تقاطع
جمعية

دليل الأمان الرقمي للناشطات والناشطين

دليل الأمان الرقمي
للناشطات والناشطين

جمعية تقاطع من أجل الحقوق والحريات
www.intersction.uno
info@intersection.uno

تم إصدار هذا الدليل بدعم من

Activity supported by the
Canada Fund for Local Initiatives
Activité réalisée avec l'appui du
Fonds canadien d'initiatives locales

Canada

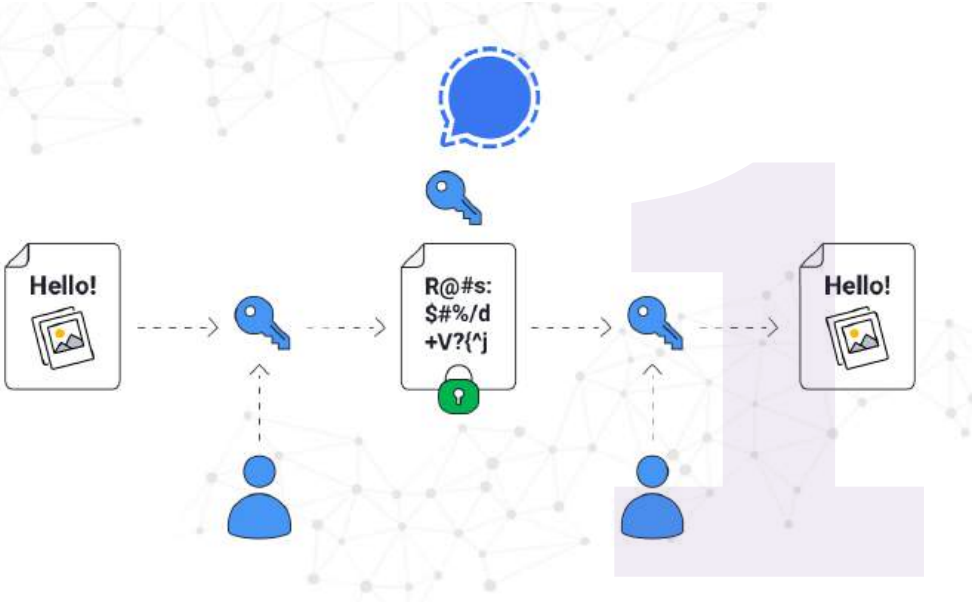
تقديم:

الدليل هذا موجه لأعضاء وعضوات المجتمع المدني والنشطاء والناشطات اللي يواجهوا مخاطر كبيرة في مجال الأمن الرقمي. الهدف متاعو هو تقديم توصيات باش يحميوا معلوماتهم الحساسة من الوصول أو الاعتراض غير المصرح بيه من قبل جهات غير موثوقة. التوصيات هاذي مصممة خصيصاً باش تلبي احتياجات المستخدمين اللي فيهم تهديدات عالية، واللي يتطلبوا مستوى عالٍ من الخصوصية والأمان في اتصالاتهم الرقميةً. الدليل يوفر إرشادات للأشخاص اللي يحتاجوا يتبعوا تدابير أمنية أكثر تقدماً، خاصةً كي التدابير الأساسية ما تكفيش.

منهجية:

«الدليل هذا يستند على أفضل الممارسات الأمنية المعترف بيها والمتوفرة للعموم، كيما إطار التدقيق الأمني للمجموعات المدافعة (SAFETAG) وتقارير وأدلة أخرى كيما «Security in a Box» ومصادر أخرى منظمات دولية. الدليل موش مخصص باش يعطي توصيات خاصة بكل بلد، أما ينجم يكون نقطة انطلاق باش تحمي معلوماتك الرقمية.»

الممارسات الأفضل:



1. استعمال تطبيقات مراسلة مشفرة

«استعمل تطبيقات مراسلة مشفرة وموثوق فيها كيما Signal. التشفير هذا يضمن اللي المرسل والمستقبل برك ينجموا يقراوا المحتوى، وحتى مطوري التطبيق ما عندهمش النفاذ. إذا كنت تستعمل التطبيق هذا، فعّل ميزة الرسائل المختفية اللي تمكّنك باش تحدد وقت تختفي فيه الرسائل القديمة والجديدة بصفة آلية.

2. تجنب استعمال شبكات الاتصال العادية للمعلومات الحساسة

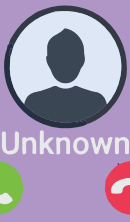
«ممنوع بش تستعمل شبكة الاتصالات الخلوية (الشبكات العادية) وقتلي تتحدث على معلومات حساسة، خاتر الاتصالات هاذي يمكن اعتراضها بسهولة. استعمل وسائل أخرى أكثر أمان.»

3. فحص بطاقات SIM

«إذا تشك اللي فما حد يتنصت على المكالمات متاعك، دور على العلامات هاذي:

وجود ضجيج
أو أصوات غير طبيعية
وقت المكالمات

المكالمات تنقطع
بشكل متكرر



استقبال مكالمات
ورسائل من أرقام غريبة

تغييرات مفاجئة في قوة
الإشارة حتى في مناطق
وين الإشارة قوية

استنزاف سريع للبطارية
متاع الهاتف، حتى كي
تستعمله بشكل عادي

نشاط غير عادي
في الفاتورة متاعك

4. حماية بطاقة SIM بكلمة سر

«دائماً استعمل رمز PIN لبطاقة SIM الخاصة بيك وتجنب الرموز السهلة كيما 0000 أو 1234. كيما يفضل تغيير الشريحة إذا كنت تشك فيها وتخلي القديمة نشطة لتجنب الشكوك.»

5. التثبت من التطبيقات

«العديد من التطبيقات كيما Truecaller توفر معلومات على المكالمات الواردة. تأكد اللي التطبيق هذا ما يعرفش معلوماتك الشخصية. تنجم تزور الموقع الخاص بيهم لإزالة اسمك ورقمك من القائمة: رابط الإلغاء.

6. استخدام خدمات بريد إلكتروني مشفرة

«إذا عندك معلومات حساسة وتحب تضمن خصوصيتها، استعمل خدمات بريد إلكتروني مشفرة وموثوقة كيما

Tutanota®

الرابـــــط

أو

Proton Mail

الرابـــــط

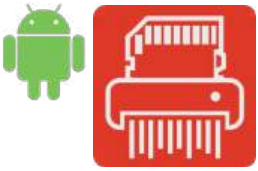
الخدمات هاذي تستخدم التشفير من طرف إلى طرف وما تعتمدش على برامج إضافية كيما PGP أو Mailvelope اللي تتطلب مكونات إضافية.»

7. إجراء نسخ احتياطي للبيانات الحساسة

«البيانات الحساسة اللي عندك على الأجهزة المحمولة أو الحواسيب ينصح ديماً بتخزين نسخة مشفرة منها في خدمات سحابية موثوقة، وما تخليش النسخة الأصلية على الجهاز إذا ما عندكش سبب قوي. وقت تحب تحذف بياناتك، لازم تستعمل أدوات تضمن الحذف الآمن، موش مجرد حذف عادي.»

أمثلة على أدوات الحذف الآمن:

BleachBit



Shreddit

أدوات النظام الخاصة

أدوات النظام الخاصة

8. تجنب حمل معلومات حساسة أثناء التنقل

«كيما ينصح بشدة إنك ما تحملش معاك معلومات حساسة على الأجهزة المحمولة كي تكون في حالة تنقل. إذا لازمك جهاز، استعمل جهاز مؤقت، كيما هاتف مسبق الدفع أو كمبيوتر ما يحتويش على بيانات مهمة.»

9. تخزين البيانات الحساسة في حاويات مشفرة

«البيانات الحساسة يلزمك تخزنها في حاويات مشفرة باستخدام أدوات كيما:

FileVault

BitLocker

Tella

EDS

10. استخدام كلمات سر قوية وفريدة

«كل حساب عندك يلزم يكون عنده كلمة سر فريدة وقوية، ما تستعملش كلمات سر سهلة كيما «123456» أو اللي تتضمن معلومات شخصية. تنجم تستعمل أدوات إدارة كلمات السر كيما

KeepassXC

Bitwarden

باش تنشئ وتخزن كلمات السر بأمان.»

11. حماية الأجهزة

«تأكد اللي جميع أجهزتك (هواتف، حواسيب، أجهزة لوحية) محمية بكلمات سر قوية. ما تعتمدش على قفل الشاشة بالبصمة أو التعرف على الوجه كوسيلة حماية وحيدة.»

12. إخفاء التطبيقات الحساسة

«إذا لقيت نفسك في موقف وين يلزمك تستعمل هاتفك للعمل، ينصح بإخفاء التطبيقات الحساسة. كل من نظامي iOS وAndroid يوفروا ميزات لإخفاء التطبيقات. إطلع على الإرشادات من هنا:

iOS

Android

13. استخدام شبكات خاصة افتراضية (VPN)

«الشبكات الخاصة الافتراضية (VPN) تحمي حركة مرور البيانات الخاصة بيك من الاعتراض. استعمل خدمات VPN ذات سمعة حسنة، كيما

Mullvad

TunnelBear

14. تعطيل تتبع الموقع

«أوقف تشغيل تتبع GPS على هاتفك لمنع أي جهة من متابعة تحركاتك. هكا تعزز خصوصيتك.»

15. تفعيل المصادقة الثنائية (2FA)

«المصادقة الثنائية تضيف طبقة أمان إضافية لحساباتك. ديماً فعّلها وقتلي تكون متوفرة. تقدر تتبع الإرشادات على موقع 2fa.directory لتفعيلها على منصات متعددة.»

16. اختيار مكان آمن

«إذا كنت تعتقد اللي فما حد يتبعك، اختار أماكن آمنة وين يكون الحضور محدود وتجنب المناطق المعزولة أو اللي فيها عدد كبير من الناس.»

17. التصرف بهدوء مع الجهات الرسمية

«في حالة تم توقيفك من قبل الشرطة، التزم بالهدوء وما تدخلش في مواجهات أو جدالات. اسألهم بوضوح على سبب توقيفك وإذا تم احتجازك، اطلب حقك في الاتصال بمحاميك.»

18. إلغاء الوصول للأجهزة في حالات الطوارئ

«إذا كنت تخاف من أن جهازك يتعرض للاختراق أو المصادرة، فكّر في إعطاء بيانات اعتماد مؤقتة لشريك موثوق. هكا تقلل من خطورة أي اختراق للمعلومات الحساسة.»

الفصل الرابع: نصائح حول التنفيذ

«التوصيات اللي يقدمها الدليل هذا تنجم تكون معقدة شوية للمستخدمين العاديين، أما العديد من الأدوات المتوفرة على الإنترنت تسهّل عملية التطبيق. ننصحك باش تعمل بحث على الأدوات اللي ذكرناها وتتعلم كيفية تفعيل المزايا الأمنية فيها.

إذا كانت الروابط أو الأدوات المذكورة في الدليل موش صالحة أو توقفت عن العمل، حاول البحث على بدائل بنفس الأسماء أو الميزات. أما ديماً تأكد من مصداقية المصدر اللي تستعمله.»

ملاحظات مهمة:

- «قبل ما تتبع أي توصيات، تأكد إن قوانين بلدك ما تمنعش استعمال التشفير أو الشبكات الافتراضية، خاتر بعض البلدان عندها قيود قانونية على الاستخدام هذا.»

- « القانون بيحملك المسؤولية كمستخدم في الالتزام بالقوانين المحلية وتطبيق الإجراءات اللي تتماشى مع الوضع الخاص بيك.»

نصيحـــــــة للمـدافعين والمدافعـات عن حقـوق الإنســـــان:

«النشـطاء والناشـطات والمدافعـين والمدافعـات علـى حقـوق الإنسـان يلزمهـم ديمـاً يكونـوا علـى درايـة بالقوانـين المتعلقـة بالنشـاط الرقمـي فـي بلادهـم. التوعيـة الذاتيـة والإعـداد الجيد تقلـل مـن أي مشـاكل قانونيـة محتملـة وتخليهـم مسـتعدين لمواجهـة أي مواقـف صعبـة.»

الموارد الإضافية:

«إلى جانب التوصيات اللي ذكرناها، فما برشا موارد أخرى اللي تعاونك باش تحسن الأمن الرقمي وتحمي الخصوصية متاعك. من بين الموارد هاذي:

Digital First Aid Kit:
مجموعة أدوات تقدم إرشادات حول الإسعافات الأولية الرقمية.

SecFirst:
منصة تقدم موارد للصحفيين والسلامة في حالات الطوارئ.

Frontline Defenders:
دليل السلامة الرقمية للمدافعين على الخط الأمامي.»

أهمية استكشاف الموارد:

«الموارد هاذي تقدم معلومات قيمة وأدوات تساعدك باش تبقى ديماً على اطلاع بأحدث الممارسات الأمنية. كيما تنجم تتيحلك حلول تتماشى مع احتياجاتك والتهديدات اللي تواجهها. تأكد ديماً إنك تستعمل الأدوات اللي تتناسب مع وضعك الأمني.»

الخـــــاتمة:

«الدليل هذا يقدم إرشادات عملية لحماية بياناتك الرقمية وتقليل المخاطر اللي تنجم تواجهها. لكن من المهم إنك تكون واعٍ إن كل إجراء تاخذه يزيد من أمانك، أما ما يضمنش الحماية المطلقة. ديماً خذ بعين الاعتبار إن الأمن الرقمي مسؤوليتك الخاصة، وحاول تبقى على اطلاع بالتقنيات والممارسات الجديدة. حافظ على يقظتك واستثمر في سلامتك الرقمية.»

تقاطع
جمعية

إصدارات جمعية تقاطع

SCAN ME
عربي

SCAN ME
ENGLISH

SCAN ME
FRANCAIS