حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

دليل الخصوصية والأمان الرقمي
في حالات الطوارئ

تشرين الأول/ أكتوبر
2023

تشهد المساحات الرقمية ومنصات التواصل ازديادًا ملحوظًا في المنشورات المحرضة في حالات الطوارئ وأثناء الحروب والأزمات، والتي تستهدف الناشطين/ات والسردية وجهود المناصرة. وقد يتفاقم الشعور بالرقابة وعدم الأمان أمام الملاحقات الرقمية ونشر البيانات الشخصية وحملات تشويه السمعة. إليكم بعض النصائح والأدوات في الأمان الرقمي لحماية خصوصيتكم وأجهزتكم خلال النشر وقت الأزمات والحروب:

حماية الأجهزة من المراقبة

- شراء الأجهزة من مصادر موثوقة فقط.
- لا تدعوا أجهزتكم تغيب عن نظركم، خصوصًا عند عبور الحدود/نقاط التفتيش.
- قوموا بتحديث البرامج. حافظوا على تحديث نظام التشغيل الخاص بك وجميع التطبيقات المثبتة على الفور.
- إزالة الأجهزة المشبوهة. تحققوا مما إذا كانت برامج المراسلة الفورية والحسابات عبر الإنترنت متصلة بأجهزة غير معروفة.
- استخدموا برامج مكافحة الفيروسات والبرامج الضارة.
- لا تستخدموا برامج من مصادر غير موثوق بها/غير أصلية.
- تغيير كلمات المرور بشكل دوري.
- استخدموا VPN أو Tor.

حماية الأجهزة والحسابات من البرامج الضارة وهجمات التصيد

التصيد الاحتيالي (fishing) هو من أكثر أنواع القرصنة شيوعًا. لحماية أجهزتكم من هجمات التصيد أو البرامج الضارة (malware):

- تأكدوا من تحديث أنظمة التشغيل (System Update).
- تأكدوا من تحديث جميع التطبيقات.
- استخدام برامج مكافحة الفيروسات مهم جدًا، حتى على أجهزة Mac.
- إلغاء تثبيت أي تطبيقات غير ضرورية أو مستخدمة.
- تأكدوا من أي روابط أو ملفات قبل فتحها.

نصائح للتوثيق أو للاحتجاجات والتظاهرات

- احتفظوا بهواتفكم المحمولة دائمًا معكم. أو سلموها لصديق موثوق في حال الانخراط بفعل قد يؤدي للاعتقال.
- استخدموا الكاميرا للتوثيق دون أن تقوموا بفتح قفل الشاشة.
- خذ وا بعين الاعتبار إذا التقطتم صورًا أو فيديو، قد تسعى الشرطة لمصادرة الهاتف للحصول على المواد كأدلة.
- حافظوا على خصوصية الناشطين/ المتظاهرين.
- إذا كنتم بحاجة للحفاظ على حقيقة مشاركتكم في مظاهرة ما سرًا، لا تأخذوا الهاتف المحمول معكم. إن كان لا بد من إحضار هاتف، حاولوا أن تجلبوا هاتفًا غير مسجل باسمكم.

عند النشر على منصات التواصل

- تأكدوا من **إعدادات الخصوصية** ومن المشاركة المحدودة والضرورية فقط للبيانات الشخصية.
- **تفادوا مشاركة موقعكم** في المنشورات وحافظوا على خصوصية الآخرين عند نشر الصور أو البيانات.
- تأكدوا من **حذف جميع البيانات الوصفية MetaData**
(التي تساعد في تنظيم البيانات والعثور عليها وفهمها) من صوركم قبل نشرها أو مشاركتها إذا كنتم تريدون الحفاظ على سرية هوياتكم ومواقعكم. بإمكانكم أخذ صورة شاشة (Screenshot) للصورة ومشاركته بدلًا من مشاركة الصورة الأصلية.

تأمين حسابات التواصل

- تفادوا مشاركة رقم هاتفكم أو عناوينكم.
- بإمكانكم إخفاء أماكن عملكم.
- إغلاق ميزة الوصول إلى الموقع وإلى الميكروفون وأرقام الهاتف المخزنة على أجهزتكم.
- بإمكانكم إغلاق إتاحة الوصول إلى صوركم.
- استبدلوا كلمات المرور القديمة بأخرى قوية ومعقدة.
- فعّلوا المصادقة الثنائية (2FA / Two factor authentication) على جميع حساباتكم واربطوها بتطبيق على جهازكم وليس برسالة نصية (يمكن اعتراض الرسائل النصية بسهولة وبدل أن تصل إليكم ستصل لخصومكم).
- دليل استخدام تطبيق المصادقة الثنائية Authy

حماية كلمات المرور (Password)

- بالإمكان تخمين كلمات المرور ، أو البحث عنها (بقرب الجهاز) أو الوصول إليها بالخداع (برامج ضارة، التصيد الاحتيالي) أو استغلال نقاط الضعف (تطبيقات غير محدثة).
- اختاروا | *كلمات مرور قوية ومعقدة | *من 16 حرف ورقم ورمز على الأقل *مختلفة لكل حساب.
- بإمكانكم استخدام برنامج لإدارة كلمات المرور، هكذا سيتيح لكم تخزين كلمات مرور قوية لجميع حساباتكم. عليكم تذكر كلمة مرور واحدة لهذا البرنامج فقط. ننصح بـ KeePassXC على ويندوز (Windows)، ماك (Mac) أو لينوكس (Linux). وبـ StrongBox لأجهزة آي أو إس (iOS) وبـ KeePassDX لأجهزة أندرويد (Android).

للتواصل الآمن استخدموا

- WhatsApp واتساب للمكالمات الصوتية المشفرة.
- Signal سيجنال للمكالمات الصوتية والرسائل النصية المشفرة والآمنة.
- Jitsi للمكالمات الصوتية أو مكالمات الفيديو المشفرة.
- **تأكدوا من ملاءمة إعدادات الخصوصية لاحتياجاتكم في كافة التطبيقات.**
- **تجنبوا استخدام المكالمات الصوتية والرسائل النصية عبر شركات الاتصالات، بدلًا من ذلك استخدموا سيجنال أو واتساب.**

للاتصال الآمن والمشفر

- استخدموا أحدث نسخة من فايرفوكس كمتصفح (Browser) أساسي.
- **أوقفوا تشغيل** مدير كلمات المرور المدمج في المتصفح.
- استخدموا الـ **VPN** (الشبكة الافتراضية الخاصة) لتشفير اتصالكم بصفحات الإنترنت والبريد الإلكتروني وتطبيقات التراسل المباشر وأي خدمة إنترنت أخرى. الـ VPN بمثابة نفق افتراضي لمزودي انترنت خارج البلاد. ملاحظة: يمكن لمزودي خدمة VPN مراقبة جميع الاتصالات. ننصح باستخدام ProtonVPN أو TunnelBear.
- **تور Tor** برنامج مفتوح المصدر تم تصميمه ليؤمّن إخفاء هوية المستخدم على الإنترنت. يوجه تور حركة مرور تصفحك للإنترنت بطريقة تسمح لك أيضًا بتجاوز الرقابة. (لاستخدام تور على لينوكس وماك OS وويندوز).

لحماية الخصوصية والبيانات

تشفير الأجهزة

لحماية بخصوصيتك في حال مصادرة أجهزتك أو سرقتها ونسخ بياناتك، قم بتشفير اجهزتك فعندها سيحتاج خصمك إلى كلمات المرور للوصول إلى بياناتك. بعض الأجهزة توفر خيار التشفير الكامل للقرص.

- آبل توفر ميزة تشفير كامل للقرص فور حماية الجهاز بكلمة مرور.

أندرويد توفر الخيار التشفير الكامل للقرص خلال الإعداد الأولي للجهاز أو عبر إعدادات "الأمان".

حفظ وتشفير البيانات

- الاحتفاظ بنسخ احتياطية من بياناتكم المهمة.
- استخدموا التخزين السحابي (Cloud) أو قرص صلب (Hard Disk) خارجي تحتفظون به في مكان آمن.
- شفروا البيانات الحساسة قبل تخزينها".

في حال الاستدعاء للتحقيق

بإمكانكم حذف الجهاز عن بعد

في حال فقدان أو مصادرة او سرقة الجهاز بإمكانكم حذفه عن بعد:

- آيفون IOS
- أندرويد Android

أو الحذف التلقائي للبيانات بعد عدد معين من محاولة ادخال رقم سري خاطيء

- أنظمة آيفون IOS : الإعدادات > بصمة الوجه ورمز المرور > اسحبوا إلى الأسفل> واختاروا "مسح البيانات".
- أنظمة أندرويد Android : بشكل عام أكثر تعقيدًا وتختلف بحسب المصنع والطراز. في الأجهزة التي تعمل بأنظمة أندرويد 10 أو الأحدث: افتحوا الإعدادات
- وابحثوا عن "سياسة المسح" wipe policy.

لاطلاعكم: كيف ننشر على منصات التواصل خلال الأزمات والحروب؟

إذا تعرضت حساباتكم ومنشوراتكم **للحذف والتقييد**، أو واجهتم **تهديدات ورسائل تحريضية** عبر منصات التواصل الاجتماعي، أو **محاولات للتصيد أو الاختراق**، بلّغوا الآن لمنصة حر:

- 7or.7amleh.org
- https://chat.whatsapp.com/F0uVNOZUvnmGVEC7wovjwF
- أو تواصلوا معنا على report@7amleh.org

حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media