EOJM
المرصد المصري للصحافة والإعلام
Egyptian Observatory for Journalism and Media

الأمان السيبراني للصحفيات: دليل إرشادي مصغّر لحماية هويتك الرقمية من العنف الرقمي

EOJM
www.eojm.org
info@eojm.org

الأمان السيبراني للصحفيات

دليل مختصر لحماية الهوية الرقمية ومواجهة العنف الإلكتروني

إصدار عن المرصد المصري للصحافة والإعلام

ضمن إنتاج وحدة الحقوق الرقمية وبرنامج العدالة الجندرية بالمؤسسة

وبالتعاون مع حملة "هن في الإعلام" – فعاليات الـ16 يوم لمناهضة العنف ضد المرأة

هذا الإصدار يُعد نسخة تمهيدية مختصرة تسبق إطلاق الدليل الشامل للأمان السيبراني للصحفيات.

تعريف موجز بالأمان السيبراني

الأمان السيبراني هو مجموعة من الإجراءات والتقنيات التي تحمي حساباتك وبياناتك وهويتك الرقمية من الاختراق أو التتبع أو الاستغلال.

جزء من جهود المرصد المصري للصحافة والإعلام لتعزيز سلامة الصحفيات وحماية الفضاء الرقمي المهني.

حمايتك الرقمية جزء من سلامتك الشخصية والمهنية.

إعداد المحتوى

وحدة الحقوق الرقمية – المرصد المصري للصحافة والإعلام

وبالتعاون مع برنامج العدالة الجندرية

التحرير اللغوي والمراجعة

إسلام الكلحي

الإخراج الفني

سمر صبري

منهجية إعداد الدليل

استند إعداد هذا الدليل إلى أحدث ممارسات الحماية الرقمية الموجّهة للعاملات في المجال الصحفي، بالاعتماد على خبرات وحدة الحقوق الرقمية في المرصد، وإلى مراجع دولية متخصصة.

وتمت مواءمة الإرشادات مع السياق المصري واحتياجات الصحفيات في البيئات الرقمية عالية الخطورة.

ويمثل هذا الإصدار نسخة تمهيدية مختصرة تسبق إصدار الدليل الشامل للأمان السيبراني للصحفيات.

الفئة المستهدفة

موجّه للصحفيات والصحفيين، والعاملات والعاملين في الإنتاج الإعلامي والمحتوى الرقمي.

تعريف موجز بالعنف الإلكتروني

العنف الإلكتروني هو أي اعتداء أو سلوك عدائي يتم عبر الإنترنت ويستهدف النساء بسبب عملهن أو وجودهن العام، ويشمل التهديد، الابتزاز، التشهير، التتبع، اختراق الحسابات، و انتحال الهوية.

بيان عدم المسؤولية

هذا الدليل للإرشاد العام، ولا يُعد بديلاً عن الاستشارات التقنية أو القانونية المتخصصة في الحالات عالية الخطورة.

الهوية الصوتية للدليل (Tone of Voice)

يعتمد الدليل لغة واضحة ومباشرة، ويرتكز على خطوات عملية قابلة للتطبيق الفوري أثناء العمل الصحفي اليومي أو في لحظات الطوارئ الرقمية.

خريطة استخدام الدليل

يُستخدم هذا الدليل في التغطيات الميدانية، والعمل عبر المنصات الرقمية، ومواجهة الاستهداف الإلكتروني، والعنف الرقمي المرتبط بالنوع الاجتماعي.

تاريخ الإصدار

ديسمبر 2025 – القاهرة

مقدمة

تُعدّ السلامة الرقمية جزءًا أساسيًا من منظومة السلامة الشخصية والمهنية للصحفيات؛ فهي مجموعة من الممارسات التي تقلل مخاطر الاستهداف الإلكتروني وتحمي الحسابات، الهوية، والبيانات أثناء العمل الصحفي.

أصبح العنف الرقمي إحدى أخطر صور العنف التي تواجه الصحفيات في مصر والمنطقة العربية، لما يحمله من تأثيرات نفسية ومهنية مباشرة، وقدرته على الانتشار السريع. وتشمل أنماط هذا العنف: التشهير، التحرش، الابتزاز، محاولات الاختراق، انتحال الهوية، تتبع الموقع، والاستهداف أثناء التغطيات الصحفية أو المشاركة في النقاش العام.

تشير البلاغات الواردة إلى المرصد المصري للصحافة والإعلام خلال الأعوام الأخيرة إلى تزايد ملحوظ في حالات الاستهداف الرقمي، كثير منها يدمج بين طبيعة العمل الصحفي والبعد الجندري للهجمة. هذا النوع من العنف لا يعكس ضعفًا فرديًا، بل يمثل تهديدًا متزايدًا للوجود المهني والنسائي في الفضاء الرقمي.

أنتِ لستِ وحدك... والتعرّض للعنف الرقمي لا يقلّل من مهنيتك أو حضورك، بل يسلّط الضوء على اتساع نطاق العنف ضد الصحفيات.

وفي ظل هذا الواقع، جاءت الحاجة إلى دليل مبسّط وعملي، يقدم إجراءات حماية فورية وسهلة التطبيق دون مصطلحات تقنية معقدة.

ويأتي هذا الدليل ضمن جهود وحدة الحقوق الرقمية وبرنامج العدالة الجندرية بالمرصد المصري للصحافة والإعلام، كجزء من عمل مؤسسي يهدف لتعزيز السلامة الرقمية للصحفيات في السياق المصري.

أخيرا، هذا الدليل ليس بديلًا عن الحماية التقنية المتقدمة، لكنه يوفر أساسًا عمليًا يساعدك اليوم—قبل الغد—على حماية وجودك الرقمي وتقليل المخاطر بشكل واضح.

⭐ لماذا هذا الدليل مهم الآن؟

يجمع كثير من الاستهداف الرقمي بين الهجوم الشخصي، والتشكيك في المهنية، وإسكات الصوت.

لذلك يقدم هذا الدليل حماية عملية وسريعة، قابلة للتطبيق مباشرة، دون الحاجة لخبرة تقنية.

إذا طبّقتِ ٪30 فقط من هذا الدليل، ستنخفض مخاطر الاستهداف الرقمي لديكِ بصورة كبيرة.

🔐 كيف يُستخدم هذا الدليل؟

هذا الدليل ليس نصًا تقنيًا معقدًا، بل مجموعة من الخطوات البسيطة الواضحة التي يمكنك تنفيذها فورًا، سواء كنتِ:

في مؤسسة صحفية،

في تغطية ميدانية،

تواجهين حملة تشهير،

أو في موقف طارئ يتطلب استجابة سريعة.

ينقسم الدليل إلى خطوات عملية تركّز على أكثر أنماط العنف الرقمي انتشارًا ضد الصحفيات في مصر، وتساعدك على حماية الحسابات، البيانات، الهوية الرقمية، ومعلومات العمل الحساسة.

💡 ما الذي ستتعلمينه؟

تأمين حساباتك على المنصات الرقمية من الاختراق.

إدارة كلمات المروروالهوية الرقمية باحتر افية.

التعامل مع محاولات الابتزازوالتشهيروالاستهداف.

حماية البيانات الحساسة ورسائل العمل والمصادر الصحفية.

تقليل الضرر بعد أي تهديد أو اختراق.

استخدام أدوات وتطبيقات مجانية أو منخفضة التكلفة.

آليات الإبلاغ والدعم المتاحة عبر المرصد.

كيف تتعاملين مع المعلومات الحساسة؟

تجنّبي تخزين المعلومات الحساسة داخل المحادثات العادية أو حسابات السوشيال ميديا.

استخدمي تطبيقات مشفّرة للتواصل عند مشاركة بيانات مهمة.

احذفي البيانات فور انتهاء الحاجة إليها.

لا تشاركي صور الهوية أو بيانات السفر إلا للضرورة القصوى.

احرصي على عدم ترك نسخ مفتوحة أو غير محمية من المستندات الحساسة.

🎯 الفئة المستهدفة

الصحفيات العاملات داخل المؤسسات الإعلامية.

الصحفيات المستقلات (Freelancers).

العاملات في إنتاج المحتوى الرقمي.

الصحفيات في المحافظات والمناطق البعيدة عن القاهرة.

أي امرأة تعمل في المجال الإعلامي وتتعرض لاستهداف أو عنف رقمي.

⚠️ حدود الدليل

لا يغطي هذا الدليل الهجمات الرقمية المعقدة أو الاستهداف عالي التنظيم. في هذه الحالات، يُنصح باللجوء إلى دعم تقني متخصص وفق نوع التهديد ومدى خطورته.

🗺️ خريطة الطريق في هذا الدليل

1. خطوات الحماية الأساسية (الضرورية لكل صحفية).
2. خطوات الحماية المتوسطة (عند وجود تهديدات متكررة).
3. خطوات الاستجابة وقت الخطر (عند وقوع ابتزاز أو اختراق مباشر).

القسم الثاني: أدوات وإرشادات التطبيق العملي

بعد استعراض مقدمة الدليل و أنماط العنف الرقمي ومستويات التهديد، يبدأ هذا القسم بتقديم أدوات عملية يمكن تطبيقها فورًا خلال العمل الصحفي أو عند مواجهة أي استهداف رقمي.

يُعد هذا الجزء هو الجانب التنفيذي للدليل، وبيقدم خطوات واضحة للتعامل مع محاولات الاختراق، الابتزاز، التشهير، سرقة الحسابات، تسريب البيانات، الاستهداف الجندري، والهجمات المفاجئة أثناء التغطيات.

كيف تستخدمين هذا القسم؟

– ابدئي بقراءة جدول الطوارئ السريع.

– استخدمي مستوى التهديد لتحديد الإجراء المناسب.

– انتقلي بعدها لأدوات تأمين الهاتف والحسابات.

– تواصلي مع المرصد عند أي مؤشر خطر عالي.

أهمية جدول الطوارئ

الجدول التالي أداة مختصرة وسريعة للتعامل مع اللحظات الأولى لأي استهداف.

ليس بديلاً عن الدعم المتخصص، لكنه يساعدك على تقليل الضرر بسرعة.

مؤشرات الألوان

1) مستوى الخطر المرتفع (High Risk)

عندما يظهر:

* تهديد مباشر على السلامة الشخصية
* محاولات اختراق مؤكدة
* نشر بيانات شخصية
* انتحال هوية متكرر
* وصول غير معروف لحساباتك
* هجوم منظم أو حملة تشهير واسعة
* رسائل تتضمن تفاصيل دقيقة تدل على مراقبة أو تتبع

إجراء:

📌 يجب التواصل فورًا مع المرصد + حفظ الأدلة + تغيير كلمات المرور + تفعيل 2 FA + مراجعة الأجهزة.

🟠 2) مستوى الخطر المتوسط (Medium Risk)

اللون: برتقالي

عندما يظهر:

* روابط مشبوهة
* رسائل غير معتادة تطلب بيانات
* تسجيل دخول غريب لمرة واحدة
* تعليق أو تهديد غير مباشر
* محتوى مزيف أو مضلل عنك
* محاولات إضافة حسابات غير موثوقة لدوائر التواصل

إجراء:

📌 تغيير كلمات المرور – فحص الروابط – تفعيل التنبيهات – توثيق أولي.

(لا تحتاجي تدخل قانوني مباشر)

🟡 3) مستوى الخطر المنخفض (Low Risk)

اللون: أصفر

عندما يظهر:

* تعليقات مزعجة أو تنمر
* رسائل عامة غير مستهدفة
* وصول إعلانات أو Spam
* محتوى عشوائي مش من دائرة الخطر

إجراء:

📌 تجاهل – حظر – إعدادات خصوصية أقوى.

((لا تحتاجي تدخل من المرصد إلا في حال تكرر)

🟢 4) منطقة الأمان (Safe Zone)

اللون: أخضر

تعني:

* لا توجد إشارات خطر
* الحساب آمن
* الإعدادات الصحيحة مفعّلة
* لا يوجد نشاط غير معتاد

إجراء:

📌 المتابعة الروتينية + صيانة أسبوعية للأمن الرقمي.

🟫 قبل الجدول.. خطوة أساسية

⚠️ احرصي على توثيق كل شيء قبل اتخاذ أي إجراء.

فالتوثيق يُعدّ أساس الدعم القانوني.

🟫 صفحة الانتقال — من المعرفة إلى التطبيق

بعد فهم طبيعة التهديدات، يبدأ التطبيق العملي لإجراءات الحماية الرقمية.

أنتِ لستِ مسؤولة عن الهجوم الرقمي الذي تتعرضين له. المسؤولية تقع بالكامل على الجاني. دورك هو حماية نفسك وتقليل الأذى، ودورنا هو دعمك في استعادة السيطرة و اتخاذ القرارات الصحيحة.

نبدأ الآن بجدول الطوارئ السريع — أول أداة عملية في الدليل.

حمايتك الرقمية جزء من سلامتك الشخصية والمهنية.

جدول الطوارئ السريع (Quick Reference Table)

كيفية التصرف خلال الدقائق الأولى عند التعرّض لأي تهديد رقمي
(.يُستخدم هذا الجدول خلال الدقائق الأولى من أي هجمة رقمية)
تنبيه أساسي قبل استخدام الجدول:
⚠️ وثّقي كل شيء قبل القيام بأي خطوة.
(لقطات شاشة – رو ابط – رسائل – توقيت الهجمة – الحسابات المتورطة)
التوثيق أساس الدعم القانوني.

الخطر	الإجراء العاجل	الأداة
⚠️ رابط مشبوه	افحصي الرابط قبل فتحه	VirusTotal
🔐 تسجيل دخول غريب	أغلقي كل الجلسات المفتوحة + غيّري كلمة المرور من جهاز آمن	Meta Security / Gmail Security Checkup
📩 تسريب بريد إلكتروني	افحصي البريد عبر HIBP+ غيّري كلمة المرور فورًا	Have I Been Pwned
🎭 انتحال شخصية	وثّقي المحتوى + قدّمي بلاغ سريع عن الحساب المنتحل	Platform Reports
📣 حملة تشهير	احفظي الأدلة + تجاهلي الردود وعدم الانخراط	المرصد
⚡ ابتزاز أو تهديد	التوثيق الكامل + عدم التفاعل نهائيًا (No Response)	المرصد
🔒 اختراق حساب	افصلي الإنترنت عن الجهاز + غيّري كلمة مرور جديدة من جهاز موثوق	Security Settings

يُفضّل تنفيذ الخطوات الواردة في الجدول قبل أي تفاعل مع المهاجم، لتقليل الضرر ومنع التصعيد.

إجراءات سريعة عند الطوارئ (Quick Actions)

الإجراء	الوصف
🔑 تغيير كلمات المرور فورًا	غيّري كلمات المرور من جهاز آمن لتجنب استمرار الاختراق.
🛡️ تفعيل المصادقة الثنائية (2FA)	استخدمي تطبيق Authenticator بدل رسائل SMS لأنها أكثر أمانًا.
🔗 فحص الروابط المشبوهة	افحصي الروابط والملفات عبر VirusTotal قبل فتحها.
📱 تسجيل الخروج من الأجهزة غير الموثوقة	أغلقي أي جهاز أو جلسة دخول غير معروفة.
📝 توثيق الوقائع	احفظي صورًا أو فيديو يثبت الاختراق أو محاولاته.
📞 التواصل مع المرصد	تواصلي للحصول على الدعم القانوني والنفسي والتقني فورًا.

ممارسات الأمان اليومية (Daily Hygiene)

الإجراء	الوصف
تحديث التطبيقات ونظام التشغيل بانتظام	لتحسين الأمان وسدّ الثغرات.
حذف الرسائل غير المعروفة وعدم فتح الروابط المجهولة	لتفادي محاولات الاختراق أو التصيّد.
مراجعة الأجهزة المتّصلة بالحسابات أسبوعيًا	للتأكد من عدم وجود أجهزة غريبة أو جلسات غير معروفة.
استخدام كلمات مرور مختلفة وقوية	لزيادة الحماية وتقليل فرص الاختراق.
تجنب استخدام الحسابات المهنية للدخول إلى مواقع غير معروفة	لتقليل المخاطر على حسابات العمل.
مراجعة Permissions للتطبيقات شهريًا	للحد من وصول التطبيقات إلى بيانات غير ضرورية.
تعطيل النسخ الاحتياطي للصور الحساسة	لتجنب تسريب صور أو ملفات شخصية بشكل غير مقصود.

هذه الممارسات البسيطة تساعدك في تقليل المخاطر اليومية وتحسين أمان حساباتك أثناء العمل الصحفي.

1. التصفح بخصوصية عبر "DuckDuckGo"

لا يجمع Profiles (ملفات تعريف) .
يحظر Trackers (أدوات التتبع) .
يوفر Bang! للبحث السريع.
يقدم Cheatsheets .

تنبيه: DuckDuckGo يحسّن الخصوصية لكنه لا يخفي الهوية بالكامل. في البيئات عالية الحساسية استخدمي Tor Browser أو Mullvad Browser .

2. التحقق من تسريب بياناتك عبر "Have I Been Pwned"

كشف تسريب البريد أو الهاتف أو اسم المستخدم.
عرض تفاصيل وتاريخ التسريب.
تنبيهات فورية عند أي اختراق جديد.
إمكانية إخفاء البريد عبر Disable Public Search .
عند تسريب بريدك، غيّري كلمة السر فورًا.

3. تفعيل "Google Alerts" لمتابعة البيانات الحساسة

ضعي كلمات مفتاحية مثل:
اسمك الكامل – رقم هاتفك – بريدك – اسم مؤسستك.

وأضيفي Alert لاسمك + لقبك + "صحفية".

4. فحص الهاتف عبر "Exodus Privacy"

(أداة لكشف الأذونات والمتتبعات داخل التطبيقات)

تحليل شامل للتطبيقات.
كشف أدوات التتبع المخفية.
عرض Permissions غير الضرورية.
إمكانية إلغاء الأذونات أو حذف التطبيق.
عند ظهور Tracker غير مبرر ← يفضّل حذف التطبيق.

5. فحص الروابط والملفات عبر "VirusTotal"

فحص الروابط قبل فتحها.
يدعم IP – URLs – Images – ZIP – APK – PDF ٠
يكشف البرمجيات الخبيثة ومحاولات Phishing ٠

6. قاعدة «3 حسابات» لحماية الهوية الرقمية

حساب شخصي.
للعائلة والمقربين فقط.
حساب مهني.
مخصص للعمل والتواصل الإعلامي.
حساب ثالث للتطبيقات.
للتسجيل في المنصات الجديدة—ويُفضل ببريد مختلف تمامًا.

7. إعدادات الأمان في منصات التواصل

تفعيل2FA
إخفاء رقم الهاتف والبريد الإلكتروني.
إيقافLocation Sharing .
التحكم فيTag/Mention .
الحد من الظهور العلني.
مراجعة المنشورات القديمة وضبط إعداداتها.
مراجعة Login Activity بانتظام.

8. بروتوكول التعامل عند الاختراق

1	عدم حذف أي رسالة أو محتوى.
2	توثيق كل التفاصيل.
3	تغيير كلمات المرور من جهاز آخر موثوق.
4	إزالة الأجهزة غير الموثوقة من تسجيلات الدخول.
5	إخطار المؤسسة أو النقابة.
6	التواصل مع المرصد.
7	فصل الإنترنت عن الجهاز المتضرر قبل الفحص.

9. حماية الصور والملفات الحساسة

استخدام Encryption (التشفير).
الاحتفاظ بنسخة احتياطية Offline Back- .
استخدام VeraCrypt أو Cryptomator .
وضع Watermark (علامة مائية) على الصور الحساسّة.
تجنب مشاركة الملفات الخاصة عبر تطبيقات ضعيفة الأمان.

10. فهم الهندسة الاجتماعية "Social Engineering"

تشمل:

- Fake Verification Links (رو ابط تحقق مزيفة) .
- Fake Support Calls (مكالمات دعم وهمية) .
- صفحات دخول مزيفة.
- رسائل تهديد مفبركة.

القاعدة الذهبية:

لا تضغطي – لا تفتحي – لا تشاركي أي معلومة دون تحقق.

11. تقليل البصمة الرقمية "Digital Footprint"

يحدث ذلك من خلال:

- حذف البيانات المكشوفة.
- استخدام بريد منفصل للتطبيقات الثانوية.
- تجنب نشر معلومات شخصية قابلة للاستغلال.
- حذف الحسابات القديمة.
- إزالة بيانات WHOIS الخاصة بأي موقع تملكينه.

12. أدوات تحقق إضافية

Meta Privacy Checkup
Mozilla Observatory
Signal
ProtonMail
Tor Browser
Bitwarden / KeePass
CoverYourTracks.eff.org

13. سلامة الصحفيات في بيئات عدائية

تشمل الحماية الرقمية مجموعة من الإجراءات والتدابير التي تهدف إلى حماية الصحفيات وبياناتهن أثناء العمل في بيئات عدائية أو غير آمنة، وتشمل ما يلي:

- تجنب الدخول في نقاشات مع اللجان الإلكترونية.
- استخدام Restrict (تقييد الحساب).
- تجنب مشاركة الموقع المباشر.
- تأمين الجهاز قبل التغطيات الميدانية.
- تعطيل Face ID / Fingerprint قبل النزول.
- استخدام PIN قوي.

14. حماية المصادر الصحفية

تشمل التدابير الرقمية لحماية المصادر الصحفية الإجراءات التالية:

- استخدام E2EE – End-to-End Encryption .
- عدم تخزين بيانات المصادر على الهاتف الأساسي.
- تشفير الملفات المصدرية.
- استخدام Burner Phone عند الحاجة (وفق القانون).

15. إرشادات منخفضة التكلفة للصحفيات

تركز هذه الأدوات على توفير حماية رقمية فعّالة وموثوقة بتكلفة منخفضة للصحفيات المستقلات:

- Signal
- Bitwarden
- Mozilla VPN
- Google Authenticator

16. حالات واقعية مختصرة

اختراق بعد فتح رابط اعتماد مزيف ← الفحص أولًا.
حملة تشهير ممنهجة ← التوثيق + التواصل مع المرصد.
انتحال شخصية صحفية ← التحذير + التوثيق + المتابعة القانونية.

17. ما الذي يجب فعله في المواقف الشائعة؟

رابط مشبوه ← افحصيه عبر VirusTotal .
اختراق حساب ← غيري كلمة المرور وأغلقي كل الجلسات.
حملة تشهير ← وثّقي ولا تتفاعلي.
تهديد مباشر ← احتفظي بالأدلة وتواصلي مع المرصد.

18. حماية الهوية أثناء التغطيات الميدانية

تركّز الإجراءات التالية على تقليل تتبّع الهوية والموقع أثناء العمل الميداني في البيئات الحسّاسة:

- تعطيل الموقع الجغرافي.
- استخدام هاتف ثانٍ لتقليل المخاطر.
- عدم النشر اللحظي من موقع التغطية.
- استخدام VPN في البيئات عالية الخطورة.
- تعطيل Bluetooth و NFC .

19. الآثار النفسية للعنف الرقمي

قد يؤدي العنف الرقمي إلى القلق، والأرق، والعزلة، وفقدان التركيز.
يوفر المرصد دعمًا نفسيًا متخصصًا للصحفيات المتعرضات للأذى الرقمي.

20. مسؤوليات المؤسسات الإعلامية

وضع سياسات حماية رقمية واضحة.
التدريب الدوري للصحفيات.
توفير دعم قانوني ونفسي فعال.
حماية البنية الرقمية الداخلية.
التعاون مع النقابة والمرصد.

21. المجموعات المهنية الآمنة "Safe Professional Circles"

وجود مجموعة صغيرة من الصحفيات الموثوقات يساهم في:

- رصد الهجمات مبكرًا.
- تبادل التحذيرات والدعم.
- تخفيف الضغط النفسي.
- التحرك الجماعي عند الأزمات.

22. متى أكتفي بالإجراءات الفردية؟ ومتى يلزم التصعيد المؤسسي؟

الإجراءات الفردية تكفي عند الهجمات المحدودة وغير المتكررة.
أما التصعيد فيلزم عندما:س

- يوجد تهديد صريح،
- أو حملة منظمة،
- أو استخدام بيانات شخصية ضدك،
- أو حدوث اختراق فعلي.

23. إشارات الخطر "Red Flags"

يبدأ الرابط http بـ بدل https
يُطلب إدخال OTP.
يظهر تسجيل دخول من مكان غير مألوف.
اتصال يدّعي أنه من "الدعم الفني".
طلب إرسال بيانات الهوية.
روابط قصيرة مجهولة المصدر.

24. إدارة الأزمات الرقمية "Digital Crisis Management"

عدم اتخاذ قرارات تحت ضغط التهديد.
تحديد شخص موثوق لإدارة الأزمة.
عدم إصدار تصريحات قبل التوثيق الكامل.
تنظيم الوقت وتجنب التصعيد.
الفصل بين الشعور بالتهديد والإجراءات الفعلية.

25. التمييز بين التهديد الحقيقي والتهويل الرقمي

ليس كل تهديد قابلًا للتنفيذ.

التقييم عبر:

- نوع المرسل.
- البيانات المستخدمة ضدك.
- تكرار الرسائل.

- السياق الزمني.
- وجود معلومات خاصة تدل على محاولة اختراق.

26. حفظ الأدلة "Evidence Preservation"

عدم حذف الرسائل أو المنشورات.
حفظ النسخة الأصلية للرابط أو المحتوى.
تسجيل الوقت والتاريخ لكل فعل ضار.
الاحتفاظ بنسخة آمنة على جهاز خارجي أو مساحة سحابية مشفرة.
ترتيب الأدلة زمنيًا لتسهيل المتابعة القانونية.

قائمة مراجعة شهرية (Monthly Checklist)

✔ تحديث كل الأجهزة
✔ مراجعة الجلسات المفتوحة
✔ فحص التطبيقات عبر Exodus
✔ تغيير كلمات المرور للحسابات الحساسة
✔ فحص تسريبات عبر HIBP
✔ مراجعة إعدادات الخصوصية
✔ تنظيف البريد
✔ مراجعة البصمة الرقمية

رسالة إلى كل صحفية

مساحتك الرقمية امتداد لمساحتك المهنية، وصوتك ليس مجرد ممارسة يومية، بل هو حق أصيل يجب أن يبقى آمنًا ومسموعًا. في عالم تتزايد فيه أشكال العنف الرقمي وتتعقد أدواته، يصبح امتلاك المعرفة والمهارات والأدوات المناسبة عنصرًا أساسيًا لحماية نفسك، و اتخاذ القرار الصحيح في لحظة الخطر، والتحكم في وجودك الرقمي دون خوف أو ارتباك.

يدرك المرصد المصري للصحافة والإعلام، حجم الضغوط التي تتعرض لها الصحفيات، سواء المهنية أو النفسية أو الاجتماعية، ويقدم دعمًا قانونيًا وتقنيًا ونفسيًا متكاملًا لمساندتك في مواجهة العنف الرقمي، وتمكينك من مواصلة عملك بثقة وأمان.

احمي وجودك الرقمي.. لأن قصتك تستحق الأمان،
وصوتك يجب أن يبقى حاضرًا وقويًا، ومهنتك لا ينبغي أن تُمارَس تحت التهديد.

للتواصل مع المرصد
01557774094
01044141468

support@eojm.org

المـــرصـد المصـــري للصـــحافة والإعـــلام
Egyptian Observatory for Journalism and Media

"المرصد المصري للصحافة والإعلام"

مؤسسة مجتمع مدني مصرية تأسست بالقرار رقم 5805 لسنة 2016. وتتخذ "المؤسسة" من الإعلان العالمي لحقوق الإنسان والمعاهدات والمواثيق الدولية الخاصة بحرية الصحافة والإعلام والدستور المصري مرجعية لها.

تهدف "المؤسسة" إلى الدفاع عن الحريات الصحفية والإعلامية وتعزيزها، والعمل على توفير بيئة عمل آمنة للصحفيين والإعلاميين في المجتمع المصري من ناحية، والعمل على دعم استقلالية ومهنية الصحافة والإعلام من ناحية أخرى.

ومن أجل تحقيق هذه الأهداف يعمل "المرصد" عبر برامج وآليات متنوعة؛ تقوم بعضها برصد الانتهاكات الواقعة بحق الصحفيين والإعلاميين وتوثيقها من ناحية، ورصد ونقد لبعض أنماط اللامهنية في عدد من الصحف والمواقع الإلكترونية ووسائل الإعلام من ناحية أخرى. كما تقدم "المؤسسة" الدعم القانوني المباشر أو غير المباشر للصحفيين أو الإعلاميين المتهمين في قضايا تتعلق بممارستهم لمهنتهم. كما تقوم "المؤسسة" بالبحوث والدراسات الخاصة بوضع حرية الصحافة والإعلام في المجتمع، وتقدم أيضًا مجموعة من التدريبات والندوات التثقيفية من أجل تعزيز قدرات الصحفيين والإعلاميين، والارتقاء بمستواهم المهني وتعريفهم بحقوقهم وواجباتهم وطرق أمنهم وسلامتهم أثناء تأدية عملهم.

رؤيتنا
دعم وتعزيز حرية الصحافة والإعلام واستقلالهما، والوصول إلى بيئة مهنية ومناخ آمن وملائم لعمل الصحفيين والإعلاميين في دولة يكون أساسها سيادة القانون واحترام حقوق الإنسان.