7 نصائح حول السلامة الرقمية للأشخاص الذين يقومون بتوثيق انتهاكات حقوق الإنسان

ملاحظة

- اقرأ الشروط والأحكام الخاصة بجميع المنصات والتطبيقات قبل استخدامها.
- اعرف من يملك الشركة ومقرها يمنع تعرضك وتعرض بياناتك للهجمات الحكومية.
- تحقق من تقارير الشفافية الخاصة بالشركة واطلع على أي تغييرات في الخدمة.

1

حماية معلوماتك الشخصية

- ابحث عن نفسك مباشرة عبر المواقع ومن خلال مواقع ارشيف الانترنت مثل Wayback machine.
- (الاسم والهاتف والعنوان ويوم الميلاد وحتى البحث العكسي للصور).
- نصيحة: استخدم خاصية التصفح الخفي او ما يعرف بال incognito.
- ابحث عن البيانات المتوفرة عن أفراد الأسرة.
- راجع إعدادات الخصوصية على حساباتك الخاصة على مواقع التواصل الاجتماعي وحاول إزالة المعلومات الشخصية أيضاً وطمس صور عنوانك الخاص على "غوغل مابس".
- تتبع أي نشاط يتعلق بمعلوماتك الشخصية كإسمك وعنوانك وما إلى ذلك باستخدام تنبيهات غوغل.

2

حماية حساباتك الخاصة

- استخدم password manager لإدارة جميع كلمات المرور والارقام الخاصة بك.
- استخدم أدوات المصادقة الثنائية 2FA مثل authy ولا تستخدم الرسائل النصية... إذا كنت معرضًا لخطر كبير، فاستخدم مفتاح أمان مثل YubiKey.
- إذا حصلت على كودات للمصادقة الثنائية، قم بطبعها واحفظها في نسخة احتياطية أو في الـ password manager الخاص بك، ومن ثم احذفها من حسابك.
- أفصل معلوماتك وبياناتك الشخصية عن تلك المهنية.
- راقب نشاط حسابك، وقم بتسجيل الخروج من الأجهزة المشتركة، وتوخي الحذر عند استخدام أجهزة الكمبيوتر في المساحات العامة.
- تحقق دائماً من حساباتك في قواعد الحوادث الأمنية من خلال البحث عن حسابك على هل تعرضت للاختراق؟

3

الحماية من هجمات التصيد الاحتيالي

- كن حذراً من الرسائل العاجلة.
- تحقق من تفاصيل المرسل.
- فكر مرتين قبل النقر على الروابط.
- اطلع على مرفقات البريد الإلكتروني قبل تنزيلها.

نصيحة: فكر في تحميل الروابط والمستندات المشبوهة على برنامج فحص Virus Total.

4

أمان الجهاز

- قم بإقفال أجهزتك الالكترونية من خلال كلمات مرور خاصة أو رموز معينة.
- قم بتحديث نظام التشغيل والتطبيقات والمتصفحات لديك عندما يُطلب منك ذلك.
- لا تستخدم الـUSB التي يتم توزيعها مجانًا في المؤتمرات والمناسبات.
- قم بإعداد أجهزتك للسماح بمسح أي بيانات عن بعد (غير متاح إذا كان غير متصل بالإنترنت).
- قم بتشفير الهواتف الذكية الخاصة بك (تأكد من تشغيل الخاصية من خلال الإعدادات الخاصة على هاتفك).
- قم بتشفير الحاسوب الخاص بك من خلال برنامج Bitlocker لنظام التشغيل Windows، أو Firevault لنظام التشغيل Mac، أو برنامج Veracrypt لوحدات التخزين الخارجية.

ملاحظة

قد يقوم جهازك بخلق نسخة احتياطية لبياناتك على حسابك المرتبط بـ cloud بالهاتف وقد لا يتم تشفير المعلومات المخزنة هناك.

نصيحة: قم بإيقاف النسخ الاحتياطي التلقائي

5

تشفير الاتصالات

- استخدم تطبيق signal عند تواصلك مع الآخرين.
- استعمل خاصية "اخفاء الرسائل" وقم بمراجعة المحتوى الحساس وحذفه بانتظام من هاتفك وتطبيقاتك.
- قم باقفال التطبيق باستخدام رقم التعريف الشخصي أو رمز المرور.
- تشفير بريدك الإلكتروني باستخدام برامج معروفة وكلمات مرور قوية، مع أخذ بعين الاعتبار أن المتلقي يجب أن يحمل البرنامج عينه.
- قم بعمل نسخة احتياطية لأجهزتك وقم بتخزين النسخ الاحتياطية بشكل آمن.

6

حماية وتأمين الانترنت الخاص بك

- حماية سجل التصفح الخاص بك باستخدام شبكة افتراضية خاصة (VPN) - استخدم Mullvad أو Tor).
- استخدام DuckDuckGo Smarter Encryption للتأكد من تشفير الموقع الذي تزوره.
- ثبت مانع الاعلانات.
- قم بتثبيت Privacy Badger لمنع مواقع الويب والمعلنين من تتبع المواقع التي تزورها عبر الإنترنت.
- تجنب استعمال الحواسيب العامة الموجودة في المقاهي و غيرها من الأماكن.

7

إذا كنت تعبر الحدود

- قم بإزالة جميع المواد الحساسة والمعلومات الخاصة من حسابك قبل ذهابك لأي مكان وسجل خروجك من كل حسابتك.
- قم بإجراء نسخ احتياطية للبيانات واستخدم أجهزة منفصلة ونظيفة للسفر خاصة للأعمال الحساسة للغاية.
- امسح سجل التصفح الخاص بك.
- قم بإيقاف تشغيل أجهزتك لتنشيط تشفير القرص.
- كن حذرًا من الرسائل النصية القصيرة والمكالمات الهاتفية التي قد لا تكون مشفرة من طرف إلى طرف وتعامل مع الأجهزة المصادرة على أنها معرضة للخطر.

لمزيد من النصائح زوروا: cpj.org