تدريب الأمن السيبراني الرقمي

UNREPRESENTED
NATIONS & PEOPLES
ORGANIZATION
unpo.org

المعلومات العامة

الوقت:

لقد أعددنا هذه المادة التدريبية لتكتمل في 4 ساعات .

ما تحتاجه:

لكي تستخدم هذا المستند بشكل مناسب، يحتاج المدرب إلى استخدام العرض التقديمي (PowerPoint) الذي تم إنشاؤه لتقديم مزيد من المعلومات العملية وكذلك لمشاركة المعلومات بأكثر الطرق فعالية .

الأنشطة:

في هذه المجموعة أدوات، قمنا بدمج أنشطة قصيرة لتقييم المشاركين في فهمهم وكذلك لتدعيم عملية التعلم.

الهدف :

ستوفر هذه المجموعة من الأدوات للنشطاء المعلومات الضرورية لتصفح الإنترنت بوعي المخاطر السيبرانية المحتملة. ستجد في هذا المستند نصائح وحيل من الخبراء لتطوير استراتيجيتك لمواصلة نشاطك بينما تكون استباقياً في رحلتك الرقمية.

الفئة المستهدفة:

هذه الوحدة مخصصة للمنظمات غير الحكومية أو الأفراد النشطين الذين يرغبون في تعلم الأمان الرقمي لنشاطهم اليومي.

كيفية استخدام هذه المجموعة من الأدوات :

قل أو إسأل	
اعرض	
نشاط	
تعريف	
نصائح عملية	

جدول المحتويات

المعلومات العامة

كيفية استخدام هذه المجموعة من الأدوات

الجزء 1: الترحيب والنظرة العامة

الجزء 2: نظرة على بعض نظريات الأمن الرقمي

الجزء 3: حماية بياناتك على جهاز الكمبيوتر والهاتف

أ) كلمة المرور

ب) مدير كلمات المرور

ج) المصادقة ذات العاملين

الجزء 4: التصفح الآمن على الإنترنت

أ)استخدام ال VPN

ب) متصفح الويب

الجزء 5: حمايتك من التصيد الاحتيالي والبرمجيات الخبيثة

الجزء 6: ضمان أمان اتصالاتك

الجزء 7: أمان الهواتف الذكية

الجزء 8: بعض النصائح الأخيرة والأسئلة الشائعة

الجزء 1: الترحيب ونظرة عامة

الترحيب

رحب بالحضور في التدريب وشكرهم على الحضور.

النشاط التمهيدي

اسأل المشاركين عن:

- أسمائهم
- استخداماتهم اليومية للكمبيوتر
- نوع الهاتف والكمبيوتر الشخصي لديهم (بدون تفاصيل دقيقة)
- إذا سبق لهم أن أخذوا أي مستوى من تدريب الأمن السيبراني

عرض الشريحة 1: فهم أهمية الأمان الرقمي في العصر الحديث ####

قل: "نستخدم الأدوات الرقمية للمزيد من الأنشطة اليومية. لقد شهدنا نموًا هائلًا في استخدام شكل ما من الكمبيوتر (غالبًا الهاتف الذكي) لأشياء مثل التسوق، إخبار ثلاجتنا بالعمل، الحملة من أجل قضية، أداء واجباتنا المدرسية أو العملية - والتكنولوجيا تتطور بشكل متزايد بحيث يمكن القيام بكل ذلك في مجتمع رقمي متصل بالشبكة. أصبحنا نعتمد على الأجهزة الرقمية في حياتنا اليومية لدرجة أننا أصبحنا عرضة للتهديدات الرقمية، بما في ذلك الدعاوى القضائية، الابتزاز، الاختراقات والمزيد

إسأل:

أين يترك هذا النشطاء؟ عرضة للغاية.

هنا بعض حالات الهجمات السيبرانية على النشطاء:

- تقديم حالة المجموعة الإيرانية التي استخدمت تطبيق تدريب رخصة القيادة للوصول إلى النشطاء. أظهر كيف يستخدم القراصنة المعلومات الشخصية لتحقيق أهدافهم بما في ذلك التظاهر بأنهم الموضوع.

- في عام 2020، تم اكتشاف برمجيات خبيثة مخفية في تطبيق رخصة القيادة في السويد. وفقًا لبحث أمير رشيدي، الباحث في مجموعة ميايان، وهي منظمة حقوق إنسان تركز على الأمن الرقمي، يستهدف التطبيق الأقليات العرقية والدينية. عند تثبيت التطبيق يمكنه تسجيل المحادثات، الموقع وسجل التصفح.

قل:

"هذه الدورة ليست فقط لتدريبكم على أن تصبحوا محترفين في الأمن الرقمي، ولكن لضمان أنكم ومجتمعكم من النشطاء أو الأشخاص على علم بالمخاطر السيبرانية المحتملة ويصبحون استباقيين للحذر في نشاطهم اليومي."

الجزء 2: نظرة على بعض نظريات الأمن الرقمي

عرض الشريحة: تعريف الأمن السيبراني

قل: "الأمن السيبراني يتعلق بحماية الأصول الرقمية من التهديدات. يمكن أن تكون الأصول أي شيء تريد حمايته: أجهزتك المادية مثل هاتفك أو ساعتك الذكية التي لا تريد سرقتها في المطار. ولكن في الأغلب الأصول التي تحميها كخبير أمن سيبراني هي البيانات.

اسأل الجمهور: "ما هي المهارات التي تعتقدون أن الشخص في مجال الأمن السيبراني يمتلكها؟

اكتب إجاباتهم على اللوحة" .

اعرض الشريحة:

الواقع هو أن الأمن السيبراني مجال متعدد التخصصات - وعلى عكس جيمس بوند لا يمكنك أن تكون خبيرًا في كل شيء - لأنه نظام واسع ومعقد. ضمن تخصص الأمن السيبراني، يشمل:

أمن البنية التحتية الحيوية

- أمن التطبيقات
- أمن الشبكات
- أمن السحابة
- أمن إنترنت الأشياء (IoT)

وأكثر...

في هذه الجلسة، لن ندخل في كل من هذه التخصصات الفرعية في الأمن السيبراني، ولكن بدلاً من ذلك ستكتسبون فهمًا أفضل للمجال بأكمله مما سيمكنكم من الاتصال بالأشخاص المناسبين لمخاوفكم.

اسأل الجمهور: "ما الفرق بين البيانات والمعلومات؟"

الهاكر غالبًا لا يهتم بمعالجة البيانات. مثل خبير الأمن السيبراني، هو ليس جيمس بوند، لا يقوم بمهام متعددة، وظيفته هي استخراج البيانات ثم إما تسليمها لأسياده لمعالجتها أو بيعها لشخص آخر للمعالجة. لذا عندما أتحدث عن البيانات، فكر فيها كالمعلومات الخام التي لم يتم معالجتها.

بمجرد أن تفهم أهمية حماية الأصول، وخاصة البيانات، دعونا نلقي نظرة على ثلاثية "CIA" للبيانات، وليس خلطها مع وكالة الاستخبارات المركزية.

ثلاثية "CIA" أو ثلاثية السرية، السلامة والتوافر هي نموذج أمني مصمم لتوجيه الأشخاص والسياسات لأمن المعلومات.

عرض الشريحة: السرية، السلامة والتوافر

- **السرية**: الحفاظ على البيانات آمنة من محاولات الوصول العمدية أو غير العمدية لعرضها.
- **السلامة**: التأكد من أن البيانات لم يتم تعديلها عمدًا من قبل أي جهات.
- **التوافر**: التأكد من أن بياناتك متاحة في جميع الأوقات وبسهولة، مع احترام سلامتها أيضًا.

اسأل: "ما الفرق بين الأمان والخصوصية في الأمن الرقمي؟"

الخصوصية تشير إلى قدرتك على التحكم، الوصول وتنظيم معلوماتك الشخصية أو معلومات المنظمة التي تعمل لها.

الأمان يشير إلى النظام بأكمله الذي يحمي البيانات من التهديدات.

يمكن أن تكون في بيئة آمنة للغاية مع خصوصية ضعيفة لأن بياناتك ستظل سليمة ولن تُسرق، ولكن المزود يمكنه النظر إليها في أي وقت.

نشاط: دعونا نقوم بتمرين يشكل جوهر تحليل الأمن السيبراني، وهو تعريف أصولك، أعدائك، الموارد المتاحة لديك، احتمالية الهجوم وقدراتك.

إطار عمل التحليل النهائي:

اسأل المشاركين: "المرور بالأسئلة التالية حول إعدادك الرقمي ومن يجب أن تكون حذرًا منهم:

- **الأصول:** ما الذي يجب عليّ حمايته؟
- **العدو:** من من؟
- **الموارد:** ما الموارد التي يمتلكها عدوي؟
- **الاحتمالية:** ما مدى احتمالية أن يستهدفني عدوي؟
- **القدرة:** إلى أي مدى سأذهب لحماية أصولي؟

الجزء 3: حماية بياناتك على جهاز الكمبيوتر والهاتف

أ) كلمات المرور

كلمة المرور هي كلمة أو عبارة سرية يجب استخدامها للدخول إلى مكان ما.

الشكل الأول لحماية لبياناتك هو كلمة المرور الخاصة بالمستخدم للدخول إلى جهازك. هذا يخلق حتماً تخصصًا كاملاً لكيفية إنشاء طرق معقدة لتشفير وفك تشفير البيانات والرسائل للحفاظ على إخفائها. يعرف هذا التخصص باسم التشفير، وقد وُجد منذ آلاف السنين وهو أساسي لفهم الأمن السيبراني. بينما لن نتعمق في المشكلات الرياضية المعقدة التي يطرحها التشفير، سنسأل أنفسنا ما الذي يجعل كلمة المرور جيدة.

اسأل الجمهور: "ما الذي يجعل كلمة المرور جيدة؟ ما الذي يجعل كلمة المرور سيئة؟"

إجابات محتملة:

- لا شيء يتعلق بحياتك الشخصية (مثل اسم كلبك أو فريقك المفضل)

- لا شيء يتكون من كلمة أو كلمتين فقط، حيث يسهل عادة اختراقها

استخدام أحرف مختلفة مثل الحروف الكبيرة والأرقام والرموز -

- أن تكون غير مفهومة؟

- مخزنة بأمان ومحمية!

- كلمة مرور جيدة قد تحتاج أن تكون قابلة للتذكر

اعرض:

كلمات المرور الجيدة و السيئة

سيئة	جيدة	جيدة جدا
password	Cynthia1970!	j5LyF*H6Ilg
admin	LayC70!	7+n*7XonGS
cynthia	*cynthia70lay	VJ(>0WuVE83V
cynthialay	CynthiaL7019	R.xzVv2m0R0;

ما الذي يجعل كلمة المرور جيدة؟

الطول:

قل: المتغير الأكثر أهمية في تحديد قوة كلمة المرور هو الطول. هذا هو المتغير الأكثر أهمية ويجب توضيحه لأي شخص عند تحديد كلمة مروره. إن وجود جملة ككلمة مرورك التي تكون طويلة أكثر أمانًا من كلمة مرور مكونة من 5 أحرف فقط مليئة بحروف مختلفة. أحد الأسباب هو أن وجود كلمة مرور طويلة يمكن أن يثني الهاكر من خلال "مسرحية الأمان".الآخر هو أنه إذا كان الهاكر يستخدم ذكاءً اصطناعياً لمحاولة "فتح" محرك الأقراص الصلب بالقوة الغاشمة، فمن المحتمل أن يجد من الأسهل كسر كلمة المرور المكونة من 5 أحرف.

.

التعقيد:

قل:غالباً عندما نقوم بإنشاء كلمة مرور، نستخدم كلمات وربما أرقام. ولكن هذه الكلمات أصبحت أكثر سهولة للكسر بفضل البرامج والأدوات الجديدة التي تتحقق من جميع الكلمات المعروفة فوراً. تستخدم هذه البرامج غالباً الذكاء الاصطناعي (AI). لذا من الأفضل دائماً أن تكون هناك سلسلة من الأحرف العشوائية بدلاً من كلمة.

الأحرف الخاصة:

قل: استخدام أحرف خاصة مثل: @ $ % & يجعل كلمة المرور أكثر أماناً وأصعب للتخمين. في الوقت الحاضر، تتطلب بعض المواقع استخدام حرف خاص لتأكيد كلمة مرورك ولكن للأسف ليس كلها.

قل: **أسوأ كلمة مرور** يمكنك استخدامها هي كلمة واحدة. بدءاً من هناك، يمكن للهاكر استخدام ما يسمى بهجوم القاموس لكسر كلمات مرورك. يمكن أن يعمل هجوم القاموس على كلمة. وكذلك تواريخ الميلاد، الأسماء أو حتى "123456789".

المشكلة الأكبر لدينا في العصر الحديث هي أن لدينا العديد من كلمات المرور للعديد من الحسابات المختلفة وأجهزتنا الخاصة. بالإضافة إلى ذلك، إذا كان لديك معلومات حساسة ترغب في تشفير محرك الأقراص الصلب وتخزين السحابة الخاصة بك بكلمة مرور قوية من 36 حرفاً والتي من المحتمل ألا تتذكرها بسهولة. الحل لهذه المشكلة هو استخدام مدير كلمات المرور.

ب) مدير كلمات المرور

اعرض الشريحة: قائمة بمديري كلمات المرور

مدير كلمات المرور يسمح للأفراد والشركات بحفظ وإدارة جميع كلمات المرور الخاصة بهم من مكان آمن واحد. وبالتالي، لن يكون المستخدمون ملزمين بتذكر كلمات مرور متعددة.

يختلف مديرو كلمات المرور في نطاق السعر، ولكن أيضاً حيث يتم تخزين كلمات المرور الخاصة بك بالفعل. على سبيل المثال، يقوم Bitwarden بتخزين كلمات المرور الخاصة بك بأمان نسبي في سحابة على خوادمها ويسمح لعدة أشخاص بالوصول إلى حسابات مختلفة. ولكن قد لا تثق في Bitwarden لأي سبب، وتريد تخزين بياناتك محلياً. KeyPassXC هو مثال جيد على مدير كلمات المرور المخزن محلياً.

وجود عبارة مرور لحفظ الوصول إلى مدير كلمات المرور الخاص بك هو أمر مهم، ولكن دعونا نلقي نظرة على طبقة أخرى من الأمان يمكنك تنفيذها: 2FA او المصادقة ذات العاملين.

ج) المصادقة ذات العاملين

المصادقة ذات العاملين، أو 2FA، هي طبقة إضافية من الحماية تستخدم لضمان أمان الحسابات عبر الإنترنت بخلاف اسم المستخدم وكلمة المرور فقط.

:يمكنك المصادقة عبر طريقتين

- شيء تعرفه (مثل كلمة المرور)

- شيء تملكه أو يكون معك (بيومتري)

الخبر الجيد هو أنه يمكنك ويجب عليك استخدام كلاهما. مع المصادقة ذات العاملين يمكنك التأكد من أنه حتى إذا قام الهاكر بكسر كلمة المرور الخاصة بك، فلديك تلك الطبقة الإضافية من الأمان. يأتي هذا غالباً في شكل:

- تطبيق على هاتفك يعطيك رمز مؤقت للوصول إلى الخدمة (انظر: Google Authenticator)

- مفتاح USB مثل Yubikeys أو Nitrokeys الذي عندما يتم توصيله يمكن أن يمنحك إما الوصول إلى الرموز أعلاه أو من خلال لمسك أو حتى بصمتك يمكن أن يمكنك من الوصول إلى حسابك

المصادقة ذات العاملين أصبحت بسرعة إجراء أساسي في الأمان الرقمي. معظم حسابات الوسائط الاجتماعية تسمح الآن بالمصادقة ذات العاملين ويجب عليك تنفيذ نظام المصادقة ذات العاملين على معظم حسابات البريد الإلكتروني والرسائل والوسائط الاجتماعية الخاصة بك فوراً إذا كنت تعتقد أنه يمكنك الحصول على الوصول.

حماية محركات الأقراص الصلبة وأنظمة التخزين السحابي

بالإضافة إلى تشفير محرك الأقراص الصلب الخاص بك، فكر في استخدام محرك أقراص خارجي لأنظمة السحابة التي تم التحقق منها مثل OneDrive، Google Cloud...

الجزء 4: تصفح الإنترنت بسرية

تم اختراع الإنترنت كوسيلة لتوزيع الاتصال وربط شخص بصفحة ويب شخص آخر. لقد تطورت هذه التقنية لتصبح عملاقًا يربط بين مليارات الأشخاص وأصبحت جزءًا لا يتجزأ من حياتنا اليومية. ومع ذلك، فإن هذا الاتصال يجلب أيضًا مخاطر على الخصوصية والأمان.

معرفة ما يلي ضرورية قبل البدء في التصفح الآمن:

- من هو مزود خدمة الإنترنت الخاص بك؟

-ما هي طبيعة عنوان IP الخاص بك؟ هل هو ثابت أم يتغير؟ عنوان IP الخاص بك يشبه المعرف لشبكة منزلك أو عملك.

- ما هي إعدادات الجدار الناري؟ هذه تنظم علاقة عنوان IP الخاص بك مع جميع عناوين IP الأخرى التي تشكل شبكة الإنترنت العالمية (فكر في الأمر مثل سياسة مراقبة الحدود لمن يدخل ويخرج)

أ) استخدام ال (VPN)

إسأل:

هل يمكن لأي شخص أن يشرح لي ما هو الـ (VPN)

قل:

VPN أو الشبكة الخاصة الافتراضية تربط جهاز الكمبيوتر الخاص بك بخادم آخر ثم تصل إلى الإنترنت من خلاله، مما يخفي نشاطك. يمكنها أيضًا في بعض الأحيان "تغيير" موقعك الجغرافي مما يسمح لك بتجاوز الحجب الجغرافي.

يجب الملاحظة أن الـ VPN لا يحميك من انقطاع الإنترنت، حيث سيكون عنوان IP الخاص بك "نشطًا" خلال انقطاع الإنترنت في محاولة للوصول إلى VPN، وهذا يجعلك عرضة للخطر!

تشمل خدمات الـ VPN الجيدة ك NordVPN أو Mullvad، ولكن بشكل عام تريد أيضًا VPN لا يسجل السجلات حيث أن ذلك ينقل السجلات من مزود خدمة الإنترنت إلى مزود VPN الذي يمكنه بعد ذلك بيع هذه البيانات أو إساءة استخدامها.

ب) متصفحات الويب

اسأل: استخدام متصفحات الويب: ما المتصفحات التي تستخدمونها جميعًا؟

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Brave؟ Vivaldi؟

بشكل عام، من الجيد أن يكون لديك متصفحان، أحدهما يحتوي على حساباتك ومتزامن للاستخدام المهني أو الخاص، والآخر للبحث عن شيء ما. هذا لأن محركات البحث تتبع تاريخ بحثك وتعدل تجربتك في التصفح.

متصفحات Mozilla Firefox وVivaldi تعتبر آمنة بشكل عام. Chrome وMS Edge مصممين من قبل مطوري برمجيات كبار يريدون الحصول على بياناتك واستخدامها لأسباب تجارية. يمكنك الحصول على ما يسمى بـ

unGoogled Chromium الذي هو مفتوح المصدر ويزيل جميع أدوات استخراج البيانات المدمجة من Google.
لدى Brave أيضًا بعض التحليلات المدمجة ولكنه يتمتع بميزات أمان قوية جدًا.

المتصفحات التي تعتبر غير آمنة تمامًا للناشطين في مجال حقوق الإنسان تشمل Opera (حيث تذهب بياناتها مباشرة إلى خادم صيني) وأيضًا المتصفحات المدمجة التي تصممها شركات الإعلانات البرمجية.

الجزء 5: حمايتك من التصيد الاحتيالي والبرامج الضارة

التصيد الاحتيالي: "الممارسة الاحتيالية لإرسال رسائل بريد إلكتروني أو رسائل أخرى تزعم أنها من شركات موثوقة من أجل حمل الأفراد على الكشف عن معلومات شخصية، مثل كلمات المرور وأرقام بطاقات الائتمان".

البرامج الضارة: "هي برامج مصممة خصيصًا لتعطيل أو تدمير أو الوصول غير المصرح به إلى نظام الكمبيوتر".

تكون هجمات التصيد الاحتيالي غالبًا مرتبطة بالبريد الإلكتروني، ولكنها موجودة أيضًا في جميع أشكال الاتصال الأخرى. فكرة التصيد الاحتيالي هي تقديم طُعم من خلال التظاهر بأنك شخص موثوق. قد تكون قد سمعت عن التصيد الاحتيالي عبر البريد الإلكتروني، ولكن قد يكون أيضًا موجودًا عبر تطبيقات المواعدة (مثل الاحتيال عبر الهوية المزيفة) أو المكالمات الهاتفية الاحتيالية.

لنلقي نظرة على بعض الرسائل التي تحتوي على روابط قد تكون تصيدًا احتياليًا:

أظهر شرائح تحتوي على أمثلة وأطلب من الجمهور كيفية تحديدها.

قل: الفكرة هنا هي أنه إذا وجدت رابطًا كهذا، يجب أن تكون قادرًا على إنشاء بيئة حيث النقر عليه وتنزيله سيعزل أي برامج ضارة محتملة عليه. هذا ما يُعرف بالحجر الصحي وهو مفهوم حيوي في الأمن السيبراني. الطريقة القديمة للحجر الصحي كانت ببساطة امتلاك جهاز كمبيوتر غير متصل بالإنترنت والعمل عليه والتأكد من عدم قدرته على الاتصال بالإنترنت. في الوقت الحاضر، يمكنك القيام بالحجر الصحي من خلال إعداد جهاز افتراضي.

الجهاز الافتراضي هو مثل إحدى الدمى الروسية التي تكشف عن نفسها: إنها تخلق نظام تشغيل داخل نظام تشغيل آخر.

أخيرًا، إذا كنت ضعيفًا بشكل خاص وتتلقى باستمرار الكثير من البرامج الضارة المحتملة من بريدك الإلكتروني، أو المواقع التي تزورها، أو خدمة المراسلة الخاصة بك - وتحب الأمن السيبراني حقًا، ألقِ نظرة على أنظمة التشغيل التي تستخدم الحجر الصحي كمبدأ. مثال على ذلك هو QubesOS، الذي يجعلك قادرًا على إنشاء "بيئات" مختلفة غير قادرة على التواصل مع بعضها البعض.

الجزء 6: ضمان أمان اتصالاتك

اسأل: لماذا نظام الرسائل النصية ليس آمنًا في بلد مثل إيران؟

قل: غالبًا ما تركز خدمات المحمول ومزودي خدمات الإنترنت في الأنظمة الديكتاتورية البيانات التي تدخل وتخرج من هاتفك عبر الخدمات التي تستخدمها مثل الرسائل النصية القصيرة (SMS). لهذا السبب يعتبر استخدام التشفير من النهاية إلى النهاية مهمًا جدًا.

التشفير من النهاية إلى النهاية (E2EE) هو طريقة أمان تحافظ على أمان محادثاتك ورسائلك. الفكرة هي أن اثنين أو أكثر من الأشخاص لديهم مفتاح عام ومفتاح خاص.

المفتاح العام متاح لأي شخص يطلبه والمفتاح الخاص بك يفك تشفير المفاتيح العامة الأخرى. للمساعدة في فهم التشفير من النهاية إلى النهاية، هنا فيديو تعليمي مفيد

<اعرض الفيديو>

قل: الآن، أفترض أن جميعكم يستخدم البريد الإلكتروني وهو تكنولوجيا قديمة مقارنة بـ WhatsApp وInstagram وSnapchat والتطبيقات الأخرى الأكثر أمانًا التي نظرنا إليها. لهذا من الضروري أن تفهم أي مزود بريد إلكتروني تستخدم، وما هي أنواع التهديدات الموجودة وأين تبحث عن موارد إضافية.

تستخدم حسابات البريد الإلكتروني نطاقات مثل gmail.com@ للإشارة إلى الخوادم التي تستخدمها لإرسال رسالة عبر الإنترنت. غالبًا ما يستخدم بريد العمل الخاص بك خوادم العمل الخاصة بك ويحتوي على organizationname.com@. تدير معظم حسابات البريد الإلكتروني مزود خدمة البريد الإلكتروني مثل Google أو Microsoft.

إحدى التهديدات الرئيسية بالإضافة إلى التصيد الاحتيالي هي انتحال النطاق.

انتحال النطاق هو محاولة استخدام نطاقك وهويتك كمنظمة أو حتى فرد من أجل اختراق بريدك الإلكتروني أو ببساطة للحصول على معلومات أثناء التظاهر بأنه أنت. لمحاربة انتحال النطاق، يجب الإبلاغ عنه.

يعتبر التشفير من النهاية إلى النهاية عبر البريد الإلكتروني أداة مفيدة أيضًا عند تبادل المعلومات أو الملفات الحساسة. لا تأتي مزودات البريد الإلكتروني مثل Gmail وOutlook مع تشفير من النهاية إلى النهاية بشكل افتراضي. لكن بالنسبة

لـ Gmail، هناك إضافة يمكنك تثبيتها تسمى Mailvelope التي يمكنها التشفير. مقدمو خدمات البريد الإلكتروني الذين يستخدمون التشفير من النهاية إلى النهاية وحتى لديهم أدوات تسمح فقط للمستلم بفك تشفير الرسالة حتى إذا لم يكن لديه مفتاحك العام، تشمل Protonmail وTutanota. العيب هو أن هذه غالبًا ما تواجه مشكلات توافق مع عملاء البريد وتكون بيئات مغلقة المصدر مع ميزات ناشئة جدًا مقارنة بـ Gmail وOutlook، لكنها بالتأكيد تستحق النظر فيها للاستخدام المتخصص.

الجزء 7: أمان الهواتف الذكية

اطلب استطلاعًا سريعًا لمعرفة من يستخدم أي نظام تشغيل هاتف (iOS مقابل Android).

قل: لقد تحدثنا باختصار عن تطبيقات المراسلة على هاتفك، ولكن ظهور الهواتف الذكية أنتج تحديات أخرى متعددة لخبراء الأمن السيبراني. أحد هذه التحديات هو أن حياتك كلها تقريبًا يمكن أن تكون الآن على هاتفك، وكما ذكرنا في بداية الفصل.

اعرض الشريحة

قل: فضيحة Pegasus أظهرت أن حتى الحكومات الديمقراطية كانت مستعدة للتجسس على المواطنين وقامت بذلك باستخدام أساليب التصيد الاحتيالي التي رأيناها أعلاه (عبر رسالة نصية). قد يكون الكثير منكم قد اعتقد أن وكالة الأمن القومي (NSA) وGCHQ والشركات الأخرى المماثلة للتجسس على الاتصالات كانت تتجسس عليكم بالفعل. لكن الحقيقة هي أنه قبل Pegasus، كانت هذه المجموعات تستطيع فقط قراءة اتصالاتك بينك وبين طرف ثالث. عالم ما بعد Pegasus مخيف لأن هاتفك كله يمكن الآن مراقبته وبالتالي يمكن لأي هاكر جيد استخدام أداة للحصول على معلومات كافية عنك لجعلك عرضة للتهديدات.

إطلاق البرامج الضارة مثل Pegasus يوفر للهاكر الوصول إلى هاتفك بالكامل، مما يجعله غير قانوني بشكل خاص. ولكن الأهم من ذلك ما يظهره هذا هو أن هواتفنا يمكن تحويلها بسهولة إلى جهاز مراقبة محمول. ويمكنك إضافة حقيقة أن Google وApple وخدمات الهواتف المحمولة الأخرى تجمع البيانات منك لأسباب تجارية يمكن أن تستخدم ضدك إذا سقطت هذه البيانات في الأيدي الخطأ.

لحسن الحظ، هناك سلسلة من البدائل لأولئك الذين لا يريدون أن يكونوا عرضة للخطر عند استخدام الهاتف الذكي. Graphene OS و Lineage OS هي أمثلة على ما نسميه تفرعات كود Android التي أزالت جميع الخدمات المتعلقة بـ Google. يمكنك أيضًا النظر إلى أنظمة تشغيل الهواتف التي يمكنها استخدام الحجر الصحي بفعالية للتأكد من أن أي تطبيقات تثبتها لا تتجسس على الأخرى.

لكن احذر، بشكل عام، هاتفك هو الأداة المثالية للتجسس عليك. من مشغلات الأجهزة إلى تطبيقات الألعاب التي تحملها، معظم التقنية على هاتفك مغلقة المصدر: لا تعرف ما الكود الذي وضعه المطور على هاتفك. مع تطورنا إلى بيئة رقمية مهيمنة على الهواتف الذكية والأجهزة اللوحية، أفضل رهان لك كناشط حقوق الإنسان هو استخدام هذه الأدوات بشكل مقتصد أو مع برامج متخصصة جدًا.

الجزء 8: بعض النصائح النهائية والأسئلة الشائعة

قل: دعونا ننتقل إلى بعض الأسئلة الشائعة التي ربما يمكن لبعضكم مساعدتي في الإجابة عليها، ثم نقوم بورشة عمل صغيرة حيث تسألوني.

اسأل: هل يجب أن أثبت برنامج مكافحة الفيروسات؟ إذا كان الأمر كذلك، أيهما؟

قل: برامج مكافحة الفيروسات غالبًا ما تكون مدمجة في أنظمة التشغيل الآن. لم تعد الأيام التي كانت تعتمد فيها Windows على مزودي برامج مكافحة الفيروسات من جهات خارجية للقيام بالكثير من العمل ضد البرامج الضارة. تميل Apple وLinux إلى أن تكون قوية ضد البرامج الضارة، الأخيرة بسبب فلسفة المصدر المفتوح. المصدر المفتوح، تذكر، يعني أن الكود مفتوح للجميع وعادة ما يتم تدقيقه من قبل مبرمجين آخرين للتحقق من سلامته.

ومع ذلك، إذا رأيت برنامج مكافحة الفيروسات مثبتًا أو أردت شراء واحد، فإن برامج مكافحة الفيروسات هي عادةً أدوات تحليلية للبيانات تراقب مكان استخدام جهاز الكمبيوتر الخاص بك للموارد وكيفية استخدامها، وما الملفات التي تبدو تالفة أو مشبوهة، ويمكنها أيضًا مساعدتك في تعزيز جدار الحماية الخاص بك - الجدار الذي يمنع المهاجمين السيئين من الدخول إلى شبكتك/عنوان IP الخاص بك. برنامج مكافحة الفيروسات الجيد هو Bitdefender، ولكن إذا تعلمت كيفية العزل الصحي واستخدام سياسات مكافحة الفيروسات العامة، فلن تحتاج إليه.

اسأل: هل Apple حقًا أكثر أمانًا من Windows؟

قل: نعم، لكنها لا تزال عرضة للثغرات. اختيار نظام التشغيل المناسب لنوع العمل الذي تقوم به هو أيضًا أمر أساسي. هناك العديد من أنظمة التشغيل المجانية المستندة إلى Linux التي تعتبر أكثر أمانًا وأمانًا مقارنة بعروض Apple و Microsoft، لكنها قد تتطلب المزيد من الإتقان الفني. ولكن إذا كنت ستدخل في مجال الأمن السيبراني، فتعلم كيفية عمل أنظمة التشغيل Linux، والإختراق الأخلاقي من خلال Kali Linux، والاختلافات الأساسية في أنظمة التشغيل لكل من الخوادم والاستخدام الشخصي هو أمر أساسي.

اسأل: من أين أبدأ إذا أردت الدخول أكثر في مجال الأمن السيبراني؟

قل: كما ذكرت سابقًا، هناك العديد من المجالات التي يمكنك الدخول إليها في مجال الأمن السيبراني. البداية الجيدة هي تعلم أساسيات البرمجة للأجهزة والبرمجيات بحيث تكون على الأقل ملما بالعلاقة بين الاثنين، ثم تعلم كيفية إعداد خادم خاص بك.

اسأل: كيف أعرف إذا تم اختراق جهاز الكمبيوتر أو الهاتف الخاص بي؟

قل: كما ذكرت سابقًا، في كثير من الأحيان لن تدرك أنك تعرضت للاختراق حتى فوات الأوان حيث يعمل المخترقون عادةً في الخلفية لنظام التشغيل الخاص بك (الوصول إلى الملفات دون أن تلاحظ).

نصائح:

- بالنسبة لجهاز الكمبيوتر، يمكنك إجراء فحوصات على الملفات المشبوهة باستخدام المواقع التالية:
- بالنسبة للهواتف، هناك أدوات رائعة الآن لمعرفة ما إذا كنت قد تأثرت ببرامج التجسس أو البرامج الضارة:
- بالنسبة للحسابات المحددة، يمكنك التحقق مما إذا كنت قد تعرضت لتسريب بيانات أو اختراق من خلال هذا الموقع:
- بالنسبة للبريد الإلكتروني أو موقعك الشخصي على وجه الخصوص، يمكنك التحقق مما إذا تم انتحال نطاقك من خلال النظر إلى النطاق:

اسأل: ما هي بعض الموارد إذا كنت بحاجة إلى مساعدة كناشط حقوق الإنسان؟

- AccessNow
- Amnesty Tech
- Center for Digital Resilience
- UNPO

ثم قم بقيادة ورشة عمل مع حالات فردية أكثر استنادًا إلى الجمهور والأجهزة التي بحوزتهم.