإمكان.
- لا تستخدم كلمات شائعة مثل 'dog' أو 'cat'.
- لا تحفظ كلمات المرور (Save Password) على
أجهزة الكمبيوتر المشتركة.

دليل الحماية (3): التعاملات المالية الآمنة



التسوق الآمن:

- ابحث دائمًا عن رمز القفل (Padlock) قبل إدخال بيانات البطاقة.
- اشتري من شركات معروفة.



: (Phishing Rule)

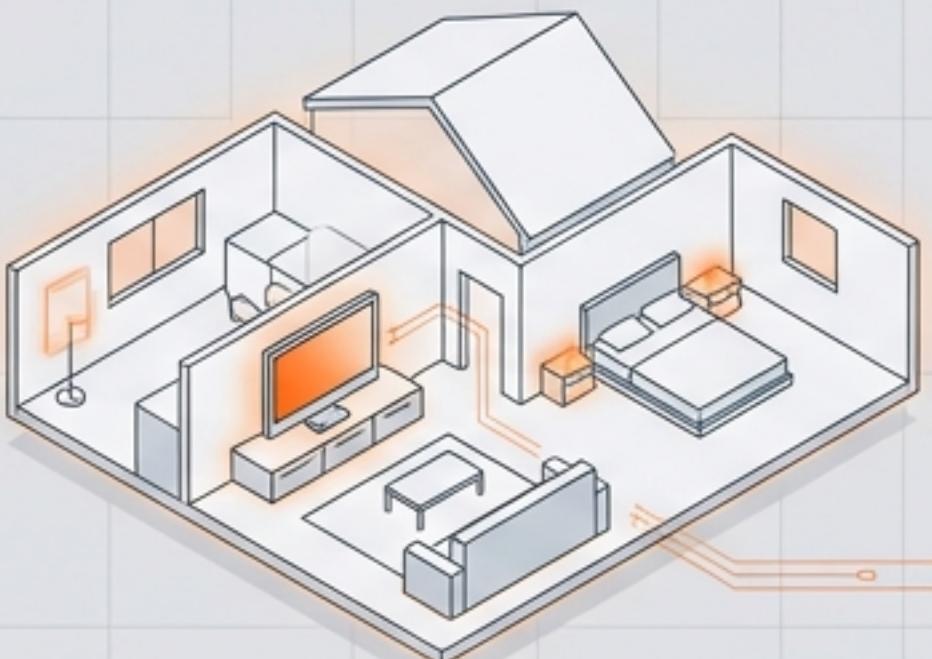


- البنك الحقيقي لا يطلب أبدًا كلمة المرور أو PIN عبر البريد أو الهاتف.
- إذا وصلك رابط لتحديث البيانات، فهو احتيال.

IBM Plex Sans Arabic

دليل الحماية (4): الأسرة والمستندات المادية

المنطقة 1: الأسرة



حماية الأطفال: Cairo

استخدم برامج الرقابة الأبوية. ضع الكمبيوتر في منطقة مشتركة (غرفة المعيشة) للإشراف.

المنطقة 2: المستندات المادية



المستندات الورقية: Cairo

العصابات تبحث في القمامة. مزق المستندات الشخصية قبل رميها لمنع سرقة الهوية.

الخلاصة: كن يقطعاً



**لا يكفي أن نحمي أنفسنا بالقوانين؛ علينا أن نحمي أنفسنا بالرياضيات (التشغير والتكنولوجيا)."

— بروس شناير