# 🟠 دليل الصحفي للتعامل مع المراقبة والتتبع

## 🎯 ما هو هذا التهديد؟

هذا النوع من الهجمات لا يهاجمك بشكل مباشر، بل:

- يراقب تحركاتك
- يحلل سلوكك
- يتتبع موقعك
- يبني ملفًا عنك (Profiling)

📌 تشير الدراسات إلى أن المراقبة الرقمية أصبحت تهديدًا أساسيًا لعمل الصحفيين، خاصة عند التعامل مع مصادر حساسة (Di Salvo, 2021)، (Shere et al., 2023).

---

# 🧭 السيناريو 1: تتبع الموقع الجغرافي

## 🚨 كيف يحدث:

- عبر GPS
- عبر التطبيقات
- عبر الشبكات (Wi-Fi / أبراج الاتصالات)

## ⚠️ علامات:

- إعلانات مرتبطة بموقعك بشكل دقيق
- تطبيقات تعرف موقعك بدون إذن واضح

## ⚡ ماذا تفعل فورًا:

1. أوقف GPS
2. أغلق مشاركة الموقع في التطبيقات
3. راجع أذونات التطبيقات

## 🧯 إجراءات متقدمة:

- استخدم هاتف مخصص للعمل الصحفي
- لا تأخذ هاتفك الشخصي لاجتماعات حساسة
- أوقف البلوتوث

## 🛡️ الوقاية:

- تفعيل الموقع فقط عند الحاجة

• حذف التطبيقات غير الضرورية

### ❌ أخطاء:

• ترك GPS مفتوح دائمًا
• مشاركة الموقع في الوقت الحقيقي

---

## 🛰️ السيناريو 2: المراقبة الصامتة (Silent Surveillance)

### 🎯 ما هي:

مراقبة دون أي إشارات واضحة، مثل:

• تحليل الاتصالات
• تتبع الأنماط
• مراقبة الإنترنت

📌 الأبحاث تشير إلى أن الصحفيين يجب أن يتصرفوا وكأنهم تحت المراقبة دائمًا (Di Salvo, 2021).

### ⚡ ماذا تفعل:

• استخدم أدوات مشفرة دائمًا
• غيّر نمط التواصل
• لا تعتمد على قناة واحدة

### 🧯 تكتيك مهم:

✔ افصل بين:

• جهاز شخصي
• جهاز للعمل
• جهاز للاتصالات الحساسة

---

## 🌐 السيناريو 3: التتبع عبر الشبكات العامة

### 🚨 كيف يحدث:

• Wi-Fi مفتوح
• شبكة مزيفة (Fake Wi-Fi)
• اعتراض البيانات

📌 الشبكات العامة من أكثر البيئات خطورة على البيانات (Sun, 2024).

### ⚡ ماذا تفعل فورًا:

1. لا تدخل حسابات حساسة
2. لا ترسل معلومات سرية
3. استخدم VPN

### 🧯 إذا اضطررت:

- استخدم بيانات الهاتف بدل Wi-Fi
- افتح مواقع HTTPS فقط

### 🛡️ الوقاية:

- تعطيل الاتصال التلقائي بالشبكات
- حذف الشبكات القديمة

### ❌ أخطاء:

- تسجيل الدخول للبريد أو الحسابات البنكية
- استخدام Wi-Fi مجاني بدون حماية

---

## 🧬 السيناريو 4: تحليل البصمة الرقمية

### 🎯 ما هي:

كل ما تفعله على الإنترنت:

- المواقع التي تزورها
- توقيت نشاطك
- نوع جهازك
- أسلوب الكتابة

📌 المهاجمون يستخدمون هذه البيانات لبناء ملف دقيق عنك (Shere et al., 2023).

### ⚡ ماذا تفعل:

- استخدم متصفح آمن (مثل Tor أو Brave)
- امسح الكوكيز باستمرار
- استخدم وضع التصفح الخاص

### 🧯 تقنيات متقدمة:

- تغيير نمط الكتابة في الحالات الحساسة
- عدم استخدام نفس الحسابات دائمًا

---

## 🕵️ السيناريو 5: تتبع عبر الأجهزة الذكية (IoT)

### 🚨 أمثلة:

- كاميرات
- ساعات ذكية
- أجهزة منزلية

📌 هذه الأجهزة قد تستخدم للتجسس دون علمك (Shere et al., 2023).

### ⚡ ماذا تفعل:

- أوقف الأجهزة أثناء الاجتماعات الحساسة
- افصل الإنترنت عنها
- لا تعتمد عليها في بيئة العمل الصحفي

---

## 🧠 القاعدة الذهبية لهذا القسم

✔ افترض أنك مراقب دائمًا
✔ قلل البيانات التي تتركها
✔ غيّر سلوكك وليس فقط أدواتك

---

## 📋 قائمة التحقق اليومية

- ✔ إيقاف GPS عند عدم الحاجة
- ✔ استخدام VPN
- ✔ مراجعة أذونات التطبيقات
- ✔ حذف الشبكات غير المعروفة
- ✔ استخدام متصفح آمن

---

### 🧾 الخلاصة

المراقبة لا تهدف لاختراقك فورًا، بل لفهمك واستهدافك لاحقًا — وكلما قلّت بياناتك، زادت حمايتك.