INNOVATION FOR CHANGE

MIDDLE EAST & NORTH AFRICA

دليل في الأمن الرقمي

تم تجميع وتصميم هذا الدليل من قبل فرع الشرق الأوسط وشمال إفريقيا لشبكة الابتكار للتغيير.

نظرة عامة على المشروع

مشروع سلامة المعلومات وتعزيز قدراتها (ISC) يوفر مساعدةً متقدمةً ومستدامة في مجال أمن المعلومات وقدراتها إلى منظمات المجتمع المدني والناشطين في مجال حقوق الإنسان والوسائط الإعلامية المستقلة في البلدان التي تكون فيها حرية التعبير وإعداد التقارير الصحفية والاتصالات عبر الإنترنت والدعوة عنصرًا حاسمًا في التحرر الاجتماعي والتنمية، ولكن ينطوي عليه مخاطر محتملة على السلامة الشخصية. يقدم مشروع معلومات السلامة وتعزيز القدرات خدمات التوجيه والدعم لمساعدة أصحاب المصلحة في تأمين اتصالاتهم عبر الإنترنت واتصالاتهم المتنقلة، بحيث يمكن استخدام هذه المنصات بأمان لدعم تنمية المجتمع المدني وحماية حقوق الإنسان. وقد يشمل ذلك: المساعدة في الهجمات أو الإغلاق القسري لمواقع الويب ورصد حركة البريد الإلكتروني ومحتواه وإصابة الحاسوب بالبرامج الضارة والفيروسات وتسجيل الرسائل النصية القصيرة/الرسائل النصية ومحادثات الهواتف النقالة.

مقدمة عن مجموعة الأدوات

مجموعة أدوات مشروع سلامة المعلومات وتعزيز قدراتها هي عبارة عن مجموعة من مفاهيم الإنترنت وأفضل الممارسات والأدوات والمبادئ التوجيهية التي تم تجميعها في مكان واحد. تعمل مجموعة الأدوات كمصدر للمستخدمين الذين يتطلعون إلى فهم أساسيات عمل العالم الرقمي وحماية خصوصياتهم ونزاهة البيانات على الإنترنت.

الوعي الأمني والمفاهيم الأساسية

نمذجة الأخطار

لا يقتصر الحفاظ على أمنك في الإنترنت على حل واحد. فالأمن الرقمي ليس عن الأدوات التي يجب استخدامها، بل عن فهم الأخطار التي تواجهك، وكيفية التصدي لهذه الأخطار. لتصبح أكثر أمنًا، يجب عليك تحديد ما تحتاج إلى حمايته ومِنْ من.

اقرأ المزيد:

https://ssd.eff.org/en/module/introduction-threat-modeling

مصفوفة المخاطر: الاحتمال والتأثير

قد يحدث أن تجدوا أخطارًا عديدة يتعرض لها عملكم، وقد يكون من الصعب الحصول على منظور حول كيفية البدء في معالجتها. في هذه الحالات، من المفيد التفكير في مختلف التهديدات من حيث احتمال حدوثها وتأثيرها على عملكم إن حدث هجوم بعينه.

قد يساعدك رسمها على "مصفوفة مخاطر" كالمصفوفة التالية:

الاحتمال				
مرتفع جدًا				
مرتفع				
متوسط				
منخفض				
التأثير	منخفض	متوسط	مرتفع	كارثي

سواء أكانت هناك احتمالية حدوث هجوم معين منخفضة أو متوسطة أو مرتفعة أو مرتفعة للغاية فهي مسألة ذاتية الحكم. ومن المأمون نسبيًا القول إنه إذا حدث نوع معين من الهجوم على زملاء أو أصدقاء أو غيرهم من المدافعين عن حقوق الإنسان في مجالكم، فإن احتمال حدوثه في مجالكم هو على الأقل متوسط أو مرتفع أو مرتفع للغاية.

يكون تقييم التأثير ذاتيًا على نحو مماثل، ولا يمكن الحكم عليه إلا شخصيًا. ومع ذلك، يمكن القول بأن أي نوع من الهجمات التي، إذا نفذت، ومنعتك أنت أو مؤسستك كليًا من تنفيذ عملك، يكون تأثيرها عالٍ أو كارثي، على سبيل المثال:

الاحتمال				
مرتفع جدًا			مصادرة المواد	
مرتفع		السطو		
متوسط			الإيقاع فى الشّرك والاعتداء	للسجن
منخفض				
التأثير	منخفض	متوسط	مرتفع	كارثي

وبمجرد أن تضع أولوية بالمخاطر على نفسك وعملك، يمكنك البدء في اتخاذ إجراءات لتقليلها ببناء القدرات ذات الصلة ودمجها في خطة أمنية.

مصطلحات الإنترنت

أساسيات عناوين بروتوكول الإنترنت(IP)وكيفية عملالإنترنت.

1. عنوان برتوكول الانترنت (IP)

عنوان بروتوكول الإنترنت هو تسمية رقمية مخصصة لكل جهاز (على سبيل المثال، الكمبيوتر والطابعة) مشاركة في شبكة حاسوب تستخدم بروتوكول الإنترنت للاتصال. تتوفر المزيد من المعلومات في هذا الفيديو : https://www.youtube.com/watch?v=7_-qWlvQQtY

2. نظام أسماء النطاق (DNS)

نظام اسم النطاق، المعروف أكثر باسم "DNS"، هو نظام الشبكات المعمول به والذي يسمح لنا بحل الأسمار صديقة الإنسان إلى عناوين بروتوكول إنترنت فريدة من نوعها.

الخصوصية على الإنترنت

خصوصية الإنترنت هي الخصوصية ومستوى أمان البيانات الشخصية المنشورة عبر الإنترنت. وهو مصطلح واسع يشير إلى مجموعة متنوعة من العوامل والتقنيات والوسائل التكنولوجية المستخدمة لحماية البيانات الحساسة والخاصة والاتصالات والتفضيلات.

وتضم الموارد معلومات أخرى عن هذا المفهوم منها:

https://www.youtube.com/watch?v=85mu9PLWCuI
https://www.youtube.com/watch?v=kp2dAgpvhW8
https://www.youtube.com/watch?v=-e98hxHZiTg

ما المقصود بالحوسبة السحابية؟

الحوسبة السحابية هي نوع من الحوسبة قائمة على الإنترنت وتوفر موارد معالجة الحاسوب والبيانات المشتركة لأجهزة الحاسوب وغيرها من الأجهزة عند الطلب.

موارد الحوسبة السحابية تشمل:

https://www.youtube.com/watch?v=uYGQcmZUTaw
https://www.youtube.com/watch?v=xLAN1EjQnhU

الخصوصية وعدم الكشف عن الهوية

من المهم أن يفهم المستخدمون الفرق بين الخصوصية وعدم الكشف عن الهوية في العالم الرقمي. توضح المقالة التالية الفرق بين المفهومين وتأثيرهما على المستخدمين:

https://invisibler.com/privacy-and-anonymity/

الهواتف النقالة

كيف تعمل الهواتف النقالة؟

في أبسط شكل، الهاتف النقال هو في الأساس لاسلكي ثنائي الاتجاه، يتكوّن من جهاز إرسال لاسلكي وجهاز استقبال لاسلكي. عند الدردشة مع صديقك على هاتفك النقال، يحوّل هاتفك صوتك إلى إشارة كهربائية، يتم إرسالها بعد ذلك عبر موجات اللاسلكي إلى أقرب برج خلوي. ثم تقوم شبكة الأبراج النقالة بتبديل موجة اللاسلكي إلى الهاتف النقال لصديقك، الذي يحولها إلى إشارة كهربائية، ثم يعود إلى الصوت مرة أخرى. في الشكل الأساسي، يعمل الهاتف النقال تمامًا مثل جهاز الاتصال اللاسلكي.

بالإضافة إلى الوظيفة الأساسية للمكالمات الصوتية، تأتي معظم الهواتف النقالة الحديثة بوظائف إضافية مثل: تصفح الإنترنت والتقاط الصور ولعب الألعاب وإرسال الرسائل النصية وتشغيل الموسيقى. تستطيع الهواتف الذكية الأكثر تطورًا تأدية وظائف مماثلة لجهاز كمبيوتر محمول.

التحويل الثلاثي

هو طريقة تحديد الموقع الفعلي للهاتف النقال ضمن مجموعة من الأبراج المتعددة للهواتف النقالة. تلعب العناصر المختلفة أدوارًا في تمكين التحويل الثلاثي، مثل رقم وحدة تعريف المشترك الفريد (SIM, أو (معرف بطاقة الدائرة المتكاملة) ICCID، وقوة الإشارة بين البرج والهاتف النقال، والأبراج التي يتصل بها الهاتف النقال. من خلال توحيد هذه المعلومات، يمكن لمشغل الهاتف المحمول تحديد موقع الهاتف النقال.

الرسائل النصية القصيرة كنص عادي

بمجرد إرسالها، تترك الرسالة النصية القصيرة هاتف المرسِل وتصل إلى المشغّل من خلال الأبراج الخلوية. يقدر مشغلي شبكات الهواتف النقالة النظر في قواعد بياناتها؛ لأجل العثور على رقم هاتف مستلم الرسالة النصية القصيرة. بالاعتماد على رقم الهاتف، يستطيع المشغل تحديد موقع المستلم، وبعد التحقق من أن المستلم متصل بالشبكة، تقوم الشبكة بدفع رسالة نصية قصيرة كنص عادي. طوال العملية برمتها (إرسال - تسليم - تلقي)، تبقى الرسالة النصية القصيرة في شكل نص عادي كي يستطيع المشغل قراءة الرسالة والوصول إليها حتى لو حذف المرسل والمتلقي الرسالة من هواتفهم.

أساسيات أمن الهاتف النقال

إذا نجح شخص ما في الوصول إلى هاتفك، فيمكنه إزالة بطاقة الذاكرة واستخدام قارئ البطاقة حتى يقرأ البيانات الموجودة على الجهاز. قد يكون الشخص الذي يصل إلى بياناتك الخاصة متطفلاً أو متصفحًا عارضًا، كالشخص في متجر إصلاح الهاتف. وقد أدت حالات الوصول غير المصرّح به في الأجهزة النقالة إلى عمل دعاية للبيانات الخاصة، مثل الصور المنتشرة على وسائل التواصل الاجتماعي، وخصوصًا عندما يكون صاحب الهاتف من الشخصيات المشهورة.

لحماية محتوى هاتفك الذي لا تريد عرضه، يمكنك اتخاذ الخطوات التالية:

تعيين كلمة مرور:

- دون كلمة مرور، لا يمكنك تمكين التشفير.
- إرشادات تعيين كلمة مرور على أنظمة الأندرويد: http://www.howtogeek.com/253101/how-to-secure-your-android-phone-with-a-pin-password-or-pattern/
- تعليمات لتعيين كلمة المرور على أجهزة الآيفون: https://support.apple.com/en-us/HT204060

تشغيل التشفير:

- أجهزة الآيفون: يتوفر تشفير الأجهزة على أجهزة آيفون s4 والإصدارات الأحدث فقط. يجب تحديث الجهاز إلى نظام iOS8 - إنها دائمًا طريقة جيدة للحفاظ على بقاء هاتفك محدّثًا. يتم تشغيل التشفير تلقائيًا عند تعيين رمز مرور iOS.
- أنظمة الأندرويد: يختلف تحديد دقة المواقع وتوافر الإعدادات مع اختلاف الجهاز، ولكن يمكن العثور على الإرشادات الحالية لجهاز Nexus هنا:

https://support.google.com/nexus/answer/2844831?hl=en

توصيات بالمتصفح

موزيلا فايرفوكس

فايرفوكس عبارة عن متصفح سطح مكتب مجاني وسريع, ومفتوح المصدر. لا تنسَ تثبيت بعض ملحقات المتصفح كي تستخدمها مع متصفح فايرفوكس.

إرشادات حول كيفية تنظيف سجل المتصفح:

https://support.mozilla.org/en-US/kb/delete-browsing-search-download-history-firefox

حزمة المتصفح تور (Tor)

هذا عبارة عن برنامج مجاني ومفتوح المصدر وشبكة مفتوحة تساعدك في الحماية من تحليل حركة مرور الويب. صُمم تور لزيادة سرية النشاط على الإنترنت، وإخفاء هوية المستخدم، وتجاوز مرشحات الإنترنت.

إليك مجموعة مهمة من التوصيات والتحذيرات التي ينبغي أن تقرأها قبل استخدام متصفح تور:

https://en.wikipedia.org/wiki/Web_analytics

أساسيات البريد الإلكتروني

التصيد الاحتيالي (Phishing)

التصيد الاحتيالي هو إصدار إلكتروني من الهندسة الاجتماعية، وجد لنفسه سوقًا ضخمًا في عالمنا المهووس بالبريد الإلكتروني. يرسل المتطفلون رسائل بريد إلكتروني احتيالية إلى عشرات الآلاف من الأشخاص، على أمل إجراء عدد قليل من النقر فوق الروابط أو المستندات أو الصور المرفقة، بهدف الحصول على متلقين يقدمون بمحض إرادتهم معلومات قيمة مثل: أرقام الضمان الاجتماعي وكلمات المرور والأرقام المصرفية وأرقام التعريف الشخصي وأرقام بطاقات الائتمان.

ويتحقق ذلك باتباع أساليب قليلة مختلفة. في بعض الأحيان، يخدع مجرمو الفضاء الإلكتروني مستلمي البريد الإلكتروني بفتح مرفق بريد إلكتروني يحمل برامج ضارة لنظامهم. وفي أحيان أخرى، يخدعون المستلمين بتقديم معلومات شخصية حساسة مباشرةً عبر نماذج الويب. وفي كلتا الحالتين، يمكن أن تؤدي هذه الأخطاء الصغيرة على ما يبدو إلى تموجات خطيرة عبر مؤسستك، مما يعرّض أمن الشركات أو الأمان الشخصي إلى الخطر. اقرأ المزيد من المعلومات عن أنواع التصيد الاحتيالي:

https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks

المصادقة ثنائية العوامل (Two factor authentication)

المصادقة ثنائية العوامل (FA2) هي عبارة عن طبقة إضافية من الأمن لحماية حسابك على الإنترنت، المعروفة أيضًا باسم التحقق بخطوتين أو مصادقة متعددة العوامل. FA2 عادةً ما يتطلب مزيج من عنصرين كالتالي:

- شيء تعرفه (كلمة مرور)
- شيء لديك (رسالة نصية قصيرة أو YubiKey أو رمز مميز للأجهزة)
- شيء يعبّر عنك (بيولوجي مثل بصمات الأصابع)

يساعد استخدام FA2 على تقليل عدد حالات سرقة الهوية على شبكة الإنترنت، وكذلك التصيد الاحتيالي. ويمكن الاطلاع على برامج تعليمية تشرح كيفية تشغيل المصادقة ثنائية العوامل لمعظم مواقع الويب الرئيسية:

https://www.turnon2fa.com/tutorials/

وسائل التواصل الاجتماعي

الفيسبوك (Facebook)

أصبح الفيسبوك أول شبكة اجتماعية يستخدمها الصحفيون والناشطون والسياسيون من جميع أنحاء العالم للتواصل وتبادل الأخبار، مما يجعلها، بطبيعة الحال هدفًا لمجموعة متنوعة من الهجمات عبر الإنترنت.

يدرك الفيسبوك التهديدات التي تواجه مستخدميه ويقدم بعض تقنيات مفيدة جدًا يستخدمها الأشخاص لزيادة أمان ملفاتهم الشخصية وصفحاتهم.

إعدادات الخصوصية:

قد تكون إعدادات خصوصية الفيسبوك مفيدة للتحكم في مَن يستطيع أن يرى مشاركاتك وصورك والأشخاص الذين يمكنهم وضع علامة لك في المشاركات والصور، وإعدادات كثيرة أخرى للتحكم في مَن لديه حق الوصول إلى المحتوى.
لمزيد من المعلومات، يُرجى زيارة:

https://www.facebook.com/help/325807937506242/
https://www.facebook.com/privacy/

الموافقة على تسجيل الدخول إلى الفيسبوك:

- من خلال ميزة "الموافقات على تسجيل الدخول"، يمكن لمستخدمي الفيسبوك تمكين FA2. وتضيف الموافقات على تسجيل الدخول طبقة ثانية من الأمن لعملية تسجيل الدخول من خلال مطالبتك بإدخال رمز وكلمة مرورك في كل مرة تحاول فيها الدخول إلى ملفك الشخصي من جهاز جديد. لتفعيل وظيفة ما، تحتاج إلى إضافة رقم هاتفك، كما يتم إرسال رموز الموافقة على تسجيل الدخول عبر رسالة نصية إلى هاتفك.
- لمزيد من المعلومات، يُرجى زيارة:
https://www.facebook.com/help/14823396524782

تويتر (Twitter)

تتوفر إرشادات عن كيفية تكوين إعداد الخصوصية والأمان على تويتر من مقاطع الفيديو هذه:

https://www.youtube.com/watch?v=gBn9Jm49wSY
https://www.youtube.com/watch?v=vmjHJSeyuwQ

الميتاداتا Metadata

الميتاداتا هي اسم لمجموعة معلومات تصف محتوى عنصر معين. على سبيل المثال، قد تتضمن صورة ما بيانات تعريف توضّح مدى كِبَر حجم الصورة، وعمق اللون، ودقة الصورة، ومكان إنشاء الصورة وزمانه، ومعلومات أخرى. قد تحتوي بيانات تعريف البريد الإلكتروني على معلومات مثل: عنوان بروتوكول إنترنت للمرسل أو الخوادم أثناء النقل أو عناوين البريد الإلكتروني للمرسل والمستلمين أو الطوابع الزمنية أو غيرها من المعلومات حول عميل البريد المستخدم ومعرّف الرسالة ونوع المحتوى. لمزيد من المعلومات عن سبب أهمية بيانات التعريف وما تكشف عنه، يُرجى مشاهدة هذا الفيديو:

https://www.youtube.com/watch?v=xP_e56DsymA

نصائح لتصفح آمن على الإنترنت

- استخدم برنامجًا معروفًا لمكافحة الفيروسات (استخدم برنامج واحد فقط). أيهما أفضل؟ تحقّق من اختبار سمعي وبصري (AV-Test) للحصول على أحدث التقييمات.
- لا تفتح بريدًا إلكترونيًا من جهات اتصال غير مألوفة
- لا تنقر فوق الروابط المرسلة من "الأصدقاء" عبر مواقع التواصل الاجتماعي المتصلة بالإنترنت وسكايب
- لا تفتح مرفقات غير معروفة
- لا تسجل الدخول مطلقًا باستخدام الروابط المرسلة بالبريد الإلكتروني
- استخدم البرامج المرخصة قانونًا فقط
- تأكد من تحديث جميع البرامج بانتظام
- احتفظ بنسخة احتياطية من بياناتك بانتظام
- تحقّق من المثبّت عند استخدام برنامج مفتوح المصدر
- احذف ملفاتك بأمان
- امسح قرصك الصلب بأمان
- استخدم التخزين السحابي المشفّر
- قم بتشفير القرص الصلب / محرك الأقراص المحمول الخاص بك
- تأكّد من أن حاسوبك محمي بكلمة مرور ومؤمّن دائمًا عندما تكون بعيدًا عنه.
- احذر من المتطفلين المرئيين والمحتالين
- استخدم أدوات إدارة كلمة المرور
- استخدم كلمات مرور طويلة وقوية لأجهزة الحاسوب وأجهزة الحاسوب اللوحية والهواتف النقالة

- قم بتشفير محتوى بريدك الإلكتروني
- اهتم بسطر الموضوع وبيانات التعريف ميتاداتا لبريدك الإلكتروني
- استخدم شيكة افتراضية خاصة على شبكة الواي فاي العامة غير المحمية
- استخدم FA2 (المصادقة ثنائية العوامل)
- قم بتغطية كاميرات الويب الخاصة بك واستخدم شاشة الخصوصية
- لا تترك الحاسوب أو الهاتف دون إشراف في مكان غير مؤمّن
- أغلق الجهاز غلقًا تامًا إذا أردت ترك الحاسوب غير مراقبٍ
- انسخ البيانات احتياطيًا وأعِد تهيئة / أعِد تثبيت الحاسوب أو الهاتف إذا وجدته لوقت كبير دون مراقبة.

برامج مكافحة الفيروسات وأمن الإنترنت

إيه في جي (AVG): برنامج مجاني يضمن السلامة من الفيروسات ومن برامج التجسس لنظام التشغيل ويندوز. يأتي AVG بإصدارات متعددة مثل: ترخيص مكافحة الفيروسات المجاني التقييدي وترخيص مكافحة الفيروسات المتقدم المدفوع وترخيص أمان الإنترنت المدفوع.

أفيرا: (Avira) إصدار "مجاني للاستخدام الشخصي" من أفيرا بريميوم (Avira Premium)؛ والمعروف بنتيجته الجيدة في حجب البرامج الضارة ومعدل الكشف عن الفيروسات

سيمانتك اند بوينت (Symantec Endpoin) : برامج مكافحة الفيروسات التجارية ومنتجات جدار الحماية الشخصية من سيمانتك (Symantec) موجهة لتوفير أمن بيئات الشركات المدارة مركزيًا بالخوادم ومحطات العمل. ويتميز بجدار حماية وحماية استباقية ومنع التسلل.

مكافحة البرامج الضارة

برنامج مكافحة البرامج الضارة (مالوير بايتس) Malwarebytes: هذا النوع من الأدوات يكتشف البرامج الضارة الموجودة على أجهزة الكمبيوتر المصابة ويزيلها وأيضًا يعمل باستمرار في الخلفية لوقف الإصابة قبل حدوثها، حيث يُجري مسحًا تلقائيًا ويوقف محاولات الهجمات.

ملحقات المتصفح

- **HTTPS Everywhere** في متصفحي (كروم وفايرفوكس)- ملحق لحماية الاتصالات من خلال تمكين تشفير HTTPS تلقائيًا على مواقع الويب المدعومة به.

- أدبلوك بلس(**AdBlock Plus**) في متصفحي (كروم وفايرفوكس)- ملحق مفتوح المصدر ومجاني يمنع جميع الإعلانات المزعجة والعناصر المنبثقة والتعقب والبرامج الضارة.

- برايفسي بادجر (**Privacy Badger**) في متصفحي (كروم وفايرفوكس)- ملحق يمنع الإعلانات والمتعقبين الخارجيين من تعقب المستخدم بشكل سري.

أدوات التحايل وعدم الكشف عن الهوية

سايفون (Psiphon) أداة تحايل مجانية مفتوحة المصدر ومتعددة المنصات تستخدم تقنية وكيل SSH VPN وHTTP لتوفر لك وصولاً إلى محتوى إنترنت لا يخضع للرقابة.

تور (Tor): برنامج مجاني مفتوح المصدر وشبكة مفتوحة تساعدك في الحماية من تحليل حركة مرور الويب. تم تصميم تور لزيادة سرية النشاط عبر الإنترنت وإخفاء هوية المستخدم وتجاوز مرشحات الإنترنت.

لانترن (Lantern) أداة تحايل مجانية مفتوحة المصدر بين النظراء للوصول إلى شبكة الإنترنت المؤدية إلى

تشفير البريد الإلكتروني

ميل فلوبي(Mailvelope) : عبارة عن ملحق مخصص لمتصفح يسمح بتبادل رسائل البريد الإلكتروني المشفرة تبعًا لمعيار التشفير POpenPG. يتوفر فيلمتصفح كروم و فايرفوكس المتطور. يمكن العثور على أحدث حزم التثبيت هنا.

Thunderbird + Enigmail + GnuPG: موزيلا ثَندَربِرْد (Thunderbird Mozilla) هو برنامج عميل لإدارة البريد الإلكتروني ومفتوح المصدر لتلقي رسائل البريد الإلكتروني وإرسالها وتخزينها. عند استخدام ثَندَربِرْد من خلال Enigmail وGnuPG، سوف تتمكّن من تشفير رسائل بريدك الإلكتروني والتوقيع عليها رقميًا. Enigmail هو ملحق أمن لمتصفحي موزيلا ثَندَربِرْد

(Mozilla Thunderbird) وسي مونكي (Seamonkey)، حيث يمكّنك من كتابة رسائل البريد الإلكتروني موقّعة و/أو مشفرة واستلامها من خلال معيار OpenPGP. ويستخدم حماية الخصوصية المتاحة مجانًا GNUوالمختصر(GnuPG) للقيام بمعظم أعماله.

- GPG4Win: GPG4Win + **GPG4Win Microsoft Outlook** هو بريد إلكتروني مفتوح المصدر وحل لتشفير ملفات مستخدمي الويندوز. يتيح للمستخدمين إرسال البريد الإلكتروني والملفات على الإنترنت بمساعدة التشفير والتوقيعات الرقمية. يتوفر Gpg4win الآن في برنامج ميكروسوفت أوتلوك 2016/2013، ويدعم إصدارات 64 بت من ميكروسوفت ويندوز.

التشفير الكامل للقرص

- بت لوكر (Bitlocker): ميزة التشفير الكامل للقرص والمدمجة في ميكروسوفت ويندوز، وهي موجودة في أنظمة التشغيل ويندوز 7 ألتميت أو إنتربرايس (Windows 7 Ultimate or Enterprise) أو ويندوز 8 برو أو إنتربرايس (Windows 8 Pro or Enterprise) أو ويندوز 10 برو أو إنتربرايس (Windows 10 Pro or Enterprise) وتدعم تشفير AES128 بت و256 بت. كما أنها تدعم تشفير محركات الأقراص المحمولة وكذلك وحدات التخزين الافتراضية.
- فايل فولت (FileVault 2) : ميزة التشفير الكامل للقرص في نظام التشغيل Mac OS X Lion أو الإصدارات الأحدث. ويستخدم تشفير XTS-AES 128 بت . كما يقوم بتشفير محرك بدء التشغيل بأكمله لجهاز ماك الخاص بك. أحدث إصدارات ماك OS X Yosemite (10.10) وMavericks (10.9) تدعم مفاتيح AES 256 بت.

فيرا كريبت (VeraCrypt) برنامج مجاني ومفتوح المصدر يشفر القرص كاملاً ويستند على تروكريبت (TrueCrypt). يلتقط فيرا كريبت حيثما يُترك تروكريبت ويضيف أمان محسّن إلى الخوارزميات المستخدمة للنظام وتشفير الأقسام، فيجعلها آمنة من التطورات الجديدة لهجمات القوة الغاشمة. يحل فيرا كريبت أيضًا نقاط ضعفٍ كثيرة ومشكلات أمنية في تروكريبت، حيث يمكنه تحميل حجم تروكريبت، ويوفر إمكانية تحويل حاويات تروكريبت والأقسام الخارجة عن النظام إلى تنسيق فيرا كريبت. وهو متاح لأنظمة ماك OSX ولينكس وويندوز.

تأمين الحذف

سي كلينر (CCleaner) أداة مجانية لتنظيف الويندوز المثبت على حاسوبك بحذف محفوظات المتصفح، وملفات تعريف الارتباط، وغيرها من الملفات المؤقتة التي تم إنشاؤها خلال جلسات العمل. يحمي سي كلينر خصوصيتك على الإنترنتويجعل حاسوبك أسرع وأكثر أمانًا.

بليتش بت (Bleachbit) أداة تنظيف مجانية ومفتوحة المصدر للنظام من شأنها أن تساعد في تفريغ ذاكرة التخزين المؤقت، وحذف ملفات تعريف الارتباط، ومسح محفوظات الإنترنت، وتقطيع الملفات المؤقتة، وحذف السجلات، وتجاهل البريد غير المرغوب فيه ومجهول المصدر. تم تصميمه لنظامي لينكس وويندوز، حيث يقوم بتنظيف عدد مهول من التطبيقات، بما في ذلك فايرفوكس (Firefox) ,وانترنت اكسبلورر (Internet Explorer), وأدوبي فلاش (Adobe Flash) وجوجل كروم (Google Chrome) وأوبرا (Opera) وسفاري (Safari) وأكثر من ذلك. والأكثر من مجرد حذف الملفات.

النسخ الاحتياطي وحماية البيانات

بوكس كريبتور (Boxcryptor): برنامج تجاري يقوم بتشفير البيانات الموجودة على جهازك قبل مزامنته إلى السحابة. ولذلك، تضمن أعلى حماية ممكنة لبياناتك. يمكن استخدام البرنامج من خلال دروب بوكس Dropbox، جوجل درايف Google Drive، و ميكروسوف وان درايف Microsoft OneDrive.

سبايدر أوك (SpiderOak): حل لنسخ احتياطي تجاري عبر الإنترنت للمستخدمين والمجموعات والشركات. تعلن الشركة أنها لا تعرف مفاتيح التشفير وبيانات التعريف الخاصة بك، ويتم تشفير بيانات المستخدمين على الخادم الخاص بهم على جانب العميل.

ملاحظة: خدمات الاستضافة الذاتية أكثر أمنًا؛ لأن خدمة مثل دروب بوكس لا تحاول الوصول إلى بياناتك الخاصة أو جمع بيانات التعريف عنك. ويعتبر أون كلاود (OwnCloud) خيارًا مجانيًا.

مديرو كلمة المرور

كيب باس إكس (KeePassX) أداة مجانية ومفتوحة المصدر لإدارة كلمة المرور المتاحة لنظام التشغيل ويندوز وماك أو إس ولينكس. تتيح للمستخدمين تخزين أسماء المستخدمين وكلمات المرور في قاعدة بيانات محمولة مشفرة.

لاست باس (Lastpass) عبارة عن مدير كلمة مرور ومُنشئ كلمة مرور واللتان تؤمّنان كلمات المرور الخاصة بك والمعلومات الشخصية في مخزن آمن. يعمل لاست باس على إجراء تعبئة تلقائية لمتصفح الويب وعمليات تسجيل دخولك إلى التطبيقات، وتُنشئ كلمات مرور جديدة وآمنة على الفور.

أنظمة التشغيل Live CD

تايلز (Tails) نظام تشغيل مباشر، يمكنك تشغيله تقريبًا على أي جهاز كمبيوتر باستخدام قرص دي في دي (DVD) أو عصا USB أو بطاقة SD. ويهدف إلى الحفاظ على خصوصيتك وعدم الكشف عن هويتك، ويساعدك على استخدام الإنترنت كمجهول أثناء التحايل على الرقابة. يوجّه تايلز جميع الاتصالات إلى الإنترنت من خلال شبكة تور.

تطبيقات الهاتف المحمول

برنامج سيجنال (للأجهزة التي تعمل بنظام الأندرويد وأي أو إس) **Signal (Android – iOS):** تطبيق الرسائل المشفرة من البداية حتى النهاية، بما في ذلك الرسائل الجماعية والمكالمات. تحتوي الإشارة على تطبيق كروم الذي يدعم الدردشة وليس المكالمات الصوتية.

برنامج تيليجرام (للأجهزة التي تعمل بنظام الأندرويد وأي أو إس) **Telegram (Android - iOS)** : تطبيق مراسلة يستخدم بروتوكول أمن خاص به وليس به وظيفة المكالمة الصوتية. تستخدم المحادثات العادية تشفير homebrew للمستخدم إلى الخادم، ولكن بوضع خاص يسمى "الدردشة السرية" يستخدم التشفير من البداية إلى النهاية.

واتس أب (للأجهزة التي تعمل بنظام الأندرويد وأي أو إس) **Whatsapp (Android - iOS):** عبارة عن مسنجر للهاتف النقال (mobile messenger) يملكه الفيسبوك التي نفّذت مؤخرًا وظيفة التشفير من البداية إلى النهاية استنادًا إلى نفس البروتوكول الذي تستخدمه الإشارة.

أفيرا موبايل سكيورتي (للأجهزة التي تعمل بنظام الأندرويد وأي أو إس) **Avira Mobile Security (Android - iOS)**: تطبيق مكافحة الفيروسات للهاتف النقال، الذي يحمي هاتفك الذكي من الفيروسات والمسارات المعروفة ويحدد الهواتف المفقودة.

موثق جوجل (للأجهزة التي تعمل بنظام الأندرويد وأي أو إس) **Google Authenticator (Android - iOS)** : أحد التطبيقات التي تعمل مع FA2 لحسابك الخاص في

جوجل من أجل توفير طبقة إضافية من الأمن عند تسجيل الدخول.

Secrecy (Android): تطبيق مجاني يعمل على تشفير ملفاتك الخاصة المهمة وإخفائها.

CameraV (Android): تطبيق مجاني يتيح لك التقاط الصور التي يمكن التحقق منها وتبادلها ودليل الفيديو على الهاتف الذكي أو الكمبيوتر اللوحي، مع الحفاظ التام على أمنها وخصوصيتها. جميع الصور ومقاطع الفيديو التي تلتقطها محمية بكلمة مرور ومشفرة بنسبة 100% على جهازك. يمكنك أيضًا إضافة ملاحظات وعلامات خاصة إلى أي صورة أو مقطع فيديو، واختيار مَن تشاركها معهم. ويعمل تطبيق CameraV أيضًا على تخزين البيانات من أدوات استشعار جهازك بشكل خاص, ويوفر أدوات مدمجة لرؤيتها ومشاركتها. وأخيرًا، به كاميرا آمنة مضمنة بسيطة وسلسة دعم حتى للصور الذاتية.

Android Device Manager (Android): خدمة مدير جهاز أندرويد (للأجهزة التي تعمل بنظام الأندرويد) تحدد الأجهزة المفقودة وتساعدك في الحفاظ على جهازك -والبيانات التي داخله آمنة ومؤمّنة. تتيح لك إدارة أجهزة أندرويد تحديد موقع أجهزة أندرويد المقترنة بحساب جوجل الخاص بك وإعادة تعيين رقم التعريف الشخصي؛ لتأمين شاشة جهازك, ومحو جميع البيانات الموجودة على الهاتف.

Find My iPhone (iOS): خدمة العثور على هاتف الآيفون (للأجهزة التي تعمل بنظام الاي او اس) سيتيح لك استخدام أي جهاز iOS للعثور على هاتفك المفقود, وحماية البيانات الخاصة بك. كل ما عليك تثبيت هذا التطبيق المجاني وفتحه وتسجيل الدخول باستخدام معرّف آبل الذي تستخدمه لبرنامج iCloud. ستساعدك خدمة العثور على الآيفون في تحديد موقع جهازك المفقود على الخريطة أو تأمينه عن بُعد.

أدوات الإنترنت

محركات البحث التي تحترم الخصوصية

يشعر بعض المستخدمين بالقلق من انتهاك حقهم في الخصوصية من قِبل محركات البحث، التي تسجّل تاريخ عمليات البحث الخاصة بهم وتحدد هويتهم. هذان مثالان على محركات البحث الخاصة التي لا تتعقّب المستخدمين:

- Startpage (ستارت بيدج)
- DuckDuckGo (داك داك جو)

خدمات المؤتمرات عن طريق الفيديو غير المحدد للهوية

تستند معظم دردشات الفيديو المجهولة عبر الإنترنت إلى تقنية WebRTC، التي تتميز بتشفير قوي. هذا التشفير يحمي المتصلين من العديد من هجمات المراقبة من مزودي خدمات الإنترنت وأنظمة SORM/PRISM. ومع ذلك، قد لا يزال الخادم يملك حق الوصول إلى محتويات الاتصالات وليس هناك طريقة يمكن للمستخدم معرفتها ما إذا كان لديه هذا الحق. تختلف الخدمات الفردية في الحد الأقصى لعدد المشاركين في المكالمات وغيرها من الميزات، ومع ذلك، لأن التعليمات البرمجية لكثير من الأنظمة مفتوحة المصدر، يوصى بقيام المستخدمون بإعداد أنظمتهم الخاصة لضمان أقصى قدر من الأمان للاتصالات. يقوم Google Hangouts باستخدام WebRTC على متصفح كروم وليس فايرفوكس. أمثلة على خدمات المؤتمرات عن طريق الفيديو غير المحدد للهوية:

- Appear.in
- Talky
- Chatb.org
- Jitsi Meet

مقاطع فيديو أخرى مفيدة

- تشفير المفتاح العام والخاص: https://mashable.com/2015/10/15/how-encryption-works/#X8RVrUifZPqh
- تشفير : https://www.youtube.com/watch?v=1-MPcUHhXoc
- تشفير القرص كاملاً: https://www.youtube.com/watch?v=UPW1Hqvx6zo
- HTTPS: https://www.youtube.com/watch?v=SJJmoDZ3il8

الأوراق البيضاء ((White Papers

مقالات مواضيعية وورقات بحثية قصصية قصيرة كتبها موظفو مشروع ISC لدراسة الموضوعات الأساسية في أمان المعلومات وتكون بمثابة مصدر قيّم لأي شخص يبحث عن المعرفة الأساسية في هذا المجال:

- المخاطر المخفية من التطبيقات – الأخذ بعين الاعتبار بيانات الصورة ورقم الهاتف
- يوفّر Chat Secure مراسلة فورية سهلة الاستخدام للهاتف المحمول بحماية مضمّنة على مستويات متعددة
- النسخ الاحتياطي للمستخدم النهائي واستعادته

مصادر أخرى

- **Privacytools.io**: موقع ويب ذو دوافع اجتماعية يوفر معلومات؛ لحماية أمان بياناتك وخصوصيتك.
- **Security in-a-box**: دليل الأمن الرقمي للناشطين والمدافعين عن حقوق الإنسان في جميع أنحاء العالم.
- **Surveillance self-defense**: نصائح وأدوات وتوصيات عن كيفية الوصول إلى اتصالات الإنترنت بصورة أكثر أمنًا.

INNOVATION FOR CHANGE

MIDDLE EAST & NORTH AFRICA

/ Innov4changeMENA

www.innovationforchange.net