⚪ دليل الصحفي للتعامل مع الأخطاء البشرية والاستهداف غير المباشر

🎯 ما هو هذا النوع من التهديدات؟

هذا النوع لا يعتمد على اختراق تقني مباشر، بل على:

- خداع الصحفي
- استغلال الثقة
- الإعلانات والرسائل الموجهة
- أخطاء بسيطة في الاستخدام

📌 تشير الدراسات إلى أن العامل البشري هو الحلقة الأضعف في الأمن السيبراني، وأن معظم الهجمات تنجح عبره وليس عبر التقنية نفسها (Jari, 2022), (Tagani et al., 2024).

🧠 السيناريو 1: الهندسة الاجتماعية (Social Engineering)

🎯 كيف يحدث:

المهاجم لا يخترق جهازك، بل يخترق **ثقتك** عبر:

- انتحال شخصية مسؤول
- طلب عاجل لمعلومة
- استغلال الضغط النفسي

🚨 علامات الخطر:

- طلب "سري وعاجل"
- شخص يدّعي أنه زميل أو مسؤول
- استعجال غير منطقي

⚡ ماذا تفعل:

1. تحقق من هوية الشخص عبر قناة ثانية
2. لا تقدم أي معلومات فورًا
3. اسأل: "لماذا يطلب هذا الآن؟"
4. وثّق الطلب

🛡️ الوقاية:

- قاعدة: "لا ثقة بدون تحقق"
- استخدام قنوات رسمية فقط
- تدريب نفسك على كشف الطلبات المشبوهة

📢 السيناريو 2: الاستهداف عبر الإعلانات

🎯 كيف يحدث:

- إعلانات خبيثة
- روابط تبدو رسمية
- صفحات مزيفة تشبه مواقع معروفة

🚨 علامات:

- إعلان يعد بجائزة أو خبر عاجل
- رابط طويل أو غريب
- طلب تسجيل دخول مفاجئ

⚡ ماذا تفعل:

- لا تضغط أي إعلان مشبوه
- ادخل للموقع يدويًا
- استخدم مانع إعلانات (Ad Blocker)

🛡️ الوقاية:

- تحديث المتصفح باستمرار
- استخدام وضع الحماية في المتصفح
- تجنب الضغط على الإعلانات

🚫 السيناريو 3: تعطيل أو حظر الحسابات

🎯 كيف يحدث:

- بلاغات جماعية ضد حسابك

- انتهاك مزيف لسياسات المنصات
- حملات منظمة لإسكاتك

📌 هذا الأسلوب يستخدم ضد الصحفيين لتقليل وصولهم للجمهور.

⚡ ماذا تفعل:

1. توثيق الحساب مسبقًا إن أمكن
2. تقديم اعتراض رسمي
3. إنشاء قناة بديلة للطوارئ
4. إبلاغ الجمهور عبر وسيلة أخرى

🛡️ الوقاية:

- وجود أكثر من منصة
- بناء جمهور متعدد القنوات
- حفظ قائمة المتابعين المهمين خارج المنصة

🧩 السيناريو 4: الاستهداف الممنهج طويل المدى

🎯 ما هو:

هجمات لا تحدث مرة واحدة، بل:

- مراقبة طويلة
- اختبارات لاختراقك
- جمع معلومات تدريجيًا

📌 الهدف: بناء ملف كامل عن الصحفي قبل استهدافه.

⚡ ماذا تفعل:

- تغيير الروتين الرقمي
- تقليل المعلومات العامة عنك
- مراجعة دورية لأمانك الرقمي

📌 تشير الأبحاث إلى أن الهجمات الحديثة تعتمد على جمع البيانات تدريجيًا لبناء نمط حياة الضحية (Sun, 2024).

🧠 القاعدة الذهبية لهذا القسم

✔ معظم الهجمات تبدأ بخطأ بسيط منك
✔ لا توجد معلومة "غير مهمة" في الإنترنت
✔ كل طلب عاجل يجب اعتباره مشبوهًا حتى يثبت العكس

📋 بروتوكول الحماية اليومية

- ✔ تحقق قبل أي رد
- ✔ لا تنشر معلومات شخصية كثيرة
- ✔ استخدم قنوات رسمية فقط
- ✔ راقب نشاطك الرقمي
- ✔ افصل بين العمل والحياة الشخصية

🗒️ الخلاصة النهائية للدليل الكامل

الأمن الرقمي للصحفي ليس مجرد أدوات، بل هو:

- وعي
- سلوك
- انضباط يومي

والخطر الحقيقي ليس في "الهاكر"، بل في اللحظة الصغيرة التي يتم فيها خداعك.