🟡 دليل الصحفي للتعامل مع استهداف الهوية والمصادر

🎯 ما هو هذا التهديد؟

هذا النوع من الهجمات يستهدف:

- هويتك الحقيقية
- هويتك المهنية
- مصادر معلوماتك

📌 وهو أخطر من الاختراق أحيانًا لأنه قد يؤدي إلى:

- كشف مصادر سرية
- تعريض أشخاص للخطر
- إنهاء مسارك المهني

📌 تشير الأبحاث إلى أن حماية المصادر هي جوهر العمل الصحفي، وأن أي تسريب قد يهدد السلامة الشخصية (Di Salvo, 2021).

🕶️ السيناريو 1: انتحال الهوية الرقمية

🚨 كيف يحدث:

- إنشاء حساب باسمك
- استخدام صورتك
- التواصل مع مصادر باسمك

⚠️ علامات:

- أشخاص يخبرونك برسائل لم ترسلها
- حسابات مشابهة باسمك
- طلبات مشبوهة من "أنت"

⚡ ماذا تفعل فورًا:

1. أعلن رسميًا أن الحساب مزيف
2. أبلغ المنصة
3. حذّر مصادرَك مباشرة

🧯 إجراءات إضافية:

- وثّق حساباتك (Verified)
- استخدم توقيع رقمي في الرسائل المهمة

🛡️ الوقاية:

- وجود قناة تواصل رسمية واحدة مع المصادر
- نشر تحذير دائم حول الحسابات المزيفة

❌ أخطاء:

- تجاهل الحساب المزيف
- الرد عليه مباشرة (يعطيه مصداقية)

🧾 السيناريو 2: كشف الهوية (Doxxing)

🎯 ما هو:

نشر معلوماتك الشخصية:

- عنوان المنزل
- رقم الهاتف
- العائلة
- بيانات خاصة

🚨 علامات:

- تهديدات بفضح معلومات
- تسريب تدريجي لمعلوماتك
- نشر معلومات صحيحة جزئيًا

⚡ ماذا تفعل فورًا:

1. لا ترد عاطفيًا
2. وثّق كل شيء
3. أبلغ الجهات القانونية (إن أمكن)
4. احذف معلوماتك من الإنترنت

🧯 إجراءات حماية:

- إزالة بياناتك من مواقع البحث
- استخدام رقم هاتف منفصل للعمل
- عدم مشاركة تفاصيل شخصية

📌 كشف الهوية يستخدم غالبًا لإسكات الصحفيين (Shere et al., 2023).

🤝 السيناريو 3: استهداف المصادر الصحفية

🎯 كيف يحدث:

- مراقبة اتصالاتك
- اختراق المصدر
- الضغط على المصدر

📌 هذا أخطر سيناريو على الإطلاق

🚨 علامات:

- توقف مفاجئ للمصدر
- سلوك غريب في التواصل
- رسائل غير معتادة

⚡ ماذا تفعل فورًا:

1. افترض أن القناة مخترقة
2. توقف عن التواصل عبرها
3. استخدم قناة بديلة آمنة
4. تحقق من هوية المصدر

🧯 إجراءات وقائية:

- لا تحتفظ بأسماء حقيقية
- استخدم أسماء رمزية
- افصل بين المصادر

📌 الأبحاث تؤكد أن الصحفيين يجب أن يفترضوا أن أجهزتهم قد تكون مخترقة دائمًا (Di Salvo, 2021).

📤 السيناريو 4: تسريب البيانات الحساسة

🚨 أمثلة:

- ملفات تحقيق
- تسجيلات
- أسماء مصادر

⚠️ علامات:

- نشر معلومات لديك فقط

- ظهور ملفاتك في الإنترنت
- تهديد بنشر ملفات

⚡ ماذا تفعل:

1. حدّد ما تم تسريبه
2. أوقف كل القنوات المرتبطة
3. أبلغ مؤسستك فورًا
4. احمِ المصادر أولًا

🧯 احتواء الأزمة:

- تقليل الضرر الإعلامي
- تغيير طرق العمل فورًا
- نقل البيانات إلى بيئة آمنة

🛡️ الوقاية:

- تشفير الملفات
- عدم تخزين كل شيء في جهاز واحد
- نسخ احتياطي مشفر

🧠 القاعدة الذهبية لهذا القسم

✔ المصدر أهم من الخبر
✔ لا تخزن كل شيء في مكان واحد
✔ افترض أن أي معلومة غير محمية ستُكشف

📋 بروتوكول حماية المصادر (مهم جدًا)

- ✔ استخدام تطبيقات مشفرة
- ✔ عدم استخدام الأسماء الحقيقية
- ✔ حذف المحادثات الحساسة
- ✔ استخدام أجهزة منفصلة
- ✔ لقاءات مباشرة بدون أجهزة عند الضرورة

⚠️ سيناريو متقدم: اختراق + استهداف مصدر

ماذا يعني؟

- تم اختراقك
- يتم استخدامك للوصول إلى المصدر

التصرف:

1. أوقف كل الاتصالات فورًا
2. أبلغ المصادر بالخطر
3. غيّر كل وسائل التواصل
4. اعتبر كل شيء مكشوف

🧾 الخلاصة

استهداف الهوية والمصادر هو أخطر تهديد على الصحفي، لأنه لا يهددك فقط — بل يهدد كل من يعمل معك.