شعاع لحقوق الإنسان
SHOAA for Human Rights

دليل التوعية

بالأمن السيبراني

للمدافعين عن حقوق الإنسان في الجزائر

2026

لماذا هذا الدليل؟

في السنوات الأخيرة، شهدت الجزائر، كغيرها من بلدان المنطقة، تطورات رقمية سريعة رافقها ازدياد في استخدام التكنولوجيا والإنترنت من قبل الأفراد، المؤسسات، والمنظمات الحقوقية. في المقابل، تزايدت التهديدات الرقمية التي تستهدف المدافعين عن حقوق الإنسان، سواء عبر الرقابة والمراقبة الإلكترونية، أو من خلال القرصنة والتصيّد، أو حتى التشويه والتضليل الرقمي.

في هذا السياق، بات من الضروري توفير أدوات عملية ومبسطة تمكّن النشطاء من حماية أنفسهم وبياناتهم أثناء استخدامهم للتكنولوجيا في عملهم اليومي. ويأتي هذا الدليل كاستجابة لحاجة ميدانية حقيقية، إذ يعاني العديد من النشطاء والمدافعين، خصوصًا غير المتخصصين في المجال التقني، من ضعف في الممارسات الرقمية الآمنة، مما يجعلهم عرضة للانتهاكات الإلكترونية.

لا يهدف هذا الدليل إلى تحويل النشطاء إلى خبراء في الأمن السيبراني، بل إلى تقديم خطوات واقعية، وأدوات مناسبة، ونصائح قابلة للتطبيق في السياق الجزائري، تراعي الخصوصية الثقافية، والسياسية، والقانونية، مع الحفاظ على بساطة اللغة وسهولة الفهم.

من هم المستفيدون؟

تم تصميم هذا الدليل ليخدم فئات متنوعة من العاملين والعاملات في مجال حقوق الإنسان في الجزائر، وعلى رأسهم:

- **المدافعون والمدافعات عن حقوق الإنسان، سواء العاملين في الميدان أو في المجال الرقمي.**
- **منسقو ومنسقات الجمعيات والمنظمات غير الحكومية ذات الطابع الحقوقي أو المدني.**
- **الصحفيون والصحفيات، وخاصة المستقلين أو المشتغلين بتوثيق الانتهاكات أو تغطية القضايا الحقوقية.**
- **النشطاء الرقميون والمشتغلون في حملات المناصرة، التعبئة المجتمعية، أو التوعية عبر الإنترنت.**
- **المحامون والمدافعون القانونيون المتعاملون مع قضايا الحريات والحقوق.**

يُعد هذا الدليل مرجعًا عمليًا لأي شخص يشعر بأن نشاطه الرقمي قد يجعله عرضة للاستهداف، حتى وإن لم يكن ينتمي مباشرة إلى منظمة أو كيان حقوقي.

كيف تستخدم هذا الدليل؟

تم تنظيم محتوى الدليل بشكل يسمح باستخدامه بعدّة طرق، وفقًا لاحتياجات القارئ ومستوى معرفته السابقة:

- **يمكن قراءته بشكل متسلسل للحصول على فهم متكامل للأمن الرقمي وممارساته الأساسية.**
- **كما يمكن الرجوع إلى أقسام محددة حسب الحاجة، مثلًا عند الرغبة في تأمين حساب معين، أو فهم طريقة استخدام تطبيق مشفّر، أو إعداد خطة استجابة في حال اختراق جهاز.**

يتكون كل قسم من:

- **شرح مبسّط يوضح طبيعة التهديد أو المشكلة.**
- **خطوات عملية يمكن تنفيذها حتى من قبل المستخدمين غير المتخصصين.**
- **أدوات أو تطبيقات موصى بها، تُذكر بأسمائها الأصلية بالإنجليزية مع شرح مبسط وواضح بالعربية.**
- **نصائح إضافية وقواعد سلوكية مفيدة في السياق الرقمي.**

وفي نهاية الدليل، ستجد قوائم تحقق مختصرة تساعدك على التأكد من مدى أمانك الرقمي في مواقف مختلفة، مثل السفر، المشاركة في حملة، أو استخدام شبكات عامة.
فهم التهديدات الرقمية في السياق الجزائري

الرقابة الحكومية

في الجزائر، كما في العديد من البلدان، تمارس بعض الجهات الرسمية شكلًا من أشكال الرقابة الرقمية التي تستهدف الأفراد والمنظمات، خصوصًا النشطاء الحقوقيين، الصحفيين، ومن يعملون في قضايا حساسة أو ذات طابع سياسي. الرقابة لا تقتصر فقط على تتبع المحتوى العلني، بل قد تشمل أيضًا مراقبة الاتصالات الخاصة، مثل الرسائل، المكالمات، أو حتى النشاطات على تطبيقات التراسل المشفّرة.

ما هي الرقابة الحكومية؟

الرقابة الرقمية هي عملية تقوم بها جهات رسمية)أو بتفويض منها(لرصد وتتبع النشاط الرقمي للأفراد أو الجماعات. وتشمل:

- تتبع ما يُنشر على شبكات التواصل الاجتماعي.
- تسجيل أو قراءة رسائل البريد الإلكتروني أو المراسلات الفورية.
- مراقبة المواقع التي يتم تصفحها أو البحث عنها.
- استخدام تقنيات مثل برامج التجسس (Spyware) أو جمع بيانات من شركات الاتصالات والإنترنت.

أمثلة من الواقع الجزائر

- تم توقيف بعض النشطاء أو استدعاؤهم بناءً على منشوراتهم على فيسبوك أو تويتر.
- وردت تقارير عن حجب مواقع إلكترونية لوسائل إعلام مستقلة أو منظمات حقوقية.
- في بعض الحالات، تم استخدام تهم تتعلق بـ «المساس بهيبة الدولة» أو «نشر أخبار كاذبة» بسبب محتوى رقمي تم تداوله.

ملاحظة: حتى المحتوى الخاص، إذا تم الوصول إليه، يمكن استخدامه ضدك.

لماذا تعتبر هذه الرقابة تهديدًا؟

- لأنها تقيّد حرية التعبير.
- تجعل النشطاء عرضة للملاحقة القانونية أو المضايقة الأمنية.
- تخلق بيئة من الخوف الذاتي .(Self-Censorship)
- تهدد أمن بيانات حساسة تخص الضحايا أو الشهود أو الحملات.

كيف تحمي نفسك من الرقابة؟

- استخدام تطبيقات تراسل مشفّرة)مثل: Signal) Session, وعدم الاعتماد فقط على .WhatsApp
- تجنّب الحديث عن مواضيع حساسة عبر شبكات غير آمنة أو دون تشفير.
- استخدام VPN موثوق عند تصفح الإنترنت)مع مراعاة أن بعضها قد يكون محجوبًا.(
- مراجعة إعدادات الخصوصية في حساباتك على وسائل التواصل بشكل منتظم.
- الاحتفاظ بالحد الأدنى من البيانات على الهاتف أو الحاسوب الشخصي.
- عدم استخدام البريد الإلكتروني الأساسي للمراسلات الحساسة – استخدم بدائل مشفّرة مثل .ProtonMail

التصيّد الإلكتروني (Phishing)؟

ما هو التصيّد الإلكتروني؟

هو محاولة احتيالية تهدف إلى خداع الضحية للحصول على معلومات حساسة مثل كلمات المرور، أو لتنزيل برمجيات خبيثة تؤدي إلى اختراق الجهاز أو الحسابات.

يأخذ التصيّد الإلكتروني عدة أشكال:

- رسائل بريد إلكتروني أو نصية تحتوي على روابط أو مرفقات خبيثة.
- مواقع وهمية تُحاكي مواقع معروفة لجمع بيانات الدخول.
- رسائل عبر تطبيقات التواصل الاجتماعي تبدو وكأنها من أصدقاء أو جهات موثوقة.

التصيّد في السياق الجزائري

في الجزائر، قد تُستخدم رسائل التصيّد لاستهداف النشطاء من خلال:

- محتوى سياسي أو حقوقي حساس.
- روابط لمواقع تبدو موثوقة لكنّها مزوّرة.
- معلومات شخصية واقعية يتم الحصول عليها من الهندسة الاجتماعية أو السجلات الرسمية)مثل الاسم الكامل، مكان العمل، أسماء الزملاء(...، مما يجعل الرسالة تبدو أكثر واقعية وخالية من الأخطاء اللغوية، خاصة عند استخدام تقنيات الذكاء الاصطناعي في كتابتها.

أنواع التصيّد:

- التصيّد العشوائي: رسائل عامة تُرسل لعدد كبير من الأشخاص.
- التصيّد الموجّه (Spear Phishing): رسائل مُصمّمة خصيصًا لك، تحتوي على تفاصيل شخصية أو مهنية لإقناعك بأنها حقيقية.

مثال: رسالة موجهة لك باسمك، وتذكر عملك في جمعية معينة، وتطلب منك «تأكيد معلومات ملف المنظمة.»

كيف تتعرف على محاولات التصيّد؟

- الضغط والإلحاح على اتخاذ إجراء فوري)مثال: حسابك سيتوقف خلال 24 ساعة.
- طلب معلومات حساسة مثل كلمات المرور أو رموز الدخول.
- روابط مشبوهة أو غير مطابقة للمواقع الأصلية (انظر أدناه.)

حتى لو كانت الرسالة خالية من الأخطاء اللغوية وتبدو احترافية، يبقى الرابط هو المفتاح الأول للكشف عن التصيّد.

فهم بنية الروابط (URLs)

لمعرفة إن كان الرابط حقيقيًا أم لا، انتبه للنقاط التالية:

- النطاق الرئيسي (Domain) هو الجزء الأهم من الرابط. مثلًا:
- الآمن الرابط: https://www.facebook.com/settings •
في المثال الثاني، النطاق الحقيقي هو login-alerts.com وليس facebook.com.
- النطاق الحقيقي هو ما يأتي مباشرة قبل «.com» أو «.org» وليس الكلمات التي تسبق ذلك.
- تأكد من وجود HTTPS في بداية الرابط، مع قفل في المتصفح.
- استخدم خاصية المعاينة قبل الضغط على الرابط بالضغط المطوّل على الهاتف أو تمرير الماوس على الرابط.

كيف تحمي نفسك؟

- لا تدخل أي كلمة مرور من خلال رابط توصلك به رسالة.
- فعّل التحقق بخطوتين (2FA) لحماية حساباتك حتى لو تم سرقة كلمة المرور.
- استخدم مدير كلمات مرور، ولا تُكرّر نفس الكلمة في عدة حسابات.
- لا تفتح المرفقات أو الصور من مرسلين غير معروفين.
- في حال الشك، تواصل مباشرة مع الجهة الأصلية من خلال موقعها الرسمي، وليس عبر الرابط الذي في الرسالة.

أدوات مفيدة:

• Have I Been Pwned: لفحص ما إذا تم تسريب بريدك الإلكتروني.
• Bitwarden / 1Password: إدارة كلمات المرور.
• uBlock Origin: إضافات متصفح تحمي من المواقع المزيفة Everywhere HTTPS +
البرمجيات الخبيثة (Malware)

ما هي البرمجيات الخبيثة؟

البرمجيات الخبيثة هي برامج أو ملفات يتم تصميمها لاختراق الأجهزة، أو سرقة البيانات، أو التجسس على المستخدمين دون علمهم. تشمل أنواعها:

• فيروسات (Viruses)
• برمجيات تجسس (Spyware)
• فدية برمجيات (Ransomware)
• أحصنة طروادة (Trojans)
• Keyloggers: برامج تسجل كل ما تكتبه على لوحة المفاتيح.

كيف تُستخدم البرمجيات الخبيثة ضد المدافعين عن حقوق الإنسان؟

في السياق الجزائري، قد تُستخدم البرمجيات الخبيثة من قبل أطراف رسمية أو غير رسمية لاستهداف النشطاء من خلال:

• زرع برمجيات تجسس على الهواتف أو الحواسيب لجمع معلومات عن الأنشطة، الملفات، وجهات الاتصال.
• الوصول إلى البريد الإلكتروني أو حسابات التواصل الاجتماعي واستخدامها لمراقبة أو تشويه سمعة المستخدم.
• تشفير الملفات الحساسة وطلب فدية مقابل فكّها (Ransomware).
• مراقبة المحادثات والصور والمواقع الجغرافية عبر الهاتف دون علم المستخدم.

كيف تصل هذه البرمجيات إلى جهازك؟

• من خلال روابط في رسائل التصيّد.
• عبر تطبيقات أو ملفات مرفقة يتم تحميلها من مصادر غير موثوقة.
• من خلال أقراص USB أو وسائط تخزين مصابة.
• عبر ثغرات في أنظمة التشغيل أو التطبيقات غير المُحدثة.
مثال: قد تصلك وثيقة بصيغة PDF عبر البريد تبدو عادية، لكنها تحمل شيفرة خبيثة تُفعل بمجرد فتحها.

أعراض وجود برمجيات خبيثة في جهازك

• بطء مفاجئ في أداء الجهاز.
• استهلاك مرتفع للبطارية أو البيانات.
• ظهور تطبيقات أو ملفات لم تقم بتثبيتها.
• تغيرات في الإعدادات دون علمك.
• الجهاز يسخن دون سبب، أو يتصرف بشكل غير طبيعي.

كيف تحمي نفسك من البرمجيات الخبيثة؟

حدّث نظام التشغيل والتطبيقات بانتظام (ولا تستخدم إصدارات مقرصنة.)
لا تفتح مرفقات أو روابط من مصادر غير موثوقة.
حمّل التطبيقات فقط من المتاجر الرسمية (Google Play، App Store).
ثبّت برنامج حماية (Antivirus) موثوق وخفيف على جهازك مثل:
Kaspersky Security Cloud – Free
Bitdefender Free Edition
لا تستخدم USB من مصادر غير موثوقة.
فعّل إعدادات الخصوصية، وتحقّق من أذونات التطبيقات.

أدوات إضافية:

• Malwarebytes
أداة موثوقة لفحص الحاسوب واكتشاف البرمجيات الخبيثة. تقدم نسخة مجانية بميزات محدودة، مناسبة للمستخدمين غير التقنيين. يُنصح بتحديث قاعدة البيانات فور التثبيت.

• ESET Online Scanner
أداة مجانية من شركة ESET تتيح فحص الجهاز عبر الإنترنت دون الحاجة لتثبيت دائم. مفيدة للفحص السريع عند الاشتباه بوجود برامج خبيثة.

• Bitdefender Virus Scanner for Mac
أداة خفيفة لفحص البرمجيات الخبيثة على أجهزة macOS. توفر حماية موثوقة وفحصًا يدويًا دون استهلاك كبير للموارد. النسخة المجانية لا تشمل الحماية في الوقت الحقيقي.

• ClamAV / ClamXAV (لأنظمة Mac وLinux)
برنامج مفتوح المصدر يُستخدم من قبل العديد من النشطاء والمنظمات لفحص البرمجيات الضارة بطريقة بسيطة وفعالة، خاصة في البيئات ذات الموارد المحدودة.

الاجتماعية الهندسة (Social Engineering)

ما هي الهندسة الاجتماعية؟

الهندسة الاجتماعية هي أحد أخطر أشكال الهجمات الرقمية لأنها لا تعتمد فقط على التكنولوجيا، بل على خداع الأشخاص أنفسهم للحصول على معلومات أو الوصول إلى أنظمة أو حسابات.
يقوم المهاجم باستغلال الثقة، أو الفضول، أو الخوف، أو الشعور بالواجب، لإقناع الضحية باتخاذ إجراء معين مثل:

- مشاركة كلمة مرور
- تنزيل ملف مشبوه
- فتح رابط خطير
- تقديم معلومات شخصية أو مهنية حساسة

الهندسة الاجتماعية لا تحتاج إلى مهارات تقنية متقدمة، بل إلى معلومات مسبقة عنك وسيناريو مُقنع – مما يجعلها سهلة التنفيذ وخطيرة في آنٍ واحد.

الهندسة الاجتماعية في السياق الجزائري

في الجزائر، يتم استغلال السياق الاجتماعي والثقافي والسياسي لبناء رسائل خداعية أكثر إقناعًا، مثل:

- رسائل أو مكالمات من «صحفيين» يطلبون معلومات من نشطاء.
- أشخاص يدّعون أنهم «حقوقيون» أو «متضامنون» للوصول إلى شبكتك أو ملفاتك.

- طلبات تبرع أو دعم لحالات إنسانية وهمية.
- رسائل تدّعي أنها من جهات رسمية)شرطة، القضاء، الإدارة(... وتطلب تفاعلًا سريعًا.

أحيانًا، يتم جمع المعلومات الأساسية من حساباتك على مواقع التواصل لبناء سيناريو مقنع جدًا.

كيف تتعرف على محاولات الهندسة الاجتماعية؟

- طلب معلومات حساسة خارج السياق أو بشكل مستعجل.
- لغة عاطفية أو مريبة «)ساعدنا قبل فوات الأوان»، «نحتاجك الآن.(«
- جهة غير معروفة أو لا يمكن التحقق منها.
- شخص يدّعي أنه من مؤسسة تعرفها، لكنه يستخدم بريدًا غريبًا أو رقمًا غير رسمي.
- عدم تطابق بين أسلوب الكتابة والجهة المدّعى تمثيلها.

كيف تحمي نفسك من الهندسة الاجتماعية؟

- لا تشارك أي معلومات شخصية أو أمنية دون التحقق من هوية الطرف الآخر.
- لا تفتح روابط أو مرفقات من أشخاص لا تعرفهم، حتى وإن بدوا موثوقين.
- درّب نفسك على الشك البنّاء Healthy): (Skepticism أي لا تثق فورًا بأي طلب يأتيك، خاصة إن كان مستعجلًا.
- اسأل دائمًا: هل هذه الجهة تتواصل معي عادة؟ هل هذه الطريقة طبيعية للتواصل؟
- استخدم قنوات بديلة للتحقق)مثلًا: اتصل برقم رسمي لتأكيد طلب وردك في بريد إلكتروني مشبوه.(
- حدّ من كمية المعلومات الشخصية المتاحة على الإنترنت)مثلًا على فيسبوك أو لينكدإن.(

أدوات مفيدة:

- Email: Analyzer Headers للتحقق من مصدر البريد الإلكتروني الحقيقي.
- WHOIS: Lookup لمعرفة من يملك نطاق الموقع الْمرسل.
- Trend: Check Micro أداة مجانية لفحص الروابط المشبوهة.
- URLscan.io: لفحص محتوى موقع دون فتحه على جهازك.

مصادرة أو سرقة الأجهزة Loss or Theft Device

لماذا يُعتبر فقدان أو مصادرة الجهاز تهديدًا خطيرًا؟

في عمل المدافعين عن حقوق الإنسان، غالبًا ما يحتوي الهاتف المحمول أو الحاسوب على معلومات حساسة مثل:

- رسائل خاصة بينك وبين ضحايا أو شهود
- وثائق أو صور تتعلّق بانتهاكات
- حساباتك على شبكات التواصل أو بريدك الإلكتروني
- معلومات عن منظمات أو شركاء آخرين

في حال فُقد الجهاز أو سُرق أو تمت مصادرته من طرف جهة رسمية، فإن هذه البيانات قد تُستخدم ضدك أو ضد الآخرين، حتى دون الحاجة لكسر كلمات المرور، خصوصًا إذا لم تكن هناك إجراءات حماية كافية.

في السياق الجزائري

شهدنا حالات يتم فيها:

- توقيف النشطاء وتفتيش هواتفهم دون أمر قانوني واضح
- مصادرة أجهزة إعلاميين أو منظمات، ثم استخدامها في ملاحقات قضائية
- اختفاء أجهزة في أماكن عامة أو أثناء السفر دون معرفة الجهة التي استولت عليها

• في هذا السياق، تصبح الوقاية الرقمية ضرورة لحماية نفسك وحماية الآخرين.

كيف تحمي نفسك من مخاطر فقدان الجهاز أو مصادرته؟

1. تشفير الجهاز
- فعّل خاصية التشفير الكامل للهاتف أو الحاسوب.
-على الهواتف الحديثة، التشفير يكون مفعّلًا تلقائيًا عند استخدام قفل شاشة قوي (رمز أو بصمة.)

2. قفل الشاشة القوي
-استخدم رمز معقّد أو بصمة، وتجنّب الأنماط البسيطة أو الرموز القصيرة.
-فعّل القفل التلقائي بعد وقت قصير 30(ثانية مثلًا.)

3. النسخ الاحتياطي المنتظم
-احتفظ بنسخة من ملفاتك المهمة على خدمة سحابية مشفّرة مثل Tresorit أو Proton Drive.
-يمكنك استخدام وحدات تخزين خارجية مشفّرة أيضًا.

4. حذف المعلومات الحساسة بعد الاستخدام
-لا تحتفظ بالصور أو الوثائق الحساسة في الهاتف لأكثر من اللازم.
-احذف المحادثات التي لم تعد بحاجة إليها على التطبيقات المشفّرة.

5. خدمات تتبع الجهاز أو القفل عن بُعد
-فعّل ميزة «Find My iPhone» في iOS. أو أندرويد في «Find My Device»
-يمكنك من خلالها مسح البيانات أو قفل الهاتف عن بعد إذا فُقد.

6. تجنّب استخدام الجهاز الشخصي في المهام الأكثر حساسية

في بعض الحالات، يُفضل فصل العمل الحساس عن الهاتف الشخصي واستخدام جهاز مخصص إن أمكن.

في حال وقوع الحادث

إذا فُقد أو صودر الجهاز:

• تصرّف بسرعة: غيّر كلمات مرور حساباتك من جهاز آمن.
• أبلغ الأشخاص المرتبطين بك أن هناك احتمال تسريب معلومات.
• استخدم أدوات المسح عن بُعد إن كانت مفعّلة مسبقًا.
• وثّق الحادث وراجع أي تبعات قانونية أو رقمية له.

التهديدات عبر وسائل التواصل الاجتماعي

لماذا تُعتبر وسائل التواصل مصدر تهديد؟

تُعد منصات مثل فيسبوك، إنستغرام، تويتر (X) وغيرها أدوات فعالة في حملات التوعية والمناصرة، لكنها أيضًا تمثل بيئة خصبة للتهديدات الرقمية، خصوصًا للمدافعين عن حقوق الإنسان في الجزائر، حيث تزداد الرقابة، والهجمات المنظمة، وحملات التشويه والاستهداف الإلكتروني.

أمثلة واقعية في السياق الجزائري

- تلقي تعليقات أو رسائل مسيئة أو تهديدات مباشرة بعد نشر محتوى حقوقي.
- اختراق صفحات جمعيات أو نشطاء بسبب كلمات مرور ضعيفة أو بدون تحقق بخطوتين.
- بلاغات كاذبة تؤدي إلى إغلاق حسابات أو تقليل ظهور المنشورات (shadow banning).
- استخدام محتوى منشور ضد الناشط في إجراءات أمنية أو قانونية.
- إنشاء حسابات مزيفة تنتحل هوية ناشط بهدف تشويه سمعته أو تضليل المتابعين.

أنواع التهديدات الشائعة:

- التنمر والتحرش الرقمي
- التصيّد عبر الرسائل الخاصة
- التعقب الرقمي (Digital Stalking)
- انتحال الهوية
- التشهير العلني أو حملات التشويه المنظمة

كيف تحمي نفسك على وسائل التواصل الاجتماعي؟

1. تأمين الحسابات
-استخدم كلمة مرور قوية وفريدة لكل حساب.
-فعّل التحقق بخطوتين (2FA) عبر تطبيقات موثوقة مثل Authy أو Google Authenticator.
-لا تشارك بيانات الدخول مع أي طرف ثالث.

2. التحكم في الخصوصية
-اضبط إعدادات الخصوصية بحيث لا تظهر كل معلوماتك)مثل رقم الهاتف أو البريد(للعموم.
-حدّد من يمكنه التعليق أو الإشارة إليك .(Mention/Tag)
-راجع قائمة الأصدقاء أو المتابعين بشكل دوري.

3. مراجعة المنشورات
-فكّر مرتين قبل نشر أي محتوى حساس أو شخصي.
-تجنّب نشر معلومات قد تُستخدم ضدك أو ضد آخرين)مثل مواقع، أسماء، صور.(...
-احذف المنشورات القديمة غير الضرورية عند الحاجة.

4. التبليغ والحظر
-لا تتردد في حظر الحسابات المزعجة أو المؤذية.
-استخدم آليات التبليغ الرسمية داخل المنصة عند الضرورة.

5. الانتباه للحسابات المزيفة
-راقب إن كان هناك من ينتحل هويتك.
-أبلغ أصدقاءك ومتابعيك في حال ظهور حسابات مشبوهة تحمل اسمك أو صورتك.

أدوات مفيدة:

- Facebook: Checkup Privacy أداة من فيسبوك لمراجعة إعدادات الخصوصية.
- X: Pro لمراقبة التفاعلات وتنظيم المحتوى بفعالية.
- Who?: What Posted للبحث في منشورات قديمة.
- Google: Search Image Reverse لكشف استخدام صورك في حسابات مزيفة.

تقييم المخاطر الشخصية

ما هو تقييم المخاطر؟

تقييم المخاطر الشخصية في السياق الرقمي هو عملية تحليل وفهم التهديدات التي قد تواجهك عند استخدامك للتكنولوجيا، وتحديد ما يمكن أن يحدث، وكيفية الحد من الضرر إذا حدث.

بمعنى آخر، هو تفكير منهجي يساعدك على تقدير مستوى الخطر الرقمي الذي تتعرض له بناءً على طبيعة عملك، والأدوات التي تستخدمها، والمعلومات التي تتعامل معها، ثم اتخاذ قرارات واعية لتقليل هذا الخطر.

لماذا يعتبر تقييم المخاطر خطوة أساسية؟

لأن الأمن الرقمي ليس مقاسًا واحدًا يناسب الجميع. فالنشاط الحقوقي، مستوى الظهور العلني، والبيئة السياسية المحيطة كلها عوامل تجعل بعض الأشخاص أكثر عرضة للاستهداف من غيرهم.

بدون تقييم مخاطر واضح، قد تبالغ في الحذر من بعض الأمور وتتجاهل أخطار حقيقية، أو تستخدم أدوات غير مناسبة لمستوى تهديدك.

أمثلة:

- صحفية مستقلة تنشر عن الفساد تحتاج لتأمين مصادرها وتشفير بياناتها.
- ناشط يعمل في التوعية الرقمية قد لا يحتاج نفس مستوى الحماية، لكنه مهدد بالتصيّد أو انتحال الهوية.
- محامية تدافع عن معتقلي الرأي تواجه خطرًا قانونيًا مباشرًا في حال تسرب ملفات القضايا.

ما الذي يتضمنه تقييم المخاطر؟

- تحديد ما هي المعلومات أو الأنشطة الحساسة.
- من يمكن أن يستهدفك)أطراف التهديد.(
- ما الوسائل التي يمكن استخدامها ضدك)تقنية أو بشرية.(
- ما الآثار المحتملة في حال حدوث اختراق أو تسريب.
- ما مدى استعدادك حاليًا للحماية أو الاستجابة.

كيف تحدد نقاط الضعف في بيئتك الرقمية؟

بعد أن تفهم معنى تقييم المخاطر، تأتي الخطوة التالية: تحليل بيئتك الرقمية واكتشاف نقاط الضعف التي قد تُستخدم ضدك. المقصود هنا ليس فقط البرامج التي تستخدمها، بل أيضًا طريقة استخدامك للأجهزة، وسلوكك اليومي على الإنترنت، ومستوى وعيك بالمخاطر.

ما المقصود بـ"بيئتك الرقمية"؟

هي كل ما يتعلق بتفاعلك مع التكنولوجيا، وتشمل:

- الأجهزة التي تستخدمها)هاتف، كمبيوتر(...
- الشبكات التي تتصل بها)واي فاي منزلي، مقهى، شبكة العمل(
- الحسابات الرقمية)بريد إلكتروني، مواقع التواصل، حسابات سحابية(...
- الأدوات التي تستخدمها للتواصل أو تخزين البيانات
- المعلومات التي تتعامل معها
- الأشخاص الذين تتواصل معهم

خطوات لتحديد نقاط الضعف:

1. **راجع الأجهزة التي تستخدمها:**
   - هل جهازك محمي بكلمة مرور أو بصمة؟
   - هل تقوم بتحديث النظام والتطبيقات بانتظام؟
   - هل جهازك مشفّر في حالة السرقة أو المصادرة؟

2. **افحص حساباتك:**
   - هل تستخدم نفس كلمة المرور في أكثر من حساب؟
   - هل قمت بتفعيل التحقق بخطوتين (2FA)؟
   - هل حساباتك متصلة ببريد إلكتروني قديم أو ضعيف الأمان؟

3. **راقب طريقة استخدام الإنترنت:**
   - هل تستخدم VPN أو متصفحًا آمنًا عند زيارة مواقع حساسة؟
   - هل تتصل أحيانًا بشبكات واي فاي عامة بدون حماية؟
   - هل تفتح روابط أو مرفقات من مصادر غير مؤكدة؟

4. **فكّر في علاقاتك ومراسلاتك:**
   - هل تشارك معلومات حساسة عبر تطبيقات غير مشفّرة؟
   - هل كل من تتواصل معهم على دراية بأساسيات الأمن الرقمي؟
   - هل سبق أن تعرض أحد معارفك لاختراق وتم استخدامه للوصول إليك؟

نقطة الضعف لا تعني أنك ترتكب خطأ، لكنها إشارة إلى جانب بحاجة لتحسين. كلما عرفت ثغراتك، زادت قدرتك على حماية نفسك ومَن حولك.

أسئلة تساعدك على معرفة مستوى الخطر

تحديد مستوى الخطر الذي تتعرض له يعتمد على تحليل ذاتي واقعي لوضعك الشخصي والمهني. لا يوجد اختبار موحد للجميع، لكن طرح الأسئلة الصحيحة على نفسك يمكّن أن يساعدك على رسم صورة واضحة لمستوى التهديدات التي قد تواجهها، وبالتالي اتخاذ قرارات مناسبة لحمايتك الرقمية.

إليك مجموعة من الأسئلة الإرشادية: من أنا في هذا السياق؟

- هل أعمل في مجال يُعتبر "حساسًا" في بلدي)حقوق إنسان، إعلام، قضايا سياسية...؟(
- هل لدي نشاط علني أو ظاهر يجعلني معروفًا/ة لدى السلطات أو جهات معارضة؟
- هل أتعامل مع مواضيع أو جهات تُعتبر "مستهدفة" من قبل أطراف رسمية أو غير رسمية؟

ما طبيعة عملي واتصالاتي؟

- هل أحتفظ بمعلومات حساسة تتعلّق بأشخاص آخرين؟
- هل أُجري مقابلات أو توثيقًا لانتهاكات؟
- هل أشارك في حملات مناصرة رقمية؟
- هل أستخدم منصات عامة)مقالات، فيديوهات، محتوى توعوي(...؟

ما هي بنيتي الرقمية؟)أجهزتي، حساباتي، أدواتي(

- هل أستخدم أجهزة مملوكة لي أم أجهزة مشتركة؟
- هل أشارك كلمة المرور مع آخرين؟ هل أستخدم كلمات مرور قوية؟
- هل لدي نسخ احتياطية؟ وهل هي مشفّرة؟
- هل أستخدم تطبيقات مؤمّنة للتواصل؟ هل فعّلت التحقق بخطوتين؟

من قد يرغب في استهدافي؟

- هل هناك جهة محددة)أمنية، إعلامية، سياسية(... قد تكون مهتمة بالحصول على بياناتي؟
- هل سبق أن تلقيت تهديدًا مباشرًا أو غير مباشر؟
- هل تم استهداف زملائي أو شركائي من قبل؟

ماذا قد يحدث في حال تم اختراق أجهزتي أو حساباتي؟

- هل يمكن أن يتعرّض الآخرون للأذى؟
- هل يمكن استخدام محتوى شخصي ضدي أو ضد المؤسسة التي أعمل معها؟
- هل قد يؤدي ذلك إلى ملاحقة قانونية أو تشويه السمعة أو فقدان الثقة؟

الهدف من هذه الأسئلة: ليس إثارة الخوف، بل بناء وعي واقعي بالخطر يساعدك على تصميم خطة حماية تناسب وضعك، دون مبالغة أو استهانة.
إعداد خطة حماية فردية بسيطة

بعد أن قمت بتقييم وضعك وتحديد التهديدات ونقاط الضعف، حان الوقت لوضع خطة حماية شخصية تساعدك على التعامل مع المخاطر الرقمية بشكل عملي ومنظّم.

الخطة لا تحتاج إلى تعقيد، بل يجب أن تكون واضحة، قابلة للتطبيق، ومتناسبة مع قدراتك وواقعك.

خطوات إعداد خطة الحماية الفردية:

1. تحديد المعلومات الحساسة التي تحتاج لحمايتها فكّر في:

- بياناتك الشخصية)هويتك، مكانك، عائلتك(...
- معلومات الآخرين التي تحتفظ بها)شهود، ضحايا، شركاء(...
- حساباتك الأساسية)بريد إلكتروني، وسائل تواصل، أدوات تخزين(...
- الملفات المهمة)صور، مستندات، تقارير، مراسلات(...

2. اختيار الأدوات المناسبة لمستوى التهديد

بناءً على تقييمك، اختر أدوات تناسب احتياجاتك:

- **هل تحتاج إلى تطبيق مشفّر للتواصل؟**
- **هل تحتاج إلى VPN؟**
- **هل تحتاج إلى تقسيم استخدامك بين جهازين)شخصي / عمل(؟**
- **هل من المناسب حذف بعض الحسابات القديمة أو تقليل الحضور الرقمي؟**

3. وضع إجراءات يومية وأسبوعية بسيطة اجعل الحماية عادة. أمثلة:

- **مراجعة إعدادات الخصوصية كل أسبوعين**
- **تغيير كلمة المرور كل 3 أشهر**
- **التحقق من سجل الدخول للحسابات الحساسة**
- **تحديث البرامج بانتظام**
- **أخذ نسخة احتياطية مشفّرة كل أسبوع**

4. التحضير لحالات الطوارئ الرقمية
فكّر في "خطة ب" لو حدث اختراق أو فقدان للجهاز:

- **هل يمكنك مسح الجهاز عن بُعد؟**
- **هل تعرف الخطوات الأولى للتصرف؟**
- **هل لديك قائمة بالأشخاص الذين يجب إبلاغهم؟**
- **هل تحفظ كلمات المرور والبيانات الأساسية في مكان آمن خارج الجهاز؟**

5. مشاركة خطتك مع الأشخاص المقرّبين أو فريقك

إذا كنت تعمل ضمن مجموعة أو شبكة، احرص على أن يكون الجميع على دراية بالمخاطر وخطوات الحماية، حتى لا تكون الحماية فردية فقط.

هذه الخطة ليست ثابتة، بل قابلة للتعديل حسب تغير وضعك أو مستوى التهديد. راجعها كل ٣ إلى ٦ أشهر، أو بعد أي حادثة رقمية.

حماية الأجهزة الشخصية

الهاتف المحمول والحاسوب هما مفتاح دخولك إلى العالم الرقمي، لكنّهما أيضًا من أكثر العناصر استهدافًا في أي محاولة لاختراقك.

في السياق الحقوقي، يكون اختراق الجهاز بمثابة اختراق لحياتك الرقمية بالكامل: الرسائل، الملفات، الصور، الحسابات، وجهات الاتصال... كلّها معرضة للخطر. ولهذا، فإن حماية الأجهزة تُعدّ الركيزة الأساسية لأي خطة أمن رقمي.

لماذا حماية الأجهزة ضرورية؟

- **لأن معظم المعلومات الحساسة موجودة فعليًا على جهازك أو تمرّ من خلاله.**
- **لأن الأجهزة تُصادر أحيانًا أو تُفتّش دون إذن قانوني واضح.**
- **لأن الكثير من البرمجيات الخبيثة (Malware) تبدأ من ملف تم فتحه على الجهاز.**
- **لأن بعض الأجهزة تكون قديمة أو غير محدّثة، ما يجعلها أكثر عرضة للاختراق.**

يشمل هذا القسم:

1. إعدادات الأمان الأساسية للهاتف والحاسوب .2 كيفية تحديث النظام والتطبيقات بشكل آمن
3. استخدام التشفير لحماية البيانات
4. التعامل مع التطبيقات والأذونات بحذر
5. خطوات إضافية عند السفر أو في حالات الخطر

إعدادات الأمان الأساسية للهاتف والحاسوب

تأمين الهاتف أو الحاسوب لا يتطلب أدوات معقدة أو مكلفة، بل يمكن البدء بمجموعة من الإعدادات الأساسية التي تُقلّل بشكل كبير من خطر الاختراق أو الوصول غير المصرّح به إلى بياناتك.

أولًا: الهاتف المحمول

1. قفل الشاشة القوي

- استخدم رمز سري معقّد لا يقل عن 6 أرقام أو حروف، أو بصمة/ميزة التعرف على الوجه.
- تجنّب الأنماط البسيطة أو الأرقام المتكررة)مثل: 1234 أو .(0000
- فعّل القفل التلقائي بعد وقت قصير 30) ثانية أو أقل.(

2. تفعيل التشفير
- معظم الهواتف الحديثة Android) / (iPhone مفعّل فيها التشفير تلقائيًا عند استخدام قفل الشاشة.
- يمكنك التحقق من ذلك في الإعدادات < الأمان < التشفير.

3. إلغاء أذونات غير ضرورية للتطبيقات
- راجع التطبيقات التي تصل إلى الكاميرا، الميكروفون، الموقع الجغرافي، جهات الاتصال.
- امنع أي إذن لا ترى ضرورة له، خصوصًا في تطبيقات غير معروفة.

4. تقييد التثبيت من مصادر خارجية
- لا تسمح بتثبيت التطبيقات من خارج المتجر الرسمي Google). Play / App (Store
- هذا يمنع تثبيت تطبيقات مزيفة أو تحتوي على برمجيات تجسس.

5. تحديثات النظام والتطبيقات
- فعّل التحديثات التلقائية أو قم بمراجعتها يدويًا كل أسبوع.
- التحديثات تحميك من ثغرات قد تُستخدم لاختراقك.

ثانيًا: الحاسوب

1. كلمة مرور قوية عند تشغيل الجهاز
- لا تترك جهازك دون كلمة مرور.
- استخدم كلمة يصعب تخمينها، وفعّل القفل التلقائي عند ترك الجهاز.

2. تحديث نظام التشغيل بانتظام
سواء كنت تستخدم Windows أو macOS أو Linux، التحديثات تحميك من الثغرات المعروفة.

3. تشفير القرص الصلب
- على Windows: استخدم أداة BitLocker)متوفرة في بعض الإصدارات.(
- على macOS: فعّل FileVault من إعدادات الأمان.
- هذا يمنع الوصول إلى بياناتك حتى لو سُرق الجهاز.

4. مضاد فيروسات خفيف وفعّال
استخدم مضاد فيروسات مجاني وموثوق، مثل:
- Windows Defender (مُدمج في Windows 10/11)
- Bitdefender Free
- Malwarebytes Free (اليدوي للفحص)

5. إلغاء تثبيت البرامج غير الضرورية
- قلل من عدد البرامج المثبتة لتقليل احتمالات الثغرات.
- خصوصًا تلك التي تتطلب الوصول للإنترنت أو البيانات الشخصية.

كيفية تحديث النظام والتطبيقات بشكل آمن

التحديثات ليست فقط لإضافة ميزات جديدة، بل هي في الأساس وسيلة لإصلاح ثغرات أمنية خطيرة قد يستخدمها المهاجمون لاختراق جهازك أو سرقة بياناتك.

في كثير من الحالات، يكون الضحية عرضة للهجوم فقط لأنه تجاهل تحديثًا بسيطًا.

لماذا تُعد التحديثات ضرورية؟

- تعالج ثغرات أمنية مكتشفة حديثًا قد يستغلها القراصنة.
- تُعزّز من أداء النظام وتحسّن الحماية ضد البرمجيات الخبيثة.
- تطوّر من أداء التطبيقات وتُصلح مشاكل قد تؤثر على الأمان.

ملاحظة: كثير من الهجمات "الهادئة" تستغل ثغرات قديمة موجودة في أنظمة لم يتم تحديثها.

تحديث الهاتف الذكي

أجهزة Android:
- انتقل إلى الإعدادات < النظام < تحديثات النظام.
- فعّل التحديث التلقائي إذا كان متاحًا.
- يُفضل إجراء التحديث أثناء الاتصال بشبكة Wi-Fi.

أجهزة iPhone:
- اذهب إلى الإعدادات < عام < تحديث البرامج.
- فعّل تحديث تلقائي ليتم تثبيت التحديثات أثناء الليل.
- تأكد من وجود مساحة كافية في الجهاز قبل التحديث.

تحديث نظام التشغيل في الحاسوب

Windows:
- اذهب إلى الإعدادات < التحديث والأمان < Windows Update.
- فعّل التحديثات التلقائية.
- تأكد من أن التحديث يشمل تعريفات الأمان وبرامج مكافحة الفيروسات.

macOS:

- افتح تفضيلات النظام < تحديث البرامج.
- فعّل خيار تحديثات تلقائية لكل من النظام والتطبيقات.

تحديث التطبيقات والبرامج

لا تكتفِ بتحديث النظام فقط، بل راجع التطبيقات المثبتة يدويًا.
قم بتحديث:

- مثل المتصفحات Chrome، Firefox
- برامج الحماية مثل Malwarebytes
- أدوات التواصل مثل Signal، Zoom
- في حال استخدامك تطبيقات خارجية)خارج المتاجر الرسمية(، راجع مواقعها الأصلية للتحديث اليدوي.

نصائح عامة لتحديث آمن:

- لا تقم بتثبيت تحديثات من روابط تصل عبر البريد أو الرسائل، بل استخدم القنوات الرسمية.
- أعد تشغيل الجهاز بعد التحديث لضمان التثبيت الكامل.
- خذ نسخة احتياطية قبل تحديث النظام الرئيسي إن أمكن، خاصة على الحاسوب.

استخدام التشفير لحماية البيانات

التشفير هو إحدى أقوى الوسائل لحماية المعلومات المخزّنة على أجهزتك. فهو يجعل البيانات غير قابلة للقراءة لأي شخص لا يمتلك كلمة السر أو مفتاح التشفير، حتى لو تمكّن من الوصول إلى الجهاز نفسه.

لماذا تحتاج إلى التشفير؟

- في حال فقدان الجهاز أو مصادرته، يمكن منع الوصول إلى الملفات.
- يحمي الملفات الحساسة)مثل الصور، التقارير، بيانات الضحايا أو الشهود.(
- يضيف طبقة أمان إضافية فوق كلمة المرور العادية.

كلمة مرور الجهاز وحدها لا تكفي: إذا لم يكن القرص مشفّرًا، يمكن استخراج البيانات منه بسهولة باستخدام أدوات خارجية.

ما الذي يمكن تشفيره؟

- القرص الصلب)الذاكرة الكاملة للجهاز(
- ملفات أو مجلدات محددة
- وحدات تخزين خارجية USB) أو أقراص صلبة(
- تطبيقات التواصل أو التخزين السحابي التي تدعم التشفير

التشفير في الحاسوب

على (Windows (BitLocker

- إصدارات بعض في مدمج Windows (Pro وEnterprise).
- لتفعيله: الإعدادات < النظام < التشفير < BitLocker
- يتطلب وجود كلمة مرور أو حساب Microsoft آمن.

ملاحظة: إذا لم يكن متاحًا، يمكن استخدام برامج بديلة مثل .VeraCrypt macOS (FileVault) على مدمج في نظام macOS.

- لتفعيله: تفضيلات النظام < الأمان والخصوصية < FileVault
- سهل الاستخدام ولا يؤثر على الأداء في الأجهزة الحديثة.

التشفير في الهواتف

Android:

- معظم الهواتف الحديثة مشفّرة افتراضيًا عند استخدام قفل شاشة قوي.
- تحقق من ذلك عبر: الإعدادات < الأمان < التشفير)قد يختلف حسب الشركة المصنّعة.(

iPhone:

- جميع أجهزة iPhone الحديثة تُشفّر البيانات تلقائيًا عند تفعيل رمز القفل أو Face ID.
- تأكد من تفعيل "محو البيانات بعد 10 محاولات فاشلة" في الإعدادات < Face ID & Passcode

تشفير وحدات التخزين الخارجية

استخدم أدوات مثل:

- VeraCrypt: مجاني ومفتوح المصدر، يدعم تشفير أقراص كاملة أو مجلدات محددة.
- BitLocker to Go (في Windows): لتشفير USB.
- Disk Utility)في macOS): لإنشاء وحدات تخزين مشفّرة بصيغة .dmg.

نصائح إضافية

- اختر كلمات مرور قوية لتشفير القرص أو الملفات.
- احتفظ بنسخة احتياطية مشفّرة في مكان مختلف.
- لا تشارك مفتاح التشفير أو كلمة المرور إلا في حالات ضرورية، ومع أشخاص موثوقين جدًا.
- لا تعتمد على تشفير التطبيقات فقط، بل فعّل التشفير على الجهاز نفسه.

التعامل مع التطبيقات والأذونات بحذر

كثير من التهديدات الرقمية لا تأتي من "اختراق خارجي"، بل من تطبيق قمتَ أنت بتثبيته بنفسك. بعض هذه التطبيقات تطلب أذونات لا تحتاجها، أو تُشارك بياناتك مع جهات خارجية، أو قد تكون في الأصل مصمّمة للتجسّس.

ماذا يجب الانتباه للأذونات؟

لأن كل تطبيق قادر على الوصول إلى الكاميرا، الميكروفون، الموقع، أو جهات الاتصال يمكن أن يراقبك أو يجمع بياناتك. كلما منحت تطبيقًا إذنًا لا يحتاجه فعليًا، فتحت بابًا قد يُستغل ضدك.

خطوات عملية للتعامل الآمن مع التطبيقات:

1. حمّل التطبيقات فقط من المتاجر الرسمية

- استخدم Play Google لأجهزة أندرويد، وApp Store لأجهزة iPhone.
- لا تثبّت أي تطبيق بصيغة APK أو من موقع غير معروف.

2. راجع الأذونات بعد التثبيت

بعد تثبيت أي تطبيق، انتقل إلى الإعدادات < التطبيقات <]اسم التطبيق[< الأذونات. اسأل نفسك:

- هل يحتاج تطبيق الملاحظات للوصول إلى الكاميرا؟

- هل يجب أن يعرف تطبيق الطقس موقعي طوال الوقت؟
- لماذا يريد تطبيق الألعاب الوصول إلى جهات الاتصال؟

3 احذف التطبيقات غير الضرورية

- كل تطبيق إضافي هو نقطة ضعف محتملة.
- إذا لم تستخدم تطبيقًا خلال الأسابيع الأخيرة، احذفه.

4. استخدم بدائل مفتوحة المصدر كلما أمكن

غالبًا ما تكون أقل استغلالًا للبيانات. أمثلة:

- Signal بديل آمن لتطبيقات المراسلة.
- DuckDuckGo بديل لمحركات البحث التي تتبع نشاطك.
- F-Droid متجر تطبيقات مفتوحة المصدر لأندرويد.

5. فعّل إشعارات استخدام الكاميرا/الميكروفون

- على iPhone وAndroid، هناك مؤشرات تظهر عند استخدام الكاميرا أو الميكروفون.
- تأكد من مراقبتها، وإذا لاحظت نشاطًا دون إذنك، راجع التطبيقات فورًا.

6. استخدم أدوات تحليل الأذونات

هناك تطبيقات مثل Privacy Exodus)لأندرويد(تساعدك على تحليل تطبيقاتك ومعرفة ما تجمعه من بيانات.

قاعدة ذهبية:

- لا تمنح أي تطبيق صلاحية لا يحتاجها فعليًا.
- كل إذن هو بوابة، وكل بوابة غير ضرورية هي خطر محتمل.

خطوات إضافية عند السفر أو في حالات الخطر

عند السفر، خصوصًا إلى أماكن تشهد توتراً سياسيًا أو أمنيًا، أو عند المشاركة في أنشطة ميدانية أو احتجاجات أو لقاءات حساسة، يرتفع خطر مصادرة الأجهزة أو مراقبتها أو اختراقها. لذلك، من الضروري اتخاذ إجراءات احتياطية إضافية لحماية نفسك وبياناتك.

قبل السفر أو المشاركة في فعالية ميدانية:

1. احذف أو انقل أي معلومات حساسة

- انقل الملفات الحساسة إلى وحدة تخزين مشفّرة أو سحابة آمنة)مثل: Tresorit أو Proton Drive) ثم احذفها من الجهاز.
- لا تحتفظ بمحادثات خاصة على تطبيقات مثل WhatsApp – احذفها أو فعّل خاصية "الرسائل ذاتية الحذف."

2. فعّل التشفير الكامل للجهاز

- تأكد من أن الهاتف والحاسوب مشفّران كما شرحنا سابقًا.
- فعّل رمز قفل قوي أو بصمة وأوقف خاصية "فتح الهاتف تلقائيًا" عند الاقتراب من المنزل أو الجهاز الذكي.

3. احذف التطبيقات غير الضرورية مؤقتًا
• أزل التطبيقات الحساسة أو غير الأساسية التي قد تحتوي على بيانات أو تعرضك للمساءلة.

4. استخدم جهازًا بديلًا للسفر (إن أمكن)
• في بعض الحالات، يُفضل استخدام هاتف مؤقت أو حاسوب خفيف يحتوي فقط على الضروريات.

أثناء السفر أو الحدث:

1. تجنّب الاتصال بشبكات Wi-Fi عامة
• استخدم شريحة إنترنت خاصة إن أمكن، أو شبكة VPN موثوقة.
• لا تقم بإرسال معلومات حساسة أثناء اتصالك بشبكات عامة أو مفتوحة.

2. راقب المؤشرات الأمنية في جهازك
• راقب استهلاك البطارية أو بيانات الهاتف – أي زيادة مفاجئة قد تعني وجود تطبيق مشبوه يعمل في الخلفية.
• إذا شعرت بأن جهازك قد تعرّض للعبث)في المطار أو الفندق(...، لا تستخدمه قبل فحصه.

2. لا تترك أجهزتك دون رقابة
• لا تترك الهاتف أو الحاسوب دون مراقبة حتى ولو لوقت قصير، خصوصًا في الأماكن العامة أو الفنادق.

بعد العودة:

1. قم بفحص أجهزتك
• استخدم أدوات مثل Malwarebytes أو Scanner ESET لفحص أي برمجيات خبيثة.
• غيّر كلمات المرور الأساسية من جهاز آمن.

2. راجع إعدادات الأمان والخصوصية
• تحقّق من عدم حدوث تسجيل دخول غير مصرح به إلى حساباتك.
• افحص إعدادات حساباتك في Google، Facebook، وغيرها للتأكد من عدم إضافة أجهزة أو تطبيقات مشبوهة.

التعامل مع التكنولوجيا في أوقات الخطر يتطلب بُعد نظر ووعي رقمي، وليس فقط أدوات تقنية. كل إجراء صغير قد يُحدث فرقًا كبيرًا في حمايتك وحماية الآخرين.

الاتصال الآمن واستخدام الإنترنت بذكاء

الإنترنت هو وسيلة أساسية لعمل المدافعين عن حقوق الإنسان، لكنّه أيضًا أداة مراقبة واختراق إذا لم يتم استخدامه بوعي. كثير من الانتهاكات الرقمية تبدأ من تصفّح غير آمن، أو اتصال بشبكة غير موثوقة، أو استخدام متصفح غير محمي.

هذا القسم يزوّدك بأساسيات التصفح الآمن، واستخدام أدوات الخصوصية، واختيار القنوات المناسبة للاتصال، بما يتناسب مع السياق الجزائري.

يشمل هذا القسم:

1. اختيار المتصفح ومحرك البحث الآمن
2. استخدام VPN بشكل فعّال وآمن
3. التعرف على بروتوكولات الاتصال المشفّر (HTTPS, Tor) .
4. حماية خصوصيتك أثناء استخدام الشبكات العامة
5. نصائح عملية للتصفح الواعي والمجهول

اختيار المتصفح ومحرك البحث الآمن

أول خطوة نحو تصفح آمن تبدأ باختيار متصفح موثوق يحترم خصوصيتك، ومحرك بحث لا يتتبعك أو يجمع بياناتك الشخصية.

المتصفح ومحرك البحث هما "البوابة" التي تمرّ منها أغلب نشاطاتك الرقمية، لذلك فإن تأمينها يُقلّل بشكل كبير من احتمالية تعرضك للمراقبة أو الاستهداف.

ما هو المتصفح؟

المتصفح (Browser) هو البرنامج الذي تستخدمه للدخول إلى الإنترنت)مثل Chrome...(.، Firefox بعض المتصفحات تقوم بجمع معلومات عنك ومشاركتها مع جهات خارجية مثل المعلنين أو الحكومات، بينما أخرى تركّز على حماية خصوصيتك.

متصفحات موصى بها:

1. Mozilla Firefox

- مفتوح المصدر ويُعدّ من أفضل المتصفحات التي توازن بين الأداء والأمان.
- يمكنك تعديل إعداداته لتعزيز الخصوصية.
- يحتوي على إضافات مفيدة كثيرة (مثل: uBlock Origin، HTTPS Everywhere).

2. Brave

- يحظر الإعلانات وأدوات التتبع تلقائيًا.
- مبني على نفس محرك Chrome، ما يجعله سريعًا وسهل الاستخدام.
- يحتوي على وضع تصفح خاص باستخدام شبكة Tor.

3. Tor Browser

- مبني على Firefox، لكنه موجّه للخصوصية القصوى.
- يُخفي عنوان IP ويمنع تتبعك، لكنه أبطأ من المتصفحات العادية.
- مناسب عند الحاجة لتصفح مجهول في سياقات عالية الخطورة.

ملاحظة: لا يُنصح باستخدام Chrome Google في الأعمال الحقوقية، لأنه يجمع بيانات المستخدم ويُضعف الخصوصية.

محركات بحث تحترم خصوصيتك:

1. DuckDuckGo

- لا يسجّل عمليات البحث، ولا يخزّن معلومات شخصية.
- يمكن استخدامه كمحرك بحث افتراضي في جميع المتصفحات.

2. Startpage

- يُقدم نتائج من Google دون مشاركة بياناتك مع Google.
- خيار ممتاز لمن يفضل دقة نتائج Google دون التتبع.

3. MetaGer (يدعم اللغة الألمانية والفرنسية)

- محرك بحث من ألمانيا يهتم بالخصوصية.
- يُقدّم نتائج من عدة محركات دون تتبع.

إعدادات مهمة داخل المتصفح:

• فعّل "عدم التتبع" (Do Not Track) في الإعدادات.
• امسح ملفات الكوكيز (Cookies) بشكل دوري.
• استخدم التصفح الخاص (Private/Incognito Mode) عند التعامل مع محتوى حساس.

• ثبّت إضافات حماية مثل:
• uBlock Origin: لحجب الإعلانات والروابط الضارة.
• Privacy Badger: لمنع أدوات التتبع.
• HTTPS Everywhere: لتحويل المواقع تلقائيًا إلى الاتصال المشفّر.

استخدام VPN بشكل فعّال وآمن

VPN أو الشبكة الافتراضية الخاصة (Virtual Private Network) هي أداة تُستخدم لإخفاء عنوان IP الحقيقي الخاص بك، وتشفير اتصالك بالإنترنت، مما يجعل من الصعب على مزوّد الخدمة أو أي جهة أخرى تتبع نشاطك الرقمي أو معرفة موقعك.

في السياق الجزائري، يُعتبر استخدام VPN من الوسائل الضرورية لتجاوز الحجب، حماية الهوية الرقمية، وتجنّب الرقابة أو المراقبة على الإنترنت.

ماذا يفعل الVPN تحديدًا؟

• يُشفّر الاتصال بين جهازك والإنترنت.
• يُخفي عنوان IP الحقيقي الخاص بك.
• يسمح لك بالوصول إلى محتوى محجوب في بلدك.
• يحميك عند استخدام شبكات Wi-Fi عامة أو غير آمنة.

ليس كل VPN آمنًا. بعض الخدمات المجانية تقوم بتسجيل نشاطك أو بيع بياناتك لأطراف ثالثة، مما يجعل استخدامها أكثر خطرًا من عدم استخدام VPN أصلًا.

معايير اختيار VPN آمن:

:(No-Logs Policy) بسجلات يحتفظ لا
.1اختر VPN يؤكد بوضوح أنه لا يحتفظ بسجلات نشاط المستخدمين.
.2 تشفير قوي:
يجب أن يستخدم بروتوكولات تشفير قوية مثل OpenVPN أو WireGuard.
.3 خوادم متعددة:
وجود خوادم في عدة دول يُعزز الأداء والمرونة.
.4 سهولة الاستخدام:
واجهة بسيطة، دعم لأجهزة متعددة)هاتف، حاسوب، متصفح.
.5 خيار القفل التلقائي (Kill Switch):
ميزة تقوم بقطع الاتصال بالإنترنت تلقائيًا إذا توقف VPN فجأة، لحمايتك من التسرب.

خدمات VPN موثوقة)مراجَعة لعام :(2025

• Proton VPN
• من شركة سويسرية معروفة بحماية الخصوصية.
• لديه نسخة مجانية محدودة لكن آمنة.
• أنظمة يدعم Windows, macOS, Android, iOS.
• Mullvad VPN

- لا يتطلب بريدًا إلكترونيًا للتسجيل.
- سياسات خصوصية قوية، مفتوح المصدر جزئيًا.
- يدعم WireGuard وOpenVPN.
- IVPN
- خفيف، شفاف، يدعم الدفع بالعملات المشفرة

سياسة "لا سجلات" موثقة.

تجنّب استخدام خدمات مجانية مثل VPN Hola أو VPN Turbo، فهي غير موثوقة وقد تبيع بياناتك.

نصائح عند استخدام VPN:

- فعّله دائمًا عند الدخول إلى مواقع حساسة أو غير مشفّرة.
- استخدم خوادم قريبة لتحسين سرعة الاتصال.
- راقب أن يعمل الااKill Switch في الخلفية دائمًا.
- لا تعتمد على VPN وحده؛ اجمعه مع متصفح آمن وسلوك رقمي واعٍ.

التعرف على بروتوكولات الاتصال المشفّر (HTTPS، Tor)

عندما تتصفح الإنترنت، فإن المعلومات التي ترسلها وتستقبلها تمر عبر عدة نقاط قبل أن تصل إلى وجهتها. إذا لم تكن هذه المعلومات مشفّرة، فإن أي جهة في الطريق)مزود الإنترنت، نقطة Wi-Fi، جهة حكومية(... يمكن أن تتجسس عليها أو حتى تغيّر محتواها.

لهذا السبب من الضروري أن تعرف وتستخدم بروتوكولات الاتصال الآمن، وعلى رأسها:
HTTPS وTor.

أولًا: بروتوكول HTTPS

هو ما HTTPS؟

- هو النسخة الآمنة من HTTP، حيث يشير حرف S إلى "Secure" أي آمن.
- عند استخدامك لموقع يبدأ بـ https://، فإن الاتصال بين جهازك والموقع يكون مشفّراً.

لماذا هو مهم؟

- يمنع الأطراف الثالثة من التجسس على ما تفعله داخل الموقع.
- يحمي كلمات المرور والمعلومات التي تدخلها على الموقع.
- يقلل من خطر التلاعب بالمحتوى الذي تشاهده.

كيف تعرف أن الموقع يستخدم HTTPS؟

- يظهر رمز في شريط العنوان قبل رابط الموقع.
- يبدأ الرابط بـ https:// بدلًا من http://.

أدوات مفيدة:

إضافة HTTPS Everywhere (تعمل مع Firefox وBrave):

- تُجبر المواقع على استخدام HTTPS تلقائيًا إن كانت تدعمه.
- طوّرها مشروع Tor وEFF.

HTTPS لا يحميك من الموقع نفسه إذا كان ضارًا، لكنه يحميك من "الطريق" إلى الموقع.

ثانيًا: شبكة Tor

ما هي Tor؟

- هي شبكة خاصة تُستخدم لتصفح الإنترنت بشكل مجهول.
- Tor يُخفي عنوان IP الخاص بك، ويُمرّر اتصالك عبر عدة طبقات من التشفير)مثل البصلة(، مما يجعل تتبعك شبه مستحيل.

متى تستخدم Tor؟

- عند الحاجة لتصفح مواقع حساسة في بيئات عالية الخطورة.
- عندما تريد إخفاء هويتك وموقعك تمامًا.
- للوصول إلى مواقع onion. (شبكة Tor الخاصة.)

كيفية الاستخدام:

- بتحميل قم Tor Browser الرسمي الموقع من: https://www.torproject.org
- لا تستخدم Tor مع شاشة كاملة .(fullscreen)
- لا تقم بتسجيل الدخول إلى حسابات مرتبطة بهويتك الحقيقية أثناء استخدامه. Tor أبطأ من المتصفحات العادية بسبب التشفير المتعدد، لكنه أكثر خصوصية.

تذكير:

- HTTPS هو الحد الأدنى للتصفح الآمن – يجب التأكد من وجوده دائمًا.
- Tor هو الخيار الأنسب للحالات التي تتطلب سرية قصوى أو في بيئات رقابة صارمة.

حماية الخصوصية أثناء استخدام الشبكات العامة

الشبكات اللاسلكية العامة)مثل Wi-Fi في المقاهي، الفنادق، الجامعات(... تبدو مريحة وسريعة، لكنها غالبًا تكون غير مؤمّنة، وتشكل بيئة خطيرة لمستخدمي الإنترنت، خاصةً إذا كنت تتعامل مع معلومات حساسة أو تعمل في مجال حقوق الإنسان.

ما الذي يجعل الشبكات العامة خطرة؟

- يمكن لأي شخص متصل بنفس الشبكة أن يراقب حركة البيانات إذا لم تكن مشفّرة.
- المهاجم يمكنه إنشاء شبكة Wi-Fi مزيفة تشبه الشبكة الأصلية)مثلًا: Café_Free_WiFi(ليخدع المستخدمين.
- بعض الشبكات تطلب تسجيل الدخول عبر صفحات غير آمنة أو تجمع بياناتك الشخصية.
- لا توفر غالبًا حماية قوية مثل الجدران النارية .(firewalls)

كيف تحمي نفسك عند استخدام شبكة عامة؟

قبل الاتصال:

- إذا لم تكن مضطرًا لاستخدام الشبكة العامة، تجنبها تمامًا.
- استخدم بيانات الهاتف (3G/4G/5G) بدلًا من Wi-Fi كلما أمكن.
- لا تتصل إلا بالشبكات التي تعرفها وتثق بها (اسأل عن اسم الشبكة الحقيقي في المكان.)

أثناء الاتصال:

- فعّل VPN قبل الاتصال بأي موقع أو خدمة.
- لا تدخل كلمات مرور أو معلومات حساسة أثناء استخدام الشبكة.
- لا تفتح حساباتك المالية أو البريد الإلكتروني المهني دون حماية.
- تأكد من أن المواقع التي تدخلها تستخدم .HTTPS

على مستوى النظام:

- عطّل خاصية الاتصال التلقائي بالشبكات المفتوحة.
- فعّل جدار الحماية (firewall) إن كان متاحًا على الجهاز.
- لا تشارك الملفات أو الطابعات عبر الشبكة (disable file sharing).

بعد الانتهاء:

- "انسَ" الشبكة من إعدادات الجهاز (Forget this network).
- راقب نشاط حساباتك بعد الاتصال بأي شبكة مشكوك فيها.
- غيّر كلمات مرور الحسابات المهمة إذا شككت بتعرضك لاختراق.

أدوات مساعدة:

- VPN موثوق مثل ProtonVPN أو Mullvad لحماية اتصالك.
- جدار حماية مفعّل (مدمج في Windows/macOS أو باستخدام تطبيق خارجي).
- إضافة HTTPS Everywhere لضمان التصفح المشفّر.
- Network Analyzer (أداة متقدمة لمراقبة سلوك الشبكة).

نصائح عملية للتصفح الواعي والمجهول

حتى مع استخدام أدوات الحماية مثل HTTPS وVPN، يبقى سلوكك أثناء التصفح جزءًا حاسمًا في حماية نفسك وهويتك الرقمية. التصفح الآمن لا يعتمد فقط على التقنية، بل على الوعي الرقمي والممارسات اليومية.

خطوات عملية لحماية نفسك أثناء التصفح:

1. فكّر قبل النقر

- لا تفتح روابط مجهولة أو غير موثوقة، حتى لو جاءت من أشخاص تعرفهم.
- استخدم خاصية "معاينة الرابط" على الهاتف أو الماوس قبل النقر عليه.

2. لا تسجّل الدخول إلى حساباتك من أجهزة أو شبكات غير موثوقة

- تجنّب الدخول إلى بريدك أو حسابات التواصل من حواسيب عامة (مكتبات، فنادق،...).
- إذا اضطررت، غيّر كلمات المرور فورًا بعد الاستخدام.

3. استخدم التصفح الخاص (Private/Incognito Mode)

- يُقلل من حفظ بيانات التصفح، خصوصًا في حالات البحث عن مواضيع حساسة أو دخول مؤقت.

4. امسح سجل التصفح وملفات الكوكيز بانتظام

- يساعد ذلك في منع تتبعك من قبل المواقع أو المعلنين.

5. استخدم متصفحات وآليات تحمي هويتك عند الحاجة للتصفح المجهول

- في الحالات الحساسة، استخدم Browser Tor أو VPN مع متصفح آمن.
- تجنّب استخدام حساباتك الحقيقية أثناء التصفح المجهول.

6. انتبِه للمواقع المزيفة أو الصفحات المقلدة

- تأكد دائمًا من كتابة عنوان الموقع بنفسك بدلًا من اتباع الروابط.
- افحص النطاق (Domain) جيدًا: مثلًا facebook.com.security-update.xyz هو موقع مزيف.

أدوات الحماية مهمة، لكن سلوكك على الإنترنت هو خط دفاعك الأول. التصفح الواعي هو التوازن بين الوصول للمعلومة، وحماية نفسك ومَن حولك.

حماية الحسابات والهوية الرقمية

في عالم الإنترنت، حساباتك الرقمية)مثل البريد الإلكتروني، وسائل التواصل الاجتماعي، أدوات التخزين السحابي(... هي بوابة الوصول إلى بياناتك، وهويتك، وشبكتك الاجتماعية والمهنية.

أي اختراق لأحد هذه الحسابات قد يؤدي إلى:

- **تسريب معلومات حساسة**
- **انتحال هويتك**
- **استهداف زملائك أو شركائك**
- **تشويه صورتك أو سمعة منظمتك**

ولهذا، فإن تأمين الحسابات يُعدّ من أولويات السلامة الرقمية لأي مدافع أو مدافعة عن حقوق الإنسان، خصوصًا في السياق الجزائري حيث تم توثيق حوادث اختراق واستهداف مباشر عبر الحسابات الشخصية.

يشمل هذا القسم:

1. **إنشاء كلمات مرور قوية وإدارتها**
2. **تفعيل المصادقة الثنائية (Two-Factor Authentication)**
3. **حماية البريد الإلكتروني كبوابة رئيسية**
4. **معرفة مؤشرات اختراق الحساب والتصرف السريع**
5. **نصائح لتأمين الهوية الرقمية وعدم ترك أثر غير ضروري**

إنشاء كلمات مرور قوية وإدارتها

كلمة المرور هي خط الدفاع الأول لحساباتك. لكن كثيرًا من المستخدمين، حتى النشطاء، ما زالوا يستخدمون كلمات مرور ضعيفة أو مكرّرة، مما يجعلهم عرضة للاختراق بسهولة.

في السياق الحقوقي، اختراق الحسابات لا يؤدي فقط إلى فقدان السيطرة على بياناتك، بل قد يعرض آخرين للخطر أيضًا.

الأخطاء الشائعة في كلمات المرور:

- **استخدام كلمات مرور بسيطة مثل: 123456 أو password أو azerty**
- **تكرار نفس الكلمة في عدة حسابات**
- **حفظ كلمات المرور في تطبيق الملاحظات أو على ورقة**
- **استخدام معلومات شخصية يسهل معرفتها)مثل تاريخ الميلاد أو اسم الأم(**

كيف تُنشئ كلمة مرور قوية؟

1. **الطول المناسب**

يجب أن لا تقل عن 12 حرفًا. كلما كانت أطول، كانت أكثر أمانًا.

2. **العشوائية**

استخدم مزيجًا من الأحرف الكبيرة والصغيرة، الأرقام، والرموز. مثال: rM$9!cT2&z@W

3. **عدم الاعتماد على الكلمات القاموسية**

تجنّب استخدام كلمات حقيقية أو أسماء مشهورة، حتى مع بعض التعديلات.

4. **تجنّب التكرار**

لا تستخدم نفس الكلمة لأي حسابين مختلفين، حتى لو كانت قوية.

أدوات لإدارة كلمات المرور

بدلًا من حفظ عشرات الكلمات أو استخدام كلمة واحدة، يمكنك استخدام مدير كلمات مرور (Password Manager) يقوم بتوليد كلمات معقّدة وتخزينها بشكل مشفّر.

أدوات موصى بها:

- Bitwarden (مفتوح المصدر، مجاني للاستخدام الفردي، يدعم اللغة العربية)
- 1Password (مدفوع، واجهة سهلة جدًا)
- KeePassXC (نسخة بدون تخزين سحابي – تُخزّن الملفات محليًا)

لا تعتمد على المتصفحات فقط في حفظ كلمات المرور، إذ يمكن استخراجها بسهولة أحيانًا.

نصائح إضافية:

- لا تُشارك كلمات مرورك مع أي شخص، حتى المقربين.
- فعّل خاصية قفل مدير كلمات المرور بكلمة مرور رئيسية قوية.
- خذ نسخة احتياطية مشفّرة من مدير كلمات المرور (خاصة إن كنت تستخدم KeePass أو ملفًا محليًا).
- تفعيل المصادقة الثنائية (Two-Factor Authentication – 2FA)

حتى لو كانت كلمة مرورك قوية، قد يتم اختراقها من خلال التصيّد أو تسريب بيانات من خدمة تستخدمها. لذلك، تعتبر المصادقة الثنائية خط الدفاع الثاني، وهي من أكثر الوسائل فعالية لحماية حساباتك.

ما هي المصادقة الثنائية؟

هي إضافة خطوة تحقق ثانية عند تسجيل الدخول إلى حسابك، إلى جانب كلمة المرور.
بدلًا من الاكتفاء بكلمة السر، يُطلب منك:

- إدخال رمز مؤقت يُرسل إلى هاتفك أو يُولّد في تطبيق خاص،
- أو استخدام مفتاح أمان (Security Key)،
- أو الموافقة على إشعار داخل تطبيق موثوق.

أنواع المصادقة الثنائية:

1. تطبيقات الرموز المؤقتة (TOTP):
تُولّد رموزًا تتغيّر كل 30 ثانية، ولا تتطلب اتصالًا بالإنترنت. أمثلة:

- Authy (يدعم النسخ الاحتياطي السحابي)
- Google Authenticator
- FreeOTP (مفتوح المصدر)
- Aegis (لأجهزة مميز Android)

2. رسائل SMS:

- يُرسل رمز إلى رقم هاتفك.
- أقل أمانًا من التطبيقات، لأنه يمكن اعتراض الرسائل، لكنه أفضل من لا شيء.

3. مفاتيح الأمان الفيزيائية (مثل: YubiKey)

- أجهزة صغيرة تُوصَل عبر USB أو NFC.
- تُستخدم غالبًا في الحالات عالية الخطورة، وتُوفّر أمانًا مرتفعًا جدًا.

كيفية التفعيل:

1. ادخل إلى إعدادات الأمان في حسابك Google، Facebook، (ProtonMail، إلخ.)
2. ابحث عن خيار "المصادقة الثنائية" أو "التحقق بخطوتين."
3. اختر طريقة التفعيل (تطبيق رموز، SMS، أو مفتاح أمان.)
4. خزّن رموز الاسترداد (Backup Codes) في مكان آمن.

تذكير مهم:

لا تستخدم نفس جهاز الهاتف لاستلام رمز التحقق والدخول إلى الحساب.
الأفضل أن تستخدم تطبيق رموز على جهاز مختلف أو مفصول عن الإنترنت.

حماية البريد الإلكتروني كبوابة رئيسية

البريد الإلكتروني هو نقطة الدخول المركزية لحياتك الرقمية.
من خلاله يتم استرجاع كلمات المرور، إرسال الملفات، التواصل مع المؤسسات... وإذا تم اختراقه، يمكن للمهاجم السيطرة على حساباتك الأخرى، أو الوصول لمراسلات حساسة، أو حتى انتحال شخصيتك.

لماذا يُعدّ البريد الإلكتروني حساسًا؟

- لأنه غالبًا مرتبط بجميع حساباتك (Facebook...)، Zoom، Google Drive)
- أي شخص يسيطر عليه يمكنه إعادة ضبط كلمات مرورك الأخرى.
- يُستخدم في التسجيل بالخدمات والمنصات الحقوقية أو المهنية.

خطوات تأمين بريدك الإلكتروني:

1. استخدم بريدًا موثوقًا وآمنًا

ابتعد عن خدمات البريد غير المشهورة أو التابعة لمزوّدي خدمات محلية غير محمية. خدمات موصى بها:

- ProtonMail (مشفر، سويسري، يدعم الواجهة بالعربية)
- Tutanota (مشفر، مفتوح المصدر، ألماني)
- Gmail (آمن نسبيًا، لكنه أقل خصوصية – يحتاج تعزيز إعدادات الأمان)

2. فعّل المصادقة الثنائية

- باستخدام تطبيق رموز وليس SMS فقط.
- معظم خدمات البريد تدعم هذا الخيار.

3. اختر كلمة مرور قوية ومخصصة

- لا تكررها في أي حساب آخر.
- اجعلها طويلة ومعقدة، وخزّنها في مدير كلمات مرور.

4. راجع إعدادات إعادة التوجيه والتصفية

- تأكد من عدم إضافة عنوان بريد غريب يعيد توجيه الرسائل دون علمك.
- افحص الفلاتر (Filters) بحثًا عن أي إعدادات مريبة.

5. احذر من رسائل التصيّد الإلكتروني

- لا تفتح روابط أو مرفقات مشبوهة.
- افحص عنوان المرسل جيدًا، خصوصًا عند استلام رسائل من جهات رسمية أو مصرفية.

6. راقب تسجيلات الدخول

- معظم خدمات البريد تُظهر آخر المواقع والأجهزة التي دخلت إلى حسابك.
- افصل أي جهاز لا تعرفه، وغيّر كلمة المرور فورًا إن لاحظت شيئًا مريبًا.

نصيحة إضافية:
• من الأفضل فصل البريد الشخصي عن المهني/الحقوقي.
• استخدم بريدًا مخصصًا فقط للعمل في قضايا حقوق الإنسان، وتجنب ربطه بحسابات شخصية أو ترفيهية.

معرفة مؤشرات اختراق الحساب والتصرف السريع

رغم كل إجراءات الحماية، قد يحدث اختراق لحساباتك بسبب ثغرة في أحد التطبيقات، أو بسبب تصيّد ذكي، أو حتى تسريب من طرف ثالث.
من المهم أن تتعرف بسرعة على علامات الاختراق، وأن تتصرف فورًا لتقليل الضرر المحتمل.

مؤشرات تدل على أن حسابك قد يكون مخترقًا:

1. تغيّر غير مبرر في إعدادات الحساب
• كلمة المرور تغيرت دون علمك
• تم تغيير رقم الهاتف أو البريد الاحتياطي
• وجود بريد إلكتروني غريب مضاف لإعادة التوجيه

2. رسائل مرسلة لم ترسلها أنت
• ظهور رسائل غريبة في البريد الصادر أو سجل الدردشة
• أصدقاء أو زملاء يتلقون رسائل مشبوهة منك

3. إشعارات بتسجيل دخول من مواقع أو أجهزة غير معروفة
• إشعار بأن جهازًا جديدًا قام بتسجيل الدخول من موقع جغرافي غير مألوف
• دخول مشبوه من بلد أو جهاز لم تستخدمه قط

4. تعذّر الدخول إلى حسابك
• كلمة المرور لم تعد تعمل
• الحساب مقفل أو معلّق دون سبب واضح

في حال تأكدك أو شكك بالاختراق، اتبع هذه الخطوات فورًا:

1. افصل الجهاز من الإنترنت مؤقتًا; لتجنّب استمرار تسريب البيانات أو الأوامر الضارة.
2. غيّر كلمة المرور من جهاز آمن; استخدم جهازًا آخر لم يتأثر، وغيّر كلمة المرور فورًا.
إن تعذّر الدخول، استخدم خاصية "نسيت كلمة المرور" مع بريد احتياطي موثوق.
3. فعّل المصادقة الثنائية)إن لم تكن مفعلة سابقًا;(خاصة إن تمكنت من استعادة الحساب.
4. افحص الأجهزة والنشاطات المصرح بها; أزل أي أجهزة أو جلسات مشبوهة من إعدادات الأمان.
5. راقب السجل للتأكد من عدم تحميل بياناتك أو تغيير إعدادات الخصوصية.
6. أخبر الأشخاص المتأثرين (إن وُجدوا;) إذا استُخدم حسابك لإرسال رسائل مزيفة، نبّه المتلقين لتجاهلها.
هذا يخفف الضرر ويوضح أنك لست المسؤول عنها.
7. احصل على مساعدة تقنية عند الحاجة; خاصة إن استمر الاشتباه بوجود برمجية خبيثة على جهازك.

تذكير:
• سرعة التصرف في أول ساعات بعد الاختراق قد تمنع الكارثة.
• لا تنتظر حتى تتأكد بالكامل، بل ابدأ الحماية والتحقق عند أول علامة شك.

نصائح لتأمين الهوية الرقمية وعدم ترك أثر غير ضروري

في العمل الحقوقي، لا يكفي أن تحمي حساباتك فنيًا، بل يجب أن تدير هويتك الرقمية بذكاء، بحيث تُقلل من الأثر الذي تتركه، وتفصل بين حياتك الشخصية والنشاط المهني أو الميداني.
كل منشور، تعليق، حساب، أو صورة يمكن أن يُستخدم ضدك أو ضد من تعمل معهم، خصوصًا في بيئات حساسة مثل الجزائر.

ممارسات لتقليل الأثر الرقمي:

1. افصل بين هوياتك الرقمية

- استخدم بريدًا وحسابات منفصلة للعمل الحقوقي.
- لا تستخدم نفس الاسم الكامل أو الصورة الشخصية في جميع الحسابات.
- فكّر في استخدام أسماء مستعارة عند الحاجة، خاصة عند النشر في مواضيع حساسة.

2. قلّل من المشاركة العلنية للمعلومات الشخصية

- لا تنشر تفاصيل عن موقعك الجغرافي، أو نشاطك القادم، أو علاقاتك المهنية الحساسة.
- أوقف خاصية "الموقع الجغرافي" في الصور والمنشورات.

3. راقب إعدادات الخصوصية في حسابات التواصل

- تأكد من أن منشوراتك لا تظهر للعامة دون داعٍ.
- لا تقبل طلبات صداقة من أشخاص لا تعرفهم.
- افصل حساباتك المهنية عن الشخصية قدر الإمكان.

4. تجنّب استخدام رقم الهاتف الحقيقي عند التسجيل في التطبيقات

- استخدم رقمًا افتراضيًا أو بريدًا مؤقتًا إن أمكن)مثل: ProtonMail)، SimpleLogin
- بعض الجهات تشتري أو تصل إلى قواعد بيانات الأرقام والبريد.

5. احذف الحسابات القديمة أو غير المستخدمة

- الحسابات المهجورة قد يتم اختراقها أو استخدامها ضدك دون علمك.
- ابحث عن حساباتك القديمة باستخدام مواقع مثل:
- https://haveibeenpwned.com

تذكير:

- هويتك الرقمية ليست فقط من تصنعه أنت، بل أيضًا ما ينشره الآخرون عنك، أو ما تتركه خلفك.
- كل ما تشاركه اليوم، قد يُستخدم ضدك غدًا في بيئة تتزايد فيها الرقابة والاختراقات.

الاتصال الآمن والتعاون الرقمي في فرق العمل

العمل الجماعي ضروري في الحملات الحقوقية، لكن التعاون الرقمي غير المؤمَّن قد يكون نقطة ضعف خطيرة. مشاركة الملفات، الاجتماعات عبر الإنترنت، إدارة الحسابات المشتركة، والمراسلات اليومية... جميعها أنشطة تُستخدم كثيرًا في فرق حقوق الإنسان، ويجب التعامل معها بأدوات وسلوكيات آمنة، خاصة في السياق الجزائري حيث يمكن أن تُراقب هذه الأنشطة أو تُستهدف مباشرة.

يشمل هذا القسم:

1. استخدام أدوات مراسلة مشفّرة وآمنة للفِرق 2. مشاركة الملفات بشكل محمي ومراقَب
3. نصائح لاجتماعات آمنة عبر الإنترنت 4. إدارة كلمات المرور والبيانات المشتركة
5. تنظيم العمل الرقمي بطريقة تحمي الفريق والمعلومات

استخدام أدوات مراسلة مشفّرة وآمنة للفِرق

التواصل اليومي بين أعضاء الفريق، خاصة عند العمل في قضايا حقوق الإنسان، يجب أن يتم عبر أدوات تحترم الخصوصية وتُوفّر تشفيرًا قويًا. فالكثير من الاختراقات والتهديدات تبدأ من رسائل غير مؤمَّنة أو تطبيقات غير موثوقة.

ما المقصود بالمراسلة الآمنة؟

هي مراسلة تتم عبر أدوات تُوفّر على الأقل:

- تشفير من الطرف إلى الطرف (End-to-End Encryption)
- مصادقة ثنائية لحماية الحساب
- عدم تخزين الرسائل على الخوادم بعد قراءتها)أو حذفها التلقائي(
- إمكانية التحكم في من يمكنه الانضمام أو رؤية الرسائل

أدوات مراسلة موصى بها للفِرق:

1. Signal

- مفتوح المصدر، يوفر تشفيرًا قويًا جدًا.
- لا يخزن أي بيانات مستخدم، ولا يحتفظ بسجل الرسائل.
- يدعم الدردشات الجماعية والمكالمات الصوتية/المرئية.
- يدعم الرسائل ذاتية التدمير.

2. Element (Matrix)

- مبني على بروتوكول Matrix الآمن والموزّع.
- مناسب للعمل الجماعي والفرق المتوسطة والكبيرة.
- يدعم الدردشة، المكالمات، مشاركة الملفات.
- يمكن استضافته محليًا إذا توفرت البنية التحتية.

3. Wire

- تصميم احترافي، تشفير شامل، وواجهة نظيفة.
- يدعم الفصل بين الحسابات الشخصية والمؤسساتية.
- مناسب للاستخدام المؤسسي ولديه نسخة مجانية محدودة.

أدوات يُفضّل تجنّب استخدامها:

- WhatsApp: رغم دعمه للتشفير، إلا أنه مملوك لشركة Meta وقد يشارك بيانات "ميتا" وليس المحتوى مع أطراف ثالثة.
- Telegram: لا يستخدم التشفير من الطرف إلى الطرف في الدردشات الجماعية أو العادية افتراضيًا، ويحتفظ بالرسائل على خوادمه.
- Facebook Messenger: غير آمن للحملات أو القضايا الحساسة.

نصائح عند استخدام أدوات المراسلة:

- فعّل التحقّق بخطوتين فورًا.
- استخدم أسماء واضحة للغرف/المجموعات ولكن تجنب ذكر تفاصيل حساسة في العنوان.
- احذف الرسائل القديمة أو فعّل الحذف التلقائي.
- لا تستخدم نفس الحساب الشخصي للتواصل المهني.
- لا تشارك روابط المجموعات بشكل عام.

تذكير:

- الاتصالات الجماعية غير المؤمّنة قد تُهدد الفريق بأكمله، حتى لو كان كل فرد محميًا على حدة.
- أداة مراسلة آمنة هي استثمار مباشر في حماية الفريق والمعلومات الحساسة.

مشاركة الملفات بشكل محمي ومراقَب

في العمل الجماعي، غالبًا ما نشارك تقارير، صورًا، بيانات حساسة، أو مستندات تنظيمية. لكن مشاركة هذه الملفات عبر أدوات غير آمنة قد تُعرّض الفريق لمخاطر جسيمة، خاصة إن تم تحميلها أو فتحها من أجهزة غير محمية.

المخاطر المحتملة عند مشاركة الملفات:

- التسريب أو الوصول غير المصرّح به
- التعديل أو الاستبدال بمحتوى مزيف

- تضمين برمجيات خبيثة داخل الملفات
- فقدان السيطرة على الملف بعد مشاركته

أدوات آمنة لمشاركة الملفات:

1. Proton Drive

- تشفير شامل للملفات.
- إمكانية مشاركة الملفات برابط مؤمّن بكلمة مرور.
- يخزن الملفات في سويسرا تحت قوانين صارمة لحماية البيانات.

2. Tresorit

- مستوى أمان مرتفع، ومناسب للفرق والمنظمات الصغيرة.
- تشفير طرف لطرف مع تحكم في من يمكنه العرض أو التعديل.
- خيار جيد لمشاركة ملفات حساسة أو تعاونية.

3. CryptPad

- أداة مفتوحة المصدر لتحرير الملفات سحابيًا وتشاركيًا.
- لا يتطلب تسجيل حساب دائم.
- التشفير يتم بالكامل على جهاز المستخدم.

4. OnionShare

- مشاركة آمنة للملفات عبر شبكة Tor.
- لا يتطلب تحميل الملف على خادم، بل يُرسل مباشرة بين المستخدمين.
- مثالي للبيئات عالية الخطورة.

عند استخدام أدوات مشاركة الملفات:

- لا تشارك الملفات الحساسة عبر البريد العادي أو Drive Google بدون تشفير.
- استخدم روابط تنتهي صلاحيتها تلقائيًا.
- إن أمكن، اضغط الملف بكلمة مرور قبل رفعه (ZIP مشفّر أو باستخدام 7z.)
- لا تضع كلمات المرور في نفس الرسالة أو البريد الذي يحتوي الرابط.
- حدّد بوضوح من يمكنه الوصول (قراءة فقط – تعديل – تنزيل.)
- مشاركة الملفات ليست مجرد "تحميل وتنزيل"، بل هي مسؤولية تتطلب أدوات محمية وسلوكًا واعيًا.
- كل من يصل إلى ملف حساس يمثل نقطة ضعف أو حماية للفريق.

نصائح لاجتماعات آمنة عبر الإنترنت

الاجتماعات الرقمية أصبحت جزءًا أساسيًا من تنظيم العمل الحقوقي، خصوصًا للفرق المنتشرة جغرافيًا. لكن هذه الاجتماعات، إذا لم تُدار بأدوات وسلوكيات صحيحة، قد تصبح وسيلة لتسريب معلومات حساسة أو حتى لمراقبة الفريق.

التهديدات المحتملة:

- انضمام أشخاص غير مصرح لهم
- تسجيل الجلسة دون علم الحضور
- مراقبة الاتصال من جهات خارجية
- استخدام روابط عامة أو غير محمية

أدوات موصى بها لعقد اجتماعات آمنة:

1. Jitsi Meet

- مفتوح المصدر، يدعم التشفير، لا يتطلب إنشاء حساب.
- يمكن استضافته على خوادم خاصة لخصوصية أكبر.
- يدعم كلمات المرور وتحديد من يمكنه الانضمام.

2. Zoom (مع إعدادات خصوصية محسّنة)

- استخدم دائمًا "Waiting Room" وكلمة مرور.
- لا تشارك رابط الاجتماع علنًا.
- فعّل التشفير من الإعدادات (End-to-End Encryption).
- راقب المشاركين دائمًا.

3. BigBlueButton

- مناسب للتدريب وورش العمل.
- يدعم الخوادم الذاتية والتنصيب المحلي للمؤسسات الصغيرة.

خطوات تأمين الاجتماع:

1. استخدم كلمة مرور للاجتماع
2. فعّل غرفة الانتظار (Waiting Room) لقبول المشاركين يدويًا 3. احصر صلاحيات الحضور:
   - من يمكنه مشاركة الشاشة
   - من يمكنه التحدث أو تسجيل
4. لا تسجّل الاجتماع إلا بموافقة واضحة من الحاضرين 5. اختر اسمًا محايدًا للاجتماع لا يوضح موضوعًا حساسًا

نصائح إضافية:

- تأكد أن المشاركين يستخدمون أجهزة آمنة ومحدثة.
- لا تُشارك ملفات حساسة مباشرة في غرفة الدردشة.
- بعد انتهاء الاجتماع، راجع من انضم فعليًا وقم بحذف رابط الجلسة.

تذكير:

- الأمان في الاجتماعات لا يتوقف على الأداة فقط، بل على طريقة إدارتها.
- كل دقيقة في جلسة غير محمية قد تكون نافذة مفتوحة على معلومات حساسة.

إدارة كلمات المرور والبيانات المشتركة

في الفرق الحقوقية، من الشائع وجود حسابات أو أدوات تُستخدم بشكل جماعي (مثل البريد المهني، أدوات إدارة الملفات، مواقع التواصل...). لكن مشاركة كلمات المرور بشكل عشوائي أو غير مؤمّن قد يكون نقطة ضعف خطيرة.

مشاكل مشاركة كلمات المرور:

- صعوبة تتبع من قام بأي تعديل أو إجراء
- خطر التسريب غير المقصود من أحد أعضاء الفريق
- فقدان الوصول في حال غادر أحد الأعضاء الفريق
- كلمات مرور غير محدثة أو ضعيفة

كيف ندير كلمات المرور بشكل آمن كفريق؟

1. استخدم مدير كلمات مرور جماعي أدوات مثل:

- Bitwarden (Teams أو Organizations)
- 1Password for Teams
- Passbolt (مفتوح المصدر ويمكن استضافته ذاتيًا)

هذه الأدوات تتيح:

- مشاركة كلمات المرور بأمان دون كشفها
- تحديد من يمكنه "رؤية" أو "استخدام فقط" الكلمة
- تتبع سجل الاستخدام والتعديلات
- تغيير سريع وآمن لكلمات المرور عند الحاجة

2. تجنّب إرسال كلمات المرور عبر البريد أو الرسائل

- لا تستخدم البريد الإلكتروني، WhatsApp أو Telegram لمشاركة كلمات المرور.
- إن اضطررت، استخدم أدوات مشفّرة ومؤقتة مثل Privnote أو Onetimesecret.com، ثم غيّر الكلمة لاحقًا.

3. قم بتغيير كلمات المرور دوريًا

- خصوصًا عند مغادرة أحد أعضاء الفريق.
- ويفضّل تغييرها كل 3-6 أشهر في الأدوات الحساسة.

4. استخدم المصادقة الثنائية (2FA) إن أمكن

- وإذا كانت أداة تدعم 2FA لحساب جماعي، يمكن مشاركة الرموز باستخدام تطبيق مثل Authy أو Teams (اليدوي للنسخ) Aegis Backup.

تذكير:

- لا يجب أن تكون إدارة البيانات المشتركة عشوائية.
- نظام موثوق لإدارة كلمات المرور هو استثمار في استمرارية وأمان الفريق.

تنظيم العمل الرقمي بطريقة تحمي الفريق والمعلومات

العمل الحقوقي الرقمي الناجح لا يعتمد فقط على الأدوات، بل على هيكلة العمل بطريقة تقلل الأخطاء البشرية، وتوزع المسؤوليات بوضوح، وتحمي البيانات المشتركة.

خطوات عملية لتنظيم العمل الرقمي بوعي أمني:

1. حدد المسؤوليات بوضوح

- من المسؤول عن إدارة الحسابات؟
- من يملك صلاحية التعديل؟
- من يمكنه الوصول إلى الملفات الحساسة؟
- يجب أن يعرف كل عضو حدوده ومسؤولياته الرقمية.

2. قلّل من الوصول غير الضروري
- استخدم مبدأ "الحد الأدنى من الوصول:"
- لا تمنح صلاحيات أو كلمات مرور إلا لمن يحتاجها فعلًا.
- استخدم مستويات صلاحية مختلفة (عرض فقط، تحرير، إدارة....)

3. أنشئ سياسة داخلية بسيطة للأمان الرقمي
- حتى لو لم تكن مكتوبة بتفصيل، يجب أن يعرف الفريق:
- كيف نشارك الملفات؟
- ما الأداة المفضّلة للتواصل؟
- متى نغيّر كلمات المرور؟
- كيف نتصرف عند اختراق أو فقدان جهاز؟

4. درّب الفريق على الأساسيات
- نظّم جلسات دورية قصيرة للتذكير بأدوات الأمان، وكيفية التصرف في حالات الطوارئ.
- تأكد من أن كل فرد يعرف استخدام أدوات مثل VPN، إدارة كلمات المرور، والمراسلة المشفّرة.

5. استخدم أسماء واضحة وآمنة للمجلدات والملفات
- لا تضع كلمات حساسة في اسم الملف أو المجلد.
- مثال: "تقرير سري عن الانتهاكات".pdf. يمكن تغييره إلى: "TQ_R2025v1.pdf"

6. احرص على نسخ احتياطية مؤمّنة
- احتفظ بنسخ احتياطية مشفّرة للمعلومات المهمة في أكثر من مكان)محرك مشفر - سحابة آمنة.(
- عيّن شخصًا مسؤولًا عن المراجعة الدورية للنسخ.

التنظيم الجيد يخفف كثيرًا من الحاجة للتدخل عند الأزمات. حين يكون لكل شخص دوره وأدواته، تقلّ فرص الخطأ أو التسريب.

التخزين الآمن للبيانات والمستندات الحساسة

في عمل المدافعين والمدافعات عن حقوق الإنسان، يتم التعامل مع مستندات تتعلق بحالات حساسة، بيانات شخصية، صور، أدلة، أو مراسلات توثيقية.

تخزين هذه البيانات بشكل غير مؤمّن، سواء على الحاسوب أو في السحابة، قد يؤدي إلى تسريب خطير أو استهداف قانوني أو رقمي.

يشمل هذا القسم:

1. أنواع البيانات التي تحتاج إلى حماية خاصة
2. خيارات التخزين الآمن على الأجهزة الشخصية
3. التخزين السحابي الآمن والمشفّر
4. التشفير المحلي للملفات والمجلدات 5. إدارة النسخ الاحتياطية بوعي أمني

أنواع البيانات التي تحتاج إلى حماية خاصة

ليس كل ما نخزّنه على أجهزتنا أو في السحابة يحمل نفس المستوى من الخطورة، ولكن هناك أنواع من البيانات، إذا تم الوصول إليها أو تسريبها، قد تُعرّضك أو تُعرّض الآخرين للخطر.

تحديد هذه الأنواع يساعدك على تنظيم أولويات الحماية والتشفير والتخزين الآمن.

أمثلة على بيانات يجب حمايتها بدرجة عالية:

1. بيانات شخصية لأشخاص آخرين
- أسماء، أرقام هواتف، عناوين بريدية أو إلكترونية.
- صور، شهادات، نسخ وثائق رسمية (بطاقات هوية، جوازات سفر...)
- بيانات ضحايا انتهاكات، شهود، أو مصادر داخلية.

2. مستندات تنظيمية أو حساسة
- تقارير غير منشورة، ملفات التحقيق أو التوثيق.
- خطط عمل، استراتيجيات حملات، أو أسماء جهات داعمة أو شريكة.
- مراسلات داخلية بين الفريق أو مع المنظمات الأخرى.

3. معلومات مالية أو قانونية
- فواتير، تحويلات مالية، حسابات مصرفية.
- عقود، توكيلات قانونية، أو مراسلات قانونية حساسة.

4. أدلة رقمية أو صور توثيقية
- صور لمواقع أو أشخاص في أماكن حساسة.
- فيديوهات توثيقية لمخالفات أو انتهاكات حقوقية.
- ملفات بيانات Excel، (CSV، إلخ(تحتوي على تحليلات ميدانية أو شهادات.

5. بيانات تسجيل الدخول والمصادقة
- كلمات مرور أو رموز نسخ احتياطي.
- مفاتيح تشفير أو رموز دخول إلى حسابات الفريق.

أي ملف يحتوي على معلومة يمكن أن تُستغل ضد شخص أو منظمة يجب أن يُعامل على أنه "بيان عالي الحساسية."

لا تستخف بأي ملف حتى لو بدا بسيطًا، لأنه قد يكون "القطعة الناقصة" التي يحتاجها من يريد استهدافك أو استهداف من تعمل لأجلهم.

خيارات التخزين الآمن على الأجهزة الشخصية

تخزين الملفات الحساسة على الحاسوب أو الهاتف هو أمر شائع، لكنه قد يكون خطيرًا إذا لم تُتخذ الاحتياطات المناسبة. سواء كان جهازك عرضة للمصادرة أو الفقدان أو الاختراق، يجب أن تكون البيانات عليه مشفرّة ومنظمة ومحمية بكلمة مرور قوية.

خطوات لتأمين التخزين على جهازك الشخصي:

1. فعّل التشفير الكامل للقرص (Full Disk Encryption)
هذا يعني أنه حتى لو تمت سرقة الجهاز أو قرص التخزين، لا يمكن قراءة محتوياته دون كلمة المرور.

- لأنظمة macOS:

  استخدم ميزة FileVault (موجودة في إعدادات الأمان.)
- لأنظمة Windows:

  استخدم BitLocker)في الإصدارات الاحترافية – .(Pro أو بديل مفتوح المصدر مثل .VeraCrypt
- لأنظمة Linux:

  استخدم تشفير LUKS أثناء تنصيب النظام، أو VeraCrypt للتشفير الجزئي.

2. استخدم مجلدات مشفّرة لبياناتك الحساسة فقط

- لا تترك الملفات في أماكن غير محمية مثل "Documents" أو "Desktop".
- أنشئ مجلد مشفّر باستخدام VeraCrypt أو Cryptomator، وضع فيه فقط الملفات التي تحتاج حمايتها.

3. أنشئ حساب مستخدم بكلمة مرور قوية

- لا تستخدم حسابًا بدون كلمة مرور.

- تأكد من أن الحساب مقفول تلقائيًا بعد وقت قصير من عدم الاستخدام.

4. احذر من التخزين المؤقت غير المحمي

- بعض البرامج تحتفظ بنسخ مؤقتة غير مشفّرة)مثل برامج تحرير النصوص أو الصور(.
- احذف الملفات المؤقتة أو استخدم برامج تتيح الحفظ داخل مجلد مشفّر فقط.

5. احرص على التحديثات الدورية

- نظام التشغيل والبرامج يجب أن تبقى محدثة باستمرار لسد الثغرات الأمنية.

أدوات مفيدة:

الأداة	الاستخدام	النظام	التكلفة
VeraCrypt	تشفير ملفات أو أقراص أو مجلدات	Win/Mac/Linux	مجاني
Cryptomator	تشفير ملفات للمزامنة مع سحابة آمنة	Win/Mac/Linux	مجاني
FileVault	تشفير كامل للقرص (مُدمج مع macOS	macOS	مجاني
BitLocker	تشفير كامل للقرص	Windows Pro	مجاني
Tails OS	نظام تشغيل مباشر للمهام الحساسة	Linux (محمول)	مجاني

لا يكفي أن تخزّن الملف في "مكان مخفي"، بل يجب أن يكون مشفّرًا. وبدون كلمة مرور قوية وتحديثات مستمرة، تبقى البيانات مهددة.

التخزين السحابي الآمن والمشفّر

استخدام التخزين السحابي ضروري لكثير من المدافعين/ات عن حقوق الإنسان، خصوصًا للعمل الجماعي أو الوصول من أماكن مختلفة.

لكن معظم الخدمات التجارية)مثل Drive Google أو Dropbox) لا توفّر تشفيرًا كاملًا من الطرف إلى الطرف، مما يجعل بياناتك عرضة للاطلاع أو المصادرة إن طُلب منها قانونيًا أو فُرض عليها اختراق.

كيف تستخدم السحابة بأمان؟

1. اختر خدمة سحابية تدعم التشفير الحقيقي

أفضل الخدمات هي التي توفّر تشفير من الطرف إلى الطرف (End-to-End Encryption)، مما يعني أن الشركة نفسها لا تستطيع الوصول لمحتوى ملفاتك.

خدمات موصى بها:

- **الخدمة: Proton Drive**
  المميزات: تشفير كامل - سويسري - يدعم واجهة بالعربية
  الدولة: سويسرا
  مجاني: نعم

- **الخدمة: Tresorit**
  المميزات: أمان عالي - للفرق - تحكم دقيق بالصلاحيات
  الدولة: المجر/سويسرا
  مجاني: محدود

.الخدمة: Internxt
المميزات: تشفير شامل - مفتوح المصدر جزئيًا
الدولة: إسبانيا
مجاني: نعم

- **الخدمة: Cryptomator**
  المميزات: يُستخدم فوق أي خدمة سحابة لحماية الملفات
  الدولة: عالمي
  مجاني: نعم

- **الخدمة: OnionShare**
  المميزات: لمشاركة الملفات عبر تور بدون تخزين دائم
  الدولة: عالمي
  مجاني: نعم

2. أمّن الوصول إلى حسابك السحابي

- استخدم كلمة مرور قوية وفريدة
- فعّل المصادقة الثنائية
- لا تفتح ملفات السحابة من أجهزة عامة أو غير موثوقة

3. استخدم أدوات تشفير إضافية قبل الرفع

- يمكنك تشفير الملفات بنفسك قبل رفعها إلى Drive Google أو Dropbox.
- أدوات مثل Cryptomator تنشئ مجلدًا مشفّرًا يُزامن تلقائيًا مع السحابة.

4. راقب صلاحيات المشاركة دائمًا

- لا تشارك روابط "مفتوحة للجميع"
- استخدم كلمات مرور وروابط تنتهي صلاحيتها تلقائيًا إن أمكن
- احذف الملفات فور الانتهاء منها

السحابة ليست مكانًا آمنًا بحد ذاتها...

الأمان الحقيقي يبدأ بمن يستطيع الدخول إلى الملف، وكيف يتم تشفيره، وأين يتم تخزينه.
التشفير المحلي للملفات والمجلدات

عندما تحتاج إلى حفظ مجموعة ملفات محدَّدة - وليس القرص كله - فإن إنشاء »حاوية« أو »مجلد« مشفّر يتيح لك وضع الملفات الحسّاسة داخل »خزنة رقمية« لا تُفتح إلا بكلمة مرور قوية أو مفتاح تشفير. بهذا تحافظ على سهولة العمل اليومي مع إبقاء البيانات المحمية بعيدة عن أعين المتطفلين إذا فُقد الجهاز أو استُهدف بالاختراق.

خطوات التشفير المحلي

1. اختَر أداة التشفير المناسبة (انظر الأدوات الموصى بها أدناه.)
2. أنشئ حاوية أو مجلداً مشفَّراً — حدِّد الحجم، ونوع التشفير (AES-256 مثلًا)، وكلمة المرور.
3. ضع ملفاتك الحسّاسة داخل الحاوية ثم أغلِقها عند الانتهاء؛ تصبح غير مقروءة لمن لا يملك كلمة المرور.

4. احفظ نسخة احتياطية مشفَّرة من الحاوية على وسيط خارجي آمن أو في سحابة مشفَّرة.
5. غيّر كلمة المرور دوريًّا وتجنَّب تخزينها في مكان غير آمن.

أدوات موصى بها:

- **الأداة: VeraCrypt**

المميزات: مجانية مفتوحة المصدر، تشفير قوي للحاويات أو الأقراص الكاملة، تعمل على / / macOS Windows
Linux
مناسب لـ: حاويات مشفَّرة كبيرة أو أقراص USB كاملة

- **الأداة: Cryptomator (نسخة سطح المكتب)**

المميزات: مفتوحة المصدر، تشفير مجلدات بحجم ديناميكي، تَعمل محليًّا ويمكن مزامنتها مع أي سحابة
مناسب لـ: مجلدات عمل تتزامن مع Drive Google أو OneDrive مع إضافة طبقة تشفير

- **الأداة: Zip-7)وضع الأرشيف المشفَّر)**

المميزات: مجانية، ضغط + تشفير AES-256 لملفات أو مجلدات، تعمل على Linux / macOS / Windows
مناسب لـ: إرسال ملفات مشفَّرة كبريد مرفق أو تخزين كأرشيف مضغوط

- **الأداة: GnuPG (GPG)**

المميزات: معيار مفتوح لتشفير الملفات والمراسلات، يدعم تشفير مفتاح عام/خاص، متوفر لكل الأنظمة
مناسب لـ: مشاركة آمنة للملفات مع زميل يملك مفتاحك العام

اختر دائماً كلمة مرور طويلة وفريدة للحاوية المشفَّرة، ولا تحفظها في ملف نصي على الجهاز نفسه. إذا فقدت كلمة المرور، لا يمكن استعادة البيانات.

إدارة النسخ الاحتياطية بوعي أمني

النسخ الاحتياطي هو خط الدفاع الأخير ضد الفقدان المفاجئ للمعلومات — سواء بسبب حذف غير مقصود، تلف الجهاز، أو هجوم إلكتروني مثل الفدية .(Ransomware)

لكن النسخ الاحتياطي بحد ذاته قد يكون خطرًا إذا لم يتم بطريقة آمنة.

مبادئ النسخ الاحتياطي الآمن:

1. النسخ الاحتياطي يجب أن يكون مشفّرًا

- سواء كنت تحفظ الملفات في قرص خارجي أو في سحابة، يجب أن تكون النسخة نفسها مشفّرة باستخدام VeraCrypt أو Cryptomator.

2. اتبع قاعدة 3-2-1

- 3 نسخ من بياناتك
- 2 منها في مواقع مختلفة (مثلًا: جهازك + قرص خارجي)
- 1 منها خارج الموقع (مثل: سحابة آمنة)

3. احفظ النسخة في وسائط مخصصة ومأمونة

- استخدم أقراص خارجية موثوقة، واحتفظ بها في مكان آمن)خزانة مغلقة – موقع منفصل.(
- لا تحفظ النسخة الاحتياطية على نفس الجهاز الرئيسي.

4. حدّث النسخ الاحتياطية بانتظام

- اجعل ذلك عادة دورية (أسبوعيًا أو شهريًا حسب نوع البيانات.)
- استخدم أدوات تزامن أو برامج جدولة.

5. اختبر استعادة البيانات

- لا تنتظر الكارثة لتكتشف أن النسخة لا تعمل.
- جرّب فتح النسخة الاحتياطية والتأكد من قدرتك على استعادة الملفات منها بشكل سليم.

أدوات مساعدة:

- **الأداة: Duplicati**

المميزات: مفتوح المصدر، يدعم التشفير، النسخ إلى سحابة أو محلي، سهل الإعداد مناسب لـ: النسخ الدوري للملفات إلى Drive Google أو قرص خارجي

- **الأداة: Cryptomator**

المميزات: تشفير مجلدات قابلة للمزامنة، مثالي للسحابة
مناسب لـ: إضافة تشفير قبل تخزين الملفات في سحابة غير مشفّرة

- **الأداة: Time Machine (macOS)**

المميزات: نسخ احتياطي تلقائي ومتكامل، يدعم تشفير النسخة مناسب لـ: مستخدمي macOS لتأمين النظام كاملًا

- **الأداة: VeraCrypt**

المميزات: إنشاء نسخ احتياطية مشفّرة يدويًا، حماية عالية مناسب لـ: نسخ حساسة تتطلب أقصى درجات الأمان

النسخة غير المشفّرة قد تكون بنفس خطورة عدم وجود نسخة أصلًا. احرص على تشفيرها، وحمايتها بكلمة مرور قوية، وتحديثها بانتظام.

الحماية من المراقبة الرقمية والتتبع

في سياق عمل المدافعين/ات عن حقوق الإنسان، تُعدّ المراقبة الرقمية والتتبع من أخطر التهديدات، خاصة في دول مثل الجزائر، حيث قد تستخدم الجهات الرسمية أو أطراف أخرى أدوات متقدمة لرصد الاتصالات، وتتبّع المواقع، وقراءة البيانات.

هذا القسم يساعدك على فهم أشكال المراقبة، وأدوات الحماية منها، وتقنيات الحد من الأثر الرقمي.

يشمل هذا القسم:

1. أنواع المراقبة الرقمية وأساليب التتبع
2. تقنيات إخفاء الهوية وتقليل البصمة الرقمية 3. حماية المتصفحات ومحركات البحث
4. التعامل مع تطبيقات تتبع الموقع والكاميرا 5. أدوات مقترحة للحماية من المراقبة

أنواع المراقبة الرقمية وأساليب التتبع

لفهم كيفية الحماية، من المهم أولًا معرفة أنواع المراقبة الرقمية التي قد يتعرض لها المدافعون/ات عن حقوق الإنسان في السياق الجزائري:

الشبكية المراقبة (Network Surveillance)

- اعتراض البيانات عبر مزوّدي الخدمة)مثل المكالمات، الرسائل، تصفح الإنترنت.(
- استخدام أنظمة DPI)تفتيش الحزم العميق(لرصد المحتوى أو حظره.

تتبّع الموقع الجغرافي

- عبر إشارات الهاتف المحمول (Triangulation) أو بيانات GPS.
- من خلال التطبيقات التي تجمع بيانات الموقع دون علم المستخدم.

مراقبة الأجهزة

- عبر برامج تجسس (Spyware) مزروعة على الهاتف أو الحاسوب.
- استخدام برمجيات متقدمة مثل Pegasus أو أدوات محلية الصنع.

المراقبة عبر الكاميرا والمايكروفون

- تفعيل غير مرئي للكاميرا أو المايك لتسجيل الصوت أو الصورة.
- التطبيقات التي تطلب صلاحيات زائدة دون مبرر.

تتبع السلوك الرقمي

- عبر ملفات تعريف الارتباط (Cookies) والبصمات الرقمية للمتصفح.
- مراقبة التفاعل على مواقع التواصل الاجتماعي أو محركات البحث.

المراقبة لا تعني دائمًا استهدافًا مباشرًا، لكن من الضروري افتراض الاحتمال والعمل على تقليله باستمرار.
تقنيات إخفاء الهوية وتقليل البصمة الرقمية

من أجل الحد من قدرتهم على تتبعك أو الربط بينك وبين نشاطك الرقمي، تحتاج إلى تقنيات تُقلّل "بصمتك الرقمية" وتُخفي هويتك أثناء التصفح أو استخدام الأدوات الرقمية.

استخدم شبكة Tor عند الحاجة

- تُخفي هويتك وموقعك الجغرافي من خلال تمرير اتصالك عبر عدة خوادم مشفّرة.
- مناسبة لتصفح مواقع حساسة أو عند الإبلاغ عن انتهاكات.

استخدم أنظمة تشغيل محمولة وآمنة

- مثل OS Tails أو OS Qubes، تُشغَّل من USB، ولا تترك أثراً على الجهاز.
- مثالية للمهام القصيرة أو التصفح من أماكن غير آمنة.

قلّل عدد الأجهزة والحسابات المرتبطة بك

- لا تستخدم نفس البريد الإلكتروني، رقم الهاتف أو الحساب على كل المنصات.
- لا تدمج بين حساباتك الشخصية والحسابات الحقوقية.

أوقف خدمات التتبع الجغرافي

- عطّل GPS، Bluetooth، وخدمات الموقع عند عدم الحاجة.
- راقب صلاحيات التطبيقات واحذف غير الضروري منها.

استخدم متصفحات تركّز على الخصوصية

- مثل Brave أو Firefox)مع إضافات الحماية.(
- لا تسجّل الدخول أثناء التصفح الحساس، وامسح البيانات بعد كل جلسة.

ابحث باستخدام محركات لا تجمع بياناتك

- مثل DuckDuckGo أو Startpage بدلًا من Google.

لا توجد وسيلة واحدة كافية، لكن كل خطوة تقوم بها تُقلّل احتمالية تعقّبك أو مراقبتك.
حماية المتصفحات ومحركات البحث

المتصفح هو البوابة الأساسية لاستخدام الإنترنت، لكنه في الوقت ذاته أحد أخطر مصادر جمع البيانات والتتبع. كل ما تبحث عنه، تضغط عليه، أو تسجّله، يُخزّن في ملفات أو يُرسل إلى خوادم خارجية، ما لم تتخذ إجراءات حماية صارمة.

خطوات لحماية المتصفح من التتبع والمراقبة:

استخدم متصفحًا يركز على الخصوصية:

- Brave: مبني على Chromium، يحظر الإعلانات والمتتبّعات تلقائيًا.
- Firefox: إعدادات الخصوصية المشددة (Enhanced Tracking Protection).
- Tor Browser: مثالي للتصفح المجهول، يُخفي عنوان IP ويمنع التعقّب.

ثبّت إضافات الحماية الضرورية:

- uBlock Origin: لحظر الإعلانات والمتتبعات.
- Privacy Badger: من مؤسسة EFF، يكشف ويحظر أدوات التتبع الخفية.
- HTTPS Everywhere: يجبر المواقع على استخدام الاتصال المشفّر (HTTPS).
- ClearURLs: يزيل الروابط الطويلة التي تحتوي على متتبعات مضمّنة.
- Cookie AutoDelete: يحذف ملفات تعريف الارتباط تلقائيًا عند إغلاق التبويب.

فعّل إعدادات الخصوصية بيدك:

- أوقف الحفظ التلقائي لكلمات المرور وسجل التصفح.
- فعّل الحظر التلقائي للنوافذ المنبثقة ومتابعة التصفح الخاصة (Private Browsing).
- احذف الكوكيز والبيانات المؤقتة عند كل إغلاق للمتصفح.

محركات بحث تحترم خصوصيتك:

لا تستخدم:

- Google أو Bing أو Yahoo: تقوم بجمع تاريخ البحث، موقعك، جهازك، وحتى عنوان IP.

استخدم بدلًا منها:

- DuckDuckGo: لا يسجل بيانات المستخدمين، نتائج بحث محايدة، واجهة عربية متوفرة.
- Startpage: يعرض نتائج Google لكن دون تتبع أو حفظ بيانات.
- Mojeek: محرك بحث مستقل تمامًا لا يتتبع المستخدمين.

حتى أقوى المتصفحات تحتاج منك أن تضبطها بنفسك، وتستخدمها بوعي دائم.
تذكّر أن كل نقرة، كل عملية بحث، كل تسجيل دخول... قد يترك أثراً يُمكن ربطه بك، ما لم تُحكم السيطرة على أدواتك.

التعامل مع تطبيقات تتبع الموقع والكاميرا

العديد من التطبيقات والخدمات التي نستخدمها يوميًا تطلب صلاحيات الوصول إلى الموقع الجغرافي، الكاميرا، أو الميكروفون، حتى دون وجود سبب واضح. في سياقات القمع أو المراقبة المكثفة – كما هو الحال أحيانًا في الجزائر – قد تُستخدم هذه الصلاحيات كوسيلة للتجسّس أو تتبّع النشاط الميداني أو الشخصي.

أولًا: تعطيل تتبع الموقع الجغرافي

- أغلق خدمة الموقع (Location Services) على الهاتف عند عدم الحاجة.
- لا تُعطِ أي تطبيق صلاحية "الوصول الدائم" للموقع.
- راجع إعدادات التطبيقات واحذف أو عطّل التطبيقات التي لا تحتاج فعلًا الموقع.
- استخدم وضع الطيران أثناء التنقل في الأماكن الحساسة، مع العلم أنه لا يوقف GPS في كل الأجهزة.

ثانيًا: حماية الكاميرا والميكروفون

- لا تمنح الصلاحية لأي تطبيق إلا إذا كنت تستخدم الكاميرا أو الميكروفون فعلًا.
- راقب التطبيقات التي تفتح الكاميرا دون إذن واضح، واحذف التطبيقات المشبوهة.
- استخدم لاصقًا صغيرًا أو غطاء للكاميرا على الحاسوب المحمول.
- في بعض الهواتف، يمكن استخدام إعدادات النظام لتعطيل الكاميرا مؤقتًا.
- عند الاجتماعات المهمة، أغلق الهاتف تمامًا أو استخدم "وضع الطائرة + إزالة البطارية" إذا أمكن.

ثالثًا: راقب الصلاحيات باستمرار

- في Android: اذهب إلى "الإعدادات" < "الخصوصية" < "مدير الصلاحيات" وتحقّق من الصلاحيات الممنوحة.
- في iOS: اذهب إلى "الإعدادات" < "الخصوصية والأمان" < "خدمات الموقع" أو "الميكروفون / الكاميرا."
- استخدم تطبيقات مراقبة الصلاحيات مثل Privacy Exodus لتحليل التطبيقات المثبّتة على جهازك.

تذكير عملي:

عند كل تثبيت لتطبيق جديد، اسأل نفسك:

- هل يحتاج فعلًا إلى هذه الصلاحيات؟
- هل هناك بديل أكثر خصوصية؟
- هل يمكنني تعطيل هذا الخيار لاحقًا؟

أدوات مقترحة للحماية من المراقبة

الأداة: Tor Browser

المميزات: يخفي هوية المستخدم عبر شبكة تور - يمنع تتبع الموقع وعنوان IP - لا يحتفظ بالسجل مناسب لـ: التصفح المجهول، فتح مواقع محجوبة، تقليل الأثر الرقمي

الأداة: Tails OS

المميزات: نظام تشغيل مباشر من USB - لا يترك أي أثر - مزود بتطبيقات حماية مسبقة مناسب لـ: العمل من أماكن عامة أو عند استخدام أجهزة غير آمنة

الأداة: Signal

المميزات: تشفير طرفي للمراسلات - حذف تلقائي للرسائل - منع لقطات الشاشة مناسب لـ: التواصل الآمن عبر الهاتف

الأداة: Privacy Badger

المميزات: إضافة للمتصفح تحجب أدوات التتبع الخفية - من تطوير مؤسسة EFF مناسب لـ: حماية الخصوصية أثناء تصفح الإنترنت

الأداة: Exodus Privacy

المميزات: تطبيق لتحليل التطبيقات على أندرويد ومعرفة الصلاحيات ومكتبات التتبع المستخدمة مناسب لـ: تقييم التطبيقات المشبوهة وإزالة الضارة منها

الأداة: Blokada

المميزات: حجب الإعلانات وأدوات التتبع على مستوى النظام - بدون روت مناسب لـ: تحسين الخصوصية على هواتف Android

استخدام الأدوات لا يغني عن الوعي، لكنّه يُعطيك درعًا رقميًا يساعدك على العمل بأمان أكثر، خصوصًا عندما تكون في بيئة مراقبة.

التحقق من المعلومات والروابط والمرفقات المشبوهة

يتعرض المدافعون/ات عن حقوق الإنسان في الجزائر، كما في العديد من السياقات القمعية، إلى حملات تصيّد، خداع رقمي، أو محاولات تضليل من خلال رسائل أو روابط خبيثة، أحيانًا تبدو واقعية جدًا.
هذا القسم يساعدك على فهم طرق التحقق من الرسائل والمرفقات والروابط، وتجنّب الوقوع في فخاخ الهندسة الاجتماعية أو البرمجيات الخبيثة.

يشمل هذا القسم:

1. خصائص الرسائل المشبوهة وكيفية كشفها
2. فحص الروابط وتفكيكها قبل الضغط عليها
3. التعامل مع المرفقات بحذر
4. التحقق من الحسابات الوهمية أو المزيفة
5. أدوات مساعدة للتحقق الآمن

خصائص الرسائل المشبوهة وكيفية كشفها

الرسائل الاحتيالية أو الخبيثة تأتي غالبًا بشكل مقنع — بريد إلكتروني يبدو وكأنه من منظمة معروفة، أو رسالة واتساب من رقم غير مسجل، أو حتى تنبيه أمني زائف.
لكن هناك علامات واضحة تساعدك على اكتشافها مبكرًا وتجنّب فتح روابط أو مرفقات قد تكون خطيرة.

إشارات تحذيرية شائعة:

- لغة غير معتادة أو مُقلقة: مثل "تم اختراق حسابك"، "هناك مشكلة طارئة"، أو "يجب التصرف فورًا."
- وجود أخطاء لغوية أو نحوية أو علامات غريبة: في بعض الحالات تكون الترجمة سيئة أو غير منطقية، رغم أن هذا قد لا ينطبق دائمًا بسبب تطور الذكاء الاصطناعي.
- عناوين بريد مشبوهة: العنوان قد يبدو قريبًا من عنوان رسمي، لكنه يحتوي حرفًا مختلفًا أو نطاقًا غير معتاد (مثلًا: @g0ogle.com بدلًا من @google.com).
- روابط مختصرة أو مخفية: مثل استخدام خدمات اختصار الروابط (bit.ly, tinyurl) لإخفاء الوجهة الحقيقية.
- معلومات شخصية دقيقة بطريقة مريبة: كما في التصيّد الموجَّه، قد تحتوي الرسالة على اسمك الكامل أو تفاصيلك، تم جمعها من سجلات أو وسائل التواصل.

ماذا تفعل عند الشك برسالة؟

- لا تضغط على أي رابط فورًا.
- لا تفتح أي مرفق ما لم تتحقق من المصدر.
- تحقق من عنوان المرسل يدويًا.
- تواصل مع الجهة المرسِلة)عبر قناة منفصلة(للتأكد.
- التقط صورة للشاشة واحفظها للتوثيق إذا كان محتوى الرسالة تهديديًا أو غريبًا.

كل رسالة تتلقاها هي نقطة دخول محتملة للخصوم.
التروّي، والتحقق، وعدم التفاعل الفوري يمكن أن يحميك من اختراق أو تسريب خطير.
فحص الروابط وتفكيكها قبل الضغط عليها

الروابط)الـ URLs) هي من أكثر الوسائل شيوعًا في الهجمات الرقمية، وخاصة في حملات التصيّد أو محاولات اختراق الحسابات.

غالبًا ما يبدو الرابط طبيعيًا، لكنه قد يكون مخادعًا أو ضارًا بمجرد الضغط عليه.

كيف تفحص الرابط قبل الضغط؟

- **مرّر المؤشر فوق الرابط لترى العنوان الكامل في الزاوية السفلية من الشاشة)قبل الضغط.(**
- **تأكد أن اسم الموقع الرسمي ظاهر بوضوح بدون إضافات مشبوهة.**
- **لاحظ وجود رموز أو كلمات غير معتادة في بداية الرابط أو نهايته.**

أمثلة على روابط سليمة:

- https://www.amnesty.org/en/report-2024/ الموقع الرسمي لمنظمة العفو الدولية.
- https://drive.google.com/file/d/abc123/view رابط رسمي من Google Drive.
- https://proton.me/ الموقع الرسمي لخدمة البريد المشفّر ProtonMail.

أمثلة على روابط مزوّرة أو خطيرة:

- https://amnesty-org.securemail.co/report نطاق مشبوه يوهم أنه تابع للمنظمة.
- https://googledrive.files-update.store/d/abc123 اسم مشابه لخدمة Google لكنه ليس تابعًا لها.
- https://proton-login.net/reset نطاق مزيّف لاستدراج المستخدمين.

أدوات مفيدة لفحص الروابط:

- **موقع VirusTotal.com: الصق الرابط لفحصه بأكثر من 60 محرك فحص.**
- **موقع CheckPhish.ai: للتحقق من وجود تهديدات تصيّد.**
- **خدمة Whois Lookup: لكشف تاريخ إنشاء الموقع ومن يملكه.**
- **خدمة URL Expander)مثل: checkshorturl.com) لفك الروابط المختصرة ومعرفة وجهتها الحقيقية.**

لا تضغط على الرابط إذا:

- **جاء من مصدر مجهول أو غير متوقّع.**
- **طلب منك تسجيل الدخول أو تحديث بيانات حساسة فجأة.**
- **احتوى على لغة تحذيرية أو مغرية مثل:**
- **"تم اختراق حسابك، اضغط هنا"!**
- **"اربح الآن"!**
- **"يجب تأكيد هويتك فورًا لتفادي تعطيل الحساب."**

كل نقرة غير محسوبة قد تكون بوابة لاختراق جهازك أو حسابك. اقرأ الرابط كاملًا، وراجع النطاق (Domain) بدقة، وتجنّب التسرع.

التعامل مع المرفقات بحذر

المرفقات)الملفات المرسلة عبر البريد أو الرسائل(قد تبدو طبيعية، لكنها أحيانًا تحتوي على برمجيات خبيثة، أدوات تجسّس، أو ملفات تقوم بتفعيل تعليمات ضارة بمجرد فتحها.

أنواع المرفقات الخطيرة:

- ملفات بصيغ .exe.، .bat.، .scr. وهي ملفات تنفيذية يمكن أن تُثبّت برمجيات خبيثة.
- ملفات Office)مثل docx. أو (xlsx. تحتوي على "وحدات ماكرو "(Macros) مفعّلة.
- ملفات PDF تبدو عادية لكنها تحمل تعليمات خفية JavaScript) أو روابط داخلية ضارة.(
- أرشيفات مضغوطة)مثل zip. أو (rar. تحوي ملفات خبيثة بداخلها.

كيف تتعامل بأمان مع المرفقات:

- لا تفتح أي مرفق ما لم تكن تتوقعه فعلًا من المرسِل.
- افحص اسم الملف: قد يبدو رسميًا لكنه يحتوي على رموز أو امتدادين مخفيين، مثل:
- CV_Kamal.pdf.exe ملف تنفيذي مقنّع على شكل PDF
- document_final2024..pdf نقطتان قد تدل على محاولة خداع
- تأكد من أن صيغة الملف واضحة ومناسبة للسياق.
- مرّر الملف أولًا عبر أدوات فحص مثل: VirusTotal.com و MetaDefender Cloud

نصائح إضافية:

- لا تفتح الملفات المضغوطة أو المحمية بكلمة مرور من مصادر غير موثوقة.
- لا تضغط على الروابط أو الأزرار داخل ملف PDF أو Word قبل فحصها.
- فعّل إعدادات الحماية في برنامج قراءة الملفات لديك، مثل تعطيل الماكرو في Office .Microsoft
- إن أمكن، افتح المرفقات في بيئة افتراضية (مثل حساب مستخدم مؤقت أو باستخدام جهاز غير أساسي.)

حتى لو بدا الملف مرسلًا من جهة تعرفها، قد يكون البريد مخترقًا. دائمًا اسأل نفسك: هل هذا الملف متوقّع؟ هل صيغته آمنة؟

التحقق من الحسابات الوهمية أو المزيفة

في منصات التواصل الاجتماعي أو عبر البريد الإلكتروني، قد تتواصل معك حسابات تدّعي أنها منظمات، صحفيون، أو نشطاء – لكنها في الحقيقة مزيفة وتستهدفك لجمع معلومات أو لاختراقك.

علامات تساعدك على كشف الحسابات المزيفة:

- صورة الملف الشخصي مأخوذة من الإنترنت أو بدون وجه واضح.
- الاسم يحتوي على رموز غير معتادة أو تكرارات غريبة، مثل:
- human.rights2024_official
- kamal free_activist
- لا توجد منشورات حقيقية، أو المحتوى منسوخ من حسابات أخرى.
- المتابعة غير متوازنة)يتابع مئات لكن لا يتابعه أحد تقريبًا.(
- الحساب أُنشئ حديثًا ولا يوجد له سجل نشاط واضح.

طرق التحقق من الحساب:

- ابحث عن صورة الحساب باستخدام Images Google أو Tineye للتأكد من أنها ليست مسروقة.
- ابحث عن اسم الحساب في محركات البحث: هل له وجود سابق؟ هل ذُكر في مواقع موثوقة؟
- في البريد الإلكتروني، افحص العنوان بدقة)قبل @ وبعده(، وتأكد أنه يتبع النطاق الرسمي.
- تواصل مع الجهة الأصلية عبر وسيلة أخرى)مثل موقعهم الرسمي أو رقم هاتف معروف(لتأكيد أن هذا الحساب تابع لهم.

كن حذرًا إذا طلب منك الحساب:

- معلومات شخصية أو صور حساسة.
- إرسال ملفات أو فتح روابط.
- إجراء مكالمات صوتية أو فيديو من خلال تطبيقات غير مألوفة.
- المشاركة في نشاط رقمي دون مرجعية واضحة.

الهندسة الاجتماعية تبدأ غالبًا عبر حساب يبدو موثوقًا.
لا تفتح باب التواصل مع أي جهة دون تحقق حقيقي من الهوية والهدف.
أدوات مساعدة للتحقق الآمن

إلى جانب الحذر الشخصي، هناك أدوات بسيطة وفعالة يمكن أن تساعدك في التحقق من الروابط، الرسائل، والمرفقات، وتكشف المحاولات المشبوهة بسرعة.

أدوات لفحص الروابط والمرفقات:

VirusTotal موقع مجاني يمكنك من خلاله فحص أي رابط أو ملف قبل فتحه. يُحلله باستخدام أكثر من 60 محرّك فحص أمني.
MetaDefender Cloud بديل آخر متقدم لفحص الملفات المشبوهة، خاصة ملفات Word و.PDF
CheckShortURL يكشف الوجهة الحقيقية لأي رابط مختصر)مثل bit.ly) قبل الضغط عليه.
URLscan.io يُظهر لك كيف يبدو الموقع دون الحاجة لزيارته، ويحذرك إذا كان الموقع خبيثًا.

أدوات للتحقق من الصور والحسابات:

Google Images / TinEye يمكنك رفع صورة للتحقق من مصدرها أو معرفة إن كانت مسروقة من الإنترنت.
Exodus Privacy (Android بهواتف خاص) يفحص التطبيقات ويكشف إن كانت تحتوي على أدوات تتبع أو صلاحيات مشبوهة.
Whois Lookup يكش ف لك معلومات عن ملكية المواقع وعمر النطاق، وهي مفيدة لمعرفة ما إذا كان الموقع جديدًا ومشبوهًا.

إضافات مفيدة للمتصفح:

Privacy Badger حظر أدوات التتبع الخفية أثناء التصفح.
ClearURLs يزيل المعلومات الإضافية من الروابط)مثل أدوات التتبع(بشكل تلقائي.

تذكير أخير:

استخدام هذه الأدوات لا يتطلب معرفة تقنية متقدمة.
مجرد تخصيص دقيقة واحدة للتحقق يمكن أن يمنع اختراقًا أو تسريبًا خطيرًا.
الاستجابة للطوارئ والهجمات السيبرانية

ماذا تفعل عند الشك في حدوث اختراق؟

المقدمة:

في بعض الأحيان، قد لا يكون من الواضح على الفور ما إذا كان جهازك أو حسابك قد تم اختراقه. ولكن وجود بعض العلامات التحذيرية قد يكون كافيًا لاتخاذ إجراءات أولية سريعة للحد من الضرر المحتمل.
اتصرف المبكر يمكن أن يقلل من الخسائر ويمنع تطور الهجوم.

إشارات قد تدل على وجود اختراق:

- تلقي تنبيهات أمنية غير مألوفة من حساباتك.
- ملاحظات عن تسجيل دخول من مواقع أو أجهزة غير معروفة.

- تباطؤ غير مبرر في الجهاز أو سلوك غير اعتيادي.
- رسائل تم إرسالها من حسابك دون علمك.
- برامج أو تطبيقات لم تقم بتثبيتها.

خطوات أولية يجب اتخاذها فورًا:

1. افصل الاتصال بالإنترنت:
لفصل الجهاز عن أي اتصال خارجي مؤقتًا لتجنب تسريب البيانات أو استمرار الاختراق.

2. لا تقم بإطفاء الجهاز فورًا:
قد يحتوي على معلومات مهمة للتحقيق لاحقًا. بدلًا من ذلك، أوقف الاتصال بالشبكة فقط.

3. وثّق كل شيء:
التقط صورًا للشاشة أو دوّن الملاحظات عن أي سلوك غير طبيعي.

4. غيّر كلمات المرور من جهاز آمن:
خاصةً لحسابات البريد الإلكتروني والخدمات المهمة.

5. تواصل مع جهة موثوقة للدعم الفني أو الأمني:
سواء كانت منظمة داعمة، خبير في مجالك، أو جهة تقنية موثوقة.

6. أبلغ الفريق أو المؤسسة إن وُجدت:
حتى يتمكنوا من اتخاذ إجراءات احترازية أيضًا.

خطوات العزل والتحقيق الأولي

لماذا العزل مهم؟
عند الشك بحدوث اختراق، الهدف الأول هو الحد من انتشار الضرر ومنع المهاجم من الاستمرار في الوصول إلى بياناتك أو الشبكة.
العزل هو الإجراء المؤقت الذي "يعزل" الجهاز أو الحساب المصاب عن باقي الأنظمة.

خطوات العزل والتحقيق الأولي:

1 .افصل الجهاز عن الإنترنت أو الشبكة اللاسلكية/السلكية:
استخدم وضع الطيران أو افصل كابل الإنترنت.
لا تطفئ الجهاز فجأة، فقد يؤدي ذلك إلى فقدان الأدلة.

توقّف عن استخدام الحسابات المصابة:
لا تفتح البريد أو تتصفح الإنترنت من الجهاز المشبوه.
استخدم جهازًا آخر موثوقًا لتغيير كلمات المرور.

افحص الأجهزة المتصلة الأخرى:
تحقق مما إذا كانت هناك أجهزة أخرى قد تأثرت (في حال استخدامك شبكة منزلية أو مشتركة.)
هل لاحظت رسائل غريبة من حساباتك على وسائل التواصل أو البريد الإلكتروني؟

ابدأ بجمع الأدلة:
سجل الملاحظات: ما الذي حدث؟ متى؟ ما هي الأعراض؟
التقط لقطات شاشة لأي رسائل خطأ، أنشطة غير معتادة، أو تنبيهات أمنية.

تحديد مصدر الاشتباه

هل نقرت على رابط مشبوه؟ فتحت مرفقًا؟ حملت تطبيقًا؟
تحديد النقطة التي بدأ منها الخطر يساعد على تقييم الضرر.

لا تحاول "إصلاح كل شيء" قبل الفهم الكامل:

تجنب حذف الملفات أو تثبيت برامج تنظيف إلا إذا كنت متأكدًا، كي لا تضيع آثار الاختراق.

تواصل مع مختص إن وُجد:

اطلب المساعدة من خبير أو جهة داعمة لتقييم الوضع بشكل أعمق.

استرجاع السيطرة وتأمين الحسابات

استرجاع السيطرة على الحسابات:

1. استخدم جهازاً آمناً لتسجيل الدخول:

إذا كنت تشك في أن جهازك مخترق، لا تستخدمه لاسترجاع حساباتك. استخدم جهازاً آخر موثوقاً وآمناً

2. غيّر كلمات المرور فوراً:

- ابدأ بالحسابات الحساسة (البريد الإلكتروني الرئيسي، الحسابات البنكية، وسائل التواصل.)
- استخدم كلمات مرور قوية وفريدة لكل حساب.
- لا تعيد استخدام كلمات المرور القديمة. 3. فعّل المصادقة الثنائية :(2FA)
- قم بتفعيلها لكل حساب يدعمها، ويفضّل استخدام تطبيق مصادقة وليس الرسائل القصيرة .SMS
- احتفظ بنسخ احتياطية من رموز الاستعادة. 4. راجع إعدادات الأمان داخل كل حساب:
- تأكد من عدم إضافة عناوين بريد أو أرقام غريبة.
- راجع الجلسات المفتوحة والأجهزة المتصلة، واغلق أي جلسة لا تعرفها.
- أزل أي صلاحيات مشبوهة لتطبيقات أو خدمات مرتبطة بالحساب. 5. أبلغ جهات الاتصال إذا لزم الأمر:

إذا استُخدم حسابك لإرسال رسائل أو روابط ضارة، أخبر الأشخاص المتأثرين حتى لا يقعوا في الفخ. 6. أعد بناء الثقة الرقمية:

- تابع سلوك الحسابات لعدة أيام للتأكد من أنها لم تُخترق مجددًا.
- استمر في مراقبة الإشعارات وتفعيل التنبيهات الأمنية أينما أمكن.

التعلّم من الحادث وتحديث الإجراءات

تقييم ما حدث:

1. ما الذي حدث بالضبط؟

ما هو نوع الحادث)اختراق حساب، فيروس، تصيّد(...؟
متى وقع؟ وكيف اكتشفته؟

2. ما هي نقاط الضعف التي استُغلّت؟

هل كانت هناك كلمة مرور ضعيفة؟
هل تجاهلت تحديثاً أمنياً؟
هل فتحت رابطاً أو مرفقاً مشبوهاً؟

3. ما هي الأضرار؟

هل سُرّبت بيانات؟
هل تم الوصول إلى حسابات أخرى؟
هل تأثرت جهة اتصالك أو عملك الحقوقي؟

تحديث سلوكك الرقمي:

1. قم بتعديل إعدادات الخصوصية والأمان على جميع حساباتك.
2. غيّر عاداتك الرقمية:

لا تفتح الروابط أو المرفقات من مصادر غير موثوقة.
لا تستخدم كلمات مرور مكررة أو سهلة.
تعوّد على مراجعة إعدادات الأمان دوريًا.

3. تعلم من الحادث، ولا تلُم نفسك:

التهديدات تتطور باستمرار، والمهم أن تتعلم وتمنع تكرارها.
شارك تجربتك - إن أمكن - مع زملائك من المدافعين ليستفيدوا منها.

أدوات للمساعدة في التحسين:

- مدونات ومصادر مهنية للأمن الرقمي.
- دورات توعية عبر الإنترنت.
- المشاركة في تدريبات سيبرانية جماعية.

من تتواصل معه؟ جهات الدعم والتبليغ

لماذا من المهم التواصل بعد الحادث؟

في بعض الحالات، قد يكون الاختراق أو التهديد محدودًا، ويمكن التعامل معه شخصيًا.
لكن في حالات أخرى، يكون من الضروري إشراك جهات داعمة للمساعدة في احتواء الخطر، خاصة إذا تعلّق الأمر بتسريب بيانات، ابتزاز، أو تهديد مرتبط بالعمل الحقوقي.

التواصل في الوقت المناسب يمكن أن:

- يوفر دعمًا تقنيًا متخصصًا.
- يساعدك في توثيق الحادث رسميًا.
- يقلّل من احتمالية تكرار الهجوم أو اتساعه.
- يقدم دعمًا قانونيًا أو نفسيًا عند الحاجة.

من يمكنك التواصل معهم؟

1. جهة دعم تقني موثوقة:

- إن كانت مؤسستك الحقوقية تعمل مع فريق تقني خارجي، أبلغهم فورًا.
- أو تواصل مع منظمات تدعم الأمن الرقمي مثل:
- Access Now – خدمة Helpline
- Front Line Defenders
- CiviCERT

2. فريق داخلي إن وجد:

- في حال وجود مسؤول تكنولوجيا أو منسق أمني داخل المؤسسة، أطلعه على الحادث فورًا.
- حتى في المجموعات الصغيرة، اختر "شخص مرجعي" تكون لديه فكرة مسبقة عن خطوات الاستجابة.

3. زملاء أو شبكة موثوقة:

- تبادل الخبرات قد يساعد في اكتشاف أن الهجوم ليس فرديًا.
- بعض الزملاء قد يكونوا تلقّوا نفس الرسالة أو الرابط ويجب تنبيههم.

4 منظمات قانونية أو داعمة للمدافعين:

- في حالة تعرضك للابتزاز، أو التهديد المرتبط بالنشاط الحقوقي، يفضل التواصل مع جهات قانونية داعمة.

ماذا تقول عند التبليغ؟

- لا تحتاج إلى لغة تقنية.
- صف ما حدث بشكل واضح:

"وصلني بريد إلكتروني بدا رسميًا، فتحت الرابط وبعدها لاحظت أن"...
"حسابي في تليغرام أرسل رسائل غريبة لم أرسلها بنفسي"...

- شارك التفاصيل الأساسية واللقطات إن وجدت.

أنت لست وحدك. هناك مجتمعات ومنصات وفرق متخصصة تعمل لحمايتك وتمكينك — لا تتردد في طلب المساعدة.
الملاحق العملية والأدوات المساعدة

قائمة مراجعة يومية للأمن الرقمي

تهدف هذه القائمة المبسطة إلى دعم المدافعين عن حقوق الإنسان في بناء عادة المراجعة اليومية أو الأسبوعية للعناصر الأساسية في السلامة الرقمية.

استخدامها لا يتطلب خبرة تقنية، ويمكن تعديلها بحسب السياق أو طبيعة العمل.

عناصر يُنصح بمراجعتها دوريًا:

هل جهازك محدّث بآخر التحديثات الأمنية؟
هل تم تحديث تطبيقات الهاتف والكمبيوتر؟
هل تستخدم كلمات مرور قوية وغير مكررة؟
هل المصادقة الثنائية مفعّلة لحساباتك الأساسية؟
هل مررت اليوم أو الأسبوع الماضي على روابط غير مألوفة؟ راجعها.
هل استقبلت أي رسائل أو مرفقات مشبوهة؟ لا تتفاعل معها.
هل يوجد نسخ احتياطي حديث للملفات المهمة؟
هل تعمل من شبكة واي فاي آمنة؟
هل قمت بتسجيل الخروج من الأجهزة التي لا تستخدمها؟
هل تفحصت صلاحيات التطبيقات؟ هل أحدها طلب صلاحيات زائدة؟
هل شاركت معلومات شخصية في مواقع أو نماذج غير موثوقة؟
هل أرسلت ملفات حساسة؟ وهل استخدمت وسيلة إرسال آمنة؟
هل راجعت إعدادات الخصوصية على وسائل التواصل؟

نصيحة:

يمكنك طباعة هذه القائمة وتعليقها قرب جهازك، أو استخدامها في بداية كل أسبوع لمراجعة عاداتك الرقمية، فرديًا أو داخل فريق العمل.

نموذج خطة حماية فردية مبسطة

وجود خطة حماية رقمية حتى لو كانت بسيطة، يساعد على تقليل المخاطر عند حدوث أي طارئ، ويعزز من وعي المدافع/ـة بكيفية إدارة أمنه الرقمي اليومي.
هذا النموذج ليس نهائيًا، ويمكن تعديله حسب السياق والاحتياجات الشخصية.

الخطوة :1 تحديد المعلومات الحساسة

- ما هي أنواع المعلومات التي أتعامل معها؟

مثل: بيانات ضحايا، تقارير، صور، وثائق قانونية، حسابات بريد

- أين تُخزن هذه المعلومات؟

على جهازك، على سحابة، في هاتفك، في فلاش USB...

الخطوة :2 تقييم الأدوات والخدمات

- هل أستخدم كلمات مرور قوية ومختلفة؟
- هل فعّلت المصادقة الثنائية على حساباتي؟
- هل أستخدم تطبيقات آمنة للتواصل)مثل Signal أو ProtonMail؟
- هل جهاز الكمبيوتر والهاتف مُحدّثان؟
- هل أملك نسخًا احتياطية للمعلومات المهمة؟

الخطوة :3 التخطيط لحالات الطوارئ

- إذا فقدت الوصول إلى حساباتي، ما هو الإجراء البديل؟
- هل يوجد شخص موثوق يمكنه مساعدتي؟
- هل أملك قائمة جهات دعم يمكنني التواصل معها؟
- ما هو التطبيق/الخدمة البديلة إن تعطل الأساسي؟

الخطوة :4 خطوات تحسين فورية (تُحدث شهريًا)

- ما هي نقطة الضعف الرئيسية لدي الآن؟
- ما أول شيء يجب أن أُصلحه؟
- هل أنشأت قائمة مراجعة شهرية؟
- ما التطبيق أو الخدمة التي عليّ التوقف عن استخدامها لأنها غير آمنة؟

يمكنك طباعة هذا النموذج وملؤه بخط اليد، أو نسخه في ملف خاص على جهازك وتحديثه كل ٣ أشهر. تذكّر: الخطة لا يجب أن تكون مثالية، لكن يجب أن تكون موجودة وتخدمك.
روابط أدوات موثوقة مختارة)مبسطة ومُحدّثة(

حماية الحسابات وكلمات المرور:

- Bitwarden – مدير كلمات مرور مجاني وآمن:
https://bitwarden.com
- 1Password – خيار مدفوع بمستوى أمان عالٍ:
https://1password.com
- Pwned Been I Have – لمعرفة ما إذا تم تسريب بريدك الإلكتروني أو كلمة مرورك:
https://haveibeenpwned.com
- List Auth Factor Two – للتحقق من المواقع التي تدعم المصادقة الثنائية:
https://2fa.directory

تطبيقات تواصل آمنة ومشفّرة:

- Signal – تطبيق مفتوح المصدر للرسائل والمكالمات المشفرة:
https://signal.org
- ProtonMail / Proton Pass / Proton Drive – بريد إلكتروني وتخزين مشفر بالكامل:
https://proton.me
- Threema – بديل آمن للواتساب)مدفوع(:
https://threema.ch
- Element) Matrix) – تواصل جماعي مشفر ومفتوح المصدر:

https://element.io

فحص الملفات والروابط:

- VirusTotal – لفحص الملفات والروابط عبر عشرات محركات الفحص:
https://virustotal.com
- MetaDefender Cloud – فحص متقدم للملفات منظمة من OPSWAT:
https://metadefender.opswat.com
- CheckShortURL – كشف الروابط المختصرة المشبوهة:
https://checkshorturl.com
- URLscan.io – تحليل محتوى الروابط دون فتحها مباشرة:
https://urlscan.io

أدوات لحماية التصفح والخصوصية:

- Browser Tor – لتصفح الإنترنت بخصوصية عالية ومنع التتبع:
https://www.torproject.org Mozilla Firefox + Extensions (HTTPS Everywhere, uBlock Origin, Privacy Badger) https://www.mozilla.org/firefox
- Browser Brave – متصفح يركّز على الخصوصية ويمنع الإعلانات تلقائيًا:
https://brave.com

أدوات تشفير وتخزين آمن:

- VeraCrypt – تشفير كامل للأقراص أو الفلاشات:
https://www.veracrypt.fr
- Cryptomator – تشفير ملفاتك قبل رفعها إلى الخدمات السحابية:
https://cryptomator.org
- Tresorit – خدمة تخزين سحابي مشفّرة (بديل لـ Dropbox):
https://tresorit.com

أدوات متفرقة مفيدة:

- Tails OS – نظام تشغيل آمن يُستخدم من الفلاش USB دون أثر على الجهاز:
https://tails.boum.org
- Privacy Exodus – لتحليل التطبيقات ومعرفة أدوات التتبع فيها (للأندرويد):
https://exodus-privacy.eu.org
- Skiff Mail / Skiff Pages – بديل لبريد ومشّفر حديث Google Docs:
https://skiff.com
- SecureDrop – منصة آمنة لتسريب الوثائق للصحفيين:
https://securedrop.org

نصائح عامة:

- تأكد دائمًا أنك تزور الموقع الرسمي، لا تنسخ الروابط من مصادر مجهولة.
- إذا كنت غير مرتاح لاستخدام أداة معينة، استعن بصديق موثوق أو مدرّب.
- لا تركّب أكثر من أداة في نفس الوقت إذا كانت تؤدي نفس الوظيفة، كي لا يحدث تضارب.
- الادوات تم اقتراحها وقت اعداد هذا الدليل، ومع التطور المتسارع، يجب المراجعة الدورية والتحقق قبل البدأ بالاستخدام.

قائمة تطبيقات موصى بها في الجزائر

رغم القيود القانونية والرقابة الرقمية المتزايدة، لا يزال بإمكان المدافعين عن حقوق الإنسان في الجزائر استخدام عدد من التطبيقات الآمنة والفعّالة، شريطة الحذر وفهم سياق استخدامها.

فيما يلي مجموعة تطبيقات وأدوات تم اختبارها واستخدامها ميدانيًا، ويمكن الاعتماد عليها في التواصل، التوثيق، الحماية، والتنقل الرقمي اليومي:

تطبيقات تواصل آمنة:

Signal
الأفضل للمراسلة المشفّرة، يدعم المكالمات والمجموعات. سهل الاستخدام، ويتيح إرسال ملفات وصور مشفّرة.
موصى به بشدة في السياقات ذات الرقابة.

- Threema https://signal.org
لا يحتاج إلى رقم هاتف، مما يجعله مثاليًا للخصوصية القصوى. مدفوع لمرة واحدة، ويُعد بديلًا ممتازًا في بعض الحالات.
https://threema.ch

تطبيقات لتوثيق الانتهاكات:

- Tella
تطبيق مفتوح المصدر لتوثيق الصور والفيديوهات بشكل آمن ومشفّر. يمكن إخفاؤه وتعيين كلمة مرور، ويدعم حذف آلي للمحتوى عند الحاجة.

- Umbrella https://tella-app.org
تطبيق تدريبي وأمني في آن واحد. يقدم نصائح فورية وإجراءات عند السفر، التهديد، أو المراقبة.
https://securityinabox.org/en/umbrella

تطبيقات تصفح محمية:

- Tor Browser
لتجاوز الحجب والتصفح دون تتبع.
يعمل على الحاسوب والهاتف، لكن يتطلب اتصالًا مستقرًا. ممنوع أحيانًا، فكن حذرًا في الاستخدام.
https://www.torproject.org
- Firefox / Brave (مع إضافات خصوصية)

بديلان ممتازان للمتصفحات التقليدية.
HTTPS Everywhere و uBlock Origin مثل إضافات تثبيت يفضل.
https://brave.com https://mozilla.org/firefox

تطبيقات تشفير وتخزين:

- Cryptomator
سهل الاستخدام على الحاسوب والهاتف لتشفير الملفات قبل رفعها إلى Drive Google أو Dropbox.

- Proton Drive https://cryptomator.org
خدمة تخزين سحابي مشفّرة بالكامل، من مطوري ProtonMail. يمكن استخدامها لتبادل ملفات مهمة بأمان.
https://proton.me/drive

تطبيقات إدارة كلمات المرور:

Bitwarden
التطبيق الأفضل حاليًا في الجمع بين السهولة والأمان.
يمكنك مزامنته بين أجهزتك، وإنشاء كلمات مرور قوية بنقرة واحدة.
https://bitwarden.com

ملاحظات خاصة بالسياق الجزائري:

- قد يتم حجب أو تعطيل بعض التطبيقات مؤقتًا)مثل Signal أو (Tor في فترات حساسة أو أثناء الحملات الأمنية.
- استخدم دائمًا VPN موثوقًا مثل VPN Proton أو VPN RiseUp لتجاوز الحجب وتأمين الاتصال.
- لا تضع كل أدواتك في هاتف واحد – حاول الفصل بين أدوات العمل والاتصال الشخصي.
- تجنب استخدام التطبيقات المقرصنة أو المعدلة)مثل نسخ WhatsApp المعدلة(، فهي غالبًا بوابات تجسس.

نصيحة ختامية:

استخدام الأدوات لا يكفي، الأهم هو الوعي بكيفية استخدامها بذكاء.
اختر الأدوات التي تناسب طبيعة عملك، ولا تتردد في استشارة أشخاص موثوقين عند التردد.
الخاتمة والتوصيات المستقبلية

في ظل تصاعد التهديدات الرقمية التي تستهدف المدافعين والمدافعات عن حقوق الإنسان، خصوصًا في السياقات الحساسة مثل الجزائر، يصبح الوعي بالأمن السيبراني ليس ترفًا تقنيًا، بل ضرورة نضالية لحماية الذات، والمحيط، والعمل الحقوقي.

هذا الدليل لا يدّعي تقديم حل نهائي أو شامل، بل يهدف إلى تمكين المستخدم/ـة غير التقني/ـة من فهم التهديدات الرقمية، واتخاذ خطوات واقعية وسهلة لتحسين سلامته الرقمية الشخصية والمهنية.

نحن نؤمن أن الأمن الرقمي هو عملية مستمرة، تتطور بتطور الأدوات والتهديدات. وبالتالي:

- راجع خطتك الرقمية بشكل دوري.
- تابع مصادر موثوقة للحصول على تحديثات.
- شارك هذا الدليل مع من يحتاج إليه.
- كن مستعدًا دائمًا، لا خائفًا.

تنويه وإخلاء مسؤولية

هذا الدليل مُعدّ لأغراض التوعية والتثقيف فقط، ولا يُعد مرجعًا قانونيًا أو تقنيًا رسميًا.
جميع التوصيات الواردة فيه تم اختيارها بناءً على المعرفة والخبرة المتوفرة وقت إعداد الدليل، وقد تتغير فعاليتها أو صلاحيتها مع مرور الوقت بسبب التطورات التقنية المستمرة.

الكاتب والمؤسسة غير مسؤولَين قانونيًا عن أي استخدام مباشر أو غير مباشر للتطبيقات أو الأساليب أو الأدوات المذكورة في الدليل.

- على كل مستخدم/ـة أن يتحمل/تتحمل مسؤولية تقييم المخاطر الشخصية واتخاذ القرار المناسب حسب السياق.
- استخدام الأدوات والتوصيات الواردة في هذا الدليل يتم على مسؤولية الفرد الخاصة.
- نوصي دائمًا باستشارة مختصين في حال وجود تهديد حقيقي أو اختراق فعلي.

هدفنا الوحيد هو دعم الوعي، وتمكين المدافعين عن حقوق الإنسان من حماية أنفسهم في بيئة رقمية سريعة التغيّر.