🔵 دليل الصحفي للتعامل مع الهجمات المالية والتخريبية

🎯 ما هو هذا النوع من الهجمات؟

هذا النوع يستهدف:

- الأموال
- الملفات والبيانات
- سير العمل الصحفي بالكامل

ويهدف إلى:

- ابتزاز الصحفي
- تعطيل عمله
- تدمير أرشيفه المهني

📌 تشير الدراسات إلى أن الهجمات مثل الفدية والابتزاز أصبحت من أكثر التهديدات تطورًا في البيئة الرقمية الحديثة (Khan, 2025).

💰 السيناريو 1: الابتزاز الإلكتروني (Blackmail)

🚨 كيف يحدث:

- تهديد بنشر معلومات خاصة
- صور أو رسائل أو ملفات
- طلب مال أو توقف عن العمل

⚠️ العلامات:

- رسائل تهديد مباشرة
- تحديد وقت نهائي للدفع
- استخدام معلومات شخصية دقيقة

⚡ ماذا تفعل فورًا:

1. لا تدفع أي مبلغ
2. لا تفاوض المهاجم
3. احتفظ بكل الأدلة (صور + محادثات)
4. غيّر كلمات المرور فورًا

🧯 إدارة الموقف:

- أبلغ فريقك أو مؤسسة إعلامية

- توثيق التهديد قانونيًا
- تقليل نشاطك الرقمي مؤقتًا

❌ أخطاء قاتلة:

- الدفع للمبتز (يشجعه على الاستمرار)
- حذف الرسائل

🧨 السيناريو 2: هجمات الفدية (Ransomware)

🎯 ما هي:

برمجيات تقوم بـ:

- قفل جهازك أو ملفاتك
- طلب مال مقابل فك التشفير

📌 تعتبر من أخطر الهجمات عالميًا بسبب قدرتها على تعطيل العمل بالكامل (Sun, 2024).

🚨 علامات الإصابة:

- ظهور رسالة "تم تشفير ملفاتك"
- عدم القدرة على فتح الملفات
- بطء شديد أو توقف الجهاز

⚡ ماذا تفعل فورًا:

1. افصل الجهاز عن الإنترنت فورًا
2. لا تعيد تشغيل الجهاز بشكل عشوائي
3. لا تدفع الفدية
4. استعن بخبير تقني

🧯 الاسترجاع:

- استخدام النسخ الاحتياطية
- إعادة تثبيت النظام
- استرجاع الملفات من نسخة آمنة

🛡️ الوقاية:

- نسخ احتياطي خارجي (Offline Backup)
- تحديث النظام باستمرار
- عدم فتح ملفات مجهولة

📂 السيناريو 3: فقدان أو تدمير البيانات

🚨 كيف يحدث:

- حذف متعمد
- اختراق
- عطل تقني
- تشفير ملفات

⚡ ماذا تفعل فورًا:

1. توقف عن استخدام الجهاز
2. لا تحفظ بيانات جديدة عليه
3. حاول استرجاع الملفات

🧯 استراتيجيات الاسترجاع:

- برامج استعادة البيانات
- نسخ احتياطية سحابية
- أقراص خارجية

🛡️ الوقاية:

- قاعدة 3-2-1:
- 3 نسخ من البيانات
- 2 وسائط مختلفة
- 1 نسخة خارج الجهاز

📌 الأبحاث تشير إلى أن ضعف إدارة البيانات يزيد من أثر الهجمات الرقمية بشكل كبير (Sun, 2024).

🏦 السيناريو 4: اختراق الحسابات المالية

🚨 كيف يحدث:

- روابط تصيد للبنوك
- سرقة بيانات الدفع
- استخدام كلمات مرور ضعيفة

⚡ ماذا تفعل فورًا:

1. أوقف البطاقة أو الحساب فورًا
2. تواصل مع البنك
3. راجع العمليات الأخيرة
4. غيّر جميع كلمات المرور

🛡️ الوقاية:

- تفعيل التنبيهات البنكية
- عدم استخدام نفس كلمة المرور
- عدم حفظ بيانات البطاقة في المتصفح

🧠 القاعدة الذهبية لهذا القسم

✔ لا تدفع للمهاجم
✔ لا تتفاعل تحت الضغط
✔ النسخ الاحتياطي أهم من أي برنامج حماية

📋 بروتوكول الحماية المالية للصحفي

- ✔ نسخ احتياطي خارجي دائم
- ✔ فصل الحسابات المالية عن العمل
- ✔ مراقبة الحسابات بشكل دوري
- ✔ استخدام أجهزة موثوقة فقط للمعاملات المالية

🧾 الخلاصة

الهجمات المالية والتخريبية لا تستهدف الصحفي فقط، بل تستهدف قدرته على الاستمرار في العمل — والوقاية تعتمد على النسخ الاحتياطي والوعي والاستجابة السريعة.