

دليل

انهضوا.. دافعوا



DEFENDDEFENDERS

East and Horn of Africa Human Rights Defenders Project

المحتويات

٣	الاختصارات
٤	شكر
٥	مقدمة
٦	الفصل الأول: تعريف المفاهيم
٨	الفصل الثاني: تحليل سياقي
١١	الفصل الثالث: حوادث الأمن والسلامة
١٣	الفصل الرابع: فهم التهديدات
١٧	الفصل الخامس: تقييم المخاطر
٢٠	الفصل السادس: تخطيط الأمن والسلامة
٢٣	الفصل السابع: الآليات الحالية لحماية المدافعين عن حقوق الإنسان
٢٧	الفصل الثامن: الرعاية الذاتية والقدرة على التعافي

الاختصارات

AU	الاتحاد الأفريقي
ACHPR	اللجنة الإفريقية لحقوق الإنسان والشعوب
CBO	منظمة مجتمعية
EU	الاتحاد الأوروبي
HRD	مدافع عن حقوق الإنسان
WHRD	مدافعة عن حقوق الإنسان
NHRI	مؤسسة وطنية لحقوق الإنسان
NGO	منظمة غير حكومية

شكر

أطلق مشروع ديفيند ديفنדרز DefendDefenders في 5 مايو 2017، دليل انهضوا.. دافعوا! STAND UP! للمدافعين عن حقوق الإنسان الأفارقة، والذي يهدف إلى تعزيز الأمن المادي والرقمي للمدافعين عن حقوق الإنسان والمنظمات، من خلال وضع سياق المعرفة الموجودة في دليل الحماية الجديد للمدافعين عن حقوق الإنسان الصادر عن منظمة الحماية الدولية وكراثة فروننت لآين ديفنדרز Front Line Defenders الخاصة بالأمن.

أطلقت ديفند ديفنדרز دليل انهضوا.. دافعوا في ديسمبر 2019، وصدر بخمس لغات أوغندية محلية: أشولي، وأتيسو، ولوغاندا، ولو، ورونيكايتارا. قررت ديفند ديفنדרز في عام 2020 مراجعة الدليل ليستوعب ملاحظات المدافعين عن حقوق الإنسان، والمفاهيم الجديدة في مجال الأمن والسلامة والرفاه الخاص بالمدافعين الأفارقة. الإصدار الحالي هو نتيجة لتجربة ديفند ديفنדרز، وملاحظات المدافعين، خلال التدريبات، والبعثات البحثية، والمشاركات المختلفة مع أصحاب المصلحة، والجوانب الجديدة في مجال الأمن والسلامة.

قام فريق إدارة الحماية والأمن المكون من جانفيير هاكيزيماننا، وماجد معالي، وكاريس موسى أوتيبا، وأن ناكينجي، و(الراحلة) مريم ناكيبوكا، وبريان باموتازي، وليون نسيكو، ودينيس كوييزيرا بمراجعة الكتاب الأول حول الأمن والسلامة الجسدية. تمت مراجعة الكتاب الثاني حول الأمن والسلامة الرقمية من قبل الفريق التكنولوجي المكون من دانييل بيكواسو، وصامويل إيبو، وجوشوا سينجونزي، ودوناتيان نيونجينداكو، وإيماكيوليت نابواير، وأبديكاني حسن.

لم تكن عملية المراجعة لتنجح بدون توجيه وإشراف فريق إدارة ديفيند ديفنדרز. قدم المدير التنفيذي لديفيند ديفنדרز- حسن شاير، ومدير البرامج والإدارة - ميموري بانديرا، ومديرة-أولى وحدة الحماية والأمن - تابيثا نيتوا، مساهمات مقدرة في التوجيه الاستراتيجي لتحرير ونشر هذه الطبعة.

مقدمة

يعد الإعلان المتعلق بالمدافعين عن حقوق الإنسان، والذي تم اعتماده في عام 1998، وتفويض المقرر الخاص المعني بحالة المدافعين عن حقوق الإنسان في الأمم المتحدة في عام 2000، من المعالم المهمة في حماية المدافعين على المستوى العالمي. لكن، لا يزال المدافعون يواجهون التهديدات والمخاطر رغم وجود هذه الآليات.

يواجه المدافعون الأفارقة، الذين يعملون على تعزيز وحماية حقوق الإنسان في سياقات سياسية متقلبة، مخاطر كبيرة، مثل القتل، والاعتداء الجسدي، والاعتقال، والترهيب وتقلص الحيز المدني. وتفشل الدول باستمرار في التحقيق في الانتهاكات التي تواجه المدافعين.

اتخذ المدافعون لضمان أمنهم واستمرارية عملهم، خطوات لإدارة الأمن الفردي والمؤسسي، من خلال تقييم المخاطر ووضع استراتيجيات فعالة للتخفيف من التهديدات المحتملة. إن تخصيص الوقت والموارد لإدارة الأمن يساعد المدافعين على مواصلة أنشطتهم في مجال حقوق الإنسان وضمان أمنهم وسلامتهم.

يهدف دليل ديفيند ديفنדרز المتعلق بالأمن، والسلامة، والقدرة على التعافي، إلى أن يكون بمثابة أداة للمدافعين عن حقوق الإنسان في أفريقيا، تزودهم بالاستراتيجيات والاستجابة اللازمة للبيئة المتقلبة التي يعملون ضمنها. وعلى الرغم من آليات الحماية المتاحة، لا يزال المدافعون يواجهون المخاطر والتهديدات التي لها تأثير لا يمكن إنكاره على صحتهم العقلية على المدى الطويل. لذا يحتاج المدافعون إلى اتخاذ خطوات لإدارة أمنهم وسلامتهم.

يعكس هذا الدليل تجارب ديفيند ديفنדרز على مدار 17 عامًا الماضية، والتي تركز على ضمان سلامة المدافعين، وأمنهم، وحمايتهم ورعايتهم الذاتية، من خلال التدريبات، والمناصرة، والبحث والدعم الفني والمؤسسي. وتعتمد الطبعة الثانية على توصيات، وملاحظات، وتفاعلات المدافعين، وشركاء الحماية، والآليات الوطنية والإقليمية والدولية لحماية المدافعين.

يضاف هذا الدليل إلى المواد الموجودة مسبقًا، والمتعلقة بالأمن والسلامة والرعاية الذاتية للمدافعين. وهو دليل سيأتي في وضع المعرفة والأدوات للمدافعين في أفريقيا.

يحدد هذا الفصل المفاهيم الأساسية المستخدمة في الدليل. حيث أن فهمها، وإدراك أوجه التشابه، والاختلاف والتكامل بينها يفيد المدافعين عند إجراء تقييمات المخاطر، ووضع استراتيجيات وتدابير فعالة للسلامة والأمن.

الْقَصْدُ الأَوَّلُ

تعريف المفاهيم

◀ مدافع عن حقوق الإنسان

المدافعون عن حقوق الإنسان (HRDs) هم أشخاص يعملون بمفردهم أو مع آخرين، بطريقة سلمية، لتعزيز أو حماية حقوق الإنسان المنصوص عليها في الإعلان العالمي لحقوق الإنسان (1948)⁽¹⁾. ينطبق إعلان الأمم المتحدة بشأن المدافعين عن حقوق الإنسان لعام 1998 على الأفراد، والمجموعات والجمعيات التي تساهم في القضاء جميع انتهاكات حقوق الإنسان والحريات الأساسية للأشخاص والأفراد بصورة فعالة.

يمكن لأي شخص أن يصبح مدافعاً عن حقوق الإنسان بغض النظر عن خلفيته التعليمية، ومؤهلاته المهنية، ونوعه الاجتماعي، وعمره، وعرقه، وفتته الاجتماعية وجنسيته. على سبيل المثال، إن استنكرت بائعة أطعمة سوء معاملة زميلاتها من قبل سلطات الضرائب المحلية، فيمكن اعتبارها مدافعة عن حقوق الإنسان. كما يمكن أن تتواجد المدافعات عن حقوق الإنسان في القطاعين العام والخاص.

◀ الأمن

يعرف الأمن على أنه حالة التحرر من أو عدم التعرض لأحداث مؤذية متعمدة

◀ السلامة

تعرف السلامة على أنها حالة التحرر من أو عدم التعرض لأحداث مؤذية غير متعمدة

يتضمن كل من الأمن والسلامة عنصر الخطر

◀ الحماية

تعرف الحماية على أنها التدابير التي يتخذها المدافعون عن حقوق الإنسان أو الجهات الفاعلة الأخرى لتعزيز الأمن والسلامة⁽²⁾. حوادث الأمن والسلامة هي الأحداث التي يمكن أن تعرض المدافعين و/أو منظماتهم للخطر

1 The Declaration's full name is the "Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms" though commonly referred to as "The Declaration on Human Rights Defenders" <http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Translation.aspx>

2 Front Line Defenders, 'Workbook on security: Practical Steps for Human Rights Defenders at Risk' 2011, <https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk>, Accessed 23 June 2016

التهديد

يمكن تعريف التهديد بأنه التصريح أو الإشارة إلى نية إلحاق الضرر أو المعاقبة أو الأذى

الخطر

يمكن تعريف الخطر على أنه احتمال وقوع حدث يؤدي إلى ضرر

الرفاه

الرفاه هي الاهتمام بصحتك الجسدية والعقلية والعاطفية

سياق عمل المدافعين، والمعروف أيضًا ببيئة العمل، هو الأساس لكل قرار يتعلق بالأمن والسلامة. حيث تختلف مخاطر الأمن والسلامة التي يواجهها المدافعون باختلاف السياق. فالمدافعون يعملون في بيئة ديناميكية تؤثر على سلامتهم وأمنهم. يتكون مجال عمل المدافعين من العوامل والجهات الفاعلة. تشمل العوامل: السياسة، والاقتصاد، والثقافة، والنوع الاجتماعي، والدين، والبيئة وجوانب أخرى مثل الصحة. في حين تشمل الجهات الفاعلة المؤيدين والمعارضين لعمل المدافعين عن حقوق الإنسان. يهدف تحليل السياق إلى مساعدة المدافعين عن حقوق الإنسان على اتخاذ قرارات مستنيرة بشأن سلامتهم وأمنهم.

الفصل الثاني

تحليل سياق سياسي

منهج التحليل المختص بالعوامل

العوامل السياسية

للسياسة آثارها الإيجابية والسلبية على المدافعين وعملهم. المدافعون ليسوا بالضرورة سياسيين، لكن معرفة الأنسب السياسية في كل سياق أمر بالغ الأهمية من أجل اعتماد الأمن، والسلامة وآليات العمل الفعال في مجال حقوق الإنسان. ينبغي للمدافعين طرح أسئلة حول ماهية العوامل السياسية الرئيسية في مجال عملهم، وكيف تؤثر على أمنهم وسلامتهم. تصاحب الانتخابات في بعض البلدان تصاعد الهجمات ضد المدافعين. وفي مناطق النزاع المسلح، تتعرض المدافعات بشكل خاص للعنف الجنسي والاعتقالات. يجبر عدم الاستقرار السياسي المدافعين على التدقيق في آليات الأمن والسلامة بشكل منتظم. كما يحتاج المدافعون إلى المراقبة الفعالة لديناميكيات السياق السياسي وتأثيرها على أمنهم وسلامتهم.

العوامل الاقتصادية

تعتبر اللوائح، والضغوط، والتسهيلات والفرص الاقتصادية، أشياء أساسية لعمل المدافعين. يحتاج المدافعون إلى معرفة القوانين واللوائح والممارسات الاقتصادية القائمة التي تؤثر على عملهم. غالبًا ما تكون هناك حاجة إلى موارد اقتصادية لتنفيذ بعض تدابير الأمن والسلامة. يجب على المدافعين تحليل الاتجاهات الاقتصادية العالمية إلى جانب الجغرافيا السياسية بهدف وضع برامج استراتيجية وتخطيط آمني ملائمين.

العوامل الثقافية والاجتماعية

ينبغي على المدافعين تقدير المعايير الثقافية والاجتماعية لدى قيامهم بعملهم، مع الأخذ في الاعتبار أن بعض هذه المعايير تتعارض مع شمولية، ورسوخ حقوق الإنسان، وعدم قابلية هذه الحقوق للتجزئة. ومن المهم دراسة القضايا المتعلقة بالأعراف التقليدية، والدين والتصورات الاجتماعية للمجتمع الذي يعمل المدافعون ضمنه. خاصة فيما يتعلق بقضايا مثل حقوق المرأة والتوجه الجنسي، والهوية الجنسية (SOGI) والتعبير عنهما. وينبغي للمدافعين رصد العوامل الثقافية والاجتماعية وتأثيرها على أمنهم وسلامتهم.

العوامل التكنولوجية

تطور استخدام التكنولوجيا بسرعة في العقود الماضية. كما يستخدم المدافعون أوجه تكنولوجية مختلفة في عملهم، بما في ذلك الحماية، والتشبيك، والرصد، والتوثيق وإعداد التقارير (MDR). تنتبه العوامل التكنولوجية لاستخدام الأدوات الرقمية وأدوات الدعم في عملية تحقيق أهداف حقوق الإنسان. على الرغم من أن التكنولوجيا تعزز عمل المدافعين، إلا أنها أصبحت أحد المصادر الرئيسية للتهديدات والمخاطر، حيث تأتي معظم هذه التهديدات والمخاطر عبر المنصات الرقمية. لذا، يحتاج المدافعون إلى مراقبة مخاطر المنصات الرقمية.

— راجع الكتيب الثاني من هذا الدليل لمزيد من المعلومات حول الأمن والسلامة الرقمية —

العوامل البيئية والجغرافية

من شأن الطقس والطبيعة تنبيه المدافعين عن مخاطر الأمن والسلامة التي يمكن أن يتسبب بها العمل في مناطق محددة. كما أنها تنبههم أيضًا بالتاريخ والتوقيت المناسبين لإجراء أنشطة معينة. على سبيل المثال، تحدد البقعة والظروف الجوية وسائل النقل، والملابس ومعدات الحماية التي يجب استخدامها. اعتمادًا على التضاريس والبنية التحتية المتاحة، قد يُطلب من المدافعين استخدام المركبات والقوارب الصالحة لجميع المناطق للوصول إلى الأماكن البعيدة. يعد ركوب الدراجات و/أو المشي و/أو التجديف من بين الخيارات التي يمكن استخدامها للوصول إلى الأماكن التي يتعذر الوصول إليها.

الأطر القانونية

توفر القوانين والديساتير الوطنية، من حيث المبدأ، الحماية القانونية للمدافعين. لكن تم إساءة تطبيق بعض الأحكام القانونية لانتهاك حقوقهم. ويواجه المدافعون، بشكل متزايد، تقييد الحيز المدني بسبب اعتماد التشريعات القمعية. بعد الهجمات الإرهابية في 11 سبتمبر 2011، أصدرت معظم الدول الأفريقية قوانين مكافحة الإرهاب واستخدمتها للحد من عمل المدافعين.

علاوة على ذلك، فقد تم إساءة استخدام بعض التشريعات التي تحكم حرية التجمع وتكوين الجمعيات لتبرير انتهاك حقوق المدافعين. قد يتمكن المدافعون من وضع تدابير آمنة للعمل إن تعرفوا على التشريعات والقوانين الخاصة بمجالات معينة. ومن خلال الدعم، بإمكانهم أن يدعوا إلى إلغاء أو تعديل بعض القوانين. إن الاطلاعات على الانتهاكات السابقة لحقوق المدافعين مفيدة في التنبؤ بما قد يحدث لهم ولمنظماتهم.

عوامل أخرى

عوامل أخرى تعرض المخاوف والمخاطر المتعلقة بالصحة العامة حياة المدافعين للخطر. يحتاج المدافعون إلى النظر في التدابير الوقائية والتفاعلية لاتقاء احتمالات الحاجة إلى تدخل طبي. المدافعون الذين يعملون في مجال تلوث البيئة وانتهاكات حقوق الإنسان في المرافق الطبية معرضون للإصابة ببعض أنواع العدوى والأمراض. تزيد فرص تعرض المدافعين الذين يعملون في المناطق المعرضة للأمراض المعدية للإصابة بالأمراض. لذا يُنصح المدافعون بتلقي العلاج الوقائي، واستخدام معدات الحماية الشخصية (PPE)، والحصول على التأمين الصحي.

منهج التحليل المختص بالفاعلين (AAM)

الفاعل هو أي شخص أو مؤسسة لها اهتمامات تجاه عمل المدافعين عن حقوق الإنسان. يجب على المدافعين تحديد الجهات الداعمة، والجهات المعارضة، والجهات ذات النوايا غير المعروفة. إن سياق المدافعين ديناميكي لأن الجهات الفاعلة تغير مواقفها وفقاً لمصالحها والبيئات السائدة. ولذلك، ينبغي للمدافعين رصد التغيرات في سياق عملهم لإعادة تقييم موقف هذه الجهات.

أنواع الجهات

يمكن للمدافعين استخدام هذا الجدول لتصنيف الجهات وفقاً لاهتماماتهم ومواقعهم.

جهات الداعمة	جهات المعارضة	ذات نوايا غير معروفة
الجهات المانحة	منهكي حقوق الإنسان	السياسيون
المدافعين عن حقوق الإنسان	جهات إنفاذ القانون في بعض السياقات	الزعماء الدينيين في بعض السياقات
المنظمات غير الحكومية الدولية	الشركات متعددة الجنسيات في بعض السياقات	الأوساط الأكاديمية في بعض السياقات

- يرجى تجنب التعميم تجاه الجهات.
- حيثما أمكن، يحتاج المدافعون ذكر أسماء الأفراد داخل الوحدة أو المؤسسة. على سبيل المثال، في حين قد يفترض المدافعون عن حقوق الإنسان أن الأجهزة الأمنية تقف ضدهم، ربما بعض العملاء داخل تلك الأجهزة يدعمون قضيتهم.

الفصل الثالث

حوادث الأمن والسلامة

حادث الأمن والسلامة هو أي حدث يعرض المدافعين و/أو منظماتهم للخطر. ويقدم دروسًا للمدافعين ومنظماتهم حول تأثير عملهم، من خلال منحهم الفرص لإعادة تقييم آليات البرمجة والحماية الخاصة بهم.

أمثلة على حوادث الأمن	أمثلة على حوادث السلامة
١. مراقبو عمل المدافعين عن حقوق الإنسان	١. اندلاع حريق أو صعقة كهربائية
٢. تسريب معلومات المدافعين السرية	٢. غرق المكاتب
٣. تفتيش منازل ومكاتب المدافعين	٣. تفشي الأمراض

الخطوة ١ تسجيل الحادث

يستخدم المدافعون طرق مختلفة لالتقاط تفاصيل الحوادث، مثل النقاط والفقرات. وأيًا كانت الصيغة المفضلة، فإنها تسترشد بركائز الأسئلة الستة الموضحة في الجدول أدناه:

من؟	ماذا؟	أين؟
متى؟	لماذا؟	كيف؟

يسعى مسجلي الحوادث إلى طرح أكبر عدد ممكن من الأسئلة ذات الصلة. لذا يجب عليهم تجنب الكلمات المعقدة، والمصطلحات والعبارات الطنانة أثناء التسجيل. ويجب عليهم أيضًا التأكد من صحة الأسماء، والعناوين، والأشخاص والحقائق، للحصول على إرشادات مناسبة في الخطوات التالية لتقييم حوادث الأمن والسلامة.

الخطوة ٢ — الإبلاغ عن الحادث

عند التعرض لحادث ما أو ملاحظته، يجب تسجيله في صورة تقرير. يمكن التبليغ عن الحوادث كتابيًا أو شفهيًا. مع ذلك، ينبغي الاحتفاظ بسجل مكتوب للحادث لمنع فقدان الحقائق المبلغ عنها. بالنسبة للمدافعين العاملين في منظمة ما، يجب إرسال تقرير الحادث إلى الإدارة. بالنسبة للمدافعين الأفراد، يمكن مشاركة تقرير الحادث مع الزملاء وأصحاب المصلحة الموثوقين. بالإشارة إلى أعمدة الأسئلة الستة، يجب أن تتضمن المعلومات الأساسية في هذا التقرير⁽³⁾: من يقوم بإعداد التقرير:

- ماذا حدث؟ أين حدث؟ متى حدث؟ بأكبر قدر ممكن من الدقة.
- من المتورط؟ مع ذكر تفاصيل ضحايا الحادث.
- تأثير الحادثة على المتضررين، مع ذكر تفاصيل حالتهم الحالية.
- من ارتكب الحادثة، مع تفاصيل مختصرة عن الأعداد، والأسلحة، والانتماء الظاهري والإجراءات التي تمت بعد الحادثة.
- لماذا وقعت الحادثة في ذلك الوقت؟ كيف وقعت؟ (الوسائل التي استخدمها مرتكب الجريمة). ملخص الوضع الحالي وهل هناك مشاكل أم لا؛ إذا كانت الإجابة بنعم، ما هي القرارات والإجراءات التي يقترح مقدم البلاغ اتخاذها/التي اتخذها، وما هي الإجراءات المطلوبة.

الخطوة ٣ — تحليل الواقعة

أثناء إجراء تحليل للواقعة، يجب أن تؤخذ بعض القضايا في الاعتبار مثل: من الذي قد يكون متورطًا، أين وقع الحادث، هل كان هناك أي إصابة جسدية أو أضرار في الممتلكات، وما هو الهدف المحتمل للجناة؟ سيحدد هذا الخطوة التالية بشأن ما إذا كان سيتم الرد ومتى. وفي هذه المرحلة ينبغي تحديد مدى خطورة الحادث لمعرفة ما إذا كان بسيطًا أم خطيرًا.

الخطوة ٤ — هل سيتم اتخاذ ردة فعل أم لا

إن أظهر التحليل أن الحادث خطير، يجب على المدافعين اتخاذ الإجراءات اللازمة. تعتمد هذه الإجراءات على طبيعة الحادث. في حالة حدوث اقتحام للمكتب، يجب وضع أقفال/نظام أمان جديد. إذا تم القبض على أحد المدافعين، سيكون رد الفعل الفوري ضمان إطلاق سراحه. إذا أصيب أحد المدافعين، فهناك حاجة إلى تقديم الإسعافات الأولية وطلب المزيد من الرعاية الطبية.

إذا تم اعتبار الحادث بسيطًا، قد لا يتفاعل المدافعون، لكن يتعين عليهم توثيق الحادث للرجوع إليه في المستقبل. يعتبر الحادث خطيرًا عندما يتعلق بعمل المدافعين، وصحتهم الجسدية وسلامتهم العقلية. لذا، يعد الحادث تهديدًا ويتطلب تحليلًا متعمقًا.

يمكن للمدافعين استخدام وسائل اتصال آمنة مختلفة للإبلاغ عن الحوادث. ويمكنهم أيضًا عقد لقاءات يقدم فيها المبلغ روايات شفوية عن الأحداث.

3 Koenraad Van Brabant 'Operational Security Management in Violent Environments' June 2000, Page 240, <https://sites.google.com/site/ngosecurity/GPR8.pdf?attredirects=0>

فهم التهديدات

ما هو التهديد؟

يمكن تعريف التهديد على أنه التصريح أو الإشارة إلى نية إلحاق الضرر، أو المعاقبة أو الأذى⁽⁴⁾. التهديدات محفزات تبلغنا بالمخاطر المقبلة. ويمكن أن تكون لفظية مباشرة أو غير لفظية.

أمثلة على التهديدات التي يتعرض لها المدافعون

تشمل بعض التهديدات الأكثر شيوعًا التي يتعرض لها المدافعون ما يلي:

- سنقوم بإغلاق منطمتك إن لم توقف عملك
- أنت التالي
- لن تعيش لترى أطفالك
- سأقوم بقتلك

التهديدات من أكثر الاستراتيجيات الشائعة التي تستخدم ضد المدافعين من قبل أصحاب المصلحة، الذين تتأثر مصالحهم سلبًا نتيجة عمل المدافعين. تُفضل التهديدات على الهجمات/الاعتداءات لأنها أرخص الأساليب لوقف عمل المدافعين

التهديدات إشارات على احتمال حدوث ضرر يحيق بالمدافعين. يجمع المعتدون معلومات عنهم وعن عملهم، ثم يستخدمونها لتهديدهم. وقد يقومون بتنفيذ تلك التهديدات إذا ما استمر المدافعون في تجاهلها. لذلك، ينبغي على المدافعين تحليل التهديدات لتحديد المخاطر المحتملة ووضع آليات للتخفيف

طرح التهديد مقابل تنفيذه

يجب على المدافعين معرفة ما إذا كان المهددون جادون في ارتكاب أي هجوم/اعتداء. قد يقوم بعض الأشخاص بالتهديد، لكنهم لا ينفذون تهديداتهم فعليًا، بينما ينفذها البعض. يعتمد الأمر كله على البيئة الاجتماعية والسياسية التي يعمل ضمنها المدافعون. كما أن هناك حاجة للإشارة إلى تنفيذ أو عدم تنفيذ التهديدات السابقة، والوثوق من نوايا مصدر التهديدات⁽⁵⁾.

4 Front Line Defenders, 'Workbook on security: Practical Steps for Human Rights Defenders at Risk' 2011, <https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk>, Accessed 23 June 2016

5 Idem



معظم الأشخاص الذين يطلقون التهديدات يشككون تهديداً في نهاية المطاف: سيهدد هؤلاء الأشخاص المدافعين، وسيستخدمون جميع الوسائل اللازمة لتنفيذ خططهم.

بعض الأشخاص الذين يقومون بالتهديدات لا يشككون تهديداً: في كثير من الحالات لا يتم تنفيذ التهديدات لأن المهددين يريدون تحقيق أهدافهم دون دفع التكاليف. على الرغم من أنه قد لا يتم تنفيذ التهديدات، إلا أنه يتم حث المدافعين على مواصلة مراقبة سلسلة التهديدات المماثلة.

بعض الأشخاص الذين نادراً ما يطلقون التهديدات يشككون تهديداً: على عكس المثالين الأولين، لا تعلن هذه الفئة من الأشخاص عن نواياهم في إلحاق الضرر. وبدلاً من ذلك يكمنون في صمت. إنهم يشككون خطراً دون سابق إنذار. يجب على المدافعين توقع كيف ومتى يمكن أن يؤديك الصمت.

المهددون مقابل منفذي التهديد

في تحليل التهديدات، يميل المدافعون إلى التركيز أكثر على الشخص الذي يصدر التهديدات. لأسباب مختلفة، يقوم المهدد الحقيقي بتكليف أشخاص آخرين لتوصيل التحذيرات أو تنفيذها. ويحتاج المدافعون إلى بذل المزيد من الجهود لتحديد المصادر الحقيقية للتهديدات. توضح الحالة أدناه أن مصادر التهديدات يمكنها تكليف أشخاص لتنفيذ تلك التهديدات:

تُظهر حالة الناشط النيجيري في مجال حقوق الأرض، الراحل كين سارو ويوا، أن الأشخاص الذين يرسلون التهديدات وينفذونها ليسوا هم المهددون الحقيقيون. سُتق هذا الناشط بأمر من الرئيس. مع ذلك، فإن التحليل المتعمق يظهر أن الأمر الرئاسي كان بدافع وتسهيل من قبل شركة متعددة الجنسيات تدعى شل.

كيفية تحليل التهديدات

من الضروري إجراء تقييم مستحق للتهديدات، لتحديد مصادر التهديدات، وأهدافها وفحص احتمالية تنفيذها. يمكن إجراء تحليل التهديدات بشكل فردي أو على المستوى التنظيمي. يمكن أن يشرك المدافعون زملائهم عند إجراء التحليل للحصول على نتيجة غير متحيزة بشأن التهديدات.

عند قيام المدافعون بتحليل التهديدات، يجب عليهم أن يأخذوا بعين الاعتبار حقائق التهديدات، وأنماطها، ومصادرها وأهدافها. يساعد هذا على التوصل إلى نتيجة حول ما إذا كان من الممكن تنفيذ التهديدات أم لا⁽⁶⁾. فيما يلي خمس خطوات لتحليل التهديدات:

تحديد الحقائق المحيطة بالتهديدات

يراقب المدافعون طبيعة التهديدات، ونوعها، ومرسلها وكيف تم إيصالها. قد تأتي هذه التهديدات في صورة رسائل، أو مكالمات هاتفية، أو نصائح بشأن أنشطة حقوق الإنسان المعرضة للخطر، أو الاستدعاءات، أو تصريحات الحكومة بشأن أنشطة المدافعون، أو زيارات المسؤولين الحكوميين والشركات المتعددة الجنسيات أو زيارات الأجهزة الأمنية، وما إلى ذلك.

تحديد أنماط التهديدات مع مرور الوقت

أورد المدافعون سلسلة من الأفعال التي حدثت في فترات معينة. كما يراقبون توقيت التهديدات وتكرارها وخطورتها. ترسل رسائل التهديد أحياناً باستخدام وسائل غير طبيعية مثل الحبر الأحمر، والدم، والجماجم والعظام وما شابه ذلك. تستخدم أيضاً وسائل تهديد مفرطة مثل التوايبت الفارغة أو التوايبت التي تحتوي على حيوانات ميتة.

فحص الهدف من التهديدات

يجب على المدافعون تقييم نية المهددين. قد لا يكون من السهل معرفة نواياهم بشكل دقيق، ولكن يجب على المدافعون أن يسعوا إلى إجراء تحليل متعمق لنواياهم المحتملة. من المهم النظر في كيفية تأثير أنشطة المدافعون سلباً على مصالح أصحاب المصلحة وأنواع التهديدات التي يتلقونها.

6 <https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf>

فحص مصدر التهديدات

من الصعب معرفة المصدر الدقيق للتهديدات لأن المهددين الحقيقيين قد يكلفون وكلاء لتنفيذ هذه التهديدات. يحتاج المدافعون إلى التعمق في تحليلاتهم لمعرفة من؟ أو من أين يأتي التهديد؟. إن معرفة مصدر التهديدات تمكن المدافعين من معرفة إمكانية تنفيذ التهديدات المرسله.



التوصل إلى استنتاج بشأن تنفيذ التهديد

تساعد هذه الخطوة الأخيرة المدافعين على تحديد ما إذا كانت التهديدات ستتحول إلى مخاطر أم لا .



يرجى الملاحظة: تعتمد معرفة حقائق التهديدات وأنماطها على الأحداث الفعلية، في حين يعتمد مصدر التهديدات وهدفها على الافتراضات والتخمينات المسبقة. أما الاستنتاج فيعتمد على الاحتمالية، ويأخذ في الاعتبار نتائج الخطوات الأربع الأولى.



الفصل الخامس

تقييم المخاطر

يعمل المدافعون على احترام، وتحقيق، وحماية حقوق الإنسان المنصوص عليها في الإعلان العالمي وغيره من موثيق حقوق الإنسان. يتعرض المدافعون الذين يعملون من أجل دمج هذه الوثائق في القوانين المحلية لمختلف البلدان ذات أنظمة الحكم المختلفة، لخطر كبير من مختلف أصحاب المصلحة بما في ذلك سلطات الدولة والقطاع الخاص والمجتمعات المحلية. وهذه المخاطر راسخة لا يمكن القضاء عليها. ويتناول هذا الفصل كيفية إدارة المدافعين للمخاطر بشكل فعال والتخفيف من حدتها.

ما هو الخطر؟

يمكن تعريف الخطر على أنه احتمال وقوع حدث يؤدي إلى ضرر. وقد تكون المخاطر هي المخاوف التي يواجهها المدافعون أثناء عملهم اليومي.

أمثلة على المخاطر

يواجه المدافعون مخاطر مثل الاعتقال، والاحتجاز، والسجن، والقتل، والاعتداءات اللفظية وغير اللفظية، والاختطاف، واغتيال الشخصية، وحملات التشويه والرفض من قبل المجتمع وزملائهم المهنيين، والاستدعاءات، والابتزاز، وإغلاق المكتب، ومداهمات المكاتب، والاقتحام، والاعتراض، والتنصت على اتصالات المدافعين وتبعهم. وبعبارة أخرى، هي مخاطر غير مؤكدة يواجهها المدافعون بسبب أنشطتهم في مجال حقوق الإنسان.

مكونات المخاطر

وتتكون المخاطر من ثلاثة متغيرات، وهي الضعف، والقدرة والتهديد. المكونات الثلاثة مترابطة وتحدد احتمالية وتأثير المخاطر.

- ١ **نقاط الضعف:** هي نقاط ضعف داخلية لدى المدافعين، تزيد من احتمالية حدوث الضرر، أو تؤدي إلى تفاقم تأثيره
- ٢ **القدرات:** هي موارد/مؤهلات/نقاط قوة داخلية، يمكن استخدامها لتقليل الضرر وتأثيره
- ٣ **التهديدات:** هي عوامل خارجية، تشير إلى المخاطر التي يمكن أن تؤثر على عمل المدافعين

طبيعة المخاطر

تختلف المخاطر وفقاً لسياق المدافعين، بما في ذلك الملف الشخصي، والموقع الجغرافي، والموارد، والمناهج والأنشطة/القضايا التي يقوم بها المدافعون.

كيفية تقييم المخاطر؟

يجب على المدافعين تحليل المخاطر بشكل صحيح لوضع التدابير المناسبة لتخفيفها. وينبغي عليهم تحديد المخاطر، ومصادرها، وقياس احتمال وقوعها وتأثيرها. كما ينبغي عليهم أن يفكروا فيما إذا كان بإمكانهم تحمل مخاطر محددة. ويمكن تقييم المخاطر باستخدام الخطوات التالية:

١. تعريف المخاطر

يعد تحديد المخاطر مرحلة أولية ولكنها حاسمة في تقييمها. وهو يتضمن إدراج المخاطر المحتملة التي يمكن أن يواجهها المدافعون. يجب على المدافع فهرسة المخاطر في قائمة مرجعية بحيث يتم تحليل كل خطر بدقة. يمكن تحديد المخاطر من خلال العصف الذهني أو المقابلات. أثناء تحليل المخاطر، يجب على المدافعين النظر في الحوادث والتهديدات الأمنية، ورد فعل أصحاب المصلحة والمخاطر التي يواجهها المدافعون الآخرون.

٢. مصادر المخاطر

يحتاج المدافعون إلى الإشارة إلى الأسباب الواضحة والكامنة وراء المخاطر. يمكن أن يكون مسببوا المخاطر مؤسسات أو أفراد تتأثر مصالحهم بعمل المدافعين. يحتاج المدافعون أيضاً إلى النظر في العلاقة بين اثنين أو أكثر من مسببي المخاطر، والتفاعلات المحتملة بين المسببين لتنفيذها.

٣. احتمالية المخاطر

هناك عوامل مختلفة تؤثر على تنفيذ المخاطر. يجتلي المدافعون فرصة حدوث خطر من خلال النظر في قدرات مسببي المخاطر على تنفيذها، وطبيعة العمل من حيث الحساسية، والسياق، والعوامل والجهات الفاعلة التي تؤثر على عمل المدافعين. من المهم كذلك دراسة معدلات احتمالية المخاطر التي واجهها المدافعون في الماضي لقياس احتمالية تنفيذ المخاطر الحالية. يتم قياس احتمالية المخاطر كعالية أو متوسطة أو منخفضة.

٤. تأثير المخاطر

يتم تقدير تأثير المخاطر من حيث الأضرار المرتبطة بها. يمكن لنقاط ضعف وقدرات المدافعين أن تجعل الضرر مرتفعاً أو متوسطاً أو منخفضاً.

٥. تحمل المخاطر

يتم قياس تحمل المخاطر من خلال قدرات المدافعين ونقاط ضعفهم لتحمل مخاطر محددة. يُطلب من المدافعين زيادة قدراتهم على قياس المخاطر والحد من آثارها.

يحتاج المدافعون إلى التوصل إلى نتيجة حول ما إذا كانت المخاطر المحددة يمكن أن تحدث أم لا. ويتناول الاستنتاج قدرتهم على تحمل المخاطر. إذا كان المدافعون قادرين على تحملها، فيجب عليهم اتخاذ تدابير للحد من تأثيرها. تمكنهم هذه الخطوة أيضاً من التفكير في السيناريوهات المحتملة لتنفيذ المخاطر واعتماد استراتيجيات فعالة.

المفاهيم الشائعة والخطئة حول إدارة المخاطر

١. التركيز على الاستراتيجيات التفاعلية

لا يضع معظم المدافعين تدابير إدارة الأمن إلا بعد مواجهة المخاطر أو التهديدات. مع ذلك، من المهم النظر في جميع المخاطر المحتملة التي قد يكون لها تأثير عليهم ووضع استراتيجيات وقائية.

٢. متلازمة النسخ واللصق

يطبق بعض المدافعين تدابير إدارة الأمن التي تعمل بشكل جيد مع المدافعين الآخرين. يعمل المدافعون على مواضيع مختلفة وسياقات مختلفة، ومن ثم يتم وضع التدابير الأمنية وفقاً للسياق. على سبيل المثال، قد يؤدي تركيب كاميرات المراقبة إلى جذب الانتباه والشكوك تجاه المدافعين العاملين في المناطق الريفية.

٣. متلازمة البطولة

تعرض الشجاعة المفرطة المدافعين في بعض الأحيان لمخاطر غير ضرورية. ومن المستحسن أن يقوم المدافعون بقياس نقاط ضعفهم إزاء حجم التهديدات أو المخاطر التي تواجههم، حيث أن أهميتهم وهم أحياء أكبر من فقدانهم.

٤. سوء فهم عمل المدافعين

في بعض الحالات، يخلط المدافعون بين النشاط السياسي والعمل في مجال حقوق الإنسان، مما قد يعيق الحوار بين السلطات والمجتمع المدني. إن الحوارات البناءة المحدودة تخلق شكوكاً متبادلة، ولكن يجب على الحكومات والمدافعين العمل بشكل متكامل.

٥. الميل إلى تجاهل سلامة الفرد وأمنه

يميل المدافعون إلى إعطاء أولوية أكبر لعملهم ولضحايا الانتهاكات بدلاً من أمنهم وسلامتهم. في حين إن أساس عمل المدافعين عن حقوق الإنسان يرتكز على أمنهم وسلامتهم، وبدون ذلك لا يمكن أن يستمر العمل في هذا المجال.

اللفظ السادس

تخطيط الأمن والسلامة

المخاطر متجذرة في عمل المدافعين، ولا يمكن القضاء عليها. مع ذلك، يمكن تخفيفها و/أو تحويلها و/أو نقلها. لذا، يحتاج المدافعون إلى إجراء تقييم منتظم للمخاطر بهدف وضع خطط فعالة للأمن والسلامة.

تخطيط الأمن والسلامة هو عملية وضع وتنفيذ تدابير وقائية وتفاعلية لتعزيز قدرات المدافعين للحد من تأثير المخاطر. وينطبق هذا على الأفراد وكذلك المجموعات والمنظمات. يتضمن هذا التخطيط تطوير السياسات العامة، والخطط والبروتوكولات.

تتكون السياسات من قواعد، ومبادئ وإرشادات عامة، بينما تركز الخطة على تنفيذ السياسات. يتكون البروتوكول من إجراءات التشغيل القياسية للتعامل مع حدث معين.

مكونات سياسة الأمن والسلامة

تصف السياسة العامة الإدارة الشاملة للأمن والسلامة التنظيميين. وينبغي أن تكون مصممة خصيصًا لاحتياجات أمن وسلامة المنظمة.

فيما يلي المكونات القياسية للسياسة العامة للأمن والسلامة

- المبادئ: أولوية الحياة على الممتلكات، والمسؤوليات الفردية والجماعية، وعدم الإضرار، وما إلى ذلك
- النهج والإطار لإدارة الأمن والسلامة
- الموقف من المخاطر - ما هو الحد المقبول

تقييم التهديدات ضد المنظمة على المستوى العام

- من يجب أن يقيم التهديد، كم مرة؟
- كيف ينبغي الإبلاغ عن التهديد؟

أدوار ومسؤوليات الأمن والسلامة: يجب أن تحدد السياسة العامة، بوضوح، الأدوار والمسؤوليات على جميع المستويات؛

- متطلبات مراقبة فعالية إدارة الأمن: على سبيل المثال، عدد المرات التي ينبغي فيها مراجعة السياسة
- لمزيد من الاقتراحات حول إنشاء سياسة أمنية، راجع السياسة العامة للعاملين في مجال الإيدز حول الأمن والسلامة، مايو 2003⁽⁷⁾.

● مكونات خطة الأمن والسلامة

تهدف خطط الأمن والسلامة إلى معالجة المخاطر والتهديدات المتعلقة بالمدافعين في مواقف أو أحداث محددة. للتوصل إلى خطة، يجب على المدافعين تبادل الأفكار حول المخاطر/التهديدات المحتملة، ونقاط الضعف والقدرات. يجب أن تحدد الخطة الجيدة المخاطر وأن يكون لها تدابير وقائية وتفاعلية للتخفيف منها. على سبيل المثال، يمكن للمدافعين الذين يعملون في مجال ختان الإناث (FGM) وضع خطة محددة لمعالجة المخاطر المتعلقة بعملهم.

● ما الذي يجب مراعاته لدى وضع الخطة؟

- ينبغي أن تكون الخطة موجزة، ودقيقة، ومتاحة كوثيقة مرجعية، وسهلة الاستخدام ومزودة بمعلومات محدثة.
- ينبغي أن تعالج المخاطر/التهديدات المحتملة من خلال التقييم المناسب.
- يجب صياغة إجراء مناسب لكل نقطة ضعف، لتلبية القدرات المطلوبة وبالتالي التخفيف من المخاطر.

● تنفيذ خطة الأمن والسلامة

من أجل التنفيذ الفعال، ينبغي إرسال خطة مفصلة إلى جميع الأطراف المعنية بلغة واضحة. وينبغي أن توضح الأدوار والمسؤوليات الدقيقة والمحددة لكل طرف، وأن تتضمن إجراءات تأديبية لضمان الالتزام بالخطة. يتطلب تنفيذ الخطة الموارد، والوقت، والمعرفة والوعي. كما يجب مراجعة الخطة بانتظام لمعالجة المخاطر/التهديدات الناشئة.

الاستراتيجيات الأمنية

هناك ثلاث استراتيجيات/مناهج أمنية رئيسية يطبقها المدافعون ومنظماتهم في عملهم اليومي في مجال حقوق الإنسان.

استراتيجية القبول

نهج يتضمن التفاوض مع جميع الجهات الفاعلة - المجتمع المحلي والسلطات وما إلى ذلك، للحصول على القبول والدعم لوجود المنظمة وعملها. وعلى الرغم من أن هذا يتطلب تخطيطاً دقيقاً وتكثيفاً للعمل، إلا أنه قد يكون الإستراتيجية الأكثر فعالية على المدى الطويل للحد من التهديدات. يستلزم هذا النهج عادةً رؤية واضحة، لذلك في أوقات التهديد الكبير، يكون من الصعب أحياناً التكيف مع كونك أقل لفتاً للانتباه.

استراتيجية الحماية

نهج يركز على الإجراءات الأمنية وعناصر الحماية. وينصب تأثيرها بشكل أساسي على الحد من نقاط الضعف، ويمكن استخدامها جنباً إلى جنب مع الاستراتيجيتين الأخرين لتعزيز الحماية.

استراتيجية الردع

نهج يعتمد على التهديدات المضادة للحماية. على سبيل المثال، في حالة التهديد، قد تتصرف المنظمة من خلال رفع قضية قانونية ضد الشخص الذي أصدره، أو من خلال نشر التهديد، أو الرد على مرتكب الجريمة من خلال شرح عواقب تنفيذ التهديد، مثل الإدانة الدولية. لا ينبغي استخدام هذا النهج إلا إذا كان لديك معلومات دقيقة وحلفاء أقوياء. عندما تقوم بتطوير خططك الأمنية، فكر في كيف يمكن لعناصر القبول والحماية والردع أن توسع قائمة الخيارات المتاحة لديك⁽⁸⁾.

الفصل السابع

آليات الحماية الحالية للمدافعين عن حقوق الإنسان

إن الاعتراف بالدور الحيوي للمدافعين عن حقوق الإنسان والانتهاكات التي يواجهونها، أقنع الأمم المتحدة بضرورة بذل جهود خاصة لحماية المدافعين وأنشطتهم. وكانت الخطوة الرئيسية الأولى هي تحديد الدفاع عن حقوق الإنسان رسميًا كحق في حد ذاته، والاعتراف بالأشخاص الذين يقومون بالعمل في مجال حقوق الإنسان كمدافعين عن حقوق الإنسان.

مقرر الأمم المتحدة الخاص بالمدافعين عن حقوق الإنسان

اعتمدت الجمعية العامة للأمم المتحدة في 9 ديسمبر 1998، بموجب قرارها 144/53، الإعلان المتعلق بحق ومسؤولية الأفراد والجماعات وهيئات المجتمع في تعزيز وحماية حقوق الإنسان والحريات الأساسية المعترف بها عالميًا (المعروف باسم الإعلان المتعلق بالمدافعين عن حقوق الإنسان).

تم اتخاذ الخطوة الثانية في أبريل 2000، عندما طلبت لجنة حقوق الإنسان التابعة للأمم المتحدة (مجلس حقوق الإنسان التابع للأمم المتحدة الآن) من الأمين العام تعيين ممثل خاص معني بالمدافعين عن حقوق الإنسان لرصد ودعم تنفيذ الإعلان⁽⁹⁾.

فوضت لجنة حقوق الإنسان في عام 2000، المقرر الخاص المعني بالمدافعين عن حقوق الإنسان (كإجراء خاص) لدعم تنفيذ إعلان عام 1998 بشأن المدافعين عن حقوق الإنسان⁽¹⁰⁾.

وينص التفويض على الأدوار الرئيسية للمقرر الخاص، وهي:

- التماس المعلومات المتعلقة بحالة المدافعين وتلقيها وفحصها والرد عليها.
- خلق تعاون وحوار مع الحكومات والجهات الفاعلة المهتمة بشأن تعزيز الإعلان وتنفيذه بفعالية.
- التوصية باستراتيجيات فعالة لحماية المدافعين بشكل أكثر فعالية ومتابعة هذه التوصيات.
- دمج منظور النوع الاجتماعي في جميع أنحاء عمله/ها.

9 Fact Sheet 29 - Human Rights Defenders: Protecting the Right to Defend Human Rights <https://www.ohchr.org/Documents/Publications/Fact-Sheet29en.pdf>

10 OHCHR, 'resolution 2000/61 establishing the mandate' <http://ohchr.org/EN/Issues/SRHRDefenders/Pages/Mandate.aspx>,

● بهدف زيادة حماية المدافعين عن حقوق الإنسان، تم إنشاء العديد من الآليات الإقليمية بعد آلية المقرر الخاص للأمم المتحدة المعني بالمدافعين عن حقوق الإنسان. وفيما يلي الآليات الإقليمية الرئيسية:

● - لمقرر الخاص المعني بالمدافعين عن حقوق الإنسان من قبل اللجنة الأفريقية لحقوق الإنسان والشعوب (2005)⁽¹¹⁾.

● - المقرر الخاص المعني بالمدافعين عن حقوق الإنسان التابع للجنة البلدان الأمريكية لحقوق الإنسان⁽¹²⁾.

● - المبادئ التوجيهية للاتحاد الأوروبي بشأن المدافعين عن حقوق الإنسان التي اعتمدها وزراء خارجية الاتحاد

● - الأوروبي في عام 2004⁽¹³⁾.

كما قام الاتحاد الأوروبي بتعيين ممثل خاص لحقوق الإنسان، مكلف بتعزيز فعالية ووضوح سياسة الاتحاد الأوروبي في مجال حقوق الإنسان⁽¹⁴⁾.

● أنشأت اللجنة الأفريقية لحقوق الإنسان والشعوب (ACHPR) في عام 2004، ولاية المقرر الخاص المعني بالمدافعين عن حقوق الإنسان في أفريقيا⁽¹⁵⁾، بالتفويض التالي⁽¹⁶⁾:

١. التماس المعلومات المتعلقة بحالة المدافعين عن حقوق الإنسان في أفريقيا وتلقيها وفحصها والتصرف بناءً عليها.

٢. تقديم التقارير في كل دورة عادية للجنة الأفريقية.

٣. التعاون والمشاركة في الحوار مع الدول الأعضاء، والمؤسسات الوطنية لحقوق الإنسان، والهيئات الحكومية الدولية ذات الصلة، والآليات الدولية والإقليمية لحماية المدافعين عن حقوق الإنسان وأصحاب المصلحة الآخرين.

٤. التوصية ب/تطوير استراتيجيات فعالة لحماية المدافعين بشكل أفضل ومتابعة توصيات المقرر.

٥. العمل على رفع الوعي وتعزيز تنفيذ إعلان الأمم المتحدة بشأن المدافعين عن حقوق الإنسان في أفريقيا.

منذ إنشاء الولاية، حافظ المقرر على تواصل منتظم مع المدافعين، من خلال مشاركتهم في المنتديات الإقليمية والقيام بعدد من زيارات البلدان، بما في ذلك الزيارات المشتركة والبيانات الصحفية مع المقرر الخاص للأمم المتحدة⁽¹⁷⁾.

11 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, <http://www.achpr.org/sessions/35th/resolutions/69/>

12 Inter-American Commission on Human Rights, AG/RES. 1842 (XXXII-O/02), 'Human Rights Defenders: Support for Individuals, Groups, and Organizations of Civil Society Working to Promote and Protect Human Rights in the Americas' http://www.oas.org/juridico/english/ga02/agres_1842.htm, accessed 1 August, 2016

13 EUR-Lex, Access to European Union Law, 'EU guidelines on human rights defenders' 8 December 2008, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33601>, accessed 1 August 2016

14 European Union, "EU Special Representatives," https://eeas.europa.eu/headquarters/headquarters-homepage_en/3606/EU%20Special%20Representatives (accessed 11 May 2020)

15 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, <http://www.achpr.org/sessions/35th/resolutions/69/> accessed 1 August 2016

16 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, <http://www.achpr.org/sessions/35th/resolutions/69/> accessed 1 August 2016

17 DefendDefenders, 'Defending Human Rights, A Resource Book for Human Rights Defenders, East and Horn of Africa Human Rights Defenders Project, 2nd edition, page 8

كما شجع المقرر الخاص الأفراد والمنظمات غير الحكومية على تقديم القضايا المتعلقة المدافعين إلى اللجنة الأفريقية لحقوق الإنسان والشعوب. وبموجب الميثاق الأفريقي لحقوق الإنسان والشعوب، تتمتع اللجنة الأفريقية بصلاحيات تلقي ودراسة الاتصالات من الأفراد والمنظمات⁽¹⁸⁾.

المبادئ التوجيهية للاتحاد الأوروبي بشأن المدافعين عن حقوق الإنسان

تعهد الاتحاد الأوروبي بتعزيز تنفيذ إعلان الأمم المتحدة بشأن المدافعين عن حقوق الإنسان من خلال سياساته الخارجية. واعتمد الاتحاد الأوروبي في عام 2004، مبادئ توجيهية بشأن كيفية مساهمة أعضائه في تعزيز ودعم وحماية المدافعين عن حقوق الإنسان. ورغم أن هذه المبادئ التوجيهية ليست ملزمة قانوناً، إلا أنها تمثل التزامات سياسية من جانب الاتحاد الأوروبي والحكومات الفردية المعنية.

وقد تم تحديد تنفيذ هذه المبادئ التوجيهية كأولوية في السياسة الخارجية للاتحاد الأوروبي في مجال حقوق الإنسان. وتتعاون ولاية الأمم المتحدة مع الآليات الإقليمية لضمان حماية المدافعين. ويشمل التعاون تبادل الخبرات والمعلومات، ومقارنة أساليب العمل وتعزيز بعضها البعض وتحديد الأهداف المشتركة. أنشأت الدول في جميع أنحاء العالم آليات على المستوى الوطني لحماية المدافعين، بما في ذلك إدراج حقوق المدافعين في الدساتير والتشريعات الوطنية، وإدراجهم في المؤسسات الوطنية لحقوق الإنسان. وقامت في بعض الحالات، بسن تشريعات محددة لحماية المدافعين.

المقرر الخاص المعني بالمدافعين عن حقوق الإنسان التابع للجنة الأفريقية لحقوق الإنسان والشعوب

المبادئ التوجيهية الدبلوماسية

بالإضافة إلى الاتحاد الأوروبي، اعتمدت بعض البلدان مبادئ توجيهية بشأن حماية المدافعين عن حقوق الإنسان⁽¹⁹⁾

أصوات في خطر	كندا
خطة عمل للمدافعين عن حقوق الإنسان	هولندا
المبادئ التوجيهية الفنلندية بشأن المدافعين عن حقوق الإنسان	فنلندا
دليل الخدمة الخارجية	النرويج
المبادئ التوجيهية السويسرية المنقحة لعام 2019 بشأن المدافعين عن حقوق الإنسان. (تحل محل نسخة 2014 من المبادئ التوجيهية السويسرية بشأن المدافعين عن حقوق الإنسان)	سويسرا
دعم المملكة المتحدة للمدافعين عن حقوق الإنسان	المملكة المتحدة
صحيفة حقائق مؤرشفة عن المدافعين عن حقوق الإنسان	الولايات المتحدة

18 Article 55 of the African Charter on Human and People's Rights

19 ISHR 'strengthening diplomatic initiatives for the protection of human rights' <https://www.ishr.ch/diplomatic-support>

الآليات الوطنية لحماية المدافعين

يشدد الإعلان الخاص بالمدافعين عن حقوق الإنسان على أن المسؤولية والواجب الأساسي لتعزيز وحماية حقوق الإنسان والحريات الأساسية تقع على عاتق الدولة. ويتعين على الدول ضمان سلامة وحماية المدافعين من خلال تنفيذ الإعلان الخاص بالمدافعين عن حقوق الإنسان. اعتمدت ساحل العاج في يونيو/حزيران 2016، قانون تعزيز وحماية المدافعين عن حقوق الإنسان. وكانت هذه هي المرة الأولى التي تسن فيها دولة أفريقية قانوناً لغرض محدد هو حماية المدافعين⁽²⁰⁾.

١. الآليات الإدارية

لمؤسسات الوطنية لحقوق الإنسان، والمؤسسات القانونية مثل القضاء، وإنفاذ القانون، والشرطة، والأمن القومي، والهيئات التشريعية والحكومات المحلية؛

٢. التشريعات

الديساتير والقوانين المحددة مثل: قانون تعزيز وحماية المدافعين عن حقوق الإنسان في ساحل العاج.

٣. مؤسسات المجتمع المدني

التشبيك بين منظمات المجتمع المدني والاتلافات الوطنية للمدافعين عن حقوق الإنسان.

عمل المدافعين مرهق بطبيعته. والمخاطر والتهديدات التي يواجهونها ليست جسدية ورقمية فحسب، بل هي في أغلب الأحيان نفسية أيضاً. كما يعاني المدافعون من الرفض والتمييز، وغالباً ما يضحون بالكثير نتيجة لعملهم.

تركز التدخلات الأمنية على المكونات المادية والرقمية. مع ذلك، يجب أن تشمل سلامة وأمن المدافعين السلامة العقلية. حيث تحدد الحالة الذهنية نوع القرارات والاختيارات الأمنية التي يتخذها المدافعون.

20 Download the Côte d'Ivoire Law on human rights defenders here (French only), http://www.ishr.ch/sites/default/files/documents/jo_loi_defenseurs.pdf

الفصل الثامن

الرعاية الذاتية والقدرة على التعافي

فهم الإجهاد في سياق عمل المدافعين عن حقوق الإنسان

● ما هو الإجهاد؟

يمكن تعريف الإجهاد على أنه رد فعل تجاه محفز يخل بتوازننا الجسدي أو العقلي. إنه رد فعل جسدي وعاطفي للشخص يحثه على التغيير. الإجهاد له مستويات مختلفة من الأقل إلى الأعلى، وهو محبط ومستنزف بسبب عدم التوازن بين قدرات المدافعين والتحديات التي يفرضها الوضع. يختلف الإجهاد من شخص لآخر، فما قد يكون مرهقًا لأحدهم قد لا يكون مرهقًا لآخر.

● أنواعه

بحسب موقع [Healthline](#)، هناك طرق مختلفة لوصف الإجهاد، ويمكن تصنيفه حسب طبيعته على مدى فترة زمنية على النحو التالي:

□ الإجهاد الحاد

وهو النوع الأكثر شيوعًا. ويأتي من متطلبات وضغوطات الماضي القريب، ومتطلبات وضغوطات المستقبل القريب المتوقعة. يحدث الإجهاد الحاد دفعة واحدة، ويؤدي إلى ارتفاع مستوى القلق بسرعة. على سبيل المثال، قد يؤدي استدعاءك لإجراء مقابلة عمل، أو تفويت رحلة جوية أو تلقي أخبار سيئة، إلى إصابتك بالذعر.

┌ الإجهاد الحاد العرضي

عندما يحدث الإجهاد الحاد بانتظام، فإنه يسمى الإجهاد الحاد العرضي. هذا النوع من التوتر متكرر، ويتخذ عادة نمطًا منتظمًا. ويمكن تشبيهه بموجة ترتفع وتهبط. يمكن أن تشمل أمثلة الإجهاد العرضي الحاد ضغط الإيجار، والرسوم المدرسية وسداد القروض.

الإجهاد المزمن



وهو النوع الذي يتعايش الناس معه بصورة دائمة. إجهاد طاحن يهكهم يوماً بعد يوم، وعمامًا بعد عام. يدمر الإجهاد المزمن الأجساد، والعقول والحياة، ويستنزفهم على المدى الطويل. ويرتبط بالأحوال الدائمة مثل الأسر المفككة، والأمراض المستعصية، والوقوع في فخ زواج غير سعيد أو في وظيفة أو مهنة محتقرة.

أسباب الإجهاد الشائعة في سياق عمل المدافعين

الحروب والصراعات	تقلص المساحة السياسية التي بإمكان المجتمع المدني المشاركة فيها
الفساد وسوء الممارسات	الصراع الانتخابي
الاعتقال والاحتجاز التعسفي	التشهير والوصم
التعذيب	ارتفاع مستويات الفقر

أعراض الإجهاد

للإجهاد أعراض سلوكية وفسولوجية ونفسية. ويمكن ملاحظته من خلال التغيير في أنماط السلوك ووظائف الجسم البيولوجية. ويمكن أن يظهر أيضًا من خلال التغيير في العواطف والعمليات العقلية. تشمل بعض الأعراض السلوكية إهمال الذات، وتغيير عادات الأكل، وعادات ارتداء الملابس، وتغيير أنماط النوم، والميول الانطوائية والعدوانية، والتهيج وما إلى ذلك. تشمل الأعراض الفسيولوجية الإرهاق الجسدي، والتعرق الزائد، والقرح، والصداع، والإسهال وتغيير في الدورة الشهرية. تشمل الأعراض العقلية/النفسية النسيان، واضطرابات الكلام، وفقدان الذاكرة، والحزن، والغضب وانخفاض الأداء الوظيفي.

ترويض الإجهاد

لا يمكن القضاء على الإجهاد بالكامل. لكن يمكن محاولة إدارة عليه بملاحظة ماهية الضغوطات، والمشاكل والمتطلبات الرئيسية التي تسببه. حيث يمكن للمرء استكشاف الخيارات التي من شأنها أن تساعد في التغلب على التأثير السلبي الناجم عن هذه الضغوطات. هناك طرق مختلفة لإدارة التوتر يمكن تطبيقها كالعلاج بالتواصل الكلامي، والعلاج البيئي، الرياضة البدنية والعلاج بالتدليك، والعلاج بالفن وغيرها الكثير. يتم تشجيع المدافعين على استخدام ممارسات الرعاية الذاتية البسيطة التي لا تتطلب أي خبرة علمية. بعضها مذكور في الصورة أدناه.

Slow Down	Keep Calm	Be Positive	Take it EASY
UNPLUG	Enjoy LIFE	Have FUN	BREATHE
	Go OUTSIDE		MEDITATE

الطرق الأخرى الموصى بها للتعامل مع التوتر مذكورة أدناه⁽²¹⁾:

- اهتم بنفسك، تناول أكلاً صحيًا، تمرن وأحصل على قسط كاف من النوم
- احصل على الدعم، وتحدث مع الآخرين حتى تزيل الأحمال عن كاهلك
- كن اجتماعيًا، لا تعزل نفسك بعد التعرض للإجهاد
- ابتعد لبعض الوقت عن مسببات الإجهاد
- ابتعد عن المخدرات والكحول، فقد يخدعناك في البداية بأنهما خففا من المشكلة، لكنهما يسببان مشاكل أكبر على المدى الطويل
- تعلم أن تقول (لا) واسمح بالرفض
- خذ قسطًا من الراحة
- قم بفعل أشياء تحبها مثل الغناء، أو الرقص أو اللعب
- رتب جدولك مثل (العمل، البيت، أوقات الفراغ)
- اترك جميع النشاطات إن كانت تؤذيك أكثر من أنها تساعدك. ومن المهم أن تتذكر أن ما يرهقك ليس العبء ولكن طريقة حملك له. ويمكن أن تكون حصيلة الإجهاد في بعض الأحيان جيدة، فقد يحث الإجهاد أحدهم على العمل بصورة أفضل.
- لكن إن لم تقم بإدارته بصورة جيدة قد يصير مؤذيًا







الأمن الرقمي

كتيب للمدافعين الأفارقة

يحتوي الجزء الخاص بكتيب الأمن الرقمي على محتوى تم تكييفه (ليو افق المُستخدِم المحلي) من دليل الدفاع عن النفس ضدّ المراقبة الذي أنتجته مؤسسة التخوم الإلكترونية، وقد تم تحريره تحت نفس الترخيص

مُرخص بموجب اتفاقية سي سي-بي-3.0 للحقوق المتروكة، والتي تنصُّ على أن: لك الحرّية في نسخ وإعادة توزيع المواد ضمن أيّ وسيط أو شكل، فضلاً عن الدمج، والتحويل، والبناء على المواد لأي غرض، شريطة أن تُنسب المواد إلى المؤلف الأصلي

المحتويات

- ٣٤ كيفية استخدام هذا الدليل
- ٤٠ التأمين الأساسي للجهاز
- ٤٦ أمن البيانات على الأجهزة
- ٥١ أمن البيانات المتنقلة عبر الشبكات
- ٦٣ أمن الحساب الإلكتروني
- ٦٨ تأمين الهواتف النقالة
- ٧٧ المصادر
- ٧٨ الملحقات

كيفية استخدام هذا الدليل

المقدمة

دليل السلامة الرقمية

أنت مدافع أفريقي، في القرن الحادي والعشرين. مسلح بفكرك الثاقب، وإحساسك القوي بالعدالة الاجتماعية، وارتباطاتك بالمجتمعات المحلية، وهاتفك وجهاز الكمبيوتر المحمول. ستحوز، قبل 20 عامًا، الثلاثة ملكات الأولى بلا شك، لكن الهاتف الذي في جيبك، والكمبيوتر المحمول في حقيبتك هما أمران يخصان القرن الحادي والعشرين.

تعمل التكنولوجيا الرقمية على تعقيد قدرتنا على تقييم المخاطر الشخصية والمهنية التي نواجهها، لأنها غالبًا ما تكون غير بديهية. بدون المعرفة المتخصصة والتقنية، من الصعب تحليل الأماكن التي تخون فيها الأجهزة الثقة الموضوعة فيها لتخزين الملفات الحساسة وتوصيل المعلومات السرية.

قيل كثيرًا إن أفريقيا قد تجاوزت التكنولوجيا القديمة المرتبطة الهواتف الأرضية السلكية، حيث انفجر سوق الهواتف المحمولة في جميع أنحاء القارة بمعدلات أسرع بكثير من أي مكان آخر في العالم. لكن بالمقابل، فإن المعايير العالمية التكنولوجية، والقانونية ومعايير حقوق الإنسان المتعلقة بالخصوصية والأمن لها تأثير هائل على البيئة بالنسبة للمدافعين الأفارقة والمجتمع ككل، دون أن يكون لديهم بالضرورة فرصة متساوية للتأثير على هذه التطورات.

بدأت الحرب العالمية على الإرهاب بالتزامن مع الاستخدام واسع النطاق لتكنولوجيا الاتصالات الشخصية مثل البريد الإلكتروني، وسكايب، وفيسبوك ماسنجر، وواتساب، مما أدى إلى مواجهة بين حقوق الخصوصية الفردية وحجج الأمن الجماعي. وفي الوقت نفسه، فإن شركات الأمن الخاصة التي تعمل على تطوير برامج وأجهزة قرصنة هجومية وبيعها لحكومات العالم، تعني أن المراقبة الرقمية المتطورة أصبحت في متناول وكالات وإنفاذ القانون بتكاليف أقل بكثير.

أجبرت جائحة كوفيد-19 المنظمات على اعتماد أساليب العمل عبر الإنترنت. وقد أدى هذا إلى زيادة المخاطر المرتبطة بعملهم، حدث الوضع الجديد بسرعة كبيرة دون إيلاء الاعتبار الواجب للمخاطر الأمنية الأساسية. سيزودك هذا الكتيب بالمعرفة التكنولوجية لتتمكن من تقييم المخاطر الرقمية بشكل أفضل، واتخاذ خطوات للتخفيف من تلك المخاطر. سنشير في هذا الكتيب إلى سيناريوهات وقصص المدافعين الأفارقة أثناء مواجهتهم تحديات رقمية في عملهم. تم تنظيم هذا الكتيب على النحو التالي:

تقييم المخاطر

يواجه جميع المستخدمين تهديدات الأمن السيبراني، فلاحين ورؤساء. ومقارنة بالمستخدمين العاديين، فإن المخاطر أعلى بالنسبة للمدافعين بسبب طبيعة أنشطتهم الرقمية.

في هذا القسم، سنُفصل مفهوم المخاطر، وننظر إلى فئات المخاطر التكنولوجية في سياق التأثيرات الواقعية. ستتعلم كيفية تحديد أصولك الأكثر عرضة للخطر والبدء في تحديد أولويات التدابير الرامية إلى تقليل نقاط الضعف.

خمسة أهداف أمنية

يستكشف الجزء المتبقي من هذا الكتيب خمس فئات للأمن الرقمي، تسهم معًا في تشكيل الأمن العام لممارساتك الرقمية. ليس المقصود من هذه الفصول أن تكون شاملة، ولا من الممكن تدريس المهارات بالكامل من خلال هذه الصفحات نظرًا لأن البرامج تتغير كثيرًا، إلا أننا سنربطك بالموارد التي تظل محدثة بأحدث المراجع. أهدافنا الأمنية الخمسة هي:

١. التأمين الأساسي للجهاز

نحن مسؤولون عن أجهزتنا (وليس العكس)، لكن هل نعرف كيفية تشغيلها بشكل صحيح؟ هل نبذل قصارى جهدنا لإبقائها في حالة تشغيل جيدة، ومقاومة للفيروسات ونقاط الضعف الأخرى التي قد تهاجمها؟ سنناقش في هذا القسم أفضل الممارسات لاستخدام نظام التشغيل والبرامج.

٢. أمن البيانات الموجودة على أجهزة الكمبيوتر، وأجهزة تخزين البيانات، ومحركات الأقراص الخارجية والهواتف المحمولة.

يتم تخزين البيانات على الكمبيوتر المحمول، وسطح المكتب، والهاتف المحمول، ومحركات الأقراص الصلبة الخارجية ومحركات أقراص USB المصغرة. إذا حصل شخص ما على هذه الأجهزة، أو نسخ الملفات منها مباشرة أو عبر الشبكة، فهل سيكون قادرًا على قراءة (وتغيير) تلك البيانات؟ سنناقش في هذا القسم مفهوم وممارسات التشفير، الذي يحمي البيانات الموجودة على أجهزتك أو وحدات التخزين عن طريق كلاود the cloud .

علاوة على ذلك، يتعرض أمن البيانات للخطر إن كنت تملك نسخة واحدة فقط من المستندات المهمة، وتم فقدان هذه النسخة بسبب الفساد، أو السرقة، أو الضرر المادي أو أي من كوارث الكمبيوتر الأخرى. سننظر في حلول النسخ الاحتياطي، ونأخذ في الاعتبار أمن ممارسته.

٣. أمن البيانات التي تنتقل عبر الشبكات

تأتي معظم قيمة أجهزة الكمبيوتر والهواتف لدينا من حقيقة أنها تتواصل مع الأجهزة الأخرى عبر الإنترنت وشبكات الهاتف المحمول. يتم الاتصال عبر العديد من الأوساط مثل البريد الإلكتروني، وتصفح الشبكة، ونقل الصوت باستعمال بروتوكول الإنترنت والهاتف العادي، والرسائل النصية (تمت مناقشته ضمن أمن الهاتف المحمول). وسوف ننظر في طبيعة تدفقات الاتصالات هذه ونفهم الآثار الأمنية المترتبة عليها، خاصة في سياق المراقبة المتزايدة.

٤. أمن الحسابات

كيف نضمن عدم اختراق حساباتنا المتصلة وغير المتصلة بالإنترنت، الذي قد يؤدي إلى فقدان البيانات، والهوية وانتحال الشخصية؟ يتم هنا تناول أفضل الممارسات مثل كلمات المرور الفريدة، والمصادقة الثنائية ومدير كلمات المرور.

٥. امن الهاتف

لم يتم تصميم الهواتف المحمولة التقليدية (الاتصالات والرسائل النصية القصيرة) مع أخذ الأمن في الاعتبار. تقدم الهواتف الذكية إمكانات جديدة ومخاطر جديدة، ونتعرف على جميع مجالات الأمان المذكورة أعلاه من حيث صلتها بالهواتف المحمولة.

يشير السؤال الأول غالبًا إلى الأصول. والأصول هي أشياء تقدرها وتريد حمايتها. عندما نتحدث عن الأمن الرقمي، فإن الأصول المعنية عادة ما تكون معلومات. على سبيل المثال، تعتبر رسائل البريد الإلكتروني وقوائم جهات الاتصال والرسائل الفورية والملفات الخاصة بك كلها أصولًا. أجهزتك هي أيضًا أصول.

تقييم المخاطر

لا يوجد حل واحد للحفاظ على أمانك على الإنترنت. كما لا يتعلق الأمن الرقمي بالأدوات التي تستخدمها؛ بل بفهم التهديدات التي تواجهها وكيفية مقاومتها. ينبغي للمرء إجراء تقييم لنمذجة التهديد.



عند إجراء التقييم، هناك خمسة أسئلة رئيسية يجب أن تطرحها على نفسك:

١. ما الذي تريد حمايته؟
٢. ممن تريد حمايته؟
٣. ما مدى احتمالية أنك ستحتاج إلى حمايته؟
٤. ما مدى سوء العواقب إذا فشلت في حمايته؟
٥. ما مقدار المشاكل التي أنت على استعداد لخوضها لمحاولة منع ذلك؟

يشير السؤال الأول غالبًا إلى الأصول. والأصول هي أشياء تقدرها وتريد حمايتها. عندما نتحدث عن الأمن الرقمي، فإن الأصول المعنية عادة ما تكون معلومات. على سبيل المثال، تعتبر رسائل البريد الإلكتروني وقوائم جهات الاتصال والرسائل الفورية والملفات الخاصة بك كلها أصولًا. أجهزتك هي أيضًا أصول.

قم بتدوين قائمة بالبيانات التي تحتفظ بها، ومكانها، ومن يمكنه الوصول إليها وما الذي يمنع الآخرين من الوصول إليها.
وللإجابة على السؤال الثاني - ممن تريد حمايتها؟ من المهم أن تعرف من قد يرغب في استهدافك أو استهداف معلوماتك، أو من هو خصمك. الخصم هو أي شخص أو كيان يشكل تهديدًا على أصل أو أصول. ومن أمثلة الخصوم المحتملين الكيانات التجارية، أو فاعلين سيئين في الحكومة أو قرصنة الانترنت.

قم بإعداد قائمة بالأشخاص الذين قد يرغبون في الحصول على بياناتك أو اتصالاتك. يمكن أن يكونوا أفرادًا أو وكالة حكومية أو شركة.

التهديد هو شيء سيء يمكن أن يحدث للأصل. هناك العديد من الطرق التي يمكن للخصم من خلالها تهديد بياناتك. على سبيل المثال، يمكن للخصم قراءة بياناتك الخاصة أثناء مرورها عبر الشبكة، أو حذفها أو إتلافها. يمكن للخصم أيضًا تعطيل وصولك إلى بياناتك الخاصة.

تختلف دوافع الخصوم بشكل كبير، وكذلك هجماتهم. قد تكتفي الحكومة التي تحاول منع انتشار مقطع فيديو يظهر عنف الشرطة بحذف هذا الفيديو أو تقليل توافره، في حين قد يرغب خصم سياسي في الوصول إلى محتوى سري ونشره دون علمك.

اكتب ما قد يرغب خصمك في فعله ببياناتك الخاصة.

يجب التفكير أيضًا في قدرات المهاجم. على سبيل المثال، يتمتع مزود خدمة الهاتف المحمول الخاص بك بإمكانية الوصول إلى جميع سجلات هاتفك وبالتالي لديه القدرة على استخدام تلك البيانات ضدك. يمكن لقرصنة الانترنت الموجود على شبكة Wi-Fi مفتوحة الوصول إلى بياناتك غير المشفرة. وربما تتمتع حكومتك بقدرات أقوى.

للإجابة على السؤال الثالث، يجب عليك أن تأخذ في الاعتبار المخاطر. الخطر هو احتمال حدوث تهديد معين ضد أصل معين، ويسير جنبًا إلى جنب مع القدرة. على الرغم من أن مزود خدمة الهاتف المحمول الخاص بك لديه القدرة على الوصول إلى جميع بياناتك، إلا أن خطر نشر بياناتك الخاصة عبر الإنترنت للإضرار بسمعتك منخفض.

ومن المهم التمييز بين التهديدات والمخاطر. في حين أن التهديد هو أمر سيء يمكن أن يحدث، فإن الخطر هو احتمال حدوث التهديد. على سبيل المثال، هناك تهديد باقتحام مكتبك، ولكن خطر حدوث ذلك أقل بكثير في مكان يوجد فيه حراس أو جيران ودودون مقارنة بمكان يُنظر إليك فيه بعدائية.

إن إجراء تحليل المخاطر هو عملية شخصية وذاتية على حد سواء؛ فليس لدى الجميع نفس الأولويات أو ينظرون إلى التهديدات بنفس الطريقة. يجد العديد من الأشخاص أن بعض التهديدات غير مقبولة بغض النظر عن المخاطر، لأن مجرد وجود التهديد لا يستحق التكلفة. وفي حالات أخرى، يتجاهل الناس المخاطر العالية لأنهم لا ينظرون إلى التهديد باعتباره مشكلة.

دعونا الآن نتدرب على نمذجة التهديدات

إذا كان مكتبك يخزن حسابات المبلغين عن الفساد في الخدمة العامة، فقد ترغب في السؤال

- هل يجب أن يكون لدى المكتب حراسة على مدار اليوم وكاميرات مراقبة؟
- ما هو نوع قفل الباب الذي يجب أن نستثمر فيه؟
- هل نحتاج إلى أمان متطور أكثر بالإضافة إلى قفل باب قوي؟
- ما مدى أهمية ما نحاول حمايته؟
- - الأدلة التي يمكن أن تضع حداً للفساد في الخدمة العامة
- ما هو التهديد؟
- - وسيحاول الجناة المتهمون اقتحام هذه الملفات والوصول إليها
- ما هو الخطر الفعلي إن قام المتهم بالاقتحام؟ هل هذا مرجح؟
- - إن حصل مرتكبو الفساد على هذه الشهادات، فيمكنهم مهاجمة المبلغين جسديًا، كما يمكنهم سرقة الملفات وتدمير الأدلة التي يمكن استخدامها ضدهم

بمجرد أن تسأل نفسك هذه الأسئلة، يمكنك تقييم التدابير التي يجب اتخاذها. إذا كانت ممتلكاتك ذات قيمة، ولكن خطر الاقتحام منخفض، فمن المحتمل أنك لن ترغب في استثمار الكثير من المال في القفل. من ناحية أخرى، إذا كانت المخاطرة عالية، فسوف ترغب في الحصول على أفضل الأقفال في السوق، وربما حتى إضافة نظام أمني.

الأمن الرقمي في خمسة أجزاء

مهم

غالبًا ما تكون الإجراءات الموضحة في الأقسام التالية تقنية ويمكن أن تحمل درجات من المخاطر. قد يؤدي إجراء تغييرات على أجهزتك إلى حدوث أخطاء غير متوقعة، أو إن نفذت بشكل خاطئ قد تؤدي إلى فقدان البيانات. يُنصح بالبحث في جميع الخطوات اللازمة لإجراء تغييرات فنية بما يتناسب مع جهازك وسياقك الخاص، وأخذ نسخ احتياطية من البيانات المهمة، وتخزين كلمات المرور الجديدة بشكل صحيح (راجع أمن الحساب للحصول على النصائح ذات الصلة)، وطلب المساعدة الفنية عند الضرورة.

علاوة على ذلك، تختلف الاختصاصات القانونية ووجهات النظر بشأن الأمن الرقمي، ويجب على كل فرد أن يسعى إلى فهم المخاطر التي ينطوي عليها الأمر وفقًا لسياقه.

كيف أحمي نفسي من البرامج الخبيثة؟

اشترت نانسوبوجا - الأوغندية المدافعة عن حقوق الأرض - جهاز كمبيوتر جديد منذ 6 أشهر، لكنه يعمل ببطء، وترى نوافذ تنبثق على شاشتها لا تفهمها، ويبدو أن بيانات الإنترنت عبر الهاتف المحمول الخاصة بها تنفذ بسرعة كبيرة. كانت قد حملت مستندات المشروع على محرك أقراص محمول، لكنها تختفي من عليه باستمرار. لا تفهم ما يحدث، إنه جهاز جديد، وقد قامت بتثبيت جميع برامجها من مواقع التنزيل عبر الإنترنت ومن الأصدقاء الجيدين.

من المرجح أن نانسوبوجا تواجه إصابات بالبرامج الخبيثة غير المرغوب فيها على جهاز الكمبيوتر الخاص بها. تشكل البرامج الخبيثة تهديد يؤثر على جميع مستخدمي الكمبيوتر. ويمكن أن تؤدي إلى فقدان المعلومات، وانخفاض الأداء، وسرقة المستندات والتجسس.

التأمين الأساسي للجهاز

علاوة على ذلك، تختلف الاختصاصات القانونية ووجهات النظر بشأن الأمن الرقمي، ويجب على كل فرد أن يسعى إلى فهم المخاطر التي ينطوي عليها الأمر وفقًا لسياقه.

تدور جميع جوانب الحياة الآن حول التكنولوجيا والإنترنت، سيكون لكل شيء تملكه (بما في ذلك الهاتف، والسيارة، والساعة، والثلاجة!) قدرة أن يكون متصلًا بالإنترنت مع القدرة على إرسال واستقبال معلومات.

نعهد إلى أجهزتنا بالكثير من المعلومات التي تحدد هويتنا، وأين نحن، وماذا نفعل، وما الذي نخطط لفعل ومع من نضع خططنا. تعتبر هذه الأجهزة أهدافًا واضحة للهجوم، والاختراق والتسلل.

مع أخذ هذه الخلفية في الاعتبار، من المهم جدًا أن يتمتع جميع مستخدمي التكنولوجيا والإنترنت بمستوى أساسي من المعرفة والمهارات اللازمة لحماية أجهزتهم ضد المتسللين، والبرامج الخبيثة وأي ثغرة أمنية أخرى يمكن أن تعرض حياتهم للخطر بسبب اختراق الجهاز أو الهجوم عليه.

يستلزم التأمين الأساسي للجهاز الممارسات والخطوات التي تضع أجهزتك في الشكل الأمثل لتجنب الاختراق.

البرامج الخبيثة، هي أي برنامج أو ملف يتم استخدامه لإيذاء مستخدمي الكمبيوتر. وهو يعمل بعدة طرق مختلفة، على سبيل المثال لا الحصر، تعطيل الكمبيوتر، أو جمع معلومات حساسة، أو انتحال شخصية مستخدمه لإرسال رسائل غير مرغوب فيها أو مزيفة، أو الوصول إلى أنظمة الكمبيوتر الخاصة. غالبية البرامج الخبيثة إجرامية، وتستخدم غالبًا ما للحصول على معلومات مصرفية أو بيانات اعتماد تسجيل الدخول للبريد الإلكتروني أو حسابات الوسائط الاجتماعية. تُستخدم هذه البرامج أيضًا من قبل الجهات الحكومية وغير الحكومية للتحايل على التشفير والتجسس على المستخدمين. على سبيل المثال⁽²²⁾، تمتلك البرامج الخبيثة قدرات واسعة النطاق؛ قد تسمح للمهاجم بالتسجيل من كاميرا الويب، والميكروفون وتعطيل إعداد الإشعارات.

22 <http://pastebin.com/MP8zpQ26>.

برامج مكافحة الفيروسات

يجب عليك استخدام برنامج مكافحة الفيروسات على جهاز الكمبيوتر الخاص بك والهاتف الذكي. يمكن أن تكون برامج مكافحة الفيروسات فعالة جدًا في مكافحة البرامج الخبيثة العامة غير المستهدفة، التي قد يستخدمها المجرمون ضد عامة السكان. مع ذلك، عادةً ما تكون برامج مكافحة الفيروسات غير فعالة ضد الهجمات المستهدفة وغيرها من الهجمات المعقدة، مثل تلك التي تبنيها شركة الأمن الإسرائيلية مجموعة إن إس أو NSO Group.

مؤشرات الاختراق

إن كان من الصعب اكتشاف البرامج الخبيثة باستخدام برامج مكافحة الفيروسات، لا يزال من الممكن، في بعض الأحيان، العثور على مؤشرات اختراق. على سبيل المثال، ستقدم قوقل Google أحيانًا تحذيرًا لمستخدمي جيميل Gmail، يفيد بأنها تعتقد أن حسابك قد تم استهدافه من قبل مهاجمين ترعاها الدولة. بالإضافة إلى ذلك، قد تلاحظ ضوءًا يشير إلى أن كاميرا الويب الخاصة بك قيد التشغيل عندما لم تقم بتنشيطها بنفسك (على الرغم من أن البرامج الخبيثة المتقدمة قد تكون قادرة على إيقاف تشغيل ذلك) — قد يكون هذا مؤشرًا آخر على وجود اختراق. هناك مؤشرات أخرى أقل وضوحًا؛ قد تلاحظ أنه يتم الوصول إلى بريدك الإلكتروني من عنوان IP غير مألوف، أو أنه تم تغيير إعداداتك لإرسال نسخ من كل رسائل البريد الإلكتروني الخاصة بك إلى عنوان بريد إلكتروني آخر. يجب أن يحتوي جهاز الكمبيوتر الخاص بك بالفعل على جدار حماية منشط مثل جدار الحماية المدمج في نظام التشغيل ويندوز Windows أو أبل OS X، ولكن من المفيد أيضًا تنشيط جدران الحماية التجارية من مجموعات أمن الإنترنت.

كيف يمكن للمهاجمين استخدام البرامج الخبيثة لاستهدافي؟

أسهل طريقة لاستهداف أحد الأشخاص بواسطة هذه البرامج هي من خلال رسائل البريد الإلكتروني التصيدية. يتظاهر المهاجم بأنه شخص تعرفه، ويرسل إليك بريدًا إلكترونيًا يحتوي على مرفق به برامج خبيثة. بمجرد تنزيل مرفق وفتحه، تصيب البرامج جهاز الكمبيوتر أو الجهاز الخاص بك.

يُعد "هجوم دون انتظار (Zero-day attacks)" طريقة أخرى أكثر تعقيدًا لإصابة الأجهزة بالبرامج الخبيثة التي تستخدمها الحكومات والمجرمين بشكل خاص.

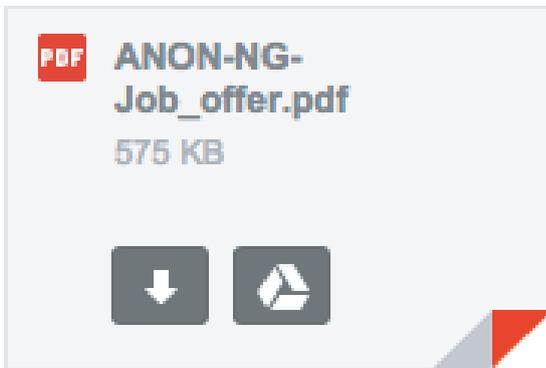
يستغل "هجوم دون انتظار" ثغرة أمنية لم تكن معروفة سابقًا في جهاز أو تطبيق تكنولوجي. تخيل أن جهاز الكمبيوتر الخاص بك هو حصن؛ سيكون "هجوم دون انتظار" بمثابة مدخل سري مخفي لا تعرف عنه أنت شيئًا، لكن اكتشافه أحد المهاجمين. لا يمكنك حماية نفسك من مدخل سري لا تعلم بوجوده. تقوم الحكومات ووكالات إنفاذ القانون بتخزين الثغرات التي يكتشفها "هجوم دون انتظار" لاستخدامها في هجماتهم بالبرامج الخبيثة. قد يتمكن المجرمون والجهات الفاعلة الأخرى أيضًا من الوصول إليه واستخدامه. نظرًا لارتفاع تكلفتها، تُستخدم هذه الهجمات لاستهداف أفراد رفيعي المستوى.

هناك العديد من الطرق التي قد يحاول المهاجم خداعك عن طريقها لتثبيت برامج خبيثة على جهاز الكمبيوتر الخاص بك. قد يخفي البرنامج كرابط في موقع ويب، أو مستند، أو ملف PDF ، أو حتى برنامج مصمم للمساعدة في تأمين جهاز الكمبيوتر الخاص بك. قد يتم استهدافك عبر البريد الإلكتروني (والذي قد يبدو كما لو أنه مرسل من شخص تعرفه)، أو عبر رسالة على سكايب أو تويتر Twitter، أو حتى عبر رابط منشور على صفحتك على فيسبوك Facebook .

في ديسمبر 2014، تم استهداف نامين زيليكي، المدير الإداري لتلفزيون إثيوبيا الفضائي (ESAT)، من مكتبه في الولايات المتحدة الأمريكية، ببرنامج مراقبة عن بعد من شركة تقنية معلومات تسمى هاكينج تيم Hacking Team ، تم تسليمه له عبر بريد إلكتروني ظن أنه يحتوي على معلومات حول الانتخابات الإثيوبية.

في عام 2013، أستخدم أحد زملاء زيليكي ببرامج خبيثة، بعد أن وصله ملف وورد Word من مايكروسوفت Microsoft . وعلموا لاحقاً أنه من قبل هاكينج تيم Hacking Team .

أفضل طريقة لتجنب الإصابة بهذا النوع من البرامج المستهدفة هي تجنب فتح المستندات وتثبيت تلك البرامج في المقام الأول. سيكون لدى الأشخاص الذين يتمتعون بقدر أكبر من الخبرة الحاسوبية والتقنية حدس أفضل إلى حد ما بشأن ما يمكن أن يكون برنامجاً خبيثاً، ولكن الهجمات الموجهة جيداً يمكن أن تكون مقنعة للغاية. إذا كنت تستخدم جيميل Gmail ، وتفتح المرفقات المشبوهة في قوقل درايف Google Drive بدلاً من تنزيلها (انظر الصورة على سبيل المثال)، فما الذي يمكن أن يحمي جهاز الكمبيوتر الخاص بك إذا كان مصاباً بالفعل. يؤدي استخدام نظام حوسبي أكثر أماناً، مثل أوبونتو Ubuntu أو كروم Chrome OS أو ماك Mac OS X إلى تحسين فرصك بشكل كبير في مواجهة العديد من حيل تسليم البرامج الخبيثة، ولكنه لن يحميك من الخصوم الأكثر تطوراً.



إن كنت تستخدم جيميل، فيمكنك عرض المستند المرفق من خلال النقر على أيقونة المثلث داخل المربع الثاني (وليس سهم التنزيل) في المربع الأول. وسيظهر على متصفحك من خلال مرشحات قوقل بدلاً من تنزيله على جهازك، ما يجنبك المخاطر.

يمكنك القيام بشيء آخر لحماية جهازك من البرامج الخبيثة، وهو التأكد دائماً من تشغيل أحدث إصدار من البرنامج، وتنزيل آخر التحديثات الأمنية. يمكن للشركات في حال اكتشاف ثغرات أمنية جديدة في البرامج، إصلاح المشكلة وتحديث البرنامج، لكنك لن تجني فوائد عملهم إلا إن قمت بتثبيت التحديث على جهازك. من المعتقدات الشائعة أنه إن كنت تشغل نسخة غير مسجلة من ويندوز، فلا يمكنك أو لا ينبغي لك قبول التحديثات الأمنية. هذا ليس صحيحاً. انظر أدناه للحصول على مزيد من المعلومات حول الحفاظ على تحديث أنظمتك.

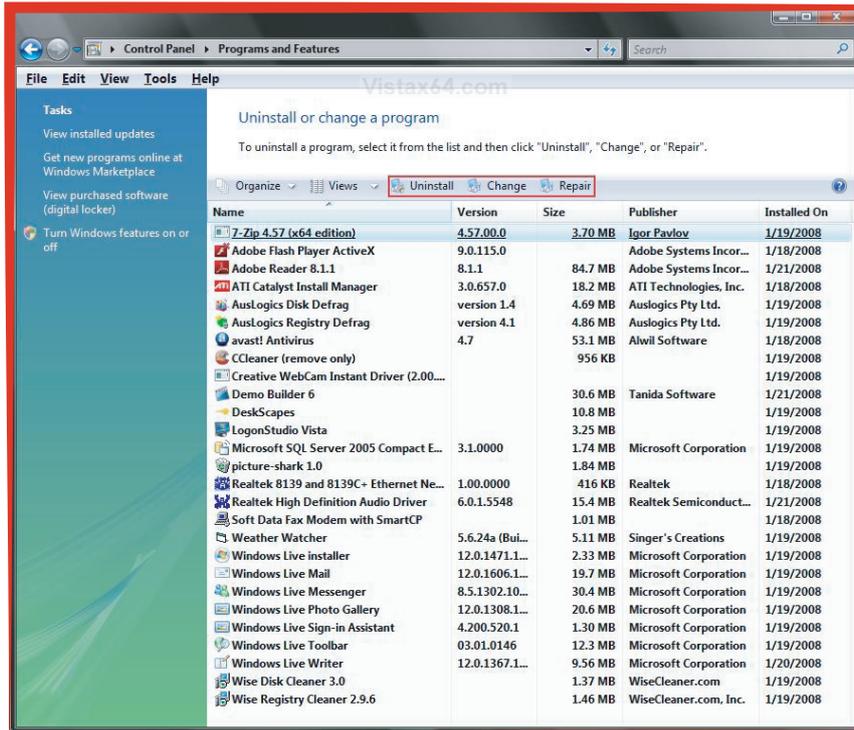
ماذا أفعل إن وجدت برامج خبيثة على جهاز الكمبيوتر الخاص بي؟

قم بفصل جهازك عن الإنترنت وتوقف عن استخدامه على الفور. ربما يتم إرسال كل ضغطة تقوم بها إلى أحد المهاجمين. خذ جهازك إلى خبير أمني، قد يتمكن من اكتشاف المزيد من التفاصيل حول البرامج الخبيثة. إن عثرت على تلك البرامج، فمجرد إزالتها لن تضمن أمان الجهاز.

إن كنت تشك في أن جهازك يحتوي على برامج خبيثة، قم بتسجيل الدخول إلى جهاز آخر تعتقد أنه آمن، وقم بتغيير كلمات المرور الخاصة بك؛ فكل كلمة مرور كتبها على جهازك الخاص أثناء إصابته قد تكون كشفت.

ربما ترغب في إعادة تثبيت نظام التشغيل على جهازك لإزالة البرامج الخبيثة. سيؤدي هذا إلى إزالة معظمها، ولكن قد تستمر بعض البرامج المعقدة.

الاستمرار في التحديث



أجهزة وبرامج الكمبيوتر ليست مثالية أبدًا. ستكون هناك دائمًا مشكلات تتعلق بالأداء، والاتزان والأمان في أي برنامج: يتضمن ذلك نظام التشغيل الخاص بك، سواء كان (ويندوز، أو لينكس، أو ماك أو إس)، وهاتفك المحمول سواء كان (أندرويد، أو آي أو إس، أو ويندوز فون)، وبرامجك (أدوبي، وجافا، وأوفيس، وكروم وفايرفوكس، الخ). هناك سوق مزدهر من الباحثين الذين يبحثون باستمرار عن نقاط الضعف في أنظمتنا. قد يكون هؤلاء الباحثون من قرصنة القبعات البيضاء الذين يكشفون عن نقاط الضعف علنًا ويشجعون المطورين على تصحيح البرامج، أو قد يكونون من قرصنة القبعات السوداء الذين يبيعون نقاط الضعف للمشتريين من المجرمين والحكوميين، من يخططون لاستخدام نقاط الضعف هذه ضد مستخدمي البرامج.

إن أردت معرفة مدى شيوع نقاط الضعف، قم بزيارة <https://www.exploit-db.com/> واعرف عدد نقاط الضعف الموجودة في البرامج التي نستخدمها. وهذا ما يفسر سبب مطالبتنا في كثير من الأحيان بتحديث النظام والبرنامج.

في أي وقت تتاح لك فرصة لتحديث البرنامج، يجب عليك القيام بذلك. إن خُبرت بين التحديث الآن أو لاحقًا، قم دائمًا بالتحديث في أقرب وقت ممكن، لا تؤجله. إن كان لديك خيار تمكين التحديثات التلقائية، قم بتشغيله. وإن كنت تستخدم النطاق العريض النقال، وتدفع مقابل استخدام الإنترنت لكل ميجابايت أو لكل جيجابايت، فحدد وقتًا للاتصال بمصدر للإنترنت غير المحدود مثل جامعة أو مكتبة أو مكتب أو مقهى، وابدأ التحديثات. قم بتشغيل التحديثات التلقائية لنظام التشغيل الخاص بك، وقم بتحديث متصفحك وجميع البرامج التي تستخدمها بشكل منتظم. يمكن أن تساعد تطبيقات مدير التحديث أيضًا في إدارة التحديثات، والتأكد من إمكانية تثبيت التحديثات المتوفرة لتطبيقاتك.

تطبيقات البرمجيات الآمنة

نظرًا لأن البرامج تضحى ضعيفة وبحاجة إلى التحديث طوال الوقت، فإن إحدى أبسط الطرق للحفاظ على أمانها هي تجنب تثبيت البرامج غير الضرورية. برنامجي أدوبي فلاش Adobe Flash وأراكل جافا Oracle Java غالبًا، لديهما عيوب خطيرة. قد لا تحتاج إلى أي من هذه البرامج على جهازك على الإطلاق⁽²³⁾. انتقل إلى قائمة البرامج المثبتة لديك (في نظام التشغيل ويندوز: إضافة/إزالة البرامج، أو إلغاء تثبيت برنامج أو تغييره) وراجع ما تم تثبيته. هل هناك برامج لا تعرف إسمها؟ قد تكون بعض هذه العناصر مهمة لعمل جهازك، لكن إذا كان هناك شيء يبدو مريبًا بالنسبة لك، فيجب عليك البحث عنه، وتحديد عن إمكانية إزالته. كن حذرًا بشكل خاص من البرامج المثبتة التي ليس لها ناشر مدرج في عمود الناشرين. ابحث أيضًا عن أشرطة أدوات المتصفح المساعد التي تم تثبيتها دون علمك.

بعد مراجعة البرامج المثبتة، قم بفتح المستعرضات الخاصة بك وابحث عن الملحق أو البرامج الإضافية، وراجع الملحقات التي قمت بتثبيتها كذلك. كما يجب عليك تقليل عدد الملحقات المثبتة الموثوقة إلى الحد الأدنى. ملحقات المتصفح حساسة،

23 Google Chrome includes a secured version of Adobe Flash inside of all of its updates.

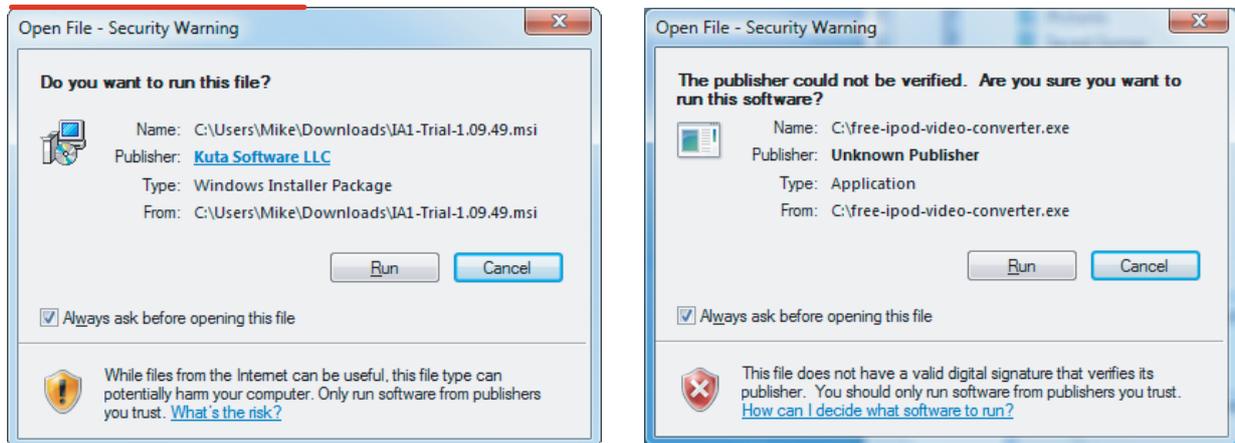
لأنها قد تكون قادرة على قراءة وتغيير المعلومات التي تكتب وتظهر على متصفحك، مثل كلمات المرور، والمعلومات المصرفية ومشاركات وسائل التواصل الاجتماعي.

مصادر آمنة

يجب الحصول على البرنامج من ناشر البرنامج مباشرة قدر الإمكان. على سبيل المثال، فمن الأفضل تنزيل أدوبي ريدر Adobe Reader من <https://get.adobe.com/reader/> بدلاً من www.download.com أو أي مصدر آخر. وبالمثل، يجب عليك تجنب تثبيت البرامج من محركات الأقراص المحمولة الخاصة بالأصدقاء، أو ملفات EXE المرسلة إليك عبر البريد الإلكتروني، أو الرسائل الفورية. قد يتم تغيير البرنامج، أو قد يكون مزيفًا تمامًا ويضر بجهازك.

غالبًا ما تجمع مواقع التنزيل المجانية تنزيلات البرامج مع التنزيلات الإضافية غير المرغوب فيها والتي تعد بميزات إضافية ولكنها ليست مرغوبة أو مطلوبة في البداية، وقد تكون مضرّة تمامًا بجهازك. راجع قصة التنزيلات العشرة على قمة قائمة التنزيلات على المتصفح العام، والتي أدت إلى تلف الأجهزة بشدة⁽²⁴⁾.

عندما تقوم بتثبيت البرنامج، تحقق من ناشر البرنامج. يقوم معظم الناشرين ذوي السمعة الطيبة بالتوقيع على برامجهم، مما يدل على أنها خاصتهم ولم يتم تعديلها أثناء النقل. قارن بين شاشتي التحذير التاليتين لنظام التشغيل ويندوز لمعرفة الفرق بين البرامج الموقعة وغير الموقعة:



تذكر أنه يمكن الحصول على معظم البرامج التي تحتاجها مجانًا، ومباشرةً، من مواقع الويب الخاصة بالناشر. إذا رأيت عرضًا للحصول على شيء ما مجانًا، وكان يتعين عليك الدفع مقابله إن أخذته من مصدر آخر، سيكون هذا العرض جيدًا لدرجة يصعب تصديقها. اتخذ بعض الاحتياطات الأساسية وستحافظ على سرعة جهازك، واستقراره وأمنه على المدى الطويل.

24 <https://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download.com-apps/>

أمن البيانات على الأجهزة

يعمل داود في منظمة غير حكومية. تعرضت مكاتبتهم، قبل بضعة أسابيع، للاقتحام، حيث سُرقت أجهزة الكمبيوتر المكتبية، والمحمولة، والكاميرات والهواتف المحمولة. كما سرقت عقود المنظمة، ووثائقها المالية، وجهات اتصالها، وملفات أبحاثها ومنشوراتها. ولم يكن هناك نسخ احتياطية لأي من أجهزة الكمبيوتر الموجودة في المكتب. تشعر إدارة داود بالقلق إزاء دوافع اللصوص، وتخشى أن تقع المعلومات السرية التي بحوزتهم في الأيدي الخطأ.

يعد فقدان البيانات أمرًا مؤلمًا لأي فرد أو مؤسسة، فهو يؤدي لسببين: من ناحية، أنت تفقد المعلومات الحيوية اللازمة لعملك، ومن ناحية أخرى، حاز شخص آخر على معلوماتك دون تصريح.

يجب على داود مكافحة هذا الخطر على مستويات متعددة. مثل تشفير البيانات بحيث لا يتمكن سوى الشخص الذي لديه كلمة المرور الصحيحة من قراءة البيانات الأصلية، وعمل نسخ احتياطية بانتظام على أغراض مادية وعلى الإنترنت.

ما هو التشفير؟

هو وسيلة لتعمية البيانات حتى تتمكن الأطراف المصرح لها فقط من فهمها.

لدينا، الآن، أجهزة كمبيوتر يمكنها القيام بهذا التشفير من أجلنا. توسعت تكنولوجيا التشفير الرقمي إلى ما هو أبعد من الرسائل السرية البسيطة؛ على سبيل المثال، يمكن استخدام التشفير لأغراض أكثر تفصيلاً مثل حماية المستندات، أو التحقق من مرسل الرسائل أو تصفح الويب مع إخفاء هويتك.

الحفاظ على أمن بياناتك بواسطة التشفير

حمل الكثير منا الاتصالات، ومعلومات حول جهات الاتصال، ومستندات العمل الحساسة على أجهزة الكمبيوتر المحمولة، وأجهزة التخزين القابلة للإزالة، وحتى الهواتف المحمولة. يمكن أن تتضمن هذه البيانات معلومات سرية حول عملك، ومجتمعك، وشبكاتك وتتبع حقوق الإنسان. لكن توجد دائمًا إمكانية سرقة الجهاز الفعلي أو نسخه في ثوانٍ.

يمكن قفل أجهزة الكمبيوتر والهواتف المحمولة بكلمات مرور، أو أرقام التعريف الشخصية أو الرموز، لكن لن تساعد هذه الأقفال في حماية البيانات إذا تم الاستيلاء على الجهاز نفسه. من السهل نسبيًا تجاوز هذه الأقفال، نظرًا لأنه يتم تخزين بياناتك في شكل يسهل قراءته داخل الجهاز.

مستخدمًا للتشفير، يمكنك أن تجعل من الصعب على أولئك الذين يسرقون البيانات كشف أسرارها، فخصمك لن يحتاج إلى جهازك فحسب، بل سيحتاج أيضًا إلى كلمة المرور الخاصة بك لفك تشفير/فتح البيانات المشفرة. هناك العديد من تطبيقات التشفير: تشفير الجهاز بالكامل، وتشفير الملفات أو حوافز الملفات، وتشفير الاتصالات (سيتم مناقشته في الفصل التالي).

الأكثر أمانًا، والأسهل، هو تشفير جميع بياناتك، وليس مجرد حافظات قليلة. توفر معظم أجهزة الكمبيوتر والهواتف الذكية تشفيرًا كاملاً لكامل الجهاز (أو القرص بالكامل) كخيار. يضمن التشفير الكامل للجهاز عدم إمكانية الوصول إلى محتويات وحدة تخزين الكمبيوتر أو الهاتف من قبل أشخاص غير مصرح لهم بذلك. ويؤدي تشفير الجهاز بالكامل إلى تشفير جميع المعلومات المكتوبة عليه، ولتفكيك المعلومات سنكون بحاجة إلى كلمة المرور حتى يصبح الجهاز قابلاً للاستخدام.

توفر هواتف أندرويد هذا الخيار ضمن إعدادات الأمان الخاصة بها، وتصنفه أجهزة أبل المحمولة مثل آيفون وآيباد بـ "حماية البيانات"، ويتم تشغيله تلقائيًا إن قمت بتعيين رمز مرور. على جهاز الكمبيوتر الذي يعمل بنظام التشغيل ويندوز بروفيشنال، يُعرف باسم بيتلوكر BitLocker. على أجهزة ماكينتوش يطلق عليه فايلفولت FileVault. في لينوكس، عادةً ما يتم تقديم التشفير الكامل للقرص عند إعداد نظامك لأول مرة من خلال نظام يسمى لوكس LUKS. يمكن للبرامج المستقلة مثل فيراكريبت VeraCrypt وديسك كريبتور Disk Cryptor أن تساعدك أيضًا على تحقيق نفس الأهداف.

بإمكانك أيضًا استخدام أنظمة تشفير القرص الكامل لغرض تشفير الوسائط المحمولة مثل الأقراص الصلبة الخارجية، وأقراص الفلاش، وذلك باستخدام بيتلوكر تو جو (ويندوز)، فيليفولت (ماك) أو فيراكريبت (ويندوز وماك ولينكس).

أحد نقاط الضعف المحتملة للتشفير الكامل للجهاز هو مركزيتها: ففي حالة اضطرارك لفك غلق الجهاز، ستكون جميع ملفاتك عرضة للهجوم. الحل الأكثر قوة هو الجمع بين التشفير الكامل للجهاز مع تشفير الملفات والمجلدات من أجل حجز المستندات الأكثر قابلية للهجوم عن كل شخص لديه حق الوصول إلى حسابات جهازك الرئيسية.

يسمح لك خيار تشفير الملفات والمجلدات بترميز ملفات بعضها أو أقسام من جهاز الكمبيوتر الخاص بك. واحدة من الخيارات الممتازة هي برنامج فيراكريت (يعمل على أجهزة كمبيوتر ويندوز، وماك، ولينكس). يسمح لك فيراكريت بخلق "حجم" سري لملفاتك يبدو ظاهريًا وكأنه قرص فلاش، ولكنه في الواقع موجود داخل ملف مشفر على جهاز الكمبيوتر الخاص بك. هناك خيار آخر سهل الاستخدام هو أكسكربت، وهو برنامج يعمل فقط مع الويندوز، ويقوم بتشفير الملفات من خلال الاختيار من القائمة عبر نقر زر الماوس الأيمن على جهاز الكمبيوتر الخاص بك، مما يسمح لك بتشفير الملفات الفردية بسهولة وقتما وأينما أردت. راجع الصندوق التالي للتعرف على مزيد من المعلومات حول هذه الخيارات.

تذكر دائمًا أن جودة تشفيرك تكون كذلك بقدر جودة كلمة المرور الخاصة بك. لا تقم بكتابة كلمة المرور على ورقة ملاحظة مرفقة بالشاشة، كذلك لا تحتفظ بقائمة كلمات المرور في دفتر ملاحظات. في حال استولى مُعتدي على جهازك، يمكنه تجريب العديد من كلمات المرور المختلفة حتى يستطيع تخمين كلمة المرور الخاصة بك. كما يمكن لبرامج كسر كلمات المرور تجريب الملايين منها في ثانية واحدة. وهذا يعني أن اختيار كلمة مرور تتكون من أربعة رموز ليس من المرجح تمامًا أن تحمي البيانات الخاصة بك لفترة طويلة، وحتى كلمة المرور الطويلة قد تبطيء فقط عمل الشخص الذي يهاجم جهازك الخاص. في ظل هذه الظروف يجب أن تكون كلمة مرورك قوية وتضم أكثر من خمسة عشر رمزًا. راجع فصل أمان الحساب الإلكتروني للحصول على مزيد من المعلومات حول إنشاء كلمات مرور قوية.

برمجيات وإرشادات التشفير

تشفير الكمبيوتر

بيتلوكر (ويندوز) - متوفر في الإصدارات البروفيشونال من ويندوز 7 و8، وعلى معظم إصدارات ويندوز 8.1 فما فوق. وهو دليل سهل الاستخدام متاح في ⁽²⁵⁾HowTGeek، بالإضافة إلى الويندوز سينترال المخصص لنظام التشغيل ويندوز 10⁽²⁶⁾. لاحظ أن بيتلوكر يتطلب بالضرورة جهاز يسمى (TPM) غالبًا ما يكون متاحًا فقط في أفي أجهزة الكمبيوتر التجارية المتطورة. يتضمن كلا الدليلين المرتبطين هنا توجيهات حول كيفية تنشيط BitLocker في أجهزة الكمبيوتر التي لا تحتوي على TPM.

فيليفولت (نظام تشغيل ماك) - من السهل إعداد تشفير الجهاز بالكامل على معظم أجهزة الكمبيوتر التي تعمل بنظام التشغيل ماك. اتبع تعليمات أبل لتنشيط فيليفولت من داخل تفضيلات النظام الخاص بك⁽²⁷⁾.

ديسكريبنتور (ويندوز)⁽²⁸⁾ - اقرأ الدليل من مؤسسة التخوم الإلكترونية الخاص ببرنامج ديسكريبنتور للتشفير الكامل للويندوز⁽²⁹⁾.

فيراكربت⁽³⁰⁾ (ويندوز، ماك، لينكس) - وهو برنامج يستطيع تشفير كامل القرص الصلب أو أقسام منه، وكذلك محركات الأقراص القابلة للإزالة. موجّهات الأمن في (Box A) توقّر توجيهات ممتازة⁽³¹⁾.

25 <http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/>

26 <http://www.windowscentral.com/how-use-bitlocker-encryption-windows-10>

27 <https://support.apple.com/en-us/HT204837>

28 <https://diskcryptor.net/>

29 <https://ssd.eff.org/en/module/how-encrypt-your-windows-device>

30 <https://veracrypt.codeplex.com/>

31 [https:// securityinabox.org/en/guide/veracrypt/windows](https://securityinabox.org/en/guide/veracrypt/windows)

تشفير الهاتف

● **تشفير الأندرويد** - اقرأ الدليل من ⁽³²⁾ HowTGeek .

تشفير آيفون وآيباد - ببساطة قم بتفعيل قفل رمز المرور على جهازك وسوف تتمكن من تشفير الجهاز. اعرف المزيد من دليل مؤسسة التخوم الإلكترونية⁽³³⁾.

محركات الأقراص الخارجية

● **بيتلوكر (ويندوز)** - تشفير الأقراص الصلبة الخارجية وأقراص الفلاش باستخدام ⁽³⁴⁾ BitLocker To Go .

● **فايلفولت (ماك)** - تشفير الأقراص الصلبة الخارجية وأقراص الفلاش عن طريق النقر بزر الماوس الأيمن فوق الجهاز القابل للإزالة وقم باختيار "تشفير" من على الباحث ثم اختار كلمة مرور. انظر الدليل لدى أبل⁽³⁵⁾.

لاحظ أن الحلول الخاصة بالأقراص الخارجية المذكورة أعلاه سوف تجعل الأقراص المشفرة مقصورة فقط لاستخدامها مع نظام التشغيل ماك أو ويندوز فقط. تقدم فيراكريبت بدلاً من ذلك حلاً لتشفير محرك الأقراص الخارجي عبر الأنظمة الأساسية.

النسخ الاحتياطي للبيانات الخاصة بك

أمن المعلومات يعني أيضاً الحصول على البيانات عندما تكون في حاجة إليها. ما هي التهديدات التي قد تحدث من توافر معلوماتك الخاصة؟ سرقة أجهزة الكمبيوتر من الأماكن العامة والخاصة هو خطر شائع، ولكن هناك أشياء أخرى مثل الفيروسات، وتعطل الكمبيوتر، والحرائق، وأضرار المياه، أو تلف القرص الصلب، جميعها قد تؤدي إلى فقدان البيانات أيضاً. لمعالجة هذه المخاطر يجب عليك الاحتفاظ بانتظام بنسخ احتياطي للملفات الخاصة بك.

يتم الاحتفاظ بالنسخ الاحتياطية تقليدياً في الأقراص الصلبة الخارجية، وأقراص الفلاش، والأقراص القابلة للإزالة مثل الأقراص المدمجة وأقراص الفيديو الرقمية. تذكر أن وسائط التخزين هذه معرضة للسرقة والحصول عليها بواسطة أشخاص غير مرغوب فيهم، لذا يجب عليك القيام بتشفير النسخ الاحتياطية. راجع قائمة المصادر في القسم السابق للتعرف على كيفية تشفير محركات التخزين الخارجية.

إجراء النسخ الاحتياطية يمكن أن يكون أمراً بسيطاً مثل عملية نسخ ولصق مواد العمل الخاصة بك على محرك أقراص خارجي. ومع ذلك توجد العديد من التطبيقات للمساعدة في إجراء عملية النسخ الاحتياطي. يحتوي ويندوز على خيارين مُدمجين في النظام لإجراء عملية النسخ الاحتياطي (غير متوفر في جميع الإصدارات): سيعمل خيار النسخ الاحتياطي والاستعادة⁽³⁶⁾ بعمل نسخ احتياطي لكامل النظام بحيث يمكنك استرداده في حالة فقدان البيانات، وعلاوة على ذلك يمكنك جدولة تحديثات عملية النسخ الاحتياطي الكامل؛ وعمل تاريخ للملف⁽³⁷⁾، وسيحتفظ بنسخ من الوثائق أثناء تغييرها بمرور الوقت.

32 <http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/>,

33 <https://ssd.eff.org/en/module/how-encrypt-your-iphon>

34 <https://technet.microsoft.com/en-us/magazine/ff404223.aspx>,

35 <https://www.uvm.edu/it/kb/article/encrypt-external-drive/>

36 <https://support.microsoft.com/en-us/help/17127/windows-back-up-restore>,

37 <https://support.microsoft.com/en-us/help/17128/windows-8-file-history>,

يمكنك استخدام أيًا من هذين النظامين أو الاثنين في الوقت نفسه. يحتوي نظام تشغيل ماك أو أس أكس أيضًا على نظام نسخ احتياطي مُدمج في النظام يسمى تايم ماشين⁽³⁸⁾، يوفر نسخ احتياطية إضافية إلى محرك الأقراص الصلبة الخارجية، والتي يمكن اختياريًا تشفيرها عن طريق تفعيل خيار التشفير أثناء الإعداد.

من المفيد أن يكون لديك نسخة احتياطية سحابية محلية وبعيدة لملفاتك. يمكنك استخدام برامج النسخ الاحتياطي السحابية الشهيرة مثل Dropbox، Google Drive، Copy، Onedrive. إذا كنت قلقًا من خصوصية النسخ الاحتياطية والوصول إليها من قبل مزود السحابة (مثل غوغل و ميكروسوفت و دروببواكس)، فيجب عليك فحص برامج النسخ الاحتياطي التي تشفر الملفات على جهاز الكمبيوتر الخاص بك قبل أن يتم تحميلها إلى مزود السحابة: انظر Mega، Sync.com، SpiderOak، Wuala.

هناك أيضًا برمجيات تعمل على تشفير الملف على الجهاز ثم نقل هذه الملفات المشفرة إلى دروبوكس أو غيره من مقدمي النسخ الاحتياطي السحابية: انظر BoxCryptor⁽³⁹⁾، Duplicati⁽⁴⁰⁾، Viivo⁽⁴¹⁾

38 Time Machine <https://support.apple.com/en-us/HT201250>

39 <https://www.boxcryptor.com/>

40 www.duplicati.com

41 <https://viivo.com/>

تأمين البيانات المتنقلة عبر الشبكات

تعمل جيرالدينا مدافعة عن الحقوق البيئية للإنسان. كانت تخطط لعقد اجتماع توعية مع جميع سكان منطقتها لإبلاغهم عن خطوة الحكومة المزمعة لإعطاء الغابات لمستثمرين أجنب. لذا كتبت رسالة وأرسلتها بالبريد الإلكتروني إلى جميع القادة المحليين، وأخبرتهم بإبلاغ جميع الناس بموعد ومكان الاجتماع. وقبل بضعة أيام من تاريخ الاجتماع، تفاجأت من معرفة أن جميع القادة المحليين لم يتلقوا بريدها الإلكتروني.

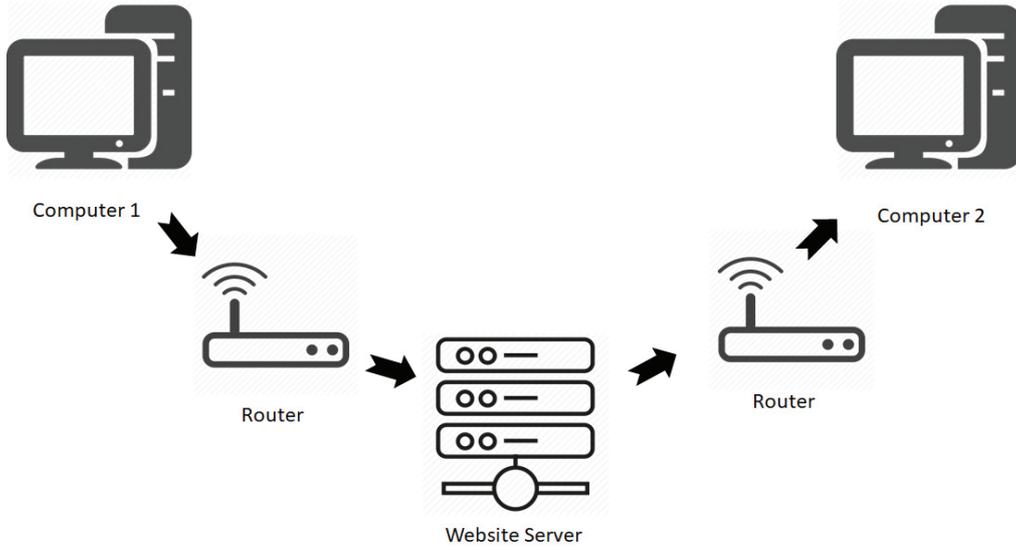
وبعد بضعة أيام زارتها الشرطة وحذرتها من تحريض الجمهور وتخريب البرامج الحكومية. تعجبت جيرالدينا مما حدث لبريدها الإلكتروني، ومن كيف حصلت الشرطة على رسالتها بدلاً من المتلقين المقصودين.

ما حدث لجيرالدينا يُسمى بالمراقبة. وهو يحدث عندما يكون شخصًا ما قادرًا على رصد الاتصالات الخاصة بك لأنه يتم إرسالها في نص غير مشفر عبر الإنترنت.

يمكن لجيرالدينا استخدام التشفير مثل HTTPS ، و GPG ، و VPN ، للحفاظ على اتصالاتها سرية وخصوصية، بحيث لا يمكن استخدامها لتخفيفها بسبب قيامها بعمله.

الحفاظ على أمن بياناتك بواسطة التشفير

الإنترنت عبارة عن شبكة من الشبكات التي توفر تبادل المعلومات بين الكمبيوتر العميل والخوادم. أجهزة الكمبيوتر العميلة هي الأجهزة التي تستخدمها مثل الكمبيوتر المحمول، والكمبيوتر المكتبي، والهواتف الذكية المحمولة؛ والتي تطلب معلومات أو خدمات مستضافة أو مخزنة على أجهزة كمبيوتر الخادم. يستخدم الكمبيوتر العميل والخادم مجموعة متنوعة من البروتوكولات (مثل لغة مشتركة يفهما كلا الجانبين) مثل بروتوكول نقل النص التشعبي (HTTP) للطلبات والاستجابات بينهما. تنتقل جميع المعلومات التي يتم إرسالها عبر بروتوكول HTTP عبر الإنترنت كنص عادي: أي شخص لديه موقع متميز في الشبكة (مثل مزود خدمة الإنترنت، أو مدير مقهى الإنترنت، أو أي واحدة من مئات الآلاف من نقاط تبادل الإنترنت يمكن أن يسجل الاتصالات الخاصة بك.



رسم تبسيطي يوضح كيفية عمل الإنترنت من خلال شخص يتصل بموقع إخباري لقراءة الأخبار

كما ترون، هناك العديد من أجهزة الكمبيوتر الأخرى المشاركة في ربط المستخدم بالخادم الذي يحتاجه. ومن خلال البروتوكولات غير الآمنة، يمكن لأجهزة الكمبيوتر الأخرى أيضاً قراءة محتويات اتصالات المستخدم وحتى تغييرها.

لحسن الحظ، تتوفر بروتوكولات أكثر أماناً للمساعدة في تأمين بياناتنا واتصالاتنا أثناء انتقالها عبر الإنترنت. ومع ذلك، يجب أن نفهم ما هي، وما هي الأدوات التي تستخدمها.

التواصل مع الآخرين

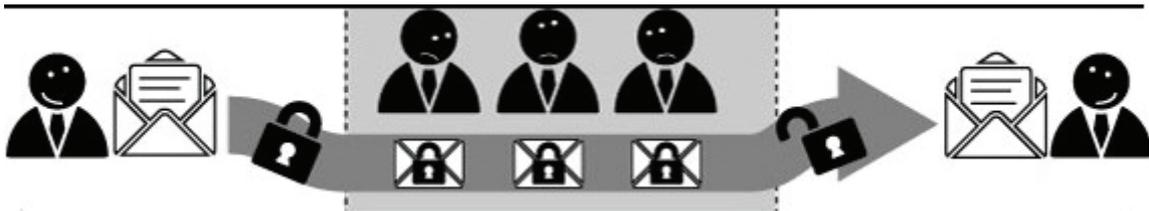
جعلت شبكات الاتصالات والإنترنت التواصل مع الناس أسهل من أي وقت مضى، ولكنها جعلت المراقبة أيضاً أكثر انتشاراً مما كانت عليه في أي وقت مضى في تاريخ البشرية. ومن دون اتخاذ خطوات إضافية لحماية خصوصيتك، فإن كل مكالمات هاتفية، ورسالة نصية، وبريد إلكتروني، ورسالة فورية، واتصال صوتي عبر بروتوكول الإنترنت (VoIP)، وكلّ دردشة مرئية، وكلّ رسالة عبر وسائل الإعلام الاجتماعية، قد تكون عرضة للمتنصتين.

في الغالب يكون التواصل وجهاً لوجه هو الأسلوب الأسلم للتواصل مع الآخرين، أي من دون استخدام أجهزة الكمبيوتر أو الهواتف على الإطلاق. وبما أن هذا الأمر لا يتوفر دائماً، فإن أفضل خيار بديل هو استخدام الشيفرة من طرف إلى طرف، وذلك عند التواصل عبر الشبكة إن كنت بحاجة لحماية محتوى اتصالاتك.



كيف يعمل التشفير المتبادل؟

عندما يريد شخصان التواصل بشكل آمن (كاماو وأبوياء على وجه المثال) يتوجب على كل منهما أن يستخدم مفاتيح تشفير. فقبل أن يرسل كاماو رسالة إلى أبوياء، يقوم بتشفيرها لمفتاح أبوياء بحيث تكون أبوياء هي الوحيدة القادرة على فك تشفيرها. ثم ترسل بالفعل كرسالة مشفرة عبر الإنترنت. إن كان هناك أحد يتنصت على كاماو وأبوياء، حتى إذا كان لديه القدرة على الوصول إلى الخدمة التي يستخدمها كاماو لإرسال هذه الرسالة (مثل حساب بريده الإلكتروني)، فلن يرى سوى بيانات مشفرة ولن يتمكن من قراءة الرسالة. وعندما تستقبل أبوياء الرسالة، يتوجب عليها أن تستخدم مفتاحها لفك تشفير الرسالة كي تتمكن من قراءتها.



ينطوي التشفير المتبادل من طرف إلى طرف على بعض الجهد الإضافي، ولكنها الطريقة الوحيدة للتحقق من أمن اتصالاتهما دون الحاجة إلى الثقة بالمنصة التي يستخدمانها. ادّعت بعض الخدمات - مثل سكايب⁽⁴²⁾ - أنها تستخدم الشيفرة من طرف إلى طرف، في حين يبدو أنها لا تقوم بذلك فعلياً. حتى تكون الشيفرة المتبادلة بين طرفين آمنة، يجب على المستخدم أن يكون قادراً على التحقق من أن مفتاح التشفير الذي يُشَقَّر رسائله تعود ملكيته إلى الأشخاص الذين يعتقد أنهم يملكونه فعلاً. إذا كان برنامج الاتصالات لا يحتوي على تلك الخاصية بشكل مُدمج، فإن أي تشفير يستخدمه يمكن اعتراضه من قبل مزود الخدمة نفسه، مثلاً في حال دفعتم الحكومة لذلك.

المكالمات الصوتية

عندما تجري مكالمة من هاتف ثابت أو محمول، فإن اتصالك لا يكون مُشفراً باستخدام الشيفرة المتبادلة بين طرفين. إذا كنت تستخدم هاتفاً محمولاً، فقد يكون اتصالك مشفراً (بشكل ضعيف) بين هاتفك وأبراج الهاتف الخلوية، ولكن مع انتقال المحادثة عبر شبكة الهاتف تكون معرضة للاعتراض من قبل شركة الهاتف، وبالتالي أي حكومة أو منظمة لها سلطة على شبكة الهاتف. أسهل طريقة لضمان حصولك على التشفير من طرف إلى طرف للمحادثات الصوتية هي استخدام الصوت عبر بروتوكول الإنترنت (VoIP) بدلاً عن ذلك.

احذر! يقدم معظم موفري خدمات VoIP (بروتوكول نقل الصوت عبر الإنترنت) مثل سكايب، وقوقل أو قوقل مييت، تشفيراً للمحتوى كي لا يستطيع المتنصتون الاستماع إليها، ولكن مزودي الخدمة أنفسهم يبقون قادرين على الاستماع إليها. اعتماداً على نموذج التهديد الخاص بك، قد يكون ذلك مشكلة، أو قد لا يكون.

ذه بعض الخدمات التي تقدم مكالمات عبر بروتوكول الإنترنت ذات تشفير متبادل عبر الطرفين:

- **Wire** (43)
- **Silent phone** (44)
- **Signal** (45)

لإجراء محادثات (VoIP) ذات شيفرة متبادلة بين الطرفين يتوجب على طرفي المحادثة استخدام البرنامج نفسه أو برامج (متوافقة).

42 <https://support.skype.com/en/faq/fa10983/what-are-p2p-communications>

43 <https://wire.coma/en/>

44 <https://www.silentcircle.com/services#mobile>

45 <https://ssd.eff.org/en/module/how-use-signal-ioshttps://ssd.eff.org/en/module/how-use-signal-android>

الرسائل النصية والرسائل الفورية

لا توفر الرسائل النصية القصيرة العادية SMS التشفير من طرف إلى طرف. إذا كنت تريد إرسال رسائل مشفرة على هاتفك فكر باستخدام تطبيقات الرسائل الفورية المشفرة عوضاً عن الرسائل النصية القصيرة. حالياً الطريقة الوحيدة لإرسال رسائل SMS مشفرة هو استخدام تطبيق Silence⁽⁴⁶⁾ الخاص بأندرويد، والذي كان يحمل سابقاً اسم SMS Secure.

هناك خيارات أخرى لمراسلة آمنة عبر الإنترنت، على سبيل المثال، يمكن لمستخدمي⁽⁴⁷⁾ أندرويد وأي أو إس الدردشة بشكل آمن باستخدام سيغنال⁽⁴⁸⁾.

بروتوكول خارج السجل (OTR) هو تشفير متبادل من طرف إلى طرف يُستخدم للمحادثات النصية الفورية، ويمكن استخدامه مع مجموعة متنوعة من الخدمات.

بعض الأدوات التي تدمج OTR مع الرسائل الفورية تشمل:

- Pidgin⁽⁴⁹⁾ (لمستخدمي لينكس)
- Adium⁽⁵⁰⁾ (لمستخدمي أو أس أكس)
- ChatSecure⁽⁵¹⁾ (لمستخدمي أندرويد)
- Jitsi⁽⁵²⁾ (لمستخدمي ويندوز، لينكس، وأو أس أكس)
- Jitsi Meet⁽⁵³⁾ (لتأمين اجتماعات الفيديو عبر متصفح الويب الخاص بك)

البريد الإلكتروني

على سبيل المثال:

<https://mail.google.com/mail/u/0/#inbox>

يوفر معظم مزودي خدمات البريد الإلكتروني إمكانية الوصول إلى بريدك الإلكتروني عبر متصفح مثل فايرفوكس أو مايكروسوفت إيدج أو كروم. أغلب هؤلاء المزودين يدعمون بروتوكول HTTPS، أو التشفير أثناء النقل transport-layer encryption. يمكنك أن تتحقق عما إذا كان مزود خدمة بريدك الإلكتروني يدعم ميزة HTTPS إذا قمت بتسجيل الدخول باستخدام المتصفح وكان العنوان يبدأ بأحرف HTTPS بدلاً من HTTP

46 <https://silence.im>

47 <https://whispersystems.org/#privacy>

48 <https://ssd.eff.org/en/module/how-use-signal-ios><https://ssd.eff.org/en/module/how-use-signal-android>

49 <https://ssd.eff.org/en/module/how-use-otr-linux>

50 <https://ssd.eff.org/en/module/how-use-otr-mac>

51 <https://guardianproject.info/howto/chatsecurely>

52 <https://jitsi.org/>

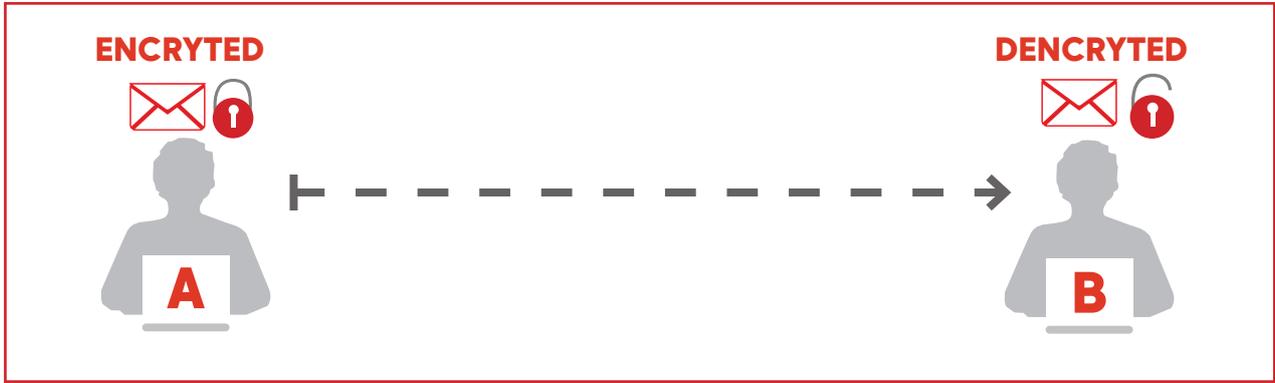
53

إن كان مزود البريد الإلكتروني الخاص بك يدعم HTTPS ، ولكن لا يفعل ذلك بشكل افتراضي، جرب استبدال HTTP في العنوان بـ HTTPS وقم بتحديث الصفحة. إذا كنت ترغب في التأكد من أنك تستخدم HTTPS دائماً على المواقع التي تدعمها، قم بتنزيل إضافة المتصفح (HTTPS Everywhere)⁽⁵⁴⁾ لفايرفوكس وكروم.

من خدمات البريد الإلكتروني التي تستخدم HTTPS بشكل افتراضي:

- Gmail
- Riseup
- Yahoo

تقوم بعض خدمات البريد الإلكتروني بتقديم خيار استخدام HTTPS بشكل افتراضي باختيار ذلك من ضمن الإعدادات، ومن أكثر الخدمات شيوعاً والتي لازالت تقوم بذلك نجد Hotmail.

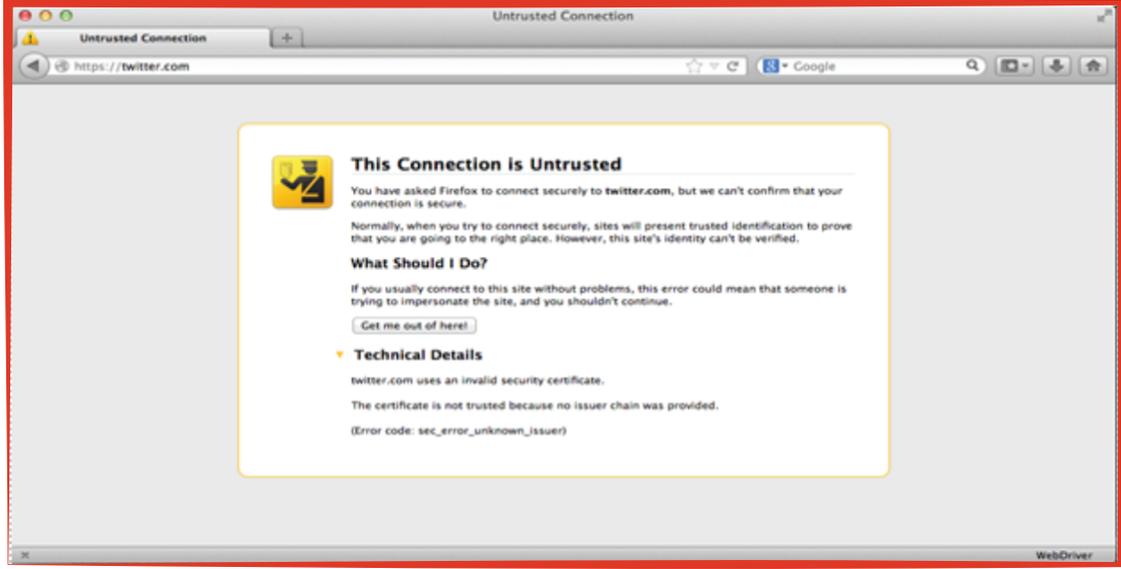


ماذا يفعل تشفير النقل ولماذا قد تحتاج إليه؟

يقوم HTTPS والذي يُشار إليه أيضاً باسم SSL أو TLS بتشفير اتصالاتك، بحيث لا يمكن قراءتها من قبل الأشخاص الآخرين على شبكتك. ويمكن أن يشمل ذلك أولئك الذين يستخدمون نفس شبكة الواي فاي في مطار أو مقهى، أو الآخرون في مقر عملك أو مدرستك، أو الموظفين في مزود خدمة الإنترنت الخاص بك، أو القرصنة (هاكرز)، أو الحكومات، أو مسؤولي الأمن. اعتراض وقراءة الاتصالات المرسله عبر متصفحك باستخدام HTTP بدلاً عن HTTPS أمر بغاية السهولة على المهاجمين، وذلك يتضمن الصفحات التي زرتها، ومحتويات رسائلك الإلكترونية، وتديوناتك، ورسائلك.

أضحت الجهات الفاعلة، حكومية وغير حكومية، بارعة على نحو متزايد في اختراق جلسات HTTPS بين الكمبيوتر والخادم. وهذه الطريقة، تتمكن من أن تقدم للمتصفح شهادة SSL وهمية من الخادم الذي تتعامل معه، وفي حال تجاهلت تحذيرات المتصفح فإن نشاطك بأكمله والمعلومات المتبادلة بين جهاز الكمبيوتر الخاص بك والخادم سوف تتعرض للاختراق. في مثل هذه الظروف، من المهم جداً عدم المضي قدماً في الاتصال ما لم تكن الشهادة المحلية موقعة ذاتياً. وعادة، يكون من المستحسن الانتظار لفترة من الوقت ومحاولة الوصول إلى الموقع مرة أخرى في وقت لاحق إذا تم تحذيرك مثلما هو مبين في الصورة أدناه.

54 https everywhere, <https://www.eff.org/https-everywhere>



إجراء متطور لتأمين البريد الإلكتروني PGP/GPG

لكن هناك بعض الأشياء التي لا يفعلها HTTPS. عند إرسال بريد إلكتروني باستخدام HTTPS، يظل مزود البريد الإلكتروني الخاص بك يحصل على نسخة غير مشفرة من اتصالاتك. قد تتمكن الحكومات وجهات إنفاذ القانون من الوصول إلى هذه البيانات بموجب أمر قضائي. في الولايات المتحدة يملك أغلب مزودي خدمة البريد الإلكتروني سياسة تقضي بإخبارك عندما يصلهم طلب حكومي للنظر في البيانات خاصتك، طالما كان مسموح لهم قانونيًا بذلك، ولكن هذه السياسات طوعية حصراً، وفي العديد من الحالات يحظر القانون على مقدمي الخدمة إعلام مستخدميهم بطلبات البيانات.

يقوم بعض مقدمي خدمة البريد الإلكتروني مثل جوجل⁽⁵⁵⁾ وياهو⁽⁵⁶⁾ ومايكروسوفت⁽⁵⁷⁾ بطرح تقارير شفافية تذكر فيها عدد الطلبات الحكومية لبيانات المستخدمين التي وصلتهم، والدول التي قامت بالطلب، وعدد المرات التي امتثلت فيها الشركة لطلبات تسليم بيانات المستخدمين.

إذا كان نموذج الخطر الخاص بك يتضمن الحكومة أو سلطات الأمن، أو إذا كانت لديك أسباب أخرى ترغب بسببها في التأكد من أن مقدم خدمة البريد الإلكتروني غير قادر على تسليم مراسلاتك عبر البريد الإلكتروني إلى طرف ثالث، عليك أن تأخذ في اعتبارك استخدام الشيفرة من طرف إلى طرف في مراسلاتك عبر البريد الإلكتروني.

إن PGP أو (Pretty Good Privacy) هو المعيار القياسي للتشفير المتبادل بين طرفين للبريد الإلكتروني. وهو يوفر حماية قوية جداً لمراسلاتك عند استخدامه بشكل صحيح. أحياناً يُطلق على PGP اسم (Gnu Privacy Guard) GPG.

55 <https://www.google.com/transparencyreport/>

56 <https://transparency.yahoo.com/>,

57 <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency>

عندما استخدام PGP يقوم كل طرف بخلق مفتاح يتكون من جزأين: جزء خاص وجزء عام. يمكنك حماية الجزء الخاص بشكل آمن على الأجهزة الخاصة بك، ولكنك تقوم بنشر الجزء العام إلى كل شخص ترغب في التواصل معه باستخدام PGP. للمساعدة في توضيح مفاهيم PGP، قامت منظمة التجمّع التكنولوجي التكتيكي بنشر سلسلة أشرطة الفيديو أطلقت عليها اسم "فك تشفير التشفير"⁽⁵⁸⁾.

لإرشادات مفصلة حول كيفية تثبيت واستخدام PGP/GPG لتشفير بريدك الإلكتروني راجع هذه الإرشادات بخصوص أنظمة الماك أو أس أكس والويندوز⁽⁵⁹⁾، واللينكس⁽⁶⁰⁾.

لاستخدام PGP/GPG⁽⁶¹⁾ في متصفح الويب الخاص بك باستخدام البريد الإلكتروني، انظر في استخدام برنامج مايلفيلوب المساعد للمتصفح أو احترس من عملاء بريد الويب المتخصصة تمامًا مثل بروتونمايل⁽⁶²⁾.

تأكد من تمكين التشفير على برنامج البريد الإلكتروني الخاص بك قبل إرسال معلومات أو مرفقات حساسة. للقيام بذلك، اتبع كيفية تمكين تشفير PGP على عملاء البريد الإلكتروني الخاص بك من الرابط: <https://ssd.eff.org/en/egories/tool-guidesmodule-cat>

أوجه قصور التشفير من طرف إلى طرف

تحمي الشيفرة المتبادلة بين طرفين محتويات مراسلاتك فقط، وليس حقيقة أن هناك اتصال قد حدث بالفعل. كما أنها لا تحمي بياناتك الوصفية Metadata، والتي تشكل كل شيء آخر، بما في ذلك موضوع (عنوان) الرسالة، ولمن ترسلها، ومتى تم إرسالها.

توفر البيانات الوصفية معلومات شديدة الخصوصية تخصك، حتى عندما تبقى محتويات اتصالاتك سرية.

تكشف البيانات الوصفية لمكالماتك الهاتفية معلومات حميمة وحساسة جداً. على سبيل المثال:

- يعلمون أنك اتصلت بخط خدمة استشارة عن الاكتئاب عند 2:24 صباحًا وتكلمت لمدة 18 دقيقة، ولكنهم لا يعلمون عمًا تحدثت.
- يعلمون أنك تكلمت مع خدمة لفحص HIV (فيروس نقص المناعة المكتسبة)، ثم مع طبيبك، ثم مع شركة التأمين الصحي في نفس الساعة، لكنهم لا يعلمون ما تمت مناقشته.
- يعلمون أنك تلقيت اتصالاً من مكتب مقر المعارضة المحلية خلال قيامها بحملة ضد التشريعات الإعلامية، ثم اتصلت برئيسك مباشرة بعد ذلك، ولكن مضمون تلك المكالمات لا يزال آمنًا من تدخل الحكومة.
- يعلمون أنك اتصلت بطبيب نسائي وتحدثت لمدة نصف ساعة، ومن ثم اتصلت بجمعية تنظيم الأسرة في منطقتك في وقت لاحق من ذلك اليوم، ولكن لا أحد يعلم عما دارت المكالمة.

58 <https://tacticaltech.org/projects/decrypting-encryption>

59 <https://ssd.eff.org/en/module/how-use-pgp-mac-os-x>

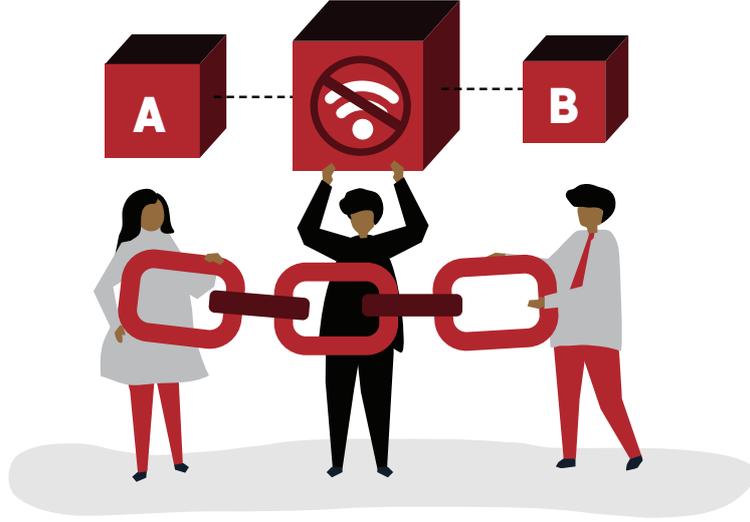
60 <https://ssd.eff.org/en/module/how-use-pgp-linux>

61 <https://www.mailvelope.com/>

62 <https://protonmail.com/>

إذا كنت تتصل من هاتف محمول، فالمعلومات حول موقعك هي بيانات وصفية. في عام 2009، رفع مالت سبيتز - وهو سياسي ينتمي لحزب الخضر - دعوى ضد شركة دويتشه تيليكونم لإجبارها على تسليمه تفاصيل ستة أشهر من بيانات هاتفه، التي قدمها بعد ذلك لصحيفة ألمانية. وقد أظهر التصور البياني⁽⁶³⁾ الذي أنتجوه تاريخاً مفصلاً لتحركات سبيتز. قدم سبيتز محاضرة مُلهمة ضمن محاضرات TED⁽⁶⁴⁾ شرح فيها تفاصيل هذه الحادثة.

كيف تتجنب الرقابة على الإنترنت



تستخدم الكثير من الحكومات، والشركات، والمدارس، والشبكات العامة لمنع مستخدمي الإنترنت من الوصول إلى مواقع وخدمات معينة على شبكة الإنترنت. ويُطلق على هذه العملية فلتر أو حجب الإنترنت، وهو شكل من أشكال الرقابة. تظهر فلتر المحتوى على الإنترنت بأشكال متعددة. في بعض الأحيان تُحجب مواقع بأكملها، وأحياناً صفحات محددة؛ وأحياناً يُحظر المحتوى اعتماداً على الكلمات الأساسية الواردة فيه. قد تقوم دولة بحظر موقع الفيسبوك كلياً، أو قد تحجب صفحات لمجموعات معينة على الموقع؛ أو تحجب أي صفحة ونتيجة بحث تحوي كلمة "مثلية" مثلاً.

بغض النظر عن كيفية فلتر أو حجب المحتوى، يمكنك الحصول على المعلومات التي تحتاجها باستخدام أداة لتجنب الرقابة. تعمل أدوات تجنب الرقابة عادة بواسطة تحويل حركة مرور بياناتك عبر كمبيوتر آخر، بحيث تتجنب الأجهزة التي تقوم بالرقابة. تُسمى الخدمة الوسيطة التي تمرّ اتصالاتك عبرها في هذه العملية بالوكيل "proxy".

لا توفر أدوات تجنب الرقابة بالضرورة أمناً إضافياً، كما لا تقوم بإخفاء هويتك، بما في ذلك الأدوات التي تعد بالخصوصية أو الأمن، أو حتى تلك التي تحوي في اسمها مصطلحات مثل anonymizer (إخفاء الهوية).

هناك طرق مختلفة لتجنب الرقابة على الإنترنت، ويوفر بعضها درجة أمان إضافية. ويعتمد اختيار الأداة المناسبة لك على نموذج التهديد الخاص بك.

63 <http://www.zeit.de/datenschutz/malte-spitz-data-retention>,

64 http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching?language=en,

تقنيات أساسية

HTTPS هو الإصدار الآمن من بروتوكول HTTP المُستخدم للوصول إلى مواقع الويب. ففي بعض الأحيان، يحجب الرقيب نسخة HTTP فقط من الموقع، مما يتيح لك الوصول إلى الموقع بإدخال العنوان مع البدء بـHTTPS. ويكون هذا شديد الفائدة خاصة في حال كانت الفلترية التي تعاني منها تعتمد على الكلمات الرئيسية أو تحجب صفحات معينة فقط، حيث يقوم HTTPS بوقف قراءة الرقيب لمُرور بياناتك على الإنترنت، ولن يتمكن من معرفة الكلمات المفتاحية التي يجري إرسالها، أو الصفحات الفردية التي تزورها (ولكن بإمكانهم رؤية أسماء نطاقات (عناوين) جميع المواقع التي تزورها).

إذا كنت تعتقد أنه يتم استخدام هذا النوع البسيط من الحجب، جرب إدخال <https://> قبل عنوان الموقع عوضاً عن <http://>.

جرب إضافة HTTPS Everywhere⁽⁶⁵⁾ للمتصفح لتفعيل HTTPS تلقائيًا على جميع المواقع التي تدعمه.

طريقة أخرى لتجنب تقنيات الرقابة البسيطة هي تجريب تنويعات أخرى لعنوان الموقع. مثلاً، بدل زيارة <http://twitter.com>⁽⁶⁶⁾، جرب زيارة <https://mobile.twitter.com>⁽⁶⁷⁾، وهي نسخة الهاتف المحمول من الموقع. لأن الرقباء الذين يحجبون المواقع أو صفحات معينة يعتمدون في العادة على قائمة محددة لمنع المواقع المحظورة. ولذلك أي شيء غير موجود على تلك القائمة لن يتم حجبه. فربما لا يعرفون جميع التنويعات على اسم نطاق (عنوان) موقع معين، وخصوصًا إذا كان الموقع يعرف أنه محجوب وقام بتسجيل أكثر من اسم نطاق واحد.

الوكلاء القائمون على الإنترنت

الوكيل القائم على الإنترنت <http://proxy.org>⁽⁶⁸⁾ هو وسيلة بسيطة لتجنب الرقابة. كي تستخدم وكيلاً على الإنترنت، كل ما عليك القيام به هو إدخال العنوان المحجوب الذي ترغب باستخدامه، وسيقوم الوكيل بعرض المحتوى المطلوب.

يُعتبر استخدام الوكلاء على الإنترنت طريقة جيدة للوصول إلى المواقع المحجوبة بسرعة، ولكنها لا توفر في الغالب أي أمان، كما أنها خيار سيئ في حال كان نموذج التهديد الخاص بك يتضمن جهة ما تراقب اتصالاتك بالإنترنت. إضافة إلى ذلك، فهي لن تفيدك في استخدام الخدمات الأخرى التي لا تعتمد على صفحات مواقع الإنترنت، مثل برامج الدردشة والتراسل المباشر.

وفي نهاية الأمر، يشكّل الوكلاء أنفسهم تهديدًا لخصوصية المستخدمين بحسب نموذج الخطر الخاص بهم، حيث أن الوكيل يملك سجلًا كاملاً بكل ما تقوم به على الإنترنت.

65 <https://www.eff.org/https-everywhere>

66 <https://twitter.com/>

67 <https://mobile.twitter.com/home>,

68 <http://proxy.org>

إعدادات نظام أسماء النطاقات (DNS)

غالبًا ما تفرض الحكومات الرقابة في بلدانها من خلال توجيه تعليمات لمزودي خدمة الإنترنت بسنّ قوائم سوداء باستخدام شيء يسمى خدمة اسم النطاق (DNS). تعد خوادم نظام أسماء النطاقات جزءًا من البنية الأساسية التي تساعد متصفحك على تحديد الموقع الفعلي لعناوين الويب الذي تعرفه. على سبيل المثال، عند الكتابة في www.bbc.co.uk، فإن السيرفر في DNS هو ما يخطر المتصفح الخاص بك أن بي بي سي تقع ضمن سيرفر على العنوان IP 212.58.244.20. ومن خلال التلاعب بخوادم DNS، يمكن أن ينخدع الكمبيوتر الخاص بك ويظن أن الموقع على شبكة الإنترنت، مثل بي بي سي، غير موجود، أو موجود في مكان وهمي.

للتحايل على هذا النوع من أنواع الحجب يمكنك ببساطة تغيير خوادم DNS الافتراضية المستخدمة من قبل جهاز الكمبيوتر الخاص بك. تقدم جوجل خادومين للجمهور⁽⁶⁹⁾ في 8.8.8.8، و 8.8.4.4. كما تقدم OpenDNS⁽⁷⁰⁾ خوادم عامة في 208.67.222.222، و 208.67.220.220، والتي بالإضافة إلى ذلك تعيق مواقع البرامج الخبيثة والتصيد الاحتيالي المعروفة.

هذه على المكتب أو جهاز الراوتر بحيث يمكن لجميع المستخدمين الاستفادة منه. DNS كما بإمكانك ضبط إعدادات يمكنك العثور على إرشادات حول كيفية تغيير إعدادات نظام أسماء النطاقات على أنظمة التشغيل والموجهات المختلفة على <https://use.opendns.com>⁽⁷¹⁾.

الشبكات الخاصة الافتراضية VPN

تقوم VPN (الشبكة الافتراضية الخاصة) بتشفير وتمرير اتصالاتك بالإنترنت بينك وبين كمبيوتر آخر. بعد ضبط إعدادات خدمة VPN بشكل صحيح، يمكنك استخدامها للوصول إلى صفحات الإنترنت، والبريد الإلكتروني، والتراسل المباشر، والمكالمات الصوتية عبر بروتوكول الإنترنت VoIP، وأي خدمة إنترنت أخرى. تقوم الشبكة الافتراضية الخاصة بحماية حركة بياناتك من اعتراضها محليًا، ولكن قد يحتفظ مزود خدمة VPN بسجلات حركة المرور خاصتك (أي المواقع التي تزورها، ومتى زرتها آخر مرة) أو حتى تمكين طرف ثالث من التجسس مباشرة على تصفحك للإنترنت.

بعض شبكات VPN المجانية التي يجب وضعها في الاعتبار هي [Betternet](https://www.betternet.com/)⁽⁷²⁾، [Psiphon](https://www.psiphon3.com/)⁽⁷³⁾، [BitMask](https://bitmask.net)⁽⁷⁴⁾، و [Opera](https://www.opera.com/apps/vpn)⁽⁷⁵⁾.

للحصول على بعض التوصيات حول خدمات VPN المدفوعة، راجع هذا الرابط⁽⁷⁶⁾. يمكن لبعض شبكات VPN التي تضع سياسات خصوصية مثالية أن تُدار من قبل أناس مخادعين.

69 <https://developers.google.com/speed/public-dns/?hl=en>

70 <https://use.opendns.com>

71 <https://use.opendns.com>

72 <https://www.betternet.com>

73 <https://www.psiphon3.com/>

74 <https://bitmask.net>

75 <https://www.opera.com/apps/vpn>

76 <https://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/>

تور Tor

تور هو برنامج مجاني ومفتوح المصدر لإخفاء هويتك، كما أنه يسمح لك بتجاوز الرقابة. عندما تستخدم تور، فإن المعلومات التي ترسلها تكون أكثر أماناً لأنه يتم توجيه حركة مرورها عبر شبكة موزعة من الخوادم، وتدعى التوجيه متعدد الطبقات (onion routers)، الذي يستطيع إخفاء هويتك بما أن الكمبيوتر الذي تتواصل معه لن يرى عنوان IP الخاص بك، بل سيرى عنوان IP الخاص بجهاز توجيه Tor الأخير الذي تنتقل من خلاله حركة المرور الخاصة بك.

عند استخدامه مع بعض الميزات الاختيارية (bridges and obfsproxy)، فإن تور هو المعيار الذهبي لتجنب رقابة الدولة التي تتواجد بها بأمان، بما أنه سيتجاوز أغلب الرقابة الوطنية، وفي حال تم ضبطه بشكل صحيح، سيحمي هويتك من أي خصم يتنصت على الشبكات في بلدك. لكنه يمكن أن يكون بطيئاً وصعب الاستخدام.

تعرف على كيفية استخدام Tor باستخدام هذا الدليل⁽⁷⁷⁾ من وثائق مشروع Tor .

77 <https://2019.www.torproject.org/docs/documentation.html.en>

أمن الحساب الإلكتروني

تلقت سيسيكو، المديرية التنفيذية لمنظمة الأقليات الجنسية، في وقت مبكر من صباح أحد الأيام، رسالة بريد إلكتروني على هاتفها تخبرها أن بريدها الإلكتروني سينتهي خلال أربع ساعات. وفي نهاية تلك الرسالة الإلكترونية، كان هناك رابط يعرض عليها تسجيل الدخول إلى بريدها الإلكتروني لمنع إغلاقه. وبدون الكثير من التفكير، نفذت الاقتراحات وفتحت الرابط الذي أوصلها إلى صفحة تسجيل الدخول التي تبدو تمامًا مثل صفحة تسجيل الدخول إلى جيميل. وسرعان ما أدخلت اسم المستخدم وكلمة المرور الخاصة بها، ولكن عند الإرسال، لم يحدث شيء حقًا. عادت وواصلت قراءة رسائل البريد الإلكتروني الأخرى الخاصة بها.

تلقت، في وقت لاحق من ذلك اليوم، تقارير تفيد بأن الموقع الإلكتروني للمنظمة قد تم اختراقه وتشويهه ولم يعد من الممكن الوصول إليه. وذلك عندما أبلغها رئيس قسم تكنولوجيا المعلومات والاتصالات بالمنظمة أنه تلقى بريدًا إلكترونيًا منها يطلب الوصول المؤقت إلى الواجهة الخلفية للموقع في وقت مبكر من ذلك الصباح.

ما شهدته سيسيكو في ذلك الصباح كان عبارة عن هجوم تصيد مستهدف لسرقة كلمة المرور. بمجرد حصول المهاجمين على حساب بريدها الإلكتروني، تمكنوا بسهولة اختراق كل جزء من المنظمة.

هناك حل بسيط جدًا ولكنه قوي يمكن لسييسيكو استخدامه لتجنب حدوث هذا النوع من الهجمات مرة أخرى. يطلق عليه المصادقة الثنائية. ومن المفيد أيضًا أن يكون لديك كلمات مرور قوية ومختلفة لكل حساب عبر الإنترنت.

إنشاء كلمات مرور قوية

نظرًا لصعوبة تذكُّر كلمات المرور العديدة والمختلفة، يجد الناس من الصعب العمل بفعالية وكفاءة مع كلمات المرور. اليوم ومع استمرار مطالبة المستخدمين بوضع كلمات جديدة لكل شيء يرغبون بفعله، فإن هناك إغراء بإعادة استخدام نفس كلمة المرور مع حسابات وخدمات ومواقع متعددة.

إن إعادة استخدام كلمات المرور ممارسة أمنية سيئة للغاية، لأنها تؤدي إلى اختراق جميع الحسابات التي تستخدم نفس كلمة المرور. مما يعني أن كلمة المرور تكون آمنة فقط بقدر أمان الخدمة المستخدمة فيها.

إن تجنُّب إعادة استخدام كلمة المرور هو إجراء أمني احترازي وذو قيمة. ولكنك لن تكون قادرًا على تذكُّر جميع كلمات المرور الخاصة بك في حال كانت كل واحدة مختلفة عن أخرياتها. لحسن الحظ توجد أدوات برمجية تُساعدك على فعل ذلك- مدير كلمات المرور (ويسمى أيضا خزانة كلمة المرور) وهي عبارة عن برنامج للمساعدة في تخزين عدد كبير من كلمات المرور بشكل آمن. وهذا يجعل من تجنُّب إعادة استخدام كلمة المرور في سياقات متعددة أمرًا عملي. تعمل أدوات إدارة كلمة المرور على حماية كل كلمات المرور الخاصة بك بواسطة استخدام كلمة مرور رئيسية (أو عبارة مروية- أنظر الشرح أدناه). ولذلك عليك تذكُّر شيء واحد فقط. وبالتالي، يمكن لإدارة كلمة المرور التعامل مع العملية برمتها من إنشاء وتذكُّر جميع كلمات مرور المستخدم.

على سبيل المثال، تُعتبر KeePassX برمجية خزانة لكلمات المرور، وهي برمجية مفتوحة المصدر ومجانية، تقوم فقط بتثبيتها على سطح المكتب. إذا كنت تستخدم هذا البرنامج، فمن المهم ملاحظة أنه لن يقوم تلقائيًا بحفظ التغييرات والإضافات. وهذا يعني أنه في حال تعطل البرنامج بعد أن أضفت له كلمات المرور، قد تفقدهم إلى الأبد. لكن يمكنك تغيير هذا في إعدادات البرنامج.

يساعدك استخدام مدير كلمات المرور أيضًا على اختيار كلمات مرور قوية يصعب على المهاجم تخمينها. وهذا أمر هام، لأن مستخدمو الكمبيوتر يقومون في الغالب باختيار كلمات مرور بسيطة وقصيرة يستطيع المهاجم تخمينها بسهولة مثل "password"، أو "12345"، أو تاريخ الميلاد، أو أسم صديق، أو الزوج، أو الزوجة، أو حيوان أليف. بإمكان مدير كلمات المرور المساعدة في توليد واستخدام كلمة مرور عشوائية بدون نمط أو هيكل مشترك، أي كلمة مرور غير قابلة للتخمين. على سبيل المثال، بمقدور مدير كلمات المرور اختيار كلمة مرور مثل "vAeJZ!Q3p\$Kdkz/CRHzj0v7"، والتي من غير المرجح على إنسان تذكرها أو تخمينها. لا تقلق، مدير كلمات المرور يستطيع تذكرها من أجلك.

اختيار كلمات مرور قوية

يوجد بعض كلمات المرور التي يتوجب تذكرها، والتي يجب أن تكون قوية بشكل خاص: وهي تلك التي تستخدمها في قفل بياناتك باستخدام التشفير. وتتضمن، على الأقل، كلمة المرور الخاصة بالتشفير الكاملة لجهازك، وكلمة المرور الرئيسية لبرنامج إدارة كلمات المرور.

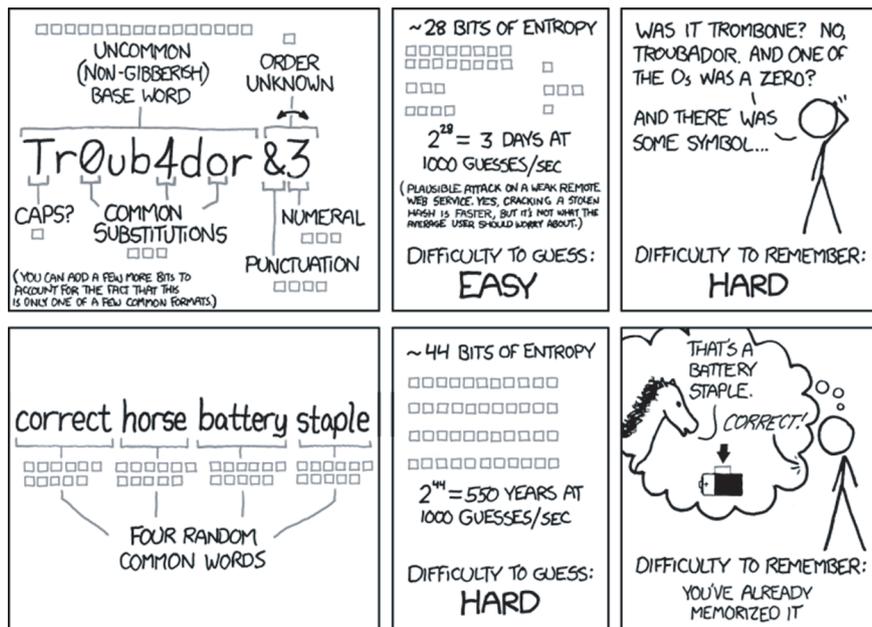
اليوم أصبحت أجهزة الكمبيوتر سريعة، بحيث يمكنها بسرعة تخمين كلمة مرور أقصر من 10 أحرف. وهذا يعني أن كلمات المرور القصيرة مهما كان نوعها- حتى العشوائية منها على شاكلة $nQ \setminus m=8^*x$ ، ليست قوية كفاية حاليًا للاستخدام مع التشفير.

هناك طرق عديدة لإنشاء وتذكر عبارة مرور، أكثرها وضوحًا ونجاحًا هي طريقة أرنولد رينهولد المسماة دايسوير⁽⁷⁸⁾.

تنطوي طريقة رينهولد على رمي زهر النرد للقيام باختيار عشوائي لعدة كلمات من قائمة تحتوي على كلمات كثيرة، وستقوم هذه الكلمات معًا بتشكيل عبارة المرور. ننصح في حالات تشفير القرص (وكلمة المرور الرئيسية) باختيار ست كلمات على الأقل.

تتضمن النسخة المبسطة من دايسوير على أن تقوم بنفسك بتنظيم مجموعة متنوعة من الكلمات العشوائية.

انظر لهذا الرسم الفكاهي الذي يوضح كيف أن هذا الأسلوب هو أسهل للاستخدام وأكثر أمنًا من استعمال كلمات المرور المعقدة مثل: $nQ \setminus m=8^*x'$.



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

المصدر⁽⁷⁹⁾ XKCD

عند استخدامك لمدير كلمات المرور، فإن درجة أمان كلمات المرور وكلمة المرور الرئيسية هي بنفس درجة أمان الكمبيوتر الذي قمت فيه بتثبيت واستخدام مدير كلمة المرور. فإذا تم اختراق الكمبيوتر أو الجهاز وتثبيت برمجية تجسس، تستطيع برمجية التجسس مراقبتك في أثناء كتابة كلمة المرور الرئيسية الخاصة بك، وبالتالي سرقة محتويات كلمة المرور الأساسية. لذا، من المهم جدًا أن يكون حاسوبك وباقي الأجهزة نظيفة من البرمجيات الخبيثة أثناء استخدام مدير كلمات المرور.

78 <http://world.std.com/~reinhold/diceware.html>

79 <https://xkcd.com/936/>

المصادقة متعددة العوامل وكلمات مرور المرة الواحدة

تتيح لك العديد من الخدمات والبرمجيات استخدام خاصية الاستيثاق الثنائي، وتُسمى أيضًا التحقق المزدوج أو تسجيل الدخول بخطوتين. الفكرة الأساسية هي أنه من أجل تسجيل الدخول، تحتاج حيازة شيء مادي معين: يكون عادة الهاتف المحمول، ولكن في بعض الإصدارات، يكون عبارة عن جهاز خاص يسمى رمز الأمان. يضمن لك استخدام هذا النظام أنه حتى إذا تمّ اختراق أو سرقة كلمة المرور الخاصة بهذه الخدمة، لن يكون بمقدور اللصّ تسجيل الدخول إلا إذا كان يملك أو يسيطر على الجهاز الثاني والرموز الخاصة التي يتحكم هو فقط في توليدها.

وهذا يعني أن على السارق أو المُخترق التحكُّم في كلِّ من اللابتوب وهاتفك المحمول قبل تمكُّنهم من النفاذ الكامل إلى حساباتك.

لا يمكنك القيام بتفعيل خاصية التحقق المزدوج في إحدى الخدمات ما لم تكن الخدمة نفسها توفرها، حيث أن هذه الخاصية يمكنها العمل فقط بالتعاون مع مقدمي الخدمات.

يمكن لعملية التحقق بخطوتين عبر الهاتف المحمول أن تتمّ من خلال طريقتين: إما أن تقوم الخدمة بإرسال رسالة نصيّة قصيرة إلى هاتفك كلما حاولت الولوج (موفرة أمان إضافي برمز تحتاج إلى إدخاله)، أو يمكنك تشغيل تطبيق تحقُّق يقوم بتوليد الرموز السريّة من خلال الهاتف نفسه. وهذا يساعدك في حماية حسابك في المواقف التي يعلم فيها المهاجم كلمة المرور الخاصة بك دون أن يتمكن من النفاذ إلى هاتفك المحمول نفسه.

حاليًا تقدم العديد من الخدمات عبر الإنترنت خاصية الاستيثاق الثنائي. وتتوفر قائمة مُحدثة بهذه الخدمات على <https://www.turnon2fa.com>. يمكنك البدء باستخدام حسابات جوجل⁽⁸⁰⁾، ياهو⁽⁸¹⁾، فيسبوك⁽⁸²⁾، وتويتر⁽⁸³⁾.

تسمح لك بعض الخدمات، مثل جوجل، بإنشاء قائمة من كلمات مرور تُستخدم مرة واحدة، وذلك بغرض طباعتها أو كتابتها على ورقة تحملها معك (على الرغم من إمكانية تذكر عدد منهم في بعض الحالات). تعمل كل كلمة مرور في القائمة لمرة واحدة فقط، فلو تمّت سرقة كلمة مرور واحدة من خلال برمجة خبيثة أثناء طباعتها فلن يستطيع السارق استخدامها لأي غرض في المستقبل.

80 <https://www.google.com/landing/2step/>

81 <https://login.yahoo.com/account>

82 <https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920>

83 <https://blog.twitter.com/2013/getting-started-with-login-verification>

● التهديد بالإيذاء الجسدي أو الحبس

في الختام، أفهم أنه توجد دائماً طريقة واحدة يمكن للمهاجمين من خلالها الحصول على كلمات المرور خاصتك: يمكنهم تهديدك مباشرة بالإيذاء الجسدي أو الاحتجاز. إذا كنت تخشى هذه الاحتمالية، يمكنك الأخذ في الاعتبار طُرُق إخفاء وجود البيانات أو الجهاز المحمي باستخدام كلمة مرور بدلاً من الوثوق في عدم إفصاحك عن كلمة المرور. إحدى تلك الطرق هي إنشاء حساب، واحد على الأقل، يحتوى على عدد ضخم من المعلومات غير الهامة، حيث يمكنك الكشف عن كلمة المرور الخاصة بذلك الحساب سريعاً.

إذا وجد سبب وجيه يجعلك تعتقد أن شخص ما قد يهددك من أجل الحصول على كلمات المرور، قد يكون من الجيد مراجعة إعدادات الأجهزة الخاصة بك للتأكد من عدم بيان أن الحساب الذي تفصح عنه ليس هو الحساب الحقيقي. هل الحساب الحقيقي ظاهر على صفحة تسجيل الدخول لحاسوبك؟ أو يظهر تلقائياً عند فتح متصفح؟ إذا كان الأمر كذلك قد تحتاج إلى إعادة ضبط الإعدادات لجعل حسابك الحقيقي أقل وضوحاً.

يُرجى ملاحظة أن التدمير المُتعمد للأدلة أو عرقلة سير التحقيق قد يتسببان في اتهامات منفصلة، وعادةً ما تكون ذات تبعات خطيرة. وفي بعض الحالات قد يسهل على الحكومة الإثبات والمطالبة بعقوبات أكبر من الجريمة المزعومة قيد التحقيق.

تأمين الهواتف النقالة

فايد ناشط يعمل في مجالات الشفافية، والمساءلة، وحرية التعبير. لديه العديد من الأصدقاء الذين هربوا من بلده بسبب قمع الحكومة. يتحدث فايد بانتظام مع أصدقاءه النشطاء في الشتات، سواء عبر المكالمات الهاتفية أو الرسائل النصية القصيرة، بغرض تحديث معلوماتهم حول الوضع في البلاد، ومشاركتهم القصص التي لا يستطيع مشاركتها داخل البلاد.

وفي صبيحة أحد الأيام، اعتقلته الشرطة من منزله وأخذته إلى المحكمة متهمة إياه بالتخطيط للإطاحة بالحكومة والتواصل مع الإرهابيين. في المحكمة قدم الادعاء أدلة تحتوي على تسجيلات لمكالماته الصوتية المنتظمة مع أصدقائه في الشتات والرسائل النصية التي كتبها يحدتهم فيها عن مدى سوء الحكومة.

كان على فايد معرفة أنه لا يمكن استخدام المكالمات الصوتية والرسائل القصيرة العادية لتوصيل المعلومات الحساسة لأنه يسهل تسجيلها بواسطة شركات الهاتف. كما كان يجب على فايد أن يعلم عن هذه الثغرات الأمنية، وعن تطبيقات الهواتف المحمولة التي يمكن استخدامها لتشفير المكالمات الصوتية والرسائل النصية.

مشكلة الهواتف النقالة

شاع استخدام الهواتف النقالة بين الناس، وصار امتلاكها أمرًا أساسيًا كونها وسيلة اتصالات هامة. ولكن، لم يعد استخدامها يقتصر حاليًا على إجراء المكالمات فقط، وإنما للدخول على شبكات الإنترنت، وإرسال الرسائل النصية القصيرة؛ هذا إلى جانب استخدامها لتسجيل الأحداث المهمة التي تدور من حولك.

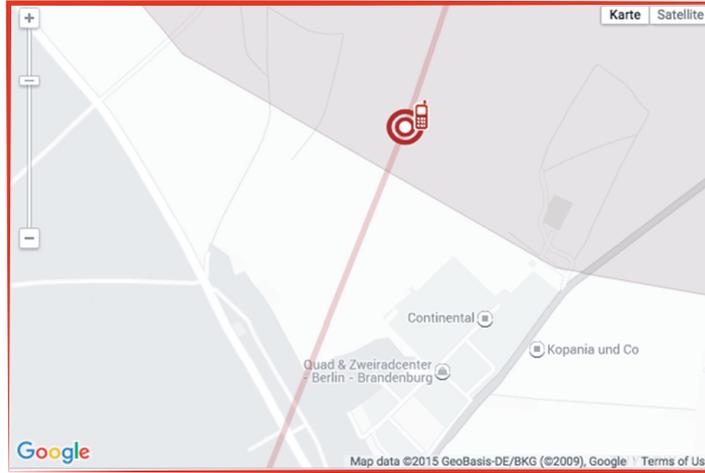
لسوء الحظ فإنّ الهواتف المحمولة لم تُصمم لحماية خصوصية وأمن مستخدميها. وهذا لا يقتصر فقط على عدم تأمين حماية اتصالاتك فقط، وإنما تجعلك أيضًا عرضة لأنواع جديدة من مخاطر المراقبة. معظم الهواتف النقالة لا تعطي المستخدم حرية السيطرة على الجهاز مثلما تفعل أجهزة الكمبيوتر واللابتوب؛ فمن الصعب جدًا استبدال نظام التشغيل، ومن الصعب جدًا التحقق من هجمات الفيروسات؛ كما يصعب جدًا إلغاء أو استبدال أيّ حزمة من الأنظمة التي لا تريدها؛ أو منع أطراف آخرين مثل مشغل نظام الهاتف من مراقبة استخدامك للجهاز.

بعض هذه المشاكل بالإمكان حلها عن طريق استخدام برنامج خصوصية كطرف ثالث؛ والبعض الآخر لا يمكن حلها بتلك الطريقة. سنقوم هنا باستعراض بعض الطرق التي تستخدم في الهواتف المحمولة والتي من شأنها إضعاف حماية خصوصية المستخدم وجعله أكثر عرضة للمراقبة.

تتبع موقع المستخدم

وهي الطريقة الأكثر تهديدًا لخصوصية المستخدم، ومع هذا قد تكون غير مرئية بشكل كامل. فهم باستطاعتهم تحديد مكانك في أيّ وقت خلال اليوم (وطوال الليل) من خلال الإشارات التي يبثونها ويستقبلها جهازك. هنالك طرق عديدة بالإمكان استخدامها لتحديد مكان هاتف المستخدم بواسطة أشخاص آخرين.

تتبع إشارة الهاتف



يمكن لمشغل الشبكة القيام بذلك من خلال مراقبة قوة الإشارة التي تلاحظها الأبراج المختلفة من الهاتف المحمول الخاص بمشترك معين، ثم حساب المكان الذي يجب أن يوجد فيه هذا الهاتف من أجل أخذ هذه الملاحظات في الاعتبار. لا توجد طريقة للاختباء من هذا النوع من التتبع إذا كان هاتفك المحمول قيد التشغيل ويرسل الإشارات إلى شبكة المشغل. وتحدد العلاقة غير المتكافئة بين الحكومة ومشغلي الاتصالات أن بمقدور الحكومة إجبار المشغل على تسليم بيانات موقع المستخدم (سواء في اللحظة الحاضرة أو السجل التاريخي لموقعه في الماضي). في عام 2010، قام أحد الناشطين في مجال حماية خصوصية الفرد يدعى مالت سبيتز، وهو ألماني الجنسية، بالحصول على سجل هاتفه النقال من مشغل الخدمة

المشترك بها مستخدمًا قوانين الخصوصية في بلاده؛ ثم بعد ذلك قام بنشرها على الملأ لتوعية الناس حول القدرات التي يمكن لمشغل الخدمة الهاتفية استخدامها في مراقبة المشتركين. (يمكنك زيارة هذا الرابط⁽⁸⁴⁾ لمعرفة ما يعرفه المشغل عنه). احتمالية إطلاع الحكومات على ذلك النوع من المعلومات ليست مجرد نظريات، وإنما هذا هو ما يحدث وعلى نطاق واسع من قبل الأجهزة الأمنية في جميع أنحاء العالم.

تظهر البيانات التي حصل عليها مالتي سبيتز من شركة الهاتف الخاصة به، تحركاته، وبيانات مكالماته الهاتفية. يمكنك استعراض ستة أشهر من هذه البيانات في Zeit Online⁽⁸⁵⁾.

وهناك نوع آخر من المعلومات تستطيع الحكومة الحصول عليه من مُشغّل الخدمة يُسمى بتحميل كافة معلومات البرج Dump Tower؛ حيث تطلب الحكومة من مُشغّل الخدمة الهاتفية تزويدها بقائمة لجميع مشركيه الذين كانوا يتواجدون في منطقة ما وفي وقت معين. يمكن استخدام ذلك النوع من المعلومات في التحقيق بجريمة ما، أو لمعرفة المتواجدين في مظاهرة احتجاجية ما. (تشير المعلومات إلى أنّ الحكومة الأوكرانية قد استخدمت تلك الطريقة للحصول على معلومات عن جميع المشاركين في مظاهرة ضدها عام 2014).

أيضًا هناك أجهزة تستخدمها أليات إنفاذ القانون أو غيرها من المنظمات المتطورة تقنيًا، يكون بإمكانها تحديد موقع وهو عبارة عن برج وهمي، يبدو وكأنه (IMSI Catcher) مستخدم الهاتف، وتُسمى مصيدة مُشركي الخدمات الهاتفية حقيقي، الغرض منه "اصطياد" هواتف مشتركين بالاسم، وتحديد أماكن تواجدهم، أو التجسس على اتصالاتهم.

مصيدة مشركي الخدمات الهاتفية هي عبارة عن جهاز، لذلك تحتاج إلى نقلها لمكان معين للبحث عن الهواتف ومشركيها الذين تحاول مراقبتهم في ذلك المكان. فلا يوجد حاليًا دفاع موثوق ضد جميع أدوات التقاط IMSI على الرغم من أن بعض التطبيقات تكتشف وجودها في بعض الحالات. وفي بعض الحالات، يمكن أن يحمي تعطيل اتصالات 2G والتجوال، من الاتصال بأجهزة IMSI Catchers.

تسرّب معلومات الموقع من التطبيقات وتصفح الإنترنت

تُوفّر الهواتف الذكية الحديثة خيارًا للهاتف من أجل تحديد موقعه الخاص، في كثير من الأحيان يحدث هذا باستخدام نظام تحديد المواقع GPS، وأحيانًا باستخدام خدمات أخرى توفرها شركات الموقع (والتي عادة ما تطلب من الشركة تخمين موقع الهاتف على أساس قائمة من أبراج الهاتف الخليوي و/أو شبكات الواي فاي أن الهاتف يمكن أن يُرى من حيث موقعه). من الممكن أن تطلب بعض التطبيقات من الهاتف معلومات الموقع هذه، وتستخدمها في توفير الخدمات استنادًا على موقعه، مثل الخرائط التي تظهر لك موقعك على الخريطة.

84 <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>

85 <http://www.zeit.de/datenschutz/malte-spitz-data-retention>

وقد تنقل بعض هذه التطبيقات بعد ذلك المعلومات عن موقعك عبر الشبكة إلى مزود الخدمة، والذي، بدوره، يوفر لأشخاص آخرين وسيلة تتبعك. (قد لا يكون دافع مطور التطبيق هو الرغبة في تتبع المستخدمين، لكن في نهاية الأمر ستكون لديهم القدرة على القيام بذلك؛ وقد يصل بهم الأمر لكشف معلومات الموقع عن مستخدميها للحكومات أو الهاكرز). بعض الهواتف الذكية توفر لك نوعًا من السيطرة على ما إذا كانت التطبيقات تستطيع معرفة موقعك الجغرافي؛ نصيحة جيدة للحفاظ على الخصوصية، وهي محاولة تقييد التطبيقات التي بإمكانها الإطلاع على هذه المعلومات. أو على الأقل التأكد من أن موقعك يتم مشاركته فقط مع التطبيقات التي تثق بها، والتي لديها سبب وجيه لمعرفة مكان وجودك.

في كل حالة، فإنّ هدف تتبع الموقع لا ينحصر فقط في إيجاد الشخص ومعرفة مكانه، مثلما نشاهد في فيلم مثير مشهّدًا لمطاردة مثيرة، حيث يلاحق عملاء الحكومة ويراقبون شخصًا ما في الشوارع. قد يكون الأمر أيضًا حول تقديم معلومات وإجابات عن أنشطة الناس وما فعلوه في الماضي، أو عن معتقداتهم ومشاركتهم في الأحداث، وعلاقاتهم الشخصية. فعلى سبيل المثال، يمكن أن يستخدم تطبيق تتبع الموقع في محاولة معرفة ما إذا كان بعض الناس يرتبطون بعلاقة رومانسية، أو معرفة من الذي حضر اجتماع معين، أو الذين كانوا في احتجاج معين، أو محاولة تحديد المصدر السري للصحفي.

إغلاق الهواتف النقالة

هناك قلق واسع النطاق من أن الهواتف يمكن استخدامها لمراقبة الناس حتى عندما لا تستخدم بنشاط لإجراء مكالمة. نتيجة لذلك، يُنصح في بعض الأحيان من لديهم محادثة حساسة بغلاق هواتفهم تمامًا، أو حتى إزالة البطاريات من هواتفهم.

يبدو أن النصيحة بإزالة البطارية تركز بشكل أساسي على وجود البرمجيات الخبيثة والفايروسات التي تجعل الهاتف يبدو مغلقًا عند الطلب (لتبين في النهاية مجرد شاشة فارغة)، في حين يبقى مشتغلًا وقادرًا على مراقبة المحادثات، أو القيام بإجراء أو استقبال مكالمة بشكلٍ خفي. وبالتالي، يمكن خداع المستخدمين في أنه قد أغلقوا هواتفهم بنجاح، بينما كانت في الواقع تعمل. هذه البرامج الخبيثة أو الفايروسات موجودة فعليًا، أو على الأقل في بعض الأجهزة، رغم أن لدينا القليل من المعلومات حول مدى نجاح عملها، أو كيفية استخدامها على نطاق واسع.

ينطوي إغلاق الهاتف على عيب محتمل خاص: إذا قام كثير من الناس في مكان واحد بفعل ذلك، وفي نفس الوقت، سيكون ذلك بمثابة رسالة لشركات اتصالات المحمول بأن جميع هؤلاء يعتقدون بوجود شيئًا يحدث بالفعل ويستحق إغلاق هواتفهم جميعًا من أجله. (هذا "الشيء" قد يكون رفع الستار عن عرض فيلم في السينما، أو خلال ركوب الطائرة في المطار، ولكن قد يكون أيضًا اجتماعًا حساسًا أو محادثة مهمة). هناك خيار آخر قد يمنح معلومات أقل، وهو ترك جميع الهواتف في غرفة أخرى، حيث لن يكون بمقدور ميكروفونات الهواتف التصنُّت على المحادثات.



التجسس على اتصالات الأجهزة الهاتفية المحمولة

الجدير بالذكر أنّ شبكات الهاتف المحمول غير مصمّمة في الأصل بحيث تسمح باستخدام الوسائل التقنية المخصصة لحماية مكالمات المشتركين من التنصّت. وهذا يعني أنّ بمقدور كلّ شخص يملك أيّ نوع من وسائل الاستقبال اللاسلكي التنصت على المكالمات.

كما تجدر الإشارة هنا إلى أنّ الوضع اليوم أفضل نوعًا ما، ولكن قد تكون هذه الأفضلية قليلة في بعض الأحيان. فقد أضافت تقنيات التشفير معايير لخدمات الاتصالات المحمولة في محاولة لمنع التنصت. ولكن العديد من هذه التقنيات تم تصميمها بشكل سيئ⁽⁸⁶⁾. (وأحيانًا حدث هذا عن عمد، وذلك بسبب ضغط الحكومات على عدم استخدام تقنيات تشفير لا يمكن فكّها).

كذلك تمّ نشرها بشكل غير متساوٍ، حيث قد تكون متاحة لأحد مزوّدي الخدمة الهاتفية دون مزوّد آخر، أو في بلد دون بلد آخر. وأحيانًا قد يكون تمّ تركيبها بشكل غير سليم. فعلى سبيل المثال، في بعض البلدان لا يسمح مزوّدو الخدمة الهاتفية بالتشفير على الإطلاق؛ أو أنهم يستخدمون معايير فنيّة قديمة عفا عليها الزمن. وهذا يعني أنها غير فعّالة، وفي كثير من الأحيان من الممكن لشخص يمتلك جهاز استقبال لاسلكي مناسب اعتراض المكالمات والرسائل النصية خلال انتقالها عبر الأنير.

حتى إذا كانت أفضل المعايير التقنية مستخدمة، مثلما هو متحقق في بعض البلدان، ولبعض مزوّدي خدمة الهاتف النقال، لا يزال هنالك أشخاص بإمكانهم التنصت على مكالماتك. وفي أدنى احتمال، تمتلك الشركات المالكة لشبكات الهاتف النقال القدرة على اعتراض وتسجيل كافة البيانات حول من قام بالإتصال، أو إرسال رسالة نصية، ولمن، ومتى، وماذا قالوا. وقد تكون هذه المعلومات متاحة للحكومات المحلية أو الأجنبية من خلال ترتيبات رسمية أو غير رسمية. وفي بعض الحالات، قامت الحكومات الأجنبية أيضًا باختراق أنظمة مشغلي ومزوّدي الخدمات الهاتفية من أجل الحصول، وبسريرة، على بيانات المستخدمين.

إنّ أفضل طريقة، والأكثر أمنًا، هو أن نفترض أنّ المكالمات التقليدية والرسائل النصية لا يتم تأمينها وحمايتها من مخاطر التنصت أو التسجيل. وبالرغم من اختلاف التفاصيل التقنية بشكل كبير من مكان إلى آخر، ومن نظام إلى نظام، غالبًا ما تكون وسائل الحماية التقنية ضعيفة، ويمكن اختراقها في كثير من الحالات.

86 <http://www.aftenposten.no/verden/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-98459b.html>

من الممكن أن يختلف الوضع عندما تستخدم في التواصل تطبيقات الاتصالات الآمنة (سواء عن طريق الصوت أو الرسائل النصية)، لأن بإمكان هذه التطبيقات توفير التشفير لحماية اتصالاتك. كما أن بمقدور هذا التشفير أن يكون أقوى ويوفر حماية أكبر. ويعتمد مستوى الحماية الذي تحصل عليه من خلال استخدام تطبيقات الاتصالات الآمنة للتواصل بشكل كبير على التطبيقات التي تستخدمها وكيفية عملها. وهنا يكون السؤال الرئيسي والمهم هو، ما إذا كان التطبيق يستخدم نظام التشفير من الطرف إلى الطرف لحماية اتصالاتك، وعمّا إذا كان مطور التطبيق يملك إمكانية إلغاء أو تجاوز التشفير.



إصابة الهواتف النقالة بالبفيروسات والبرامج الخبيثة

قد تُصاب الهواتف النقالة بالبفيروسات وغيرها من أنواع البرمجيات الخبيثة، إما بسبب أنه تم خداع المستخدم عن طريق تحميل هذه البرامج، أو لأنّ أحدهم كان قادرًا على اختراق الجهاز من خلال ثغرة أمنية موجودة في أنظمة الجهاز نفسه. وكما هو الحال مع أنواع أجهزة الحاسبات الأخرى، فإنّ تلك البفيروسات والبرامج تستطيع التجسّس على جهاز المستخدم.

على سبيل المثال، بإمكان البفيروسات والبرامج الخبيثة التي تخترق الهاتف المحمول قراءة البيانات الخاصة على الجهاز (مثل الرسائل النصية المخزنة أو الصور). ويمكنها أيضًا تفعيل أجهزة استشعار الجهاز (مثل الميكروفون، الكاميرا، ونظام الجي بي أس) لمعرفة موقع الهاتف الجغرافي، أو مراقبة البيئة المحيطة، أو حتى تحويل الهاتف إلى فايروس يؤثر على أجهزة أخرى.

وقد استخدمت هذه التقنية من قبل بعض الحكومات للتجسّس على الناس بواسطة هواتفهم الخاصة. مما تسبّب في قلق الناس من إجراء محادثات حساسة عندما تكون الهواتف المحمولة موجودة في نفس الغرفة. بعض الناس يستجيبون لهذا الاحتمال بوضع الهواتف النقالة في غرفة أخرى عندما يريدون إجراء محادثة حساسة، أو إغلاقها تمامًا. (الحكومات نفسها، لا تسمح في كثير من الأحيان للأشخاص، حتى موظفي الحكومة، من إحضار الهواتف المحمولة الشخصية في بعض المرافق الحساسة، وذلك اعتمادًا على احتمالية إصابتها ببفيروسات أو برامج خبيثة تجعلها قادرة على تسجيل المحادثات).

هناك مصدر آخر للقلق، وهو أن البرامج الخبيثة تستطيع أن تجعل الهاتف وكأنه في وضع الإغلاق، بينما هو في الواقع يعمل (فتظهر شاشة سوداء بحيث يعتقد المستخدم خطأ بأن الهاتف قد تمّ إطفائه). وقد أدى هذا القلق ببعض الأشخاص إلى إزالة البطاريات من أجهزتهم عندما يقومون بإجراء محادثات شديدة الحساسية.

أفضل ممارسات السلامة الموصى بها للهواتف الذكية

من المستحيل تخيل الحياة بدون هاتف ذكي خاصة إذا كان الشخص منخرطاً في شكل من أشكال العمل أو التنظيم أو التعاون الجماعي. ما يجعل استهداف الأفراد والمنظمات والمجتمعات أمراً سهلاً للغاية، حيث تتمتع الهواتف دائماً بإمكانية الوصول إلى الأماكن الأكثر حماية في المنازل والمنظمات والمجتمعات. بعض الخطوات التي يمكن للمجتمعات، والأفراد اتخاذها للبقاء آمنين أثناء استخدام الهواتف الذكية هي:



إعداد قفل الشاشة

قد تكون كلمة مرور، أو رقم تعريف شخصي، أو نمط/ رمز يعمل عبر سحب أصابعك على الشاشة.. سيضمن هذا أن محتويات هاتفك لن تكون في متناول الأشخاص العشوائيين/غير المصرح لهم الذين يمكنهم الوصول إلى هاتفك. سيكون واحدًا على الأقل من الخيارات الأربعة جيدًا، لكن كلمة المرور هي الخيار الأكثر أمانًا للهاتف المحمول. لمعرفة كيفية تشفير القرص الصلب لهاتفك الذكي، انظر أدناه للحصول على مزيد من المعلومات.

حافظ على تحديث نظام تشغيل هاتفك وتطبيقاته

يحاول صانعو الهواتف ومطورو التطبيقات دائمًا تحسين أمان وكفاءة وأداء منتجاتهم من خلال إنشاء التحديثات وإرسالها بانتظام. يضمن تنزيل هذه التحديثات وتثبيتها أن يكون برنامجك أو جهازك آمنًا من الفيروسات، ويعمل أيضًا بكفاءة. يمكن إجراء تثبيت التحديثات في متجر التطبيقات الخاص بك أو في إعدادات جهازك.

تثبيت التطبيقات من المصادر الموثوقة فقط

تحتوي معظم الهواتف الذكية على متجر تطبيقات موثوق به محدد مسبقًا حيث يتم تنزيل التطبيقات. تقوم متاجر التطبيقات هذه باختبار والتحقق من أن التطبيقات الموجودة في متاجرها آمنة للاستخدام. من الصعب جدًا التحقق من تطبيقات الهاتف التي يتم تنزيلها مباشرةً من الإنترنت والتأكد من أنها ليست ضارة. ولهذا السبب يوصى بتنزيل التطبيقات فقط من متجر تطبيقات موثوق به مثل متجر قوقل بلي Google Play أو متجر أبل Apple. يؤدي أيضًا إلغاء تثبيت التطبيقات التي لم تعد تستخدمها إلى توفير مساحة على هاتفك مما يجعله أكثر كفاءة.

في ملاحظة ذات صلة، من المفيد أن تعرف دائمًا التطبيقات المثبتة على هاتفك، وإزالة التطبيقات التي لم تتعرف عليها، أو التي لم تعد تستخدمها. هذا يمكن أن يساعد في تحسين سرعات النظام، والحد من مخاطر فقدان الخصوصية، وتقليل عدد تحديثات التطبيق التي تحتاج إلى تحميل.

قم بإيقاف تشغيل واي فاي Wi-Fi و بلوتوث Bluetooth بالهاتف إذا لم يكن قيد الاستخدام

ستحاول تقنيتنا بلوتوث وواي فاي الموجودتان على الهاتف الاتصال بالشبكات اللاسلكية أو بلوتوث الأجهزة القريبة. يحدث هذا تلقائيًا عندما يتم بث معلومات تفصيلية حول الجهاز، مثل معرفات الجهاز وإمكانيات نقل البيانات. يمكن للمهاجمين جمع هذه المعلومات واستخدامها لاستهداف الجهاز. يوصى بتشغيل واي فاي وبلوتوث فقط عند استخدامها. تأكد أيضًا من إيقاف تشغيل وضع اكتشاف بلوتوث.

التواصل بشكل آمن عبر الهاتف الذكي

المكالمات الهاتفية العادية والرسائل النصية القصيرة ليست آمنة، ويمكن اعتراضها من قبل موفري الاتصالات. لذا ينبغي إجراء الاتصالات الخاصة أو الحساسة عبر تطبيقات ومنصات آمنة. تحتوي تطبيقات الاتصالات الآمنة على تشفير مدمج. التشفير من طرف إلى طرف هو أكثر أشكال التشفير الموثوق بها لأنظمة الاتصالات. فهو يضمن عدم اعتراض المكالمات والرسائل النصية القصيرة أو التنصت عليها. يتم تشفير الرسالة أو المكالمة من جهاز المرسل ولا يتم فك تشفيرها إلا على جهاز المستقبل. تحتوي تطبيقات مثل واتساب، وسيفنال، وتليغرام، وواير وسلاك و Signal و Telegram و Wire و Slack على هذه التقنية المضمنة، ويُنصح باستخدامها للاتصالات الحساسة أو الخاصة. يجب على جميع أطراف الاتصال تثبيت التطبيق على اتصال آمن.

تعمل الهواتف المحمولة على تسريع الوصول والاتصال بالإنترنت خاصة في المجتمعات ذات الدخل المنخفض والمتوسط كل عام. وهذا يعني أن المزيد والمزيد من الناس يعتمدون على الهواتف المحمولة للتواصل والتنظيم والتعاون. لسوء الحظ، فإن التواصل عبر الإنترنت باستخدام الهاتف الذكي يكون عرضة للمراقبة والاعتراض من قبل الحكومات وشركات الاتصالات. المراقبة تعني أن يكون الشخص قادرًا على مراقبة وتتبع أنشطة الشخص عبر الإنترنت. لحماية خصوصية الأنشطة عبر الإنترنت، هناك أدوات يمكن استخدامها ليس فقط لتشفير الأنشطة عبر الإنترنت ولكن أيضًا لإخفاء هوية المستخدمين.

من الموارد المفيدة جدًا لمساعدتك في تحديد ما إذا كان تطبيق المراسلة الخاص بك يمنحك الأمان والخصوصية، وهو "بطاقة التراسل الآمنة"، الذي تقدمه مؤسسة التخوم الإلكترونية⁽⁸⁷⁾.

تقوم الشبكات الافتراضية الخاصة أو شبكات VPN بإخفاء أنشطة المستخدم على الإنترنت عن طريق الوصول إلى الإنترنت من خلال شبكة كمبيوتر موجودة في موقع جغرافي مختلف. تتجاوز شبكات VPN أيضًا الرقابة على الإنترنت عن طريق الوصول إلى الصفحات الخاضعة للرقابة بشكل غير مباشر من خلال جهاز كمبيوتر مختلف باستخدام الاتصالات المشفرة. يعد Onion Router أو Tor فريدًا من نوعه لأنه يوفر إخفاء الهوية بالإضافة إلى جميع خدمات VPN. يوفر خدمة إخفاء الهوية عن طريق تقسيم كل خطوة من خطوات الاتصال وتخصيصها لجهاز كمبيوتر مختلف داخل شبكة Tor، مما يجعل من الصعب معرفة أي جهاز كمبيوتر يطلب موردًا عبر الإنترنت. يمكن أن تكون شبكات VPN مجانية أو مدفوعة، وعادة ما تحتوي الإصدارات المدفوعة على وظائف وميزات إضافية بينما Tor مجاني.

87 <https://www.eff.org/secure-messaging-scorecard>

أمن الحسابات

تعتمد الحسابات عبر الإنترنت مثل بريد الويب، وفيسبوك وتويتر، دائماً، على كلمات مرور للأمان والتحكم في الوصول. كان اكتشاف عمليات اختراق الشركات الكبرى لكلمات مرور المستخدم - ما جعل عمليات الاستيلاء على الحساب واختطافه أمراً سهلاً - كارثة بكل المقاييس. أدى هذا إلى إعادة التفكير في أمان الحساب عبر الإنترنت من خلال نظام يعتمد على كلمة المرور فقط إلى نظام التحقق من خطوتين وهو أكثر أماناً. تتطلب المصادقة الثنائية إرسال رمز إلى الهاتف أو قراءته من أحد التطبيقات الموجودة على هاتف المستخدم بالإضافة إلى كلمة المرور. ويضمن هذا النظام أنه حتى في حالة سرقة كلمة مرور الحساب، فإنه يكاد يكون من المستحيل الوصول إلى الحساب بدون الرمز من الهاتف. تتمتع جميع الحسابات الرئيسية الآن بهذه الميزة، وهي الخيار الأفضل لضمان أمن الحساب.

الأمن التشغيلي

بالإضافة إلى المسائل الأمنية أعلاه، قد يساعدك الهاتف على تنفيذ عملك بأمان وفعالية. وفيما يلي مسح موجز لبعض التطبيقات ذات الصلة:

Tella⁽⁸⁸⁾ هو تطبيق توثيق لنظام أندرويد. في البيئات المليئة بالتحديات - مع اتصال محدود أو معدوم بالإنترنت أو في مواجهة القمع. تجعل تيللا توثيق الأحداث أسهل وأكثر أماناً، سواء كان عنفًا، أو انتهاكات حقوق إنسان، أو فساد، أو تزوير الانتخابات.

Mobile martus⁽⁸⁹⁾ هو تطبيق لتجميع البيانات يتصل بقاعدة بيانات توثيق مارتوس الأمانة⁽⁹⁰⁾. يسمح التطبيق للمستخدم بإرسال التقارير الميدانية بشكل آمن إلى مشروع التوثيق الحالي، ثم يتم مسح التقرير بشكل آمن من الهاتف فور إرساله. وهو متاح للأندرويد.

Umbrella⁽⁹¹⁾ هو تطبيق مجاني للتعليم ذاتي التوجيه متاح لأنظمة أندرويد. يقوم بتغطية العديد من موضوعات الأمن الرقمي، والتنظيمي، والتشغيلي، في إصداره يمكن تحميلها على الهاتف. وهو يتضمن قوائم مرجعية مفيدة عند قيامك بتخطيط، وتنفيذ ممارسات أمنية مُحسَّنة. تعرف على المزيد من سيكيوريتي فيرست⁽⁹²⁾.

88 <https://play.google.com/store/apps/details?id=org.hzontal.tella&hl=en&gl=US>

89 <https://play.google.com/store/apps/details?id=org.martus.android&hl=en>

90 <https://www.martus.org/>

91 <https://play.google.com/store/apps/details?id=org.secfirst.umbrella>

مصادر

- سيكوري تي إن أبوكس⁽⁹³⁾ - فصول تكتيكية وأدلة خطوة بخطوة حول كيفية استخدام العديد من البرامج التي نوقشت في الكتيب الذي بين يديك. انظر أيضاً دليلهم المجتمعي للمدافعين الأفارقة عن حقوق البيئة⁽⁹⁴⁾، والأقليات الجنسية⁽⁹⁵⁾.
- الدفاع عن النفس ضدّ الرقابة⁽⁹⁶⁾ - فصول عن الحماية من المراقبة وإرشادات حول التعامل مع البرمجيات.
- معدات الإسعافات الأولية الرقمية⁽⁹⁷⁾ - إرشادات عن الاستجابة لمختلف أنواع الهجمات الرقمية.
- صحفي أكثر أماناً⁽⁹⁸⁾ - دليل التدريب على الأمن الرقمي الخاص للصحفيين.
- إلى الأمام⁽⁹⁹⁾ - منهج تدريب الأمن الرقمي للمُدربين.
- SAFETAGE⁽¹⁰⁰⁾ - إطار تدقيق الأمن الرقمي للمتخصصين في الأمن.
- فيروس توتال⁽¹⁰¹⁾ - مسح ملفات أو روابط عناوين البرامج الخبيثة.
- مجموعة الإسعافات الأولية الرقمية⁽¹⁰²⁾ - شراكة المدافعين عن الحقوق الرقمي.
- Umbrella⁽¹⁰³⁾ - تطبيق مجاني للتعلم ذاتي التوجيه مُتاح لنظام أندرويد.

93 <https://securityinabox.org/en>

94 <https://securityinabox.org/en/eco-rights-africa>

95 <https://securityinabox.org/en/lgbt-africa>

96 <https://ssd.eff.org/>

97 <https://www.digitaldefenders.org/digitalfirstaid/>

98 <https://saferjourno.internews.org/>

99 <https://www.level-up.cc/>

100 <https://safetage.org/>

101 <https://www.virustotal.com/>

102 <https://www.digitaldefenders.org/digitalfirstaid/>

103 [tps://play.google.com/store/apps/details?id=org.secfirst.umbrella](https://play.google.com/store/apps/details?id=org.secfirst.umbrella)

ملحقات

● ملحق 1: ملخص إعلان الأمم المتحدة بشأن المدافعين عن حقوق الإنسان

بدأت صياغة الإعلان الخاص بالمدافعين عن حقوق الإنسان في عام 1984، وانتهت باعتماد الجمعية العامة للنص في عام 1998، بمناسبة الذكرى الخمسين للإعلان العالمي لحقوق الإنسان. ساعد الجهد الجماعي الذي بذلته العديد من المنظمات غير الحكومية المعنية بحقوق الإنسان، وبعض وفود الدول، على ضمان أن تكون النتيجة نصاً قوياً ومفيداً وعملياً. ولعل الأهم من ذلك هو أن الإعلان ليس موجهاً إلى الدول والمدافعين عن حقوق الإنسان فحسب، بل إلى الجميع. إنه يخبرنا أن لدينا جميعاً دوراً يجب أن نؤديه كمدافعين عن حقوق الإنسان، ويؤكد أن هناك حركة عالمية لحقوق الإنسان تشملنا جميعاً.

الاسم الكامل للإعلان هو "الإعلان المتعلق بحق ومسؤولية الأفراد والجماعات وهيئات المجتمع في تعزيز وحماية حقوق الإنسان والحريات الأساسية المعترف بها عالمياً" - وكثيراً ما يتم اختصار هذا العنوان الأطول إلى "الإعلان المتعلق بالمدافعين عن حقوق الإنسان".

1. الطابع القانوني

الإعلان ليس صكاً ملزماً قانونياً، لكنه يحتوي على سلسلة من المبادئ والحقوق التي تستند إلى معايير حقوق الإنسان المنصوص عليها في الصكوك الدولية الأخرى الملزمة قانونياً - مثل العهد الدولي الخاص بالحقوق المدنية والسياسية.

علاوة على ذلك، تم اعتماد الإعلان بتوافق الآراء من قبل الجمعية العامة، وبالتالي يمثل التزاماً قوياً للغاية من جانب الدول بتنفيذه. وتنظر الدول بشكل متزايد إلى اعتماد الإعلان باعتباره تشريعاً وطنياً ملزماً.

ينص الإعلان على دعم وحماية المدافعين عن حقوق الإنسان في سياق عملهم. فهو لا يخلق حقوقاً جديدة، ولكنه بدلاً من ذلك يوضح الحقوق القائمة بطريقة تسهل تطبيقها على الدور والوضع العملي للمدافعين عن حقوق الإنسان. ويولي الاهتمام، على سبيل المثال، إلى الوصول إلى التمويل من قبل منظمات المدافعين عن حقوق الإنسان وجمع وتبادل المعلومات حول معايير حقوق الإنسان وانتهاكها.

ويحدد الإعلان بعض الواجبات المحددة للدول ومسؤوليات الجميع فيما يتعلق بالدفاع عن حقوق الإنسان، بالإضافة إلى شرح علاقته بالقانون الوطني. وتتلخص معظم بنود الإعلان في الفقرات التالية⁽¹⁰⁴⁾. ومن المهم التأكيد مرة أخرى على أن المدافعين عن حقوق الإنسان لديهم التزام بموجب الإعلان بالقيام بأنشطة سلمية.

أ. الحقوق والحماية الممنوحة للمدافعين عن حقوق الإنسان

توفر المواد 1 و5 و6 و7 و8 و9 و11 و12 و13 من الإعلان حماية محددة للمدافعين عن حقوق الإنسان، بما في ذلك حقوق:

- السعي إلى حماية، وإعمال حقوق الإنسان على الصعيدين الوطني والدولي.
- العمل في مجال حقوق الإنسان بشكل فردي وبالاشتراك مع الآخرين.
- تشكيل الجمعيات والمنظمات غير الحكومية.
- الالتقاء أو التجمع السلمي.
- البحث عن المعلومات المتعلقة بحقوق الإنسان، والحصول عليها والاحتفاظ به.
- تطوير ومناقشة أفكار ومبادئ جديدة في مجال حقوق الإنسان والدعوة إلى قبولها.
- تقديم الانتقادات والمقترحات إلى الأجسام، والهيئات الحكومية، والمنظمات المعنية بالشأن العام، لتحسين أدائها
- ولفت الانتباه إلى أي جانب من جوانب عملها قد يعيق تحقيق حقوق الإنسان.
- تقديم الشكاوى حول السياسات العامة والأفعال الرسمية المتعلقة بحقوق الإنسان، ومراجعتها.
- تقديم المساعدة القانونية، أو غيرها من النصائح والدعم من أجل الدفاع عن حقوق الإنسان.
- حضور جلسات الاستماع العامة، والإجراءات، والمحاكمات من أجل تقييم امتثالها للقانون الوطني والالتزامات الدولية الخاصة بحقوق الإنسان.
- الوصول دون عوائق إلى المنظمات غير الحكومية والمنظمات الحكومية الدولية.
- حضور جلسات الاستماع العامة، والإجراءات، والمحاكمات من أجل تقييم امتثالها للقانون الوطني والالتزامات الدولية الخاصة بحقوق الإنسان.
- الوصول دون عوائق إلى المنظمات غير الحكومية والمنظمات الحكومية الدولية.
- الحصول على المساعدة من سبل الانتصاف الفعالة.
- الممارسة المشروعة لمهنة المدافع عن حقوق الإنسان.
- الحماية الفعالة بموجب القانون الوطني عند الرد على/أو معارضة - بالوسائل السلمية - الأفعال أو أوجه التقصير المنسوبة إلى الدولة، والتي تؤدي إلى انتهاكات لحقوق الإنسان.
- التماس الموارد وتلقيها واستخدامها لغرض حماية حقوق الإنسان (بما في ذلك تلقي الأموال من الخارج).

يرد تعليق مفصل أكثر على الإعلان في تقرير الأمين العام المقدم إلى لجنة حقوق الإنسان في دورتها السادسة والخمسين، في عام 2000 (E/CN.4/2000/95). 104. ويتضمن التقرير أيضاً مقترحات لتنفيذ الإعلان. علاوة على ذلك، أصدرت مارجريت سيكاجيا، في يوليو 2011، تعليقا على الإعلان الخاص بالمدافعين عن حقوق الإنسان، وهي وثيقة رئيسية تحدد الحقوق المنصوص عليها في الإعلان وتستند في الغالب إلى المعلومات الواردة والتقارير الصادرة عن الولاية.

ب. واجبات الدول

تقع على عاتق الدول مسؤولية تنفيذ واحترام جميع أحكام الإعلان. مع ذلك، تشير المواد 2 و9 و12 و14 و15 بشكل خاص إلى دور الدول، ومسؤولية وواجب كل دولة:

- حماية، وتعزيز وتنفيذ جميع حقوق الإنسان.
- التأكد من أن جميع الأشخاص الخاضعين لولايتها القضائية قادرون على التمتع بجميع الحقوق والحريات الاجتماعية، والاقتصادية والسياسية، وغيرها من الحقوق والحريات من الناحية العملية.
- اعتماد الخطوات التشريعية، والإدارية وغيرها من الخطوات التي قد تكون ضرورية لضمان التنفيذ الفعال للحقوق والحريات.
- توفير سبل انتصاف فعالة للأشخاص الذين يدعون أنهم ضحايا انتهاك حقوق الإنسان.
- إجراء تحقيقات سريعة ونزيهة في الانتهاكات المزعومة لحقوق الإنسان.
- اتخاذ جميع التدابير اللازمة لضمان حماية كل فرد من أي عنف، أو تهديد، أو انتقام، أو تمييز ضار، أو ضغط، أو أي إجراء تعسفي آخر نتيجة لممارسته المشروعة للحقوق المشار إليها في الإعلان.
- تعزيز الفهم العام للحقوق المدنية، والسياسية، والاقتصادية، والاجتماعية والثقافية.
- ضمان ودعم إنشاء وتطوير مؤسسات وطنية مستقلة، لتعزيز وحماية حقوق الإنسان، مثل ديوان المظالم أو لجان حقوق الإنسان.
- تعزيز وتسهيل تدريس حقوق الإنسان في جميع مستويات التعليم الرسمي والتدريب المهني.

ج. مسؤوليات الجميع

يؤكد الإعلان أن لكل فرد واجبات تجاه وداخل المجتمع، وبشجعنا جميعاً على أن نكون مدافعين عن حقوق الإنسان. وتحدد المواد 10 و11 و18 مسؤوليات كل فرد في تعزيز حقوق الإنسان، وحماية الديمقراطية ومؤسساتها، وعدم انتهاك حقوق الآخرين. وتشير المادة 11 بشكل خاص إلى مسؤوليات الأشخاص الذين يمارسون المهن التي يمكن أن تؤثر على حقوق الآخرين، وهي ذات أهمية خاصة لضباط الشرطة والمحامين والقضاة، وغيرهم.

د. دور القانون الوطني

وتحدد المادتان 3 و4 علاقة الإعلان بالقانون الوطني والدولي بهدف ضمان تطبيق أعلى المعايير القانونية الممكنة لحقوق الإنسان.