NDI
NATIONAL DEMOCRATIC INSTITUTE

دليل الأمن السيبراني

الموجه إلى

منظمات المجتمع المدني

دليل لمنظمات المجتمع المدني التي تتطلع إلى وضع الخطة للأمن السيبراني

NDI
NATIONAL DEMOCRATIC INSTITUTE

دليل الأمن السيبراني

الموجه إلى

منظمات المجتمع المدني

دليل لمنظمات المجتمع المدني التي تتطلع إلى وضع الخطة للأمن السيبراني

هذا العمل مُرخص بموجب الترخيص الدولي Creative Commons Attribution-ShareAlike 4.0 International License.
لعرض نسخة من هذا الترخيص، قم بزيارة http://creativecommons.org/licenses/by-sa/4.0/ أو أرسل خطابًا إلى العنوان
Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

جدول المحتويات

الرموز المرئية 4

أفضل 10 6

المؤلفون والتقدير والعرفان 7

من نحن؟ 7

لمن هذا الدليل؟ 8

ما خطة الأمان ولماذا يجب على منظمتي أن تضع واحدة؟ 8

ما الأصول التي تمتلكها منظمتك وما الذي ترغب في حمايته؟ 9

من خصومك وما قدراتهم ودوافعهم؟ 9

ما التهديدات التي تواجه منظمتك؟ وما مدى احتماليتها وتأثيرها؟ 10

إنشاء خطة تنظيمية للأمن السيبراني 11

بناء ثقافة الأمان 12

دمج الأمان في هيكل التشغيل العادي 13

تحقيق التعاون التنظيمي 14

وضع خطة تدريبية 14

أساس قوي: تأمين الحسابات والأجهزة 16

تأمين الحسابات: كلمات المرور والمصادقة ثنائية العامل 18

تأمين الأجهزة 26

التصيّد الاحتيالي: تهديد شائع للأجهزة والحسابات 32

توصيل البيانات وتخزينها بأمان 37

الاتصالات ومشاركة البيانات 38

تخزين البيانات بشكل آمن 50

البقاء آمنًا على الإنترنت 53

التصفّح بأمان 54

أمان وسائل التواصل الاجتماعي 64

الحفاظ على استمرارية عمل مواقع الويب عبر الإنترنت 66

حماية شبكة **WiFi** الخاصة بك 67

حماية الأمن الفعلي 68

حماية الأصول الفعلية 70

ما الذي يجب القيام به عندما تسوء الأمور 74

الملحق أ: المصادر المُوصى بها 78

الملحق ب: مجموعة أدوات إطلاق خطة الأمان 79

الرموز المرئية

بالإضافة إلى النص الرئيسي، ستجد في هذا الدليل بعض العناصر المختلفة والمتكررة والمميزة. فيما يلي لائحة "رموز" بسيطة لمساعدتك في فهم العناصر الأساسية:

دراسة الحالة

يشير إلى دراسات الحالة التي تُسلّط الضوء على التأثير الواقعي لموضوع معين عن منظمات المجتمع المدني عالميًا أو في بلد معين

نصائح إضافية

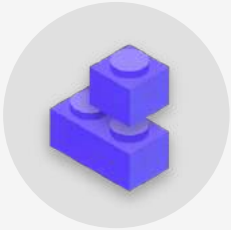
يُسلّط الضوء على بعض النصائح والمعلومات الإضافية التي يجب الانتباه إليها أثناء قراءة الدليل.

العالم الحقيقي

يُظهر أمثلة شائعة عن أدوات الأمن السيبراني التكتيكية المستخدمة في "العالم الحقيقي"، سواء في الخير أو الشرّ.

متقدم

يُشير إلى موضوع متقدم – معلومات مهمة لمنظمتك للنظر فيها، ولكن قد تكون أكثر تقنية أو معقّدة بعض الشيء.



العناصر الأساسية لخطة الأمن السيبراني

يُشير إلى "العناصر الأساسية لخطة الأمن السيبراني"، التي تعتبر العناصر الرئيسية في كل قسم من أقسام الدليل.

1

بناء ثقافة
الأمان

2

أساس قوي: تأمين الحسابات
والأجهزة

3

توصيل البيانات
وتخزينها بأمان

4

البقاء آمنًا
على الإنترنت

5

حماية الأمن
الفعلي

6

ما الذي يجب القيام به
عندما تسوء الأمور

أفضل 10

تُعد هذه العناصر العشرة ضرورية لخطة أمان منظمتك. إذا كنت تبحث عن مكان لتبدأ منه، فابحث هنا أولاً.

1. إجراء تدريب أمني منتظم داخل منظمتك
2. البقاء في حالة يقظة ضد التصيّد الاحتيالي وإيجاد نظام تبليغ
3. إستخدام التشفير من طرف إلى طرف لكل الاتصالات، متى أمكن ذلك
4. فرض كلمات مرور قوية وتزويد منظمتك بنظام إدارة كلمات المرور.
5. اعتماد المصادقة ثنائية العامل حيثما أمكن ذلك
6. التأكد من تحديث جميع أجهزة وبرامج الموظفين باستمرار
7. إستخدام التخزين السحابي الآمن
8. إستخدام بروتوكول HTTPS، والشبكة الخاصة الافتراضية VPN حيث تدعو الحاجة، للوصول إلى الإنترنت
9. حماية الأصول الفعلية لمنظمتك
10. وضع خطة تنظيمية للاستجابة للحوادث

المؤلفون والتقدير والعرفان

المؤلف الرئيسي: **إيفان سامرز (NDI) Evan Summers**

المؤلفون المساهمون: **سارة مولتون (NDI) Sarah Moulton; وكريس دوتن (NDI) Chris Doten**

بمناسبة تأليف هذا الدليل، نوّد أن نخصّ بالشكر الخبراء المراجعين الخارجيين الذين قدموا لنا ملاحظات وتعديلات واقتراحات ذات قيمة أثناء جمعنا هذا المحتوى، بما في ذلك:

Fiona Krakenburger، Open Technology Fund؛ وBill Budington و Shirin Mori، Electronic Frontier Foundation؛ وJocelyn Woolbright، Cloudflare؛ وMartin Shelton، Freedom of the Press Foundation؛ وDave Leichtman، Microsoft؛ وStephen Boyce، International Foundation for Electoral Systems؛ وAmy Studdart، International Republican Institute؛ وEmma Hollingsworth، Global Cyber Alliance؛ وCaroline Sinders، Convocation Design Research؛ و Dhyta Caturani؛ وSandra Pepera، NDI؛ وAaron Azelton، NDI؛ و Whitney Pfeifer، NDI.

ونوّد أيضًا أن نعترف بفضل جميع الأدلة والدليلات وكُتب العمل ووحدات التدريب وغيرها من المواد المذهلة التي وضعها مجتمع الأمن التنظيمي (OrgSec). ولقد وُضع هذا الدليل لاستكمال تلك المواد الأكثر تعمّقًا وجمع الدروس الرئيسية في مورد شامل وسهل القراءة لمنظمات المجتمع المدني التي تتطلع إلى البدء في خطة الأمن السيبراني.

وبالإضافة إلى الاستلهام بشكل غير مباشر من العديد من المصادر الرائعة التي جمعها المجتمع، فإننا قمنا بنسخ مواد مفيدة مباشرةً من عدد قليل من المصادر، وبخاصة "دليل الدفاع الذاتي ضد المراقبة" التابع إلى Electronic Frontier Foundation، ودليل الأمان الشامل التابع إلى منظمة Tactical Tech، ومجموعة من الشروحات من Center for Democracy and Technology وFreedom of the Press Foundation. يمكنك العثور على اقتباسات محددة لهذه المصادر من خلال الأقسام التالية،والروابط الكاملة ومعلومات حول المؤلف والترخيص في الملحق أ.

وكذلك، نُوصي بشدة أن يستفيد أي شخص يقرأ هذا الدليل من المكتبة الشاملة لأدلة الأمان الرقمية والمصادر التي جمعها Open Technology Fund وحدثها.

من نحن؟

إنّ المعهد الديمقراطي الوطني للشؤون الدولية National Democratic Institute for International Affairs (NDI) منظمة غير ربحية وغير حزبية، مقرها في واشنطن، تعمل بالشراكة حول العالم لتعزيز وحماية المنظمات الديموقراطية والإجراءات والمعايير والقيم لضمان نوعية حياة أفضل للجميع.

ويرى المعهد الديموقراطي الوطني بأن لجميع الناس الحق في العيش في عالم يحترم كرامتهم وأمنهم وحقوقهم السياسية—وأن العالم الرقمي ليس استثناءً.

يسعى فريق الديموقراطية والتكنولوجيا في المعهد الديمقراطي الوطني للشؤون الدولية إلى تعزيز نظام بيئي رقمي شامل يتم فيه حماية القيم الديموقراطية وتعزيزها، وضمان نجاحها وتكون فيه الحكومات أكثر شفافية وشمولية؛ ويتمتع جميع المواطنين بصلاحية مسائلة الحكومة. نقوم بهذا العمل من خلال دعم شبكة عالمية من النشطاء الملتزمين بالمرونة الرقمية، ومن خلال تعاون مع الشركاء فيما يتعلق بالأدوات والمصادر كمثل هذا الدليل. يمكنك معرفة المزيد حول عملنا على موقع الويب الخاص بنا، أو بمتابعتنا على Twitter، أو عن طريق التواصل مباشرة على cyberhandbook@ndi.org. ويُسعدنا دائمًا أن نستمع إليكم ونرد على تساؤلاتكم حول فريقنا وعملنا في الأمن السيبراني والتكنولوجيا والديموقراطية.

لمن هذا الدليل؟

خُصص هذا الدليل لوضع هدف بسيط في الاعتبار: مساعدة منظمات المجتمع المدني في وضع خطة أمن سيبراني مفهومة وقابلة للتنفيذ.

نظرًا لأن العالم ينتقل لاستخدام الإنترنت بشكل متزايد، فإن الأمن السيبراني ليس مجرد كلمة طنانة ولكنه مفهوم حاسم لنجاح ايّ منظمة وسلامة فريقها. بالنسبة لمنظمات المجتمع المدني العاملة في مجالات الديموقراطية والمناصرة والمسؤولية وحقوق الإنسان على وجه الخصوص، يمثّل أمان المعلومات (سواء التي عبر الإنترنت او التقليدية) تحديًا يتطلب التركيز والاستثمار واليقظة.

من المحتمل أن تجد منظمتك نفسها – إذا لم تكن بالفعل – هدفًا لهجوم سيبراني. وليس المقصود من هذا أن نثير القلق؛ ولكنّه الواقع حتى بالنسبة للمنظمات التي لا تعتبر نفسها أهدافًا لهكذا هجومات.

قام مركز الدراسات الاستراتيجية والدولية، Center for Strategic and International Studies، الذي يحتفظ بقائمة تشغيل لما يسمونه "الحوادث السيبرانية المهمة"، بسرد مئات الهجمات السيبرانية الخطيرة في العام، والتي يستهدف العديد منها العشرات، إن لم يكن المئات، من المنظمات في وقت واحد. وبالإضافة إلى مثل هذه الهجمات المبلغ عنها، هناك على الأرجح المئات من الهجمات الأصغر حجمًا، في كل عام والتي لا يتم اكتشافها أو الإبلاغ عنها، وتستهدف العديد من منظمات المجتمع المدني التي تعمل على دعم الديموقراطية والمسائلة وحقوق الإنسان. وغالبًا ما يتم استهداف منظمات تمثل النساء أو المجموعات المهمّشة الأخرى بشكل خاص.

ويكون لمثل هذه الهجمات الإلكترونية عواقب وخيمة. سواء كان هدفهم هو أخذ أموالك أو قمع صوتك أو تعطيل عملياتك التنظيمية أو تدمير سمعتك أو حتى سرقة معلومات من الممكن أن تؤدي إلى ضرر نفسي أو مادي لشركائك أو موظفيك، لذلك يجب أن يتم أخذ هذه التهديدات على محمل الجد.

إن الأمر الجيد هو إنك لست بحاجة إلى أن تصبح مبرمجًا أو خبيرًا تقنيًا للدفاع عن نفسك أو منظمتك ضد التهديدات الشائعة. وعلى الرغم من ذلك، يجب عليك أن تكون مستعدًا لاستثمار الجهد والطاقة والوقت في تطوير وتنفيذ خطة أمان تنظيمية قوية.

وإذا لم تفكر مطلقًا في الأمن السيبراني في منظمتك، أو لم يكن لديك الوقت للتركيز عليه، أو تعرف بعض الأساسيات حول الموضوع ولكنك تعتقد أن بإمكان منظمتك أن تعزز أمنها السيبراني، فإن هذا الدليل مناسب لك. وبغضّ النظر عن المكان الذي تأتي منه، يهدف هذا الدليل إلى تزويد منظمتك بالمعلومات الأساسية التي تحتاج إليها لوضع خطة أمان قوية، خطة تتجاوز مجرد الكلمات على الورق وتمكنّك من وضع أفضل الممارسات موضع التنفيذ.

ما خطة الأمان ولماذا يجب على منظمتي أن تضع واحدة؟

إن خطة الأمان عبارة عن مجموعة من السياسات والإجراءات والتعليمات المكتوبة التي وافقت عليها منظمتك لتحقيق مستوى الأمان الذي تعتقد أنت وفريقك أنه مناسب للحفاظ على أمان الأشخاص والشركاء والمعلومات.

ويمكن لخطة أمان تنظيمية جيدة الإعداد ومُحدثة أن تحافظ على سلامتك وتجعلك أكثر فاعلية من خلال توفير راحة البال اللازمة للتركيز على العمل اليومي المهم لمنظمتك. بدون التفكير في خطة شاملة، من السهل جدًا إغفال بعض أنواع التهديدات، أو التركيز على نوع واحد من المخاطر أو حتى تتجاهل الأمن السيبراني إلى أن تحدث أزمة. عندما تبدأ في تطوير خطة أمان، يكون هناك بعض الأسئلة المهمة التي يجب أن تطرحها على نفسك فيما يُعرف بعملية **تقييم المخاطر**. وتُساعد الإجابة عن هذه الأسئلة منظمتك في فهم التهديدات الفريدة التي تواجهها وتسمح لك بالرجوع خطوة إلى الوراء والتفكير بشكل شامل حول ما ومن وممّن تحتاج حمايته. يمكن للخبراء الاستشاريين المدربين، بمساعدة أنظمة مثل إطار عمل التدقيق SAFETAG الخاص بشركة Internews، المساعدة في قيادة منظمتك خلال هذه العملية. وإذا كان بإمكانك الوصول إلى هذا المستوى من الخبرة المهنية، فإن الأمر يستحق ذلك، ولكن حتى إذا لم تتمكن من الخضوع لتقييم كامل، فإنه يجب أن تلتقي بمنظمتك للنظر بعناية في هذه الأسئلة الرئيسية:

1 ما الأصول التي تمتلكها منظمتك وما الذي ترغب في حمايته؟

يمكنك البدء في الرد على هذه الأسئلة عن طريق إنشاء بيان لجميع أصول المنظمة. وتُعدّ المعلومات مثل الرسائل ورسائل البريد الإلكتروني وجهات الاتصال والمستندات والتقويمات والمواقع كلها أصول محتملة. ويمكن أن تكون الهواتف وأجهزة الكمبيوتر والأجهزة الأخرى أصولاً. وقد يكون الأشخاص والاتصالات والعلاقات أصولاً أيضًا. اكتب قائمة بالأصول لديك وحاول تصنيفها حسب أهميتها للمنظمة، ومكان الاحتفاظ بها (ربما عدة أماكن رقمية أو مادية)، وما الذي يمنع الآخرين من الوصول إليها أو إتلافها أو تعطيلها. وضع في اعتبارك أنه لا يكون كل شيء على القدر نفسه من الأهمية. وإذا كانت بعض بيانات المنظمة تتعلق بسجل عام أو معلومات قمت بنشرها بالفعل، فإنها ليست أسرارًا تحتاج إلى حمايتها.

2 من خصومك وما قدراتهم ودوافعهم؟

يُعد "الخصم" مصطلحاً شائع الإستخدام في الأمن المؤسسي. وبعبارات بسيطة، الخصوم هم الفاعلون (أفراد أو مجموعات) مهتمون باستهداف منظمتك وتعطيل عملك والوصول إلى معلوماتك أو تدميرها: الأشرار. ويمكن أن تشمل الأمثلة الخصوم المحتملين المحتالين الماليين أو المنافسين أو السلطات أو الحكومات المحلية أو الوطنية أو المتطفلين أصحاب الدوافع الأيديولوجية أو السياسية. ومن المهم وضع قائمة بخصومك والتفكير بشكل نقدي حول من قد يرغب في التأثير سلبًا على منظمتك وموظفيك. في حين أنه من السهل تصور الجهات الخارجية (مثل حكومة أجنبية أو مجموعة سياسية معينة) كخصوم، وضع في اعتبارك أيضًا أن الخصوم يمكن أن يكونوا أشخاصًا تعرفهم، مثل الموظفين الناقمون وأفراد الأسرة أو الشركاء غير الداعمين. ويُشكل الخصوم تهديدات مختلفة ولديهم موارد وقدرات مختلفة لتعطيل عملياتك والوصول إلى معلوماتك أو تدميرها.
على سبيل المثال، غالبًا ما تمتلك الحكومات الكثير من الأموال والإمكانات القوية التي تتضمن إغلاق الإنترنت أو إستخدام تقنية مراقبة باهظة الثمن؛ ومن المحتمل أن تتمتع شبكات الهاتف المحمول وموفري خدمة الإنترنت بإمكانية الوصول إلى سجلات المكالمات وتصفح السجلات؛ ويتمتع المتطفلون المهرة على شبكات Wi-Fi بالقدرة على اعتراض الاتصالات أو المعاملات المالية غير المؤمنة بشكل جيد. ويمكنك أن تكون أنت الخصم لنفسك، على سبيل المثال، عن طريق حذف ملفات مهمة عن طريق الخطأ أو إرسال رسائل خاصة إلى الشخص الخطأ.

ومن المرجح أن تختلف دوافع الخصوم مع اختلاف قدراتهم أو اهتماماتهم وإستراتيجياتهم. هل هم مهتمون بتشويه سمعة منظمتك؟ ربما يكونوا عازمون على القضاء على رسالتك؟ أو ربما يرون منظمتك على أنها منافسة ويريدون التفوق عليها؟ ومن المهم فهم دوافع الخصم لأن القيام بذلك يمكن أن يساعد منظمتك في تقييم التهديدات التي يمكن أن تطرأ بشكل أفضل.

3 ما التهديدات التي تواجه منظمتك؟ وما مدى احتماليتها وتأثيرها؟

عندما تحدد التهديدات المحتملة، فمن المحتمل أن ينتهي بك الأمر بقائمة طويلة قد تكون كبيرة جدًا. وقد تشعر أن أية جهود لن تكون مجدية، أو لا تعرف من أين تبدأ. للمساعدة في تمكين منظمتك من اتخاذ خطوات مثمرة تالية، من المفيد أن يتم تحليل كل تهديد استنادًا إلى عاملين: احتمالية حدوث التهديد وتأثير التهديد إذا ما حدث.

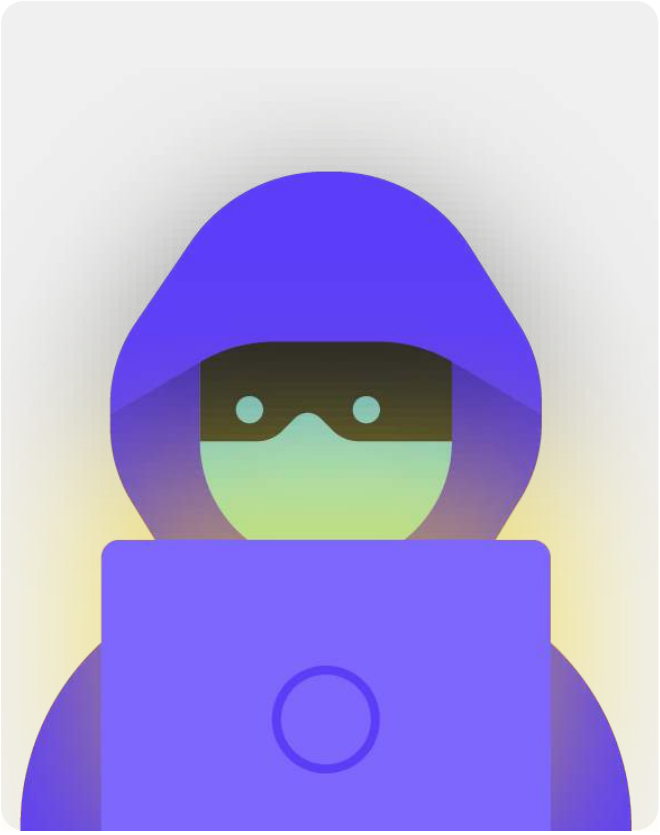
ولقياس احتمالية حدوث تهديد (ربما "منخفضة أو متوسطة أو عالية"، استنادًا إلى ما إذا كان من غير المحتمل وقوع حدث معين أو يمكن أن يحدث أو يحدث بشكل متكرر)، فإنه يمكنك إستخدام المعلومات التي تعرفها عن قدرة خصومك ودوافعهم وتحليل الحوادث الأمنية السابقة وتجارب المنظمات الأخرى المماثلة وبالطبع وجود أية إستراتيجيات تخفيف حالية وضعتها منظمتك.

لقياس تأثير تهديد ما، فكّر في الشكل الذي سيبدو عليه عالمك إذا حدث التهديد بالفعل. واطرح أسئلة مثل "كيف أضرّنا التهديد بصفتنا منظمة وبصفتنا أشخاص، جسديًا وعقليًا؟"، و"ما مدى استمرار التأثير؟"، و"هل يؤدي هذا إلى حدوث مواقف ضارة أخرى؟"، و"كيف يعيق ذلك قدرتنا على تحقيق أهداف منظمتنا التنظيمية الآن وفي المستقبل؟" أثناء إجابتك عن هذه الأسئلة، ضع في اعتبارك درجة تأثير التهديد، سواء كانت درجة منخفضة أو متوسطة أو عالية.

وبمجرد أن تقوم بتصنيف التهديدات الخاصة من خلال الاحتمالية والتأثير، فإنه يمكنك البدء في وضع خطة عمل أكثر استنارة. ومن خلال التركيز على تلك التهديدات التي من المرجّح أن تحدث "و" التي سيكون لها آثارًا سلبية كبيرة، فسوف تقوم بتوجيه مواردك المحدودة بأكثر الطرق كفاءة وفعالية ممكنة.

وإن هدفك دائمًا هو تقليل أكبر قدر ممكن من مستوى المخاطر، ولكن لا يمكن لأي شخص – ليست الحكومة أو الشركة التي تتمتع بموارد جيدة – القضاء على المخاطر بشكل كامل. ولا بأس بذلك: يمكنك فعل الكثير لحماية نفسك وزملائك ومنظمتك من خلال الاهتمام بالتهديدات الأكبر.

ولمساعدتك في إدارة عملية تقييم المخاطر هذه، فكر في إستخدام ورقة عمل، مثل هذه التي وضعتها Electronic Frontier Foundation. وتذكّر أن المعلومات التي تضعها كجزء من هذه العملية (مثل قائمة خصومك والتهديدات التي تُشكلها) قد تكون في حد ذاتها معلومات حساسة، لذلك من المهم الحفاظ على أمانها.



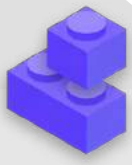
إنشاء خطة مؤسساتية للأمن السيبراني

في حين أن خطة الأمان لكل منظمة ستبدو مختلفة قليلاً بناءً على تقييم المخاطر والديناميكيات التنظيمية، فإن بعض المفاهيم الأساسية تكون عالمية تقريبًا.

ويتناول هذا الدليل هذه المفاهيم الأساسية بطريقة تساعد منظمتك في بناء خطة أمان ملموسة تستند إلى الحلول العملية والتطبيقات الواقعية.

ويسعى هذا الدليل إلى توفير خيارات واقتراحات مجانية أو منخفضة التكلفة. وضع في اعتبارك أن أهم تكلفة مرتبطة بتنفيذ خطة أمان فعالة ستكون عبارة عن الوقت الذي ستحتاجه منظمتك للتحدّث عن خطتك الجديدة وتعلّمها وتنفيذها. وبالنظر إلى المخاطر التي من المحتمل أن تواجهها منظمتك، فإن هذا الاستثمار يستحق العناء.

في كل قسم، ستجد شرحًا لموضوع رئيسي يجب أن تكون منظمتك وموظفيها على دراية به – وبماهيّته وسبب أهميته. يتم إقران كل موضوع بالإستراتيجيات والأساليب والأدوات المُوصى بها للحد من المخاطر والنصائح وروابط إلى موارد إضافية يمكن أن تساعد في تنفيذ هذه التوصيات عبر منظمتك.



أدوات إطلاق خطة الأمان

لمساعدة منظمتك في التعامل مع دروس الدليل وتحويلها إلى خطة حقيقية، استخدم أدوات الإطلاق هذه. ويمكنك إما طباعة الأدوات أو تعبئتها رقميًا أثناء قراءة الدليل عبر الإنترنت. وأثناء تدوين الملاحظات وبدء تحديث خطة الأمان أو صياغتها، تأكد من الرجوع إلى "العناصر الأساسية لخطة الأمان" المذكورة بالتفصيل في كل قسم. لا توجد خطة أمان كاملة بدون التعامل مع هذه العناصر الأساسية، في الحدّ الأدنى.

استفد من المصادر الأخرى التي يمكن أن تساعدك في وضع خطة وتنفيذها أيضًا. كمنظمة مجتمع مدني، يمكن أن يساعد التطبيق المجاني SOAP ("تأمين المنظمات عن طريق صناعة السياسات المؤتمتة") في تبسيط إنشاء خطة الأمان وأتمتتها.

كذلك، استفد من مصادر التدريب المجانية مثل مخطط أمان Consumer Reports، وتطبيق Umbrella من Security First، ومشروع Totem من Free Press Unlimited وGreenhost، وGlobal Cyber Alliance مجموعة أدوات الأمن السيبراني للمنظمات القائمة على البعثات، التي تتضمن مصادر عن العديد من أفضل الممارسات المذكورة في هذا الدليل وروابط لعشرات أدوات التدريب لمساعدتك في تنفيذ العديد من الخطوات الأساسية.

بناء ثقافة الأمان

يتمحور منطق الأمان حول الأشخاص، ولحماية منظمتك تحتاج إلى التأكد من أن جميع المعنيين يأخذون الأمن السيبراني على محمل الجدّ. ويُعدّ تغيير الثقافة أمرًا صعبًا، ولكن يمكن لبضع خطوات بسيطة ومحادثات مهمة أن تقطع شوطًا طويلاً نحو خلق أجواء تخلق مرونة لدى موظفيك ومنظمتك تمكّنهم من مواجهة تهديدات الأمن السيبراني. إن واحدة من أبسط وأهمّ الخطوات التي يجب اتخاذها لتأسيس ثقافة الأمان التنظيمي هي التواصل داخل المنظمة وقيام القادة بنمذجة السلوك الجيد دائمًا.

دمج الأمان في هيكل التشغيل الإعتيادي

كما هو موضح بالتفصيل في دليل الأمان الشامل التابع إلى Tactical Tech، فمن الضروري إنشاء مساحات آمنة للتحدث حول الجوانب المختلفة للأمان.

وبهذه الطريقة، إذا كان لدى أحد أعضاء الفريق مخاوف حول الأمان، فإنه سيكون أقل قلقًا بشأن الظهور بحالة جنون الريبة أو إهدار وقت الآخرين. كذلك، يعمل **تحديد موعد محادثات منتظمة عن الأمان** على جعل وتيرة التفاعل والتفكير في أمور متعلقة بالأمان أمرًا طبيعيًا، فلا يتم نسيان المشكلات ولا يكون أعضاء الفريق أكثر عُرضة للوعي السلبي للأمان لعملهم الجاري على الأقل. ولا يلزم أن يكون الموعد كل أسبوع، ولكن اجعله تذكيرًا دوريًا. يجب ألا تنحصر هذه المناقشات بموضوعات الأمن التقني فقط، بل يجب أيضًا أن تتناول المشكلات التي تؤثر على راحة الموظفين وسلامتهم مثل الصراع المجتمعي والمضايقات عبر الإنترنت (ودون الاتصال بالإنترنت) أو المشكلات المتعلقة بإستخدام الأدوات الرقمية وتنفيذها. يمكن أن تشمل المحادثات موضوعات مثل المعلومات دون اتصال- مشاركة العادات والطرق التي يتبناها الموظفون لتأمين وحماية المعلومات خارج العمل. بعد كل ما تقدّم، من المهم أن نتذكر أن أمان المنظمة يكون قويًا بقدر حلقتها الأضعف فقط. تتمثل إحدى طرق تحقيق المشاركة المتسقة عن طريق إضافة الأمان إلى جدول أعمال اجتماع عادي. ويمكنكم أيضًا تناوب المسؤولية لتنظيم وتسهيل مناقشة حول الأمان بين أعضاء المنظمة، مما يمكن أن يساعد في تطوير فكرة أن الأمن مسؤولية الجميع وليس فقط مسؤولية قلّة مختارة أو "فريق تكنولوجيا المعلومات". وعندما تبدأ في إضفاء الطابع الرسمي على المناقشة حول الأمن، من المرجح أن يشعر الموظفون براحة أكبر عند مناقشة هذه القضايا المهمة فيما بينهم أيضًا في أماكن أقل رسمية.

ومن المهم أيضًا دمج عناصر الأمان في الأداء الطبيعي للمنظمة، مثل أثناء إعداد الموظف – والتفكير في حجب الوصول إلى الأنظمة عند التسريح او الفصل. لا ينبغي أن يكون الأمان "شيئًا إضافيًا" تقلق بشأنه، ولكن يجب أن يكون ***جزءًا لا يتجزأ من إستراتيجيتك وعملياتك***.

تذكر أنه يجب اعتبار كل خطط الأمان وثائق حية، ويجب إعادة تقييمها ومناقشتها بانتظام، خاصة عندما ينضمّ موظفون جدد أو متطوعون إلى منظمتك أو عند تغيير سياق الأمان لديك.

خطّط لإعادة النظر في إستراتيجيتك وقم بإجراء التحديثات سنويًا، أو إذا ما كان هناك تغييرات كبيرة في الإستراتيجية أو الأدوات أو التهديدات التي تواجهها.

تحقيق التعاون على مستوى المنظمة

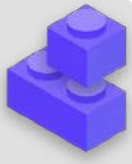
إن جزء من ثقافة الأمان الناجحة هو ضمان التعاون عبر منظمتك لخطة الأمان الخاصة بك.

ويجب أن يشمل هذا بشكل حاسم دعمًا قويًا وصريحًا وتوجيهًا من القادة التنظيميين الذين سيتخذون، في كثير من الحالات، القرار النهائي بتخصيص الوقت والموارد والطاقة لوضع وتنفيذ خطة أمان فعالة. إذا لم يأخذ القادة الأمر على محمل الجد، فلن يقوم غيرهم بذلك. لتحقيق هذا التعاون عبر المنظمة، فكّر جيدًا في وقت تقديم خطتك وكيفية حدوث ذلك، وافعل ذلك بطريقة واضحة وتأكد من أن القيادة تعزّز الرسائل وأطلع الجميع على كافة عناصر الخطة وخطواتها بحيث لا يكون هناك أمور غامضة أو ارتباكًا فيما يتعلق بما تحاول تحقيقه. يطالب العديد من المانحين الآن من المستفيدين الحفاظ على أمن قوي، لذا فإن التشديد على هذا الأمر يمكن أن يكون وسيلة جيدة لخلق تعاون تنظيمي أعمق لدى الموظفين. وعند التحدث عن الأمان، تجنّب الأساليب الترويعية. في بعض الأحيان، قد تكون التهديدات التي تواجهها منظمتك وموظفيك مخيفة، ولكن حاول التركيز على مشاركة الحقائق وخلق مساحة هادئة للأسئلة والتساؤلات. يمكن أن يؤدي تضخيم الأخطار لدرجة تبدو بها أنها مهددة للغاية إلى رفض الناس لك بصفتك مروّج للأخبار المثيرة أو الاستسلام ببساطة، معتقدين أنه لا شيء يفعلونه مهم - أو ان ما تقوله يبعد جداً عن الحقيقة.

وضع خطة تدريبية

بمجرد وضع خطة والالتزام بها، فكر في كيفية تدريب جميع الموظفين (والمتطوعين) على الممارسات الفضلى.

يمكن أن يكون فرض تدريبًا دوريًا - وجعل حضور التدريب إلزاميًا ونقطة للتقييم ضمن مراجعات أداء الموظفين - أسلوبًا مفيدًا. تجنّب خلق عواقب وخيمة وسلبية للموظفين الذين يعانون من التعامل مع مفاهيم الأمان. وضع في اعتبارك أن بعض الموظفين قد يتكيّفون ويتعرّفون على التكنولوجيا بشكل مختلف عن الآخرين استنادًا إلى المستويات المختلفة من الإلمام بالأدوات الرقمية والإنترنت. يزيد الخوف من الفشل من تثبيط الموظفين فيما يتعلق بالإبلاغ عن المشكلات أو طلب المساعدة. ومع ذلك، قد يكون لإنشاء مبدأ المسائلة الإيجابية ووضع المكافآت للتدريب الناجح وعند اعتماد السياسات دوراً مساعداً في تحفيز التحسينات عبر المنظمة. قد تجد دعمًا قيمًا إضافيًا من خلال شبكات التدريب على الأمان الرقمي المحلي أو الدولي ومصادر تدريب مجانية مثل تطبيق Umbrella من Security First ومشروع Totem من Free Press Unlimited وGreenhost ومدخل التعلم من Global Cyber Alliance.



بناء ثقافة الأمان

- حدد مواعيد محادثات وتدريبات منتظمة عن الأمان وخطة الأمان لديك.
- أشرك الجميع - ووزع مسؤولية تنفيذ خطة الأمان الخاصة بك عبر المنظمة بأكملها.
- تأكد من لعب القيادة دورا نموذجياً للسلوك الأمني الجيد والالتزام بخطتك.
- تجنب أساليب الترهيب أو العقاب - وضع مكافأة للتحسين وقم بإنشاء مساحة مريحة للموظفين للإبلاغ عن المشكلات وطلب المساعدة.
- حدّث خطة الأمان لديك سنويًا أو بعد التغييرات الكبيرة في المنظمة.

أساس قويّ: تأمين الحسابات والأجهزة

لماذا التركيز على الحسابات والأجهزة؟ لأنها تُشكل الأساس لكل شيء تقوم به منظمتك رقميًا.

ومن المؤكد أنك تصل إلى معلومات حساسة وتتواصل داخليًا وخارجيًا وتحتفظ بمعلومات خاصة عليها. وإذا لم تكن هذه الحسابات والأجهزة آمنة، فمن المحتمل تعريضها للخطر. على سبيل المثال، إذا كان المتسللون يشاهدون ضغطات المفاتيح أو يستمعون إلى الميكروفون، فإنه سيتم الاستماع إلى المحادثات الخاصة مع الزملاء بغض النظر عن مدى أمان تطبيقات المراسلة الخاصة بك. أو، إذا تمكّن أحد الخصوم من الوصول إلى حسابات وسائل التواصل الاجتماعي الخاصة بمنظمتك، فإنه يمكنهم الإضرار بسمعتك ومصداقيتك بسهولة، مما يعمل على زعزعة نجاح عملك. لذلك، من الضروري بصفتك منظمة التأكد من أن الجميع يتخذ بعض الخطوات البسيطة والفعالة للحفاظ على أمان أجهزتهم وحساباتهم. ومن المهم ملاحظة أن هذه التوصيات تشمل حسابات وأجهزة شخصية أيضًا، حيث إنها غالبًا ما تكون أهدافًا سهلة للخصوم. وسوف يسعى المتسللون بكل سرور وراء الهدف الأسهل واقتحام حساب شخصي أو كمبيوتر منزلي إذا كان فريقك يستخدمه للتواصل والوصول إلى المعلومات المهمة.

تأمين الحسابات والمجتمع المدني

تم الكشف عن اختراق SolarWinds الذي تم نشره على نطاق واسع في أواخر عام 2020، والذي أدى إلى اختراق أكثر من 250 منظمة، بما في ذلك معظم الإدارات الحكومية الأمريكية وشركات توريد التكنولوجيا مثل Microsoft (مايكروسوفت) وCisco (سيسكو)، والمنظمات غير الحكومية، وكان ذلك ولو بشكل جزئي نتيجة لتخمين المتسللين لكلمات المرور الضعيفة التي تم إستخدامها في حسابات المسؤولين المهمة. وبشكل عام، تحدث الاختراقات المتعلقة بالقرصنة بسبب كلمات المرور الضعيفة أو المُعاد إستخدامها بنسبة 80 بالمائة.

ومع الانتشار المتزايد لاختراقات كلمات المرور مثل ما تقدّم وسهولة وصول جميع أنواع الخصوم إلى الأدوات المتطورة لاختراق كلمات المرور، يعتبر إتباع الممارسات الفضلى المتعلقة بكلمات المرور والمصادقة ثنائية العامل من متطلبات الأمان لمنظمات المجتمع المدني. تم الإبلاغ عن أحد الأمثلة على حسابات المجتمع المدني التي تعرضت للهجوم بواسطة موقع التواصل الاجتماعي فيسبوك في عام 2020. وفقًا للتقرير، استهدفت مجموعات القرصنة في بنغلاديش حسابات نشطاء المجتمع المدني المحليين والصحفيين والأقليات الدينية. ولسوء الحظ، تمكن المتسللون من اختراق بعض حسابات موقع التواصل الاجتماعي Facebook هذه، بما في ذلك مسؤول صفحة Facebook لمجموعة محلية. ومن خلال الوصول إلى حساب المسؤول، أزال المتسللون المسؤولون الباقون وتولوا الأمر وقاموا بتعطيل الصفحة، مما منع المجموعة من مشاركة المعلومات الرئيسية والتواصل مع جمهورها. اكتشف تحقيق موقع تواصل Facebook أنه من المحتمل أن يكون اختراق الحسابات من خلال وسائل مختلفة، بما في ذلك إساءة إستخدام عملية استرداد الحساب. إذا كانت جميع الحسابات تستخدم المصادقة ثنائية العامل، لكان من الصعب على المتسللين تنفيذ هجمات مثل هذه بشكل فعال.

تأمين الحسابات: كلمات المرور والمصادقة ثنائية العامل

في الوقت المعاصر، من المحتمل أن يكون لدى منظمتك وموظفيها العشرات، إن لم يكن المئات، من الحسابات التي، إذا تم اختراقها، يمكن أن تكشف عن معلومات حساسة أو حتى تُعرّض الأفراد للخطر.

فكر في الحسابات المختلفة التي قد يمتلكها الموظفون والمنظمة ككل: البريد الإلكتروني وتطبيقات الدردشة ووسائل التواصل الاجتماعي والأعمال المصرفية عبر الإنترنت وبيانات التخزين عبر السحابة، بالإضافة إلى المطاعم المحلية والصُحف والعديد من مواقع الويب أو التطبيقات الأخرى التي تقوم بتسجيل الدخول إليها. وفي وقتنا الحاضر، يتطلب الأمان الجيّد نهجًا مختلفًا لحماية جميع هذه الحسابات من الهجمات. ويبدأ ذلك بضمان سلامة كلمة المرور الجيدة وإستخدام مصادقة ثنائية العامل عبر المنظمة بأكملها.

ما الذي يجعل كلمة المرور جيدة؟

هناك ثلاثة مفاتيح للحصول على كلمة مرور جيدة وقوية: الطول والعشوائية والتفرّد.

الطول

كلما كانت كلمة المرور طويلة، كان من الصعب على الخصم تخمينها. وتتم معظم عمليات اختراق كلمات المرور بواسطة برامج الكمبيوتر هذه الأيام، ولا تستغرق هذه البرامج الشائنة وقتًا طويلاً لاختراق كلمة مرور قصيرة. ونتيجة لذلك، يجب ألا تقلّ كلمات المرور الخاصة بك عن 16 حرفًا بحدّ أدنى أو خمسة كلمات على الأقل ويُفضّل أن تكون أطول من ذلك

العشوائية

حتى إذا كانت كلمة المرور طويلة، فإنها لا تكون جيدة بالقدر الكافي إذا كانت شيئًا من السهل على الخصم تخمينه عنك. وتجنب تضمين معلومات مثل تاريخ ميلادك أو مسقط رأسك أو أنشطتك المفضلة أو أية معلومات أخرى يمكن أن يكتشفها عنك أي شخص من خلال القيام ببحث سريع على الإنترنت.

التفرّد

ربما تكون "الممارسة الأسوأ" الأكثر شيوعًا لكلمة المرور هي إستخدام كلمة المرور نفسها لمواقع متعددة. ويُعد تكرار كلمات المرور مشكلة كبيرة لأنه يعني أنه عندما يتم اختراق أحد هذه الحسابات، فإن أية حسابات أخرى تستخدم كلمة المرور نفسها تكون عُرضة للاختراق أيضًا. وإذا كنت تستخدم عبارة المرور نفسها على مواقع متعددة، فإنه يمكن أن تزيد من تأثير خطأ واحد أو خرق للبيانات بشكل كبير. على سبيل المثال، أنك لا تهتم بكلمة المرور الخاصة بك للمكتبة المحلية، فإذا تم اختراقها واستخدمت أنت كلمة المرور نفسها على حساب أكثر حساسية، فإنه يمكن سرقة المعلومات المهمة.

وهناك طريقة سهلة لتحقيق أهداف الطول والعشوائية والتفرد هذه ألا وهي اختيار ثلاث أو أربع كلمات شائعة ولكنها عشوائية. على سبيل المثال، يمكن أن تكون كلمة مرورك "وردة مصباح أخضر دب" والتي يسهل تذكرها ولكن يصعب تخمينها. يمكنك إلقاء نظرة على موقع الويب هذا من Better Buys لمعرفة مدى سرعة اختراق كلمات المرور السيئة.

إستخدام تطبيق لإدارة كلمات مرور للمساعدة

إذن، أنت تعرف أنه من المهم لكل شخص في المنظمة إستخدام كلمة مرور طويلة وعشوائية ومختلفة لكل حساب من الحسابات الشخصية والتنظيمية، ولكن كيف تفعل ذلك بالفعل؟ يُعد حفظ كلمة مرور جيدة لعشرات (إن لم يكن المئات) من الحسابات أمرًا مستحيلاً، لذلك يتعين على الجميع الخداع. وإن الطريقة الخاطئة للقيام بذلك هي إعادة إستخدام كلمات المرور. ولحسن الحظ، يمكننا اللجوء إلى برامج ادارة كلمات المرور الرقمية لجعل حياتنا أسهل بكثير (وممارساتنا في ما يخص كلمات المرور الخاصة بنا أكثر أمانًا). ويمكن لهذه التطبيقات، التي يمكن الوصول إلى العديد منها عبر جهاز الكمبيوتر أو الهاتف المحمول، إنشاء كلمات مرور وتخزينها وإدارتها لك ولمنظمتك بالكامل. وإن اعتماد تطبيق لإدارة كلمات مرور آمن يعني أنه يجب عليك فقط تذكر كلمة مرور واحدة قوية جدًا وطويلة تسمى كلمة المرور الأساسية (يُشار إليها تاريخيًا باسم كلمة المرور "الرئيسية") بالإضافة على القدرة على الحصول على ميزات الأمان لإستخدام كلمات مرور جيدة وفريدة عبر جميع حساباتك. ستستخدم كلمة المرور الأساسية هذه (وبشكل مثالي المصادقة ثنائية العامل (2FA)، التي ستتم مناقشتها في القسم التالي) لفتح تطبيق إدارة كلمات المرور وتأمين الوصول إلى كل كلمات المرور الأخرى. ويمكن أيضًا مشاركة تطبيق إدارة كلمات المرور عبر حسابات متعددة لتسهيل المشاركة الآمنة لكلمة المرور في جميع أنحاء المنظمة.

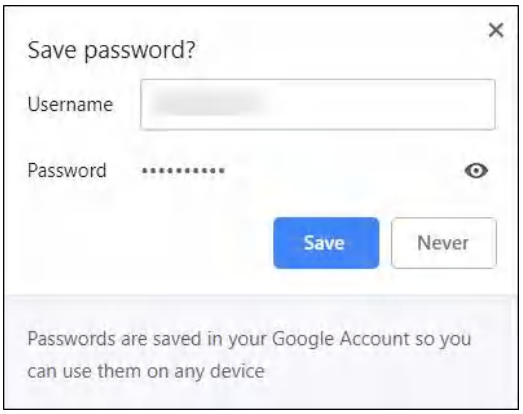
لماذا نحتاج إلى إستخدام شيء جديد؟ ألا نستطيع تدوينها على الورق أو في جدول بيانات على الكمبيوتر فقط؟

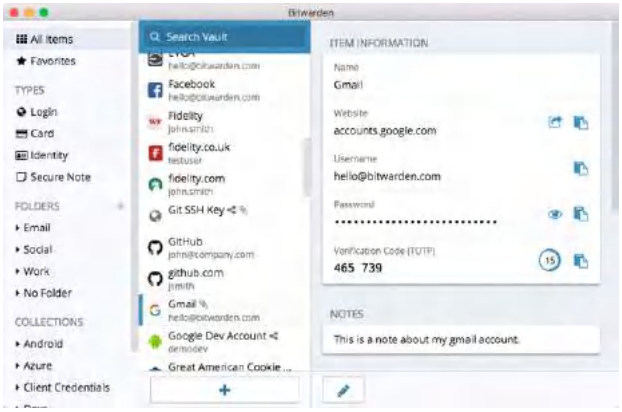
لسوء الحظ، يوجد العديد من الأساليب الشائعة لإدارة كلمات المرور غير الآمنة. ويمكن أن يؤدي الاحتفاظ بكلمات المرور على الورق (ما لم يتم الاحتفاظ بالورق في مكان مغلق في خزنة ما) إلى تعرضها للسرقة وللمتطفلين وفقدانها وتلفها بسهولة. يؤدي حفظ كلمات المرور في مستند على الكمبيوتر إلى تسهيل وصول المتسلل إليه بشكل كبير – أو شخص ما يسرق الكمبيوتر وبذلك لا تخسر فقط الكمبيوتر الخاص بك ولكن يقوم المتسلل بالوصول إلى جميع حساباتك كذلك. ويُعد إستخدام تطبيق إدارة كلمات مرور جيد أمرًا سهلاً مثل ذلك المستند، ولكنه أكثر أمانًا.

لماذا يجب أن نثق في تطبيق إدارة كلمات المرور؟

يلجأ تطبيق إدارة كلمات المرور الجيّدة إلى اعتماد كلمات المرور ذات الطول غير العادي (ويوظفون فرق أمان ممتازة) للحفاظ على أمان أنظمتهم. ويتم أيضًا إعداد تطبيقات كلمات مرور جيدة (يُوصى ببعضها فيما يلي) بحيث لا يمكن لأي شخص أن يقوم "بإلغاء تأمين" حساباتك. وهذا يعني أنه في معظم الحالات، حتى لو تم اختراقهم أو إجبارهم قانونيًا على تسليم المعلومات، فلن يتمكنوا من فقدان كلمات المرور أو التخلي عنها. كذلك، من المهم أن تتذكر أنه من المرجح بشكل غير محدود أن يخمن الخصم كلمة مرور من كلمات المرور الضعيفة أو المتكررة، أو يعثر على واحدة في خرق البيانات العامة، بالمقارنة مع احتمالية أن يتم تعطيل أنظمة الأمان الخاصة بتطبيق إدارة كلمات المرور الجيد. ومن المهم أن تكون شكاكًا، ويجب عليك عدم الوثوق في جميع البرامج والتطبيقات ثقة عمياء، ولكن تطبيقات إدارة كلمات المرور ذات السمعة الجيدة تتمتع بجميع الميزات المناسبة لفعل الشيء الصحيح.

بدلاً من إستخدام المستعرض الخاص بك (مثل Chrome، الذي يظهر على اليسار) لحفظ كلمات المرور، استخدم تطبيق إدارة كلمات مرور مخصص (مثل Bitwarden، الذي يظهر على اليمين). تتمتع هذه التطبيقات بميزات تجعل الحياة أكثر أمانًا وملائمة بالنسبة لمنظمتك.





ماذا عن تخزين كلمات المرور في المستعرض؟

يختلف حفظ كلمات المرور في المستعرض الخاص بك عن إستخدام تطبيق إدارة كلمات مرور آمن. وباختصار، يجب ألا تستخدم Chrome أو Firefox أو Safari أو أي متصفح آخر لإدارة كلمات المرور. على الرغم من أنه يُعد بالتأكيد أفضل من كتابتها على الورق أو حفظها في جدول بيانات، إلا أن الميزات الأساسية لحفظ كلمة المرور في متصفح الويب لديك تهمل شيئًا مطلوبًا من منظور الأمان. كذلك، هذه العيوب تسلب منك الكثير من الراحة التي يجلبها لك تطبيق إدارة كلمات المرور الجيد. ويؤدي فقدان هذه الراحة إلى زيادة احتمالية استمرار الأشخاص في القيام بممارسات إنشاء كلمة مرور ضعيفة ومشاركتها في منظمتك.

على سبيل المثال، على عكس البرامج المتخصصة في إدارة كلمات المرور المخصصين، لا توفر ميزات المستعرضات المضمنة "حفظ كلمة المرور هذه" أو "تذكر كلمة المرور هذه" توافقًا بسيطًا مع الأجهزة المحمولة والوظائف عبر المستعرض وإنشاء كلمة مرور قوية وأدوات التدقيق. تُعدّ هذه الميزات جزءًا كبيرًا مما يجعل تطبيق كلمات مرور متخصص أمرًا مفيدًا جدًا وذا منفعة لأمان منظمتك. كذلك، يتضمن تطبيق كلمات المرور ميزات خاصة بالمنظمة (مثل مشاركة كلمة المرور) لا توفر قيمة أمان فردية فحسب، بل قيمة للمنظمة ككل. إذا كنت تحفظ كلمات المرور في المستعرض الخاص بك (عن قصد أو عن غير قصد)، فخذ من وقتك لحظة لإزالتها.

ما هو برنامج ادارة كلمات المرور الذي يجب أن نستخدمه؟

توجد العديد من أدوات إدارة كلمات المرور الجيدة التي يمكن إعدادها في أقل من 30 دقيقة. إذا كنت تبحث عن خيار موثوق عبر الإنترنت لمنظمتك يمكن للأشخاص الوصول إليه من أجهزة متعددة في أي وقت، 1Password (يبدأ من 2.99 دولارًا أمريكيًا لكل مستخدم في الشهر) أو Bitwarden مفتوح المصدر المجاني وكلاهما مدعومين جيدًا ومُوصى بهما. يمكن أن يكون الخيار عبر الإنترنت مثل Bitwarden رائعًا لتحقيق الأمان والراحة. سيساعدك Bitwarden، على سبيل المثال، في إنشاء كلمات مرور قوية وفريدة والوصول إلى كلمات المرور من أجهزة متعددة من خلال ملحقات المستعرض وتطبيق الهاتف المحمول. ومع الإصدار المدفوع (10 دولارات أمريكية لمدة عام كامل) يوفر Bitwarden كذلك تقارير حول كلمات المرور المُعاد إستخدامها والضعيفة وربما

المخترقة لمساعدتك في البقاء مطلعًا بالمستجدات. وبمجرد إعداد كلمة المرور الأساسية (يُشار إليها باسم كلمة المرور الرئيسية)، يجب عليك كذلك تشغيل المصادقة ثنائية العامل للحفاظ على أمان مخزن تطبيق إدارة كلمات المرور قدر الإمكان.

ومن الضروري **ممارسة الأمان الجيد عند إستخدام تطبيق إدارة كلمات المرور أيضًا**. على سبيل المثال، إذا قمت بإستخدام ملحق مدير كلمات المرور على المستعرض أو قمت بتسجيل الدخول إلى Bitwarden (أو أي مدير كلمات مرور آخر) على جهاز ما، فتذكر تسجيل الخروج بعد الإستخدام إذا كنت تشارك ذلك الجهاز أو تعتقد أنك قد تكون في خطر متزايد بالتعرض لسرقة الجهاز. وهذا يتضمن تسجيل الخروج من مدير كلمات المرور الخاص بك إذا تركت الكمبيوتر أو الجهاز المحمول بدون رقابة. إذا كنت تشارك كلمات المرور عبر المنظمة، فتأكد كذلك من إبطال الوصول إلى كلمات المرور (وتغيير كلمات المرور نفسها) عندما يترك الأشخاص العمل في المنظمة. فإنك لا تريد أن يحتفظ موظف سابق بحق الوصول إلى كلمة مرور حساب Facebook الخاص بالمنظمة، على سبيل المثال.

ماذا يحدث إذا نسي شخص ما كلمة المرور الأساسية الخاصة به؟

من الضروري أن تتذكر كلمة المرور الأساسية الخاصة بك. ولن تتذكر أنظمة إدارة كلمة المرور الجيدة، مثل تلك المُوصى بها أعلاه، كلمة المرور الأساسية من أجلك أو تسمح لك بإعادة تعيينها مباشرة عبر البريد الإلكتروني بالطريقة التي تستطيع بها القيام بذلك لمواقع الويب. وهذه ميزة أمان جيدة، ولكنها تجعل من الضروري تعيين كلمة مرور أساسية يمكن تذكّرها عند إعداد مدير كلمات المرور الخاص بك. للمساعدة في هذا، وفور إنشاء حساب إدارة كلمات مرور، ضع في اعتبارك إعداد تذكير يومي لكي تستذكر كلمة المرور الأساسية.

إستخدام تطبيق إدارة كلمات المرور لمنظمتك

يمكنك تقوية ممارسات كلمات المرور لمنظمتك بالكامل وتأكد من أن جميع الموظفين الأفراد لديهم حق الوصول (ويستخدمون) تطبيق إدارة كلمات المرور عن طريق تنفيذ كلمة مرور واحدة عبر المنظمة ككل. وبدلاً من أن يقوم كل موظف بإعداد كلمة المرور الخاصة به، فكر في الاستثمار في خطة "الفريق" أو "الأعمال". على سبيل المثال، تبلغ تكلفة خطة "تنظيم الفريق" 3 دولارات أمريكية لكل مستخدم شهريًا. بإستخدام الخطة (أو خطط فرق أخرى من مديري كلمات المرور مثل 1Password)، يكون لديك القدرة على إدارة جميع كلمات المرور المشتركة عبر المنظمة. ولا توفر ميزات تطبيق إدارة كلمات المرور على مستوى المنظمة قدرًا أكبر من الأمان فحسب، بل راحة الموظفين أيضًا. ويمكنك مشاركة بيانات الاعتماد بأمان داخل تطبيق إدارة كلمات المرور نفسه مع حسابات مستخدمين مختلفة. على سبيل المثال، يوفر Bitwarden أيضًا ميزتين مريحتين من طرف إلى طرف ألا وهما النص المشفر ومشاركة الملفات تسمى "Bitwarden Send" (إرسال Bitwarden) ضمن خطة الفريق. وتقدم هاتان الميزتان لمنظمتك المزيد من التحكم فيمن يمكنه رؤية كلمات المرور ومشاركتها، وتوفر خيارًا أكثر أمانًا لمشاركة بيانات الاعتماد للحسابات على مستوى الفريق أو المجموعة. إذا قمت بإعداد تطبيق إدارة كلمات مرور على مستوى المنظمة، فتأكد من أن يكون شخص معين مسؤول بشكل خاص عن إزالة حسابات الموظفين وتغيير أية كلمات مرور مشتركة عندما يترك أي موظف الفريق.

ما المصادقة ثنائية العامل؟

بغضّ النظر عن مدى جودة كلمة المرور الخاصة بك، فمن الشائع جدًا أن يتغلّب المتسللون على كلمات المرور. ويتطلب الحفاظ على أمان الحسابات الخاصة بك من بعض جهات التهديد الشائعة حاليًا طبقة أخرى من الحماية. وهذا هو مكان إستخدام المصادقة متعددة العامل أو ثنائية العامل – يُشار إليها باسم MFA أو 2FA. هناك العديد من الأدلة والموارد الرائعة التي تشرح المصادقة ثنائية العامل، بما في ذلك مقال مصادقة ثنائية العامل للمبتدئين لـ Martin Shelton والدليل الميداني 101 للأمن السيبراني للانتخابات التابع Center for Democracy & Technology. يقتبس هذا القسم بشكل كبير من كلا هذين المصدرين للمساعدة في توضيح سبب أهمية المصادقة ثنائية العامل عند اعتمادها ضمن المنظمة. باختصار، تعمل المصادقة ثنائية العامل على تعزيز أمان الحساب عن طريق طلب معلومة ثانية – شيء ما أكثر من مجرد كلمة مرور – للوصول. عادةً ما تكون المعلومة الثانية شيئًا تمتلكه، مثل رمز من تطبيق موجود على هاتفك أو رمز مميز أو مفتاح فعلي. تكون هذه المعلومة الثانية بمثابة طبقة دفاع إضافية. إذا سرق متسلل ما كلمة المرور الخاصة بك أو تمكن من الوصول إليها من خلال تفريغ كلمات المرور من اختراق بيانات كبير، فيمكن للمصادقة الثنائية الفعالة منعه من الوصول إلى حسابك (وبالتالي يكون بعيدًا عن المعلومات الخاصة والحساسة). إن ضمان أن كل شخص في المنظمة يضع المصادقة ثنائية العامل في حسابه موضع التنفيذ يُعد أمرًا مهمًا للغاية.

كيف يمكننا إعداد المصادقة ثنائية العامل؟

هناك ثلاث طرق شائعة للمصادقة ثنائية العامل: مفاتيح الأمان وتطبيقات المصادقة رموز الرسائل القصيرة لمرة واحدة.

مفاتيح الأمان

تُعد مفاتيح الأمان الخيار الأمثل، ويرجع ذلك جزئيًا إلى أنها تكاد تكون مقاومة للتصيّد الاحتيالي بالكامل. وتُعد هذه "المفاتيح" عبارة عن رموز مميزة للأجهزة (مثل أقراص USB صغيرة) يمكن ربطها بسلسلة مفاتيح (أو البقاء في جهاز الكمبيوتر الخاص بك) لسهولة الوصول إليها وحفظها. عندما يحين وقت إستخدام المفتاح لإلغاء تأمين حساب معين، فإنك تقوم ببساطة بإدخاله في جهازك وتضغط عليه فعليًا عند مطالبتك بذلك أثناء تسجيل الدخول. وهناك مجموعة كبيرة من الطرازات التي يمكنك شراؤها عبر الإنترنت (20-50 دولارًا أمريكيًا)، بما في ذلك YubiKeys التي تحظى بتقدير كبير. تحتوي Wirecutter التابعة لـ New York Times على دليل مفيد مع وجود بعض التوصيات بشأن اختيار المفتاح المناسب. ضع في اعتبارك أنه يمكن إستخدام مفتاح الأمان نفسه لأي عدد تريده من الحسابات. في حين أن مفاتيح الأمان باهظة الثمن بالنسبة للعديد من المنظمات، توفر المبادرات مثل برنامج الحماية المتقدمة من Google أو AccountGuard من Microsoft هذه المفاتيح مجانًا لبعض المجموعات المؤهلة والمُعرضّة للخطر. اتصل بالأشخاص الذين قدموا لك الدليل لمعرفة ما إذا كان بإمكانهم إيصالك بهذه البرامج أو تواصل على cyberhandbook@ndi.org.

تطبيقات المصادقة

يُعد **ثاني أفضل خيار للمصادقة ثنائية العامل هو تطبيقات المصادقة.** تتيح لك هذه الخدمات الحصول على رمز تسجيل الدخول ثنائي العامل المؤقت من خلال تطبيق جوال أو إعلام مؤقت على هاتفك الذكي. تتضمن بعض الخيارات الشائعة والموثوقة Google Authenticator وAuthy وDuo Mobile. تُعدّ تطبيقات المُصادقة رائعة أيضًا لأنها تعمل عندما لا يكون لديك وصول إلى شبكتك الخلوية وتكون مجانية لاستخدام الأفراد. ومع ذلك، تكون تطبيقات المُصادق أكثر عُرضة للتصيّد الاحتيالي من مفاتيح الأمان لأنه يمكن خداع المستخدمين لإدخال رموز الأمان من تطبيق مصادقة إلى موقع ويب مزيف. احرص على إدخال رموز تسجيل الدخول على مواقع الويب الشرعية فقط. ولا "تقبل" إعلامات مباشرة لتسجيل الدخول إلا إذا كنت متأكدًا من أنك الشخص الذي قمت بطلب تسجيل الدخول. من الضروري أيضًا عند استخدام تطبيق المصادقة أن تكون جاهزًا لاستخدام رموز النسخ الاحتياطي (الموضحة فيما يلي) في حالة ضياع هاتفك أو سرقته.

رموز عبر الرسائل القصيرة (SMS)

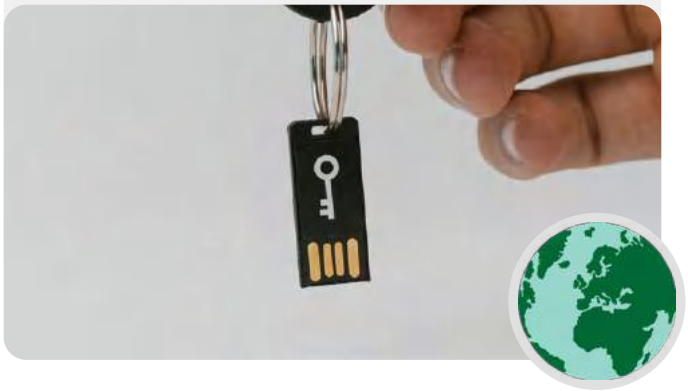
ويُعد الشكل الأقل أمانًا ولكنه الأكثر شيوعًا للمصادقة ثنائية العامل لسوء الحظ هو الرموز المرسلة عبر الرسائل القصيرة (SMS). ولأنه يمكن اعتراض الرسائل القصيرة ويمكن تزييف أرقام الهاتف أو اختراقها عبر مشغل شبكة الهاتف المحمول، تقدّم الرسائل القصيرة أقل مما هو مرغوب فيه كطريقة لطلب الرموز بالمقارنة مع المصادقة ثنائية العامل. فإنه أفضل من إستخدام كلمة مرور فقط، ولكن يُوصى باستخدام تطبيقات المصادقة أو مفتاح الأمان الفعلي عندما يكون ذلك ممكنًا. يمكن لخصم محدد الوصول إلى رموز المصادقة ثنائية العامل عبر الرسائل القصيرة، عادةً فقط عن طريق الاتصال بشركة الهاتف وتبديل بطاقة SIM الخاصة بك. عندما تكون مستعدًا لبدء تمكين المصادقة ثنائية العامل لجميع حسابات منظمتك المختلفة، استخدم موقع الويب هذا (https://2fa.directory/) للبحث بسرعة عن المعلومات والتعليمات الخاصة بخدمات معينة (مثل Gmail وOffice 365 وFacebook وTwitter وما إلى ذلك) ولمعرفة الخدمات التي تسمح بأنواع المصادقة ثنائية العامل.

المصادقة ثنائية العامل والمجتمع المدني

وفقًا لتقرير Amnesty International، استخدم المتسللون الذين يستهدفون المدافعين عن حقوق الإنسان في أوزبكستان هجمات التصيّد الاحتيالي لإستدراج المستخدمين لمشاركة كلمات المرور *و* رموز المصادقة ثنائية العامل الخاصة بحسابات البريد الإلكتروني عبر صفحات تسجيل دخول مزيفة إلى Gmail. تُعدّ هذه الهجمات طريقة شائعة بشكل متزايد "لتجاوز" المصادقة ثنائية العامل. ومن المهم – حتى مع وجود المصادقة ثنائية العامل – توخي الحذر فيما يتعلق بمكان كتابة الرموز الخاصة بك. والأفضل من ذلك أنه يمكنك القضاء على هذا الخطر من خلال مفاتيح أمان فعلية.

مفاتيح الأمان في العالم الواقعي

من خلال توفير مفاتيح أمان فعلية للمصادقة ثنائية العامل لكل الموظفين الذين يبلغ عددهم أكثر من 85،000، قامت Google (منظمة عالية الخطورة ومستهدفة للغاية) بالقضاء على أية هجمات تصيّد احتيالي ناجحة ضد المنظمة. توضح هذه الحالة مدى فاعلية مفاتيح الأمان حتى بالنسبة للمنظمات الأكثر عُرضة للخطر.



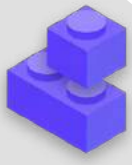
ماذا يحدث إذا فقد شخص ما جهاز المصادقة ثنائية العامل؟

في حالة إستخدام مفتاح أمان، تعامل معه بالطريقة نفسها التي تتعامل بها مع مفتاح منزلك أو شقتك، إذا كان لديك واحدًا. باختصار، لا تفقده. تمامًا مثل مفاتيح منزلك، إنه لفكرة جيدة أن يكون لديك مفتاحًا احتياطيًا مسجل في حسابك يظل مغلقًا في مكان آمن (مثل خزنة في المنزل أو صندوق ودائع آمن) فقط في حالة فقدان أو سرقة المفتاح الأوّل. وبدلاً من ذلك، يمكنك إنشاء رموز احتياطية للحسابات التي تسمح بذلك. ويجب عليك الاحتفاظ بهذه الرموز في مكان آمن جدًا، مثل تطبيق إدارة كلمات المرور الخاص بك أو في خزنة فعلية. يمكن إنشاء هذه الرموز الاحتياطية في معظم إعدادات المصادقة ثنائية العامل الخاصة بالمواقع (المكان نفسه الذي تقوم فيه بتمكين المصادقة ثنائية العامل في المقام الأول)، ويمكن أن تكون بمثابة مفتاح احتياطي في حالة الطوارئ. يقع خطأ المصادقة ثنائية العامل الأكثر شيوعًا عندما يستبدل الأشخاص هواتفهم التي يستخدمونها لتطبيقات المصادقة أو يفقدونها. وإذا كنت تستخدم Google Authenticator، فلن يحالفك الحظ إذا تمّت سرقة هاتفك، إلا إذا قمت بحفظ الرموز الاحتياطية التي يتم إنشائها في الوقت الذي تقوم فيه بتوصيل حساب بتطبيق Google Authenticator. وبالتالي، إذا كنت تستخدم Google Authenticator كتطبيق مصادقة ثنائية العامل، تأكد من حفظ الرموز الاحتياطية لجميع الحسابات التي تتصل بها في مكان آمن. أما إذا كنت تستخدم تطبيق Authy أو Duo، فإن كلا التطبيقين يحتويان على ميزات النسخ الاحتياطي المضمنة مع إعدادات أمان قوية يمكنك تفعيلها. إذا قمت باختيار أيًا من هذه التطبيقات، فإنه يمكنك تكوين خيارات النسخ الاحتياطي تلك في حالة تعطل الجهاز أو فقده أو سرقته. راجع تعليمات تطبيق Authy هنا، وتعليمات تطبيق Duo هنا. تأكد من أن يكون كل شخص في منظمتك على دراية بهذه الخطوات عند بدء تمكين المصادقة ثنائية العامل عبر جميع الحسابات.

فرض المصادقة ثنائية العامل عبر منظمتك

إذا كانت منظمتك توفر حسابات بريد إلكتروني لكل الموظفين من خلال Google Workspace (المعروف سابقًا باسم GSuite) أو Microsoft 365 بإستخدام المجال الخاص بك (على سبيل المثال، @ndi.org)، فإنه يمكنك فرض المصادقة ثنائية العامل وإعدادات أمان قوية لجميع الحسابات. لا يساعد هذا الفرض في حماية هذه الحسابات فقط، بل يعمل أيضًا كطريقة لتقديم المصادقة ثنائية العامل وتطبيعها لموظفيك حتى يكونوا أكثر راحة في تبنيها مع الحسابات الشخصية أيضًا. وبصفتك مسؤول Google Workspace، يمكنك اتباع هذه التعليمات لفرض المصادقة ثنائية العامل للمجال الخاص بك. يمكنك القيام بشيء ما مشابه في Microsoft 365 باتباع هذه الخطوات كمسؤول عن المجال.

كذلك، ضع في اعتبارك تسجيل حسابات المنظمة الخاصة بك في برنامج الحماية المتقدمة (Google) أو AccountGuard (Microsoft) لفرض ضوابط الأمان الإضافية والمطالبة بمفاتيح الأمان للمصادقة ثنائية العامل.



تأمين الحسابات

- **اطلب كلمات مرور قوية لجميع الحسابات ضمن المنظمة؛ وشجع الموظفين والمتطوعين على القيام بالشيء نفسه فيما يتعلق بحساباتهم الشخصية.**
- **قم بإستخدام تطبيق إدارة كلمات مرور موثوق للمنظمة (وشجّع إستخدامه فيما يتعلق بالحياة الشخصية للموظفين أيضًا).**
  - اطلب كلمة مرور أساسية قوية ومصادقة ثنائية العامل لجميع حسابات تطبيق إدارة كلمات المرور.
  - ذكّر الجميع بتسجيل الخروج من تطبيق إدارة كلمات المرور على الأجهزة المشتركة أو عند إزدياد خطر سرقة الجهاز أو مصادرته.
- **قم بتغيير كلمات المرور المشتركة عندما يترك الموظفون عملهم في المنظمة.**
- **لا تشارك كلمات المرور إلا بطريقة آمنة، على سبيل المثال، خلال تطبيق إدارة كلمات المرور الخاص بالمنظمة أو التطبيقات المشفّرة من طرف إلى طرف.**
- **اطلب المصادقة ثنائية العامل لجميع الحسابات التابعة للمنظمة وشجع الموظفين على إعداد المصادقة ثنائية العامل في جميع الحسابات الشخصية أيضًا.**
  - إذا أمكن ذلك، قم بتوفير مفاتيح أمان فعلية لجميع الموظفين.
  - وإذا لم تكن مفاتيح الأمان ضمن ميزانيتك، فقم بالتشجيع على إستخدام تطبيقات المصادقة بدلاً من الرسائل القصيرة أو المكالمات الهاتفية للمصادقة ثنائية العامل.
- **اعقد تدريبًا منتظمًا للتأكد من أن الموظفين على علم بكلمة المرور وأفضل ممارسات المصادقة ثنائية العامل، بما في ذلك ما يجعل كلمة المرور قوية وأهمية عدم إعادة إستخدام كلمات المرور مطلقًا وقبول طلبات المصادقة ثنائية العامل المشروعة فقط وإنشاء رموز مصادقة ثنائية العامل احتياطية.**

تأمين الأجهزة

بالإضافة إلى الحسابات، من الضروري أن تجعل جميع الأجهزة – أجهزة الكمبيوتر والهواتف ومنافذ USB ومحركات الأقراص الصلبة الخارجية وما إلى ذلك – محمية بشكل جيّد.

تبدأ هذه الحماية بالحذر فيما يتعلق بنوع الأجهزة التي تقوم منظمتك وموظفيك بشرائها وإستخدامها. يجب أن يكون لدى أي بائع أو جهة مُصنّعة قمت باختيارها سجل حافل بالالتزام بالمعايير العالمية فيما يتعلق بالتطوير الآمن للأجهزة (مثل الهواتف وأجهزة الكمبيوتر). يجب أن تشتري أجهزة صنعت بواسطة شركات موثوقة ليس لديها حافز لتسليم البيانات والمعلومات إلى خصم محتمل. وتجدر هنا الإشارة إلى أن الحكومة الصينية تُطالب الشركات الصينية بتقديم بيانات إلى الحكومة المركزية. مما يعني أنه على الرغم من انتشار هواتف ذكية غير مكلفة مثل Huawei أو ZTE، إلا أنه يجب تجنّب امتلاك واحدًا منها. فعلى الرغم من إمكانية انجذاب المنظمة لشراء جهاز رخيص، إلا أنه يجب أن تجعلك المخاطر الأمنية المحتملة تجاه المنظمات التي تدافع عن الديموقراطية أو حقوق الإنسان أو المسائلة أن تتجه نحو خيارات الأجهزة الأخرى، فالوصول إلى البيانات سهّل على الحكومة الصينية والحكومات الأخرى استهداف بعض الأفراد والمجتمعات. يمكن لخصومك تعريض أمان أجهزتك – وكل شيء تقوم به من خلال تلك الأجهزة – للخطر إما عن طريق الوصول الفعلي أو الوصول "عن بُعد" إلى جهازك.

أمان الأجهزة والمجتمع المدني

تم تطوير أكثر البرامج الضارة تقدمًا في العالم ونشرها في جميع أنحائه من أجل استهداف منظمات المجتمع المدني والمدافعين عن حقوق الإنسان. في الهند على سبيل المثال، أفادت Amnesty International أن تسعة مدافعين عن حقوق الإنسان على الأقل قد تم استهدافهم في عام 2020 بإستخدام برامج التجسس (نوع من البرامج الضارة) على الأجهزة المحمولة وأجهزة الكمبيوتر. وتم استلام برامج التجسس من خلال سلسلة رسائل البريد الإلكتروني التي تحتوي على روابط لملفات مصابة تمت مشاركتها عبر Firefox Send (برنامج مشاركة ملفات متوقف منذ ذلك الحين). وبالنسبة لأولئك المستهدفين الذين فتحوا الملفات، أصبحت أجهزتهم مصابة ببرنامج يُسجل الصوت ويعترض ضغطات المفاتيح والرسائل، وفي الواقع يضعهم المهاجمون من خلاله تحت المراقبة الكاملة. ولسوء الحظ تُعد مثل هذه الهجمات، التي غالبًا ما تستهدف مجموعات المجتمع المدني والموظفين بها، طريقة شائعة للمهاجمين للوصول إلى جهاز "عن بُعد".

الوصول الفعلي إلى جهاز جرّاء ضياعه أو سرقته

لمنع الاختراق الفعلي، من المهم الحفاظ على أمان أجهزتك فعليًا. وباختصار، لا تجعل من سرقة جهازك أو حتى الاستحواذ عليه مؤقتًا أمراً سهلاً على خصمك. قم بإيقاف تشغيل الأجهزة إذا تركتها في المنزل أو في المكتب. أو دعها تعمل ولكن احفظها معك ان كنت ترى ذلك أكثر أمانًا. وبالطبع هذا يعني أن جزءًا من أمان الجهاز هو الأمان الفعلي في مساحات العمل (سواء في المكتب أو في المنزل). وستحتاج إلى تركيب أقفال قوية وكاميرات أو أنظمة مراقبة أخرى – وبصورة خاصة إذا كانت منظمتك مُعرّضة لخطر كبير. ذّكر الموظفين بأن يتعاملوا مع الأجهزة بالطريقة نفسها التي يتعاملون بها مع مبلغ كبير من المال – ولا يتركوها دون رقابة أو حماية.

ماذا يحدث إذا تمّ سرقة جهاز؟

للحد من الضرر، في حال تمكّن شخص ما من سرقة جهاز – أو حتى إذا تمكّن من الوصول إليه لفترة زمنية قصيرة فقط – فتأكد من **فرض إستخدام كلمات مرور أو رموز مرور قوية على أجهزة الكمبيوتر والهواتف الخاصة بالجميع**. تنطبق نصائح كلمة المرور نفسها من قسم كلمات المرور لهذا الدليل على كلمة المرور الجيدة لكمبيوتر أو كمبيوتر محمول. عندما يتعلق الأمر بإغلاق هاتفك، استخدم رموزًا مكونة من ستة إلى ثمانية أرقام على الأقل وتجنب إستخدام "أنماط التمرير" لإلغاء تأمين الشاشة. للحصول على نصائح إضافية حول أقفال الشاشة، تحقق من Data Detox Kit الخاصة بمنظمة Tactical Tech. إستخدام كلمات مرور جيدة يصعّب مهمة الخصم للوصول إلى المعلومات المخّزنة على جهازك بشكل سريع في حالة السرقة أو الاستحواذ لمدة وجيزة. ومع وجود رمز مرور قوي، يمكن أن يكون تنشيط Face ID (مُعرف الوجه) أو الفتح بإستخدام بصمة الإصبع أمرًا مقبولاً، ولكن تأكد من الغاء تنشيط هذه الميزات (بينما تبقي على رمز مرورك القوي) قبل إجراء أية أنشطة عالية الخطورة مثل الاحتجاجات أو عند المرور بالمعابر الحدودية إذا كنت أنت وموظفيك قلقون بشأن مصادرة الجهاز من السلطات. إذا كانت أية أجهزة صادرة عن المنظمة تحتوي على ميزة "Find my Device" (العثور على جهازي) وميزة Find My iPhone (العثور على جهاز iPhone الخاص بي) الخاصة بنظام iPhone وميزة Find My Device الخاصة بنظام Android، ففكر في مطالبة الموظفين بتفعيلها. شجّع الموظفين على إستخدام هذه الميزات على الأجهزة الشخصية أيضًا. وعند تشغيل هذه الميزات، يمكن لمالك الجهاز (أو جهة اتصال موثوقة) تحديد موقع الجهاز أو مسح محتوياته عن بُعد في حالة السرقة أو الضياع أو المصادرة. بالنسبة لنظام iPhones، يمكنك أيضًا أعداد الجهاز ليقوم بالمسح التلقائي بعد عدة محاولات تسجيل دخول فاشلة. تصبح ميزات إدارة هذا الجهاز ذات أهمية بالغة للمنظمة عند ضياع جهاز يحتوي على معلومات حساسة أو وقوعه في الأيدي الخطأ.

ماذا عن تشفير الجهاز؟

من المهم إستخدام التشفير وتعمية البيانات بحيث تكون غير قابلة للقراءة والإستخدام على جميع الأجهزة، خاصة أجهزة الكمبيوتر والأجهزة الذكية. ويجب عليك إعداد جميع الأجهزة عبر منظمتك بما يُسمّى **تشفير القرص بالكامل** إن أمكن. وتشفير القرص بالكامل يعني أن الجهاز مُشفّر لذلك لا يكون الخصم، في حالة سرقته فعليًا، قادرًا على استخراج محتويات الجهاز دون معرفة كلمة المرور أو المفتاح الذي استخدمته لتشفيره. يتيح العديد من الهواتف الذكية الحديثة وأجهزة الكمبيوتر إمكانية التشفير الكامل للقرص. وتقوم أجهزة Apple مثل أجهزة iPhone وiPad بتشغيل تشفير القرص بالكامل بشكل ملائم تمامًا عند تعيين رمز مرور عادي للجهاز. توفر أجهزة الكمبيوتر Apple التي تستخدم نظام التشغيل mac ميزة تُسمى FileVault يمكنك تشغيلها لتشفير القرص بالكامل. تقدم أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows والتي تعمل بتراخيص احترافية أو مؤسسية أو تعليمية ميزة تُسمى BitLocker التي يمكنك تشغيلها لتشفير القرص بالكامل. يمكنك تشغيل ميزة BitLocker باتباع هذه التعليمات من Microsoft، والتي قد يلزم تمكينها أولاً بواسطة مسؤول منظمتك. إذا كان لدى الموظفين ترخيص منزلي لأجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows، فلن تتوافر ميزة BitLocker. ومع ذلك، لا يزال بإمكانهم تشغيل ميزة تشفير القرص بالكامل عن طريق الانتقال إلى "Update & Security" (التحديث والأمان) > "Device encryption" (تشفير الجهاز) ضمن إعدادات نظام التشغيل Windows.

يتم شحن الأجهزة التي تعمل بنظام التشغيل Android، بدءًا من الإصدار 9.0 وما بعده، مع تشغيل التشفير الذي يستند إلى ملف بالوضع الافتراضي. يعمل التشفير الذي يستند إلى ملف في نظام التشغيل Android بشكل مختلف من تشفير القرص بالكامل ولكن يوفر أماناً قوياً. إذا كنت تستخدم هاتف يعمل بنظام التشغيل Android جديد نسبيًا وقمت بتعيين رمز مرور، فإنه يجب تمكين التشفير المستند إلى ملف. ومع ذلك، من الجيد التحقق من إعداداتك الخاصة للتأكد فقط، خاصة إذا كان عمر هاتفك أكثر من عامين. للتحقق، انتقل إلى Settings (الإعدادات) > Security (الأمان) على جهازك الذي يعمل بنظام التشغيل Android. ضمن إعدادات الأمان، يجب عليك أن ترى مقطعًا فرعيًا "للتشفير" أو "التشفير وبيانات الاعتماد"، والذي سيشير إلى أنه إذا تم تشفير هاتفك، وإذا لم يكن الأمر كذلك، فسيتيح لك تشغيل التشفير.

بالنسبة لأجهزة الكمبيوتر (سواء التي تعمل بنظام التشغيل Windows أو Mac)، من المهم بشكل خاص وضع أية مفاتيح تشفير (يُشار إليها باسم مفاتيح الاسترداد) في مكان آمن. وتُعد "مفاتيح الاسترداد" هذه، في معظم الحالات، كلمات مرور أو عبارات مرور طويلة. وفي حالة أنك نسيت كلمة مرور جهازك العادية أو حدث شيء ما غير متوقع (مثل عُطل في الجهاز)، فإن مفاتيح الاسترداد هي الطريقة الوحيدة لاسترداد بياناتك المشفرة ونقلها، إذا لزم الأمر، إلى جهاز جديد. لذلك، عند تشغيل تشفير القرص بالكامل، تأكد من حفظ هذه المفاتيح أو كلمات المرور في مكان آمن، مثل حساب سحابة آمن أو تطبيق إدارة كلمات المرور الخاص بمنظمتك.

الوصول إلى الجهاز عن بُعد - يُعرف أيضًا باسم القرصنة

بالإضافة إلى الحفاظ على أمان الأجهزة ماديًا، فمن المهم إبقائها خالية من البرامج الضارة. تقدم لك الأداة Security-in-a-Box التابعة لشركة Tactical Tech وصفًا مفيدًا لماهية البرامج الضارة وسبب أهمية تجنبها، الأمر الذي تم تكييفه قليلاً في بقية هذا القسم.

فهم البرامج الضارة وتجّنبها

هناك العديد من الطرق لتصنيف "البرامج الضارة" (مصطلح يعني برامج خبيثة). تُعد الفيروسات وبرامج التجسس والفيروسات المتنقلة وفيروسات حصان طروادة وبرامج الاحتيال وبرامج الفدية والاختطاف المُشفر من أنواع البرامج الضارة. وتنتشر بعض أنواع البرامج الضارة عبر الإنترنت من خلال البريد الإلكتروني والرسائل النصية وصفحات الويب الضارة ووسائل أخرى. وينتشر البعض منها من خلال أجهزة مثل رقاقات ذاكرة USB يتم إستخدامها لتبادل البيانات وسرقتها. وبالرغم من أن بعض البرامج الضارة تتطلب هدفًا غير متشككاً لارتكاب خطأ، إلا أن يمكن للبعض الآخر إصابة الأنظمة الضعيفة بهدوء دون القيام بأي شيء خاطئ على الإطلاق.

وبالإضافة إلى البرامج الضارة العامة، التي يتم إصدارها على نطاق واسع وتستهدف العموم، فإنه يتم إستخدام البرامج الضارة الموجّهة للتداخل مع جهاز أو منظمة أو شبكة معينة أو التجسس عليها. يستخدم المجرمون العاديون هذه التقنيات، وكذلك الخدمات العسكرية والاستخباراتية والإرهابيون والمتحرشون عبر الإنترنت والأزواج المسيؤون والسياسيون المشبوهون.

وبغض النظر عن التسمية، كيفما يتم التوزيع، يمكن للبرامج الضارة أن تدمر أجهزة الكمبيوتر وتسرق البيانات وتدمرها وتفلس المنظمات وتنتهك الخصوصية وتُعرّض المستخدمين إلى الخطر. باختصار، البرامج الضارة خطيرة بحق. ومع ذلك، هناك بعض الخطوات البسيطة التي يمكن أن تتخذها منظمتك لحماية نفسها من هذا التهديد الشائع.

هل ستحمينا أداة مكافحة البرامج الضارة؟

لسوء الحظ، إن أدوات مكافحة البرامج الضارة ليست حلاً كاملاً. ومع ذلك، من الجيد جدًا إستخدام الأدوات الأساسية والمجانية كخط أساس. تتغير البرامج الضارة بشكل سريع جدًا، ومع وجود المخاطر في العالم الحقيقي بشكل متكرر لا يمكن أن يكون الاعتماد على أي من هذه الأدوات هو دفاعك الوحيد.

وإذا كنت تستخدم نظام التشغيل Windows، فإنه يجب عليك إلقاء نظرة على Windows Defender المدمج في النظام. لا تحتوي أجهزة الكمبيوتر التي تحتوي على نظامي التشغيل Mac وLinux على برامج مكافحة البرامج الضارة المضمنة، والأمر نفسه يحدث مع أجهزة Android وiPhone. يمكنك تثبيت أداة جيدة ومجانية مثل Bitdefender أو Malwarebytes لتلك الأجهزة (ولأجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows أيضًا). **ولكن لا تعتمد على ذلك باعتباره خط دفاعك الوحيد** لأنه لن يغطي بعض الهجمات الجديدة الأكثر استهدافًا وخطورة.

وبالإضافة إلى ذلك، كن حريصًا جدًا على تنزيل أدوات مكافحة البرامج الضارة أو أدوات مكافحة الفيروسات من مصادر مشروعة (مثل روابط مواقع الويب المذكورة أعلاه). ولسوء الحظ، توجد العديد من الإصدارات المزيفة أو المخترقة من أدوات مكافحة البرامج الضارة التي تضر أكثر مما تنفع.

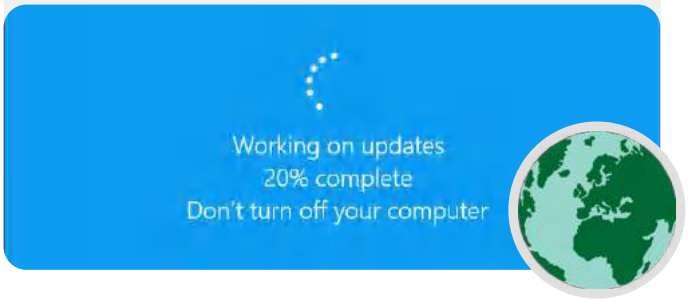
وإلى الحد الذي تستخدم فيه Bitdefender أو أداة أخرى لمكافحة البرامج الضارة عبر منظمتك، تأكد من عدم تشغيل اثنين منهما في الوقت نفسه. فإن معظم تلك البرامج تُحدد سلوك برنامج آخر لمكافحة البرامج الضارة على أنه برنامج مشبوه ويقوم بإيقافه عن العمل، مما يؤدي إلى حدوث خلل في كلا البرنامجين. يمكن تحديث Bitdefender أو برامج جيدة أخرى لمكافحة البرامج الضارة مجانًا، ويتلقى برنامج Windows Defender تحديثات مع جهاز الكمبيوتر الخاص بك. تأكد من أن تقوم برامج مكافحة البرامج الضارة بتحديث نفسها بانتظام (سيتم تعطيل بعض الإصدارات التجريبية من البرامج التجارية التي يتم شحنها مع جهاز الكمبيوتر بعد انتهاء الفترة التجريبية، مما يجعل خطورتها أكبر من فائدتها). تتم كتابة البرامج الضارة الجديدة وتوزيعها يوميًا، وسيُصبح الكمبيوتر الخاص بك أكثر عُرضة للخطر وبسرعة إذا لم تواكب تعريفات البرامج الضارة الجديدة وتقنيات مكافحة البرامج الضارة. وإذا أمكن، يجب عليك إعداد البرامج الخاصة بك لتثبيت التحديثات تلقائيًا. وإذا كانت أداة مكافحة البرامج الضارة الخاصة بك تحتوي على ميزة "always on" (تشغيل دائمًا) اختيارية، فإنه يجب عليك تفعيلها، والقيام بفحص جميع الملفات على الكمبيوتر الخاص بك، من حين الى حين.

تحديث الأجهزة باستمرار

التحديثات ضرورية. استخدم أحدث إصدار من أي نظام تشغيل يعمل على الجهاز (Windows أو Mac أو Android أو iOS وما إلى ذلك) واستمر في تحديثه. استمر كذلك في تحديث البرامج والمستعرض وأية مكونات إضافية باستمرار. قم بتثبيت التحديثات بمجرد أن تصبح متوفرة، بشكل مثالي عن طريق تشغيل التحديثات التلقائية. كلما كان نظام تشغيل الجهاز محدّثًا، قلّت نقاط الضعف لديك. اعتبر التحديثات وكأنها لاصقة طبية توضع على جرح مفتوح: فإنها تغلق إحدى نقاط الضعف وتقلل من فرصة إصابتك بالعدوى بشكل كبير. كذلك، قم بإلغاء تثبيت البرامج التي لم تعد تستخدمها. غالبًا ما يكون للبرامج القديمة مشكلات أمنية، وربما تكون قد قمت بتثبيت أداة لم يعد يتم تحديثها بواسطة المطوّر، مما يجعلها أكثر عُرضة للقراصنة.

البرامج الضارة في العالم الحقيقي: التحديثات ضرورية

في عام 2017، أصابت هجمات برنامج الفدية الضار WannaCry ملايين الأجهزة حول العالم وأغلقت المستشفيات والكيانات الحكومية والمنظمات الصغيرة والكبيرة والشركات في عشرات البلدان. لماذا كان الهجوم فعالاً جدًا؟ نظرًا لأن أنظمة تشغيل Windows تكون غير محدثة و"لم يتم تصحيح الأخطاء بها"، فقد تمّت قرصنة العديد منها في البداية. كان من الممكن تجنب الكثير من الضرر -البشري والمالي - بإستخدام الممارسات الفضلى والتحديث التلقائي وإستخدام أنظمة التشغيل المرخصة.



الحذر من أجهزة USB

كن حذرًا عند فتح الملفات التي يتم إرسالها إليك كملفات مرفقة أو من خلال روابط التنزيل أو بأي وسيلة أخرى. كذلك، **فكر مرتين قبل إدخال وسائط قابلة للإزالة مثل رقاقات USB** وبطاقات الذاكرة المحمولة وأقراص DVD والأقراص المضغوطة إلى الكمبيوتر، لأنها يمكن أن تكون أداة موجهة للبرامج الضارة. ومن المحتمل جدًا أن تحتوي أجهزة USB التي تمت مشاركتها منذ مدة على فيروسات. للحصول على خيارات بديلة لمشاركة الملفات بأمان عبر المنظمة، ألق نظرة على قسم مشاركة الملفات من هذا الدليل.

كذلك، كن حذرًا بشأن الأجهزة الأخرى التي تتصل بها من خلال Bluetooth. لا بأس بربط هاتفك أو الكمبيوتر مع مكبر صوت Bluetooth معروف وموثوق لتشغيل الموسيقى المفضلة لديك، ولكن كن حذرًا بشأن الرابط أو قبول طلبات من أية أجهزة لا تعرفها. اسمح بوصل الأجهزة الموثوقة فقط وتذكر إيقاف تشغيل Bluetooth عندما لا يكون قيد الإستخدام.

كن ذكيًا أثناء الاستعراض

لا تقبل أبدًا بتطبيقات تأتي من مواقع ويب لا تعرفها ولا تثق بها ولا تقم بتشغيلها. بدلاً من قبول "تحديث" معروض في نافذة متصفح منبثقة، على سبيل المثال، تحقق من وجود تحديثات على الموقع الرسمي للتطبيق ذي الصلة. كما ناقش قسم التصيّد الاحتيالي من هذا الدليل، من الضروري أن تظل متيقظًا عند استعراض مواقع الويب. تحقق من وجهة الروابط (عن طريق التمرير فوق الرابط) قبل نقره، وألق نظرة سريعة على عنوان موقع الويب بعد اتباع أي رابط وتأكد من أنه يبدو صحيحًا قبل إدخال معلومات حساسة مثل كلمة مرورك. لا تنقر على رسائل الخطأ أو التحذيرات، وراقب نوافذ المستعرض التي تظهر تلقائيًا واقرأها بعناية بدلاً من مجرد نقر، "نعم" أو "موافق".

ماذا عن الهواتف الذكية؟

كما هو الحال مع أجهزة الكمبيوتر، قم بتحديث نظام التشغيل والتطبيقات الموجودة على هاتفك باستمرار وقم بتشغيل التحديثات التلقائية. قم بالتثبيت فقط من مصادر رسمية أو موثوقة مثل Play Store من Google وApp Store من Apple (أو F-droid، وهو تطبيق مفتوح المصدر مجاني لنظام Android). يمكن أن تحتوي التطبيقات على برامج ضارة ولكن لا تزال تعمل بشكل طبيعي، لذلك لن تعرف دائمًا ما إذا كان أحدها ضارًا أم لا. كذلك، تأكد من تنزيل إصدار شرعي من التطبيق. فيما يخص الأجهزة التي تعمل بنظام التشغيل Android، توجد إصدارات "زائفة" من التطبيقات الشائعة. لذلك، تأكد من قيام شركة أو مطور مناسب بإنشاء التطبيق وأنه يحتوي على تقييمات جيدة وبه عدد تنزيلات متوقع (على سبيل المثال، قد يحتوي إصدار زائف من تطبيق WhatsApp على بضعة آلاف فقط من التنزيلات، لكن الإصدار الحقيقي يحتوي على تنزيلات تتعدى خمسة مليارات). انتبه إلى الأذونات التي تطلبها تطبيقاتك، إذا بدت الأذونات زائدة عن الحد (مثل آلة حاسبة تُطالب بالوصول إلى الكاميرا أو لعبة Angry Birds تطلب الوصول إلى موقعك، على سبيل المثال)، ارفض الطلب أو قم بإلغاء تثبيت التطبيق. كذلك، يمكن أن يساعد إلغاء تثبيت التطبيقات التي لم تعد تستخدمها في حماية الهاتف الذكي أو الجهاز اللوحي. أحيانًا يبيع المطورون ملكية تطبيقاتهم لأشخاص آخرين. قد يحاول هؤلاء المالكين الجدد كسب المال عن طريق إضافة تعليمات برمجية ضارة.

البرامج الضارة في العالم الحقيقي: تطبيقات الهاتف الضارة

يستخدم المتسللون في العديد من الدول تطبيقات مزيفة في متجر Google Play لتوزيع البرامج الضارة لسنوات. ظهرت حالة معينة استهدفت المستخدمين في فيتنام في أبريل، عام 2020. استخدمت حملة التجسس هذه تطبيقات زائفة، وكان من المفترض أن تساعد هذه التطبيقات المستخدمين في العثور على المقاهي القريبة أو البحث عن معلومات عن الكنائس المحلية. بمجرد تثبيتها بواسطة مستخدمي نظام التشغيل Android، جمعت التطبيقات الضارة سجلات المكالمات وبيانات الموقع والمعلومات المتعلقة بجهات الاتصال والرسائل النصية دون علمهم. وإن هذا مجرّد أحد الأسباب العديدة التي تدفعك أن تكون حذرًا فيما يتعلق بالتطبيقات التي تقوم بتنزيلها على أجهزتك.

وفر المال وقم بزيادة أمان الجهاز بإستخدام Tails لمنظمتك

يُعد نظام التشغيل Tails أحد الخيارات الآمنة التي تتطلب القليل من المهارات الفنية من أجل إعدادها. يُعد نظام التشغيل هذا مجاني للإستخدام ويمكنك تشغيله مباشرة من USB، متجاوزًا الحاجة إلى الاعتماد على نظامي التشغيل Windows أو Mac. يُعد Tails أيضًا خيارًا جيدًا لأولئك الذين يتعرضون لمخاطر عالية للغاية، حيث تشتمل على مجموعة كبيرة من الميزات المُعززة للخصوصية. تشمل هذه الميزات تكامل Tor (تمت مناقشته أدناه) لتأمين حركة الويب ومحو الذاكرة بالكامل في كل مرة تقوم فيها بإيقاف نظام التشغيل. وبشكل أساسي تسمح لك هذه الميزات بالبدء بسجل أعمال جديد في كل مرة تقوم فيها بإعادة تشغيل الكمبيوتر. كذلك، يحتوي Tails على وضع الاستمرارية الذي يسمح لك بحفظ الملفات والإعدادات المهمة عبر جلسات متعددة إذا رغبت في ذلك.

يُعد Qubes OS خيارًا آخراً لنظام تشغيل مجاني وآمن. وعلى الرغم من أنه ليس الخيار الأبسط للمستخدمين غير المتخصصين في التقنية، إلا أنه تم تصميم Qubes للحد من تهديد البرامج الضارة وإنه خيارًا آخر يجب التفكير به للمستخدمين الأكثر تقدمًا وأصحاب مستوى عالي من الخطورة في منظمتك، وخاصة إذا كانت تكاليف الترخيص تمثل تحديًا.

ماذا لو كنا لا نستطيع تحمل تكلفة البرامج المرخّصة؟

قد يكون شراء إصدارات مرخصة من البرامج الشهيرة مثل Microsoft Office (Word وPowerpoint وExcel) لكامل منظمتك أمرًا مكلفًا، ولكن الميزانية المحدودة ليست عذرًا لتنزيل إصدارات مقرصنة للبرامج أو عدم تحديثها. إنها ليست مسألة أخلاقية – بل مسألة أمن. كثيرًا ما تمتلئ البرامج المقرصنة بالبرامج الضارة وغالبًا لا يمكن إصلاح الثغرات الأمنية. إذا كنت لا تستطيع تحمل تكاليف البرامج التي تحتاجها منظمتك، فهناك مجموعة كبيرة من البرامج المجانية الرائعة مفتوحة المصدر، مثل LibreOffice (بديل لبرامج Microsoft Office الاساسية GIMP (بديل لبرنامج photoshop)، التي يمكن أن تفي باحتياجاتك. كذلك، ضع في اعتبارك التسجيل من خلال Tech Soup، وهي منظمة تقدم خصومات كبيرة على البرامج الشائعة للمنظمات غير الربحية. حتى إذا كنت تستطيع تحمل تكلفة البرامج والتطبيقات الشرعية، فلا يزال جهازك معرضًا للخطر إذا كان نظام التشغيل الأساسي غير شرعي. لذلك، إذا كانت منظمتك لا تستطيع تحمل تكاليف تراخيص Windows، فكر في بدائل أرخص مثل أجهزة كروم بوك، التي تُعد خيارًا رائعًا وسهل تأمينه إذا كانت منظمتك تعمل عبر السحابة غالبًا. إذا كنت تستخدم Google Docs أو Microsoft 365، فلن تحتاج إلى العديد من تطبيقات سطح المكتب على الإطلاق – فالمستند ومحررات جداول البيانات المجانية المضمنة في المستعرض تكون كافية جدًا لأي إستخدام تقريبًا. ويوجد خيار آخر، إذا كان لديك موظفين يتمتعون بالمهارات الفنية، ألا وهو تثبيت نظام تشغيل مبني على Linux (بديل مصدر مفتوح لأنظمة التشغيل Windows وMac) على كل كمبيوتر. ويُعد Ubuntu هو أحد خيارات Linux الشائعة وسهلة الإستخدام إلى حد ما. بغض النظر عن نظام التشغيل الذي تختاره، تأكد من أن شخصًا ما في المنظمة يكون مسؤولاً عن تسجيل الدخول بانتظام مع الموظفين للتأكد من قيامهم بتطبيق التحديثات الأخيرة.

عند اتخاذ قرار يتعلق بأداة أو نظام جديد، فكر في الكيفية التي ستقوم بها منظمتك بدعمها فنيًا وماليًا على المدى الطويل. اطرح على نفسك أسئلة مثل: هل يمكن أن تتحمل تكاليف الموظفين الضروري تواجدهم للحفاظ على أمان النظام؟ هل يمكنك الدفع مقابل الاشتراكات المتكررة؟ هل يمكنك الحصول على حسابات من مجموعات مثل TechSoup المذكورة أعلاه؟ يمكن أن يساعد الرد عن هذه الأسئلة في ضمان نجاح برامجك وإستراتيجيات التقنية بمرور الوقت.

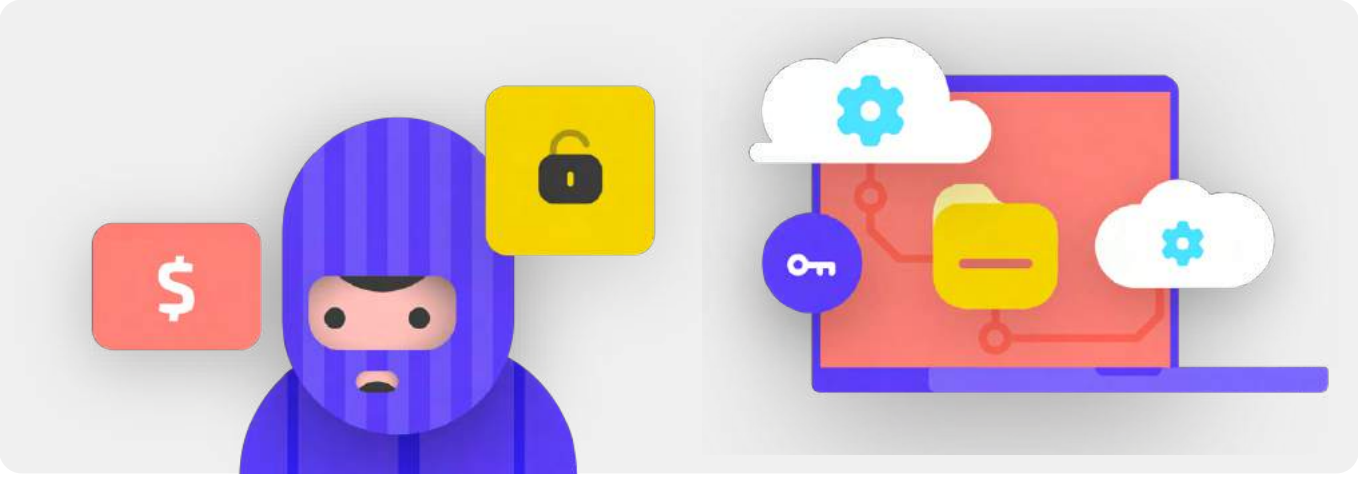
الحفاظ على أمان الأجهزة

- **قم بتدريب الموظفين على مخاطر البرامج الضارة وأفضل الممارسات لتجنبها.**
  - قم بتقديم سياسات حول توصيل الأجهزة الخارجية والنقر فوق الروابط وتنزيل الملفات والتطبيقات والتحقق من أذونات البرامج والتطبيقات.
- **افرض استمرارية تحديث الأجهزة والبرامج والتطبيقات بشكل كامل.**
  - قم بتشغيل التحديثات التلقائية كلما كان ذلك ممكنًا.
- **تأكد من أن جميع الأجهزة تستخدم برامج مرخصة.**
  - إذا كانت التكلفة باهظة، فانتقل إلى برامج بديلة مجانية.
- **اطلب حماية كلمة المرور لكافة الأجهزة داخل المنظمة، بما في ذلك الأجهزة المحمولة الشخصية التي يتم إستخدامها لإجراء اتصالات متعلقة بالعمل.**
- **قم بتمكين تشفير القرص بالكامل على الأجهزة.**
- **بشكل متكرر، ذكّر الموظفين بالحفاظ على أمان أجهزتهم فعليًا – وتعامل مع أمان مكتبك بإستخدام أقفال وطرق مناسبة لتأمين أجهزة الكمبيوتر.**
- **لا تشارك ملفات بإستخدام أجهزة USB أو لا تقم بتوصيل أجهزة USB بأجهزة الكمبيوتر الخاصة بك.**
  - بدلاً من ذلك، استخدم خيارات مشاركة ملفات آمنة بديلة.

التصيّد الاحتيالي: تهديد شائع للأجهزة والحسابات

يُعد التصيّد الاحتيالي الهجوم الأكثر شيوعًا وفاعلية على المنظمات حول العالم. ويستخدم جيوش الدول القومية الأكثر تقدمًا بالإضافة إلى المحتالين الصغار هذه التقنية.

ببساطة، يُعد التصيّد الاحتيالي محاولة الخصم خداعك لمشاركة المعلومات التي يمكن إستخدامها ضدك وضد منظمتك. ويمكن أن يحدث التصيّد الاحتيالي عن طريق رسائل البريد الإلكتروني والرسائل النصية/الرسائل القصيرة (غالبًا ما يُشار إليها باسم التصيّد الاحتيالي عبر الرسائل القصيرة "smishing") وتطبيقات المراسلة مثل WhatsApp ورسائل أو منشورات وسائل التواصل الاجتماعي أو المكالمات الهاتفية (غالبًا ما يُشار إليها باسم التصيّد الاحتيالي الصوتي "vishing"). وقد تحاول رسائل التصيّد الاحتيالي إقناعك بكتابة معلومات حساسة (مثل كلمات المرور) في موقع ويب زائف للوصول إلى حساب ما أو مطالبتك بمشاركة معلومات خاصة (مثل رقم بطاقة الائتمان) عبر الرسائل الصوتية أو النصية أو إقناعك بتنزيل برامج ضارة (برامج مخادعة) التي يمكن أن تؤثر على جهازك. وبالنسبة للأمثلة غير التقنية، يتلقى ملايين الأشخاص يوميًا مكالمات هاتفية آلية زائفة تخبرهم بأنه قد تم اختراق حسابهم البنكي أو بأنه قد تمت سرقة هويتهم - وكلها أساليب مصممة لخداع من هم ليسوا على دراية بخطورة مشاركة معلومات حساسة.



كيف يمكننا التعرف على التصيّد الاحتيالي؟

قد يبدو التصيّد الاحتيالي خبيثًا ومن غير الممكن اكتشافه، ولكن هناك بعض الخطوات البسيطة التي يمكن أن يتخذها كل شخص في منظمتك للحماية من معظم الهجمات. يتم تعديل نصائح الدفاع عن التصيّد الاحتيالي وتوسيعها من دليل التصيّد الاحتيالي المتعمق الذي طورته Freedom of the Press Foundation، ويجب مشاركتها مع منظمتك (وجهات الاتصال الأخرى) ودمجها في خطة الأمان الخاصة بك:

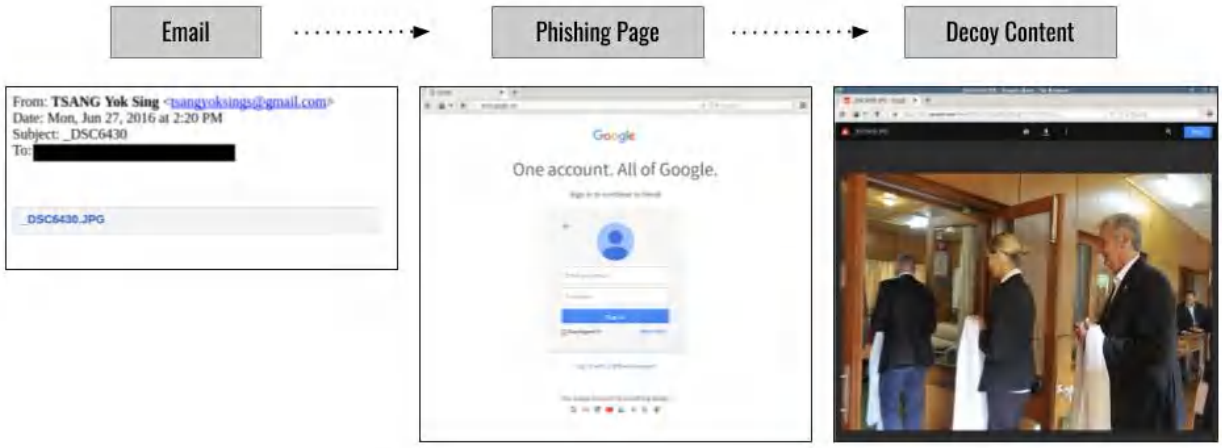
أحيانًا، يكذب الحقل "من" عليك

كن على دراية بأن الحقل "من" في رسائل البريد الإلكتروني يمكن أن يكون زائفًا أو مزورًا لخداعك. ومن الشائع بالنسبة للمخادعين قيامهم بإعداد عنوان بريد إلكتروني يشبه كثيرًا عنوانًا شرعيًا مألوفًا لك، مع تعمّد خطأ إملائيًا بسيطاً لخداعك. على سبيل المثال، قد تتلقى بريدًا إلكترونيًا من شخص ما بعنوان "john@gooogle.com" بدلاً من (john@google.com). لاحظ وجود حرف O زائد في كلمة google. كذلك، قد تعرف شخصًا ما بعنوان بريد إلكتروني "john@gmail.com"، ولكنك تستلم رسالة بريد إلكتروني للتصيّد الاحتيالي من منتحل قام بإعداد بريد إلكتروني "johm@gmail.com" - والاختلاف الوحيد هو تغيير بسيط للحرف الموجود في نهاية الاسم. تأكد دائمًا من التحقق جيدًا من عنوان إرسال البريد الإلكتروني قبل المتابعة. ينطبق مفهوم مشابه على التصيّد الاحتيالي عبر الرسائل النصية أو المكالمات أو تطبيقات المراسلة. إذا تلقيت رسالة من رقم مجهول، فكر مرتين قبل الرد على الرسالة أو التفاعل معها.

التصيّد الاحتيالي والمجتمع المدني

تستهدف هجمات التصيّد الاحتيالي الشخصية والمتطورة مجموعات المجتمع المدني يوميًا حول العالم.

تم إلقاء الضوء على أحد الأمثلة، وهو الهجوم في تقرير خاص بمعمل The Citizen Lab (معمل المواطن) لعام 2018، التجسس على الميزانية: داخل عملية تصيّد احتيالي بأهداف في المجتمع التيبتي. وكان هجوم التصيّد الاحتيالي غير المكلف للغاية والبسيط - ولكنه كان فعالاً بشكل لا يصدق - يستهدف المدافعين عن حقوق الإنسان في التبت وغيرهم من النشطاء. بدأ الهجوم برسالة بريد إلكتروني للتصيّد الاحتيالي (معروضة على اليسار) من عنوان Gmail قياسي تحتوي على رابط ملف صورة فقط. وعند النقر فوقه، ينقل الرابط الهدف إلى صفحة تسجيل دخول بريد إلكتروني زائفة (معروضة في المنتصف) تم إستخدامها لسرقة بيانات الحساب. إذا قدّم الضحايا بيانات حساباتهم إلى صفحة زائفة، فسيتم اختراقها بسهولة. وبعد تقديم اسم المستخدم وكلمة المرور إلى موقع زائف، سيتم إعادة توجيه الضحايا إلى صورة (معروضة على اليمين) تعرض المندوبين في اجتماع التبت. وقد تم تضمين الصورة كخدعة لجعل أهداف التصيّد الاحتيالي يصدقون أنهم قد قاموا بالفعل بتسجيل الدخول إلى حساب Google الحقيقي الخاص بهم ولتقليل أية شكوك محتملة حول طبيعة رسالة البريد الإلكتروني المخادعة.



الحذر من الملفات المرفقة

يمكن أن تحمل الملفات المرفقة برامج ضارة وفيروسات وعادة ما تصاحب رسائل البريد الإلكتروني التي تسعى للتصيّد الاحتيالي. **إن أفضل طريقة لتجنب البرامج الضارة من الملفات المرفقة هي عدم تنزيلها على الإطلاق.** كقاعدة عامة، لا تفتح أيّة ملفات مرفقة على الفور، خاصة إذا كانت من أشخاص لا تعرفهم. وإذا أمكن، اطلب من الشخص الذي أرسل المستند بنسخ النص ولصقه في رسالة بريد إلكتروني أو مشاركة المستند عبر خدمة مثل Google Drive أو Microsoft OneDrive، والتي تحتوي على ميزة الكشف عن الفيروسات المضمنة لمعظم المستندات التي تم تحميلها على الأنظمة السياسية. قم ببناء ثقافة تنظيمية لا تشجّع على ارسال الملفات المرفقة.
في حالة وجوب فتح الملف المرفق، فإنه يجب أن يتم فتحه في بيئة آمنة (انظر القسم متقدم أدناه) حيث يتعذر نشر البرامج الضارة على جهازك.

إذا كنت تستخدم Gmail واستلمت مرفقًا في رسالة بريد إلكتروني، فبدلاً من تنزيله وفتحه على الكمبيوتر الخاص بك، ببساطة انقر فوق الملف المرفق وقم بقراءته في "المعاينة" داخل المستعرض. تسمح لك هذه الخطوة بعرض نص الملف ومحتوياته دون تنزيله أو السماح له بتحميل برامج ضارة محتملة على الكمبيوتر الخاص بك. وتنجح هذه الخطوة في مستندات word وملفات PDF وحتى في عروض الشرائح التقديمية. إذا كنت بحاجة إلى تحرير المستند، فكر في فتح الملف في برنامج سحابة مثل Google Drive وتحويله إلى Google Doc أو Google Slides.

إذا كنت تستخدم Outlook، فإنه يمكنك بشكل مشابه معاينة الملفات المرفقة دون تنزيلها من عميل ويب Outlook. إذا كنت بحاجة إلى تحرير الملف المرفق، فكر في فتحه في OneDrive إذا كان ذلك خيارًا متاحًا لك. إذا كنت تستخدم Yahoo Mail، تنطبق الخطوات نفسها. لا تقم بتنزيل أي ملفات مرفقة، بل قم بمعاينتها من داخل مستعرض الويب.

وبغض النظر عن الأدوات التي تملكها وتحت تصرفك، فإن الطريقة الأفضل هي ببساطة عدم تنزيل الملفات المرفقة التي لا تعرفها أو لا تثق بها على الإطلاق، وبغض النظر عن مدى أهمية الملف المرفق، لا تقم أبدًا بفتح شيئًا يحتوي على نوع مستند لا تعرفه أو ليس لديك النية في إستخدامه على الإطلاق.

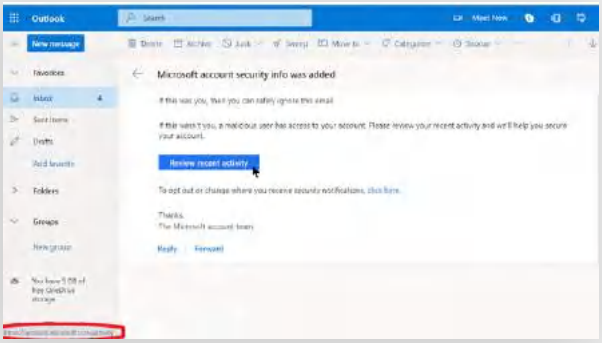
الدفاع عن منظمتك ضد التصيّد الاحتيالي

إذا كانت منظمتك تستخدم Microsoft 365 للبريد الإلكتروني والتطبيقات الأخرى، فإنه يجب على مسؤول المجال تكوين سياسة الملفات المرفقة الآمنة للحماية من الملفات المرفقة الخطيرة. إذا كنت تستخدم إصدار enterprise من Google Workspace (المعروف سابقًا باسم GSuite)، فيوجد خيارًا فعالاً مشابه يجب على المسؤول لديك تكوينه يُسمى Google Security Sandbox. وبإمكان المستخدمين الفرديين الأكثر تقدمًا التفكير في إعداد برامج معقدة لوضع الحماية، مثل Dangerzone أو، بالنسبة لأولئك الذين لديهم إصدار Pro أو Enterprise من Windows Sandbox، Windows 10.
وهناك خيار آخر متقدم يجب وضع تنفيذه عبر منظمتك في الاعتبار ألا وهو خدمة تصفية لنظام أسماء المجالات (DNS) الآمنة. يمكن للمنظمات إستخدام هذه التكنولوجيا لحظر الموظفين من الوصول إلى المحتوى الضار أو التفاعل معه عن طريق الخطأ، مما يوفر طبقة حماية إضافية ضد التصيّد الاحتيالي.
تقدم الخدمات الجديدة مثل Gateway من Cloudflare هذه الإمكانات إلى المنظمات دون الحاجة إلى إنفاق مبالغ كبيرة (فعلى سبيل المثال، Gateway مجاني لما يصل إلى 50 مستخدم). ستساعد أدوات مجانية إضافية، بما في ذلك Quad9 من Global Cyber Alliance Toolkit في حظرك من الوصول إلى المواقع المعروفة التي تحتوي على فيروسات أو برامج ضارة أخرى ويمكن تنفيذها في أقل من خمس دقائق.

النقر بحذر

كن شديد الحذر من الروابط الواردة في رسائل البريد الإلكتروني أو الرسائل النصية الأخرى. يمكن تمويه الروابط لتنزيل الملفات الضارة أو نقلك إلى مواقع زائفة قد تطلب منك تقديم كلمات المرور أو المعلومات الحساسة الأخرى. عند إستخدام كمبيوتر، توجد خدعة بسيطة للتأكد من أن الرابط الموجود في رسالة البريد الإلكتروني أو رسالة ستنقلك إلى المكان الذي من المفترض أن تنتقل إليه: استخدم فأرة الكمبيوتر للتمرير فوق أي رابط قبل النقر فوقه وانظر أسفل نافذة المستعرض لمعرفة عنوان URL الفعلي (انظر الصورة التالية).

من الصعب التحقق من الروابط الموجودة في رسالة بريد إلكتروني من جهاز محمول دون النقر فوقها دون قصد – لذا كن حذرًا. يمكنك التحقق من وجهة الرابط على معظم الهواتف الذكية بالنقر مطولاً (الضغط باستمرار) على الرابط حتى يظهر لك عنوان URL بالكامل. في التصيّد الاحتيالي عبر الرسائل القصير وتطبيقات الرسائل، تُعد الروابط المختصرة ممارسة شائعة جدًا تُستخدم لإخفاء وجهة عنوان URL. إذا رأيت رابطاً قصيرًا (على سبيل المثال، bit.ly أو tinyurl.com) بدلاً من عنوان URL الكامل، فلا تنقر فوقه. إذا كان الرابط مهمًا، انسخه في موسع عنوان URL، مثل https://www.expandurl.net/، لمعرفة الوجهة الفعلية لعنوان URL المختصر. علاوة على ذلك، لا تنقر فوق روابط إلى مواقع ويب لا تعرفها. وإذا كنت مرتابًا، قم بإجراء بحث عن الموقع، مع وضع اسم الموقع بين علامتي اقتباس (على سبيل المثال: "www.badwebsite.com") لمعرفة ما إذا كان موقعًا شريعًا أم لا. يمكنك أيضًا فتح الروابط المشكوك بها من خلال برنامج البحث عن عناوين URL من VirusTotal. وإن هذه الخطوة ليست دقيقة بنسبة 100%، ولكنها تُعد إجراءً احترازيًا جيدًا يجب اتخاذه.



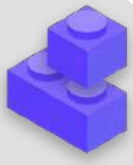
وأخيرًا، إذا قمت بالنقر فوق أي رابط من رسالة وتمت مطالبتك بتسجيل الدخول إلى شيء ما، فلا تقم بذلك إلا إذا كنت متأكدًا بنسبة 100% أن البريد الإلكتروني شرعيًا ويقوم بإرسالك إلى الموقع المناسب. ستقدم العديد من هجمات التصيّد الاحتيالي روابط تقوم بإرسالك إلى صفحات تسجيل دخول زائفة إلى Gmail أو Facebook أو مواقع شهيرة أخرى. فلا تقع فريسة لتلك الروابط. يمكنك دائمًا فتح مستعرض جديد والانتقال مباشرة إلى موقع معروف مثل Gmail.com أو Facebook.com وما إلى ذلك بنفسك إذا كنت ترغب في ذلك أو تحتاج إلى تسجيل الدخول. سينقلك ذلك أيضًا إلى المحتوى بأمان – إذا كان ذلك شرعيًا في المقام الأول.

ماذا يجب أن نفعل عندما نستلم رسالة تصيّد احتيالي إلكتروني؟

إذا استلم أي شخص في منظمتك ملفاً مرفقًا أو رابطًا أو صورة أو أية رسالة أو مكالمة مشبوهة أخرى غير مرغوب فيها، فإنه من المهم الإبلاغ عن هذا الأمر على الفور إلى مسؤول أمن تكنولوجيا المعلومات في منظمتك. إذا لم يكن لديك شخص مسؤول مثل هذا، فإنه يجب عليك التفكير في تعيينه على اعتباره جزءًا من تطوير الخطة الأمنية. كذلك، يمكن للموظفين الإبلاغ عن رسالة بريد إلكتروني على إنها بريد عشوائي أو تصيّد احتيالي في Gmail أو Outlook مباشرة.

يُعد وضع خطة لما يجب على الموظفين أو المتطوعين القيام به عندما يستلمون رسالة تصيّد احتيالي محتملة أمرًا مهم جدًا. بالإضافة إلى ذلك، نُوصي باتباع أفضل ممارسات التصيّد الاحتيالي – عدم النقر فوق روابط مشبوهة وتجنب الملفات المرفقة والتحقق من عنوان الحقل "من" – ومشاركتها مع الآخرين الذين تعمل معهم ويُفضل أن يكون ذلك من خلال قناة اتصال مستخدمة على نطاق واسع. وهذا يوضح أنك تهتم بالأشخاص الذين تتواصل معهم وتشجع الثقافة عبر شبكاتك بحيث تكون منتبهة لخطر التصيّد الاحتيالي وتدركه. يعتمد الأمان الخاص بك على تلك المنظمات التي تثق بها والعكس صحيح. تعمل الممارسات الفضلى على حماية الجميع.

بالإضافة إلى مشاركة النصائح المذكورة أعلاه مع جميع الموظفين والمتطوعين، فإنه يمكنك كذلك ممارسة التعرف على التصيّد الاحتيالي بإستخدام اختبار التصيّد الاحتيالي من Google. (اختبار التصيّد الاحتيالي من Google). كذلك، نُوصي بشدة بإعداد تدريب منتظم عن التصيّد الاحتيالي للموظفين لاختبار مستوى الوعي والحفاظ على مستوى اليقظة لدى الأشخاص. ويمكن إضفاء الطابع الرسمي على هذا التدريب كجزء من الاجتماعات التنظيمية أو عقدها بشكل غير رسمي. والمهم في ذلك التدريب أن يشعر الجميع في المنظمة بالراحة أثناء طرح الأسئلة المتعلقة بالتصيّد الاحتيالي والإبلاغ عنه (حتى إذا شعروا بأنهم ارتكبوا خطأ مثل النقر فوق رابط ما) وأن كل شخص لديه الصلاحية للمساعدة في الدفاع عن منظمتك ضد هذا التهديد عالي التأثير والاحتمالية.



التصيّد الاحتيالي

- **درّب الموظفين بانتظام على ماهية التصيّد الاحتيالي وكيفية اكتشافه والدفاع ضده، بما في ذلك التصيّد الاحتيالي في الرسائل النصية وتطبيقات المراسلة والمكالمات الهاتفية وليس رسائل البريد الإلكتروني فقط.**
- **بشكل متكرر، ذكّر الموظفين بالممارسات الفضلى مثل:**
  - لا تقم بتنزيل الملفات المرفقة غير المعروفة أو التي من المحتمل أن تكون مشبوهة.
  - تحقق من عنوان URL الخاص برابط ما قبل النقر فوقه. لا تنقر فوق الروابط غير المعروفة أو التي من المحتمل أن تكون مشبوهة.
  - لا تقدم أية معلومات حساسة أو شخصية عبر البريد الإلكتروني أو رسالة نصية أو مكالمة هاتفية إلى عناوين أو أشخاص غير معروفين أو غير مؤكدين.
- **شجّع الإبلاغ عن التصيّد الاحتيالي.**
  - قم بإنشاء آلية للإبلاغ وعيّن شخصًا بعينه يكون مسؤولاً عن التصيّد الاحتيالي داخل منظمتك.
  - خصص مكافأة عن الإبلاغ ولا تعاقب من يفشل.

توصيل البيانات وتخزينها بأمان

الاتصالات ومشاركة البيانات

لاتخاذ أفضل القرارات لمنظمتك فيما يتعلق بكيفية التواصل، من الضروري فهم أنواع مختلفة من الحماية التي يمكن أن تتمتع بها اتصالاتنا وسبب أهمية هذه الحماية.

يتعلق أكثر عناصر أمن الاتصالات أهمية بالحفاظ على خصوصية الاتصالات - التي يتم الاهتمام بها بشكل كبير في العصر الحديث عن طريق التشفير. وبدون التشفير المناسب، يمكن رؤية الاتصالات الداخلية بواسطة أي عدد من الخصوم. ويمكن أن تكشف الاتصالات عن المعلومات والرسائل الحساسة أو المربكة وتكشف عن كلمات المرور أو البيانات الخاصة الأخرى ومن المحتمل تعريض موظفيك ومنظمتك للخطر وفقًا لطبيعة الاتصالات والمحتوى الذي شاركته.

تأمين الاتصالات والمجتمع المدني

يعتمد الآلاف من نشطاء حقوق الإنسان والمنظمات الديموقراطية على قنوات الاتصالات الآمنة يوميًا للحفاظ على سرية المحادثات في البيئات السياسية الصعبة. وبدون مثل ممارسات الأمان هذه، يمكن للسلطات أعتراض الرسائل الحساسة وإستخدامها لاستهداف النشطاء وتفريق الاحتجاجات. أحد الأمثلة البارزة والموثقة جيدًا على ذلك هو ما وقع في أعقاب انتخابات عام 2010 في بيلاروسيا. وكما هو مفصل في تقرير Amnesty International هذا، اعترضت الحكومة تسجيلات الهاتف وغيرها من الاتصالات غير المشفرة واستخدمتها في المحكمة ضد السياسيين المعارضين البارزين والناشطين، الذين قضى العديد منهم سنوات في السجن. وفي عام 2020، شهدت موجة أخرى من الاحتجاجات التي تلت الانتخابات في بيلاروسيا إستخدام الآلاف من المتظاهرين تطبيقات مراسلة آمنة وسهلة الإستخدام لم تكن متاحة بسهولة قبل عشر سنوات فقط لحماية الاتصالات الحساسة.

ما التشفير وما سبب أهميته؟

يُعد التشفير عملية حسابية تُستخدم لتشفير رسالة أو ملف بحيث يمكن فقط لشخص أو كيان ما لديه المفتاح "فك تشفيره" وقراءته. يقدم دليل الدفاع الذاتي ضد المراقبة الخاص بمؤسسة Electronic Frontier Foundation شرحًا عمليًا (مع الرسومات) لما يعنيه التشفير:

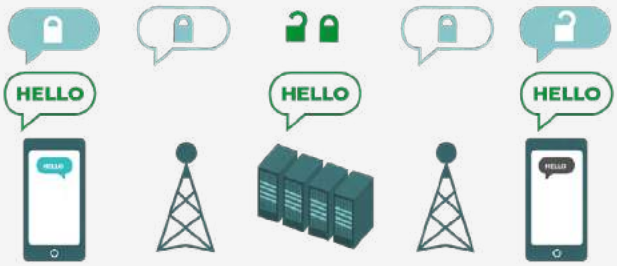
المراسلة غير المشفرة

بدون أي تشفير، يمكن لأي شخص أن يشارك في نقل الرسالة وأي شخص يمكنه رؤية الرسالة سريعًا وقراءة محتواها أثناء مرورها. وقد لا يكون هذا مهمًا إذا كان كل ما تقوله هو "مرحبًا"، ولكن قد يكون مشكلة كبيرة إذا كانت الرسالة تحتوي على شيء ما أكثر خصوصية أو حساسية لا تريد أن يراه موفر خدمة الاتصالات أو موفر خدمة الإنترنت أو حكومة غير ودية أو أي خصم آخر. ولهذا السبب، من المهم تجنب إستخدام أدوات غير مشفرة لإرسال أية رسائل حساسة (ويُفضل أية رسائل على الإطلاق). ضع في اعتبارك أن بعض طرق الاتصالات الأكثر شيوعًا – مثل الرسائل القصيرة والمكالمات الهاتفية – تعمل دون أي تشفير (مثل الصورة السابقة) عمليًا.

كما ترى في الصورة أعلاه، يرسل هاتف ذكي رسالة نصية غير مشفرة خضراء ("مرحبًا") إلى هاتف ذكي آخر في أقصى اليمين. على طول الطريق، ينقل برج الهاتف المحمول (أو في حالة إرسال شيء ما عبر الإنترنت، موفر خدمة الإنترنت، المعروف باسم ISP) الرسالة إلى خوادم الشركة. ومن هناك ينتقل عبر الشبكة إلى برج هاتف خلوي آخر يمكنه رؤية الرسالة غير المشفرة "مرحبًا"، ثم يتم توجيهها إلى الوجهة أخيرًا. من المهم ملاحظة أنه دون أي تشفير، يمكن لأي شخص أن يشارك في نقل الرسالة وأي شخص يمكنه رؤية الرسالة سريعًا وقراءة محتواها أثناء مرورها. وقد لا يكون هذا مهمًا إذا كان كل ما تقوله هو "مرحبًا"، ولكن قد يكون مشكلة كبيرة إذا كانت الرسالة تحتوي على شيء ما أكثر خصوصية أو حساسية لا تريد أن يراه موفر خدمة الاتصالات أو موفر خدمة الإنترنت أو حكومة غير ودية أو أي خصم آخر. ولهذا السبب، من المهم تجنب إستخدام أدوات غير مشفرة لإرسال أية رسائل حساسة (ويُفضل أية رسائل على الإطلاق). ضع في اعتبارك أن بعض طرق الاتصالات الأكثر شيوعًا – مثل الرسائل القصيرة والمكالمات الهاتفية – تعمل دون أي تشفير (مثل الصورة السابقة) عمليًا.

وهناك طريقتين لتشفير البيانات أثناء نقلها: ***تشفير طبقة النقل*** و***التشفير من طرف إلى طرف***. من المهم معرفة نوع التشفير الذي يدعمه مزود الخدمة لأن منظمتك تتخذ خيارات لاعتماد ممارسات وأنظمة اتصالات أكثر أمانًا. يتم وصف هذه الاختلافات جيدًا بواسطة دليل الدفاع الذاتي ضد المراقبة، والذي نعرضه بتصرف في ما يلي:

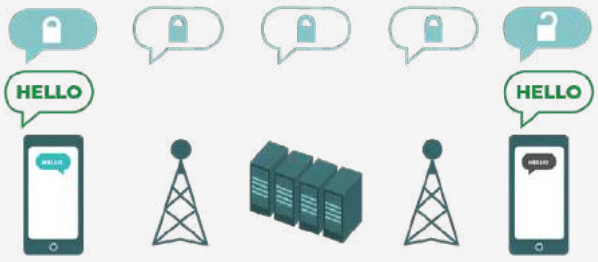
تشفير طبقة النقل



يعمل **تشفير طبقة النقل**، المعروف أيضًا باسم أمان طبقة النقل (TLS)، على حماية الرسائل أثناء انتقالها من جهازك إلى خوادم تطبيق/خدمة المراسلة ومن هناك إلى جهاز المستلم. وهذا يحميها من أعين المتسللين إلى شبكتك أو موفري خدمة الإنترنت أو الاتصالات. وعلى الرغم من ذلك، في المنتصف، يمكن لمزود خدمة المراسلة/البريد الإلكتروني أو موقع الويب الذي تستعرضه أو التطبيق الذي تستخدمه رؤية نُسخًا غير مشفرة من الرسائل الخاصة بك. ونظرًا لأنه يمكن رؤية رسائلك بواسطة خوادم الشركة (وتكون غالبًا مُخزنة عليها)، فقد تكون عُرضة لطلبات إنفاذ القانون أو السرقة إذا تم اختراق خوادم الشركة.

توضح الصورة السابقة مثالاً على تشفير طبقة النقل. على اليسار، يرسل هاتف ذكي رسالة خضراء غير مشفرة: "مرحبًا". يتم تشفير تلك الرسالة ثم تمريرها إلى برج هاتف محمول. في المنتصف، تكون خوادم الشركة قادرة على فك تشفير الرسالة وقراءة المحتوى وتحديد مكان إرسالها وإعادة تشفيرها وإرسالها إلى برج الهاتف المحمول التالي باتجاه وجهتها. في النهاية، يتلقى الهاتف الذكي الآخر الرسالة المشفرة ويفك تشفيرها ليقرأ "مرحبًا".

التشفير من طرف إلى طرف



التشفير من طرف إلى طرف يحمي الرسائل أثناء التنقل على طول الطريق من المرسل إلى المستلم. إنه يضمن أن يتم تحويل المعلومات إلى رسالة سرية من قبل المرسل الأصلي ("الطرف" الأول) ويتم فك التشفير فقط بواسطة المستلم النهائي ("الطرف" الثاني). لا يمكن لأي شخص، بما في ذلك التطبيق أو الخدمة التي تستخدمها، "الاستماع" والتنصت على نشاطك.

توضح الصورة السابقة مثالاً على التشفير من طرف إلى طرف. على اليسار، يرسل هاتف ذكي رسالة خضراء غير مشفرة: "مرحبًا". يتم تشفير تلك الرسالة ثم تمريرها إلى برج هاتف محمول ثم إلى خوادم التطبيق/الخدمة، التي يتعذر عليها قراءة المحتويات ولكنها ستنقل الرسالة السرية إلى وجهتها. في النهاية، يتلقى الهاتف الذكي الآخر الرسالة المشفرة ويفك تشفيرها ليقرأ "مرحبًا". وعلى عكس تشفير طبقة النقل، يتعذر على موفر خدمة الإنترنت أو مضيف المراسلة فك تشفير الرسالة. تحتوي نقاط النهاية فقط (الأجهزة الأصلية التي ترسل وتستقبل الرسائل المشفرة) على مفاتيح فك تشفير الرسالة وقراءتها.

ما نوع التشفير الذي نحتاجه؟

عند اختيار نوع التشفير الذي تحتاج إليه منظمتك سواء كان تشفير طبقة النقل أو التشفير من طرف إلى طرف لاتصالاتك (أو مزيج من الاثنين لأنظمة وأنشطة مختلفة)، فإن الأسئلة الكبيرة التي يجب أن تطرحها تتضمن الثقة. على سبيل المثال، هل تثق في التطبيق أو الخدمة التي تستخدمها؟ هل تثق في بنيتها الأساسية التقنية؟ هل أنت قلق بشأن احتمالية أن تجبر حكومة غير صديقة الشركة على تسليم رسائلك – وإذا كان الأمر كذلك، هل تثق في سياسات الشركة فيما يتعلق بالحماية من طلبات إنفاذ القانون؟
إذا كانت الإجابة "لا" على أي من هذه الأسئلة، فإنك تحتاج إلى تشفير من طرف إلى طرف. إذا كانت الإجابة "بنعم"، فقد تكون الخدمة التي تدعم فقط تشفير طبقة النقل كافية – ولكن من الأفضل عمومًا إستخدام الخدمات التي تدعم التشفير من طرف إلى طرف عندما يكون ذلك ممكنًا.

عند المراسلة مع مجموعات، ضع في اعتبارك أن أمان رسائلك يوازي أمان كل شخص يستلم رسائلك. بالإضافة إلى اختيار التطبيقات والأنظمة الآمنة بدقة، فمن المهم أن يتبع كل شخص في المجموعة الممارسات الفضلى الأخرى التي تتعلق بأمان الحساب وأمان الجهاز. إن كل ما يتطلبه الأمر شخص واحد لا يتبع التعليمات أو جهاز واحد مخترق لكي يتم تسريب محتويات مكالمة جماعية أو مجموعة دردشة كاملة.

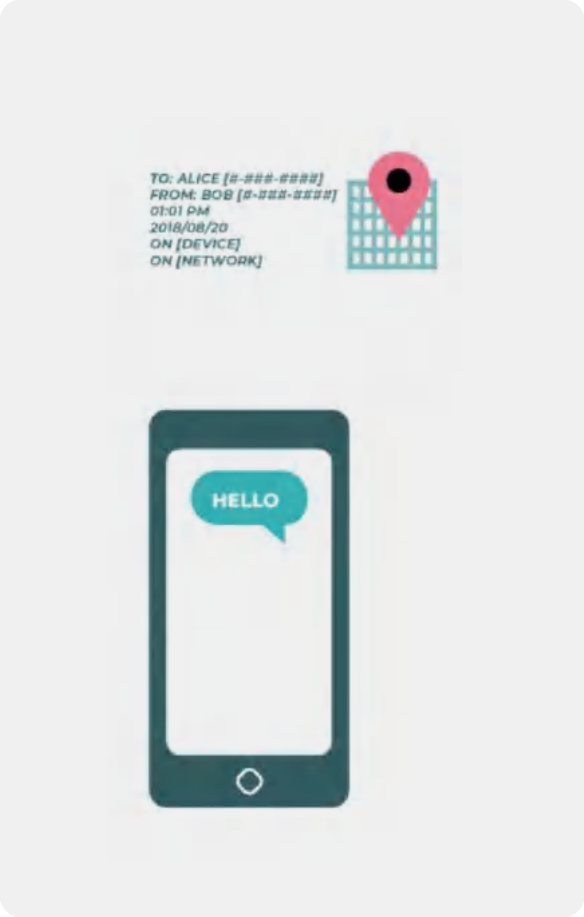
ما أدوات المراسلة المشفرة من طرف إلى طرف التي يجب أن نستخدمها (اعتبارًا من عام 2022)؟

إذا كنت بحاجة إلى إستخدام تشفير من طرف إلى طرف، أو ترغب في التكيف مع الممارسات الفضلى بغض النظر عن سياق تهديد منظمتك، فإليك بعض الأمثلة الموثوقة على الخدمات التي تقدم مكالمات ومراسلة من طرف إلى طرف **اعتبارًا من 2022**. سيتم تحديث هذا القسم من الدليل بانتظام عبر الإنترنت، ولكن يُرجى ملاحظة أن الأشياء تتغير سريعًا في عالم المراسلة الآمنة، لذلك قد تكون هذه التوصيات غير محدثة في الوقت الذي تقرأ به هذا القسم. ضع في اعتبارك أن الاتصالات الخاصة بك تكون آمنة بقدر مستوى أمان جهازك فقط. لذلك، بالإضافة إلى اعتماد ممارسات المراسلة الآمنة، من المهم تنفيذ الممارسات الفضلى المذكورة في قسم تأمين الأجهزة من هذا الدليل.

أدوات الاتصالات المشفرة من طرف إلى طرف المُوصى بها

المراسلة النصية (الفردية أو الجماعية)	• **Signal** • **WhatsApp** (فقط مع تكوينات إعدادات محددة مفصلة فيما يلي)
المكالمات الصوتية ومكالمات الفيديو	• **Signal** (يصل إلى 40 شخصًا) • **WhatsApp** (يصل إلى 32 شخصًا للرسائل الصوتية وثمانية لمكالمات الفيديو)
مشاركة الملفات	• **Signal** • **Keybase / Keybase Teams** • **OnionShare** + تطبيق مراسلة مشفر من طرف إلى طرف مثل **Signal**

ما بيانات التعريف وهل يجب أن نقلق بشأنها؟



إن معلومات مثل من الذي تتحدث إليه أنت وموظفيك ومتى وأين تتحدث معهم يمكن أن تكون حساسة مثل ما تتحدث عنه. من المهم تذكر أن التشفير من طرف إلى طرف يحمي فقط المحتويات ("ما تتحدث عنه") من اتصالاتك. وهنا يأتي دور بيانات التعريف. يقدم دليل الدفاع الذاتي ضد المراقبة من EFF نظرة عامة على بيانات التعريف وسبب أهميتها للمنظمات (بما في ذلك توضيح لما تبدو عليه بيانات التعريف):

غالبًا ما يتم وصف بيانات التعريف على أنها كل شيء باستثناء محتوى الاتصالات الخاص بك. ويمكنك التفكير في بيانات التعريف على أنها مغلّفاً رقمياً. تمامًا مثل مغلف يحتوي على معلومات حول المرسل والمستلم ووجهة الرسالة، تقوم بيانات التعريف بهذا كذلك. تُعد بيانات التعريف معلومات حول الاتصالات الرقمية التي تقوم بإرسالها واستقبالها.

تتضمن بعض أمثلة بيانات التعريف ما يلي:

- مع من تتواصل
- موضوع رسائل البريد الإلكتروني الخاصة بك
- طول محادثاتك
- الوقت الذي تحدث به المحادثة
- موقعك عند الاتصال

يمكن حتى لعينة صغيرة من بيانات التعريف أن تقدم معلومات دقيقة عن أنشطة منظمتك. فلنلقي نظرة على ما تكشف بيانات التعريف فعليًا للمتسللين والجهات الحكومية والشركات التي تجمعها:

إنهم على علم بتواصلك مع صحفي وحديثك معه قبل ساعة من نشر هذا الصحفي لقصة مع اقتباسات من مصدر مجهول. وعلى الرغم من ذلك، فإنهم يجهلون ما تحدثتم بشأنه.

إنهم يعرفون أن العديد من الموظفين داخل منظمتك قد أرسلوا رسائل إلى مدرب محلي بارز في الأمن الرقمي. ولكن لا زال موضوع الرسائل سرًا.

إنهم على علم باستلامك بريدًا إلكترونيًا من مركز خدمة اختبار كوفيد، ثم تواصلت مع الطبيب وزرت موقع ويب منظمة الصحة العالمية في الساعة نفسها. وعلى الرغم من ذلك، فإنهم لا يعلمون بمحتوى البريد الإلكتروني أو المواضيع التي تحدثت عنها عبر الهاتف.

إنهم يعرفون أنك استلمت رسالة بريد إلكتروني من مجموعة محلية للدفاع عن حقوق الإنسان بسطر عنوان "أخبر الحكومة: توقفي عن استغلال قوّتك". ولكن مازال محتوى البريد الإلكتروني غير مرئي.

إن بيانات التعريف ليست محمية بواسطة التشفير الذي تقدمه معظم خدمات الرسائل. إذا كنت ترسل رسالة على WhatsApp، على سبيل المثال، ضع في اعتبارك أنه على الرغم من محتويات رسالتك تخضع للتشفير من طرف إلى طرف، إلا أنه لا يزال من الممكن على الآخرين معرفة من تقوم بمراسلته وعدد مرات مراسلته والمكالمات الهاتفية والمدة. وكنتيجة لذلك، يجب أن تضع في اعتبارك المخاطر الموجودة (إن وجدت) إذا كان بعض الخصوم قادرين على اكتشاف مع من تتحدث منظمتك ومتى حدث ذلك و(في حالة رسائل البريد الإلكتروني) سطور الموضوع العامة لاتصالات منظمتك.

وإن أحد أسباب التوصية بإستخدام تطبيق **Signal** بشدة، بالإضافة إلى تقديم التشفير من طرف إلى طرف، هو أنه **قد قدم ميزات والتزامات بتقليل كمية بيانات التعريف التي يسجلها ويخزنها**. على سبيل المثال، تعمل ميزة Sealed Sender (المرسل المؤمن) على تشفير بيانات التعريف المتعلقة بمن يتحدث إلى من، لذلك يعرف تطبيق Signal مستلم الرسالة فقط وليس المرسل. وبالوضع الافتراضي، تعمل هذه الميزة فقط عند الاتصال بجهات اتصال حالية أو ملفات تعريف (الأشخاص) الذين تواصلت معهم بالفعل أو الذين قمت بتخزينهم في قائمة جهات الاتصال. وعلى الرغم من ذلك، يمكنك تمكين الإعداد "Sealed Sender" (المرسل المؤمن) هذا على "Allow from anyone" (السماح من أي شخص) إذا كان من المهم بالنسبة إليك التخلص من بيانات التعريف هذه عبر جميع محادثات تطبيق Signal، حتى تلك التي تحتوي على أشخاص مجهولين بالنسبة إليك.

ماذا عن البريد الإلكتروني؟

يستخدم معظم موفري البريد الإلكتروني، على سبيل المثال، Gmail وMicrosoft Outlook وYahoo Mail، تشفير طبقة النقل. لذلك، إذا كان يجب عليك توصيل محتوى حساس بإستخدام البريد الإلكتروني وكنت تشعر بالقلق من أن موفر البريد الإلكتروني الخاص بك قد يكون ملزمًا قانونيًا بتقديم المعلومات المتعلقة باتصالاتك إلى الحكومة أو أي خصم آخر، فقد ترغب في التفكير بإستخدام خيار بريد إلكتروني يخضع للتشفير من طرف إلى طرف. وعلى الرغم من ذلك، ضع في اعتبارك أنه حتى خيارات البريد الإلكتروني المشفرة من طرف إلى طرف تفتقر الى أمر مطلوب من منظور أمني، على سبيل المثال، عدم تشفير سطور الموضوع في رسائل البريد الإلكتروني وعدم حماية بيانات التعريف. إذا كنت بحاجة إلى توصيل معلومات حساسة بشكل خاص، فإن البريد الإلكتروني ليس الخيار الأمثل. وبدلاً من ذلك، اختر خيارات مراسلة آمنة مثل Signal.

إذا استمرت منظمتك في إستخدام البريد الإلكتروني، فمن المهم اعتماد نظام على مستوى المنظمة. وهذا يساعدك في الحد من المخاطر الشائعة عندما يستخدم الموظفين عنوان البريد الإلكتروني الشخصي لعملهم، مثل ممارسات أمان حساب ضعيفة. على سبيل المثال، من خلال توفير حسابات البريد الإلكتروني الصادرة عن المنظمة للموظفين، فإنه يمكنك فرض الممارسات الفضلى مثل كلمات المرور القوية والمصادقة ثنائية العامل على أية حسابات تديرها منظمتك. وإذا، وفقًا لتحليلك السابق، كان التشفير من طرف إلى طرف ضروريًا لرسالة البريد الإلكتروني، فإن كلاً من Protonmail وTutanota يقدمان خططًا للمنظمات. أمّا إذا كان تشفير طبقة النقل كافيًا للبريد الإلكتروني الخاص بالمنظمة، فإن الخيارات مثل Google Workspace (Gmail) أو Microsoft 365 (Outlook) قد تكون مفيدة.

هل يمكننا حقًا الوثوق في تطبيق WHATSAPP؟

يُعد تطبيق WhatsApp الخيار الشائع للمراسلة الآمنة، ويمكن أن يكون خيارًا جيدًا بسبب توافره في كل مكان. ويشعر بعض الأشخاص بالقلق تجاه فكرة أن تطبيق WhatsApp مملوك ومسيطر عليه بواسطة Facebook، حيث يتم العمل على دمجه مع أنظمته الأخرى. ويشعر الأشخاص بالقلق فيما يتعلق بكمية بيانات التعريف (على سبيل المثال، المعلومات الخاصة بمن تتواصل معهم ومتى) التي يجمعها تطبيق WhatsApp. إذا اخترت إستخدام تطبيق WhatsApp كخيار مراسلة آمن، فتأكد من قراءة القسم السابق الذي يتعلق ببيانات التعريف. كذلك، يوجد بعض الإعدادات التي تحتاج إلى تعيينها بشكل صحيح. الأهم من ذلك، تأكد من إيقاف تشغيل النسخ الاحتياطي عبر السحابة، أو على الأقل، قم بتمكين ميزة النسخ الاحتياطي المشفر من طرف إلى طرف الجديدة من WhatsApp بإستخدام مفتاح التشفير المكون من 64 رقمًا أو رمز مرور طويل وعشوائي وفريد محفوظ في مكان آمن (مثل تطبيق إدارة كلمات المرور الخاص بك). كذلك، تأكد من عرض إعلامات الأمان وتحقق من رموز الأمان. يمكنك العثور على أدلة إرشادية بسيطة لتكوين هذه الإعدادات للهواتف التي تعمل بنظام التشغيل Android هنا وأجهزة iPhone هنا. **إذا لم يقم موظفوك *وأولئك الذي تتواصل معهم* بتكوين هذه الخيارات بشكل صحيح، فإنه يجب عليك عدم التفكير في تطبيق WhatsApp كخيار جيد للاتصالات الحساسة التي تتطلب التشفير من طرف إلى طرف.** فلا يزال تطبيق Signal هو الخيار الأفضل لاحتياجات المراسلة المشفرة من طرف إلى طرف وذلك بسبب إعدادات الأمان الافتراضية وحماية بيانات التعريف.

ماذا عن الرسائل النصية؟

تُعد الرسائل النصية الأساسية غير آمنة إلى درجة كبيرة (الرسائل القصيرة القياسية غير مشفرة بفاعلية)، ويجب تجنبها لأي شيء غير مخصص للمعرفة العامة. وفي حين أن رسائل من جهاز iPhone إلى آخر (المعروفة باسم iMessages) من Apple مشفرة من طرف إلى طرف، فإذا كان هناك طرف ليس iPhone في المحادثة، فستكون الرسائل غير مؤمنة. من الأفضل أن تكون آمنًا **وتجنب الرسائل النصية لأي شيء حساس أو خاص أو سري.**

لماذا لا يُوصى بإستخدام TELEGRAM أو FACEBOOK MESSENGER أو VIBER لإجراء دردشات آمنة؟

تقدم بعض الخدمات، مثل Facebook Messenger وTelegram، تشفيرًا من طرف إلى طرف فقط إذا قمت بتشغيله عمدًا (وللدردشات الفردية فقط)، لذلك فإنها ليست خيارات جيدة لإرسال المعلومات الحساسة أو الخاصة، خاصة بالنسبة لمنظمة. لا تعتمد على هذه الأدوات إذا كنت بحاجة إلى إستخدام التشفير من طرف إلى طرف، لأنه من السهل جدًا نسيان تغيير الإعدادات الافتراضية الأقل أمانًا. يدعي تطبيق Viber تقديم التشفير من طرف إلى طرف، ولكنه لم يوفر الرمز للمراجعة لباحثي الأمان الخارجيين. كذلك، لم يتم توفر رمز تطبيق Telegram للتدقيق العام. وكنتيجة لذلك، يخشى الكثير من الخبراء من أن يكون تشفير تطبيق Viber (أو "الدردشات السرية" الخاصة بتطبيق Telegram) دون المستوى وبالتالي يكون غير مناسب للاتصالات التي تتطلب تشفيرًا حقيقيًا من طرف إلى طرف.

تستخدم جهات الاتصال والزملاء تطبيقات المراسلة الأخرى - كيف يمكننا إقناعهم بتنزيل تطبيق جديد للتواصل معنا؟

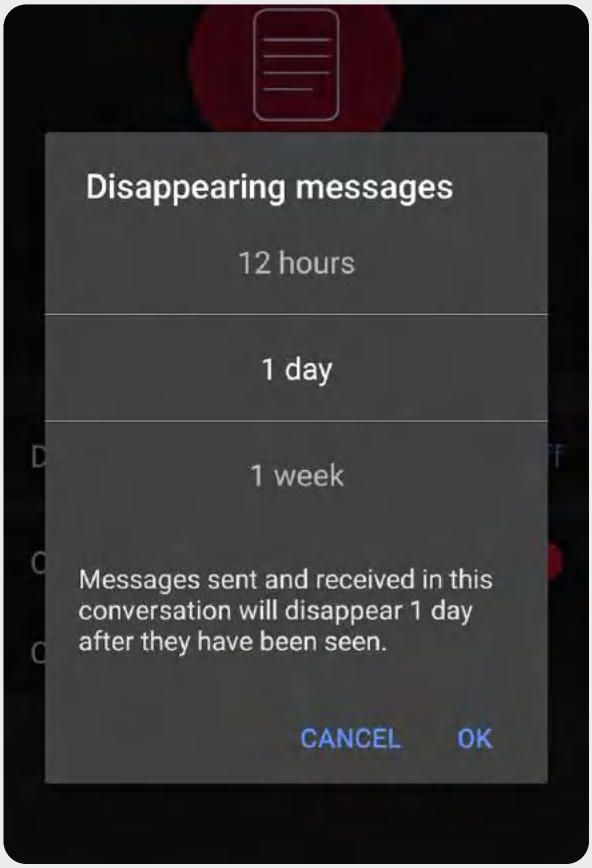
في بعض الأحيان، يكون هناك مفاضلة بين الأمان والراحة، ولكن القليل من الجهد الإضافي يستحق العناء في سبيل الحفاظ على أمان الاتصالات الحساسة. كن مثالاً جيدًا لجهات الاتصال الخاصة بك. إذا كان عليك إستخدام أنظمة أخرى أقل آمانًا، فكن واعيًا ومدركًا تمامًا لما تقوله. تجنب مناقشة الموضوعات الحساسة. بالنسبة لبعض المنظمات، قد تستخدم نظامًا واحدًا للدردشة العامة ونظامًا آخر للقيادة لإجراء المناقشات الأكثر سرية. بالطبع، من الأسهل أن يتم تشفير كل شيء تلقائيًا طوال الوقت - لا شيء لتتذكره أو تفكر فيه.

لحُسن الحظ، أصبحت التطبيقات المشفرة من طرف إلى طرف مثل Signal شائعة بشكل متزايد وسهلة الإستخدام - ناهيك عن ترجمتها إلى عشرات اللغات للإستخدام العالمي. إذا احتاج شركاؤك أو جهات اتصال أخرى المساعدة في تحويل الاتصالات إلى خيار مشفر من طرف إلى طرف مثل Signal، فاستغرق بعض الوقت للتحدث معهم حول سبب أهمية حماية اتصالاتك بشكل صحيح. عندما يفهم الجميع الأهمية، فلن تبدو الدقائق القليلة المطلوبة لتنزيل تطبيق جديد واليومين اللذين قد تحتاجهما للتعود على إستخدامه مشكلة كبيرة.

هل هناك إعدادات أخرى للتطبيقات المشفرة من طرف إلى طرف يجب أن نكون على علم بها؟

في التطبيق Signal، من المهم كذلك التحقق من رموز الأمان (التي يُشار إليها باسم أرقام الأمان). لعرض رقم الأمان والتحقق من صحته في التطبيق Signal، يمكنك فتح الدردشة الخاصة بك مع جهة اتصال، المس على الاسم في أعلى الشاشة ومرر لأسفل والمس "عرض رقم الأمان". إذا كان رقم الأمان الخاص بك يتوافق مع جهة اتصالك، فإنه يمكنك وضع علامة "تم التحقق" من الشاشة نفسها. بشكل خاص، من المهم الانتباه إلى أرقام الأمان هذه وللتحقق من جهات الاتصال الخاصة بك إذا استلمت إشعارًا في دردشة بتغيير رقم الأمان الخاص بك مع جهة اتصال معينة. إذا احتجت أنت أو أحد الموظفين المساعدة في تكوين هذه الإعدادات، يوفر التطبيق Signal نفسه إرشادات مفيدة. إذا كنت تستخدم التطبيق Signal، الذي يعتبر أفضل خيار سهل الإستخدام على نطاق واسع للمراسلة الآمنة والمكالمات الفردية، فتأكد من **تعيين رقم تعريف شخصي قوي**. استخدم على الأقل ستة أرقام ولا تكون أرقامًا سهلة التخمين مثل تاريخ ميلادك. للحصول على المزيد من النصائح حول كيفية تكوين التطبيق Signal والتطبيق WhatsApp بشكل صحيح، فإنه يمكنك التحقق من أدلة الأدوات لكل منهما المطورين بواسطة EFF في دليل الدفاع الذاتي ضد المراقبة.

إستخدام تطبيقات الدردشة في العالم الحقيقي



لتقليل الضرر في حالة ضياع هاتف أو سرقته أو مصادرته، فإن تقليل سجل الرسائل المحفوظ على هاتفك إلى الحد الأدنى يُعد الممارسة الأفضل. تتمثل إحدى الطرق السهلة للقيام بذلك في تشغيل **"الرسائل ذاتية الاختفاء"** لدردشات المنظمة الجماعية ولتشجيع الموظفين على القيام بذلك في دردشاتهم الشخصية أيضًا.

في التطبيق Signal وتطبيقات المراسلة الشائعة الأخرى، يمكنك ضبط مؤقت لإخفاء الرسائل بعد عددًا معينًا من الدقائق أو الساعات بعد القراءة. يمكن تخصيص هذا الإعداد بناءً على الدردشة الفردية أو الجماعية. وبالنسبة لمعظمنا، يمنحك تعيين نافذة تخفي لمدة أسبوع واحد متسعًا من الوقت للبحث عن الأشياء مع عدم الاحتفاظ بالرسائل التي لن تحتاجها على الإطلاق - ولكن يمكن إستخدامها ضدك مستقبلاً. تذكر أنه لا يمكن سرقة ما ليس بحوزتك.

لتشغيل الرسائل المختفية في Signal، افتح دردشة والمس اسم المجموعة/الشخص الذي تدردش معه والمس "الرسائل ذاتية الاختفاء" واختر "مؤقت" ثم المس "موافق". يوجد إعداد مشابه في تطبيق WhatsApp.

في المواقف الأكثر خطورة حيث الحاجة إلى حذف الرسائل فورًا، ربما بسبب سرقة هاتف شخص ما أو قمت بإرسال رسالة إلى الشخص الخطأ، لاحظ أن التطبيق Signal يسمح لك بحذف رسالة إلى مجموعة أو فرد من هاتف الجميع في غضون ثلاث ساعات من إرساله فقط عن طريق حذفه من الدردشة. لا يزال التطبيق Telegram شائعًا في العديد من الدول على الرغم من قيود التشفير الخاصة به لميزة مشابهة تسمح للمستخدمين بحذف الرسائل عبر الأجهزة دون قيود.

ومع ذلك، إذا كانت منظمتك مهتمة بسلامة الموظفين كنتيجة للاتصالات التي قد تتم رؤيتها على هواتفهم، فمن المحتمل أن يكون إستخدام الرسائل المختفية ذات المؤقتات القصيرة هو الخيار الأبسط والأكثر استدامة.

ماذا عن مكالمات الفيديو الجماعية الأكبر؟ هل هناك خيارات مشفرة من طرف إلى طرف؟

مع زيادة العمل عن بُعد، من المهم أن يكون لديك خيار آمن لمكالمات الفيديو الجماعية الأكبر للمنظمة. ولسوء الحظ، لا توجد خيارات رائعة حاليًا تحدد مربعات الاختيار جميعها: سهلة الإستخدام وتدعم أعدادًا كبيرة من الحضور وميزات التعاون وتمكين التشفير من طرف إلى طرف بالوضع الافتراضي.

بالنسبة للمجموعات التي تصل إلى 40 شخصًا، يُوصى بشدة بإستخدام تطبيق Signal على أنه خيار مشفر من طرف إلى طرف. يمكن الانضمام إلى مكالمات الفيديو الجماعية على Signal إما من هاتف ذكي أو تطبيق Signal لسطح المكتب على كمبيوتر، مما يسمح بمشاركة الشاشة. ومع ذلك، ضع في اعتبارك أنه يمكن إضافة جهات الاتصال الذين يستخدمون Signal بالفعل إلى مجموعة Signal فقط.

إذا كنت تبحث عن خيارات أخرى، يُعد **Jitsi Meet** نظام أضاف حديثًا الإعداد المشفر من طرف إلى طرف. يُعد Jitsi Meet حل المؤتمرات الصوتية ومؤتمرات الفيديو المستند إلى الويب الذي ينجح مع عدد كبير من الأشخاص (يصل إلى 100 شخصًا) ولا يتطلب تنزيل تطبيق أو برنامج خاص. لاحظ أنه إذا قمت بإستخدام هذه الميزة مع مجموعات كبيرة (أكثر من 15-20 شخصًا)، فقد تقل جودة المكالمة. لإعداد اجتماع على Jitsi Meet، يمكنك الانتقال إلى **meet.jit.si** واكتب رمز الاجتماع وشارك ذلك الرابط (عبر قناة آمنة مثل Signal) مع المشاركين المرغوبين. لإستخدام التشفير من طرف إلى طرف، ألق نظرة على هذه الإرشادات التي حددها Jitsi. لاحظ أن جميع المستخدمين الفرديين سيحتاجون إلى التشفير من طرف إلى طرف بأنفسهم للعمل. عند إستخدام Jitsi، تأكد من إنشاء أسماء غرف اجتماعات عشوائية واستخدام رموز مرور قوية لحماية المكالمات.

إذا لم ينجح هذا الخيار في منظمتك، فإنه يمكنك التفكير في إستخدام خيار تجاري شائع مثل Webex أو Zoom مع تمكين التشفير من طرف إلى طرف. سمح Webex بالتشفير من طرف إلى طرف؛ ومع ذلك، لا يتم تشغيل هذا الخيار افتراضيًا ويُطالب المشاركين بتنزيل Webex للانضمام إلى اجتماعك. للوصول إلى الخيار المشفر من طرف إلى طرف لحساب Webex، فإنه يجب عليك فتح حالة دعم Webex واتباع هذه الإرشادات لضمان تكوين التشفير من طرف إلى طرف. يحتاج مضيف الاجتماع فقط إلى تمكين التشفير من طرف إلى طرف. إذا قام بذلك، فإنه سيتم تشفير الاجتماع بالكامل. إذا كنت تستخدم Webex لتأمين اجتماعات وورش عمل جماعية، تأكد أيضًا من تمكين رموز مرور قوية على المكالمات.

بعد شهور من الآراء السلبية، عمل تطبيق Zoom على تطوير خيار التشفير من طرف إلى طرف للمكالمات. ومع ذلك، لا يتم تشغيل ذلك الخيار بالوضع الافتراضي، ويتطلب أن يربط مضيف المكالمة الحساب برقم الهاتف، ويعمل فقط إذا انضم جميع المشاركين إلى تطبيق Zoom لسطح المكتب أو للهاتف المحمول بدلاً من الاتصال. لأنه من السهل تكوين هذه الإعدادات بالخطأ عن غير قصد، فليس من الذكاء الاعتماد على تطبيق Zoom كخيار مشفر من طرف إلى طرف. ومع ذلك، إذا كان التشفير من طرف إلى طرف مطلوبًا وتطبيق Zoom هو الخيار الوحيد لديك، فإنه يمكنك اتباع الإرشادات الخاصة بالتطبيق Zoom لتكوينه. فقط تأكد من التحقق من أية مكالمة قبل البدء لضمان أنها مشفرة من طرف إلى طرف بالنقر فوق القفل الأخضر الموجود في الزاوية اليسرى العلوية لشاشة تطبيق Zoom ورؤية عبارة "طرف إلى طرف" بجانب إعداد التشفير. كذلك، يجب عليك تعيين رمز مرور قوي لأي اجتماع على تطبيق Zoom.

بالإضافة إلى الأدوات المذكورة أعلاه، يلقي المخطط الانسيابي هذا المطور بواسطة Frontline Defenders الضوء على بعض خيارات مكالمات الفيديو والمؤتمرات التي قد تكون منطقية لمنظمتك وفقًا لسياق المخاطر الخاص بك.

ومع ذلك، تجدر الإشارة إلى أن هناك ميزات شائعة معينة من الأدوات المذكورة أعلاه تعمل مع تشفير طبقة النقل فقط. على سبيل المثال، يعمل تشغيل التشفير من طرف إلى طرف في Zoom على تعطيل الغرف الفرعية وإمكانات الاستطلاع والتسجيل عبر السحابة. في Jitsi Meet، يمكن للغرف الفرعية تعطيل ميزة التشفير من طرف إلى طرف، مما يؤدي إلى انخفاض غير مقصود في مستوى الأمان.

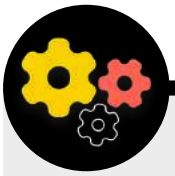
ماذا لو كنا حقًا لا نحتاج إلى التشفير من طرف إلى طرف لجميع اتصالاتنا؟

إذا لم يكن التشفير من طرف إلى طرف مطلوبًا لجميع الاتصالات الخاصة بمنظمتك استنادًا إلى تقييم المخاطر، فإنه يمكنك التفكير بإستخدام التطبيقات المحمية بواسطة تشفير طبقة النقل. تذكر أن هذا النوع من التشفير يتطلب منك أن تثق بموفر الخدمة، مثل Google لـ Gmail أو Microsoft لـ Outlook/Exchange أو Facebook لـ Messenger، لأنه يمكن أن يرى أو يسمع اتصالاتك (وأي شخص قد يضطر إلى مشاركة المعلومات معك). مرة أخرى، ستعتمد الخيارات الأفضل على نموذج التهديد الخاص بك (على سبيل المثال، إذا كنت لا تثق في Google أو إذا كانت حكومة الولايات المتحدة الأمريكية هي خصمك، فلا يُعد Gmail خيارًا جيدًا)، ولكن تشمل بعض الخيارات الشائعة والموثوقة:

البريد الإلكتروني	• **Gmail (عبر Google Workspace)** • **Outlook (عبر Office 365)** • لا تستضيف خادم Microsoft Exchange الخاص بك للبريد الإلكتروني للمنظمة. إذا كنت تقوم بذلك حاليًا، فإنه يجب عليك الترحيل إلى Office 365.
المراسلة النصية (الفردية أو الجماعية)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
المؤتمرات الجماعية، المكالمات الصوتية ومكالمات الفيديو	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
مشاركة الملفات	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**

ملاحظة حول مشاركة الملفات

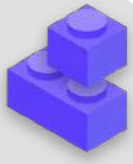
بالإضافة إلى مشاركة الرسائل بأمان، من المحتمل أن تكون مشاركة الملفات بأمان جزءًا مهمًا من خطة أمان منظمتك. إن معظم خيارات مشاركة الملفات مضمنة في تطبيقات أو خدمات المراسلة التي قد تستخدمها بالفعل. على سبيل المثال، تُعد مشاركة الملفات عبر تطبيق Signal خيارًا رائعًا إذا كنت تحتاج إلى التشفير من طرف إلى طرف. أما إذا كان تشفير طبقة النقل كافيًا، فقد يكون إستخدام Google Drive أو SharePoint خيارًا جيدًا لمنظمتك. تأكد فقط من تكوين إعدادات المشاركة بشكل صحيح حتى يتمكن الأشخاص المناسبون فقط من الوصول إلى مستند أو مجلد معين، وتأكد من أن هذه الخدمات متصلة بحسابات البريد الإلكتروني للموظفين الخاصة بالمنظمة (وليست الشخصية). إذا استطعت، احظر مشاركة الملفات الحساسة عبر مرفقات البريد الإلكتروني أو ماديًا بإستخدام منافذ USB. يعمل إستخدام أجهزة مثل أجهزة USB داخل منظمتك بشكل كبير على زيادة احتمالية وجود برامج ضارة أو سرقة ويعمل الاعتماد على البريد الإلكتروني والأشكال الأخرى من الملفات المرفقة على إضعاف دفاع منظمتك ضد هجمات التصيّد الاحتيالي.



البدائل التنظيمية لمشاركة الملفات

إذا كنت تبحث عن خيار مشاركة ملفات آمن لمنظمتك غير مضمن مباشرةً في النظام الأساسي للمراسلة (أو ربما تكون قد وصلت إلى حدود حجم ملف عند مشاركة مستندات كبيرة)، ففكر في OnionShare. يُعد **OnionShare** أداة مصدر مفتوح تسمح لك بمشاركة ملف بأي حجم بشكل آمن ومجهول. إنه يعمل عندما يقوم المرسل بتنزيل التطبيق OnionShare (المتوفر على الأجهزة التي تعمل بنظام Mac وWindows وLinux)، وتحميل الملف (الملفات) الذي يرغب في مشاركته وإنشاء رابط فريد. بعد ذلك، يمكن مشاركة هذا الرابط، الذي لا يمكن معالجته إلا في مستعرض Tor، عبر أي قناة مراسلة آمنة (Signal، على سبيل المثال) إلى المستلم المقصود. يمكن للمستلم بعد ذلك فتح الرابط في المستعرض Tor وتنزيل الملف (الملفات) على جهاز الكمبيوتر. ضع في اعتبارك أن الملفات آمنة فقط مثل الطريقة التي تشارك من خلالها الرابط. سيتم التحدث عن Tor بمزيد من التفصيل في القسم "متقدم" اللاحق من هذا الدليل، ولكن لأغراض مشاركة الملفات داخل منظمتك، ضع OnionShare في اعتبارك كبديل أكثر أمانًا لمشاركة الملفات الكبيرة على أجهزة USB في أرجاء المكتب إذا لم يكن لديك خيار موفر تخزين سحابي موثوق.

إذا كانت منظمتك تستثمر بالفعل في برنامج إدارة كلمات مرور، كما هو موضح في هذا القسم من الدليل المتعلق بكلمات المرور، واختارت حساب Premium Bitwarden أو حساب Bitwarden المخصص للفرق، تُعد الميزة **Bitwarden Send** خيارًا آخر لمشاركة الملفات بأمان. تتيح هذه الميزة للمستخدمين إنشاء روابط آمنة لمشاركة الملفات المشفرة عبر أي قناة مراسلة آمنة (مثل Signal). إن أقصى حجم للملف 100 ميجا بايت، ولكن يسمح لك Bitwarden Send بتعيين تاريخ انتهاء صلاحية الروابط وتحمي كلمة المرور الوصول إلى الملفات المشتركة والحد من عدد المرات التي يمكن فيها فتح الرابط بها.



توصيل البيانات ومشاركتها بأمان

- **اطلب إستخدام خدمات المراسلة المشفرة من طرف إلى طرف الموثوقة للاتصالات الحساسة لمنظمتك (ولجميع الاتصالات بشكل مثالي).**
  - استغرق الوقت اللازم لتشرح للموظفين والشركاء الخارجيين سبب أهمية الاتصالات الآمنة؛ وسيعمل هذا على تعزيز نجاح خطتك.
- **ضع سياسة فيما يتعلق بالمدة التي ستحتفظ بها بالرسائل وعند/إذا كانت المنظمة ستستخدم الاتصالات "المخفية" أم لا.**
- **تأكد من وجود الإعدادات المناسبة لتطبيقات الاتصالات المؤمنة، بما في ذلك:**
  - تأكد من أن جميع الموظفين يهتمون بإعلامات الأمان ولا يقومون بنسخ الدردشات إذا كانوا يستخدمون التطبيق WhatsApp.
  - إذا كنت تستخدم تطبيقًا لا يتم به تمكين التشفير من طرف إلى طرف بالوضع الافتراضي (على سبيل المثال Zoom أو Webex)، فتأكد من قيام المستخدمين المطلوبين بتشغيل الإعدادات المناسبة في بداية أي اجتماع أو مكالمة.
- **استخدم خدمات البريد الإلكتروني المستندة إلى السحابة مثل Office 365 أو Gmail لمنظمتك.**
  - لا تحاول استضافة خادم البريد الإلكتروني الخاص بك.
  - لا تسمح للموظفين بإستخدام حسابات البريد الإلكتروني الشخصية للعمل.
- **ذكّر المنظمة بأفضل ممارسات الأمان المتعلقة بالمراسلة الجماعية وبيانات التعريف باستمرار.**
  - كن على علم بمن يتواجد في الرسائل الجماعية والدردشات وسلاسل البريد الإلكتروني.

تخزين البيانات بأمان

بالنسبة لمعظم منظمات المجتمع المدني، فإن أحد أهم القرارات التي يجب اتخاذها هو اختيار مكان تخزين البيانات.

هل يُعد تخزين البيانات على أجهزة الكمبيوتر الخاصة بالموظفين "أكثر أمانًا" أم على خادم محلي أم على أجهزة تخزين خارجية أم على سحابة؟ في نسبة 99 بالمائة من الحالات، يكون الخيار الأسهل والأكثر أمانًا هو تخزين البيانات بإستخدام خدمات تخزين موثوقة عبر السحابة. وربما من الأمثلة الأكثر شيوعًا هو Microsoft 365 وGoogle Drive. ولكن بدون خطة تخزين شاملة عبر السحابة، فمن المحتمل أن يتم تخزين بيانات منظمتك في أماكن متعددة – بما ذلك أجهزة الكمبيوتر الخاصة بالموظفين، ومحركات الأقراص الصلبة الخارجية وحتى القليل من الخوادم المحلية. وعلى الرغم من احتمالية تأمين البيانات المخزنة على جميع تلك الأجهزة، إلا أنه يصعب القيام بذلك بنجاح دون إنفاق مبلغًا كبيرًا وتعيين موظفين متخصصين في تكنولوجيا المعلومات.

عند تحديد أداة أو خدمة لتخزين البيانات، تأكد من أنك تثق في الشركة أو المجموعة المعنية. يمكن لإجراء بحث سريع والتحقق من خبراء الأمن الرقمي تقديم المساعدة إليك بشكل كبير في التحقق من مصداقية بائع التقنية المحتمل. تتضمن بعض الأسئلة التي يجب وضعها في الاعتبار ما يلي: هل يبيع بياناتك الخاصة أو يشاركها؟ هل لديه مصادر أمان مناسبة للموظفين؟ هل يقدم ميزات أمان (مثل المصادقة ثنائية العامل) لمساعدتك في حماية حسابك؟

تخزين البيانات والمجتمع المدني

أدى ظهور تخزين البيانات المستندة إلى السحابة ذات التكلفة اليسيرة (مجانية أحيانًا) إلى تسهيل الحياة على العديد من منظمات المجتمع المدني محدودة الموارد (وجعلها أكثر أمانًا). ولسوء الحظ، لا يزال الكثيرون يحاولون استضافة خوادمهم الخاصة بإستخدام ميزانية محدودة لتكنولوجيا المعلومات محدودة وتعيين الموظفين والدعم التقني. في مارس 2021، أصبح تهديد البنية التحتية التنظيمية حقيقيًا بالنسبة لعشرات الآلاف من المنظمات المنتشرة في جميع أنحاء العالم، وذلك عندما أطلقت جهة تهديد تابعة للحكومة الصينية، تدعى هافنيوم، العنان لكارثة عالمية للأمن السيبراني بهجوم معقد على خوادم Microsoft Exchange ذاتية الاستضافة. وقد شمل الهجوم خوادم محلية، مما مكّن المتسللين من الولوج إلى حسابات البريد الإلكتروني للمنظمات وتثبيت برامج ضارة إضافية على خوادم ضحاياهم والأنظمة المتصلة بها والوصول في نهاية الأمر إلى استخراج بيانات حساسة. وبمجرد ظهور الاختراقات علنًا، سارعت Microsoft (مايكروسوفت) في نشر تحديث وتعليمات من شأنها تحديد المخترقين المحتملين والتخلص منهم، ولكن افتقرت العديد من المنظمات إلى قدرة تكنولوجيا المعلومات لتطبيق هذه التحديثات بسرعة، مما تركها عُرضة لهذه الاختراقات لفترة أطول. كشف نطاق وتأثير هذا الاختراق العالمي عن خطر اختيار المنظمات المدنية خوادم بريد إلكتروني ذاتية الاستضافة وغيرها من البيانات الحساسة، خاصة دون استثمار كبير في موظفي الأمن السيبراني المتخصص.

فوائد التخزين عبر السحابة

حتى إذا قمت باتخاذ جميع الخطوات الصحيحة لحماية أجهزة الكمبيوتر من البرامج الضارة والسرقة الفعلية، لا يزال قيام خصم محدد بالتسلل إلى الكمبيوتر أو الخادم المحلي أمرًا يمكن حدوثه. لكن يصعب عليهم هزيمة الدفاعات الأمنية لـ Google أو Microsoft. على سبيل المثال. تمتلك الشركات الجيدة للتخزين عبر السحابة موارد أمان لا مثيل لها وكما لديها الحافز التجاري القوي لتوفير أقصى مستويات الأمان لمستخدميها. باختصار: ستكون إستراتيجية التخزين عبر السحابة الموثوقة أسهل بكثير في التنفيذ وتحافظ على الأمان بمرور الوقت. لذلك، بدلاً من القلق فيما يتعلق بمحاولة تأمين حاسوبك الخادم الخاص بك، يمكنك تركيز طاقتك على عدد قليل من المهام الأكثر بساطة. يساعد جمع معلوماتك عبر السحابة فيما يتعلق بمجموعة من المخاطر الشائعة. هل ترك شخص ما الكمبيوتر الخاص به في مطعم أو ترك هاتفه في الحافلة؟ هل قام طفلك بسكب كوبًا من العصير على لوحة المفاتيح مما تسبب في تعطيل جهازك؟ هل يعاني موظف من وجود برامج ضارة ويحتاج إلى مسح ما يوجد على جهاز الكمبيوتر والبدء من جديد؟ إذا كانت معظم المستندات والبيانات على السحابة، فمن السهل إعادة المزامنة والبدء من جديد على جهاز كمبيوتر نظيف أو جديد تمامًا. كذلك، إذا دخلت البرامج الضارة على كمبيوتر أو إذا قام لص بمسح محرك الأقراص الصلبة، فلن يجد شيئًا لسرقته إذا كان يتم الوصول إلى معظم المستندات من خلال مستعرض الويب.

ما موفر خدمة التخزين عبر السحابة الذي يجب أن نختاره؟

يُعد أشهر خيارين للتخزين عبر السحابة هما Google Workspace (يُعرف مسبقًا باسم GSuite) وMicrosoft 365. إذا كنت أنت وموظفيك تستخدمون بالفعل Gmail، فإن تسجيل منظمتك في Google Workspace وتخزين البيانات على Google Drive، من خلال تطبيقات Docs وSheets وSlides المضمنة في Google لمعالجة الكلمات وجداول البيانات والعروض التقديمية، يُعد أمرًا منطقيًا للغاية. وبالمثل، إذا كنت منظمة تعتمد على Excel وWord، فالخيار السهل هو التسجيل في Microsoft 365، الذي يمنح منظمتك حق الوصول إلى Outlook للبريد الإلكتروني والإصدارات المرخصة من Microsoft Word وExcel وPowerpoint وTeams. بغض النظر عن الموفر الذي تختاره، فإن تخزين البيانات بأمان عبر السحابة يتطلب تنفيذ إعدادات مشاركة جيدة وتدريب الموظفين لفهم كيفية مشاركة المجلدات والمستندات ومتى يمكن مشاركتها (ومتى لا يجب مشاركتها). وبشكل عام، يجب عليك إعداد المجلدات داخل محرك التخزين عبر السحابة الذي يحد الوصول ولا يسمح إلا للموظفين الذين يحتاجون إلى ملفات معينة. بشكل روتيني، راجع نظامك للتأكد من أنك لا "تُفرط في مشاركة" أية ملفات (مثل تشغيل مشاركة الرابط العام للملفات بحيث يجب أن يقتصر الوصول إليها على عدد قليل فقط من الأشخاص).

ماذا لو لم نثق في GOOGLE أو MICROSOFT أو موفري خدمة التخزين عبر السحابة الآخرين؟

إذا كان بإمكان أحد خصومك (على سبيل المثال، حكومة أجنبية أو محلية) إجبار Google أو Microsoft (أو موفر خدمة التخزين عبر السحابة آخر) على تسليم البيانات، فحينها لن يكون اختيارهم كخيارات تخزين بيانات أمرًا منطقيًا. قد تمثل الخطورة درجة أعلى إذا كان خصمك هو حكومة الولايات المتحدة الأمريكية، على سبيل المثال، ولكن تكون الخطورة أقل إذا كان خصمك نظامًا استبداديًا. ضع في اعتبارك أن لدى Google وMicrosoft سياسات فيما يتعلق بتسليم البيانات فقط عندما تكون ملزمة قانونيًا بالقيام بذلك، وكن على علم بأن منظمتك نفسها يمكن أن تكون عُرضة لنفس النوع من الطلبات القانونية من حكومتك إذا استضافت البيانات محليًا. في الحالات التي لا يكون فيها التخزين عبر السحابة بإستخدام Google أو Microsoft مفيدًا لمنظمتك، ضع خيار Keybase في اعتبارك كخيار بديل. تسمح الميزة "teams" في Keybase لمنظمتك بمشاركة الملفات والرسائل بإستخدام التشفير من طرف إلى طرف في بيئة سحابية آمنة دون ضرورة الاعتماد على موفر جهة أخرى. ونتيجة لذلك، يمكن أن يكون خيارًا جيدًا لتخزين المستندات والملفات بأمان عبر منظمتك. وعلى الرغم من ذلك، يُعد Keybase خيارًا غير مألوف بشكل كبير لمعظم المستخدمين، لذا اعلم أن التكيف مع هذه الأداة قد يتطلب وقت تدريب أطول والمزيد من الجهد بالمقارنة مع الحلول الأخرى المذكورة سابقًا. ومع ذلك، إذا اخترت القيام بذلك بمفردك ولا تستخدم التخزين عبر السحابة على الإطلاق، فمن المهم أن تستثمر الوقت والموارد في تقوية الدفاعات الرقمية بأجهزة منظمتك، والتأكد من تكوين أية خوادم محلية بشكل صحيح وتشفيرها وتأمينها فعليًا. يمكنك التوفير في رسوم الاشتراك الشهري، ولكن ستتحمل منظمتك تكاليف من وقت الموظفين والموارد وستكون منظمتك أكثر عُرضة للهجوم.

نسخ البيانات احتياطيًا

سواء كانت منظمتك تقوم بتخزين البيانات على أجهزة فعلية أو عبر السحابة، فمن المهم أن يكون لديك نسخة احتياطية. وضع في اعتبارك أنه إذا كنت تعتمد على التخزين الفعلي على الجهاز، فمن السهل جدًا أن تفقد حق الوصول إلى بياناتك. قد تسكب القهوة

على الكمبيوتر وتدمر محرك الأقراص الصلبة. يمكن اختراق أجهزة الكمبيوتر الخاصة بالموظفين وإغلاق تأمين جميع الملفات المحلية بإستخدام برامج الفدية الضارة. قد يفقد شخص ما جهاز في القطار أو يُسرق منه مع حقيبته. وكما ذكرنا سابقًا، يُعد هذا سببًا آخر لأهمية إستخدام التخزين عبر السحابة، لأنه غير مرتبط بجهاز معين يمكن إصابته أو ضياعه أو سرقته. تأتي الأجهزة التي تعمل بنظام Mac مع برنامج النسخ الاحتياطي المضمن يسمى Time Machine الذي يتم إستخدامه مع جهاز تخزين خارجي؛ وبالنسبة للأجهزة التي تعمل بنظام التشغيل Windows، يقدم File History (محفوظات الملفات) وظيفة مشابهة. يمكن لأجهزة iPhone وAndroid أن تنسخ تلقائيًا المحتويات الأكثر أهمية عبر السحابة إذا تم تمكين ذلك ضمن إعدادات الهاتف. إذا كانت منظمتك تستخدم التخزين عبر السحابة (مثل Google Drive)، فإن مستوى خطورة إزالة Google أو تدمير بياناتك في كارثة منخفض للغاية، لكن الخطأ البشري (مثل حذف الملفات المهمة عن طريق الخطأ) لا يزال أمرًا محتمل الحدوث. قد يكون استكشاف حل النسخ الاحتياطي عبر السحابة Backupify أو SpinOne Backup حلاً جديرًا بالاهتمام. إذا تم تخزين البيانات على خادم محلي و/أو الأجهزة المحلية، يصبح النسخ الاحتياطي الآمن أمرًا مهمًا للغاية. يمكنك نسخ بيانات منظمتك احتياطيًا على محرك أقراص صلبة خارجي، ولكن تأكد من تشفير محرك الأقراص الصلبة هذا بإستخدام كلمة مرور قوية. يمكن لبرنامج Time Machine تشفير محركات الأقراص الصلبة لك، أو يمكنك إستخدام أدوات تشفير موثوقة لمحرك الأقراص الصلبة بالكامل مثل VeraCrypt أو BitLocker. تأكد من الاحتفاظ بأية أجهزة نسخ احتياطي في موقع منفصل عن أجهزتك وملفاتك الأخرى. تذكر، أن النيران التي دمرت كلاً من أجهزة الكمبيوتر والنسخ الاحتياطية تعني أنه ليس لديك نسخ احتياطية على الإطلاق. فكر في الاحتفاظ بنسخة في مكان آمن جدًا، مثل صندوق ودائع آمن.

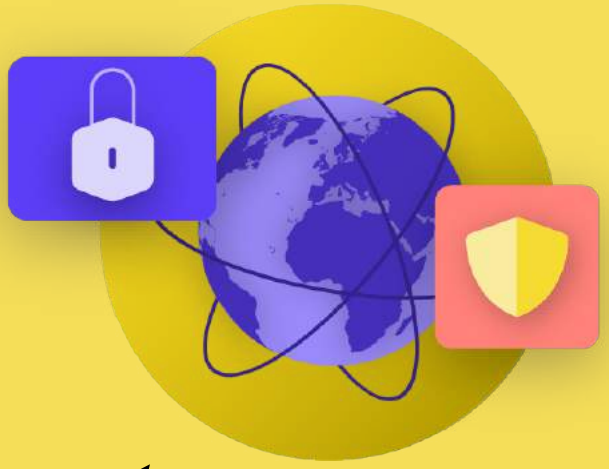
ملاحظة: إذا كنت تستخدم موفر سحابة في بلد به قوانين محددة لكيفية معالجة البيانات تحقق مع الخبراء القانونيين لفهم أفضل لكيفية امتثال حل التخزين عبر السحابة لأية متطلبات محلية. وعلى سبيل المثال، يقدم الآن العديد من موفري خدمة التخزين عبر السحابة، بما في ذلك Google وMicrosoft،خيارات تسمح لبعض العملاء باختيار الموقع الجغرافي لبياناتهم على السحابة.

تعزيز أمان حسابات السحابة الخاصة بالمنظمة

إذا اختارت منظمتك إعداد مجال في Google Workspace أو Microsoft 365، فاعلم أن كلتا الشركتين تقدمان مستويات أعلى من الأمان (مجانًا في بعض الحالات) لمنظمات المجتمع المدني. يوفر برنامج الحماية المتقدمة من Google وAccountGuard من Microsoft أمانًا أكثر قوة لجميع حسابات السحابة الخاصة بمنظمتك، كما تساعدك بشكل كبير في خفض احتمالية التعرض للتصيّد الاحتيالي الفعال واختراق الحسابات. إذا كنت تعتقد أن منظمتك مؤهلة وتهتم بتسجيل منظمتك في أي من الخطتين، فقم بزيارة مواقع الويب المذكورة أعلاه أو تواصل مع cyberhandbook@ndi.org للحصول على مساعدة إضافية.

تخزين البيانات بأمان

- **قم بتخزين البيانات الحساسة بشكل حصري في خدمة تخزين موثوقة عبر السحابة.**
  - تأكد من تمتع أية حسابات متصلة مستخدمة للوصول إلى هذه الخدمة بكلمات مرور قوية ومصادقة ثنائية العامل.
- **قم بتعيين سياسة للحد من إعدادات المشاركة داخل السحابة وافرضها.**
  - قم بتدريب جميع الموظفين على كيفية مشاركة المستندات بشكل صحيح (وعدم الإفراط في المشاركة).
- **إذا اختارت منظمة لتخزين البيانات محليًا، فاستثمر في موظفي تكنولوجيا معلومات مهرة.**
- **حافظ على أمان النسخ الاحتياطية للبيانات – قم بتشفير محركات الأقراص الصلبة الاحتياطية أو غيرها من أجهزة النسخ الاحتياطي.**



البقاء آمنًا على الإنترنت

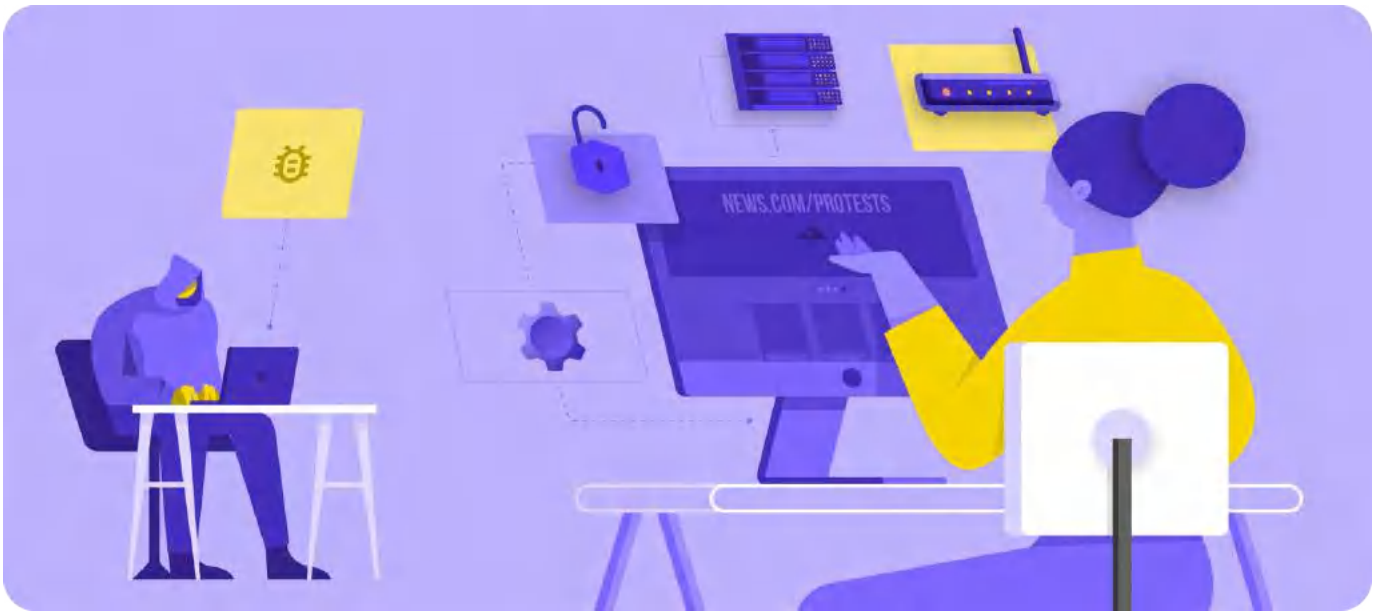
عندما تقوم بإستخدام الإنترنت على الهاتف أو الكمبيوتر، فيمكن لنشاطك أن يخبرنا بالكثير عنك وعن منظمتك.

من المهم الحفاظ على المعلومات الحساسة – مثل أسماء المستخدمين وكلمات المرور التي تكتبها في موقع ويب أو منشوراتك على مواقع التواصل الاجتماعي أو في سياقات معينة أسماء مواقع الويب التي تزورها – بعيدًا عن المتطفلين. كذلك، يُعد حظر وصولك إلى مواقع أو تطبيقات معينة أو تقييده أمرًا مقلقًا وشائعًا. وتسير هاتان المشكلتان – مراقبة الإنترنت والرقابة على الإنترنت – جنبًا إلى جنب وتعد إستراتيجيات تقليل التأثيرات متشابهة.

الاستعراض بأمان

إستخدام HTTPS

تُعد الخطوة الأكثر أهمية للحد من قدرة الخصم على مراقبة منظمتك عبر الإنترنت هي تقليل كمية المعلومات المتاحة المتعلقة بك وبنشاط زملائك على الإنترنت إلى الحد الأدنى. تأكد دائمًا من أنك تتصل بمواقع الويب بأمان: تأكد من أن عنوان URL (الموقع) يبدأ بـ "https" ويعرض رمز القفل الصغير في شريط العنوان الخاص بالمستعرض. عندما تستعرض الإنترنت **بدون تشفير**، يتم الكشف عن كافة المعلومات التي تكتبها في موقع ما (مثل كلمات المرور أو أرقام الحسابات أو الرسائل)، وتفاصيل الموقع والصفحات التي تقوم بزيارتها. وهذا يعني أن (1) أي متسللين على شبكتك و(2) مسؤول الشبكة الخاص بك و(3) موفر خدمة الإنترنت وأي كيان قد يشارك معه البيانات (مثل السلطات الحكومية) و(4) موفر خدمة الإنترنت للموقع الذي تقوم بزيارته وأي كيان قد يشارك معه البيانات وبالطبع (5) الموقع الذي تزوره نفسه لديه حق الوصول إلى قدر كبير من المعلومات التي قد تكون حساسة.

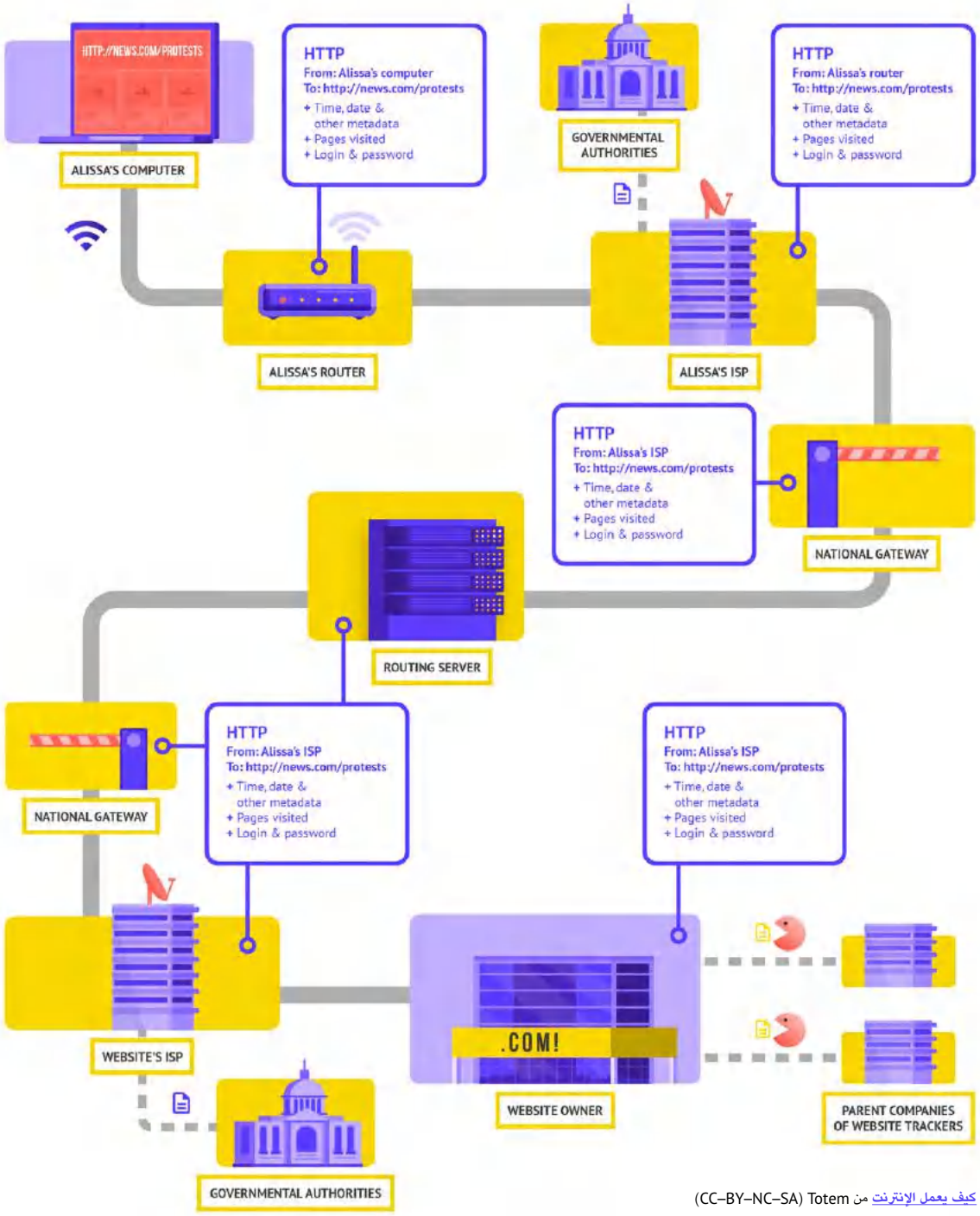


المراقبة والرقابة والمجتمع المدني

تستخدم الحكومات نفوذها وسلطتها على مزودي خدمة الإنترنت والبنية الأساسية المحلية الأخرى للإنترنت بشكل متزايد، لمنع الأفراد ومجموعات المجتمع المدني من الوصول إلى المعلومات عبر الإنترنت. في بعض الحالات، تهدف مثل هذه الاضطرابات عبر الإنترنت إلى تعطيل الأنظمة الأساسية للاتصالات ومشاركة المعلومات الرئيسية بما في ذلك وسائل التواصل الاجتماعي والمواقع الجديدة. على سبيل المثال، ردًا على الاحتجاجات الناتجة عن الانقلاب العسكري، عمل جيش منمار على إجبار مشغلي الهاتف المحمول على إيقاف تشغيل شبكة بيانات الهاتف المحمول بالكامل مؤقتًا في البلاد. جاء ذلك بعد فترة قصيرة من الحظر المستهدف لمواقع Facebook وTwitter وInstagram. بالإضافة إلى حظر الوصول إلى الإنترنت ومواقع الويب، تستخدم الحكومات والجهات المهددة الأخرى في جميع أنحاء العالم تكنولوجيا مراقبة يمكن الوصول إليها بشكل متزايد لمراقبة نشاط المواطنين عبر الإنترنت. على سبيل المثال، وفقًا لتقرير Freedom on the Net 2020 الصادر عن Freedom House، تشاركت الحكومة الأوغندية مع شركة التكنولوجيا الصينية Huawei لمراقبة شخصيات المعارضة والنشطاء المدنيين في الفترة التي سبقت وحتى ما بعد الانتخابات الرئاسية المثيرة للجدل في البلاد.

يُلقي التكرار المتزايد لمثل هذه الهجمات فيما يتعلق بالوصول إلى المعلومات عبر الإنترنت وحرية تلك المعلومات الضوء على مدى أهمية فهم مجموعات المجتمع المدني لمخاطر العمل عبر الإنترنت ووضع خطط لكيفية التواصل عند تعذّر الاتصال.

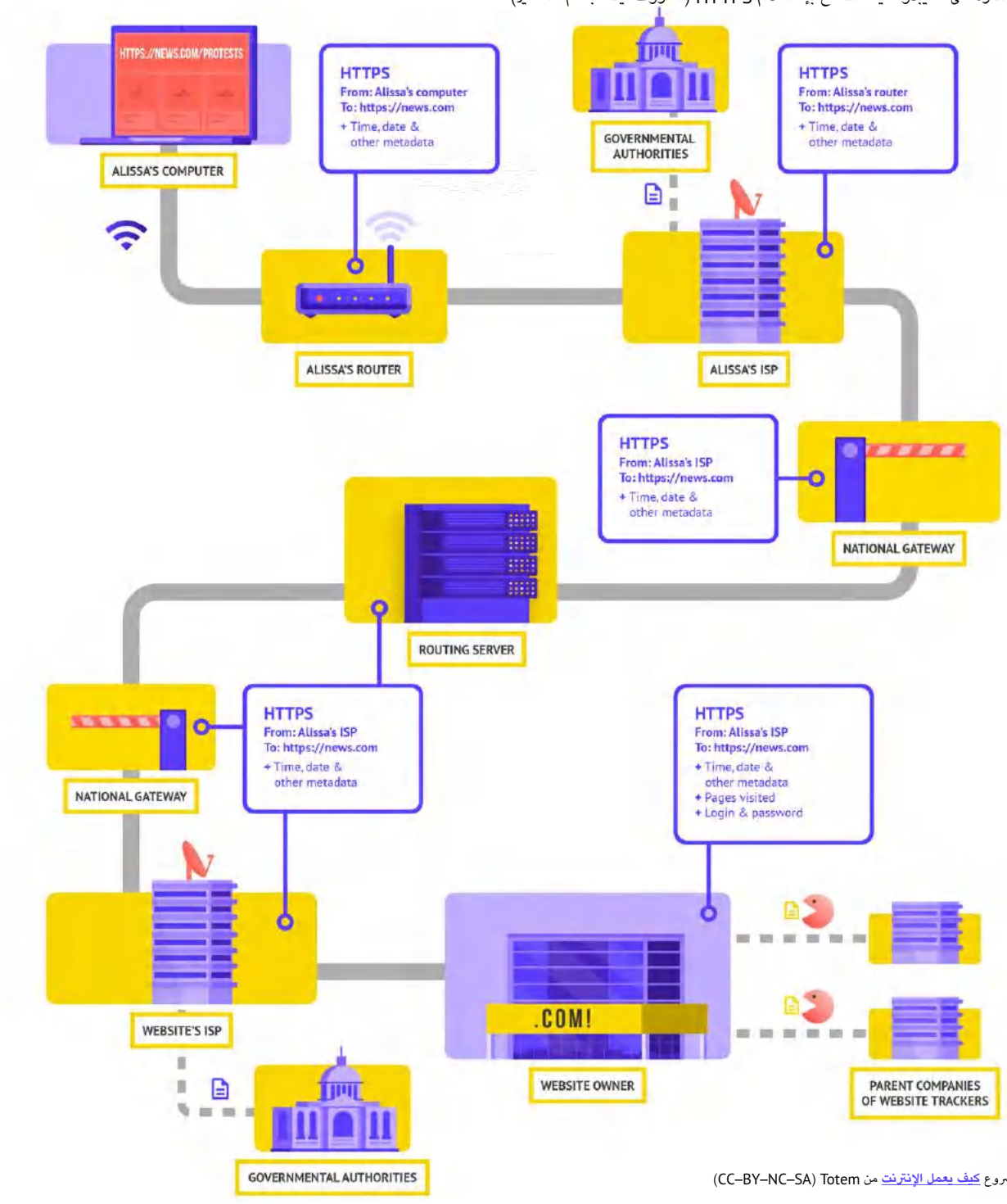
فلنأخذ مثالاً حقيقيًا لما يبدو عليه الاستعراض بدون تشفير:



مقتبس من مشروع كيف يعمل الإنترنت من Totem (CC–BY–NC–SA)

عند الاستعراض بدون تشفير، يتم الكشف عن جميع بياناتك. كما هو موضح أعلاه، يمكن للخصم رؤية مكانك وأنك تنتقل إلى الموقع news.com وتحديدًا تنظر إلى الصفحة الخاصة بالاحتجاجات في بلدك ويرى كلمة مرورك التي تشاركها لتسجيل الدخول إلى الموقع نفسه. عندما تقع هذه المعلومات في الأيدي الخطأ، فإنها لا تكشف حسابك فقط بل تعطي أيضًا للخصوم المحتملين فكرة جيدة عما قد تفعله أو تفكر به.

إن إستخدام HTTPS (يعني الحرف "s" الأمان) يعني أن التشفير في موضعه. وهذا يوفر لك المزيد من الحماية.
دعونا نلقي نظرة على ما يبدو عليه التصفح بإستخدام HTTPS (المعروف أيضًا باسم التشفير):



مقتبس من مشروع كيف يعمل الإنترنت من Totem (CC–BY–NC–SA)

بإستخدام HTTPS، لن يتمكن خصم محتمل من رؤية كلمة مرورك أو المعلومات الحساسة الأخرى التي قد تشاركها على موقع ويب. وعلى الرغم من ذلك، لا يزال بإمكانه رؤية المجالات التي تزورها (على سبيل المثال، news.com). وبينما يقوم HTTPS كذلك بتشفير المعلومات المتعلقة بالصفحات الفردية داخل موقع ما (على سبيل المثال، website.com/protests) تقوم بزيارته، لا يزال بإمكان الخصوم المتمرسين رؤية هذه المعلومات عن طريق فحص حركة الإنترنت الخاصة بك. ومع وجود HTTPS، قد يعرف خصم ما أنك ستنتقل إلى news.com، ولكنه غير قادر على رؤية كلمة مرورك وسيكون من الصعب (وليس مستحيل) عليه رؤية أنك تبحث عن معلومات حول الاحتجاجات (لإستخدام هذا المثال). ويُعد هذا فرقًا مهمًا. تحقق دائمًا من أن HTTPS في مكانه قبل التنقل عبر موقع الويب أو إدخال معلومات حساسة. كذلك، يمكنك إستخدام ملحق مستعرض HTTPS Everywhere للتأكد من أنك تستخدم HTTPS في جميع الأوقات، أو إذا كنت تستخدم Firefox، فقم بتشغيل وضع HTTPS فقط في المستعرض.

إذا كنت تلقيت تحذيرًا من مستعرضك بأن موقع ويب ما قد يكون غير آمن، فلا تتجاهله. فهذا يعني أن هناك شيء ما غير صحيح. قد يكون غير ضار – مثل أن الموقع به شهادة أمان منتهية الصلاحية – أو قد يكون الموقع مخادعًا أو مزيفًا. في كلتا الحالتين، من المهم الانتباه إلى التحذير وعدم المتابعة إلى الموقع. يُعد HTTPS ضروريًا ويوفر DNS المشفر بعض الحماية الإضافية ضد المتطفلين وحظر المواقع، ولكن إذا كانت منظمتك مهتمة بالمراقبة المستهدفة بشدة فيما يتعلق بالأنشطة عبر الإنترنت وتواجه رقابة متطورة عبر الإنترنت (مثل حجب مواقع الويب والتطبيقات)، فقد ترغب في إستخدام شبكة خاصة افتراضية موثوقة (VPN).

إستخدام DNS مشفر

إذا كنت تريد أن تجعل الأمر أكثر صعوبة (ولكن ليس مستحيلاً) على موفر خدمة الإنترنت بخصوص معرفة تفاصيل مواقع الويب التي تقوم بزيارتها، فإنه يمكنك إستخدام DNS مشفر.

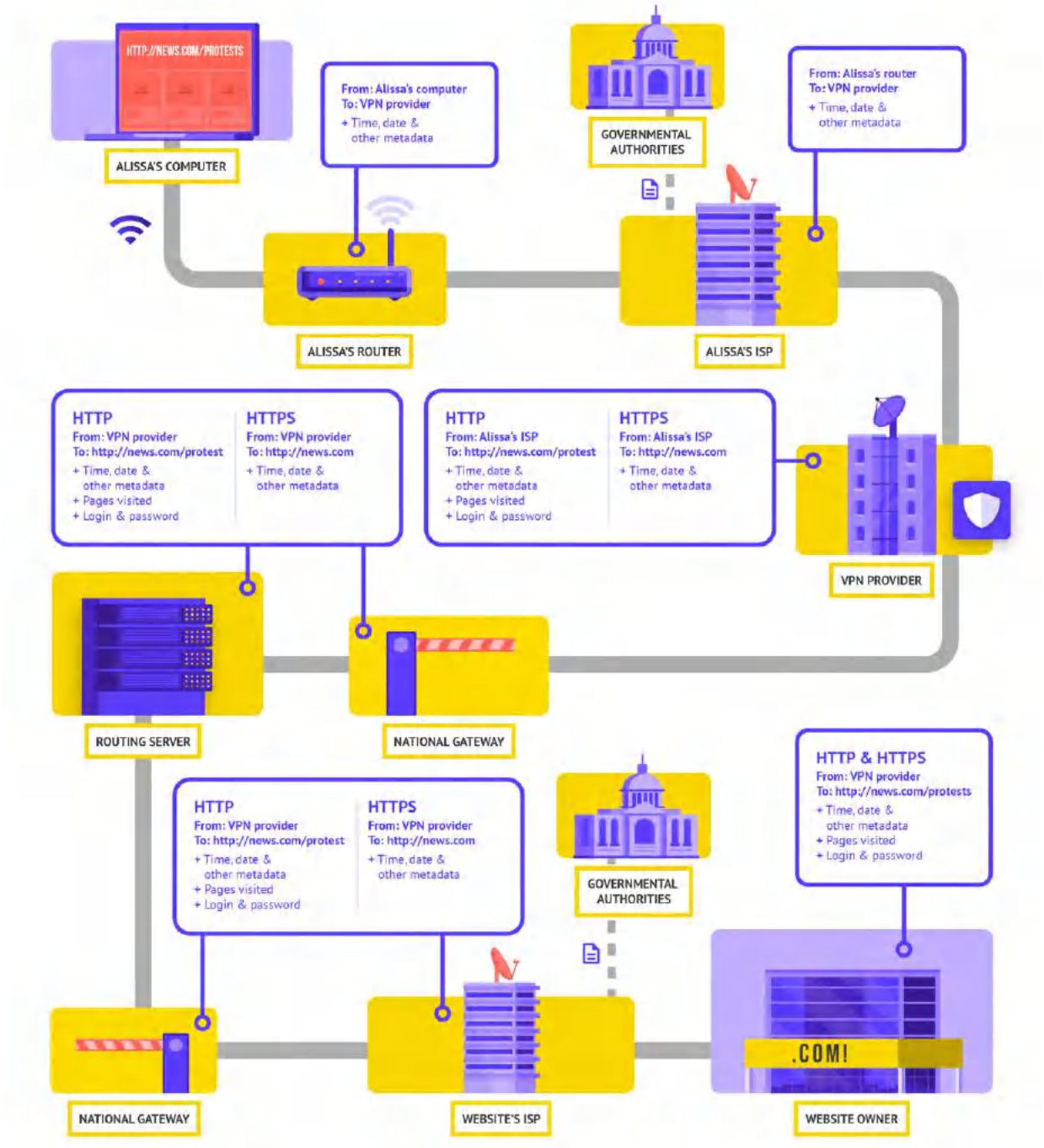
إذا كنت تتساءل، DNS تعني نظام أسماء المجالات. إنه في الأساس دليل الهاتف الخاص بالإنترنت، فإنه يترجم أسماء المجالات السهلة (مثل ndi.org) إلى عناوين برتوكول إنترنت مناسب للويب (IP). وهذا يسمح للأشخاص بإستخدام مستعرضات الويب للبحث بسهولة عن موارد الإنترنت وتحميلها وزيارة مواقع الويب. على الرغم من ذلك، لا يتم تشفير DNS بالوضع الافتراضي.

لإستخدام DNS المشفر وإضافة مستوى قليل من الحماية إلى حركة الإنترنت في الوقت نفسه، يُعد تنزيل التطبيق Cloudflare's 1.1.1.1 وتشغيله على الكمبيوتر والجهاز المحمول هو أحد الخيارات السهلة. تتوفر خيارات DNS مشفرة أخرى، بما في ذلك 8.8.8.8 الخاص بـ Google، ولكنها تتطلب المزيد من الخطوات التقنية لتكوينها. إذا كنت تستخدم المستعرض Firefox، فسيتم الآن تشغيل DNS المُشفر بالوضع الافتراضي. يمكن لمستخدمي مستعرض Chrome أو مستعرض Edge تشغيل DNS المشفر من خلال إعدادات الأمان المتقدمة للمستعرض عن طريق تشغيل "إستخدام DNS الآمن" وتحديد "مع: (1.1.1.1) Cloudflare" أو موفر من اختيارهم.

يعمل Cloudflare's 1.1.1.1 مع WARP على تشفير DNS وتشفير بيانات الاستعراض الخاصة بك – مما يوفر خدمة مشابهة لشبكة VPN التقليدية. على الرغم من أن WARP لا يحمي موقعك بالكامل من جميع مواقع الويب التي تقوم بزيارتها، إلا إنه يُعد ميزة سهلة الإستخدام يمكن أن تساعد الموظفين في منظمتك في الاستفادة من DNS مُشفر وتقديم حماية إضافية من مرفر خدمة الإنترنت الخاص بك في الحالات التي لا تكون فيها شبكة VPN كاملة لا تعمل أو لا تكون مطلوبة في ضوء سياق التهديد. في 1.1.1.1 مع إعدادات DNS المتقدمة في ميزة WARP، يمكن للموظفين كذلك تشغيل 1.1.1.1 for Families لتوفير حماية إضافية ضد البرامج الضارة أثناء الوصول إلى الإنترنت.

ما معنى VPN؟

تُعد شبكة VPN نفق يحمي بشكل أساسي من المراقبة وحظر حركة الإنترنت الخاصة بك من المتسللين على شبكتك ومسؤول الشبكة وموفر خدمة الإنترنت وأي شخص قد تشارك معه البيانات. لا يزال من الضروري إستخدام HTTPS ولضمان أنك تثق في الشبكة VPN التي تستخدمها منظمتك، إليك مثالاً عما يبدو عليه التصفح بإستخدام VPN:



مقتبس من مشروع كيف يعمل الإنترنت من Totem (CC–BY–NC–SA)

لوصف شبكات VPN بمزيد من التفصيل، يشير هذا القسم إلى دليل الدفاع الذاتي ضد المراقبة الخاص بـ EFF:

يتم تصميم شبكات VPN التقليدية لإخفاء عنوان IP الفعلي للشبكة وإنشاء نفق مشفر لحركة الإنترنت بين الكمبيوتر (أو الهاتف أو أي جهاز "ذكي") وخادم VPN. نظرًا لأنه يتم تشفير الحركة في النفق وإرسالها إلى VPN، فمن الصعب جدًا على الجهات الخارجية مثل موفري خدمة الإنترنت أو المتسللين على شبكة Wi-Fi العامة لمراقبة حركتك أو تعديلها أو حظرها. بعد المرور عبر النفق من عندك إلى VPN، فستترك حركة المرور الخاصة بك شبكة VPN إلى وجهتها النهائية، مما يعمل على إخفاء عنوان IP الأصلي. وهذا يساعد في إخفاء موقعك الفعلي لأي شخص يبحث في الحركة بعد أن تغادر VPN. ويوفر لك المزيد من الخصوصية والأمان، ولكن لا يجعلك إستخدام VPN مجهول الهوية بالكامل عبر الإنترنت: فلا تزال حركة المرور الخاصة بك مرئية لمشغل VPN. كذلك، سيعرف مزود خدمة الإنترنت أنك تستخدم VPN، الأمر الذي قد يرفع مستوى المخاطر لديك.

وهذا يعني أن **اختيار موفر VPN الجدير بالثقة أمرًا ضروريًا**. في بعض الأماكن مثل إيران، أنشأت الحكومات المعادية شبكات VPN لتكون قادرًا على تتبع ما يقوم به المواطنين. للعثور على VPN المناسب لمنظمتك وموظفيها، فإنه يمكنك تقييم شبكات VPN استنادًا إلى نموذج الشركة وسمعتها والبيانات التي تجمعها أو لا تجمعها وبالطبع أمان الأداة نفسها.

لماذا يجب عليك عدم إستخدام VPN مجانية فقط؟ إن الإجابة المختصرة هي أن معظم شبكات VPN المجانية، بما في ذلك تلك التي تأتي مثبتة مسبقًا على بعض الهواتف الذكية، تأتي بمشكلة كبيرة. مثل جميع الشركات وموفري الخدمات، يجب على شبكات VPN الحفاظ على نفسها بطريقة ما. وإذا لم تبيع VPN خدمتها، فكيف تحافظ على أعمالها؟ هل تطلب التبرعات؟ هل يتم تحصل رسوم مقابل الخدمات المميزة؟ هل هي مدعومة من قبل المنظمات الخيرية أو المولين؟ لسوء الحظ، فإن العديد من شبكات VPN المجانية تكسب أموالها عن طريق جمع بياناتك وبيعها.

ويُعد موفر شبكة VPN الذي لا يجمع بياناتك في المقام الأول هو الخيار الأفضل. إذا لم يتم جمع البيانات، فلا يمكن بيعها أو تسليمها إلى حكومة إذا طلبت ذلك. عند النظر إلى سياسة خصوصية موفر شبكة VPN، تحقق مما إذا كانت شبكة VPN تجمع بيانات المستخدم بالفعل أم لا. وإذا لم يُذكر صراحة أنه لم يتم تسجيل بيانات اتصال المستخدم، فمن المحتمل أنها تجمع البيانات. حتى إذا ادعت شركة عدم تسجيل بيانات الاتصال، فقد لا يكون هذا ضمانًا للسلوك الجيد.

ومن المفيد إجراء بحث على الشركة التي تقف خلف VPN. هل قام متخصصو أمن باعتمادها؟ وهل تمتلك شبكة VPN مقالات إخبارية مكتوبة حول هذا الموضوع؟ وهل سبق أن تم ضبطها بتهمة تضليل عملائها والكذب عليهم؟ إذا تم إنشاء شبكة VPN بواسطة أشخاص معروفين في مجتمع أمن المعلومات، فمن المرجح أن تكون شبكة VPN جديرة بالثقة. كن مرتابًا من تقديم شبكة VPN لخدمة لا يرغب أي شخص في المخاطرة بسمعته، أو خدمة تقدمها شركة لا يعرفها أحد.

شبكات VPN الزائفة في العالم الواقعي

في أواخر عام 2017، بعد تزايد الاحتجاجات في البلاد، بدأ الإيرانيون في اكتشاف نسخة "مجانية" (لكنها زائفة) من شبكة VPN مشهورة تتم مشاركتها عبر الرسائل النصية. وعدت شبكة VPN المجانية، التي لم تعد تعمل في الواقع، بمنح حق الوصول إلى Telegram، الذي كان محظورًا محليًا في ذلك الوقت. ولسوء الحظ، لم يكن التطبيق الزائف أكثر من مجرد برنامج ضار سمح للسلطات بتتبع الحركة ومراقبة الاتصالات الخاصة بأولئك الذين قاموا بتنزيله.

إذن، ما شبكة VPN التي يجب علينا إستخدامها؟

إذا كانت شبكة VPN مفيدة لمنظمتك، فهناك خياران جديران بالثقة هما TunnelBear وProtonVPN. هناك خيار آخر ألا وهو تكوين الخادم الخاص بك بإستخدام Outline الخاص بـ Jigsaw، حيث لا توجد شركة تدير حسابك ولكن في المقابل عليك إعداد الخادم الخاص بك. إذا كانت منظمتك أكبر قليلاً، فقد ترغب في التفكير في شبكة VPN للشركة توفر ميزات إدارة حساب مثل خطة Teams الخاصة بـ TunnelBear. وبالنسبة لبعض المنظمات المؤهلة في المجتمع المدني وحقوق الإنسان، توفر TunnelBear أرصدة للإستخدام المجاني لشبكة VPN (التي تكلف عادة 3 دولارات أمريكية شهريًا). إذا كنت تعتقد أن منظمتك مؤهلة ومهتمة، تواصل على cyberhandbook@ndi.org للحصول على المزيد من المعلومات.
على الرغم من أن معظم شبكات VPN الحديثة قد تم تحسينها فيما يتعلق بالأداء والسرعة، إلا أنه من الجدير بالذكر معرفة أن إستخدام شبكة VPN قد يؤدي إلى إبطاء سرعة الاستعراض الخاصة بك إذا كنت تستخدم شبكة ذات نطاق ترددي منخفض جدًا، أو يجعلك تعاني من وقت استجابة مرتفع أو تأخيرات في الشبكة أو انقطاعات متقطعة للإنترنت. إذا كنت تستخدم شبكة أسرع، فإنه يجب أن تستخدم VPN بالوضع الافتراضي طوال الوقت.

إذا قمت بتوصية الموظفين بإستخدام شبكة VPN، فمن المهم أيضًا التأكد من استمرار تشغيل شبكة VPN. قد يبدو الأمر واضحًا، لكن لا تقدم شبكة VPN التي يتم تثبيتها ولكنها ليست قيد التشغيل أي نوع من أنواع الحماية.

إخفاء الهوية من خلال Tor

بالإضافة إلى شبكات VPN، قد تكون قد سمعت عن Tor كأداة أخرى لإستخدام الإنترنت بشكل أكثر أمانًا. من المهم أن تفهم ماهية كل منهما وسبب إستخدامك لأحدهما أو الآخر وكيف يمكن أن يؤثر كلاهما على منظمتك.

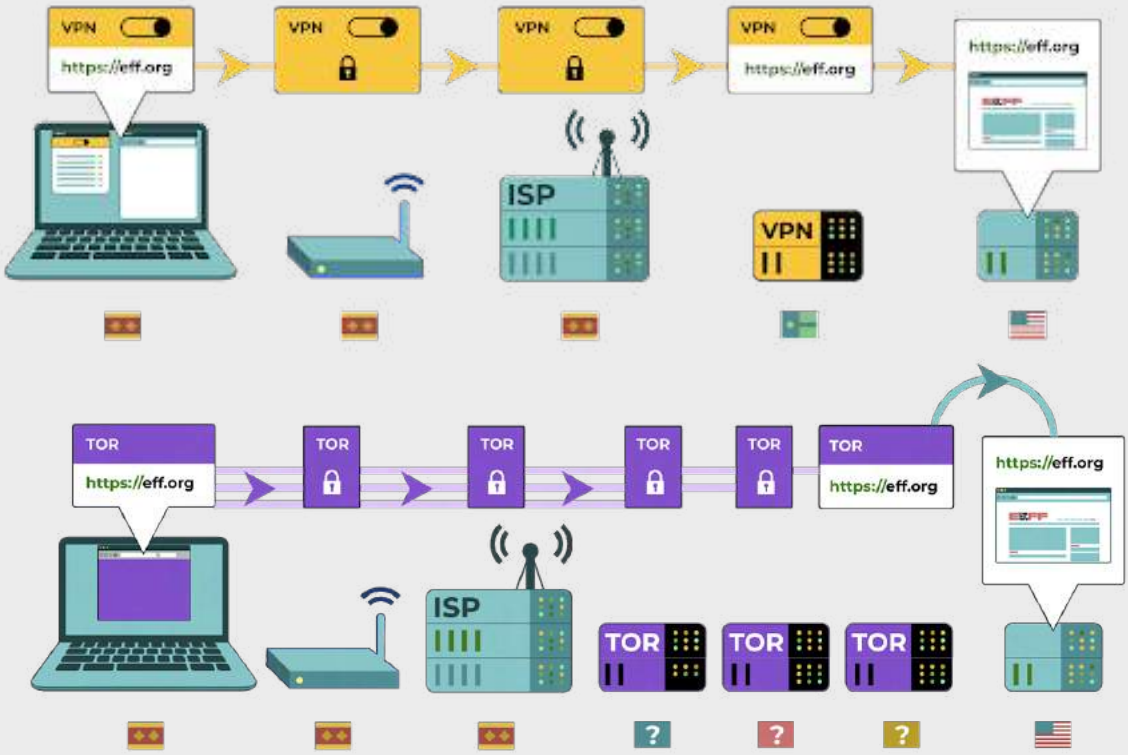
يُعد Tor برتوكول لنقل البيانات بشكل مجهول عبر الإنترنت عن طريق توجيه الرسائل أو البيانات عبر شبكة مركزية. يمكنك معرفة المزيد حول كيفية عمل Tor هنا، ولكن باختصار، إنه يقوم بتوجيه حركتك عبر نقاط متعددة على طول الطريق إلى وجهتها بحيث لا تحتوي نقطة واحدة على معلومات كافية لكشف هويتك وما تقوم به عبر الإنترنت في وقت واحد.

ويختلف Tor عن شبكة VPN في نقاط قليلة. وبشكل أساسي، إنه يختلف لأنه لا يعتمد على الثقة في أي نقطة محددة (مثل موفر شبكة VPN).

يوضح هذا الرسم، المطور بواسطة EFF، الفرق بين شبكة VPN تقليدية وTor.

إن أسهل طريقة لإستخدام Tor هي عبر مستعرض ويب Tor. وإنه يعمل مثل أي مستعرض عادي باستثناء أنه يوجه حركة المرور الخاصة بك عبر شبكة Tor. ويمكن تنزيل المستعرض Tor على أجهزة تعمل بنظام التشغيل Windows أو Mac أو Linux أو Android. ضع في اعتبارك أنه عند إستخدام المستعرض Tor، فإنك تحمي فقط المعلومات التي تصل إليها **أثناء وجودك في المستعرض**. إنه لا يوفر أية حماية للتطبيقات الأخرى أو الملفات التي تم تنزيلها والتي قد تفتحها بشكل منفصل على جهازك. كذلك، ضع في اعتبارك أن Tor لا يقوم بتشفير حركتك، لذلك – كما هو الحال عند إستخدام شبكة VPN – لا يزال من الضروري إستخدام أفضل الممارسات مثل HTTPS عند الاستعراض.

إذا كنت ترغب في زيادة درجات الحماية لإخفاء الهوية في Tor لتشمل الكمبيوتر بالكامل، فيمكن للمستخدمين الأكثر خبرة في التكنولوجيا تثبيت Tor بصفته اتصال إنترنت على مستوى النظام، أو فكر في إستخدام نظام التشغيل Tails، الذي يوجّه جميع الحركات عبر Tor بالوضع الافتراضي. كذلك، يستطيع مستخدمو Android إستخدام التطبيق Orbot لتشغيل Tor لجميع حركات وتطبيقات الإنترنت على الجهاز. بغض النظر عن كيفية إستخدام Tor، من المهم معرفة أنه عند إستخدامه، فإنه يتعذر على موفر خدمة الإنترنت الخاص بك رؤية مواقع الويب التي تقوم بزيارتها ولكنه *يستطيع* رؤية أنك تستخدم Tor نفسه. يتشابه الأمر إلى حد كبير عند إستخدام شبكة VPN، قد يؤدي ذلك إلى رفع



مستوى المخاطر لمنظمتك إلى حد كبير، لأن Tor ليس أداة شائعة الإستخدام بشكل كبير وبالتالي فإنها تبرز أمام الخصوم الذين قد يراقبون حركة الإنترنت الخاصة بك.

لذلك، هل يجب على منظمتك إستخدام Tor؟ الإجابة: حسب ما يقتضيه الأمر. بالنسبة لمعظم المنظمات المعرضة للخطر، تُعد شبكة VPN الموثوقة التي يستخدمها جميع الموظفين بشكل صحيح في جميع الأوقات هي الأداة الأسهل والأكثر ملائمة، وفي عصر الإستخدام المتزايد لشبكة VPN على مستوى العالم، تقل احتمالية وضع علامات استفهام حول نشاطك. وعلى الرغم من ذلك، إذا كنت لا تستطيع تحمل تكلفة شبكة VPN الجديرة بالثقة أو العمل في بيئة يتم فيها حظر شبكات VPN بشكل روتيني، فإن Tor يمكن أن تكون خيارًا جيدًا، إذا كان قانونيًا، للحد من تأثير المراقبة وتجنب الرقابة عبر الإنترنت.

هل هناك أية أسباب تمنعنا من إستخدام VPN أو Tor؟

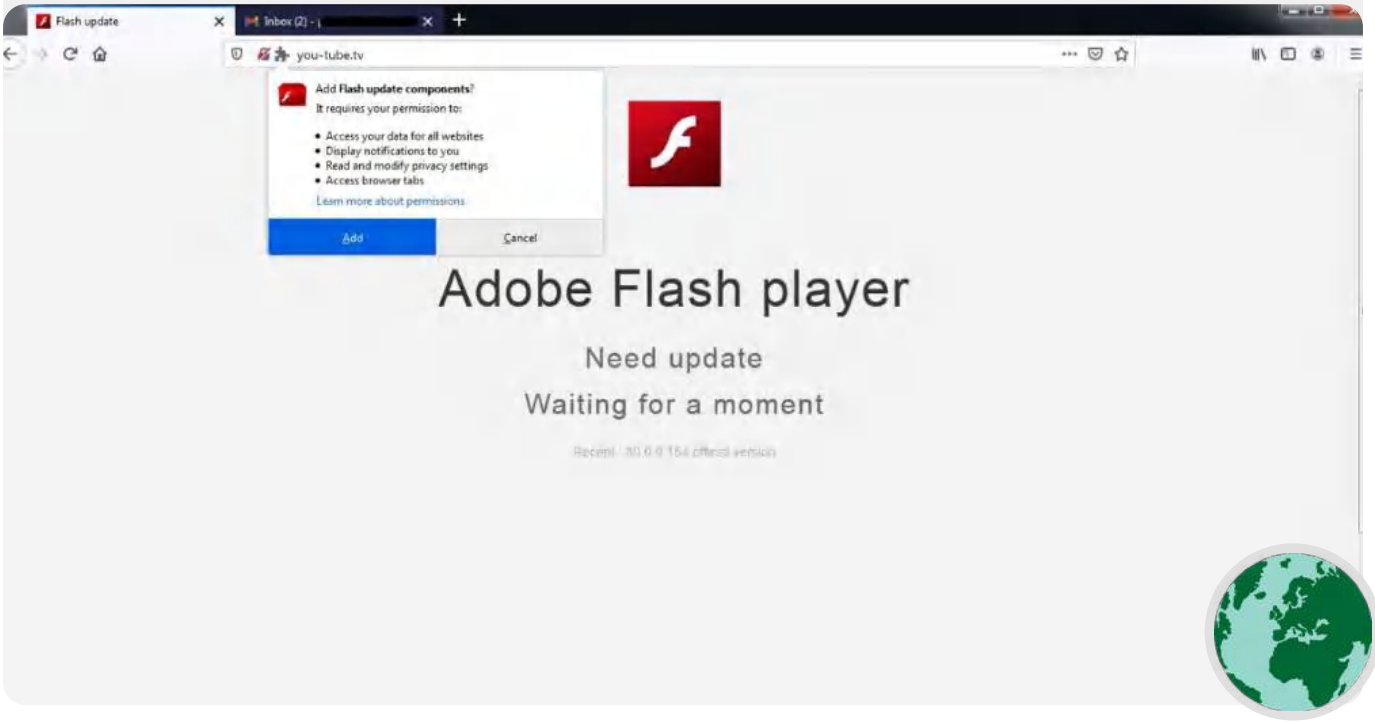
بصرف النظر عن المخاوف المتعلقة بخدمات VPN ذات السمعة غير الجيدة، فإن أهم شيء يجب مراعاته هو ما إذا كان إستخدام شبكة VPN أو Tor قد يجذب انتباه جهات غير مرغوب فيها أو، في بعض الدوائر القضائية، يكون مخالفًا للقانون. وعلى الرغم من عدم قدرة مزود خدمة الإنترنت على معرفة المواقع التي تزورها أثناء إستخدام هذه الخدمات، إلا أنه يكون على علم بأنك متصل بـ Tor أو VPN. إذا كان ذلك غير قانوني حيث تعمل منظمتك أو قد يجذب المزيد من الانتباه أو المخاطرة أكثر من التنقل ببساطة على الويب بإستخدام HTTPS القياسي أو DNS المشفر، فربما لا تكون شبكة VPN أو Tor على وجه الخصوص (وهو أقل إستخدامًا بكثير وبالتالي يمثل "علامة حمراء" أكبر) خيار مناسب لمنظمتك. وعلى الرغم من ذلك، نظرًا لأن إستخدام شبكة VPN يصبح أكثر شيوعًا، فإن هذا ليس عاملاً مميزًا. بالوضع الافتراضي، يكون الحصول على شبكة VPN طوال الوقت هو الاختيار الأمثل إذا كان قانونيًا وممكنًا.

ما المستعرض الذي يجب أن نستخدمه؟

استخدم متصفحًا ذا سمعة جيدة مثل مستعرض Chrome أو Firefox أو Brave أو Safari أو Edge أو Tor. يتم إستخدام كلاً من Chrome وFirefox على نطاق واسع جدًا وإنهما يقومان بعمل رائع فيما يتعلق بالأمان. يفضل بعض الأشخاص إستخدام Firefox بسبب تركيزه على الخصوصية. في كلتا الحالتين، من المهم إعادة تشغيله وجهاز الكمبيوتر بشكل متكرر نسبيًا للاستمرار في تحديث المستعرض. إذا كنت مهتمًا بمقارنة ميزات المستعرض، فتحقق من هذا المصدر من Freedom of the Press Foundation (مؤسسة حرية الصحافة). بغض النظر عن المستعرض، من الجيد أيضًا إستخدام ملحق أو وظيفة إضافية مثل Privacy Badger أو uBlock Origin أو Privacy Essentials من DuckDuckGo تمنع المعلنين والمتتبعين الخارجيين الآخرين من تتبع الأماكن التي تذهب إليها والمواقع التي تزورها. وعند استعراض الإنترنت، ضع في اعتبارك تحويل عمليات بحث الويب الافتراضية من Google إلى DuckDuckGo أو Startpage، أو محرك بحث آخر لحماية الخصوصية. سيساعد مثل هذا التبديل في الحد من المعلنين والمتتبعين الخارجيين أيضًا.

أمان المستعرض في العالم الواقعي

تم استهداف نشطاء المجتمع المدني من التبت في أوائل عام 2021، وذلك بإستخدام وظيفة إضافية لمتصفح ضار صمم بشكل ذكي لسرقة البريد الإلكتروني وبيانات الاستعراض. تم تقديم الوظيفة الإضافية، التي كانت باسم "مكونات تحديث الذاكرة المحمولة"، إلى المستخدمين الذين قاموا بزيارة المواقع الإلكترونية التي تم ربطها برسائل البريد الإلكتروني الخاصة بالتصيّد الاحتيالي. يمكن أن تكون هجمات ملحق المستعرض أو الوظيفة الإضافية ضارة تمامًا مثل البرامج الضارة التي تتم مشاركتها بشكل مباشر من خلال تنزيلات التصيّد الاحتيالي أو البرامج الأخرى.



أمان وسائل التواصل الاجتماعي

يمكن لمنظمتك الكشف عن الكثير – وأحيانًا أكثر مما تنوي الإفصاح عنه – عن طريق النشر والتعليق على وسائل التواصل الاجتماعي.

سواء كانت Facebook أو Twitter أو Instagram أو YouTube أو مواقع وسائل التواصل الاجتماعي الخاصة بالمنطقة مثل VKontakte أو Odnoklassniki، فإنه يجب عليك دائمًا التفكير بعناية فيما تقوم بنشره وقم بتهيئة أية إعدادات خصوصية قد تكون متوفرة بشكل صحيح. وهذا لا ينطبق على الصفحات الرسمية للمنظمة فقط، بل ينطبق أيضًا في بعض الحالات على الحسابات الشخصية للموظفين وحسابات عائلاتهم وأصدقائهم أيضًا.

أمان وسائل التواصل الاجتماعي والمجتمع المدني

حتى المنظمات منخفضة المخاطر يمكن استهدافها ومضايقتها على وسائل التواصل الاجتماعي في غياب سياسات أمنية مناسبة. في هذا المثال من عام 2018، خسر مأوى حيوانات غير ربحي الآلاف من الدولارات وابتعد داعميه عنه بعد أن أنشأ مسؤول حساب غير مصرح له بإطلاق حملة جمع تبرعات زائفة وظهر على النظام الأساسي حسابات مزيفة تنتحل شخصيات موظفين. إذا بذل المتسللون هذا الجهد لجني بضعة آلاف من الدولارات من مأوى للحيوانات، فإنه يمكنك أن تتخيل حجم الضرر الذي قد يتمكن الخصوم المتمرسين من إلحاقه إذا تمكنوا من الوصول إلى حسابات منظمتك أو انتحال هويتك عبر الإنترنت بنجاح.

بالإضافة إلى اختراق الحسابات، يواجه كذلك مجموعات المجتمع المدني والمستخدمين الفرديين في العديد من الدول تبعات للمحتوى المنشور على وسائل التواصل الاجتماعي. في أحد الأمثلة في زامبيا منذ عام 2020، قامت الشرطة بإلقاء القبض على طالب يبلغ من العمر 15 عامًا بتهمة التشهير بالرئيس في منشور على Facebook. وتم التعرف على الطفل، الذي نشر المنشور باسم مستعار، من خلال رقم الهاتف المستخدم لتسجيل الحساب ومن عنوان بروتوكول الإنترنت (IP) الخاص به.

وضع سياسة تنظيمية لوسائل التواصل الاجتماعي

افترض أن أي شيء يتم نشره على وسائل التواصل الاجتماعي يمكن أن يصبح معرفة عامّة فقم بصياغة سياسة تنظيمية لوسائل التواصل الاجتماعي وفقًا لذلك. يجب أن تُجيب هذه السياسة عن أسئلة مثل: من لديه حق الوصول إلى حسابات وسائل التواصل الاجتماعي؟ من الذي يتم السماح له بالنشر ومن يحتاج إلى الموافقة على منشوراته؟ ما المعلومات التي يجب/يجب عدم مشاركتها على وسائل التواصل الاجتماعي؟ إذا نشرت صورًا أو معلومات الموقع أو أية معلومات تعريفية أخرى عن موظفيك أو شركائك أو الحاضرين في الحدث، فهل طلبت إذنهم وهل وضعوا المخاطر في الاعتبار؟ بالإضافة إلى وضع سياسة وتوضيحها للموظفين، تأكد من أنه يتم تكوين إعدادات الخصوصية والأمان (غالبًا ما يُشار إليها باسم "السلامة") بشكل صحيح. تتضمن بعض الأسئلة الرئيسية التي يجب أن تطرحها على نفسك أثناء تحديد إعدادات الخصوصية والسلامة الأكثر منطقية لحساباتك الشخصية والتنظيمية ما يلي:

- هل ترغب في مشاركة منشوراتك مع العامة أو مع مجموعة معينة من الأشخاص داخليًا أو خارجيًا؟
- هل يجب أن يتمكن أي شخص من التعليق أو الرد أو التفاعل مع رسائلك أو منشوراتك؟
- هل يجب أن يتمكن الأشخاص من العثور عليك وعلى منظمتك بإستخدام عنوان البريد الإلكتروني أو رقم الهاتف (الشخصي أو المتعلق بالعمل)؟
- هل ترغب في مشاركة موقعك تلقائيًا عندما تقوم بالنشر؟
- هل ترغب في حظر حسابات معادية أو كتم صوتها؟
- هل ترغب في حظر كلمات معينة أو علامات كلمات رئيسية؟

سيكون لكل موقع من مواقع التواصل الاجتماعي إعدادات خصوصية وسلامة مختلفة، ولكن هذه المفاهيم تنطبق عالميًا. عندما تفكر في هذه الأسئلة، استفد من أدلة الخصوصية المفيدة من الأنظمة الأساسية الرئيسية: Facebook وTwitter وInstagram و YouTube. بالنسبة إلى Facebook بشكل خاص، كن حذرًا بشأن خيارات الخصوصية الخاصة بك فيما يتعلق بالمجموعات. تُعد مجموعات Facebook مكانًا شائعًا للمشاركة والتأييد ومشاركة المعلومات، ولكن يمكن لأي شخص الانضمام إلى المجموعات غير المقيدة. ليس من غير المألوف أن تظهر الحسابات "المزيفة" كأشخاص حقيقيين في محاولة للتسلل إلى مجموعات أو صفحات خاصة على وسائل التواصل الاجتماعي. وبالتالي، أقبل طلبات "الأصدقاء" و"المتابعة" بعناية. تذكر أن حسابات وسائل التواصل الاجتماعي في المنظمة تكون آمنة بمقدار مستوى الأمان في الحسابات التي "ترتبط" بها. تذكر هذا الأمر المهم بالنسبة لموقع التواصل Facebook، حيث يمكن إدارة صفحة منظمتك بواسطة حساب شخصي مرتبط بشخص ما.

المضايقات عبر الإنترنت

لسوء الحظ، تواجه العديد من المنظمات مضايقات كبيرة عبر الإنترنت، وخاصة على وسائل التواصل الاجتماعي. وغالبًا **ما يتم توجيه تلك المضايقات بشكل أكبر ضد النساء والسكان المهمشين**. يمكن للعنف عبر الإنترنت ضد النساء بشكل خاص أن يخلق بيئة معادية تؤدي إلى الرقابة الذاتية أو الانسحاب من الخطاب السياسي أو المدني. وكما تم تحديده في تقرير Tweets that Chill الخاص بفريق الجندر والنساء والديموقراطية في المعهد الوطني الديموقراطي، عندما يتم توجيه الهجمات عبر الإنترنت ضد النساء الناشطات سياسيًا، فيمكن أن يؤدي الوصول الواسع لوسائل التواصل الاجتماعي إلى تضخيم تأثير المضايقات والإساءات النفسية، مما يعمل على القضاء على إحساس النساء بالأمان الشخصي بطرق لا يختبرها الرجال.

وأثناء قيام منظمتك بوضع سياسة وسائل التواصل الاجتماعي، فمن المهم أن تكون على علم بهذه الديناميكيات. اجعل خطة الأمان الخاصة بك تشتمل على دعم منظم للموظفين الذين يواجهون رسائل سلبية وإهانات وتهديدات على وسائل التواصل الاجتماعي، سواء كان ذلك في حياتهم الوظيفية أو في حياتهم الشخصية. ضع بنية أساسية لمكافحة المضايقات داخل منظمتك، بما في ذلك إجراء استطلاع رأي لموظفيك لفهم الكيفية التي تؤثر بها المضايقات عبر الإنترنت عليهم وقم بإنشاء فريق استجابة سريعة لمساعدة الموظفين في مواجهة المواقف الصعبة. كذلك، يقدم دليل ميداني للحماية من المضايقات عبر الإنترنت التابع لمنظمة PEN America توصيات مفصلة حول كيفية دعم الموظفين الذين يواجهون هذه المضايقات. قد تضع، إذا كان موظفيك لا يمانعون القيام بذلك، في اعتبارك الإبلاغ عن حوادث المضايقات و/أو الحسابات المسببة للمشاكل مباشرة إلى الأنظمة الأساسية أيضًا.

عند التعامل مع الموظفين الذين كانوا ضحايا للمضايقات عبر الإنترنت (وفي العالم الحقيقي أيضًا)، فمن المهم أن تكون حساسًا. وكما تم توضيحه في حملة Take Back the Tech الخاصة ببرنامج حقوق المرأة التابع لجمعية Association for Progressive Communications، افهم أن الناجية قد تتعامل مع الصدمة وعليك أن تدرك أن العنف (سواء كان عبر الإنترنت أو دون اتصال بالإنترنت) ليس خطأ الناجية أبدًا. تأكد من إمكانية إثارة الحديث حول هذه المشكلات ومناقشتها (إذا كان فريقك يرغب في القيام بذلك) في بيئة سرية وآمنة، مع وجود خيار إخفاء الهوية. احرص على أن تضم خطة أمان منظمتك قائمة بالمهنيين والمنظمات ووكالات إنفاذ القانون التي يمكنك توصيل الموظفين بها للحصول على مساعدة قانونية أو طبية أو مساعدة خاصة بالصحة العقلية أو مساعدة فنية، إذا لزم الأمر. للحصول على أفكار إضافية، تحقق من دليل السلامة عبر الإنترنت الخاص بمنظمة Feminist Frequency.

المحافظة على استمرار وجود مواقع الويب عبر الإنترنت

بالإضافة إلى حماية قدرتك على الوصول إلى الإنترنت بأمان، من المهم أيضًا القيام بما تستطيع فعله لضمان وصول الآخرين إلى مواقع الويب الخاصة بمنظمتك.

بالنسبة لصفحات وسائل التواصل الاجتماعي، فهذا يعني حماية هذه الحسابات بإستخدام كلمات مرور فريدة والمصادقة ثنائية العامل. بالنسبة إلى موقع الويب الخاص بك، فهذا يعني حمايته من هجمات القرصنة ومنع الخدمة. وتُعد هجمات منع الخدمة الموزعة (DDoS) هجمات يتم بها إستخدام مجموعة كبيرة من أجهزة الكمبيوتر لسحب خادمك إلى حركة ضارة. إذا كنت منظمة مجتمع مدني أو منظمة غير ربحية أخرى، فإنه من المحتمل أن تكون مؤهلاً للحصول على حماية DDoS مجانية – مما يجعل إيقاف موقع الويب الخاص بك أمرًا أكثر صعوبة على خصمك. تتضمن بعض الخيارات مشروع Galileo من Cloudflare أو مشروع Project من Google أو خدمة Deflect من eQualitie.

استضافة موقع الويب الخاص بمنظمتك بأمان

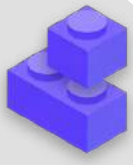
تتم استضافة مواقع الويب على أجهزة الكمبيوتر – وإنها عُرضة للقرصنة تمامًا كما يحدث مع أجهزتك الخاصة. إذا كان ممكنًا، يجب أن تستفيد منظمتك من خدمات الاستضافة الحالية مثل Wordpress.com أو Wix أو غيرها من الخدمات التي تدير أمان الموقع بالكامل بالنيابة عنك. إذا كنت تقرأ هذا الدليل، فمن المحتمل كذلك أن تكون منظمتك مؤهلة للحصول على استضافة آمنة مجانية لموقع Wordpress بواسطة eQualitie من خلال خدمة الاستضافة eQPress Hosting. ويُعد هذا خيارًا رائعًا للمنظمات المدنية التي لديها مواقع Wordpress حالية أو إذا كانت منظمتك تتطلع إلى إنشاء موقع جديد. إذا كانت احتياجات موقع الويب الخاص بك أكثر تعقيدًا، أو إذا كنت تحتاج إلى استضافة موقع الويب الخاص بك بنفسك، فتأكد من التركيز على استمرار تحديث نظام التشغيل وبرامج استضافة الويب، تمامًا مثلما تفعل مع الكمبيوتر الشخصي الخاص بك. فكر في إستخدام موفري خدمات الاستضافة عبر السحابة مثل(Amazon Web Services (AWS أو Microsoft Azure أو eclips.is من Greenhost، الذي يوفر خيارات أمان محسنة لمواقع الويب المستضافة. بغض النظر عن الأدوات التي تستخدمها لاستضافة موقع الويب الخاص بك، تأكد من حماية أية حسابات مستخدمة للوصول إلى إعدادات تحرير المحتوى والتكوين بكلمات مرور قوية والمصادقة ثنائية العامل.

إذا كانت منظمتك تتمتع بالذكاء التقني لاستضافة موقع الويب الخاص بها، فإنه يجب عليك التفكير في اختيار ما يُطلق عليه "موقع ثابت". على عكس مواقع الويب الديناميكية، تقلل أنواع المواقع هذه مستوى هجوم المتسللين وستجعل موقع الويب الخاص بك أكثر مقاومة للهجوم.

حماية شبكة WiFi الخاصة بك

تُعد كل هذه الخطوات مهمة لحماية حركة الويب من المراقبة والرقابة، ولكنها ليست بديلاً عن أمان الشبكة الأساسي في المكتب والمنزل.

لا تنس الأساسيات مثل إستخدام كلمة مرور قوية (وليست كلمة المرور الافتراضية) على جهاز (أجهزة) توجيه WiFi، مما يضمن حق الوصول إلى شبكتك فقط للمستخدمين المصرح لهم عن طريق تغيير كلمة المرور بشكل متكرر وتمكين جدار الحماية المضمن في أجهزة التوجيه اللاسلكية. فكر في إنشاء شبكة ضيف في مكتبك أيضًا إذا كان لديك زائرين يستخدمون الإنترنت يدخلون من المبنى ويخرجون منه.



البقاء آمنًا على الإنترنت

- قم بإجراء تدريب منتظم للموظفين لمعرفة مدى أهمية اتباع تدابير أمان الويب الأساسية.
- ذكّر الموظفين بالاستعراض بإستخدام **HTTPS** و**DNS** المشفر.
- طالب الموظفين بإعادة تشغيل المستعرضات بانتظام لتثبيت التحديثات.
- شجّع على إستخدام الخصوصية لحماية المستعرضات والملحقات.
- إذا كانت شبكة **VPN** مناسبة لسياق منظمتك، فاختر واحدة ذات سمعة جيدة، وقم بتدريب الموظفين على إستخدامها وتأكد من إستخدامها باستمرار.
- ضع سياسة تنظيمية واضحة تتعلق بإستخدام وسائل التواصل الاجتماعي وقم بتوزيعها.
- قم بتمكين إعدادات الخصوصية والأمان على جميع حسابات وسائل التواصل الاجتماعي.
- افهم تأثيرات المضايقات عبر الإنترنت وكن مستعدًا لدعم الموظفين المتضررين.
- ضع قائمة بالمهنيين والمنظمات ووكالات إنفاذ القانون التي يمكنك توصيل الموظفين بها للحصول على مساعدة قانونية ومساعدة خاصة بالصحة العقلية مساعدة تقنية ردًا على المضايقات عبر الإنترنت، إذا لزم الأمر.
- قم بالتسجيل في حماية **DDOS** لمواقع الويب الخاصة بك.
- استخدم موفر استضافة ويب موثوق ويمكن الاعتماد عليه.
- استخدم كلمة مرور قوية وشبكة ضيف لشبكة **WiFi** في مكتبك.

حماية الأمن الفعلي

من المهم الحفاظ على أمان أجهزتك فعليًا. ضع في اعتبارك أن الأمان الفعلي يتجاوز مجرد أمان الأجهزة، ويجب أن يضمن إستراتيجيات لحماية كل شيء آخر في عالمك. وهذا يتضمن المستندات المطبوعة؛ ومكتب المنظمة أو مساحات العمل الخاصة بها؛ وبالطبع أنت وموظفيك ومتطوعيك.

المراقبة والرقابة والمجتمع المدني

لسوء الحظ، إن الهجمات الفعلية على منظمات المجتمع شائعة، وغالبًا ما تترك تأثيرات كبيرة على الأمان الفعلي وأمن المعلومات. تتضمن إحدى الطرق الشائعة التي يتخذها الخصوم لقمع نشاط منظمات المجتمع المدني (CSO) الهجوم على المكاتب وإغلاقها - لترهيب الموظفين وفي بعض الحالات لسرقة المعلومات والمعدات التقنية ومصادرتها. وغالبًا ما تستهدف مثل هذه التهديدات الأقليات ومجموعات حقوق الإنسان ومنظمات المجتمع المدني التي تعمل في المجال الديموقراطي والحوكمةُ. على سبيل المثال، تم تهديد مكاتب حركة حقوق المثليين في غانا، وهي منظمة مدنية افتتحت في أوائل عام 2021 أول مركز مجتمعي في البلد للمجتمع المحلي للمثليين، بالحرق، وقامت الشرطة بمداهمتها وإغلاقها في النهاية. مثل هذه المداهمات لا تؤثر فقط على العمليات الفعلية للمنظمة، ولكن يمكن أن تقضي على شعور الموظفين بالأمان.

حماية الأصول الفعلية

يُعد الأمان الفعلي لأجهزتك هو أحد المكونات الأساسية لأمن المعلومات.

وبالإضافة إلى التخفيف من تأثير الجهاز المسروق بإستخدام شاشات حماية وكلمات مرور وتنفيذ تشفير القرص بالكامل وتشغيل ميزات المسح عن بُعد، فإنه يجب عليك كذلك وضع كيفية حماية تلك الأجهزة من السرقة في الاعتبار في المقام الأول. ولجعل عملية السرقة أكثر صعوبة، تأكد من تركيب أقفال قوية (وقم بتغييرها عند تغيير الموظفين) في المكتب و/أو المنزل. وبالإضافة إلى ذلك، فكر في شراء خزنة كمبيوتر محمول أو خزانة قابلة للقفل للحفاظ على حماية الأجهزة طوال الليل. أصبحت الكاميرات الأمنية أقل تكلفة بكثير، مع توفر إصدارات بسيطة مصممة للإستخدام المنزلي على نطاق أوسع. يمكن للكاميرا أو لأنظمة استشعار الحركة حول أماكن العمل الكشف عن عمليات الاقتحام والسرقة الفعلية ومنعها. ابحث عن خيار احترام الخصوصية متاح في بلدك، وتأكد من اختيار الكاميرات التي توفرها شركات موثوقة ليس لديها حافز لتسليم البيانات والمعلومات إلى خصم محتمل.

إذا كان مستوى مخاطر الاقتحام أو مداهمة المكتب عاليًا، فاحتفظ بالبيانات الأكثر حساسية الخاصة بالمنظمة بعيدًا عن المكتب - إما عن طريق تخزينها بأمان عبر السحابة (كما تمت مناقشته سابقًا) أو عن طريق نقلها فعليًا إلى موقع أقل استهدافًا. إذا كانت الأجهزة القديمة لا تزال تحتوي على معلومات مخزنة عليها ولكنها لم تعد قيد الإستخدام، ففكر في مسحها - يُعد هذا الدليل من Wirecutter موردًا رائعًا حول كيفية القيام بهذا لمعظم الأجهزة الحديثة. إذا كان مسح أجهزتك غير ممكن، فإنه يمكنك تدميرها فعليًا أيضًا. وإن أسهل طريقة للقيام بذلك، إذا لم تكن الأكثر حساسية تجاه البيئة، هي تفكيك الأجهزة ومحركات الأقراص الصلبة بإستخدام مطرقة. فأحيانًا تكون الحلول الأقدم هي الأفضل! حتى قبل اتخاذ هذه الخطوات التقنية، استغرق لحظة للقيام بجرد جميع الأجهزة في المنظمة. إذا لم يكن لديك قائمة بجميع الأجهزة، فمن الصعب تتبع ما قد يكون مفقودًا في حالة السرقة.

إعداد نظام الأمن في مكتبك الخاص

إذا كان نظام الأمان الكامل للمكتب يتعدى ميزانية المنظمة وكنت قلقًا بشكل خاص بشأن الخصوصية، فإنه يمكنك تجربة خيار إبداعي مثل تطبيق Haven من مشروع Guardian لإعلامك بالتطفل المحتمل على مكتبك. يُعد Haven تطبيق للهواتف الذكية يمكنه تحويل أي هاتف يعمل بنظام التشغيل Android إلى كاشف للحركة والاهتزاز والضوء. يمكنك إعداد التطبيق على عدد قليل من أجهزة Android رخيصة في نقاط مختلفة في المكتب لإعلامك وتسجيل أي ضيوف غير متوقعين ومتسللين غير مرغوب فيهم. كذلك، يمكن أن يكون تطبيق Haven مفيدًا في إعداد غرفة في فندق أو شقة إذا كنت في خطر متزايد. يُعد نظام الأمان الكامل هو الأفضل، ولكن إذا كان ذلك صعب تحقيقه وترغب في معرفة المزيد حول كيفية إستخدام التطبيق Haven، فإنه يمكنك زيارة موقع الويب الخاص بالمشروع.

ماذا نفعل بكل تلك الأوراق؟

من المحتمل أن يكون لدى منظمتك الكثير من المعلومات التي تتم طباعتها على الورق أو مكتوبة في دفاتر الملاحظات أو مكتوبة على أوراق الملاحظات اللاصقة. قد يكون بعضًا من هذه الأوراق حساسًا جدًا: مطبوعات خاصة بالميزانيات وقوائم المشاركين والخطابات الحساسة من المتبرعين وملاحظات من اجتماعات خاصة. من الضروري التفكير في أمان هذه المعلومات أيضًا. إذا كنت بحاجة ماسة إلى الاحتفاظ بنسخ ورقية من المعلومات الحساسة، فتأكد من تخزينها بأمان في خزانة مقفلة أو مكان آمن آخر. لا تحتفظ بأية معلومات خاصة أو حساسة (بما في ذلك كلمات المرور) على مكتب أو على لوح أبيض. إذا كنت تعتقد أن منظمتك معرضة لخطر اقتحام أو مداهمة كبير، فاحتفظ بالمعلومات الحساسة للغاية في موقع أقل استهدافًا.

حاول قدر الإمكان التخلص من المعلومات الورقية غير الضرورية. تذكر: لا يمكن سرقة ما ليس بحوزتك. ضع سياسة تنظيمية تتعلق بملكية الملاحظات الورقية، وتأكد من جمع أية ملاحظات ورقية من الموظفين إذا قرروا المغادرة أو ترك المنظمة، (تمامًا مثلما تجمع كمبيوتر أو هاتف صادر عن المنظمة). للتخلص من الأوراق الحساسة، قم بشراء آلة تمزيق ذات جودة. يمكن أن يكون نشاط نهاية الأسبوع الممتع هو أخذ استراحة مدتها 15 دقيقة مع موظفيك لتمزيق أية بقايا أو مطبوعات أو ملاحظات حساسة من الأسبوع السابق.

سياسة المكتب

على الرغم من أنه قد تم تغيير العديد من حقائق "المكتب" بشكل كبير منذ بداية جائحة كوفيد-19، إلا أنه لا يزال من المهم لمنظمتك وضع سياسة واضحة تتعلق بالوصول إلى المكتب. يجب أن تتناول هذه السياسة الأسئلة الرئيسية بما في ذلك من الذي يُسمح له بدخول المكتب (ومتى) ومن يستطيع الوصول إلى موارد المكتب (مثل شبكة WiFi) وما الذي يجب فعله فيما يتعلق بالضيوف.

إنه سؤال بسيط ولكنه مهم ويجب الرد عليه، من الذي يحصل على مفاتيح المكتب. يجب أن يمتلك الموظفون الموثوق بهم فقط المفاتيح، ويجب تغيير الأقفال عند مغادرة الموظفين و/أو على أساس شبه منتظم. خلال اليوم، يجب أن تكون أية أبواب مفتوحة في مرمى بصر شخص ما موثوق داخل المنظمة باستمرار. كذلك، ضع في اعتبارك ما إذا كان للمنظمة علاقة موثوقة مع المالك أو مسؤولي النظافة. فكر في المعلومات أو الأجهزة التي قد يتمكن هؤلاء الأشخاص من الوصول إليها وتأكد من أنها محمية، وبخاصة إذا لم تكن تلك العلاقة موثوقة. أيًا كان من له حق الدخول، يجب دائمًا تعيين شخص ما موثوق لإغلاق المكتب والتأكد من أنه يتم تأمين الأجهزة بشكل صحيح قبل المغادرة في نهاية اليوم.

هل مسموح بتواجد الضيوف داخل المكتب؟ إذا كان الأمر كذلك، فتأكد من أنهم لا يستطيعون الوصول (أو على الأقل وصول غير مراقب) إلى الأجهزة أو البيانات المطبوعة الحساسة. إذا كان من المتوقع أو من المتطلبات أن يصل الضيوف إلى الإنترنت عند الزيارة، فإنه يجب عليك إعداد شبكة "ضيف" حتى يكون الضيوف غير قادرين على مراقبة حركتك العادية. بشكل عام، يجب أن يتمكن الموظفون الموثوق بهم من الوصول إلى الشبكة وأجهزة الشبكة مثل الطابعات. عادةً يكون من الجيد أيضًا طلب تسجيل الضيف حتى يكون لديك سجل عمن قاموا بالزيارة.

أثناء قيامك بوضع سياسة للمكتب، يجب أن يكون الهدف هو السماح للأشخاص الموثوق بهم الوصول إلى الأجهزة الحساسة والمستندات والأماكن والأنظمة.

دعم الموظفين والمتطوعين

يمكن أن تؤثر تهديدات الأمان الفعلي لمنظمتك على الموظفين أيضًا. وعلى نحو مشابه للمضايقات على وسائل التواصل الاجتماعي، غالبًا ما تؤثر هذه التهديدات الأمنية الفعلية بشكل غير متناسب على النساء والمجتمعات المهمشة. إن الأمر لا يتعلق فقط بالنوافذ المكسورة وأجهزة الكمبيوتر المحمولة المسروقة. يمكن أن يؤثر الترهيب أو التهديدات أو حالات العنف الجسدي أو الجنسي والعنف المنزلي والخوف من الهجوم تأثيرًا سلبيًا خطيرًا على حياة الموظفين. بالنسبة للمنظمات التي تعمل مع أو تدعم النساء الناشطات سياسيًا على وجه الخصوص، تُعد أداة تخطيط السلامة #Think10 الخاصة بالمعهد الديموقراطي الوطني مورداً مفيداً لتزويده للذين قد يتعرضون لمخاطر شخصية متزايدة نتيجة لنشاطهم.

من الواضح أن رفاهية الموظفين هي أحد الأصول المهمة بالنسبة إليهم كأفراد، ولكنها تُعد كذلك عنصرًا حاسمًا في منظمة صحية وتعمل بشكل جيد. ومن أجل تحقيق ذلك الهدف، ضع في اعتبارك الموارد الإضافية التي يمكنك تقديمها للموظفين لحمايتهم ومساعدتهم على التعافي في حالة الهجوم المادي أو الرقمي. كما ذكرنا سابقًا في الدليل، فإن هذا يعني على الأقل وضع قائمة بالموارد التي يمكنك توصيل الموظفين بها للحصول على مساعدة قانونية وطبية والصحة النفسية والتقنية إذا لزم الأمر. مرة أخرى، يتضمن الدليل الميداني للحماية من المضايقات عبر الإنترنت التابع لمنظمة PEN America أفكارًا حول كيف يمكن للمنظمات دعم الموظفين أثناء الأزمات وبعدها ويتضمن دليل الأمان الشامل التابع لمنظمة Tactical Tech الكيفية التي تستجيب بها المنظمات غالبًا أثناء أوقات التهديدات الشديدة.

الأمان أثناء السفر

غالبًا ما يزيد السفر – سواء السفر إلى دولة أخرى أو بلدة على الطريق – من مخاطر أمن المعلومات الفعلية. بشكل عام، من السليم افتراض أنك لا تتمتع أنت وأجهزتك بحقوق الخصوصية عند عبور الحدود. وعلى هذا النحو، من الجيد تضمين سياسة سفر على المستوى التنظيمي ضمن خطة الأمان التي تشمل تذكيرات حول أفضل ممارسات الأمان الرئيسية. يجب أن تشتمل سياسة السفر الخاصة بمنظمتك على الكثير من المعلومات المغطاة في الأقسام الأخرى من الدليل، بما في ذلك إستخدام الإنترنت بأمان وتأمين الأجهزة ومصادر المعلومات الأخرى فعليًا وبقائها معك في كل الأوقات عند السفر. إذا كان ذلك ممكنًا، اترك معلوماتك الحساسة واستخدم جهاز كمبيوتر جديد لا يحتوي على أية معلومات على الإطلاق وقم بالوصول إلى الملفات التي تحتاجها بالفعل عبر السحابة، ثم امسحها عند العودة من السفر مرة أخرى.

بالإضافة إلى الاستعداد للسفر وتقليل حجم البيانات التي تتم مشاركتها عند السفر، هناك بعض النصائح التشغيلية الأساسية التي يجب عليك التفكير فيها وتضمينها في سياسة السفر التنظيمية الخاصة.

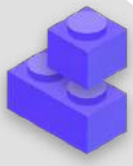
فكر في إستخدام أجهزة كمبيوتر محمول أو هواتف خاصة بالسفر لا تحتوي على بيانات حساسة أو بها قدر قليل منها. إذا كان يتم إنجاز عمل المنظمة عبر السحابة، فإن كروم بوك يمكن أن يكون خيارًا جيدًا غير مكلف نسبيًا لمثل هذا الجهاز. قم بإعادة تعيين إعدادات المصنع، أو "امسح"، لهذه الأجهزة عند عودتها قبل الاتصال بشبكات WiFi الشائعة في المنزل أو في المكتب.

قم بتحضير الموظفين لما يقومون به إذا قامت السلطات باستجوابهم أو توقفوا عند نقطة عبور حدودية. فكر في كيفية تحديد كمية المعلومات التي يسافر بها شخص ما إذا كان هذا مصدر قلق، وقم بإنشاء بروتوكولات تسجيل الوصول للموظفين الذين يسافرون إلى مناطق مهمة. قم بتزويد الموظفين بمعلومات الاتصال وخطة العمل لما يجب عليهم فعله إذا حدث خطأ ما في رحلتهم. وهذا يتضمن المعلومات المتعلقة بالمستشفيات المحلية أو العيادات أو الصيدليات في حالة كانوا بحاجة إلى مساعدة طبية أثناء السفر.

يجب على الموظفين أيضًا المحافظة على جميع الأجهزة على مسؤوليتهم الشخصية أثناء السفر. على سبيل المثال، ضع الكمبيوتر المحمول عند قدميك (ليس في المقصورة العلوية أو في الأمتعة المسجلة) عندما تكون على حافلة أو قطار أو طائرة. لا تفترض أن غرفة في فندق – أو حتى خزنة فندق – "مكان آمن" للاحتفاظ بالأجهزة والأشياء المهمة. لا تثق في منافذ الشحن USB العامة. أصبحت منافذ شحن USB في المطارات والمحطات والمركبات شيئًا مألوفًا بشكل متزايد وطريقة مريحة جدًا لشحن الأجهزة. وعلى الرغم من ذلك، يمكن أن تكون وسيلة سهلة للإصابة بالبرامج الضارة. لذلك، تأكد من شحن الأجهزة إما بالطريقة التلقيدية من خلال قابس في الجدار أو قم بشراء أجهزة حظر البيانات USB للسماح للموظفين المسافرين بشحن أجهزتهم عبر USB.

حجز السفر بأمان لمنظمتك

عند وضع سياسة سفر، ضع في اعتبارك المعلومات التي قد يتم كشفها عند تنظيم رحلة سفر أو حجزها. وبشكل خاص، يمكن أن يكون هذا مهمًا إذا كنت تنظم أحداث كبيرة أو تدريبات أو مؤتمرات تتعامل فيها مع معلومات حساسة من مجموعة متنوعة من الموظفين أو الشركاء أو الحاضرين. فكر جيدًا في كيفية مشاركة المعلومات الشخصية مثل تفاصيل جواز السفر ومسارات السفر والسجلات الطبية بأمان وتخزينها (إذا لزم الأمر). يحتوي كتاب أنشطة المنظم من منظمة Tactical Tech على ورقة عمل رائعة لمساعدة منظمتك على التفكير في الأسئلة الرئيسية المتعلقة بأمن السفر، اضغط على الرابط هنا.



حماية الأمن الفعلي الخاص بك

- **ذكّر الموظفين بضرورة حماية أجهزتهم فعليًا في جميع الأوقات.**
- **تحقق من جميع الطرق التي يمكن للأشخاص الوصول من خلالها إليك - الأبواب والنوافذ وقم بتأمينها.**
- **ضع سياسة لضيف المكتب وسياسة وصول.**
- **استخدم أقفال قوية وقم بتغييرها عند الحاجة.**
- **فكر في إعداد كاميرا أو نظام أمان مكتبي آخر.**
- **احصل على آلة تمزيق الورق واستخدمها.**
  - قم بإعداد وقت مخصص للموظفين للتخلص من المستندات المطبوعة التي تحتوي على معلومات حساسة.
- **ضع قائمة بالمهنيين والمنظمات ووكالات إنفاذ القانون التي يمكنك توصيل الموظفين بها للحصول على مساعدة قانونية وطبية ومساعة في الصحة النفسية ردًا على الهجمات أو التهديدات الفعلية.**
- **وضع سياسة تنظيمية للسفر.**
- **تأكد من أن الموظفين يعرفون ما يقومون به في حالة الطوارئ أثناء السفر، بما في ذلك تحضير الموظفين لما يجب القيام به إذا توقفوا عند الحدود أو نقطة تفتيش.**
- **قبل أي سفر محلي أو وطني أو دولي، ذكّر الموظفين بضرورة تقليل المعلومات المخزنة على الأجهزة.**
- **ضع في اعتبارك البيانات الإضافية التي يتم إنشائها ومشاركتها عند تنظيم السفر أو الأحداث.**

ما الذي يجب القيام به عندما تسوء الأمور

إذاً، إنك تعرف الأشياء الصحيحة التي يجب عليك القيام بها. لقد وضعت سياسات ودربت كل شخص في المنظمة على جميع الممارسات الفضلى. حتى مع كل هذا العمل الشاق، فمن المحتمل جدًا أن يحدث خطأ ما في النهاية.

وتحدث أشياء. عندما يحدث ذلك، من المهم أن يكون لديك خطة الاستجابة للحوادث. تُعد الاستجابة للحوادث جزءًا مهمًا، وغالبًا ما يتم التقليل من أهميتها، من خطة أمان المنظمة لأنها يمكن أن تكون الفرق بين الهجوم الذي يدمّر سمعة المنظمة أو عائق مزعج في الطريق. ضع في اعتبارك أنه يمكنك فقط الاستجابة إلى حادث إذا كنت على علم به. ويُعد وجود ثقافة أمنية تنظيمية قوية وتشجيع الموظفين على الإبلاغ عن المشكلات أمر مهم جدًا. وهذا هو السبب في أنه من الأفضل تحديد مكافأة عن السلوك الأمني الجيد بدلاً من معاقبة مرتكبي الهفوات والأخطاء. ومن المهم أيضًا التعبير عن التعاطف والتحقق من رفاهية الموظفين عند الإبلاغ عن حادثة. إنك تريد من الموظفين الإبلاغ على الفور عن رابط في رسالة تصيّد احتيالي تم النقر فوقه أو هاتف مسروق أو حساب وسائل تواصل اجتماعي مخترق – فلا يترددوا خوفًا من العقاب أو قلة الدعم. وبعد كل شيء، تُعد الاستجابة للحوادث، تمامًا مثل إستراتيجيات التخفيف المذكورة في الأقسام الأخرى من هذا الدليل، جهدًا على مستوى المنظمة.

- ما الذي يجب أن تخطط له؟ باختصار، أي شيء من المحتمل أن يحدث إلى حد ما. سيبدو ذلك مختلفًا بالنسبة لكل منظمة، ولكن الأسئلة الشائعة التي ستساعد خطة الاستجابة للحوادث في الرد وتشمل:
- ما الذي يجب علينا القيام به إذا تم اختراق حساباتنا أو مواقع الويب الخاصة بنا؟
- ماذا نفعل إذا قام شخص ما بالنقر فوق رسالة بريد إلكتروني للتصيّد الاحتيالي أو إذا كان الجهاز يعمل بشكل مريب؟
- ماذا نفعل إذا تمت سرقة رسائل بريد إلكتروني أو معظم المستندات الحساسة وتسريبها؟
- ماذا نفعل إذا تعرض أحد الموظفين لخطر فعلي أو تم إلقاء القبض عليه؟ أو إذا كان يعاني من التوتر والقلق بسبب مثل هذه التهديدات؟
- ماذا نفعل إذا تضرر مكتبنا في نشوب حريق أو فيضان أو كارثة طبيعية؟
- ماذا نفعل إذا تم ضياع كمبيوتر خاص بموظف أو هاتف أو سرقته؟

ستختلف الإجابة عن هذه الأسئلة وغيرها حسب المنظمة، ولكن من المهم التفكير بها معًا ووضع خطة واضحة ومشاركتها بحيث يستعد كل شخص في منظمتك باتخاذ إجراء فوري للحد من الضرر.

يعمل الاقتراض من دليل الأمان الشامل التابع لمنظمة Tactical Tech، مكان جيد للبدء بخطة الاستجابة السريعة على تحديد حادث أو حالة طوارئ في سياق منظمتك. حدد ما "حالة الطوارئ" – على سبيل المثال، النقطة التي يجب عندها البدء في تنفيذ الإجراءات وتدابير الطوارئ المخطط لها. وهذا مهم لأنه في بعض الأحيان سيكون غير واضح – إذا تخيلت سيناريو مثل فقدان الاتصال مع زميل في مهمة ميدانية؛ ما المدة التي ستنتظرها قبل إعلان حالة الطوارئ؟ لا يرغب الشخص في تصعيد الأمر مبكرًا جدًا، ولكن الانتظار لفترة طويلة قد يكون كارثيًا في بعض الحالات.

من المهم أيضًا التفكير في أي خطوة من الخطوات **التشغيلية** أيضًا. خصص لكل شخص دورًا واضحًا يكون على علم به ويوافق عليه مسبقًا – وسيعمل هذا على تقليل الإرتباك والذعر في حالة وقوع حادث. وفي حالة كل تهديد، فكر في الأدوار المختلفة التي قد يجب عليك القيام بها والجوانب العملية التي ينطوي عليها الاستجابة لحالة الطوارئ. وضمن هذه الإستراتيجية المهمة في حالات الطوارئ، يتم تنشيط شبكة دعم – شبكة حلفاء واسعة – والتي يمكن أن تضم الأصدقاء والعائلة والمجتمع والحلفاء المحليين والموارد الحكومية والحلفاء الوطنيين أو الدوليين مثل المنظمات غير الحكومية والصحفيين. كيف يمكن أن يدعمك حلفاؤك؟ هل يجب أن تتواصل معهم مقدمًا للتحقق من استعدادهم لتقديم المساعدة إليك في حالة الطوارئ وإخبارهم بما تتوقعه منهم؟

وعند الاستجابة إلى حادث ما، تزداد أهمية **الاتصالات** الفعالة. حدد أكثر الوسائل أمانًا وفاعلية للتواصل مع كل طرف في سيناريوهات مختلفة وحدد وسائل النسخ الاحتياطي. كن على علم أنه بالنسبة لحالات الطوارئ، قد يكون من المفيد حصولك على إرشادات واضحة حول ما يجب عليك القيام به (وما لا يجب عليك القيام به) للتواصل ومتى تتواصل وما القنوات التي يجب إستخدامها ومع من يجب أن تتواصل. كذلك، فكر في تأثير الحادثة على سمعة منظمتك، واستعد للرد وفقًا لذلك. تأكد من أن مسؤول الاتصالات في المنظمة (في بعض المنظمات قد يكون الشخص الذي يدير صفحة Facebook أو حساب Twitter) على دراية بالحادث ويمكنه مشاهدة وسائل التواصل الاجتماعي أو الوسائط الأخرى لمعرفة التأثير المحتمل الوقوع. كذلك، يجب أن يكون مستعدًا للإجابة على استفسارات عامة أو إعلامية حول حادث ما إذا كان ذلك مناسبًا. وهذا مهم بشكل خاص للقضاء على أية قصص سلبية محتملة أو الإضرار بالسمعة. في حين أن كل حادث وسياق مختلف، فإن الاتصالات الصادقة والشفافة غالبًا ما تبني الثقة بعد وقوع الحادث.

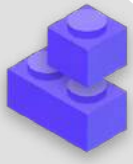
إنشاء نظام الإنذار المبكر والاستجابة

فكر في إنشاء نظام الإنذار المبكر والاستجابة. يبدو هذا النظام ممتازًا، ولكنه في الأساس مجرد وثيقة مركزية (إلكترونية أو غير ذلك) يتم فتحه في حالة الطوارئ. في المستند، يجب عليك تسجيل كافة التفاصيل المتعلقة بمؤشرات الأمان والحوادث التي حدثت في خط زمني وتقديم وصفًا واضحًا للإجراءات وتسلسل الاستجابة المخطط لها وتحديد ما يجب تحقيقه للإشارة إلى أن الخطر الذي حدث قد عاد وانخفض. كذلك، يجب أن يتضمن الإجراءات التي يجب اتخاذها بعد وقوع حادث لحماية المتورطين من وقوع المزيد من الأذى ومساعدتهم على التعافي جسديًا وعاطفيًا. يجب أن يوفر نظام الإنذار المبكر والاستجابة وثائق مفيدة للمشاركة في إنفاذ القانون (إن أمكن) والتحليل اللاحق لما حدث وإرشادات حول كيفية تحسين طرق الوقاية والاستجابات إلى التهديدات في المستقبل.

بالإضافة إلى المفاهيم المهمة للاستجابة للحوادث، يجب أن تستعد منظمتك لأي استجابة **تقنية** محددة. في بعض الحالات، يمكن إدارة الاستجابة التقنية بواسطة موظفي تكنولوجيا المعلومات أو مسؤولي النظام. على سبيل المثال، إذا ظهر أنه قد تم اختراق حساب بريد إلكتروني، فإنه يجب على مسؤول الحساب لديك الاستعداد وأن يكون قادرًا على إيقاف تشغيل الحساب المتأثر أو تعطيله. وعلى الرغم من ذلك، قد تتطلب بعض الحوادث التقنية خبرة لا تمتلكها داخل منظمتك. وبالنسبة لمثل هذه المواقف، من المهم تحديد قائمة موثوق بها تضم الخبراء الفنيين الخارجيين الذين يمكنهم مساعدتك في الاستجابة للحوادث. وفي بعض الحالات، قد ترغب في التفاوض مسبقًا على الشروط مع موفري الخدمة (مثل استضافة موقع الويب أو مستشار تكنولوجيا المعلومات) للتأكد من أنهم متاحون (ولن يفرضوا رسومًا إضافية) على مثل هذه الاستجابة الفنية.

وأخيرًا وليس آخرًا، يجب عليك وضع الخطوات **القانونية** في الاعتبار. من المهم فهم مستويات الحماية القانونية التي قد تكون لديك، بالإضافة إلى الالتزامات القانونية أو العواقب التي قد تواجهها منظمتك كنتيجة لخرق البيانات أو أي حادث أمني آخر. يمكن أن تتمثل الخطوة الأولى في اختيار مستشار قانوني موثوق به يفهم القوانين واللوائح الخاصة ببلدك أو منطقتك. خصص وقتًا لمراجعة الحوادث محتملة الوقوع مع المستشار القانوني ذي الصلة إذا لزم الأمر، وضع خطة لما ستقوم به عند الاستجابة. من الجيد عقد اتفاقًا مع هذا المستشار الموثوق لتمثيلك أنت ومصالحك إذا لزم الأمر بعد وقوع حادث. وكجزء من هذا الاستعداد القانوني، تأكد من فهمك للالتزامات القانونية تجاه أي بائعين أو شركاء. هل يجب عليهم إخطارك في حالة خرق البيانات الخاصة بهم؟ وما الدعم (إن وُجد) المطلوب منهم تقديمه في حالة وقوع حادث؟ أثناء قيامك بإبرام العقود والاتفاقيات مع بائعين خارجيين، ضع في اعتبارك احتمالية حدوث خرق بيانات أو أي حادث آخر.

في حين أنه لا يوجد مقاييس واحدة تلائم الجميع للاستجابة للحوادث، فإنه من الضروري وضع خطط تشغيلية وخطط اتصالات وخطط تقنية وخطط قانونية. أثناء وضع خطة الاستجابة للحوادث، فإننا نشجعك بشدة على الاستفادة من بعض الموارد الممتازة المتوفرة في الوقت الحالي والمصممة لمساعدة منظمات المجتمع المدني والمجموعات الأخرى ذات مستويات الخطورة العالية في التعامل مع الاستجابة للحوادث. تشمل هذه الموارد أدوات الإسعافات الأولية الرقمية والتي وضعتها RaReNet وCiviCERT والدليل الميداني للحماية من المضايقات عبر الإنترنت من PEN America ودليل مبادئ حملة الأمن السيبراني من Belfer Center ونموذج خطة اتصالات الحوادث الإلكترونية وخط مساعدة الأمن الرقمي من Access Now.



الاستجابة للحوادث

- **وضع خطة استجابة للحوادث التنظيمية وممارستها.**
  - فكر بإبداع في الحوادث المحتملة قبل حدوثها واستعد لاستجابتك.
- **تأكد من أن كل شخص داخل المنظمة على علم بكيفية التواصل وبالخطوات التقنية التي يجب اتخاذها في حالة وقوع حادث.**
- **خصص وقتًا لفهم تدابير الحماية والالتزامات القانونية الخاصة بك.**
- **استعد لتزويد الموظفين داخل المنظمة بالدعم العاطفي والاجتماعي الذي يحتاجونه بعد وقوع حادث.**

الملحق أ:
المصادر المُوصى بها

- دليل الأمان الشامل التابع لمنظمةTactical Tech؛ Creative Commons Attribution-ShareAlike 4.0 رخصة دولية
  - الفصل 2.4 – فهم معلوماتنا وفهرستها
  - الفصل 1.5 – التواصل فيما يتعلق بالتهديدات في الفرق والمنظمات
  - الفصل 3.4 – الأمان في المجموعات والمنظمات
- Security Education Companion الخاص بـ Electronic Frontier Foundation؛ Creative Commons Attribution 3.0 رخصة أمريكية
  - بيان نشاط نمذجة التهديد
- دليل الوقاية من التصيّد الاحتيالي ونظافة البريد الإلكتروني الخاص بـ Freedom of the Press Foundation؛ Creative Commons Attribution 4.0 رخصة دولية
- تأمين دليل الإشارة الخاص بـ Freedom of the Press Foundation؛ Creative Commons Attribution 4.0 رخصة دولية
- دليل الدفاع الذاتي ضد المراقبة (SSD) الخاص بـ Electronic Frontier Foundation؛ Creative Commons Attribution 3.0 رخصة أمريكية
  - ما الذي يجب أن أعرفه عن التشفير
  - التواصل مع الآخرين
  - اختيار VPN المناسب لك
- الدليل إلى تأمين أدوات الدردشة الجماعية والمؤتمرات الخاص بـ Frontline Defenders
- Tactical Tech›s Data Detox Kit
  - اسمح للشخص المناسب بالدخولاجعل كلمة مرورك أقوى
  - تقوية أقفال الشاشة
- دليل أمان الانتخابات المتعلق بكلمات المرور الخاص بـ Center for Democracy and Technology؛ Creative Commons Attribution 4.0 رخصة دولية
- دليل أمان الانتخابات المتعلق بالمصادقة ثنائية العامل الخاصة بأCenter for Democracy and Technology؛ Creative Commons Attribution 4.0 رخصة دولية
- المصادقة ثنائية العامل للمبتدئين الخاصة بـ Martin Shelton؛ Creative Commons Attribution 4.0 رخصة دولية
- الأمان في علبة الخاص بـ Tactical Tech وFrontline Defender؛ Creative Commons Attribution-ShareAlike 3.0 رخصة غير محمولة
  - حماية جهازك من البرامج الضارة وهجمات التصيّد الاحتيالي
  - حماية معلوماتك من الهجمات الفعلية
- أوه! النشرة الإخبارية الخاصة بـ SANS: أوقف تلك البرامج الضارة
- الوصول إلى الجهاز والبيانات عندما تكون السلامة الشخصية في خطر من Apple
- النظافة الإلكترونية للمنظمات القائمة على المهام الخاصة بـ Global Cyber Alliance Cyber

الملحق ب:
أدوات إطلاق خطة الأمان

استخدم أدوات إطلاق خطة الأمان التالية أثناء قيامك أنت وأعضاء منظمتك بقراءة هذا الدليل واستيعاب المادة، وفكر في الأسئلة الواردة مع زملائك للمساعدة في إنشاء مناقشة مثمرة.

تأكد من الرجوع إلى "العناصر الأساسية" الرئيسية في كل قسم من هذا الدليل للتأكد من أنك تغطي الموضوعات المهمة أثناء وضع خطة الأمان الخاصة بك. بنهاية الدليل، يجب عليك وضع العناصر الأساسية والإجابات على أسئلة المناقشة هذه وملاحظاتك من أساس الخطة الأمنية الناجحة!

بناء ثقافة الأمان

أساس قوي: تأمين الحسابات والأجهزة

توصيل البيانات وتخزينها بأمان

البقاء آمنًا على الإنترنت

حماية الأمن الفعلي

ما الذي يجب القيام به عندما تسوء الأمور

بناء ثقافة الأمان

أسئلة يجب وضعها في الاعتبار:

- متى يمكنك تحديد موعد لمحادثة لمراجعة خطة الأمان الخاصة بك مع موظفي المنظمة بالكامل؟
- ما الأيام أو الأوقات التي تناسب منظمتك لتحديد موعد للمحادثات المنتظمة والتدريب حول الأمن؟
- ما الخطوات التي يمكن أن تتخذها القيادة لتحقيق السلوك الأمني الجيد والالتزام بخطة الأمان الخاصة بك؟ كيف يمكن للآخرين في المنظمة لعب دورًا في الأمان؟

ملاحظاتك وأفكارك:

أساس قوي: تأمين الحسابات والأجهزة

أسئلة يجب وضعها في الاعتبار:

- كيف ستقوم بتنفيذ تدابير أمان الحساب – مثل تطبيق إدارة كلمات مرور والمصادقة ثنائية العامل – عبر المنظمة؟ ما العقبات التي قد تواجهها أثناء التنفيذ؟
- كيف ستضمن منظمتك الحفاظ على أمان الأجهزة وتحديثها؟ كجزء من هذا، هل ستحتاج المنظمة إلى خطة للتعامل مع البرامج أو أجهزة الكمبيوتر غير المرخصة؟
- ما الوقت المناسب لإعداد تدريب لجميع الموظفين حول مخاطر التصيّد الاحتيالي والبرامج الضارة وأفضل ممارسات أمان الأجهزة؟

ملاحظاتك وأفكارك:

توصيل البيانات وتخزينها بأمان

أسئلة يجب وضعها في الاعتبار:

- كيف ستعمل منظمتك على تنفيذ المراسلة المشفرة من طرف إلى طرف لتحقيق الاتصال الآمن؟ ما العقبات التي قد تواجهها أثناء التنفيذ؟
- كيف ستفرض منظمتك حل مشاركة الملفات الآمن داخليًا وخارجيًا؟ ما العقبات التي قد تواجهها أثناء التنفيذ؟
- كسف ستعمل منظمتك على تنفيذ حل تخزين بيانات ونسخ احتياطي آمن؟ ما العقبات التي قد تواجهها أثناء التنفيذ؟

ملاحظاتك وأفكارك:

البقاء آمنًا على الإنترنت

أسئلة يجب وضعها في الاعتبار:

- كيف ستعمل منظمتك على تنفيذ متطلبات الاستعراض الآمن مثل HTTPS ومستعرض موثوق، وإذا كان ذلك مناسبًا، شبكة VPN للموظفين؟
- ما العناصر الأساسية لسياسة وسائل التواصل الاجتماعي لمنظمتك؟ كيف سيتم تطبيقها؟
- كيف ستعمل منظمتك على حماية مواقع الويب وخصائص الويب الخاصة بها؟

ملاحظاتك وأفكارك:

حماية الأمن الفعلي

أسئلة يجب وضعها في الاعتبار:

- كيف ستعمل منظمتك على توزيع سياسة الضيف والوصول إلى المكتب وتنفذها؟
- من المسؤول عن تحضير الموظفين لتحديات الأمن الفعلي والرقمي التي قد يواجهونها أثناء السفر بغرض العمل؟
- ما الخطوات التي يمكن للموظفين اتخاذها للحفاظ على سلامة الأجهزة وتأمينها سواء في المكتب أو أثناء السفر؟

ملاحظاتك وأفكارك:

ما الذي يجب القيام به عندما تسوء الأمور

أسئلة يجب وضعها في الاعتبار:

- كيف ستقوم المنظمة بتوزيع سياسة الاستجابة للحوادث وممارستها؟
- هل هناك موارد متاحة للموظفين الذين قد يحتاجون إلى دعم عاطفي واجتماعي بعد وقوع حادث ما؟ إذا لم يكن الأمر كذلك، كيف يمكن أن تكون المنظمة قادرة على توفير تلك الموارد في حالة وقوع حادث؟

ملاحظاتك وأفكارك:

الملحق ج:
اقتباسات الصور

الصفحة 17: CNP Collection ,"Security Protection Anti-Virus Software cms"، 2014، صورة رقمية، Alamy Stock Photo،
https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.

الصفحة 24: Cottonbro، "Person Holding Black and Silver Key"، 2020، صورة رقمية، Pexels،
https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.

الصفحة 26: Blogtrepreneur، "Malware Infection"، 2016، صورة رقمية Flickr، https://www.flickr.com/photos/143601516@N03/.

الصفحة 29: "Microsoft Loading Screen"، صورة رقمية، Kompass، 23 سبتمبر، 2019
https://asset.kompas.com/crops/kYVdzylbrYB5llpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.

الصفحة 30: Mateuz Dach، "Turned-on iPhone and Displaying Icons"، 2017، صورة رقمية Pexels،
https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.

الصفحة 33: "Human right protection survey lure"، صورة رقمية، Mandiant، نوفمبر 2021،
https://www.mandiant.com/sites/default/files/2021-11/PeriscopeCambodia2.png.

الصفحة 38: Andrew Keymaster، "People Gathering on Street During Daytime Photo"، 2020، صورة رقمية، Unsplash،
https://unsplash.com/photos/JXQ2bizu7kc.

الصفحة 39: Surveillance Self-Defense، "No Encryption in Transit"، صورة رقمية، Electronic Frontier Foundation، 17 يناير، 2019.
https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

الصفحة 40: Surveillance Self-Defense، "Transport-layer-alternate.4"، الصورة الرقمية، Electronic Frontier Foundation، 17 يناير، 2019،
https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png.

الصفحة 42: Surveillance Self-Defense، "End-to-end Alternate .6"، الصورة الرقمية، Electronic Frontier Foundation، 17 يناير، 2019
https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.
Surveillance Self-Defense، "endtoendencryptionmetadata_.9"، 2019، صورة رقمية، Electronic Frontier Foundation,
https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

الصفحة 50: Brett Sayles، "Server Racks on Data Center"، 2020، صورة رقمية، Pexels،
https://www.pexels.com/photo/server-racks-on-data-center-4508751/.

الصفحة 55: PhotoMIX Company، 2016، "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky"، صورة رقمية، Pexels،
https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.

الصفحة 60: Stefan Coders، "laptop-screen-vpn-cyber-security"، 2020، صورة رقمية، Unsplash،
https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.

الصفحة 62: Surveillance Self-Defense، "Using the Tor Browser"، صورة رقمية، Electronic Frontier Foundation، 25 إبريل، 2020.
https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png

الصفحة 64: Nathan Dumlao، "White Samsung Android Smartphone on Brown Wooden Table"، 2020، صورة رقمية،
Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.

الصفحة 69: Matt Artz، "Two Broken 6-Pane On White Painted Wall Photo"، صورة رقمية، Unsplash، 1 أكتوبر، 2017،
https://unsplash.com/photos/vT684iB7Ejg.

NDI

NATIONAL
DEMOCRATIC
INSTITUTE