كتيب
الأمن السيبراني

للبرلمانات

دليل للبرلمانات التي تتطلع لإعداد خطة للأمن السيبراني

كُتيب
الأمن السيبراني

للبرلمانات

دليل للبرلمانات التي تتطلع لإعداد خطة للأمن السيبراني

جدول المحتويات

رسم بياني

ستجد في الكتيب عدة عناصر متكررة ومميزة بالإضافة إلى النص الرئيسي. إليك "وسيلة إيضاح" قصيرة لمساعدتك على فهم العناصر الأساسية:

دراسة حالة

يشير إلى دراسات الحالة التي تسلط الضوء على التأثير الواقعي لموضوع معين على البرلمانات على مستوى العالم أو في بلد معين.

نصائح إضافية

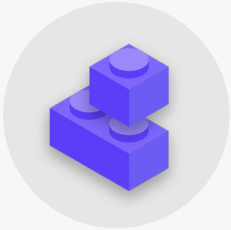
يبرز بعض النصائح والمعلومات الإضافية التي يجب الانتباه إليها أثناء قراءة الدليل.

العالم الحقيقي

يستدعي أمثلة شائعة لأدوات تدابير الأمن السيبراني المستخدمة في "العالم الحقيقي"، للأهداف الجيدة والسيئة على حدٍ سواء.

متقدم

يشير إلى موضوع متقدم - معلومات مهمة ليأخذها البرلمان في الاعتبار، ولكنها قد تكون أكثر تقنية أو معقدة بعض الشيء.



اللبنات الأساسية لخطة الأمان

يشير إلى "اللبنات الأساسية لخطة الأمان"، والتي تعتبر العناصر الأساسية من كل قسم من أقسام الدليل.

أفضل 10 نصائح

هذه العناصر العشرة بالغة الأهمية لخطة برلمانكم الأمنية. إذا كنت تبحث عن مكان لتبدأ منه، فابحث هنا أولاً.

1. قم بإجراء تدريب أمني منتظم داخل برلمانك
2. كن متيقظًا ضد التصيد الاحتيالي واحصل على نظام إبلاغ
3. استخدم التشفير من طرف إلى طرف في جميع الاتصالات، إن أمكن
4. برنامج أو تطبيق إدارة كلمات المرور
5. اطلب المصادقة ذات العاملين حيثما أمكن ذلك
6. تأكد من تحديث جميع أجهزة وبرامج الموظفين
7. استخدام التخزين السحابي الآمن
8. استخدم HTTPS، وإذا كان ذلك مناسبًا، VPN، للوصول إلى الإنترنت
9. قم بحماية الأصول المادية للبرلمان الخاص بك
10. ضع خطة تنظيمية للاستجابة للحوادث

1

بناء ثقافة الأمان

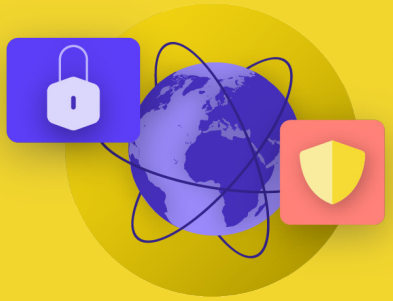
2

أساس قوي: تأمين الحسابات والأجهزة

3

توصيل و تخزين البيانات بشكل آمن

4



البقاء آمنًا على الإنترنت

5

حماية الأمن المادي المتقدم

6

ما الذي يجب القيام به عندما تسوء الأمور

المؤلفون والتقدير والعرفان

تم اعداد هذا الدليل من قبل المعهد الديمقراطي الوطني (NDI) وشراكة الديمقراطية في مجلس النواب (HDP).

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

المؤلفون المساهمون: **Sarah Moulton (NDI)؛ و Chris Doten (NDI) سارة مولتون و كريس دوتن**

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

فيونا كراكنبرغر Open Technology Fund؛ بيل بودينغتون وشيرين موري، Electronic Frontier Foundation؛ جوسلين وولبرايت، Cloudflare؛ مارتن شيلتون، Freedom of the Press Foundation؛ ديف ليختمان، Microsoft؛ ستيفن بويس، International Foundation for Electoral Systems؛ آمي ستودارت، International Republican Institute؛ إيما هولينجسورث، Global Cyber Alliance؛ كارولين سيندرز، Convocation Design + Research؛ ديتا كاتوراني ساندرا بيبيرا، المعهد الديمقراطي الوطني؛ آرون أزلتون، المعهد الديمقراطي الوطني؛ فريدا أرينوس، المعهد الديمقراطي الوطني؛ أنتوني دي أنجيلو، المعهد الديمقراطي الوطني؛ ويتني فايفر، المعهد الديمقراطي الوطني؛ وديريك لويتن، House Democracy Partnership كما نود أن نشكر بول كولي في خدمات المعلومات التشريعية في ليبيريا، ونهاد بهرام وفؤاد أحمد في برلمان كردستان-العراق، ودينا بلاتا في مجلس الشيوخ في كولومبيا؛ إياد عباس وماجد خضر في مجلس النواب العراقي، وتانيا دانيلوفسكا في مجلس جمهورية مقدونيا الشمالية على رؤاهم وإسهاماتهم القيمة.

ونودّ أيضًا أن نعترف بفضل جميع الأدلة والكتب الإرشادية وكُتب العمل ووحدات التدريب وغيرها من المواد المذهلة التي وضعها مجتمع الأمن التنظيمي (OrgSec). تم تصميم هذا الدليل لاستكمال تلك المواد الأكثر تعمقًا، حيث يجمع بين الدروس الرئيسية في مورد شامل وسهل القراءة للبرلمانات التي تتطلع إلى البدء في خطة للأمن 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 لمنظمة Tactical Tech، ومجموعة من الشروحات من Center for Democracy and Technology و Freedom of the Press Foundation. يمكنك العثور على اقتباسات محددة لهذه المصادر من خلال الأقسام التالية، والروابط الكاملة ومعلومات حول المؤلف والترخيص في الملحق أ.

من نحن؟

يُعد National Democratic Institute for International Affairs (NDI) منظمة غير ربحية وغير حزبية، مقرها في واشنطن، تعمل بالشراكة حول العالم لتعزيز وحماية المنظمات الديموقراطية والعمليات والمعايير والقيم لضمان نوعية حياة أفضل للجميع.

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

وفي نطاق NDI، يسعى فريق الديموقراطية والتكنولوجيا إلى تعزيز نظام بيئي رقمي شامل يتم فيه حماية القيم الديموقراطية وتعزيزها، ويمكن أن ينجح هذا الأمر؛ وتُعد الحكومات أكثر شفافية وشمولية؛ ويتمتع جميع المواطنين بصلاحية مساءلة الحكومة. وإننا نقوم بهذا العمل من خلال دعم شبكة عالمية من النشطاء الملتزمين بالمرونة الرقمية، ومن خلال تعاون الشركاء فيما يتعلق بالأدوات والمصادر مثل هذا الكُتيب. 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 إليك ونرد على تساؤلاتك حول فريقنا وعملنا في تكنولوجيا الأمن السيبراني والديموقراطية.

تعمل شراكة مجلس النواب للديمقراطية (HDP) مع الهيئات التشريعية في جميع أنحاء العالم لتعزيز استجابة الحكومة الفعالة وتعزيز المؤسسات الديمقراطية. يتمثل محور عملنا في التعاون بين الأقران لبناء الخبرة الفنية في الهيئات التشريعية الشريكة التي من شأنها تعزيز المساءلة والشفافية والاستقلال التشريعي والوصول إلى المعلومات والرقابة الحكومية. لدى HDP حاليًا شراكات مع أكثر من 20 هيئة تشريعية وطنية حول العالم. تشمل مجالات التعاون مع البرلمانات الشريكة لـ HDP معالجة قضايا الميزانية وضمان عمليات أكثر فاعلية للجان وتعزيز الخدمات التأسيسية وتوفير أدوات لإشراف أقوى وتعزيز الأخلاقيات التشريعية وتحسين تكنولوجيا المعلومات والمكتبات والبحوث والعمليات والإجراءات التشريعية. يتم تنفيذ برامج HDP من قبل المعهد الديمقراطي الوطني (NDI) والمعهد الجمهوري الدولي (IRI) من خلال اتفاقية تمويل تعاوني مع الوكالة الأمريكية للتنمية الدولية (USAID).

من يدير الأمن السيبراني البرلماني؟

يتطلب البرلمان الفعال والآمن موظفين يتمتعون بالمهارة والسلطة المناسبة لتنفيذ التوصيات الواردة في هذا الدليل. مع ذلك، يمكن للمسؤولين عن الأمن السيبراني في البرلمانات أن يتفاوتوا على نطاق واسع، ولا يوجد نموذج واحد "مناسب" لمن يجب أن يتعامل مع الأمن السيبراني. في بعض الحالات، قد يكون فريقًا مخصصًا للأمن السيبراني داخل وحدة تكنولوجيا المعلومات الخاصة بك، وفي حالات أخرى مجموعة من الموظفين الإداريين والأعضاء على حد سواء. بغض النظر، ضع في اعتبارك أنه في حين أنه من المهم أن يكون لديك فريق جيد مسؤول عن الأمن السيبراني للبرلمان الخاص بك، فإنه من مسؤولية الجميع في البرلمان وحوله اتباع السياسات والإجراءات اللازمة للحفاظ على أمان البرلمان. فيما يلي بعض الأمثلة على نماذج التوظيف المختلفة لإدارة الأمن السيبراني البرلماني:

مجلس النواب الأمريكي

في مجلس النواب الأمريكي، تقوم بعض المكاتب الأعضاء منفردة بتعيين مسؤول أنظمة يكون مسؤولاً عن إدارة جميع أجهزة الكمبيوتر وأنظمة البرامج التي يستخدمها المكتب - بما في ذلك إدارة اعتبارات الأمن السيبراني - وتدريب الموظفين على أفضل الممارسات. على المستوى المؤسسي، يضم كبير المسؤولين الإداريين في مجلس النواب فريق موارد المعلومات، والذي يضم قسمًا مخصصًا لأمن المعلومات.

جمعية زامبيا الوطنية

تعتمد جمعية زامبيا الوطنية على إدارة تكنولوجيا المعلومات والاتصالات (ICT) لديها لمجموعة متنوعة من الوظائف، بما في ذلك إدارة برمجيات البرلمان والأجهزة والبنية التحتية للمعلومات، وتدريب الأعضاء أو البرلمان والموظفين على أنظمة التكنولوجيا، وتأمين البنية التحتية للمعلومات في البرلمان من تهديدات الأمن السيبراني الداخلية والخارجية.

برلمان ماليزيا

يضم البرلمان الماليزي قسم تكنولوجيا المعلومات التابع له تحت إشراف مدير البرلمان، مما يسمح له بخدمة مجلسي البرلمان. يتضمن هذا القسم وظيفة محددة لأمن الشبكة، مما يسمح له بالتأكد من أن أنظمة الشبكة ومراكز البيانات والبنية التحتية لتكنولوجيا المعلومات والاتصالات محدثة وآمنة قدر الإمكان.

لمن هذا الدليل؟

تمت كتابة هذا الكتيب لهدف بسيط: مساعدة برلمانك على تطوير خطة أمن إلكتروني مفهومة وقابلة للتنفيذ.

نظرًا لأن العالم يتنقل عبر الإنترنت بشكل متزايد، فإن الأمن السيبراني ليس مجرد كلمة طنانة ولكنه مفهوم حاسم لنجاح البرلمانات، وأمن المعلومات (سواء عبر الإنترنت أو خارجها) و يمثل تحديًا يتطلب التركيز والاستثمار واليقظة.

من المحتمل أن يجد برلمانك نفسه - إن لم يكن بالفعل - هدفًا لهجوم الأمن السيبراني. وليس المقصود من هذا أن نثير القلق؛ ولكنّه الواقع حتى بالنسبة للبرلمانات التي لا تعتبر نفسها أهدافًا معينة.

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. بالإضافة إلى مثل هذه الهجمات المبلغ عنها، هناك على الأرجح المئات من الهجمات الصغيرة الأخرى كل عام التي لا يتم اكتشافها أو الإبلاغ عنها، والعديد منها يستهدف المؤسسات الحكومية والهيئات التشريعية والمنظمات السياسية.

ويكون لمثل هذه الهجمات الإلكترونية عواقب وخيمة. سواء كان هدفهم هو تعطيل العمليات البرلمانية، أو الإضرار بسمعتك، أو حتى سرقة المعلومات التي يمكن أن تؤدي إلى ضرر نفسي أو جسدي لأعضائك أو موظفيك، يجب أن تؤخذ 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 برلمانية قوية.

إذا لم تفكر مطلقًا في الأمن السيبراني لبرلمانك، أو لم يكن لديك الوقت للتركيز عليه، أو تعرف بعض الأساسيات حول هذا الموضوع ولكنك تعتقد أن برلمانك يمكن أن يعزز الأمن السيبراني الخاص به، فهذا الدليل مناسب لك. **بغض النظر عن خلفيتك، يهدف هذا الدليل إلى تزويد البرلمان بالمعلومات الأساسية التي يحتاجها لوضع خطة أمنية قوية - وهي خطة تتجاوز مجرد وضع الكلمات على الورق وتمكنك من تطبيق أفضل الممارسات.**

ما خطة الأمان ولماذا يجب على برلماننا أن يضع واحدة؟

إن خطة الأمان عبارة عن مجموعة من السياسات والإجراءات والتعليمات المكتوبة التي وافق عليها برلمانك لتحقيق مستوى الأمان الذي تعتقد أنت وفريقك أنه مناسب للحفاظ على أمن موظفيك وشركائك ومعلوماتك.

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 لبرلمانك. بدون التفكير في خطة شاملة، من السهل جدًا إغفال بعض أنواع التهديدات، أو التركيز على نوع واحد من المخاطر أو حتى تجاهل الأمن السيبراني إلى ان تحدث أزمة. عندما تبدأ في تطوير خطة أمان، هنالك بعض الأسئلة المهمة التي يجب أن تطرحها على نفسك فيما يُعرف بعملية **تقييم المخاطر**. وتُساعد الإجابة عن هذه الأسئلة برلمانك في فهم التهديدات الفريدة التي تواجهها وتسمح لك بالرجوع خطوة إلى الوراء والتفكير بشكل شامل حول ما وممّن تحتاج حمايته. يمكن للخبراء الاستشاريين المدربين تقديم المساعدة في قيادة برلمانكم خلال هذه العملية، من خلال مساعدة بعض الانظمة مثل إطار عمل التدقيق SAFETAG الخاص بشركة Internews. في حال كان بإمكانك الوصول الى هذا المستوى من الخبرة المهنية، فان الامر يستحق الجهد المبذول. ولكن حتى إذا لم تتمكن من الخضوع لتقييم كامل، فإنه يجب يجب ان تلتقي مع اصحاب المصلحة عبر البرلمان للنظر بعناية في هذه الأسئلة الرئيسية:

1 ما الأصول التي يمتلكها برلمانكم وما الذي ترغب في حمايته؟

يمكنك البدء في الإجابة على هذه الأسئلة من خلال إنشاء بيان لجميع أصول البرلمان الخاص بك. وتُعد 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 للبرلمان، ومكان الاحتفاظ بها (ربما عدة أماكن رقمية أو مادية)، وما الذي يمنع الآخرين من الوصول إليها أو إتلافها أو تعطيلها. مع الأخذ بالاعتبار ليست جميع الأمور أو الملفات على نفس القدر من الأهمية. إذا كانت بعض بيانات البرلمان تتعلق بسجل عام أو معلومات قمت بنشرها بالفعل، فإنها ليست أسرارًا تحتاج إلى حمايتها.

2 من خصومك وما قدراتهم ودوافعهم؟

يُعد "الخصم" مصطلح شائع الاستخدام في الأمن التنظيمي. بعبارات بسيطة، الخصوم هم الفاعلون (أفراد أو مجموعات) المهتمون باستهداف برلمانك وتعطيل عملك والوصول إلى معلوماتك أو تدميرها. يمكن أن تشمل أمثلة الخصوم المحتملين المحتالين الماليين أو الحكومات المعادية أو المخترقين ذوي الدوافع الأيديولوجية أو السياسية. ومن المهم وضع قائمة بخصومك والتفكير بشكل نقدي حول من قد يرغب في التأثير سلبًا على برلمانك 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 استخدام 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 برلمانك؟ ربما يكونون عازمين على مسح رسالتك بشكل نهائي أو تعطيل عمل البرلمان؟ ومن المهم فهم دوافع الخصم لأن القيام بذلك يمكن أن يساعد برلمانك في تقييم التهديدات التي يمكن أن تطرأ بشكل أفضل.

3 ما هي التهديدات التي يواجهها برلمانكم؟ 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 برلمانك من اتخاذ خطوات مثمرة تالية، من المفيد تحليل كل تهديد استنادًا إلى عاملين:احتمالية حدوث التهديد وتأثير التهديد إذا حدث.

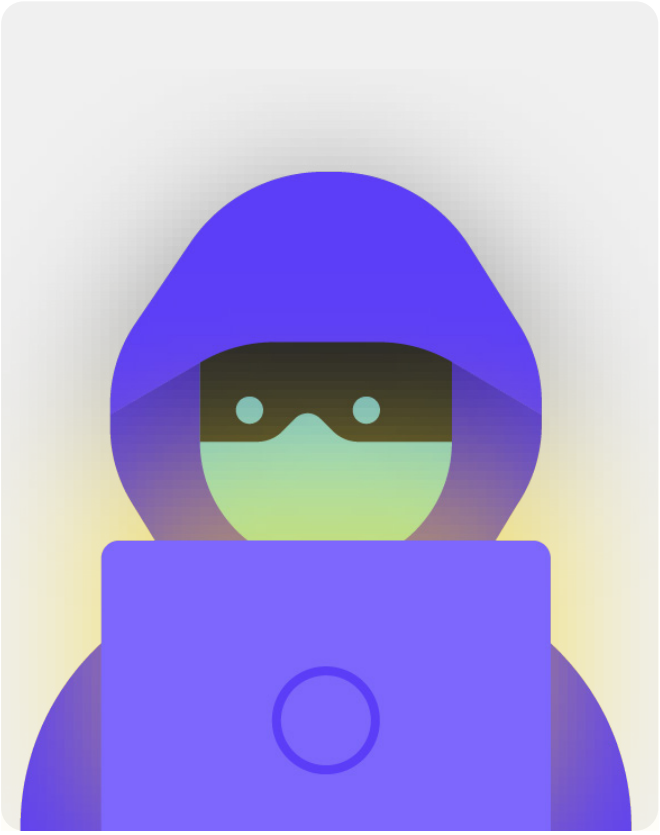
ولقياس احتمالية حدوث تهديد (ربما "منخفضة أو متوسطة أو عالية"، استنادًا إلى ما إذا كان من غير المحتمل وقوع حدث معين أو يمكن أن يحدث أو يحدث بشكل متكرر)، فإنه يمكنك استخدام المعلومات التي تعرفها عن قدرة خصومك ودوافعهم وتحليل الحوادث الأمنية السابقة وتجارب برلمانات أخرى مماثلة وبالطبع وجود أية إستراتيجيات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

لقياس تأثير تهديد ما، فكر في الشكل الذي سيبدو عليه عالمك إذا حدث التهديد بالفعل. واطرح أسئلة مثل "كيف أضرنا التهديد بصفتنا برلمانًا 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 أهدافنا 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 مدروسة. ومن خلال التركيز على تلك التهديدات التي من المرجح 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.ويبدو هذا جيدًا: يمكنك فعل الكثير لحماية نفسك وزملائك وبرلمانك من خلال الاهتمام بالتهديدات الأكبر.

ولمساعدتك في إدارة عملية تقييم المخاطر هذه، فكر في استخدام ورقة عمل، مثل هذه التي وضعتها Electronic Frontier Foundation. وتذكر 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.



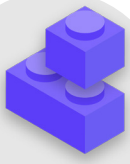
إنشاء خطة الأمن السيبراني لبرلمانك

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

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

ويسعى هذا الدليل إلى توفير خيارات واقتراحات مجانية أو منخفضة التكلفة للغاية. وضع في اعتبارك أن أهم تكلفة مرتبطة بتنفيذ خطة أمان فعالة ستكون عبارة عن الوقت الذي تحتاجه أنت والموظفون والأعضاء والفرق عبر البرلمان للتحدث عن خطتك الجديدة وتعلمها وتنفيذها. وبالنظر إلى المخاطر التي من المحتمل أن يواجهها برلمانكم، فإن هذا الاستثمار يستحق العناء.

وفي كل قسم، ستجد شرحًا لموضوع رئيسي يجب أن يكون برلمانك وموظفيه على دراية به - وبماهيته وسبب أهميته. ويتم إقران كل موضوع بالإستراتيجيات الأساسية والأساليب والأدوات المُوصى بها للحد من المخاطر والنصائح وروابط إلى موارد إضافية يمكن أن تساعدك في تنفيذ مثل هذه التوصيات عبر برلمانك.



أدوات إطلاق خطة الأمان

لمساعدة برلمانك 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 الحد الأدنى.

استفد من المصادر الأخرى التي يمكن أن تساعدك في وضع خطة وتنفيذها أيضًا.

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

بناء ثقافة الأمان

يتعلق الأمن بالناس، ولحماية برلمانك تحتاج إلى التأكد من أن كل من يشارك - بما في ذلك أعضاء البرلمان (النواب) وموظفي الدعم التشريعي وموظفي خدمات البحث والموظفين الإداريين في الشؤون المالية والموارد البشرية وتكنولوجيا المعلومات من بين العديد من الآخرين - يأخذ الأمن السيبراني على محمل الجد. ويُعد تغيير الثقافة أمرًا صعبًا، ولكن يمكن لبضع خطوات بسيطة ومحادثات مهمة أن تقطع شوطًا طويلاً نحو خلق أجواء تخلق مرونة لدى موظفيك وبرلمانك و تمكّنهم من مواجهة تهديدات الأمن السيبراني. إن واحدة من أبسط وأهم الخطوات التي يجب اتخاذها لتأسيس ثقافة الأمان التنظيمي هي التواصل داخل وعبر برلمانك وقيام القادة بنمذجة السلوك الجيد دائمًا.

بناء ثقافة الأمن في البرلمانات

في فبراير 2019، تعرضت أستراليا لهجوم إلكتروني أضر بشبكات البرلمان الوطني الأسترالي وثلاثة أحزاب سياسية بارزة. تمكن المهاجمون من الوصول إلى أوراق السياسة ومراسلات البريد الإلكتروني الخاصة بين النواب وموظفيهم وناخبيهم. وقع الهجوم قبل ثلاثة أشهر فقط من الموعد المقرر لإجراء الانتخابات، مما يسلط الضوء على ضعف الشبكات غير الآمنة أثناء الانتخابات.

ردًا على هذا الهجوم الكبير والناجح، بذل البرلمان جهودًا لتعزيز استعداده على صعيد الأمن السيبراني. وشمل هذا الاستثمار تحقيق اللجنة المشتركة للحسابات العامة ومراجعي الحسابات في المرونة الإلكترونية للكومنولث. اعتمد التحقيق على نتائج عمليات التدقيق التي أجريت على مدى عدة سنوات والتي وجدت أن عمليات التخفيف من مخاطر الأمن السيبراني غير موجودة داخل البرلمان والوكالات الحكومية الأخرى. على سبيل المثال، سلط مكتب التدقيق الوطني الأسترالي الضوء على فشل البرلمان في التركيز على الأهداف الإستراتيجية طويلة المدى وفي تطوير نهج قائم على المخاطر عندما يتعلق الأمر بالأمن السيبراني. وعلى الرغم من أن الاستفسارات وعمليات التدقيق لم تكن مُرضية، فإن رغبة البرلمان في تحديد مشاكل الأمن السيبراني والاستثمار في معالجتها هي مثال على خلق ثقافة تفضي إلى الأمن السيبراني البرلماني الفعال.
و يبدأ بالتعرف على المشاكل والاستثمار في الحلول التقنية والبشرية، حيث لا يتم تجنب الأمن بل يتم تحديد أولوياته. على سبيل المثال، من خلال تعيين فريق "رفع مستوى الأمن السيبراني" والاستثمار في الميزانية لـ "صندوق الاستجابة للأمن السيبراني"، يجب أن يكون البرلمان (والهيئات الحكومية الأخرى) مجهزًا بشكل أفضل للتخفيف من الهجمات المستقبلية إذا تم نشر هذه الموارد بشكل صحيح واستدامتها و لا يزال التركيز على الأمن السيبراني كعنصر منتظم في العمليات البرلمانية. مع ذلك، من الأفضل بالطبع بناء هذا الالتزام بالأمن داخل برلمانكم *قبل* حدوث خرق أمني كبير.

دمج الأمان في هيكل التشغيل العادي

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 المذعور 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 أسبوعيًا، ولكن اجعله تذكيرًا دوريًا. يجب ألا تترك هذه المناقشات مساحة لموضوعات الأمن التقني فقط، بل يجب أيضًا أن تترك المشكلات التي تؤثر على راحة الموظفين وسلامتهم مثل المضايقات عبر الإنترنت (ودون الاتصال بالإنترنت) أو المشكلات المتعلقة باستخدام الأدوات الرقمية وتنفيذها. يمكن أن تشمل المحادثات موضوعات مثل المعلومات دون اتصال- مشاركة العادات والطرق التي يتبناها الموظفون أو عدم تأمين المعلومات خارج البرلمان. بعد كل شيء، من المهم أن نتذكر أن أمان البرلمان يكون قويًا بقدر ارتباطه الأضعف فقط. تتمثل إحدى طرق تحقيق المشاركة المتسقة عن طريق إضافة الأمان إلى جدول أعمال اجتماع عادي. ويمكنك أيضًا تناوب المسؤولية لتنظيم وتسهيل مناقشة حول الأمان بين مختلف الموظفين، مما يمكن أن يساعد في تطوير فكرة أن الأمن مسؤولية الجميع وليس فقط مسؤولية قلة 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 للبرلمان، مثل أثناء تهيئة الموظفين والتفكير في قطع الوصول إلى الأنظمة أثناء المغادرة. 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 عند تغيير الأوضاع الأمنية لديك.

خطط 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 التنظيمي

وإن جزء من ثقافة الأمان الناجحة كذلك هو ضمان التعاون عبر البرلمان لخطة الأمان الخاصة بك.

ويجب أن يشمل هذا بشكل حاسم دعمًا قويًا وصريحًا وتوجيهًا من القادة الذين سيتخذون، في كثير من الحالات، القرار النهائي بتخصيص الوقت والموارد والطاقة لوضع خطة أمان فعالة وتنفيذها. إذا لم يأخذوا الأمر على محمل الجد، فلن يقوم أحد بذلك. لتحقيق هذا التعاون، فكر جيدًا في وقت تقديم خطتك وكيفية حدوث ذلك، وافعل ذلك بطريقة واضحة وتأكد من أن القيادة تعزز الرسائل واطلع الجميع على كافة عناصر الخطة وخطواتها بحيث لا يكون هناك أمور غامضة أو ارتباكًا فيما يتعلق بما تحاول تحقيقه. تأكد من تخصيص ميزانية مناسبة للأمن السيبراني عبر البرلمان أيضًا. على الرغم من أن الموارد المالية قد تكون محدودة، فمن الضروري الاستثمار بشكل مناسب في الأمن السيبراني، وإلا فمن المحتمل أن تتعرض الاستثمارات الأخرى للخطر. وعند التحدث عن الأمان، تجنب الأساليب الترويعية. قد تكون التهديدات التي يواجهها البرلمان والموظفون مخيفة في بعض الأحيان، لكن حاول التركيز على مشاركة الحقائق وخلق مساحة هادئة للأسئلة والمخاوف. يمكن أن يؤدي تضخيم الأخطار لدرجة تبدو بها أنها مهددة للغاية إلى رفض الناس لك بصفتك مروج للأخبار المثيرة أو الاستسلام ببساطة، معتقدين أنه لا شيء يفعلونه مهم – ولا شيء أبعد عن الحقيقة.

وضع خطة تدريبية

بمجرد وضع خطة والالتزام بها، فكر في كيفية تدريب جميع الموظفين والمتطوعين على أفضل هذه الممارسات الجديدة.

يمكن أن يكون طلب التدريب المنتظم - وجعل حضور التدريب إلزاميًا - أسلوبًا مفيدًا. تجنب خلق عواقب وخيمة وسلبية للموظفين الذين يعانون من التعامل مع مفاهيم الأمان. وضع في اعتبارك أن بعض الموظفين قد يتكيفون ويتعرفون 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 فقط. ومع ذلك، يمكن أن يساعد إنشاء المساءلة الإيجابية والمكافآت للتدريب الناجح واعتماد سياسات في تحفيز التحسينات عبر البرلمان. 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 (منظمة الصحافة الحرة والمحدودة) و Greenhost ومدخل التعلم من Global Cyber Alliance (التحالف الدولي لحماية الأمن السيبراني).

فكر كيف يمكن أن تصل خطة التدريب الخاصة بك إلى النواب والموظفين البرلمانيين والإدارة البرلمانية أيضًا. مع الوضع في الاعتبار أن الأعضاء البارزين يحتاجون في كثير من الأحيان إلى مزيد من التدريب والاهتمام عندما يتعلق الأمر بالأمن بسبب مكانتهم العالية. تأكد من أن خطة التدريب وخطة الأمان الخاصة بك تنطبق على جميع هذه الأنواع المختلفة من الأفراد وأي أصول قد تكون لديهم في داخل وخارج البرلمان.

بناء ثقافة الأمان

- **حدد مواعيد محادثات وتدريبات منتظمة عن الأمان وخطة الأمان الخاصة بك.**
- **أشرك الجميع - ووزع مسؤولية تنفيذ خطة الأمان الخاصة بك عبر البرلمان بأكمله.**
- **تأكد من نماذج القيادة للسلوك الأمني الجيد والالتزام بخطتك.**
- **تجنب أساليب الترهيب أو العقاب - وضع مكافأة للتحسين وقم بإنشاء مساحة مريحة للموظفين للإبلاغ عن المشكلات وطلب المساعدة**
- **قم بتحديث خطتك الأمنية سنويًا أو بعد تغييرات كبيرة في طاقم العمل البرلماني أو الهيكلية أو بيئة التشغيل.**

أساس قوي: تأمين الحسابات والأجهزة

لماذا التركيز على الحسابات والأجهزة؟ لأنها تُشكل أساس كل شيء رقمي يقوم به برلمانك.

معظمنا يصل إلى معلومات حساسة ويتواصل داخليًا وخارجيًا ويحفظ معلومات خاصة على الأجهزة والحسابات. اهتم فقط بمشاركة الأعضاء في الجلسات العامة، والتصويت (بما في ذلك الافتراضي)، وعمليات الصياغة التشريعية، والتواصل مع الموظفين والجمهور العام. بدون حسابات وأجهزة آمنة، يمكن تعريض هذه العمليات البرلمانية الهامة وغيرها للخطر.

على سبيل المثال، إذا كان المخترقون 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 تمكن أحد الخصوم من الوصول إلى حسابات برلمانك على وسائل التواصل الاجتماعي، فيمكنه بسهولة الإضرار بسمعتك ومصداقيتك، مما يقوض الثقة مع الجمهور. لذلك، من الضروري كبرلمان التأكد من أن الجميع يتخذ بعض الخطوات البسيطة والفعالة للحفاظ على أمان أجهزتهم وحساباتهم. ومن المهم ملاحظة أن هذه التوصيات تشمل حسابات شخصية وأجهزة أيضًا، حيث إنها غالبًا ما تكون أهدافًا سهلة للخصوم. وسوف يسعى المخترقون بكل سرور وراء الهدف الأسهل واقتحام حساب شخصي أو كمبيوتر منزلي إذا كان الأعضاء والموظفون يستخدمونه للتواصل والوصول إلى المعلومات المهمة.

تأمين الحسابات و البرلمانات

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) و Cisco (سيسكو)، وكانت المنظمات غير الحكومية نتيجة جزئية لتخمين المخترقين لكلمات المرور الضعيفة التي تم استخدامها في حسابات المسؤولين المهمة. وبشكل عام، تحدث الاختراقات المتعلقة بالقرصنة بسبب كلمات المرور الضعيفة أو المُعاد استخدامها بنسبة 80 بالمائة.

ومع الانتشار المتزايد لاختراقات كلمات المرور مثل هذا وسهولة وصول جميع أنواع الخصوم إلى الأدوات المتطورة لاختراق كلمات المرور، تُعد أفضل ممارسات كلمات المرور والمصادقة ثنائية العامل من متطلبات الأمان لجميع المنظمات، بما في ذلك البرلمانات. لا توجد حادثة توضح هذا أكثر من هجوم عام 2017 على نظام البريد الإلكتروني في البرلمان البريطاني. في هذه الحادثة، أدت ممارسات كلمات المرور الضعيفة من عدد صغير ولكن ذو مغزى من أعضاء البرلمان إلى كشف حسابات البريد الإلكتروني والمحادثات، وآلاف من بيانات الاعتماد المسربة، وتعطيل هائل للعمليات البرلمانية. وفقًا للمكتب الصحفي للبرلمان البريطاني، تم اختراق الحسابات المخترقة نتيجة لضعف كلمات المرور التي لا تتوافق مع الإرشادات الصادرة عن الخدمة الرقمية البرلمانية.

تأمين الحسابات: كلمات المرور والمصادقة ثنائية العامل

في الوقت المعاصر، من المحتمل أن يكون لدى برلمانك وموظفيه 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 الفرديون والبرلمان 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 الجيد نهجًا مختلفًا لحماية جميع هذه الحسابات من الهجمات. ويبدأ ذلك بضمان سلامة كلمة المرور الجيدة واستخدام المصادقة ذات العاملين من قبل الجميع.

ما الذي يجعل كلمة المرور جيدة؟

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

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 تقل كلمات المرور الخاصة بك عن 16 حرفًا بحد أدنى أو خمسة كلمات على الأقل ويُفضل 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.
التفرد	ربما تكون "الممارسة الأسوأ" الأكثر شيوعًا لكلمة المرور هي استخدام 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 الضعيفة.

استخدام مدير كلمات مرور للمساعدة

إذن أنت تعلم أنه من المهم أن يستخدم كل فرد في البرلمان كلمة مرور طويلة وعشوائية ومختلفة لكل حساب من حساباتهم الشخصية والبرلمانية، ولكن كيف تفعل ذلك بالفعل؟ يُعد حفظ كلمة مرور جيدة لعشرات (إن لم يكن المئات) من الحسابات أمرًا مستحيلاً، لذلك يتعين على الجميع الاحتيال. وإن الطريقة الخاطئة للقيام بذلك هي إعادة استخدام كلمات المرور. ولحسن الحظ، يمكننا اللجوء إلى مديري كلمات المرور الرقمية لجعل حياتنا أسهل بكثير (وممارسات كلمة المرور الخاصة بنا أكثر أمانًا) بدلاً من ذلك. 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 مدير 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 لاستخدام كلمات مرور جيدة وفريدة عبر جميع حساباتك. ستستخدم كلمة المرور الأساسية هذه (وبشكل مثالي المصادقة ثنائية العامل (2FA)، التي سنتم مناقشتها في القسم التالي) لفتح مدير كلمات المرور وإلغاء تأمين الوصول إلى كل كلمات المرور الأخرى. ويمكن أيضًا مشاركة مديري كلمة المرور عبر حسابات متعددة لتسهيل المشاركة الآمنة لكلمة المرور في جميع أنحاء البرلمان.

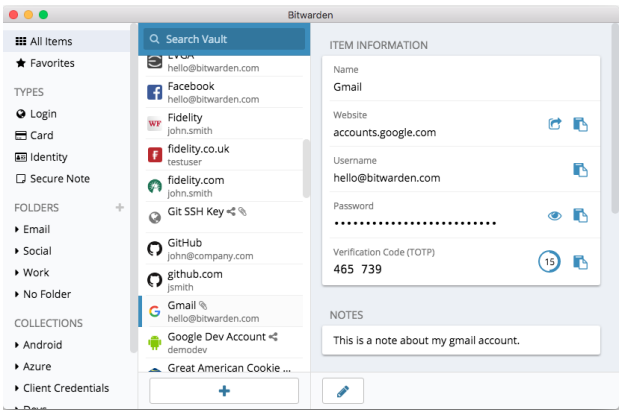
لماذا نحتاج إلى استخدام شيء جديد؟ ألا نستطيع تدوينها على الورق أو في جدول بيانات على الكمبيوتر فقط؟

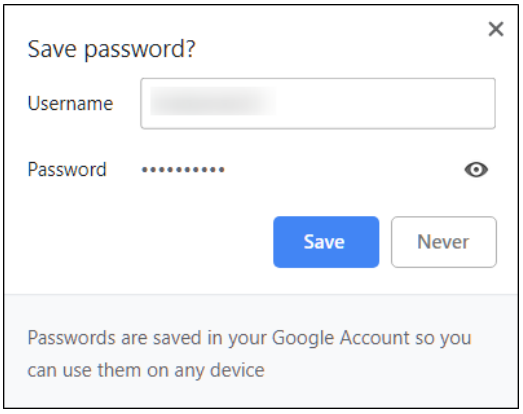
لسوء الحظ، يوجد العديد من الأساليب الشائعة لإدارة كلمات المرور غير الآمنة. ويمكن أن يؤدي الاحتفاظ بكلمات المرور على الورق (ما لم يتم الاحتفاظ بالورق في مكان مغلق في خزنة ما) إلى تعرضها للسرقة وللمتطفلين وفقدانها وتلفها بسهولة. يؤدي حفظ كلمات المرور في مستند على الكمبيوتر إلى تسهيل وصول المخترق إليه بشكل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

لماذا يجب أن نثق في مدير كلمات مرور؟

يلجأ مديرو كلمات مرور الجودة إلى 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، أفضل من أن يتم تعطيل أنظمة الأمان الخاصة بمدير كلمات المرور الجيد. ومن المهم أن تكون شكاكًا، ويجب عليك عدم الوثوق في جميع البرامج والتطبيقات ثقة عمياء، ولكن يتمتع مديرو كلمات المرور ذوي السمعة الجيدة بجميع الميزات المناسبة لفعل الشيء الصحيح.

وبدلاً من استخدام المستعرض الخاص بك (مثل Chrome، الذي يظهر على اليسار) لحفظ كلمات المرور، استخدم مدير كلمات مرور مخصص (مثل Bitwarden، الذي يظهر على اليمين). يتمتع مديرو كلمات المرور بميزات تجعل الحياة أكثر أمانًا وملائمة بالنسبة لبرلمانك.





ماذا عن تخزين كلمات المرور في المستعرض؟

يختلف حفظ كلمات المرور في المستعرض الخاص بك عن استخدام مدير كلمات مرور آمن. وباختصار، يجب ألا تستخدم Chrome أو Firefox أو Safari أو أي متصفح آخر كمدير كلمات مرور. 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 تترك شيئًا مطلوبًا من منظور الأمان. كذلك، هذه العيوب تسلب منك الكثير من الراحة التي يجلبها لك مدير كلمات المرور الجيد. ويؤدي فقدان هذه الراحة إلى زيادة احتمالية استمرار الأشخاص في جميع أنحاء البرلمان في القيام بممارسات إنشاء كلمة مرور ضعيفة ومشاركتها في.

على سبيل المثال، على عكس مديري 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. تُعد هذه الميزات جزءًا كبيرًا مما يجعل مدير كلمات مرور مخصص أمرًا مفيدًا جدًا وذا منفعة لأمان برلمانك. كذلك، يتضمن مديرو كلمات المرور ميزات خاصة بالمنظمة (مثل مشاركة كلمة المرور) لا توفر قيمة أمان فردية فحسب، بل قيمة لبرلمانك ككل. إذا كنت تحفظ كلمات المرور في المستعرض الخاص بك (عن قصد أو عن غير قصد)، فخذ من وقتك لحظة لإزالتها.

ما مدير 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 استخدامها 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 مدير كلمات المرور قدر الإمكان.

ومن الضروري **ممارسة الأمان الجيد عند استخدام مدير كلمات المرور أيضًا.** على سبيل المثال، إذا قمت باستخدام ملحق مستعرض مدير كلمات المرور أو قمت بتسجيل الدخول إلى Bitwarden (أو أي مدير كلمات مرور آخر) على جهاز ما، فتذكر تسجيل الخروج بعد الاستخدام 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 الفرق أو البرلمان ككل، فتأكد أيضًا من إلغاء الوصول إلى كلمات المرور (وتغيير كلمات المرور نفسها) عندما يترك الأشخاص العمل في المنظمة. لا تريد أن يحتفظ الموظف السابق بالوصول إلى كلمة مرور Facebook الخاصة بالبرلمان، 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 المرور الأساسية للذاكرة عند إعداد مدير كلمات المرور الخاصة بك. للمساعدة في هذا، ضع في اعتبارك إعداد تذكير يومي لاستدعاء كلمة مرور أساسية عند إنشاء حساب مدير كلمات مرور لأول مرة.

استخدام مدير كلمات المرور لبرلمانك

يمكنك تقوية ممارسات كلمات المرور لبرلمانك وتأكد من أن جميع الموظفين الأفراد لديهم حق الوصول (ويستخدمون) مدير 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 "منظمة الفريق" الخاصة بـ Bitwarden 3 دولارات أمريكية لكل مستخدم شهريًا. باستخدام الخطة (أو خطط فرق أخرى من مديري كلمات المرور مثل 1Password)، يكون لديك القدرة على إدارة جميع كلمات المرور المشتركة عبر المنظمة. لا توفر ميزات البرلمان أو مدير كلمات المرور على مستوى الفريق أمانًا أكبر فحسب، بل توفر أيضًا راحة للموظفين. ويمكنك مشاركة بيانات الاعتماد بأمان داخل مدير 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 لبرلمانك 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 مدير كلمات مرور على مستوى البرلمان، فتأكد من أن شخصًا ما مسؤول بشكل خاص عن إزالة حسابات الموظفين وتغيير أية كلمات مرور مشتركة عندما يترك موظف ما الفريق.

ما المصادقة ثنائية العامل؟

بغض النظر عن مدى جودة كلمة المرور الخاصة بك، فمن الشائع جدًا أن يتغلب المخترقون على كلمات المرور. ويتطلب الحفاظ على أمان الحسابات الخاصة بك من بعض جهات التهديد الشائعة حاليًا طبقة أخرى من الحماية. وهذا هو مكان استخدام 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 في التنفيذ عبر البرلمان.

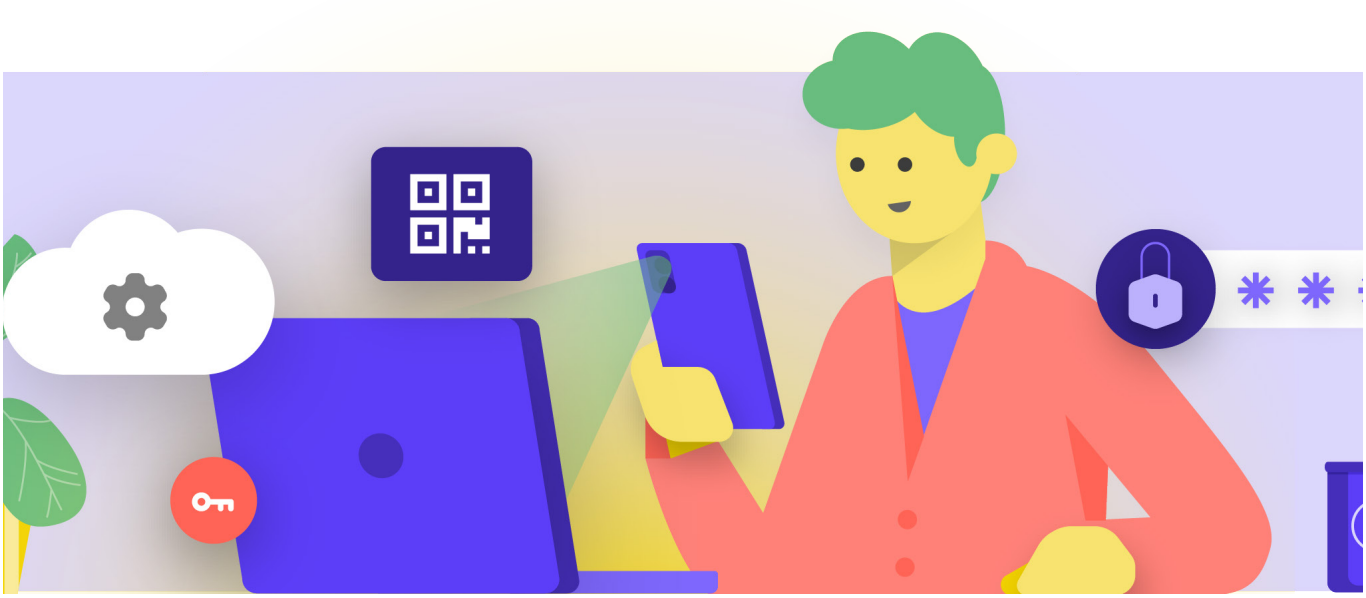
باختصار، تعمل المصادقة ثنائية العامل على تعزيز أمان الحساب عن طريق طلب معلومة ثانية – شيء ما أكثر من مجرد كلمة مرور – للوصول. عادةً ما تكون المعلومة الثانية شيئًا تمتلكه، مثل رمز من تطبيق موجود على هاتفك أو رمز مميز أو مفتاح فعلي.
تكون هذه المعلومة الثانية بمثابة طبقة دفاع ثانية. إذا سرق مخترق ما كلمة 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 البرلمان 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 هي الخيار الأمثل، ويرجع ذلك جزئيًا إلى أنها تكاد تكون مقاومة للتصيد الاحتيالي بالكامل. وتُعد هذه "المفاتيح" عبارة عن رموز مميزة للأجهزة (مثل محركات أقراص USB صغيرة) يمكن ربطها بسلسلة مفاتيح (أو البقاء في جهاز الكمبيوتر الخاص بك) لسهولة الوصول إليها وحفظها. عندما يحين وقت استخدام 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 مفاتيح الشراء. ضع في اعتبارك أنه يمكن استخدام مفتاح الأمان نفسه لأي عدد تريده من الحسابات.



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 و Authy و Duo Mobile. يُعد تطبيقات المُصدق رائعة أيضًا لأنها تعمل عندما لا يكون لديك وصول إلى شبكتك الخلوية وتكون مجانية لاستخدام الأفراد. ومع ذلك، تكون تطبيقات المُصادق أكثر عُرضة للتصيد 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 باستخدام 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، تترك الرسائل القصيرة الكثير مما هو مرغوب فيه كطريقة لطلب رموز المصادقة ثنائية العامل. فإنه أفضل من استخدام كلمة مرور فقط، ولكن يُوصى باستخدام تطبيقات المصادقة أو مفتاح الأمان الفعلي عندما يكون ذلك ممكنًا على الإطلاق. يمكن لخصم محدد الوصول إلى رموز المصادقة ثنائية العامل للرسائل 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 و Office 365 و Facebook و Twitter وما إلى ذلك) ولمعرفة الخدمات التي تسمح بأنواع المصادقة ثنائية العامل.

2FA والبرلمانات

وفقًا لتقارير عام 2020، اخترق المخترقون نظام البريد الإلكتروني البرلماني النرويجي، مما أدى إلى اختراق حسابات البريد الإلكتروني الخاصة بالعديد من المسؤولين البرلمانيين وحتى تنزيل بعض المعلومات من الأنظمة البرلمانية. في حين لم يتم الكشف عن التفاصيل الكاملة للاختراق للجمهور، فقد عزت النرويج التدخل إلى APT28، وهي مجموعة قرصنة تابعة لأجهزة الأمن الروسية. في حين أن APT28 متطور للغاية، إلا أن المخترقين الآخرين غالبًا ما يستخدمون تكتيكات أقل تعقيدًا مثل "هجمات القوة الغاشمة" (حيث يستخدم المهاجم أدوات لتجربة العديد من كلمات المرور على أمل تخمين الكلمة الصحيحة في النهاية) للوصول إلى الحساب. يسمح هذا التكتيك للمخترقين بتخمين حتى كلمات المرور القوية - مثل ما كان يُعتقد أنه هو الحال في النرويج. الأخبار الجيدة؟ من غير المرجح أن تنجح أنواع الهجمات مع اعتماد مصادقة ثنائية تعتمد على تطبيق مصادقة أو مفتاح!

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 تصيد احتيالي ناجحة**. توضح هذه الحالة مدى فاعلية مفاتيح الأمان حتى بالنسبة للمنظمات الأكثر عُرضة للخطر.

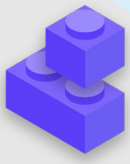
ماذا يحدث إذا فقد شخص ما جهاز المصادقة ثنائية العامل؟

في حالة استخدام 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 فقده أو سرقته. وبدلاً من ذلك، يجب عليك إنشاء رموز احتياطية للحسابات التي تسمح بذلك. ويجب عليك الاحتفاظ بهذه الرموز في مكان آمن جدًا، مثل مدير 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. وتحدث حادثة المصادقة ثنائية العامل الأكثر شيوعًا عندما يستبدل الأشخاص هواتفهم التي يستخدمونها لتطبيقات المصادقة أو يفقدونها. وإذا كنت تستخدم Google Authenticator، فلن يحالفك الحظ إذا تمت 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 تمكينها. 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 الجميع على دراية بهذه الخطوات عندما يبدأون في تمكين المصادقة الثنائية (2FA) عبر جميع حساباتهم.

فرض المصادقة ثنائية العامل عبر برلمانكم

إذا كانت برلمانك يوفر حسابات بريد إلكتروني لكل الموظفين من خلال Google Workspace (المعروف سابقًا باسم GSuite) أو Microsoft 365 باستخدام المجال الخاص بك (على سبيل المثال، @ndi.org)، فبإمكانك 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 لأعضائك وموظفيك 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 نظام

كذلك، ضع في اعتبارك تسجيل حسابات برلمانك 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 البرلمانية؛ وشجع الموظفين والمتطوعين على القيام بالشيء نفسه فيما يتعلق بحساباتهم الشخصية.**
- **قم بتطبيق مدير كلمات مرور موثوق به للبرلمان (وشجع استخدامه في الحياة الشخصية للموظفين أيضًا).**
  - اطلب كلمة مرور أساسية قوية ومصادقة ثنائية العامل لجميع حسابات مدير كلمات المرور.
  - ذكّر الجميع بتسجيل الخروج من مدير كلمات المرور على الأجهزة المشتركة أو عند وجود خطر متزايد بسرقة الجهاز أو مصادرته.
- **قم بتغيير كلمات المرور المشتركة عندما يغادر الموظفون والأعضاء البرلمان.**
- **لا تشارك كلمات المرور إلا بطريقة آمنة، على سبيل المثال من خلال مدير كلمات المرور في البرلمان أو التطبيقات المشفرة من طرف إلى طرف.**
- **اطلب المصادقة ثنائية العامل لجميع حسابات البرلمان، 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 في ميزانيتك، فقم بالتشجيع على استخدام تطبيقات المصادق 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 استخدام 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 الثابتة الخارجية وما إلى ذلك – محمية بشكل جيد.

تبدأ هذه الحماية بالحذر فيما يتعلق بنوع الأجهزة التي تقوم منظمتك وموظفيك بشرائها واستخدامها. يجب أن يكون لدى أي بائع أو جهة مُصنعة 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 تجنب امتلاك واحدًا منها. على الرغم من أن تكلفة الأجهزة الرخيصة يمكن أن تكون جذابة للغاية، إلا أن المخاطر الأمنية المحتملة للبرلمانات يجب أن توجهك نحو خيارات الأجهزة والمعدات الأخرى.

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 والبرلمانات

تم تطوير أكثر البرامج الضارة تقدمًا في العالم ونشرها في جميع أنحائه لاستهداف أعضاء البرلمان والمسؤولين الحكوميين الآخرين وموظفيهم. في الهند، على سبيل المثال، كشف اتحاد من الصحفيين أن العديد من أعضاء البرلمان ووزراء الحكومة قد تم استهدافهم بواسطة برنامج التجسس Pegasus، وهو نوع من البرامج الضارة التي احتلت العناوين الرئيسية في عام 2020. تشتهر Pegasus بقدرتها على إصابة الأجهزة المحمولة وإعطاء الجاني القدرة على تسجيل الصوت واعتراض ضغطات المفاتيح والرسائل، وفي الواقع وضع الضحية تحت المراقبة الكاملة. دون الحاجة إلى تفاعل الضحية. ومع ذلك، تنجح الغالبية العظمى من برامج التجسس في تعريض ضحاياها للخطر.

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 أمرًا 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. ذكّر الموظفين بأن يتعاملوا مع الأجهزة بالطريقة نفسها التي يتعاملون بها مع مبلغ كبير من المال - ولا يتركوها دون رقابة أو حماية.

ماذا يحدث إذا تمت سرقة جهاز؟

للحد من الضرر، في حال تمكن شخص ما من سرقة جهاز – أو حتى إذا تمكن من الوصول إليه لفترة زمنية قصيرة فقط – فتأكد من **فرض استخدام 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 استخدام "أنماط التمرير" لإلغاء تأمين الشاشة. للحصول على نصائح إضافية حول أقفال الشاشة، تحقق من Data Detox Kit الخاصة بمنظمة Tactical Tech. استخدام كلمات مرور جيدة يصعّب مهمة الخصم للوصول إلى المعلومات المخزنة على جهازك بشكل سريع في حالة السرقة أو الاستحواذ لمدة وجيزة. تأكد من أن أي أجهزة صادرة عن البرلمان مسجلة أيضًا في **جهاز محمول أو نظام إدارة نقطة النهاية.** على الرغم من أنها ليست غير مكلفة، إلا أن هذه الأنظمة تسمح للبرلمان الخاص بك بفرض سياسات الأمان عبر جميع الأجهزة وتحديد موقع واحد، ومسح محتوياته الحساسة المحتملة، في حالة سرقته أو فقده أو مصادرته. على الرغم من وجود العديد من الحلول المختلفة لإدارة الأجهزة المحمولة، إلا أن هناك عددًا قليلاً من الخيارات الموثوقة التي تعمل عبر الأنظمة الأساسية (أجهزة iPhone و Android و Mac و Windows) تشمل Hexnode و Meraki Systems Manager من Cisco و IBMs MDM وميزة إدارة الأجهزة المحمولة المدمجة في Google Workspace . إذا كانت التكلفة عاملاً مقيدًا، فعلى الأقل شجع الأعضاء والموظفين على استخدام ميزات "العثور على جهازي" المضمنة على هواتفهم الذكية الشخصية والصادرة عن البرلمان، مثل Find My iPhone الخاص بـ iPhone و Find My Device على Android.

ماذا عن تشفير الجهاز؟

من المهم استخدام التشفير وتعمية البيانات بحيث تكون غير قابلة للقراءة والاستخدام على جميع الأجهزة، خاصة أجهزة الكمبيوتر والأجهزة الذكية. ويجب عليك إعداد جميع الأجهزة عبر منظمتك بشيء ما يُسمى **تشفير القرص بالكامل** إن أمكن. وتشفير القرص بالكامل يعني أن الجهاز مُشفر لذلك لا يكون الخصم، في حالة سرقته فعليًا، قادرًا على استخراج محتويات الجهاز دون معرفة كلمة المرور أو المفتاح الذي استخدمته لتشفيره. تتيح 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 macOS 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 أمانًا قويًا. 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 ببرلمانك.

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 وتجنبها

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 استخدامها لتبادل البيانات وسرقتها. وبالرغم من أن بعض البرامج الضارة تتطلب هدفًا غير مشكوك به 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 استخدام 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 وتعطل العمليات البرلمانية، وتنتهك الخصوصية، وتعرض المستخدمين للخطر. باختصار، البرامج الضارة خطيرة بحق. ومع ذلك، هناك بعض الخطوات البسيطة التي يمكن أن يتخذها برلمانك لحماية نفسه 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 استخدام 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 و Linux على برامج مكافحة البرامج الضارة المضمنة، والأمر نفسه يحدث مع أجهزة Android و iPhone. 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). لسوء 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 برلمانك، 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 إلى 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 محدثًا، قلت 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 المطور، 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 تمت قرصنة العديد منها في البداية. كان من الممكن تجنب الكثير من الضرر -البشري والمالي - الممارسات الفضلى والتحديث التلقائي واستخدام أنظمة التشغيل المرخصة.

احذر من أجهزة USB

كن حذرًا عند فتح الملفات التي يتم إرسالها إليك كمرفقات 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 البرلمان، 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 الاستخدام.

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"

البرامج الضارة في العالم الحقيقي: تطبيقات الهاتف الضارة

يستخدم المخترقون 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 مجرد من أحد الأسباب العديدة التي تدفعك يجب أن تكون حذرًا في ما يتعلق بالتطبيقات التي تقوم بتنزيلها على أجهزتك.

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. يمكن أن يساعد أيضًا إلغاء تثبيت التطبيقات التي لم تعد تستخدمها في حماية هاتفك الذكي أو جهازك اللوحي. أحيانًا يبيع المطورون ملكية تطبيقاتهم لأشخاص آخرين. قد يحاول هؤلاء المالكين الجدد كسب المال عن طريق إضافة تعليمات برمجية ضارة.

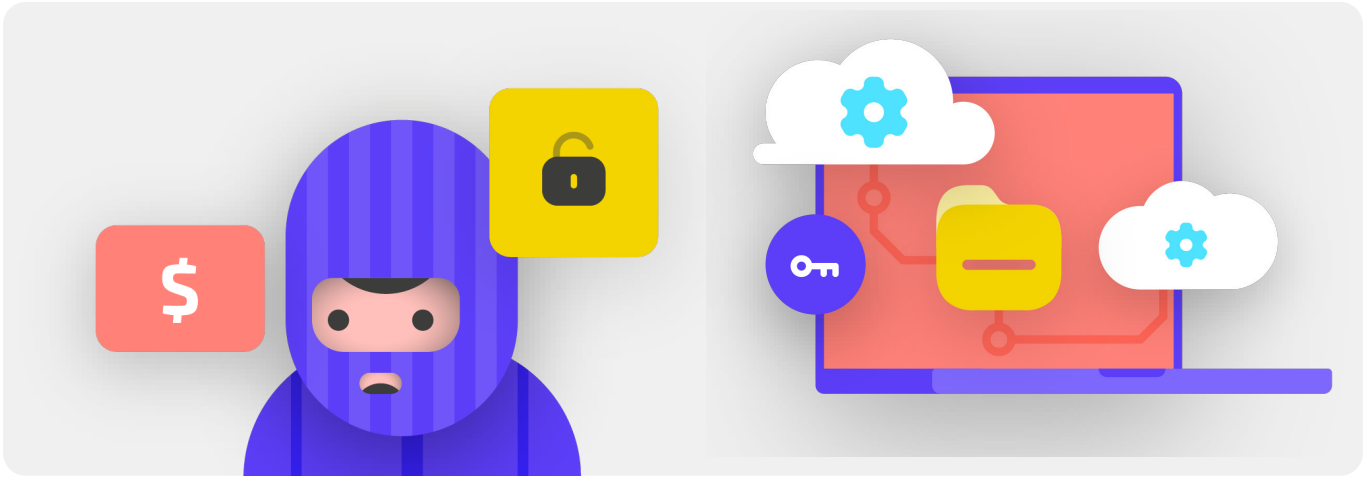
الحفاظ على أمان الأجهزة

- **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.
- **سجل جميع الأجهزة البرلمانية في جهاز محمول أو نظام إدارة نقطة النهاية.**
- **تأكد من أن جميع الأجهزة تستخدم برامج مرخصة.**
- **اطلب حماية كلمة المرور لكافة الأجهزة داخل البرلمان، بما في ذلك الأجهزة المحمولة الشخصية التي يتم استخدامها في الاتصالات المتعلقة بالبرلمان.**
- **قم بتمكين تشفير القرص بالكامل على الأجهزة.**
- **بشكل متكرر، ذكّر الأعضاء و الموظفين بالحفاظ على أمان أجهزتهم فعليًا - وتعامل مع أمان مكتبك باستخدام أقفال وطرق مناسبة لتأمين أجهزة الكمبيوتر.**
- **لا تشارك ملفات باستخدام 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 بما في ذلك البرلمانات، 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 استخدامها 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 البرلمان 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 الجميع داخل البرلمان وحوله ودمجها في خطتك الأمنية:

أحيانًا، يكذب حقل "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 خطأ إملائيًا بسيطًا 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.

التصيد والبرلمانات


Thu 4/8/2021 8:48 AM

@aop.gov.af>

Kindlty mention this email Most Urgent.

To @nsc.gov.af

Message NSC Press conference.rar (38 KB)

Yesterday I called your office and no one answered it. We have received your file and modified it. There is an error in the third line of the second page. Please confirm whether the error exists.
File Pass: nsc2021
Press conference by 5:00PM.

Regards |

Press office | Spokesman
Presidential Palace (ARG) | Islamic Republic of Afghanistan
Mobile: | | | ocs.gov.af
Mail: | |

تستهدف هجمات التصيد المتطورة والمخصصة البرلمانات والجهات الحكومية الأخرى في جميع أنحاء العالم بانتظام.

تم استهداف المسؤولين البرلمانيين الفيدراليين والمحليين في ألمانيا من خلال رسائل البريد الإلكتروني التصيدية في الفترة التي سبقت الانتخابات في خريف عام 2021. قبل بضعة أشهر فقط في أفغانستان، استخدمت مجموعة قرصنة تقنيات التصيد للتسلل بنجاح إلى مجلس الأمن القومي السابق من خلال انتحال هوية المتحدث الصحفي للرئيس الأفغاني السابق أشرف غني. أرسل المخترقون رسائل بريد إلكتروني تصيدية (كما هو موضح أعلاه) تطلب من الضحايا فتح ملف مرفق ادعى "المتحدث" أنه يحتوي على خطأ. عندما قام الضحايا بتنزيل الملف وفتحه "لتأكيد الخطأ"، قام المرفق الضار بنشر البرامج الضارة التي منحت المخترقين وصولاً مستدامًا إلى أجهزة الكمبيوتر. مكّن هذا الوصول المخترقين من تحميل الملفات وتنزيلها، وتشغيل الأوامر على الأجهزة حسب الرغبة، وسرقة البيانات الحكومية شديدة الحساسية.

الحذر من الملفات المرفقة

الحذر من الملفات المرفقة يمكن أن تحمل المرفقات برامج ضارة وفيروسات وعادة ما تصاحب رسائل البريد الإلكتروني لتي تسعى للتصيّد الاحتيالي. **إن أفضل طريقة لتجنب البرامج الضارة من الملفات المرفقة هي عدم تنزيلها على الإطلاق.** كقاعدة عامة، لا تفتح أية 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 تشجع على إرسال 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 استخدامه على الإطلاق.

الدفاع عن برلمانك ضد التصيّد الاحتيالي

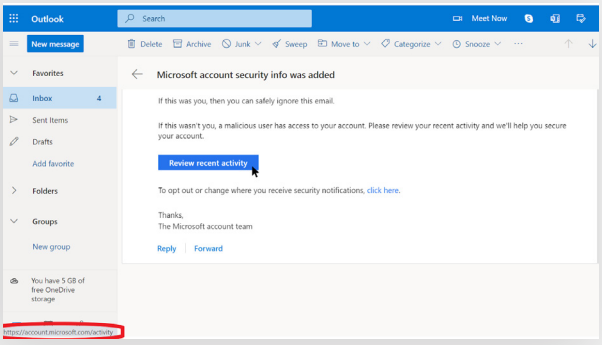
إذا كان برلمانك يستخدم Microsoft 365 للبريد الإلكتروني والتطبيقات الأخرى، فإنه يجب على مسؤول المجال تكوين**سياسة الملفات المرفقة الآمنة** للحماية من الملفات المرفقة الخطيرة. إذا كنت تستخدم إصدار enterprise من Google Workspace (المعروف سابقًا باسم GSuite)، فيوجد خيارًا فعالاً مشابه يجب على المسؤول لديك 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 10، **Windows Sandbox**. وهناك خيار آخر متقدم يجب وضع تنفيذه عبر برلمانك في الاعتبار ألا وهو خدمة تصفية لنظام أسماء المجالات (DNS) الآمنة.

يمكن للبرلمانات استخدام هذه التكنولوجيا لحظر الموظفين من الوصول إلى المحتوى الضار أو التفاعل معه عن طريق الخطأ، مما يوفر طبقة حماية إضافية ضد التصيّد الاحتيالي. توفر الخدمات الجديدة مثل **Cloudflare's Gateway** مثل هذه الإمكانات للمؤسسات دون الحاجة إلى مبالغ كبيرة من المال. 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 استخدام 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 رابطًا 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 شرعيًا 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.



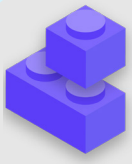
وأخيرًا، إذا قمت بالنقر فوق أي رابط من رسالة وتمت مطالبتك بتسجيل الدخول إلى شيء ما، فلا تقم بذلك إلا إذا كنت متأكدًا بنسبة 100% أن البريد الإلكتروني شرعيًا ويقوم بإرسالك إلى الموقع المناسب. ستقدم العديد من هجمات التصيّد الاحتيالي روابط تقوم بإرسالك إلى صفحات تسجيل دخول زائفة إلى Gmail أو Facebook أو 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 تلقى أي شخص داخل البرلمان مرفقًا أو رابطًا أو صورة أو رسالة أو مكالمة مشبوهة غير مرغوب فيها، فمن المهم أن يقوم بإبلاغ مسؤول أو فريق أمن تكنولوجيا المعلومات بذلك على الفور. إذا لم يكن لديك شخص مسؤول مثل هذا، فإنه يجب عليك التفكير في تعيينه على اعتباره جزءًا من تطوير الخطة الأمنية. يمكن للموظفين والأعضاء أيضًا الإبلاغ عن البريد الإلكتروني كرسائل غير مرغوب فيها أو تصيد احتيالي مباشرةً في Gmail أو Outlook.

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 الممارسات الفضلى في مواجهة التصيّد الاحتيالي - عدم النقر فوق روابط مشبوهة وتجنب المرفقات 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 أعلاه مع الجميع، يمكنك أيضًا التدرب على التعرف على التصيد الاحتيالي باستخدام Google Phishing Quiz. كذلك، نُوصي بشدة بإعداد تدريب منتظم عن التصيّد الاحتيالي للموظفين لاختبار مستوى الوعي والحفاظ على مستوى اليقظة لدى الأشخاص. يمكن إضفاء الطابع الرسمي على هذا التدريب كجزء من اجتماعات الفريق والبرلمان المنتظمة، أو عقدها بشكل غير رسمي. المهم هو أن يشعر كل من يشارك في العمليات البرلمانية بالراحة في طرح أسئلة حول التصيد الاحتيالي، والإبلاغ عن التصيد (حتى لو شعروا أنهم ربما ارتكبوا خطأً مثل النقر فوق رابط ما)، وأن كل شخص مخول للمساعدة في الدفاع عن البرلمان 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 البرلمان.
  - خصص مكافأة عن الإبلاغ ولا تعاقب من يفشل.

توصيل البيانات ومشاركتها بأمان

الاتصالات ومشاركة البيانات

لاتخاذ أفضل القرارات لبرلمانك 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. بدون التشفير المناسب، يمكن رؤية الاتصالات البرلمانية الداخلية من قبل أي عدد من الخصوم. يمكن أن تكشف الاتصالات غير الآمنة معلومات ورسائل حساسة أو محرجة، وتكشف كلمات المرور أو غيرها من البيانات الخاصة، وربما تعرض أعضاءك أو موظفيك للخطر اعتمادًا على طبيعة اتصالاتك والمحتوى الذي تشاركه. كبرلمان، من المهم أيضًا التأكد من أن الاتصالات الحكومية الرسمية للأعضاء والموظفين تتوافق مع جميع الالتزامات الحكومية المفتوحة ذات الصلة (مثل طلبات الوصول للمعلومات) والتزامات أمن البيانات. لذلك، عند تصميم وتنفيذ أنظمة وسياسات اتصالات آمنة عبر البرلمان، تأكد من وضع هذه العوامل في الاعتبار حتى يتم تأمين الرسائل ذات الصلة بشكل صحيح والحفاظ عليها عند الضرورة بموجب القانون.

تأمين الاتصالات والبرلمانات

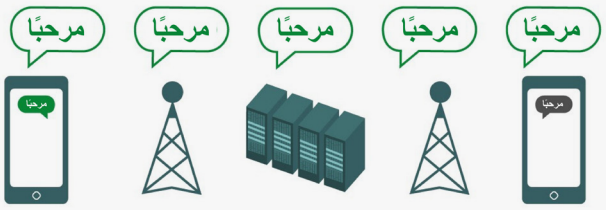
وقعت العديد من الحوادث في السنوات الأخيرة حيث تعرضت أنظمة الاتصالات للبرلمانات وحسابات النواب وموظفيهم للخطر، مما أدى إلى تعطيل العمليات البرلمانية وفي بعض الحالات سرقة الاتصالات الحساسة. في يوليو 2021، على سبيل المثال، أعلنت السلطات البولندية أنه تم اختراق حسابات البريد الالكتروني لما يقرب من عشرة أعضاء في البرلمان المحلي، بما في ذلك حساب شخصي لكبير مساعدي رئيس الوزراء وحسابات لأعضاء من كل تجمع معارضة برلماني تقريبًا. جاء هذا التقرير بعد أشهر قليلة من ظهور أخبار مماثلة حول هجوم إلكتروني على أنظمة المعلومات والاتصالات في البرلمان الفنلندي. ووصفت السلطات في فنلندا هذا الهجوم بأنه "تجسس مشدد واعتراض الرسائل" استهدف برلمانها.

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، تُترك رسائلنا مفتوحة للقراءة من قبل الخصوم المحتملين، بما في ذلك الحكومات الأجنبية غير الصديقة أو المخترقين على الويب. مثل هذا التشفير مهم ليس فقط للاتصالات البرلمانية الداخلية ولكن أيضًا للاتصالات الخارجية التي تحتاج فيها الخصوصية والنزاهة إلى الحماية.



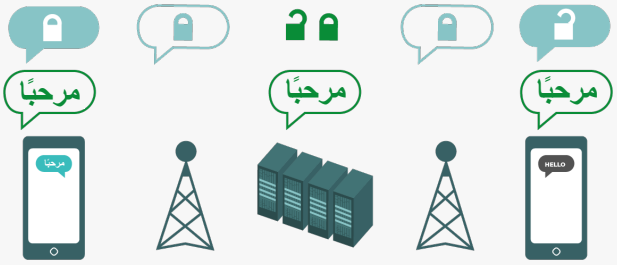
كما ترى في الصورة أعلاه، يرسل هاتف ذكي رسالة نصية غير مشفرة خضراء ("مرحبًا") إلى هاتف ذكي آخر في أقصى اليمين. على طول الطريق، ينقل برج الهاتف المحمول (أو في حالة إرسال شيء ما عبر الإنترنت، موفر خدمة الإنترنت، المعروف باسم ISP) الرسالة إلى خوادم الشركة. ومن هناك ينتقل عبر الشبكة إلى برج هاتف خلوي آخر 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 استخدام 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 برلمانك يتخذ خيارات لاعتماد ممارسات وأنظمة اتصالات أكثر أمانًا. يتم وصف هذه الاختلافات جيدًا بواسطة **دليل الدفاع الذاتي** ضد المراقبة، والذي تم تعديله مرة أخرى هنا:

تشفير طبقة النقل

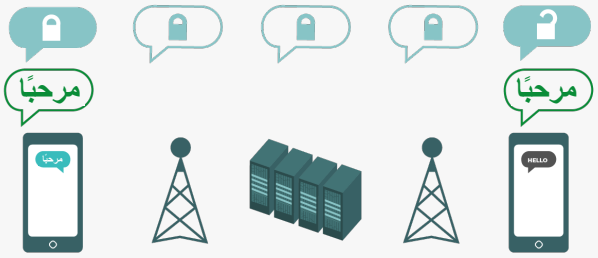
تشفير طبقة النقل، المعروف أيضًا باسم أمان طبقة النقل (TLS)، على حماية الرسائل أثناء انتقالها من جهازك إلى خوادم تطبيق/خدمة المراسلة ومن هناك إلى جهاز المستلم. وهذا يحميها من أعين المخترقين إلى شبكتك أو موفري خدمة الإنترنت أو الاتصالات. وعلى الرغم من ذلك، في المنتصف، يمكن لمزود خدمة المراسلة/البريد الإلكتروني 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 هذه الرسالة، ثم يتم تمريرها إلى برج الهاتف المحمول ثم إلى خوادم التطبيق / الخدمة، والتي لا يمكنها 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 يحتاج إليه برلمانك 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 تتمحور حول 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 في ما 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 استخدام الخدمات التي تدعم التشفير من طرف إلى طرف عندما يكون ذلك ممكنًا.

هناك مجموعة أخرى من الأسئلة التي يجب مراعاتها وهي ما إذا كنت ملزمًا بموجب القانون بالحفاظ على الوصول الوحيد إلى أي اتصالات برلمانية، وما إذا كانت هناك أي متطلبات لتوطين البيانات في بلدك، و/أو إذا كانت هناك حاجة إلى الحفاظ على اتصالات معينة (على سبيل المثال ليست بشكل دائم) حذفها من قبل الموظفين) من أجل الامتثال لقوانين والتزامات الحكومة المفتوحة. إذا كان الأمر كذلك، فقد تفكر في نظام اتصالات على مستوى المؤسسات يدعم التشفير من طرف إلى طرف حيث يمكنك، بصفتك برلمانًا، التحكم في مفاتيح التشفير بنفسك. يمكن أن تكون مثل هذه الأنظمة (التي ستتم مناقشتها بمزيد من التفصيل في قسم "تخزين البيانات بشكل آمن" من الدليل) قوية، ولكنها تتطلب مهارات تقنية متقدمة للتنفيذ.

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.

ماذا يجب ان نفعل بخصوص البريد الالكتروني؟

بشكل عام، لا يعد البريد الإلكتروني هو الخيار الأفضل عندما يتعلق الأمر بالأمان. حتى أفضل خيارات البريد الإلكتروني المشفرة من طرف إلى طرف عادةً ما تترك شيئًا مطلوبًا من منظور أمني، على سبيل المثال، عدم تشفير سطور موضوع رسائل البريد الإلكتروني وعدم حماية البيانات الوصفية (وهو مفهوم مهم سيتم وصفه أدناه). إذا كنت بحاجة إلى توصيل معلومات حساسة للغاية لا تحتاج إلى الاحتفاظ بها في السجل العام، فضع في اعتبارك أنه من الأفضل تجنب البريد الإلكتروني (كل من نظام البرلمان وخاصة الحساب الشخصي لشخص ما) لصالح خيارات المراسلة الآمنة (التي سيتم إبرازها في القسم التالي).

ومع ذلك، كبرلمان، قد لا تزال ترغب أو تحتاج إلى أن يقوم الأعضاء والموظفون بتوصيل محتوى حساس أو خاص من خلال نظام تتم إدارته مركزيًا كجزء من عملياتهم اليومية. يمكن أن يكون نظام البريد الإلكتروني على مستوى البرلمان، مع ضوابط الحساب المناسبة بالطبع، مفيدًا هنا. إذا كان تشفير طبقة النقل كافياً، وفقًا لتحليلك أعلاه، فإن عروض الأعمال القياسية من موفري البريد الإلكتروني مثل Google Workspace (Gmail) و Microsoft 365 (Outlook) يمكن أن تكون خيارات قوية للبرلمان الخاص بك. ومع ذلك، إذا كنت قلقًا من أن مزود البريد الإلكتروني الخاص بك قد يكون ملزمًا قانونًا بتقديم معلومات حول اتصالاتك إلى حكومة أجنبية أو خصم آخر، أو إذا كانت متطلبات الإقامة المحلية للبيانات مثيرة للقلق، فستحتاج إلى التفكير في استخدام طرف إلى طرف خيار البريد الإلكتروني المشفر. تتضمن بعض هذه الخيارات إضافة إدارة مفاتيح التشفير الخاصة بك إلى Google Workspace أو Microsoft 365 (كما هو موضح في قسم "تخزين البيانات بشكل آمن" من هذا الدليل)، أو اعتماد خدمات بريد إلكتروني مشفرة من طرف إلى طرف مصممة للمؤسسات الكبيرة مثل ProtonMail Business أو Tutanota Business

ما بيانات التعريف وهل يجب أن نقلق بشأنها؟

من الذي تتحدث إليه أنت وموظفوك وأعضاء وفرقك ومتى وأين تتحدث معهم يمكن أن يكون في الغالب حساسًا 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. يوفر دليل الدفاع عن النفس ضد الرقابة التابع لـ EFF نظرة عامة على البيانات الوصفية وسبب أهميتها (بما في ذلك توضيح لما تبدو عليه البيانات الوصفية):

غالبًا ما يتم وصف بيانات التعريف على أنها كل شيء باستثناء محتوى الاتصالات الخاص بك. ويمكنك التفكير في بيانات التعريف على أنها مغلفًا رقميًا. 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 تمت به المحادثة
- موقعك عند الاتصال

في حين أن شفافية العمليات البرلمانية المطبقة ضرورية، فإن تقييد الوصول غير المصرح به إلى البيانات الوصفية (بالإضافة إلى حماية محتوى الاتصالات) مهم أيضًا. في النهاية، يمكن أن تكشف البيانات الوصفية معلومات حساسة للمخترقين أو الحكومات الأجنبية أو الشركات أو الآخرين الذين قد لا ترغب أن تصل إليهم. فيما يلي بعض الأمثلة لما يمكن أن تكشفه البيانات الوصفية:

يمكنهم معرفة تواصل عضو برلماني مع صحفي وحديثه معه قبل ساعة من نشر هذا الصحفي لقصة مع اقتباسات من مصدر مجهول. وعلى الرغم من ذلك، فإنهم يجهلون ما تحدثتم بشأنه.

يمكنهم معرفة استلامك 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.

أدوات الاتصالات المشفرة من طرف إلى طرف الموصى 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** • **Tresorit**

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

إذا كنت بحاجة إلى استخدام التشفير من طرف إلى طرف، أو ترغب فقط في تبني أفضل الممارسات بغض النظر عن سياق تهديد البرلمان الخاص بك، فإليك بعض الأمثلة الموثوقة للخدمات التي تقدم، **اعتبارًا من عام 2022**، رسائل ومكالمات مشفرة من طرف إلى طرف . 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.

البيانات الوصفية غير محمية بالتشفير الذي توفره 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 ومتى حدث ذلك و(في حالة رسائل البريد الإلكتروني) سطور الموضوع العامة لاتصالات برلمانك.

وإن أحد أسباب التوصية باستخدام 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.

قد لا يكون هذا أمرًا بالغ الأهمية بالنسبة لغالبية الاتصالات البرلمانية، ولكن من المهم إدراك المخاطر التي تشكلها البيانات الوصفية واختيار أدوات وسياسات الاتصال المناسبة وفقًا لذلك.

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 استخدام 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 باستخدام 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 باستخدام TELEGRAM أو FACEBOOK MESSENGER أو VIBER لإجراء دردشات آمنة؟

تقدم بعض الخدمات، مثل Facebook Messenger و Telegram، تشفيرًا من طرف إلى طرف فقط إذا قمت بتشغيله عمدًا (وللمحادثات الفردية فقط)، لذا فهي ليست خيارات جيدة للرسائل الحساسة أو الخاصة، خاصة بالنسبة للفرق . لا تعتمد على هذه الأدوات إذا كنت بحاجة إلى استخدام التشفير من طرف إلى طرف، لأنه من السهل جدًا نسيان تغيير الإعدادات الافتراضية الأقل أمانًا. تدعي Viber أنها تقدم تشفيرًا من طرف إلى طرف، لكنها لم تجعل الكود الخاص بها متاحًا للمراجعة لباحثي الأمن الخارجيين. لم يتم أيضًا توفير رمز Telegram للمراجعة العامة. نتيجة لذلك، يخشى العديد من الخبراء من أن تشفير Viber (أو "المحادثات السرية" في Telegram) قد يكون دون المستوى المطلوب وبالتالي غير مناسب للاتصالات التي تتطلب تشفيرًا حقيقيًا من طرف إلى طرف.

يستخدم زملاؤنا البرلمانيون والناخبون تطبيقات وأنظمة مراسلة أخرى للاتصال - 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 قدوة حسنة لجهات الاتصال الخاصة بك - سواء كانت في وكالات حكومية أخرى أو مؤسسات أو عبر البرلمان أو ناخبين خارجيين. إذا كان عليك استخدام أنظمة أخرى أقل آمانًا، فكن واعيًا ومدركًا تمامًا لما تقوله. تجنب مناقشة الموضوعات الحساسة. قد يكون لبعض البرلمانات بروتوكولات مختلفة للدردشة العامة أو الاتصالات العامة مقارنة بالمناقشات السرية مع القيادة، على سبيل المثال. صنف اتصالاتك البرلمانية (الداخلية والخارجية) على أساس الحساسية وتأكد من أن الأعضاء والموظفين يستخدمون آليات الاتصال المناسبة وفقًا لذلك! بالطبع، من الأسهل أن يتم تشفير كل شيء تلقائيًا طوال الوقت - دونما الحاجة للتفكير بالأمر أو تذكر أي شيء.

لحُسن الحظ، أصبحت التطبيقات المشفرة من طرف إلى طرف مثل Signal شائعة بشكل متزايد وسهلة الاستخدام - ناهيك عن ترجمتها إلى عشرات اللغات للاستخدام 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 استخدامه مشكلة كبيرة.

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

في تطبيق Signal، من المهم أيضًا التحقق من رموز الأمان (التي يشار إليها باسم أرقام الأمان). لعرض رقم الأمان والتحقق منه في Signal، يمكنك فتح الدردشة مع جهة اتصال، والنقر على اسمه في الجزء العلوي من شاشتك، والتمرير لأسفل للنقر على "عرض رقم الأمان". إذا كان رقم الأمان الخاص بك يتطابق مع جهة الاتصال الخاصة بك، فيمكنك تمييزها على أنها "تم التحقق منها" من نفس الشاشة. من المهم بشكل خاص الانتباه إلى أرقام الأمان هذه والتحقق من جهات الاتصال الخاصة بك إذا تلقيت إشعارًا في محادثة تفيد بتغيير رقم الأمان الخاص بك مع جهة اتصال معينة. إذا احتجت أنت أو أي موظف آخر إلى مساعدة في تكوين هذه الإعدادات، فإن تطبيق Signal نفسه يوفر إرشادات مفيدة. إذا كنت تستخدم التطبيق Signal، الذي يعتبر أفضل خيار سهل الاستخدام 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 مزيد من النصائح حول كيفية تكوين تطبيق **Signal**، و **WhatsApp** بشكل صحيح، يمكنك التحقق من أدلة الأدوات لكليهما التي قام بتطويرهما مؤسسة EFF في دليل الدفاع الذاتي ضد المراقبة.

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 الكبيرة في مكتبك أو قاعات المدينة الافتراضية للنواب. ولسوء الحظ، لا توجد خيارات رائعة حاليًا تحدد مربعات الاختيار جميعها:سهلة الاستخدام وتدعم أعدادًا كبيرة من الحضور وميزات التعاون وتمكين التشفير من طرف إلى طرف بالوضع الافتراضي.

ستتم مناقشة الاحتياجات المحددة للجلسات العامة واجتماعات اللجان لاحقًا في هذا الدليل، ولكن بالنسبة لاجتماعاتك العامة الأخرى التي لا تتطلب ميزات تعاون مثل مشاركة الشاشة أو الغرف الفرعية، هناك خياران. بالنسبة للمجموعات التي تصل إلى ثمانية أشخاص، يوصى بشدة باستخدام Signal. يمكن الانضمام إلى مكالمات الفيديو

الجماعية على Signal إما من هاتف ذكي أو تطبيق Signal لسطح المكتب على جهاز الكمبيوتر. ومع ذلك، ضع في اعتبارك أنه يمكن إضافة جهات الاتصال الذين يستخدمون Signal بالفعل إلى مجموعة Signal فقط.

إذا كنت تبحث عن خيارات أخرى، فقد أضاف نظام **Jitsi Meet** 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 باستخدام 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. لاستخدام 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 استخدام Jitsi، تأكد من إنشاء أسماء غرف اجتماعات عشوائية واستخدام رموز مرور قوية لحماية المكالمات.

إذا كان هذا الخيار لا يعمل مع فرقك، فيمكنك التفكير في استخدام 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.
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.

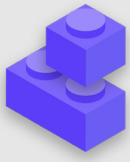
ملاحظة حول مشاركة الملفات

بالإضافة إلى مشاركة الرسائل بأمان، من المحتمل أن تكون مشاركة الملفات بأمان جزءًا مهمًا من خطة أمان برلمانك. 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 استخدام Google Drive أو SharePoint خيارًا جيدًا لبرلمانك. 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 باستخدام منافذ USB. يؤدي استخدام أجهزة مثل USB داخل البرلمان إلى زيادة احتمالية حدوث برامج ضارة أو سرقة بشكل كبير، كما يؤدي الاعتماد على البريد الإلكتروني أو غيره من أشكال المرفقات إلى إضعاف دفاعات البرلمان ضد هجمات التصيد الاحتيالي.

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 باستخدام 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 لبرلمانك. 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**



توصيل البيانات بشكل آمن

- **تصنيف الاتصالات على أساس حساسيتها.**
  - تحديد الأنظمة والأدوات المناسبة للاتصال.
  - ضع سياسة حول المدة التي ستحتفظ فيها بالرسائل، مع مراعاة الأمن والالتزامات تجاه الشفافية البرلمانية.
- **اطلب استخدام خدمات المراسلة المشفرة من طرف إلى طرف وموثوق بها للاتصالات الحساسة في برلمانك.**
  - خذ الوقت اللازم لتشرح للموظفين والشركاء الخارجيين سبب أهمية الاتصالات الآمنة؛ وسيعمل هذا على تعزيز نجاح خطتك.
- **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 المعنيين بتشغيل الإعدادات المناسبة في بداية أي اجتماع أو مكالمة.
- **لا تحاول استضافة خادم البريد الإلكتروني الخاص بك - استخدم خدمات البريد الإلكتروني المستندة إلى التخزين السحابي مثل Office 365 أو Google Workspace كبدائل.**
  - لا تسمح للموظفين باستخدام حسابات البريد الإلكتروني الشخصية للعمل.
- **ذكّر الموظفين والأعضاء بشكل متكرر بأفضل الممارسات الأمنية المتعلقة بمراسلة المجموعة والبيانات الوصفية.**
  - كن على علم بمن يتواجد في الرسائل الجماعية والدردشات وسلاسل البريد الإلكتروني.

البرلمانات الرقمية (البرلمان الإلكتروني)

كبرلمان، من المهم أن تولي اهتمامًا خاصًا لسياسات الاتصالات والأمن التشغيلي لوظائفك الأساسية، بما في ذلك تلك التي تحدث عبر الإنترنت وفي الفضاء الرقمي.

سواء كان برلمانك يدرس نظام "البرلمان الإلكتروني" الكامل الذي يمكنه رقمنة كل شيء بدءًا من صياغة مشاريع القوانين مرورًا بالمناقشة والتصويت الإلكتروني (مثل Nextsense أو Propylon أو Granicus على سبيل المثال لا الحصر)، أو أنك تستخدم أبسط وأقل - أدوات غير مكلفة لتسهيل العمليات البرلمانية الخاصة بك، فمن الضروري النظر في كيفية أخذ أي أداة (أو أدوات) وعملية (أو عمليات) في الاعتبار أمن وسلامة وتوافر المعلومات.

الأمان و البرلمانات الرقمية

كما يتضح من سلسلة من الحوادث في جنوب إفريقيا، فإن انتقال العمليات البرلمانية إلى العالم الرقمي يستلزم الانتباه إلى الأمن السيبراني ليس فقط لتجنب فقدان البيانات الحساسة أو سرقتها، ولكن أيضًا الإحراج المحتمل والإهانة والأذى للأعضاء والموظفين. في مايو 2020، ظهرت صور إباحية قبل دقائق قليلة من بدء الاجتماع الافتراضي للجمعية الوطنية في البلاد. بعد عرض الصور المسيئة، ألقى "الهاكر" أو "zoom bomber" إهانات عنصرية وجنسية على المتحدث باسم الجمعية التي كانت تستضيف الجلسة، مما أجبر المنظمين على تأجيل الاجتماع. ووقعت حادثة مماثلة قبل شهر عندما تعطل اجتماع ترأسه وزيرة المرأة والشباب والأشخاص ذوي الإعاقة بسبب صور إباحية.

الجلسات العامة عن بعد واجتماعات اللجان

ومن أهم هذه العمليات الجلسات العامة واجتماعات اللجان. هذه الجلسات والمحادثات والقرارات والتصويت التي تحدث داخلها هي في صميم الكثير من عمل برلمانكم، وبالتالي يمكن أن تكون هدفًا خاصًا للخصوم. وفي عالم حديث متأثر بالوباء، تُعقد مثل هذه الجلسات والاجتماعات بطريقة متنوعة بشكل متزايد اعتمادًا على سياق بلدك، سواء حضوريًا أو عبر الإنترنت تمامًا أو بطريقة "مختلطة".

كما هو موضح في **"استجابة البرلمانات الأخيرة لدليل الوباء" الذي أجرته** شراكة مجلس النواب للديمقراطية، يختلف هيكل النقاش البرلماني النموذجي عن مناقشة المؤتمر العادية أو الاجتماع التنظيمي القياسي. غالبًا ما تتطلب احتياجات التصويت عن بُعد، وتقديم المقترحات الرسمية والتعديلات، والمناقشة المنظمة، وحتى الترجمة الفورية لضمان إدراج جميع الدوائر الانتخابية، ميزات إضافية غير موجودة في معظم الحلول التقنية الأساسية أو التقليدية. نتيجة لذلك، عند استضافة جلسة افتراضية أو مختلطة، من المحتمل أن يحتاج برلمانك إلى تطوير (أو طور بالفعل) برامج مخصصة، أو شراء حلول مؤسساتية باهظة الثمن (مثل **Webex Legislate من Cisco**) المصممة خصيصًا لإدارة الجلسات البرلمانية عن بعد. أيا كان الخيار الذي يختاره البرلمان الخاص بك، فمن المهم التفكير، كما هو موضح في **دليل استجابة البرلمانات للجائحة**، في كيفية تمكن جميع الأعضاء والموظفين من الوصول إلى مثل هذا النظام. من الضروري أيضًا ضمان تأمين مثل هذا النظام بشكل صحيح.

عند بناء الحلول التقنية وتنفيذها للجلسات البرلمانية، من المهم التأكد من وجود أساسيات الأمن الأساسية. تتضمن هذه الخطوات لضمان تأمين البيانات "في حالة السكون" داخل النظام نفسه، وتشفيرها بشكل صحيح أثناء النقل، وأن المستخدمين المصرح لهم فقط هم القادرون على الوصول إلى النظام. هناك العديد من الأساليب التي يمكن اتباعها لضمان مثل هذا الأمن، بما في ذلك العديد من الأساسيات الموضحة في بقية هذا الدليل. التشفير من طرف إلى طرف على أي مشاركة بيانات وأنظمة اتصالات مستخدمة، وكلمة مرور قوية ومتطلبات مصادقة ثنائية و/أو تقييد عنوان IP للمستخدمين للوصول إلى هذه الأنظمة (ما لم يكن المقصود منها أن تكون مفتوحة للجمهور)، المتطلب من الشبكات الخاصة الافتراضية (التي ستتم مناقشتها لاحقًا في الدليل)، وتقييد الوصول إلى الأجهزة النظيفة والموثوقة فقط، كلها خطوات مفيدة.

التصويت عن بعد

ربما تكون الحاجة إلى أمان قوي أكثر أهمية عند التعامل مع التصويت عن بُعد. كما **يسلط الضوء على استجابة البرلمانات المذكورة أعلاه لدليل الوباء**، يتم انتخاب أعضاء البرلمان لغرض محدد هو التصويت نيابة عن ناخبيهم. إن القدرة على الوثوق بهذه الأصوات والتحقق منها أمر بالغ الأهمية ليس فقط لعمل البرلمان نفسه ولكن للنظام الديمقراطي ككل. يتم التحقق من هذه الأصوات بسهولة نسبيًا عندما يصوت عضو البرلمان شخصيًا، ولكن عند المشاركة افتراضيًا، تصبح المصادقة الفنية تحديًا أكبر يتطلب عناية وتركيزًا كبيرين. كما هو موضح في **شهادة** الخبراء المقدمة إلى اللجنة الدائمة للإجراءات وشؤون مجلس العموم الكندي، تختار البرلمانات عادةً أحد الخيارات الأربعة للتصويت عن بُعد:

- التصويت عبر البريد الإلكتروني: حيث يتلقى الأعضاء نموذج الاقتراع إلكترونيًا ويقدمون تصويتهم عبر البريد الإلكتروني. يعتبر هذا الخيار بشكل عام غير آمن، ويرجع ذلك جزئيًا إلى افتقاره للتشفير من طرف إلى طرف، ويجب تجنبه.
- التصويت عبر الإنترنت: حيث يقوم الأعضاء بالوصول والإدلاء بأصواتهم عبر موقع ويب إما على جهاز كمبيوتر أو هاتف محمول. يتطلب هذا النهج الاستثمار في البنية التحتية الآمنة، بما في ذلك الأجهزة المؤمنة مع ضوابط المصادقة القوية كما هو مذكور أعلاه.
- التصويت على أساس التطبيق: حيث يقوم الأعضاء بتنزيل تطبيق للوصول إلى الأصوات والإدلاء بأصواتهم. يشبه التصويت عبر الويب، ولكنه يستخدم تطبيقًا محددًا يمكن تنزيله على الهاتف أو الجهاز اللوحي بدلاً من الوصول إليه من خلال متصفح.
- التصويت بالفيديو: حيث يصوت الأعضاء على الشاشة برفع الأيدي أو التصويت الصوتي. بالنسبة للتصويت العلني، يمكن أن يكون هذا هو الأقل تعقيدًا من الناحية الفنية والأقل تعقيدًا من الناحية الفنية من حيث الإعداد والأمن. لا يزال يتطلب أنظمة تشفير ومصادقة قوية، ومع ذلك، يضمن عدم انتحال الهوية أو الانقطاع أثناء جلسات التصويت.

أيًا كان الخيار الذي يختاره البرلمان الخاص بك لتنفيذه للتصويت عن بُعد - إذا كان يستخدم التصويت عن بُعد- فمن المهم أيضًا معالجة أساسيات الأمن السيبراني خلال عملية التصويت أيضًا. تتضمن هذه الأساسيات التأكد من أن الأجهزة التي يستخدمها النواب للإدلاء بأصواتهم مؤمنة فعليًا وخالية من البرامج الضارة، وأن وصول الأعضاء إلى الإنترنت مؤمن كما ينبغي عند التصويت (وكذلك عند إجراء أعمال برلمانية أخرى)، وأن يكون اتصال الإنترنت لديهم ثابتًا بحيث يمكنهم التصويت عند دعوتهم. كما

هو موضح في دليل استجابة البرلمانات للجائحة، عند اعتماد التصويت عن بعد، هناك حاجة إلى اختبار مكثف للنظام قبل أن يبدأ العمل به، والحاجة إلى توفير الدعم والتدريب لأعضاء البرلمان لضمان استخدامهم للنظام بشكل فعال. من المهم أن تتذكر أن *التوفر* هو جزء من الأمان. هناك أيضًا حاجة على وجه الخصوص لضمان أن البرلمانيات والموظفات قادرات على استخدام الأنظمة عبر الإنترنت بأمان، بما في ذلك التصويت عن بعد، والوصول إلى التكنولوجيا للقيام بذلك. عندما تتصل النساء، ولا سيما النساء المنتخبات، بالإنترنت، فإنهن يواجهن مستويات أعلى من الترهيب والمضايقة، ويجب أخذ هذا العامل في الاعتبار عند تطوير واستخدام تكنولوجيا مثل التصويت عن بعد للتأكد من أن جميع أعضاء البرلمان قادرون على أداء وظائفهم بفعالية. علاوة على ذلك، من الأهمية بمكان ضمان الوصول الملائم متعدد اللغات عن بُعد في البلدان التي يتحدث فيها الأعضاء والموظفون لغات رسمية متعددة.

مزوّد نظام البرلمان الالكتروني وأمن البرامج

يجب أن يأتي أي برنامج تشتريه - سواء تم استخدامه للتصويت عن بُعد أو نطاق أوسع من الاحتياجات البرلمانية - **من مصدر آمن ومعتمد، وأن يتم تدقيقه من أجل الأمان من قبل فرق مستقلة، والحصول على الشهادات المناسبة.** من المهم أن تتذكر أن مطوري البرامج، أولئك الذين توظفهم لبناء تطبيق أو أداة، ليسوا دائمًا خبراء أمان أنفسهم. لذلك، يعد جلب خبراء الأمن لاختبار التطبيق بحثًا عن ثغرات أمنية محتملة عبر التدقيق أمرًا بالغ الأهمية لتقليل مخاطر اختراق النظام الأساسي أو الأداة أو التطبيق أو اختراقه. حتى أفضل مطوري البرامج يرتكبون أخطاء إن لم تقم مجموعة ثانية (أو ثالثة) من الخبراء بفحص عملهم!

التصويت عن بعد في العالم الحقيقي

نفذت العديد من البرلمانات أنظمة التصويت عن بعد، وبذلك اتخذت خطوات كبيرة لضمان أمن وسلامة أصوات الأعضاء. أحد العناصر في هذه العملية، من بين العناصر الأخرى المذكورة أعلاه، هو ضمان المصادقة الصحيحة. تتضمن بعض الأمثلة في مجلس العموم في المملكة المتحدة حيث يستخدم الأعضاء عملية تسجيل واحدة للدخول إلى حساباتهم البرلمانية قبل التصويت، الأمر الذي يتطلب استخدام كلمة مرور على جهاز معين مخصص. في إسبانيا، يتم تعيين رموز شخصية لأعضاء البرلمان يجب إدخالها عبر تطبيق هاتف ذكي قبل تسجيل التصويت عن بُعد. في تشيلي، أعضاء مجلس الشيوخ الذين يصوتون عن بعد عبر تطبيق التصويت عن بعد المصمم بعناية في المجلس يجب أن يكون مرئيًا على الشاشة للادلاء بصوت.

تخزين البيانات بشكل آمن

بالنسبة لمعظم البرلمانات، فإن أحد أهم القرارات التي يجب اتخاذها هو مكان تخزين بياناتهم.

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 باستخدام خدمات تخزين موثوقة عبر السحابة. وربما من الأمثلة الأكثر شيوعًا هو Microsoft 365 وGoogle Drive. بدون خطة تخزين سحابية شاملة، من المحتمل أن يتم تخزين بيانات البرلمان في مجموعة متنوعة من الأماكن - بما في ذلك أجهزة كمبيوتر الموظفين والنواب ومحركات الأقراص الصلبة الخارجية وحتى عدد قليل 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.

تخزين البيانات والبرلمانات

أدى ظهور تخزين البيانات السحابية قليل التكلفة (المجاني أحيانًا) إلى جعل الحياة أسهل (وأكثر أمانًا) للعديد من البرلمانات والمنظمات الأخرى. ولسوء الحظ، لا يزال الكثيرون يحاولون استضافة خوادمهم الخاصة باستخدام ميزانية محدودة لتكنولوجيا المعلومات ولتعيين 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. أدى الهجوم إلى اختراق الخوادم المحلية، بما في ذلك خادم البرلمان النرويجي، مما مكّن المخترقين من الوصول إلى حسابات البريد الإلكتروني البرلمانية، وتثبيت برامج ضارة إضافية على خوادم الضحية والأنظمة المتصلة، واستخراج البيانات الحساسة في النهاية.

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. يكشف نطاق وتأثير هذا الاختراق العالمي عن خطر اختيار البرلمانات والمنظمات الأخرى لخوادم البريد الإلكتروني ذاتية الاستضافة وأنواع أخرى من البيانات الحساسة، لا سيما بدون استثمار كبير في موظفي الأمن السيبراني المخصص.

فوائد خدمة التخزين السحابية

حتى إذا اتخذت جميع الخطوات الصحيحة لحماية أجهزة الكمبيوتر الخاصة بك من البرامج الضارة والسرقة المادية، فلا يزال بإمكان الخصم المصمم على اختراق جهاز الكمبيوتر أو الخادم البرلماني المحلي أن ينجح بذلك. لكن يصعب عليهم هزيمة الدفاعات الأمنية لشركة Google أو Microsoft. تمتلك شركات التخزين الجيدة على السحابة موارد أمان لا مثيل لها كما 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. لذا بدلاً من محاولة تحديد (والاحتفاظ) بعدد موظفي الأمن السيبراني المتفانين وذوي المهارات العالية المطلوبين لحماية الخوادم المحلية في برلمانك، ركز طاقتك على عدد قليل من المهام الأبسط. يتضمن ذلك تحديد خيار التخزين السحابي المناسب لاحتياجاتك المتعلقة بخصوصية البيانات وتوطينها، وتطبيق أمان الحساب جيدًا، وتدريب الموظفين على مشاركة المجلدات والمستندات (وعدم مشاركتها) بشكل صحيح (بوجه عام، ينبغي عليك إعداد المجلدات داخل محرك التخزين السحابي الخاص بك الذي يقيد الوصول فقط على الموظفين الذين يحتاجون إلى ملفات معينة)، وتدقيق نظامك بانتظام للتأكد من أن الموظفين والأعضاء لا "يبالغون في مشاركة" أي ملفات (مثل تشغيل الرابط العام لمشاركة الملفات الذي يجب أن يقتصر بدلاً من ذلك على عدد قليل من الناس). 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 تحتاج إلى تجزئة البيانات التي تخص النائب نفسها من المعلومات التي تنتجها للبرلمان نفسه؟ 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 الثابتة، فلن يجد شيئًا لسرقته إذا كان يتم الوصول إلى معظم المستندات من خلال مستعرض الويب.

هل يمكننا حقًا الوثوق بالتخزين السحابي؟

باختصار، لا يوجد شيء غير جدير بالثقة بطبيعته بشأن التخزين السحابي. كما ذكرنا سابقًا، يمتلك معظم مزودي التخزين السحابي فرقًا من أفضل مهندسي الأمان في العالم يعملون على حماية منتجاتهم كل يوم، ويقدمون دعمًا أمنيًا لعملائهم يتجاوز ما يمكن أن تقدمه معظم أقسام تكنولوجيا المعلومات الصغيرة بمفردها. ومع ذلك، ضع في اعتبارك أن خدمات التخزين السحابية التقليدية تتطلب عادةً منح حق الوصول إلى البيانات الحساسة لشركة خارجية تقدم الخدمة. **مع ذلك، سيكون لكل برلمان فردي اعتباراته السياسية ومتطلباته القانونية (مثل تفويضات توطين البيانات) التي يجب مراعاتها عند اختيار ما إذا كان بإمكانه الوثوق بمزود تخزين سحابي معين واستخدامه.**

أي مزود تخزين سحابي يجب أن تختار؟

إذا لم يكن البرلمان الخاص بك مضطرًا للنظر في أي متطلبات لتوطين البيانات، ولم يكن لديه مشكلة في السماح لشركة خارجية موثوق بها للوصول إلى البيانات، فإن أكثر خيارات التخزين السحابية شيوعًا هما Google Workspace (المعروف سابقًا باسم GSuite) و Microsoft 365. إذا كان البرلمان الخاص بك يستخدم Gmail بالفعل، فإن الاشتراك في Google Workspace وتخزين البيانات في Google Drive من خلال تطبيقات Google Docs و Sheets و Slides المدمجة لمعالجة الكلمات وجداول البيانات والعروض التقديمية أمر منطقي للغاية. وبالمثل، إذا كان برلمانك يعتمد على Excel و Word، فالخيار السهل هو الاشتراك في Microsoft 365، والذي يمنح الوصول إلى Outlook للبريد الإلكتروني والإصدارات المرخصة من Microsoft Word و Excel و PowerPoint و Teams.

ماذا لو احتجنا إلى التحكم في بياناتنا الخاصة أو الامتثال لقوانين توطين البيانات؟

بالنسبة للعديد من البرلمانات، قد لا يكون مثل هذا الخيار البسيط ممكنًا نظرًا لمتطلبات توطين البيانات أو التوقعات المحددة التي تتطلب سيطرة برلمانية حصرية على بياناتها الخاصة. الخبر السار هو أن موفري التخزين السحابي الأمن قد طوروا مؤخرًا خيارات تسمح لعملاء المؤسسات إما باختيار موقع بياناتهم (لاحظ أن هذا يقتصر في الغالب على العملاء الأوروبيين في الوقت الحالي)، أو للتحكم في مفاتيح التشفير الخاصة بهم. **من الناحية العملية، هذا يعني أن البرلمان الخاص بك لديه خيارات للتحكم في بياناته الخاصة مع الاستمرار في الاستفادة من البنية التحتية وأمن التخزين السحابي.**

إذا كان برلمانك يستخدم حاليًا أو مهتمًا بـ Google Workspace لتخزين البيانات السحابية ومشاركتها، فقد قدمت Google ميزة تمكن **التشفير من جانب العميل** لمؤسسات Enterprise Plus. أثناء وجودها حاليًا في مرحلة الاختبار ومتاحة فقط لأغلى خطط Google Workspace، توفر هذه الميزة خيارًا للاستفادة من مجموعة Google Drive الكاملة لوظائف تخزين البيانات ومشاركتها - وميزات الأمان المضمنة فيها - مع الحد من قدرة Google على الوصول إلى معلومات البرلمان الحساسة أو الخاصة. باستخدام التشفير من جانب العميل، يمكنك اختيار دمج خدمة إدارة مفاتيح إضافية، مثل Virtru، والسماح للمستخدمين بإدارة مفاتيح التشفير الخاصة بهم دون السماح بالوصول إلى Google نفسها. تتطلب مثل هذه الخدمة من الجميع توخي الحذر الشديد في حماية هذه المفاتيح لحماية الوصول بشكل صحيح إلى أي نظام إدارة مفتاح تختار دمجه في Google Workspace. يمكن لمسؤولي الحساب معرفة المزيد حول كيفية تمكين التشفير من جانب العميل على Google Workspace **صفحة الدعم.**

إذا كان برلمانك يستخدم حاليًا Microsoft 365 أو مهتمًا به لتخزين البيانات السحابية ومشاركتها، فإنه يوفر خيارًا أكثر تعقيدًا ولكنه راسخ لإدارة مفاتيح التشفير الخاصة بك والمعروفة باسم **Microsoft 365 Double Key Encryption**. يتطلب خيار الأمان هذا **Microsoft 365 E5**، ولكنه يسمح لك بالتحكم في أي بيانات برلمانية حساسة أو خاصة وتقييد الوصول حتى إلى Microsoft نفسها.

Tresorit هو خيار آخر أسهل في التنفيذ إذا كان برلمانك مهتمًا بالسماح لطرف ثالث بالوصول إلى معلوماتك الداخلية. يوفر Tresorit تشفيرًا شاملاً للتخزين السحابي ومشاركة الملفات، ويقدم مجموعة من ملفات **خيارات موقع البيانات.**

ماذا لو لم نتمكن من الوثوق بأي حل تخزين سحابي؟

إذا اخترت القيام بذلك بمفردك والاعتماد على الخوادم المحلية لتخزين بيانات البرلمان الخاص بك بدلاً من ذلك، فمن الأهمية بمكان أن تستثمر الكثير من الوقت والموارد في تعزيز الدفاعات الرقمية لأجهزة البرلمان الخاص بك، والتأكد من تكوين هذه الخوادم وتشفيرها بشكل صحيح، وظلوا آمنين جسديًا. كما هو مذكور أعلاه، يتطلب مثل هذا النهج تحديد عدد من موظفي الأمن السيبراني المتفانين وذوي المهارات العالية وتوظيفهم والاحتفاظ بهم للحفاظ على أمان البنية التحتية للخادم المحلي.

تعزيز أمان حسابات السحابة الخاصة بالبرلمان

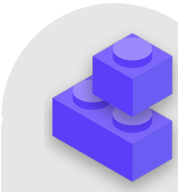
إذا اختار البرلمان الخاص بك إعداد مجال في Google Workspace أو Microsoft 365، فاحذر من أن الشركتين توفران مستويات أعلى من الأمان للحسابات المعرضة للخطر. يوفر **برنامج الحماية المتقدمة من Google** و **AccountGuard من Microsoft** أمانًا أكثر قوة للحسابات السحابية للمؤسسات المؤهلة، ويساعدك على تقليل احتمالية التصيد الفعال واختراق الحساب بشكل كبير. إذا كنت تعتقد أن برلمانك مؤهل وتهتم بتسجيل أعضائك وموظفيك في أي من الخطتين، فتفضل بزيارة مواقع الويب المرتبطة أعلاه أو اتصل بـ **cyberhandbook@ndi.org** للحصول على مزيد من المساعدة.

نسخ البيانات احتياطيًا

سواء كان البرلمان الخاص بك يخزن البيانات على الأجهزة المادية والخوادم أو في السحابة، فمن المهم أن يكون لديك نسخة احتياطية. ضع في اعتبارك أنه إذا كنت تعتمد على التخزين الفعلي على الجهاز، فمن السهل جدًا أن تفقد الوصول إلى بياناتك. قد تسكب القهوة على الكمبيوتر وتدمر محرك الأقراص الثابتة. يمكن اختراق أجهزة الكمبيوتر الخاصة بالموظفين وإغلاق تأمين جميع الملفات المحلية باستخدام برامج الفدية الضارة. قد يفقد شخص ما جهاز في القطار أو يُسرق منه مع حقيبته. وكما ذكرنا سابقًا، يُعد هذا سببًا آخر لأهمية استخدام 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 استخدامه مع جهاز تخزين خارجي؛ وبالنسبة للأجهزة التي تعمل بنظام التشغيل Windows، يقدم **File History** (محفوظات الملفات) وظيفة مشابهة.يمكن لأجهزة iPhone و Android أن تنسخ تلقائيًا المحتويات الأكثر أهمية عبر السحابة إذا تم تمكين ذلك ضمن إعدادات الهاتف.

إذا كان برلمانك يستخدم 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 البرلمان احتياطيًا إلى محرك أقراص ثابت خارجي أو سلسلة من محركات الأقراص، ولكن تأكد من تشفير محركات الأقراص هذه بكلمة مرور قوية. يمكن لبرنامج Time Machine تشفير محركات الأقراص الصلبة لك، أو يمكنك استخدام 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.



تخزين البيانات بشكل آمن

- **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 الأعضاء والموظفين على كيفية مشاركة المستندات بشكل صحيح (وعدم الإفراط في المشاركة).
- **إذا اختار برلمانك تخزين البيانات محليًا، فاستثمر في موظفين مهرة في مجال تكنولوجيا المعلومات.**
- **حافظ على أمان النسخ الاحتياطية للبيانات - قم بتشفير محركات الأقراص الصلبة الاحتياطية أو غيرها من أجهزة النسخ الاحتياطي.**

البقاء آمنًا على الإنترنت

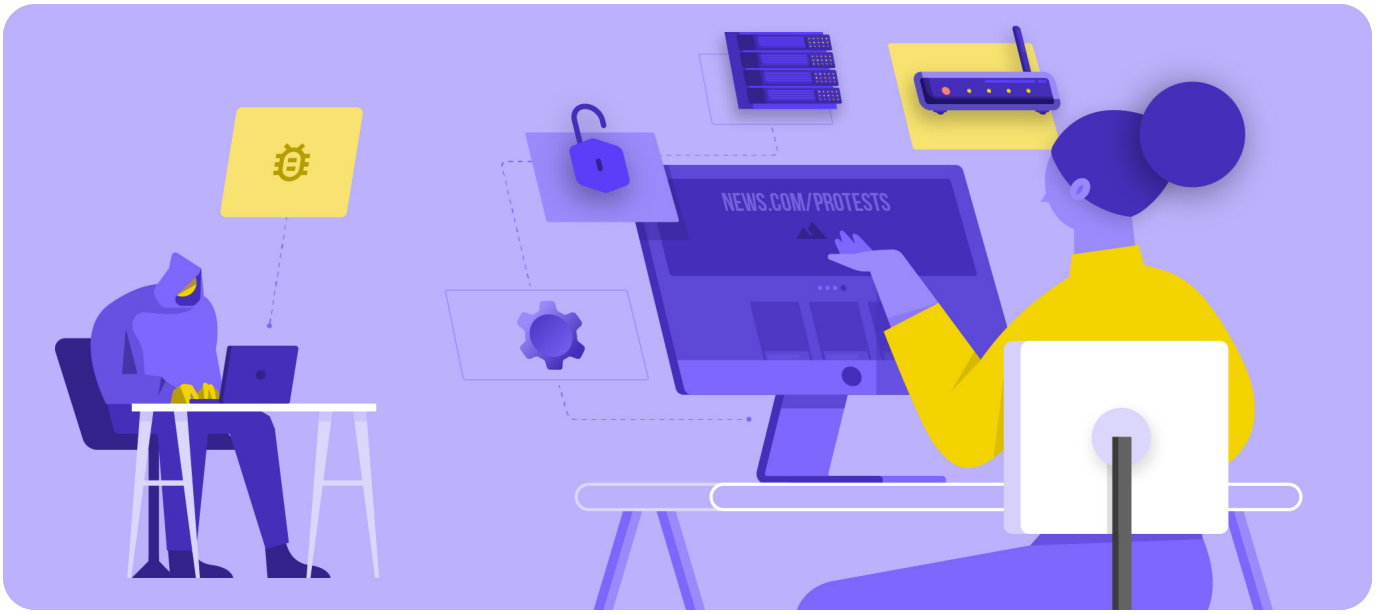
عند استخدام الإنترنت على هاتفك أو جهاز الكمبيوتر، يمكن لنشاطك أن يخبرنا كثيرًا عنك وعن مؤسستك.

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.

التصفّح بأمان

استخدام HTTPS

تُعد الخطوة الأكثر أهمية للحد من قدرة الخصم على مراقبة برلمانك 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 ببروتوكول "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 مخترقين 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.



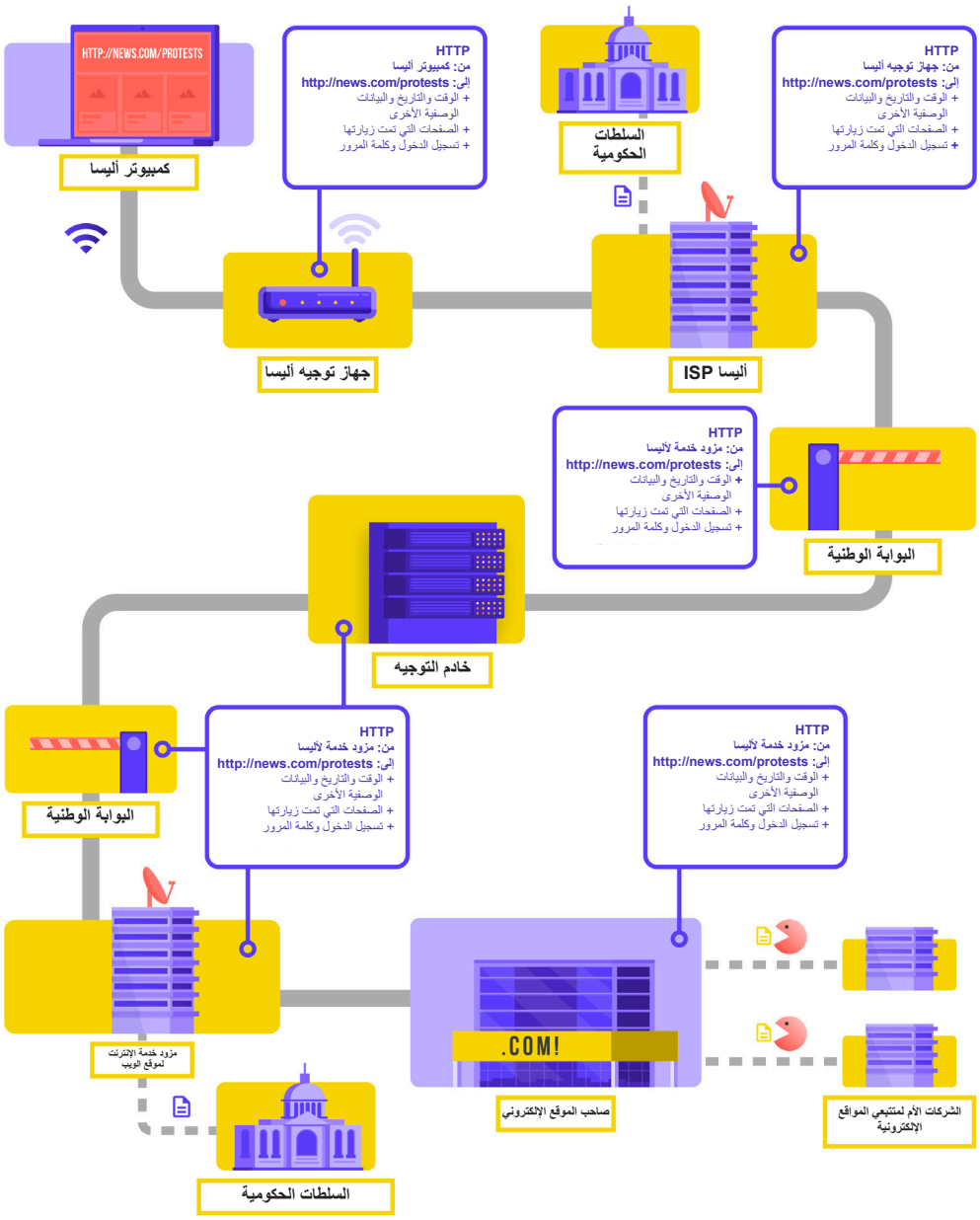
المراقبة والرقابة والبرلمانات

تستخدم الحكومات غير الصديقة وغيرها من الجهات الفاعلة في مجال التهديد في جميع أنحاء العالم تكنولوجيا المراقبة التي أصبحت متاحة بصورة متزايدة، وقد تلجأ في بعض الحالات إلى اختراق بسيط لشبكة Wi-Fi، لمراقبة نشاط أعضاء البرلمان وغيرهم من العاملين في البرلمان عبر الإنترنت. على سبيل المثال، سرق المخترقون بيانات من أعضاء البرلمان الأوروبي والزائرين من خلال انتحال شبكة Wi-Fi العامة للبرلمان في عام 2013. معاينة للهجمات الأكثر تعقيدًا في السنوات التالية.

بالإضافة إلى اختطاف حركة الإنترنت وسرقة البيانات، يقوم الخصوم أيضًا بتعطيل العمليات البرلمانية الهامة عن طريق منع الوصول إلى الإنترنت والأنظمة. في بروكسل، توقف البرلمان البلجيكي عن العمل بسبب هجوم الحرمان الهائل من الخدمة في مايو 2021. أجبر الهجوم على تأجيل بعض المناقشات واجتماعات اللجان، حيث لم يتمكن المستخدمون من الوصول إلى الخدمات الافتراضية المطلوبة للمشاركة في الجلسة.

إن التكرار المتزايد لمثل هذه الهجمات على الوصول إلى المعلومات عبر الإنترنت وإعادة توجيهها يسلط الضوء على مدى أهمية فهم البرلمانات لمخاطر العمل على الإنترنت ووضع خطط لكيفية الاتصال عند تأثر الاتصال.

فلنأخذ مثالاً حقيقيًا لما يبدو عليه الاستعراض بدون تشفير:

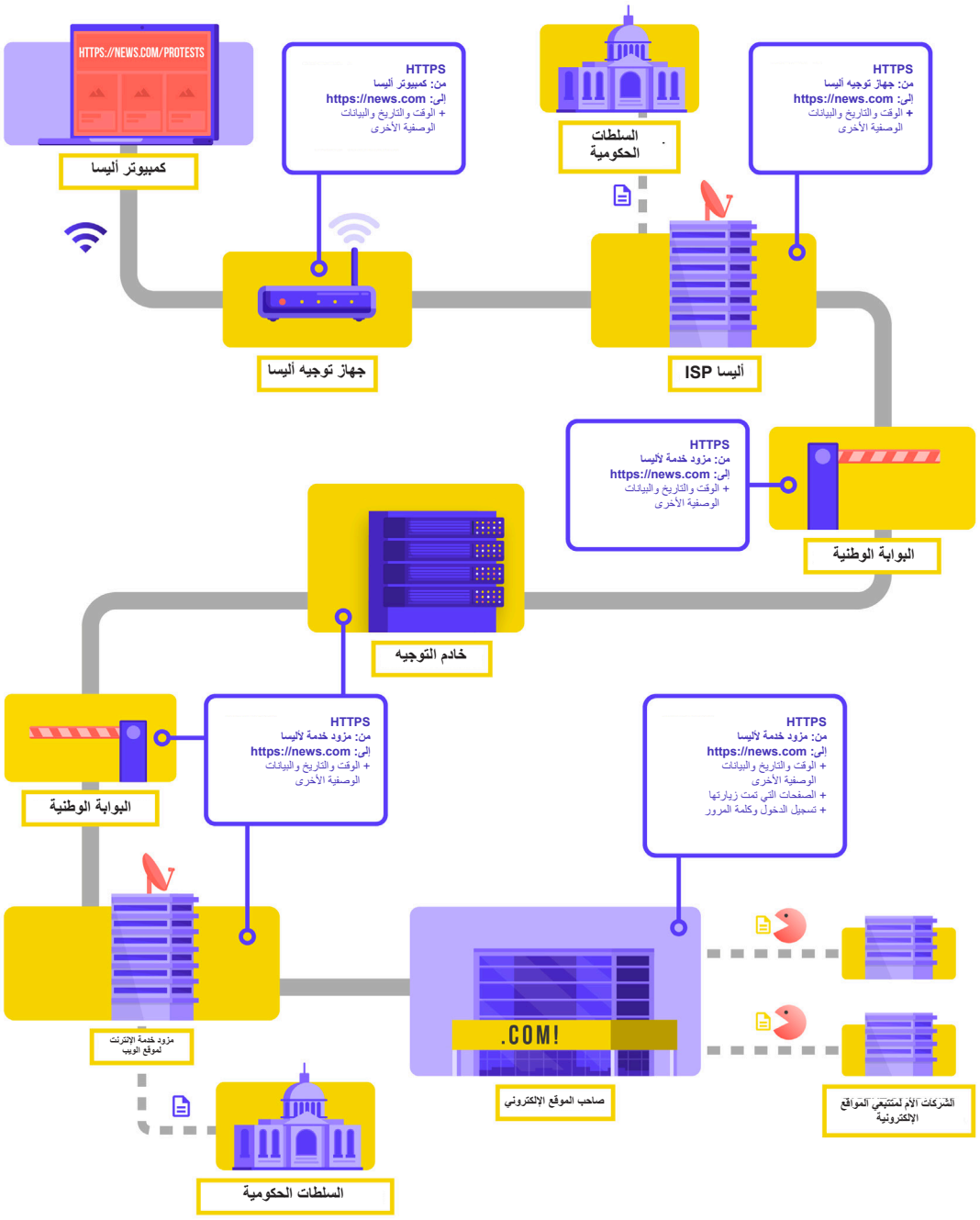


مقتبس من مشروع Totem [How the Internet Works](#) (CC-BY-NC-SA)

عند الاستعراض بدون تشفير، يتم الكشف عن جميع بياناتك. كما هو موضح أعلاه، يمكن للخصم رؤية مكانك وأنك تنتقل إلى الموقع news.com، والنظر على وجه التحديد إلى الصفحة الخاصة بالاحتجاجات في بلدك، وربما الأهم من ذلك، بصفتك نائبًا أو عضوًا في البرلمان، الاطلاع على كلمة المرور الخاصة بك شارك 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 استخدام **HTTPS (يعني الحرف "s" الأمان) يعني أن التشفير في موضعه.** وهذا يوفر لك المزيد من الحماية.

دعونا نلقي نظرة على ما يبدو عليه التصفح باستخدام HTTPS (المعروف أيضًا باسم التشفير:)



مقتبس من مشروع Totem [How the Internet Works](#) (CC-BY-NC-SA)

باستخدام 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 (لاستخدام هذا المثال.) ويُعد هذا فرقًا مهمًا. تحقق دائمًا من أن HTTPS في مكانه قبل التنقل عبر موقع الويب أو إدخال معلومات حساسة. كذلك، يمكنك استخدام 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 كان برلمانك مهتما بالمراقبة المستهدفة بشدة فيما يتعلق بالأنشطة عبر الإنترنت ويواجه رقابة متطورة عبر الإنترنت (مثل حجب مواقع الويب والتطبيقات)، فقد ترغب في استخدام شبكة خاصة افتراضية موثوقة (VPN).

استخدام 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 استخدام DNS مشفر.

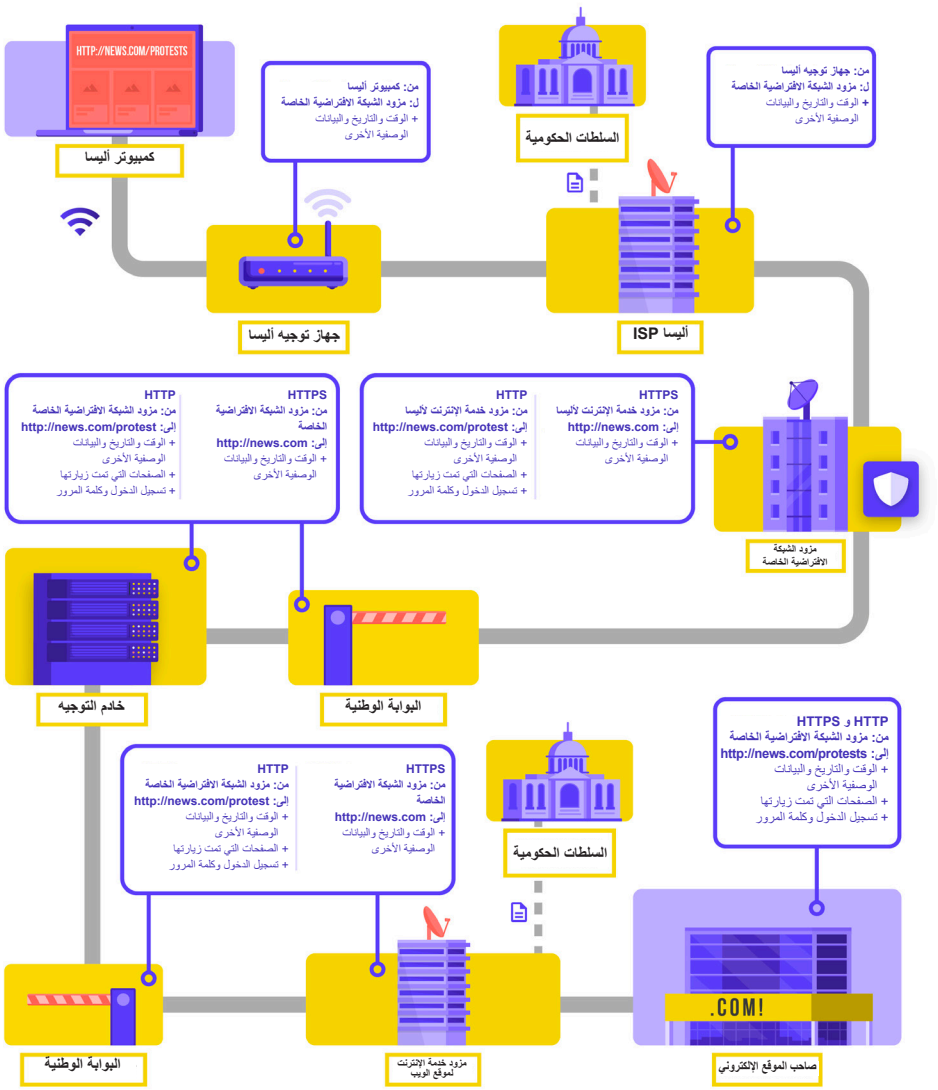
إذا كنت تتساءل، DNS تعني نظام أسماء المجالات. إنه في الأساس دليل الهاتف الخاص بالإنترنت، فإنه يترجم أسماء المجالات السهلة مثل ndi.org إلى عناوين برتوكول إنترنت مناسب للويب (IP). وهذا يسمح للأشخاص باستخدام مستعرضات الويب للبحث بسهولة عن موارد الإنترنت وتحميلها وزيارة مواقع الويب. على الرغم من ذلك، لا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

لاستخدام DNS المشفر وإضافة مستوى قليل من الحماية إلى حركة الإنترنت في الوقت نفسه، يُعد تنزيل تطبيق 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 بشركة 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 "استخدام 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 الاستخدام يمكن أن تساعد الموظفين في برلمانك في الاستفادة من DNS مُشفر وتقديم حماية إضافية من مزود 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 المخترقين على شبكتك ومسؤول الشبكة وموفر خدمة الإنترنت وأي شخص قد تشارك معه البيانات. في مؤسسة كبيرة - مثل البرلمان - غالبًا ما تُستخدم شبكات VPN "للأعمال" أو "الشركات" للمساعدة في حماية سلامة الوصول إلى الأنظمة والتطبيقات الداخلية (مثل تلك المستخدمة في التصويت عن بُعد) أيضًا. سواء كنت تستخدم VPN شخصيًا أو مصممًا لأغراض تجارية، فإن مفهوم حماية حركة المرور على الإنترنت من التطفل يعمل بشكل عام، ويظل من الضروري الاستمرار في استخدام HTTPS (حتى مع وجود VPN في مكانه). من المهم أيضًا التأكد من أنك تثق في VPN التي يستخدمها برلمانك. إليك مثالاً عما يبدو عليه التصفح باستخدام VPN:



مقتبس من مشروع Totem [How the Internet Works](#) (CC-BY-NC-SA)

لوصف شبكات VPN بمزيد من التفصيل، يشير هذا القسم إلى دليل الدفاع الذاتي ضد المراقبة الخاص بمؤسسة 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 المخترقين 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 استخدام 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 لبرلمانك وموظفيه، فإنه يمكنك تقييم شبكات VPN استنادًا إلى نموذج الشركة وسمعتها والبيانات التي تجمعها أو لا تجمعها وبالطبع أمان الأداة نفسها.

لماذا يجب عليك عدم استخدام 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 الممولين؟ 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 أجنبية 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 الايرانيون 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 استخدامها؟

إذا كنت بحاجة أيضًا إلى حل، بالإضافة إلى ضمان أمن حركة الإنترنت البرلمانية، لتقييد الوصول بشكل آمن لأولئك الموجودين على الشبكة البرلمانية فقط (حتى أثناء العمل عن بُعد) على الأنظمة والتطبيقات البرلمانية الداخلية، فقد ترغب في استخدام خدمة VPN المخصص للشركات أو المؤسسات. توجد مجموعة من الخيارات باستخدام تقنيات مختلفة قد تفكر فيها، بما في ذلك AnyConnect من Cisco، أو PaloAlto's Global Protect، أو Cloudflare's Access (تقنيًا Zero Trust Access System، وليس VPN) على سبيل المثال لا الحصر. في كلتا الحالتين، تتطلب هذه الأنظمة موظفين مهرة في تكنولوجيا المعلومات للتنفيذ والإدارة الفعالة.

إذا كان نظام VPN "الشركة" المتقدم إما خارج الميزانية أو معقدًا بشكل غير ضروري للبرلمان الخاص بك، فيمكنك أيضًا التفكير في استخدام خيارات VPN الشخصية مثل ProtonVPN أو TunnelBear (والتي تقدم أيضًا خطة Teams لجعل إدارة الحساب أبسط) لجميع أعضاء البرلمان و طاقم عمل. هناك خيار آخر ألا وهو تكوين الخادم الخاص بك باستخدام Outline الخاص بمنصة Jigsaw، حيث لا توجد شركة تدير حسابك ولكن في المقابل عليك إعداد الخادم الخاص بك.

على الرغم من أن معظم شبكات VPN الحديثة قد تم تحسينها فيما يتعلق بالأداء والسرعة، إلا أنه من الجدير بالذكر معرفة أن استخدام 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 طويل 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 باستخدام شبكة VPN، فمن المهم أيضًا التأكد من استمرار تشغيل شبكة VPN. قد يبدو الأمر واضحًا، لكن لا تقدم شبكة VPN التي يتم تثبيتها دون تشغيلها أي نوع من أنواع الحماية.

إخفاء الهوية من خلال Tor

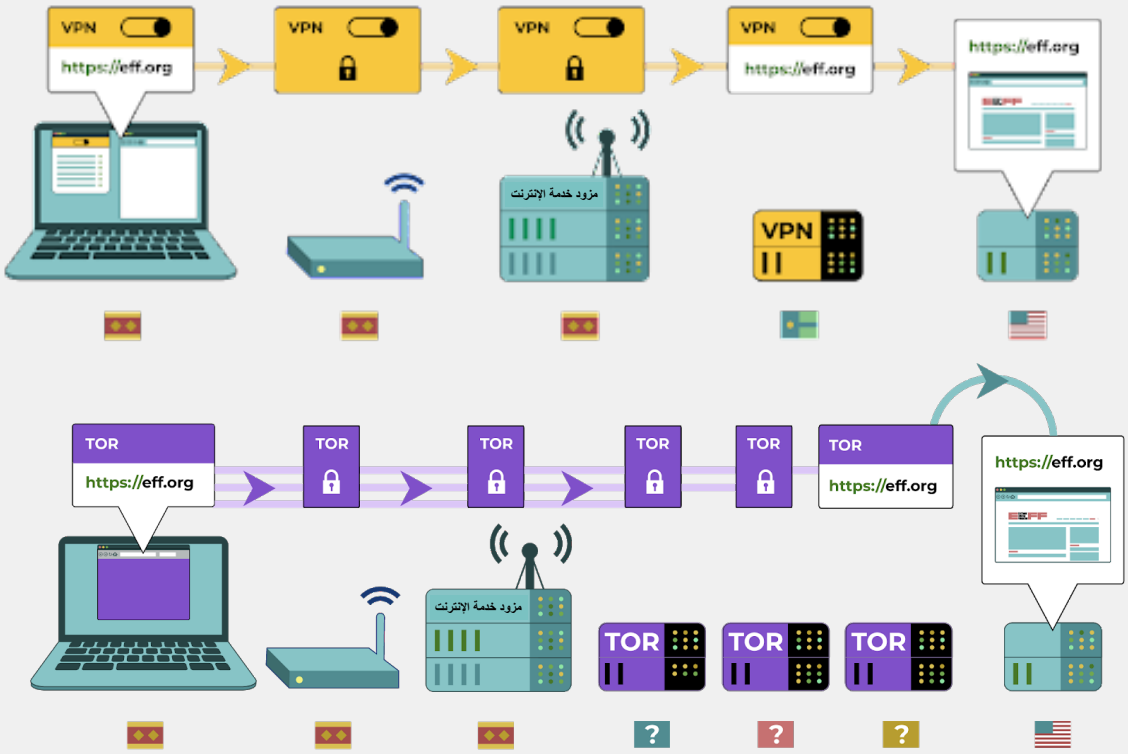
بالإضافة إلى شبكات VPN، قد تكون قد سمعت عن Tor كأداة أخرى لاستخدام الإنترنت بشكل أكثر أمانًا. من المهم أن تفهم ماهية كليهما، ولماذا قد تستخدم أحدهما أو الآخر.

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 لاستخدام 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 استخدام 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 استخدام شبكة VPN - لا يزال من الضروري استخدام 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 استخدام نظام التشغيل Tails، الذي يوجّه جميع الحركات عبر Tor بالوضع الافتراضي. كذلك، يستطيع مستخدمو Android استخدام التطبيق Orbot لتشغيل Tor لجميع حركات



وتطبيقات الإنترنت على الجهاز. بغض النظر عن كيفية استخدام Tor، من المهم معرفة أنه عند استخدامه، 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 استخدام شبكة VPN، قد يؤدي ذلك إلى رفع مستوى المخاطر لمنظمتك إلى حد كبير، لأن Tor ليس أداة شائعة الاستخدام بشكل كبير وبالتالي فإنها تبرز أمام الخصوم الذين قد يراقبون حركة الإنترنت الخاصة بك.

لذلك، في حين أنه من المحتمل جدًا وجود حالات قليلة جدًا يكون فيها Tor ضروريًا للاستخدام في سياق برلماني، إذا كنت لا تستطيع تحمل تكلفة VPN جديرة بالثقة أو وجدت برلمانك يعمل في بيئة يتم فيها حظر الشبكات الافتراضية الخاصة بشكل روتيني، يمكن أن يكون Tor خيارًا جيدًا، إذا كان قانونيًا، للحد من تأثير المراقبة وتجنب الرقابة عبر الإنترنت.

هل هناك أية أسباب تمنعنا من استخدام VPN أو Tor؟

بصرف النظر عن المخاوف المتعلقة بخدمات VPN ذات السمعة غير الجيدة، فإن أهم شيء يجب مراعاته هو ما إذا كان استخدام شبكة VPN أو Tor قد يجذب انتباه جهات غير مرغوب فيها أو ان يكون مخالفًا للقانون في بعض الدوائر القضائية، . وعلى الرغم من عدم قدرة مزود خدمة الإنترنت على معرفة المواقع التي تزورها أثناء استخدام هذه الخدمات، إلا أنه يكون على علم بأنك متصل بمتصفح Tor أو VPN. إذا كان هذا غير قانوني حيث يعمل برلمانك أو موظفوه أو قد يتسبب في مزيد من الاهتمام أو المخاطرة من مجرد تصفح الويب باستخدام HTTPS القياسي ونظام أسماء النطاقات المشفر، ربما يكون VPN أو Tor على وجه الخصوص (وهو أقل استخدامًا بكثير وبالتالي يمثل "علامة حمراء أكبر" ") ليس هو الخيار الصحيح.

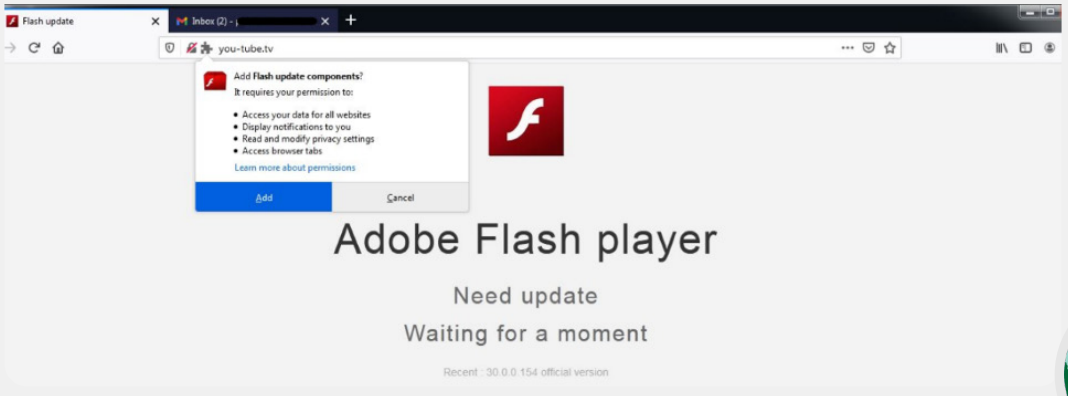
ما المستعرض الذي يجب أن نستخدمه؟

استخدم متصفحًا ذا سمعة جيدة مثل مستعرض Chrome أو Firefox أو Brave أو Safari أو Edge أو Tor. يتم استخدام كلاً من Chrome و Firefox على نطاق واسع جدًا وإنهما يقومان بعمل رائع فيما يتعلق بالأمان. يفضل بعض الأشخاص استخدام 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 استخدام 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

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. على سبيل المثال، استهدفت إضافة خبيثة مصممة بذكاء بعنوان "مكونات تحديث الفلاش" المنظمات السياسية التبتية في أوائل عام 2021. تم تقديم الوظيفة الإضافية للمستخدمين الذين زاروا مواقع الويب المرتبطة برسائل البريد الإلكتروني المخادعة، وعند تثبيتها، مكنت المخترقين من سرقة البريد الإلكتروني وبيانات التصفح.

يمكن أن تكون الوظائف الإضافية للمتصفح أيضًا ناقلًا لإصابة الموارد البرلمانية مثل مواقع الويب، والتي بدورها يمكن أن تنشر البرامج الضارة إلى مجموعة واسعة من زوار الموقع (بما في ذلك عامة الناس وموظفي البرلمان والأعضاء أنفسهم). خذ، على سبيل المثال، استغلال المخترقين لبرنامج Browsealoud الإضافي الشهير في المتصفح (المعروف الآن باسم ReachDeck)، وهو برنامج يحول نص موقع الويب إلى صوت للمستخدمين ضعاف البصر. في عام 2018، أدخل المخترقون رمزًا ضارًا في الوظيفة الإضافية للمتصفح، والتي كانت مستخدمة على مواقع الويب لكيانات حكومية مختلفة، بما في ذلك برلمان ولاية فيكتوريا في أستراليا. مع وجود الوظيفة الإضافية للمستعرض المصابة في مكانها وتكوينها بشكل غير صحيح، أصيبت أجهزة زوار الموقع ببرامج ضارة عند زيارة الموقع. في هذه الحالة، تم استخدام البرامج الضارة للاستفادة من الأجهزة لتعدين العملات المشفرة، ولكن يمكن استخدام هذه التكتيكات من قبل المخترقين لنشر البرامج الضارة لأغراض سرقة البيانات أو التجسس أيضًا.



أمان وسائل التواصل الاجتماعي

يمكن للموظفين البرلمانيين والنواب الكشف عن الكثير - وأحيانًا أكثر مما تنوي الإفصاح عنه - من خلال 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. لا ينطبق هذا على الصفحات الرسمية للبرلمانات فحسب، بل ينطبق أيضًا في بعض الحالات على الحسابات الشخصية للموظفين وحسابات عائلاتهم وأصدقائهم أيضًا.

أمن وسائل التواصل الاجتماعي والبرلمانات

حتى المنظمات التي لا تمثل تهديدًا على جهة معينة 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 وابتعاد 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 المخترقون 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 البرلمان أو انتحال بنجاح شخصية نائب أو موظف بارز متصل عبر الإنترنت.

بالإضافة إلى اختراق حسابات وسائل التواصل الاجتماعي، تعد مواقع البرلمان أيضًا أهدافًا شائعة نظرًا لظهورها العام وأهميتها في السمعة. في أحد الأمثلة من عام 2017، تمت إزالة موقع الويب البرلماني النمساوي من قبل مجموعة قرصنة يُفترض أنها غاضبة من العلاقات المتوترة للبلاد مع تركيا في ذلك الوقت.

قم بتطوير سياسة برلمانية لوسائل التواصل الاجتماعي

افترض أن أي شيء يتم نشره على وسائل التواصل الاجتماعي يمكن أن يصبح معرفة عامة، وصياغة سياسة برلمانية لوسائل التواصل الاجتماعي وفقًا لذلك. نظرًا للطبيعة العامة لمعظم العمل البرلماني، من المحتمل أنك سترغب في مشاركة معظم المنشورات والرسائل علنًا، ولكن لا يزال من الضروري طرح أسئلة والإجابة عليها مثل: من لديه حق الوصول إلى حسابات وسائل التواصل الاجتماعي؟ من الذي يتم السماح له بالنشر ومن يحتاج إلى الموافقة على منشوراته؟ ماذا عن التعليقات والردود؟ ما المعلومات التي يجب/يجب عدم مشاركتها على وسائل التواصل الاجتماعي؟ إذا نشرت صورًا أو معلومات عن الموقع أو معلومات تعريفية أخرى عن موظفيك أو أعضائك أو شركائك، فهل طلبت إذنهم، وهل فكروا في أي مخاطر محتملة؟ هذه الأسئلة مهمة بشكل خاص إذا كان برلمانك يتعامل علنًا مع المواطنين من خلال وسائل التواصل الاجتماعي أو بوابات الإنترنت المماثلة للمشاركة العامة.

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 والأمان الأكثر منطقية للحسابات البرلمانية والشخصية 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 باستخدام عنوان بريدك الإلكتروني أو رقم هاتفك (الشخصي أو المهني)؟
- 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** و **Twitter** و **Instagram** 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 برلمانك تكون آمنة بمقدار مستوى الأمان في الحسابات التي "ترتبط" بها. تذكر هذا الأمر المهم بالنسبة لموقع التواصل Facebook، حيث يمكن إدارة صفحاتك بواسطة حساب شخصي مرتبط بشخص ما.

المضايقات عبر الإنترنت

لسوء الحظ، يواجه العديد من البرلمانات والمجموعات التابعة مضايقات كبيرة عبر الإنترنت، خاصة 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 ب NDI's Gender, Women, and Democracy team، 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.

بينما يطور برلمانكم سياسته الخاصة بوسائل التواصل الاجتماعي، فمن المهم أن تكون على علم بهذه الديناميكيات. اجعل خطة الأمان الخاصة بك تشتمل على دعم منظم للأعضاء والموظفين الذين يواجهون رسائل سلبية وإهانات وتهديدات على وسائل التواصل الاجتماعي، سواء كان ذلك في حياتهم الوظيفية أو في حياتهم الشخصية. قم بتطوير بنية تحتية لمكافحة التحرش داخل البرلمان، بما في ذلك إجراء مسح لموظفيك لفهم كيفية تأثير التحرش عبر الإنترنت عليهم وإنشاء فريق استجابة سريعة لمساعدة الموظفين على مواجهة المواقف الصعبة. كذلك يقدم الدليل الميداني 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** لمضايقات و/أو الحسابات المسببة للمشاكل مباشرة إلى الأنظمة الأساسية أيضًا.

عند التعامل مع الأعضاء أو 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. وقم بتضمين خطة الأمن الخاصة ببرلمانك قائمة بالمهنيين المحليين والمنظمات ووكالات إنفاذ القانون المحلية التي يمكنك توصيل الموظفين بها للحصول على المساعدة القانونية والطبية والصحية العقلية والفنية إذا لزم الأمر. للحصول على أفكار إضافية، تحقق من Feminist Frequency's **دليل الأمان عبر الإنترنت**.

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 البرلمان أو مواقع الويب الخاصة ببرلمانك.

بالنسبة لصفحات وسائل التواصل الاجتماعي، فهذا يعني حماية هذه الحسابات باستخدام 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 استخدام مجموعة كبيرة من أجهزة الكمبيوتر لسحب خادمك إلى حركة ضارة. تتضمن بعض الخيارات لحماية DDoS - والتي تجعل الأمر أكثر صعوبة على الخصم لإيقاف موقع الويب الخاص بك - تشمل **Cloudflare** أو Amazon's **AWS Shield** أو خدمة eQualitie's **Deflect**.

استضافة موقع الويب الخاص ببرلمانك بأمان

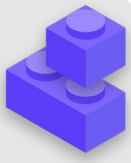
تتم استضافة مواقع الويب على أجهزة الكمبيوتر - وإنها عُرضة للقرصنة تمامًا كما يحدث مع أجهزتك الخاصة. إذا كان ذلك ممكنًا، يجب أن يستفيد برلمانك من خدمات الاستضافة الحالية مثل WordPress أو Wix أو غيرها التي تدير جميع أمان الموقع نيابة عنك. إذا كانت احتياجات موقع الويب الخاص بك أكثر تعقيدًا، أو إذا كنت تحتاج 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 استخدام موفري خدمات الاستضافة عبر السحابة مثل AWS (Amazon Web Services) أو Microsoft Azure أو النظام الأساسي **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 كان برلمانك يتمتع بالذكاء التقني لاستضافة موقع الويب الخاص به، فإنه يجب عليك التفكير في اختيار ما يُطلق عليه "موقع ثابت". على عكس مواقع الويب الديناميكية، تقلل أنواع المواقع هذه مستوى هجوم المخترقين وستجعل موقع الويب الخاص بك أكثر مقاومة للهجوم.

حماية شبكة WiFi الخاصة بك

كل هذه الخطوات لحماية حركة مرور الويب من المراقبة والرقابة مهمة، لكنها ليست بديلاً عن أمان الشبكة الأساسي في البرلمان والمنزل.

لا تنس الأساسيات مثل استخدام 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 المباني البرلمانية أيضًا إذا كان لديك زائرين يستخدمون الإنترنت يدخلون من المبنى ويخرجون منه.



البقاء آمنًا على الإنترنت

- **قم بإجراء تدريب منتظم للأعضاء والموظفين لمعرفة مدى أهمية اتباع تدابير أمان الويب الأساسية.**
- **ذكّر الموظفين بالاستعراض باستخدام HTTPS وDNS المشفر.**
- **طالب الموظفين بإعادة تشغيل المستعرضات بانتظام لتثبيت التحديثات.**
- **شجّع على استخدام الخصوصية لحماية المستعرضات والملحقات.**
- **إذا كانت شبكة VPN مناسبة، فاختر واحدة ذات سمعة جيدة، وقم بتدريب الموظفين على استخدامها، وتأكد من استخدامها باستمرار.**
- **قم بتطوير وتوزيع سياسة برلمانية واضحة حول استخدام وسائل التواصل الاجتماعي.**
- **قم بتمكين إعدادات الخصوصية والأمان على جميع حسابات وسائل التواصل الاجتماعي.**
- **افهم تأثيرات المضايقات عبر الإنترنت وكن مستعدًا لدعم الأعضاء والموظفين المتضررين.**
- **ضع قائمة بالمهنيين والمنظمات ووكالات إنفاذ القانون التي يمكنك توصيل الموظفين بها للحصول على مساعدة قانونية ومساعدة خاصة بالصحة العقلية و المساعدة التقنية 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 Wi-Fi المحلية.**

حماية الأمن المادي

من المهم الحفاظ على أمان أجهزتك فعليًا. ضع في اعتبارك أن الأمان الفعلي يتجاوز مجرد أمان الأجهزة، ويجب أن يتضمن إستراتيجيات لحماية كل شيء آخر في عالمك. وهذا يشمل المستندات المطبوعة؛ مكاتب البرلمان؛ غرف، أو أماكن عمل؛ وبالطبع أنت وموظفيك وأعضاء فريقك.

الأمان الفعلي و البرلمان

لسوء الحظ، فإن الاعتداءات المادية على البرلمانات والهيئات التشريعية الأخرى شائعة، وغالبًا ما تترك تأثيرات كبيرة على الأمان الفعلي وأمن المعلومات. في 6 يناير 2021، اقتحم المتمردون مبنى الكابيتول بالولايات المتحدة - موطن مجلسي البرلمان الأمريكي - في محاولة لوقف التصديق على نتائج الانتخابات الرئاسية. أدى الاعتداء المادي بشكل مأساوي إلى مقتل خمسة أشخاص وتسبب في معاناة نفسية كبيرة لأعضاء الكونغرس وموظفيه. ومع ذلك، لم يكن هذا هو التأثير السلبي الوحيد. قام المهاجمون أيضًا بتدمير معدات تكنولوجيا المعلومات، وتمكنوا من الوصول إلى مواد حساسة في مكاتب الأعضاء، وربما الأكثر ضررًا، سرقوا أجهزة كمبيوتر وأجهزة أخرى تحتوي على معلومات سرية محتملة من الكابيتول الأمريكي.

مرافق المعلومات المجزأة الحساسة (SCIFs)

لإجراء محادثات حساسة للغاية، قامت بعض البرلمانات بتأمين غرف فعلية تسمى SCIFs. يتم إنشاء هذه المساحات بحيث يمكن الاطلاع على المعلومات الحساسة، مثل القضايا المتعلقة بالأمن القومي أو الاستخبارات، ومناقشتها بين النواب وموظفيهم دون القلق من المراقبة الخارجية أو التجسس. بالإضافة إلى البناء المادي المناسب، يتطلب SCIF المناسب أن يترك الأشخاص الأجهزة (مثل هواتفهم المحمولة) خارج الغرفة قبل الدخول للمناقشة.

حماية الأصول الفعلية

يُعد الأمان الفعلي لأجهزتك هو أحد المكونات الأساسية لأمن المعلومات.

وبالإضافة إلى التخفيف من تأثير الجهاز المسروق باستخدام شاشات حماية وكلمات مرور وتنفيذ تشفير القرص بالكامل وتشغيل ميزات المسح عن بُعد، فإنه يجب عليك كذلك وضع آليات 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 مبنى البرلمان و/أو المنزل. وبالإضافة إلى ذلك، فكر في شراء خزنة كمبيوتر محمول أو خزانة قابلة للقفل للحفاظ على حماية الأجهزة طوال الليل. يمكن للكاميرات الأمنية أو أنظمة استشعار الحركة في جميع أنحاء المبنى الكشف عن عمليات الاقتحام والسرقة المادية وردعها. ابحث عن خيار احترام الخصوصية المتاح في بلدك، وتأكد من اختيار الكاميرات وأنظمة الأمان التي توفرها الشركات الموثوقة التي ليس لديها حافز لتسليم البيانات والمعلومات إلى خصم محتمل.

إذا كانت الأجهزة القديمة لا تزال تحتوي على معلومات مخزنة عليها ولكنها لم تعد قيد الاستخدام، 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 الثابتة باستخدام مطرقة. فأحيانًا تكون الحلول الأقدم هي الأفضل!

حتى قبل اتخاذ هذه الخطوات التقنية، استغرق لحظة للقيام بجرد جميع الأجهزة في جميع أنحاء البرلمان. إذا لم يكن لديك قائمة بجميع الأجهزة، فمن الصعب تتبع ما قد يكون مفقودًا في حالة السرقة.

ماذا نفعل بكل تلك الأوراق؟

من المحتمل أن يكون لدى برلمانك الكثير من المعلومات التي تتم طباعتها على الورق أو مكتوبة في دفاتر الملاحظات أو مكتوبة على أوراق الملاحظات اللاصقة. قد يكون بعض هذا حساسًا للغاية - ملاحظات من شهادة سرية أو اجتماعات خاصة، على سبيل المثال. 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. احتفظ بالمعلومات الحساسة للغاية في مكان أقل استهدافًا ومحميًا جيدًا.

حاول قدر الإمكان التخلص من المعلومات الورقية غير الضرورية. تذكر: لا يمكن سرقة ما ليس بحوزتك. ضع سياسة برلمانية 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 البرلمان. 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.

السياسة البرلمانية

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

سؤال بسيط ولكن الإجابة عليه مهمة جدًا، والسؤال عليه هو من يحصل على مفتاح المكتب أو شارة الوصول. يجب أن يكون لدى الموظفين الموثوق بهم فقط مفاتيح أو شارات، ويجب تغيير الأقفال عند مغادرة الموظفين و/أو على أساس شبه منتظم. خلال النهار، يجب أن تكون أي أبواب تُترك مفتوحة معروضة باستمرار لشخص موثوق به و/أو حارس أمن. بالإضافة إلى ذلك، تأكد من أن البرلمان الخاص بك لديه علاقة موثوقة مع مقدمي الخدمات مثل موظفي التنظيف والفنيين الخارجيين الذين يمكنهم الوصول إلى المبنى. فكر في المعلومات أو الأجهزة التي قد يتمكن هؤلاء الأشخاص من الوصول إليها وتأكد من أنها محمية، وبخاصة إذا لم تكن تلك العلاقة موثوقة. يجب دائمًا تعيين شخص ما موثوق لإغلاق المكتب والتأكد من أنه يتم تأمين الأجهزة بشكل صحيح قبل المغادرة في نهاية اليوم.

هل يُسمح بتواجد المواطنين داخل مبنى البرلمان؟ ربما يحق للمواطنين الوصول إلى أجزاء من المبنى البرلماني؟ 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 يكون لدى الجمهور الزائر أو الضيوف إمكانية الوصول إلى الإنترنت عند زيارتهم، فيجب عليك إنشاء شبكة "ضيف" حتى لا يكون لدى هؤلاء الضيوف القدرة على مراقبة حركة المرور العادية الخاصة بك. 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 لبرلمانك 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 يكون للترهيب والتهديدات أو حالات العنف الجسدي أو الجنسي والعنف المنزلي والخوف من الهجوم تأثير سلبي خطير على حياة الأعضاء والموظفين. تعد أداة تخطيط السلامة **#Think10** من المعهد الديمقراطي الوطني (NDI) مورداً مفيداً لتزويد النساء الناشطات سياسياً اللواتي قد يتعرضن لمخاطر شخصية متزايدة نتيجة لمشاركتهن في البرلمان والسياسة بشكل عام.

من الواضح أن رفاهية الموظفين هي أحد الأصول المهمة بالنسبة إليهم كأفراد، ولكنها أيضًا عنصر حاسم لبرلمان سليم يعمل 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 PEN America's **دليل المضايقات الميدانية على الإنترنت** يتضمن أفكارًا حول كيفية دعم المنظمات للموظفين أثناء الأزمات وبعدها.

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 أو أجهزتك بحقوق الخصوصية عند عبور الحدود. على هذا النحو، من الجيد تضمين سياسة السفر البرلمانية في خطتك الأمنية التي تتضمن تذكيرات حول أفضل الممارسات الأمنية الرئيسية.

يجب أن تتضمن سياسة السفر الخاصة ببرلمانك الكثير من المعلومات التي يتم تناولها في أقسام أخرى من الدليل، بما في ذلك استخدام الإنترنت بأمان والحفاظ على الأجهزة ومصادر المعلومات الأخرى آمنة ماديًا معك في جميع 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 يتم مشاركتها عند السفر، هناك بعض النصائح التشغيلية الأساسية التي يجب عليك التفكير فيها وتضمينها في سياسة السفر البرلمانية الخاصة بك.

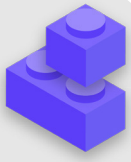
فكر في استخدام أجهزة كمبيوتر محمول أو هواتف خاصة بالسفر لا تحتوي على بيانات حساسة أو بها قدر قليل منها. إذا كان يتم إنجاز عمل البرلمان عبر السحابة، فإن Chromebook يمكن أن يكون خيارًا جيدًا غير مكلف نسبيًا لمثل هذا الجهاز. قم بإعادة تعيين إعدادات المصنع، أو "امسح" هذه الأجهزة عند إعادتها قبل الاتصال بشبكات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

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. ولا تثق في منافذ شحن USB العامة. أصبحت منافذ شحن USB في المطارات والمحطات والمركبات شيئًا مألوفًا بشكل متزايد وطريقة مريحة جدًا لشحن الأجهزة. ومع ذلك، يمكن أن تكون وسيلة سهلة لالتقاط البرامج الضارة. لذلك، تأكد من شحن الأجهزة إما بالطريقة التقليدية من خلال قابس في الجدار أو قم بشراء أجهزة **حظر بيانات USB** للسماح للموظفين المسافرين بشحن أجهزتهم عبر USB.

حجز السفر بأمان للبرلمان الخاص بك

عند وضع سياسة سفر، ضع في اعتبارك المعلومات التي قد يتم كشفها عند تنظم رحلة سفر أو حجزها. يمكن أن يكون هذا مهمًا بشكل خاص إذا كنت تنظم أحداثًا كبيرة أو مؤتمرات تعالج فيها معلومات حساسة من مجموعة متنوعة من الموظفين أو الأعضاء أو الحاضرين. فكر جيدًا في كيفية مشاركة المعلومات الشخصية مثل تفاصيل جواز السفر ومسارات السفر والسجلات الطبية بأمان وتخزينها (إذا لزم الأمر).



حماية الأمن الفعلي الخاص بك

- **ذكّر الموظفين بضرورة حماية أجهزتهم فعليًا في جميع الأوقات.**
- **تحقق من جميع الطرق التي يمكن للناس من خلالها الوصول إلى أماكن العمل الخاصة بك وتأمينها.**
- **ضع سياسة لضيف المكتب وسياسة الوصول.**
- **استخدم الأقفال القوية وأنظمة الهوية / الشارات وقم بتدويرها / تغييرها عند الحاجة.**
- **ضع في اعتبارك إنشاء كاميرات أو أنظمة أمان محلية أخرى.**
- **احصل على آلة تمزيق الورق واستخدمها.**
  - قم بإعداد وقت مخصص للموظفين للتخلص من المستندات المطبوعة التي تحتوي على معلومات حساسة.
- **ضع قائمة بالمهنيين المحليين والمنظمات ووكالات إنفاذ القانون المحلية التي يمكنك توصيل الأعضاء والموظفين بها للحصول على المساعدة القانونية والطبية والصحية العقلية ردًا على الهجمات الجسدية أو التهديدات.**
- **ضع سياسة سفر خاصة بالبرلمان.**
- **تأكد من معرفة الموظفين بما يجب القيام به في حالة الطوارئ أثناء السفر.**
- **ضع في اعتبارك البيانات الإضافية التي يتم إنشائها ومشاركتها عند تنظيم السفر أو الأحداث.**

ماذا تفعل عندما تسوء الأمور

إذًا، إنك تعرف الأشياء الصحيحة التي يجب عليك القيام بها. لقد وضعت السياسات ودربت الجميع في البرلمان على أفضل الممارسات. حتى مع كل هذا العمل الشاق، فمن المحتمل جدًا أن يحدث خطأ ما في النهاية.

عندما يحدث ذلك، من المهم أن يكون لديك خطة الاستجابة للحوادث. تعتبر الاستجابة للحوادث جزءًا مهمًا، وغالبًا ما يتم التقليل من شأنها، وهي جزء من الخطة الأمنية لبرلمانك لأنه يمكن أن تكون الفرق بين الهجوم الذي يدمر سمعتك 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 الأعضاء والموظفين 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 البرلمان.

ما الذي يجب أن تخطط له؟ باختصار، أي شيء من المحتمل أن يحدث إلى حد ما. سيبدو ذلك مختلفًا بالنسبة لكل برلمان، ولكن الأسئلة الشائعة التي ستساعد خطة الاستجابة للحوادث في الإجابة عليها تشمل:

- 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 موظفينا لخطر جسدي؟ 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 في حالة ضياع أو سرقة جهاز الكمبيوتر أو الهاتف الخاص بالعضو؟

سيختلف البرلمان في الإجابات على هذه الأسئلة وغيرها، ولكن من المهم التفكير فيها معًا وصياغة خطة ومشاركتها بوضوح حتى يكون الجميع على استعداد لاتخاذ إجراءات فورية 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 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. هنالك أنواع مختلفة من التهديدات، لذلك عليك التفكير في الأدوار المختلفة التي قد يجب عليك القيام بها والجوانب العملية التي ينطوي عليها الاستجابة لحالة الطوارئ. ضمن هذه الإستراتيجية المهمة لحالات الطوارئ، يتم تنشيط شبكة الدعم - شبكة واسعة من الحلفاء، والتي قد تشمل فروعًا مختلفة لحكومتك، وحكومات صديقة أخرى، وشركات تقنية، وبائعي خدمات أمنية، ومؤسسات متعددة الأطراف على سبيل المثال لا الحصر. 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 وفعالية للتواصل مع كل جهة فاعلة في سيناريوهات مختلفة وحدد وسيلة 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 استخدامها ومع من يجب أن تتواصل. كذلك، فكر في تأثير الحادثة على سمعة برلمانك، واستعد للرد وفقًا لذلك. تأكد من أن قائد الاتصالات في البرلمان على علم بالحادث ويمكنه مشاهدة وسائل التواصل الاجتماعي أو وسائل الإعلام الأخرى لمعرفة التأثير المحتمل. 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

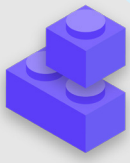
فكر في إنشاء نظام الإنذار المبكر والاستجابة. يبدو هذا النظام ممتازًا، ولكنه في الأساس مجرد وثيقة مركزية)إلكترونية أو غير ذلك(يتم فتحه في حالة الطوارئ. في المستند، يجب عليك تسجيل كافة التفاصيل المتعلقة بمؤشرات الأمان والحوادث التي حدثت في خط زمني وتقديم وصفًا واضحًا للإجراءات وتسلسل الاستجابة المخطط لها 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 يستعد برلمانك 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 برلمانك. وبالنسبة لمثل هذه المواقف، من المهم تحديد قائمة موثوق بها تضم الخبراء الفنيين الخارجيين الذين يمكنهم مساعدتك في الاستجابة للحوادث. في بعض الحالات، قد ترغب في التفاوض مسبقًا على الشروط مع مزودي الخدمة (مثل مضيف موقع الويب الخاص بك أو شركة أمن تكنولوجيا المعلومات) للتأكد من أنها متاحة (ولن تفرض رسومًا إضافية) على الاستجابة التقنية للحوادث.

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 يواجهها برلمانك كنتيجة لخرق البيانات أو أي حادث أمني آخر. بصفتك برلمانًا، فأنت في موقع يتمتع بسلطة وبروز خاصين عندما يتعلق الأمر بفهم واحترام اللوائح المحلية لأمن البيانات والخصوصية.

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 ثابتة تلائم الجميع للاستجابة للحوادث، فإنه من الضروري وضع خطط تشغيلية وخطط اتصالات وخطط تقنية وخطط قانونية. أثناء قيامك بوضع خطة الاستجابة للحوادث، فإننا نشجعك بشدة على الاستفادة من بعض الموارد الحالية الممتازة، والمصممة لمساعدة المؤسسات على التعامل مع الاستجابة للحوادث. على الرغم من عدم تصميم كل هذه الموارد خصيصًا للبرلمانات، إلا أن محتواها لا يزال وثيق الصلة بالموضوع. تشمل هذه الموارد أدوات الإسعافات الأولية الرقمية التي 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 و خط مساعدة الأمن الرقمي من Access Now.



الاستجابة للحوادث

- **وضع خطة برلمانية للاستجابة للحوادث وممارستها.**
  - فكر بإبداع في الحوادث المحتملة قبل حدوثها واستعد لاستجابتك.
- **تأكد من أن الجميع في البرلمان على دراية بكيفية التواصل والخطوات الفنية التي سيتم اتخاذها في حالة وقوع حادث.**
- **خصص وقتًا لفهم تدابير الحماية والالتزامات القانونية الخاصة بك.**
- **كن مستعدًا لتزويد الأعضاء والموظفين بالدعم العاطفي والاجتماعي الذي يحتاجون إليه في أعقاب أي حادث.**

الملحق أ:
المصادر المُوصى بها

- دليل الأمان الشامل التابع لمنظمة Tactical Techl; 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
- The Electronic Frontier Foundation's Security Education Companion; Creative Commons Attribution 3.0 US License
  - 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
- Electronic Frontier Foundation's Surveillance Self-Defense (SSD) Guide; Creative Commons Attribution 3.0 US License
  - ما الذي يجب أن أعرفه عن التشفير
  - التواصل مع الآخرين
  - اختيار VPN المناسب لك
- دليل Front Line Defender لتأمين أدوات الدردشة الجماعية والمؤتمرات
- Tactical Tech's Data Detox Kit
  - اسمح للشخص المناسب بالدخول: اجعل كلمة مرورك أقوى
  - تقوية أقفال الشاشة
- Center for Democracy & Technology's Elections Security Guide on Passwords; Creative Commons Attribution 4.0 International License
- Center for Democracy and Technology's Elections Security Guide on Two Factor Authentication; Creative Commons Attribution 4.0 International License
- Martin Shelton's Two Factor Authentication for Beginners; Creative Commons Attribution 4.0 International License
- الأمان في علبة الخاص بـ Tactical Tech و Creative Commons Attribution-ShareAlike 3.0 ; Frontline Defender رخصة غير محمولة
  - حماية جهازك من البرامج الضارة وهجمات التصيّد الاحتيالي
  - الحماية من التهديدات الجسدية
- أوه! النشرة الإخبارية الخاصة بـ SANS: أوقف تلك البرامج الضارة
- جهاز Apple والوصول إلى البيانات عندما تكون السلامة الشخصية في خطر
- مجموعة أدوات الأمن السيبراني للتحالف السيبراني العالمي للمنظمات القائمة على المهام
- أداة تقييم الأمن السيبراني لمؤسسة فورد

الملحق ب:
أدوات إطلاق خطة الأمان

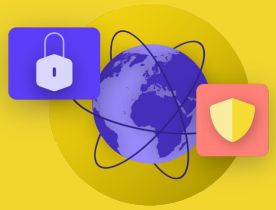
استخدم مجموعة أدوات البدء التالية لتدوين الملاحظات بينما تقرأ أنت والبرلمان الخاص بك الدليل وتستوعب المواد، واعتبر الأسئلة المصاحبة مع زملائك للمساعدة في توليد مناقشة مثمرة.

تأكد من الرجوع إلى "اللبنات الأساسية" الرئيسية في كل قسم من أقسام الدليل للتأكد من أنك تغطي الموضوعات المهمة أثناء بناء خطتك الأمنية. بنهاية الكتيب، يجب أن تشكل اللبنات الأساسية، والإجابات على أسئلة المناقشة هذه، وملاحظاتك الأساس لخطة أمنية ناجحة.

بناء ثقافة الأمان

أساس قوي: تأمين الحسابات والأجهزة

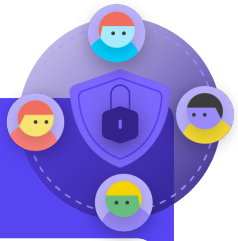
توصيل البيانات بشكل آمن



البقاء آمنًا على الإنترنت

حماية الأمن المادي

ماذا تفعل عندما تسوء الأمور



بناء ثقافة الأمان

الأسئلة التي ينبغي التفكير فيها:

- متى يمكنك جدولة محادثة لمراجعة خطتك الأمنية مع البرلمان بأكمله؟
- ما هي الأيام أو الأوقات التي تعمل بشكل جيد للبرلمان لجدولة محادثات منتظمة وتدريب حول الأمن؟
- ما هي الخطوات التي يمكن للقيادة اتخاذها لنموذج السلوك الأمني الجيد والالتزام بخطة أمنية؟ كيف يمكن للآخرين في البرلمان أن يلعبوا دورًا في الأمن؟

ملاحظاتك وأفكارك:

أساس قوي: تأمين الحسابات والأجهزة

الأسئلة التي ينبغي التفكير فيها:

- كيف ستنفذ تدابير أمان الحساب - مثل مدير كلمات المرور والمصادقة الثنائية - عبر البرلمان؟ ما هي العقبات التي قد تواجهها أثناء التنفيذ؟
- كيف سيضمن برلمانكم أن تظل الأجهزة آمنة ومحدثة؟ وكجزء من هذا، هل سيحتاج البرلمان إلى خطة للتعامل مع البرامج أو أجهزة الكمبيوتر غير المرخصة؟
- ما هو الوقت المناسب لإعداد تدريب لجميع الموظفين حول مخاطر التصيد الاحتيالي والبرامج الضارة وأفضل ممارسات أمان الجهاز؟

ملاحظاتك وأفكارك:

توصيل البيانات ومشاركتها بأمان

الأسئلة التي ينبغي التفكير فيها:

- كيف سيطبق برلمانكم الرسائل المشفرة من طرف إلى طرف من أجل اتصال آمن؟ ما هي العقبات التي قد تواجهها أثناء التنفيذ؟
- كيف سيقوم برلمانكم بفرض حل آمن لمشاركة الملفات داخليًا وخارجيًا؟ ما هي العقبات التي قد تواجهها أثناء التنفيذ؟
- كيف سيقوم برلمانكم بتنفيذ حل آمن لتخزين البيانات والنسخ الاحتياطي؟ ما هي العقبات التي قد تواجهها أثناء التنفيذ؟

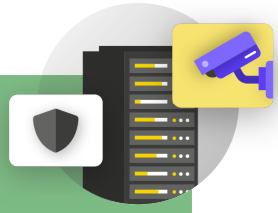
ملاحظاتك وأفكارك:

البقاء آمنًا على الإنترنت

الأسئلة التي ينبغي التفكير فيها:

- كيف سيقوم برلمانك بتنفيذ متطلبات التصفح الآمن مثل HTTPS، ومتصفح موثوق به، وإذا كان ذلك مناسبًا، VPN للموظفين؟
- ما هي العناصر الأساسية لسياسة برلمانكم الخاصة بوسائل التواصل الاجتماعي؟ كيف سيتم تطبيقها؟
- كيف سيحمي برلمانكم مواقعه وممتلكاته على شبكة الإنترنت؟

ملاحظاتك وأفكارك:



حماية الأمن المادي

الأسئلة التي ينبغي التفكير فيها:

- كيف سيوزع البرلمان ويفرض سياسة الضيف والوصول إلى المكاتب؟
- من المسؤول عن إعداد الموظفين لتحديات الأمن المادية والرقمية التي قد يواجهونها أثناء السفر للعمل؟
- ما الخطوات التي يمكن للموظفين اتخاذها للحفاظ على أجهزتهم آمنة في المكتب وأثناء السفر؟

ملاحظاتك وأفكارك:

ماذا تفعل عندما تسوء الأمور

الأسئلة التي ينبغي التفكير فيها:

- كيف سيقوم البرلمان بتوزيع وممارسة سياسة الاستجابة للحوادث؟
- هل هناك موارد متاحة للموظفين الذين قد يحتاجون إلى دعم عاطفي واجتماعي في أعقاب الحادث؟ إذا لم يكن الأمر كذلك، فكيف يمكن للبرلمان توفير هذه الموارد في حالة وقوع حادث؟

ملاحظاتك وأفكارك:

الملحق ج:
اقتباسات الصورة

الصفحة 14: نيويورك تايمز، "البرلمان الأسترالي يبلغ عن هجوم إلكتروني على شبكة حاسوبه"، 2019، صورة رقمية .Getty Images، https://www.nytimes. com/2019/02/07/world/australia/cyberattack-paricture-hack.html.

الصفحة 18: CNP Collection, "Security Protection Anti-Virus Software cms", 2014, digital image, 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: Bleeping Computers, "Norway parliament data stolen in Microsoft Exchange attack", 2021, digital image, https://www. .bleepstatic.com/content/hl-images/2021/03/10/storting.jpg

الصفحة 25: Cottonbro, "Person Holding Black and Silver Key", 2020, digital image, Pexels, https://www.pexels.com/photo/ .person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels

الصفحة 27: .Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/

الصفحة 30: "Microsoft Loading Screen," digital image, Kompass, September 23, 2019, https://asset.kompas.com/crops/kYVdzylbrYB5lI .puKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png

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

الصفحة 33: ZDNet, "Chinese hacking group impersonates Afghan president to infiltrate government agencies," 2021, digital image, https://www.zdnet.com/article/chinese-hacking-group-impersonates-afghan-president-to-infiltrate-government-agencies/

الصفحة 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash. .com/photos/JXQ2bizu7kc

الصفحة 39: Surveillance Self-Defense, "No Encryption in Transit," digital image, Electronic Frontier Foundation, January 17, 2019. .https://ssd.eff.org/en/module/what-should-i-know-about-encryption

الصفحة 40: Surveillance Self-Defense, "4.Transport-layer-alternate," digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, "6. End-to-end Alternate", digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/ .files/2018/11/26/6.end-to-end-alternate.png

الصفحة 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https:// .ssd.eff.org/en/module/what-should-i-know-about-encryption

الصفحة 49: African News Agency, "Parliament meeting falls victim to hacking as MPs greeted by pornographic images," 2020, digital image, Reuters, https://www.iol.co.za/news/politics/parliament-meeting-falls-victim-to-hacking-as-mps-greeted-by-pornographic-images-47657120

الصفحة 51: UK Parliament, digital image, Jessica Taylor, https://e3.365dm.com/20/04/768x432/skynews-parliament-house-of- commons_4974709.jpg?20200422191547

الصفحة 52: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/ .server-racks-on-data-center-4508751/

الصفحة 58: PhotoMIX Company, 2016, "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky," digital image, Pexels, .https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/

الصفحة 63: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/ .laptop-screen-vpn-cyber-security-5534556/

الصفحة 65: Surveillance Self-Defense, "Using the Tor Browser," digital image, Electronic Frontier Foundation, April 25, 2020. https:// ssd.eff.org/files/2020/04/25/circumvention-tor_0.png

الصفحة 67: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https:// .unsplash.com/photos/kLmt1mpGJVg

الصفحة 72: Matt Artz, "Two Broken 6-Pane On White Painted Wall Photo," digital image, Unsplash, October 1, 2017, https://unsplash. .com/photos/vT684iB7Ejg


HOUSE
DEMOCRACY
PARTNERSHIP


NDI
NATIONAL
DEMOCRATIC
INSTITUTE


USAID
FROM THE AMERICAN PEOPLE


IRI
INTERNATIONAL
REPUBLICAN
INSTITUTE
Advancing Democracy Worldwide