🔴 دليل الصحفي للتعامل مع الاختراق والسيطرة المباشرة

🎯 ما هو هذا التهديد؟

هو أخطر أنواع الهجمات، حيث يتمكن المهاجم من:

- الدخول إلى حساباتك
- التحكم في جهازك
- قراءة رسائلك
- انتحال شخصيتك

📌 تشير الأبحاث إلى أن هذه الهجمات غالبًا تبدأ عبر التصيد أو استغلال أخطاء بشرية (Tagani et al., 2024)، (Jari, 2022).

🧨 السيناريو 1: اختراق حساب (بريد / فيسبوك / واتساب)

🚨 علامات الاختراق:

- وصول إشعارات تسجيل دخول من مواقع غريبة
- إرسال رسائل لم ترسلها
- تغيير كلمة المرور دون علمك

⚡ ماذا تفعل فورًا (خلال أول 10 دقائق):

1. استخدم جهاز آخر آمن (ليس المخترق)
2. غيّر كلمة المرور فورًا
3. فعّل التحقق الثنائي (2FA)
4. سجّل الخروج من كل الأجهزة
5. راجع "نشاط تسجيل الدخول"

🧯 ماذا تفعل خلال أول ساعة:

- أبلغ فريقك أو مؤسستك
- حذّر مصادرك من التواصل مع الحساب
- راجع الرسائل المرسلة (هل تم استهداف مصادر؟)

🛡️ الوقاية:

- كلمة مرور طويلة وفريدة (12+ حرف)
- مدير كلمات مرور
- لا تضغط روابط غير موثوقة

❌ أخطاء قاتلة:

- محاولة حل المشكلة من الجهاز المخترق
- تجاهل الاختراق البسيط

🧨 السيناريو 2: اختراق الجهاز (هاتف أو لابتوب)

🚨 علامات:

- بطء مفاجئ
- حرارة غير طبيعية
- تطبيقات لم تثبتها
- استهلاك بيانات مرتفع

⚡ التصرف الفوري:

1. افصل الإنترنت فورًا
2. فعّل وضع الطيران
3. لا تفتح أي ملفات
4. لا تكتب كلمات مرور

🧯 خطوات المعالجة:

- فحص الجهاز ببرنامج موثوق
- نسخ البيانات المهمة فقط
- إعادة ضبط المصنع (Factory Reset)

📌 تشير الدراسات إلى أن الهجمات المتقدمة قد تبقى مخفية لفترات طويلة (Sun, 2024).

🛡️ الوقاية:

- تحديث النظام باستمرار
- تثبيت التطبيقات من مصادر رسمية فقط
- عدم استخدام USB مجهول

🧨 السيناريو 3: التصيد الاحتيالي (Phishing)

🎯 كيف يحدث:

- رسالة تبدو رسمية (بنك / منصة / صديق)
- رابط مزيف

- طلب إدخال كلمة المرور

📌 التصيد هو أكثر الهجمات شيوعًا عالميًا (V et al., 2024).

🚨 علامات:

- رابط غريب
- ضغط نفسي ("تحرك الآن")
- أخطاء لغوية

⚡ ماذا تفعل:

- لا تضغط الرابط
- تحقق من المصدر
- افتح الموقع يدويًا

🛡️ الوقاية:

- تدريب نفسك على كشف الروابط
- استخدام إضافات حماية المتصفح

❌ أخطاء:

- الثقة في الرسائل "العاجلة"
- إدخال كلمة المرور بسرعة

🧨 السيناريو 4: التجسس عبر التطبيقات

🚨 علامات:

- تطبيق يطلب صلاحيات غير منطقية
- وصول للكاميرا/الميكروفون بدون سبب

⚡ ماذا تفعل:

- احذف التطبيق فورًا
- راجع صلاحيات التطبيقات
- حدّث النظام

📌 برامج التجسس تستهدف الصحفيين بشكل خاص لحساسية عملهم (Di Salvo, 2021).

🧨 السيناريو 5: التنصت على الاتصالات

🚨 علامات:

- صدى في المكالمات
- انقطاع متكرر
- نشاط غير طبيعي

⚡ ماذا تفعل:

- توقف عن مناقشة معلومات حساسة
- انتقل لتطبيق مشفر (Signal)
- غيّر الجهاز إذا لزم

🛡️ الوقاية:

- استخدام التشفير دائمًا
- عدم استخدام الشبكات العامة

🧠 القاعدة الذهبية لهذا القسم

✔ تصرّف بسرعة
✔ لا تثق بالجهاز المصاب
✔ افترض أن المهاجم لديه وصول كامل

📋 قائمة الطوارئ (احتفظ بها دائمًا)

- جهاز بديل آمن
- كلمات مرور احتياطية
- وسيلة تواصل بديلة
- نسخة احتياطية من البيانات

🧾 الخلاصة

الهجمات المباشرة تعتمد غالبًا على خطأ بسيط، لكن الاستجابة السريعة والواعية يمكن أن تمنع كارثة كبيرة.