الحماية عبر الإنترنت والأمن الرقمي

دليل المستخدم للمدافعين عن حقوق الإنسان

#كُن_آمن

Human Rights Office
United Nation Assistance Mission for Iraq
(UNAMI)
بعثة الأمم المتحدة لمساعدة العراق
(يونامي)

INSM
الشبكة العراقية
للإعلام المجتمعي

المادة 19

الإعلان العالمي لحقوق الإنسان

لكلِّ شخص حقُّ التمتُّع بحرِّية الرأي والتعبير، ويشمل هذا الحقُّ حرِّيته في اعتناق الآراء دون مضايقة، وفي التماس الأنباء والأفكار وتلقِّيها ونقلها إلى الآخرين، بأيَّة وسيلة ودونما اعتبار للحدود.

المحتويات

اخلاء المسؤولية

يرحب مكتب حقوق الإنسان التابع لبعثة الأمم المتحدة لمساعدة العراق (يونامي) بفرصة الترويج لأنشطتها ومنشوراتها بالتعاون مع شركائها. يرجى العلم أن المعلومات والنصائح والتوصيات (بما في ذلك البرامج والتطبيقات الموصى بها) مقدمة من قبل مؤلفي هذا الدليل لأغراض المعلومات العامة فقط، ولا تمثل بالضرورة آراء بعثة الأمم المتحدة لمساعدة العراق.

بينما سعى مؤلفو هذه الوثيقة إلى توفير معلومات محدثة وصحيحة في وقت النشر، تتغير تهديدات تكنولوجيا المعلومات والأمن الرقمي بسرعة وبالتالي لا يمكن ضمان الدقة في جميع الأوقات. على هذا النحو، لا تقدم يونامي أي تعهدات أو ضمانات من أي نوع حول الاكتمال أو الدقة أو الموثوقية أو الملاءمة أو التوافر فيما يتعلق بالمعلومات أو المنتجات أو الخدمات الواردة هنا. يجب على المستخدمين التحقق من دقة وأمان المعلومات أو البرامج الحالية قبل استخدامها. يتم توفير الموارد في نهاية هذا الدليل لمساعدة المستخدمين على مواكبة الأساليب والبرامج الآمنة.

المقدمة

حماية حقوق الإنسان على الإنترنت في العراق

تنطبق حقوق الإنسان بالتساوي على الإنترنت وخارجه

في ندائه للعمل من أجل حقوق الإنسان[1]، أكد الأمين العام للأمم المتحدة أن التقنيات الرقمية فتحت آفاقاً جديدة، وتوفر وسائل جديدة للمناصرة حول حقوقنا والدفاع عنها وممارستها. في الوقت نفسه، غالباً ما تُستخدم هذه التقنيات الجديدة لانتهاك حقوق الإنسان وتقليص المساحة المدنية، بما في ذلك المراقبة عبر الإنترنت والقمع والرقابة والمضايقات.

في العراق، يعتمد المدافعون عن حقوق الإنسان بشكل متزايد على التقنيات الرقمية لرصد حقوق الإنسان وتوثيقها والإبلاغ عنها والدفاع عنها. يذهب الصحفيون ومنظمات المجتمع المدني والنشطاء وغيرهم من الجمهور إلى الإنترنت لمشاركة آرائهم وتعزيز النقاش وتوليد الدعم. على سبيل المثال، عندما بدأت المظاهرات واسعة النطاق المناهضة للحكومة على نطاق غير مسبوق في أكتوبر 2019 في العديد من المحافظات في جميع أنحاء العراق، وفرت المساحة على الإنترنت منصة رئيسية للتعبئة والتنظيم ومشاركة المعلومات في الوقت الفعلي والإبلاغ عن التطورات، بما في ذلك انتهاكات حقوق الإنسان.

ومع ذلك، في الوقت نفسه، يمكن أن تعمل المنصات عبر الإنترنت أيضاً كمواقع للتهديد والترهيب والمضايقة للمتظاهرين، بما في ذلك عن طريق اختراق الحسابات الخاصة أو "التشهير" بالأفراد، وتعريضهم لتهديدات أمنية إضافية خارج الإنترنت. علاوة على ذلك، تستمر حالات القرصنة والابتزاز الإلكتروني وسرقة البيانات وانتهاك الملكية الفكرية وانتهاكات الخصوصية في الارتفاع في العراق.

تطرح الحماية الفعالة لحقوق الإنسان عبر الإنترنت تحديات هائلة بسبب التقنيات المتطورة باستمرار و "إخفاء" الجناة. في هذا السياق، يحتاج المستخدمون الأفراد للتقنيات الرقمية إلى مواكبة التطورات واتخاذ تدابير استباقية لحماية خصوصيتهم وسلامتهم وسرية بياناتهم.

[1] إن النداء إلى العمل من أجل حقوق الإنسان هي رؤية الأمين العام التحويلية لحقوق الإنسان. والتي تُدعِم عمل منظومة الأمم المتحدة بأكملها، حقوق الإنسان ضرورية لمعالجة الأسباب والتأثيرات الواسعة لجميع الأزمات المعقدة، وبناء مجتمعات مستدامة وآمنة وسلمية.

تم تطوير هذا الدليل من قبل شبكة انسم للحقوق الرقمية (INSM - انسم)، بدعم من مكتب حقوق الإنسان، بعثة الأمم المتحدة لمساعدة العراق (UNAMI - يونامي) لتزويد المدافعين عن حقوق الإنسان على وجه الخصوص بأدوات عملية لحماية أنفسهم من المتسللين ومنتهكين آخرين. تشكل المبادئ التوجيهية جزءاً من مشروع "الحقوق الرقمية والأمن الرقمي،" الذي تم تنفيذه منذ عام 2021 من قبل انسم بدعم من يونامي، لزيادة الوعي والتخفيف من المخاطر عبر الإنترنت مع زيادة حماية المدافعين العراقيين عن حقوق الإنسان في الفضاء الرقمي.
هذا الدليل للجميع. يرشد المستخدمين من خلال الخطوات والأدوات الأساسية التي يحتاجون إليها لمواجهة المخاطر الرقمية ومنع الخطر عبر الإنترنت وخارجه.

كن_آمن

02

الأساسيات العشرة الأهم لحماية الكمبيوتر والمحمول

01 تحديث نظام التشغيل والأجهزة والتطبيقات

02 قم بإنشاء كلمات سر قوية على جميع الاجهزة

03 استخدم المصادقة متعددة العوامل (MFA) كلما امكن ذلك

04 تثبيت برامج (مكافح البرامج الضارة)

05 استخدم متصفحاً آمناً

06 تثبيت شبكة افتراضية خاصة (VPN)

07 استخدم برامج وتظبيقات آمنة ومفتوحة المصدر

08 قم بتنزيل التطبيقات والبرامج من متاجر التطبيقات المعترف بها

09 تشفير أجهزة الكمبيوتر والهواتف

10 قم بعمل نسخة احتياطية من بياناتك

أهم عشرة أساسيات لحماية الكمبيوتر والمحمول

يقدم هذا القسم "أهم عشر نصائح" لتحسين الأمان الرقمي للمستخدم. توفر هذه الخطوات الأساسية نقطة دخول إلى الموضوعات الرئيسية التي يتم تناولها بتعمق في الفصول اللاحقة.

النصيحة الاولى: قم بتحديث نظام التشغيل والأجهزة والتطبيقات والهاتف والبرامج بانتظام

تقدم الشركات تحديثات دورية لأنظمة التشغيل والتطبيقات الخاصة بها لمعالجة الثغرات الأمنية. يؤدي التحديث المنتظم إلى تحسين حماية المستخدم بشكل كبير ضد الانتهاكات الأمنية.

في ويندوز 11، يحدد المستخدم وقت وكيفية الحصول على آخر التحديثات للحفاظ على تشغيل الأجهزة بسلاسة وأمان. لإدارة الخيارات وعرض التحديثات المتاحة، إختر التحقق من وجود تحديثات ويندوز. أو اختر **ابدأ > الإعدادات > تحديث ويندوز.**

- على أجهزة ال **Mac**، اتبع التعليمات المتوفرة هنا.
- لتحديث هاتف **Android**، اتبع التعليمات المتوفرة هنا.
- لتحديث **iOS (iPhone)**، انتقل إلى App Store واتبع التعليمات المتوفرة هنا.

أياً كان نظام التشغيل والتطبيقات والبرامج المستخدمة، اجعل تحديثها المنتظم أولوية.

النصيحة الثانية: أنشئ كلمات مرور قوية على جميع الأجهزة

يجب على المستخدمين التأكد من أن جميع كلمات المرور:

- طويلة (أكثر من 12 حرفاً).
- مركبة (تحتوي على مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز).
- عشوائية، لا تحتوي على كلمات شائعة أو شخصية أو سلسلة أرقام، إلخ.

- فريدة (كلمة مرور منفصلة لكل حساب).
- سرية (ليس من السهل العثور عليها في الأوراق أو الأجهزة).

راجع القسم الثالث للحصول على مزيد من المعلومات حول كيفية إنشاء وإدارة وتخزين جميع كلمات المرور بشكل سري.

النصيحة الثالثة: استخدم المصادقة متعددة العوامل (MFA) كلما أمكن ذلك

- تعمل المصادقة متعددة العوامل على زيادة الأمن الرقمي بشكل كبير.
- تعد التطبيقات المصممة خصيصاً للمصادقة متعددة العوامل، مثل Duo Mobile و Aegis Authenticator و Google Authenticator أكثر أماناً من مصادقة الرسائل النصية القصيرة.

انظر القسم الثالث لمزيد من المعلومات والروابط للتطبيقات الموصى بها.

النصيحة الرابعة: قم بتثبيت برنامج لاكتشاف نقطة النهاية والاستجابة Endpoint Detection and Response (EDR) (مكافحة البرامج الضارة)

- يمكن للبرامج الضارة تدمير جهاز أو سرقة المعلومات الشخصية أو الأصول المالية أو التحكم في الجهاز عن بُعد.
- توفر برامج EDR الحماية من البرامج الضارة على الإنترنت.
- قم بتثبيت إصدارات مرخصة من برنامج EDR على كل جهاز يعمل بنظام ويندوز أو Mac أو Linux أو iOS أو Android. لا تستخدم البرامج "المقرصنة."
- قم بتثبيت برامج مثل Malwarebytes و Avira.

انظر القسم الرابع لمزيد من المعلومات.

النصيحة الخامسة: استخدم متصفحاً آمناً

- يعد المتصفح بمثابة نافذة على الإنترنت. إذا لم تكن النافذة آمنة، فإن الوصول والتنقل غير آمنين وقد يكونان طريقاً للإصابة بالبرامج الضارة.
- العديد من المتصفحات هي أدوات تجارية لجمع المعلومات وتتبع البيانات والاستهداف لأغراض التسويق.
- استخدم متصفحات آمنة، مثل Tor و Firefox و Brave و Firefox Focus و Ghostery Dawn و DuckDuckGo؛ وقم تحديث برنامج المتصفح بانتظام.
- تحقق من أمان الوظائف الإضافية / ملحقات المتصفح قبل إضافتها إلى المتصفح.

انظر القسم الخامس أدناه لمزيد من المعلومات.

النصيحة السادسة: قم بتثبيت شبكة افتراضية خاصة (VPN)

- يعني مصطلح VPN "الشبكة الافتراضية الخاصة" - خدمة تحمي اتصال المستخدم بالإنترنت وخصوصيته عبر الإنترنت من خلال إنشاء نفق مشفر لبيانات المستخدم وإخفاء عنوان IP الخاص بالمستخدم. وتسمح بالاستخدام الآمن لشبكة Wi-Fi العامة. بدون استعمال الشبكة الافتراضية الخاصة للحماية، قد يتم تعقب الأجهزة ومواقعها أو قد يتم اعتراض البيانات.
- اختر الشبكة الافتراضية الخاصة بعناية. هناك خدمات مجانية ومدفوعة تحتوي على برامج ضارة، أو تبيع معلومات المستخدمين إلى طرف ثالث، أو تتعاون مع الحكومات لتزويدهم بمعلومات المستخدمين.
- الشبكات الافتراضية الخاصة التي تعتبر آمنة وقت النشر تشمل Psiphon أو TunnalBear أو Riseup VPN.

انظر القسم الثالث أدناه لمزيد من المعلومات.

النصيحة السابعة: استخدم برامج وتطبيقات آمنة مفتوحة المصدر

- تعد البرامج والتطبيقات "مفتوحة المصدر" أكثر أماناً بشكل عام من البرامج الاحتكارية، لأنها توفر شفرة المصدر الخاصة بها للمستخدمين. ثم يتم تحديث كود المصدر هذا باستمرار لمعالجة الثغرات الأمنية.
- استخدام البرامج والتطبيقات مفتوحة المصدر يمنع المستخدمين من استخدام البرامج الاحتكارية المقرصنة بدون ترخيص. قد تحتوي البرامج المقرصنة على عناصر ضارة تضر بالأجهزة ويجب عدم استخدامها مطلقاً.
- إعلم أنه ليست كل البرامج مفتوحة المصدر آمنة: اتبع دائماً نصائح خبراء الأمن الرقمي قبل تثبيت برنامج أو تطبيق جديد.

النصيحة الثامنة: قم بتنزيل التطبيقات والبرامج من متاجر التطبيقات المعروفة حصراً

- تحتوي متاجر التطبيقات غير المعترف بها على عشرات التطبيقات والبرامج الملوثة بالبرامج الضارة والأبواب الخلفية التي توفر للمُنشئ القدرة على إدارة الأجهزة والتحكم فيها.
- استخدم متاجر التطبيقات المعترف بها ومواقع التطبيقات الرسمية للتنزيلات فقط.

النصيحة التاسعة: تشفير أجهزة الكمبيوتر والهواتف

- يوفر التشفير السري وهو أمر أساسي لأمن المعلومات.
- استخدم التشفير لإرسال رسائل مشفرة وتخزين المعلومات بأمان وتصفح الإنترنت بشكل مجهول ومشاركة المعلومات بشكل أكثر أماناً.

راجع القسم السادس لمزيد من المعلومات حول أدوات التشفير.

النصيحة العاشرة: قم بعمل نسخة احتياطية من بياناتك

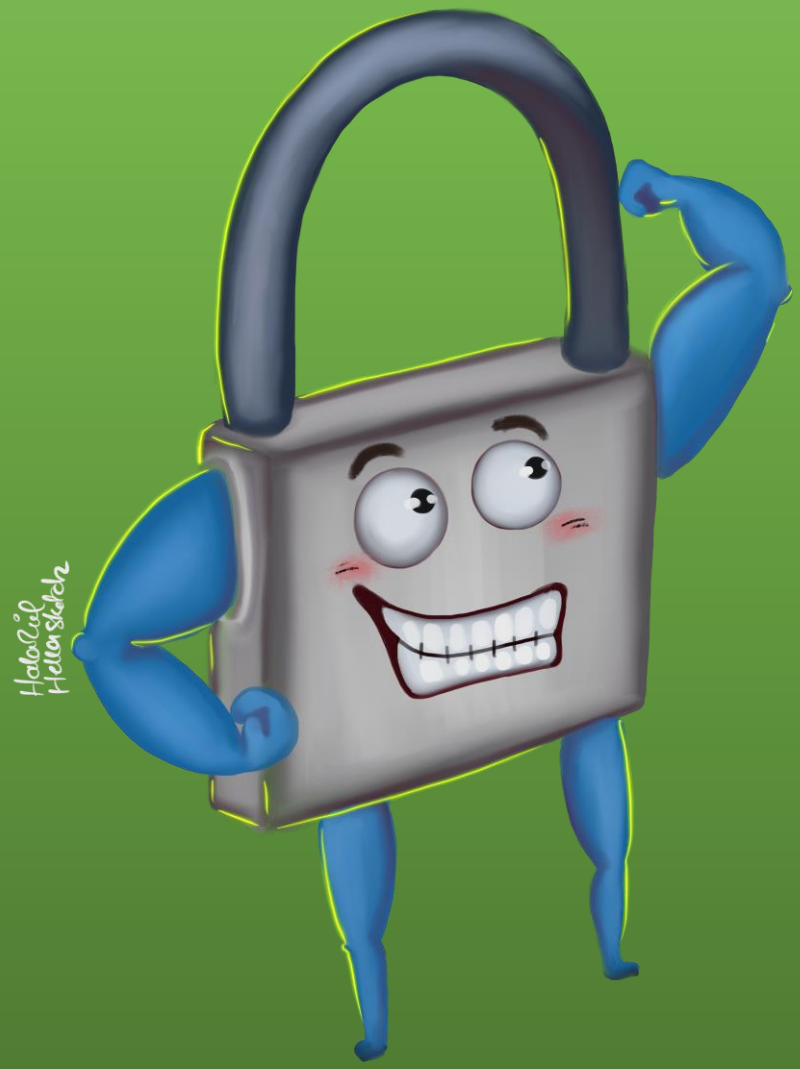
- تشبه عملية النسخ الاحتياطي تخزين المعلومات القيمة في مكان آمن بحيث يمكن استعادتها في حالة فقدان البيانات الأصلية أو تلفها أو اختراقها.

- قم بتنشيط أداة النسخ الاحتياطي المتوفرة مع نظام التشغيل يدوياً (سواء في نظام ويندوز أو MacOS) وتأكد من إكمال النسخ الاحتياطية بشكل دوري.
- قم بتشفير النسخ الاحتياطية من البيانات للتخزين.
- قم بتخزين النسخة الاحتياطية إما على محرك أقراص ثابت خارجي أو عبر خدمة سحابية، على سبيل المثال، Mega.

انظر القسم السادس لمزيد من المعلومات.

03

إنشاء كلمات مرور قوية وقم بتمكين المصادقة متعددة العوامل



بإنشاء كلمات مرور قوية وقم بتمكين المصادقة متعددة العوامل

كلمات مرور قوية

توفر كلمات المرور القوية أساس الحماية الرقمية. تسمح لها قوتها بمقاومة العديد من الهجمات التي تستهدف كلمات المرور، بما في ذلك عمليات التصيد و keyloggers وهجمات أخرى تهدف إلى اعتراض البيانات أو الحصول على دخول غير مصرح به إلى حسابات أو بيانات محمية[2].

أفضل دفاع ضد هذهِ الهجمات هو منعها من خلال إنشاء كلمات مرور قوية وتغييرها بانتظام.

كلمة المرور القوية هي:

1. **طويلة:** استخدم أكثر من 12 حرفاً. كلما كانت كلمة المرور أقصر، كان التعرف عليها أسرع.
2. **معقدة:** استخدم الأحرف الكبيرة والصغيرة والأرقام والرموز.
3. **عشوائية:** تجنب استخدام الأرقام أو الأحرف بطريقة متسلسلة أو استخدام المعلومات الشخصية أو العائلية. تجنب استخدام تواريخ الميلاد أو أسماء أفراد الأسرة أو الحيوانات الأليفة في كلمات المرور.
4. **يسهل تذكرها:** يبدأ نسيان كلمات المرور بدورة استرجاع تتطلب مزيداً من المعلومات. استخدم مدير كلمات المرور (أدناه) إذا أصبح تذكر كلمات مرور متعددة أمراً معقداً.
5. **سرية:** قم بإنشاء وحفظ كلمات مرور في الأماكن الآمنة فقط. تشمل الأماكن غير الآمنة مباشرة في المتصفح أو تطبيق ملاحظات الهاتف أو تطبيق التذكيرات بالهاتف أو الملاحظات اللاصقة على جهاز كمبيوتر أو داخل دفتر ملاحظات / جدول أعمال. هذه المواقع غير آمنة لأنه يسهل الوصول إليها.

[2] الهجمات التي تهدف إلى الكشف عن كلمات المرور تشمل الرجل في الوسط (MITM)، والقوة المفرطة وهجمات القاموس، وحشو بيانات الاعتماد. لمعرفة المزيد حول هجمات كلمات المرور الشائعة، راجع Password Cracking 101: شرح الهجمات والدفاعات.

6. **فريدة:** يجب أن يكون لكل حساب أو خدمة كلمة مرور خاصة. سيؤدي اكتشاف كلمة المرور لحساب واحد إلى جعل الحسابات الأخرى عرضة للخطر إذا كانت تستخدم نفس كلمة المرور.
7. **يتم تغييرها بشكل دوري:** تعتمد المدة التي يمكن خلالها استخدام كلمة المرور قبل التغيير على مستوى المخاطر التي يواجهها كل مستخدم. في الحالات العادية، يوصى بتغيير كلمات المرور كل ثلاثة أشهر. عند تغيير كلمة المرور، يجب على المستخدم الخروج بالكامل من التطبيق أو الخدمة على جميع الأجهزة.
8. **أصيلة:** لا تستخدم أنماط لوحة المفاتيح الشائعة ، على سبيل المثال، "Qwerty12345" أو "Password123".

يمكن حفظ كلمات المرور في ذاكرات التخزين المؤقت التي يصعب الوصول إليها أو في أدوات مدير كلمات المرور. تعد ذاكرات التخزين المؤقت هذه مولدات كلمات مرور قوية، ويمكن حفظ عدد كبير من كلمات المرور فيها.

تشمل أدوات مدير كلمات المرور التي تعتبر آمنة وقت النشر ما يلي:

1. KeePassXC
2. Bitwarden

المصادقة متعددة العوامل (MFA)

يوفر تنشيط ميزة المصادقة متعددة العوامل على الحسابات حماية قوية من القرصنة والتصيد الاحتيالي. المصادقة متعددة العوامل هي ميزة إضافية تطالب المستخدمين بإدخال رمز مرور أحادي الاستخدام يتم إنشاؤه بعد إدخال كلمة المرور العادية الخاصة بهم. يتم إرسال كلمة المرور أحادية الاستخدام هذه إلى المستخدم عبر الرسائل القصيرة أو البريد الإلكتروني أو الوصول إليها عبر تطبيق مصادقة محدد.

يقوم العديد من المستخدمين بتنشيط هذه الميزة عبر الرسائل النصية القصيرة SMS على هواتفهم المحمولة. ومع ذلك، فإن استخدام المصادقة متعددة العوامل المستندة إلى الرسائل القصيرة ينطوي على مخاطر إضافية في العراق، بسبب نقاط الضعف المستخدمة لمهاجمة بطاقات SIM (تسمى هجمات "Simjacker"[3]).

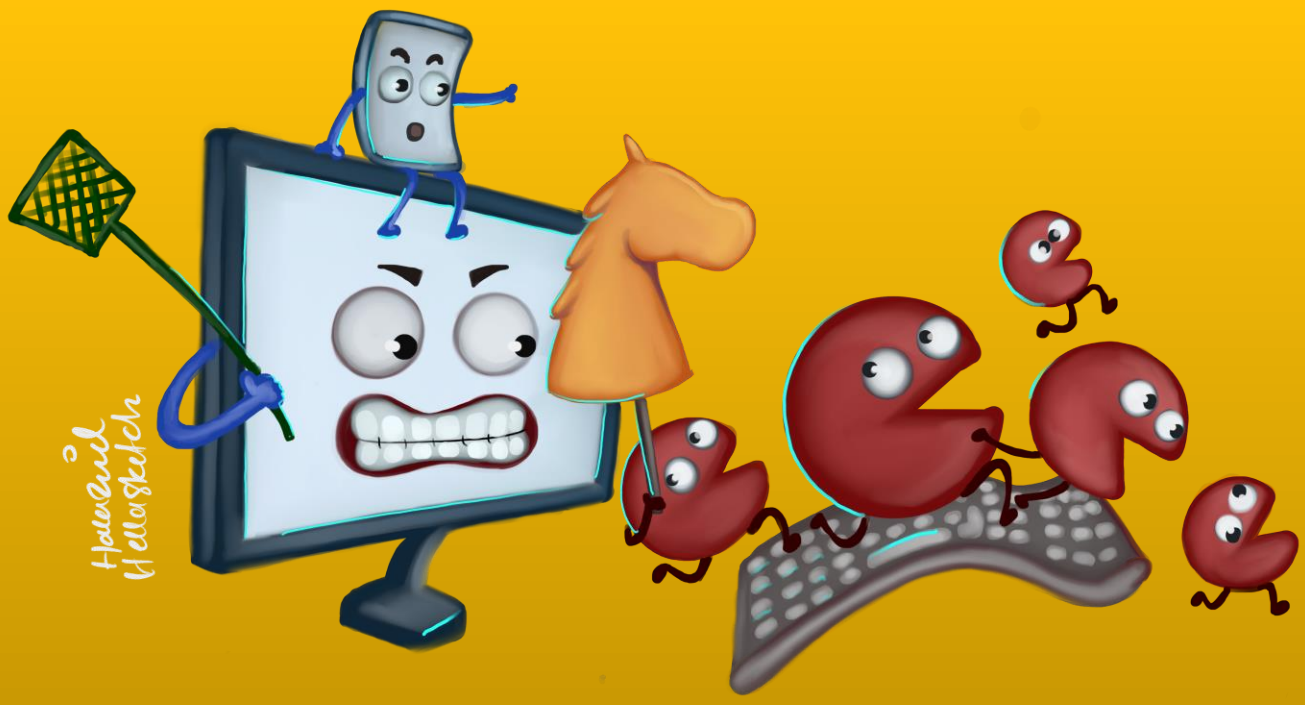
ان أفضل طريقة لتمكين التحقق من خطوتين هي تمكينه باستخدام تطبيق خارجي. تم اعتبار التطبيقات التالية آمنة وقت النشر:

1. Duo Mobile
2. Aegis Authenticator (لنظام Android فقط)
3. Google Authenticator (iOS أو Android)

[3] وفقًا لتقرير نُشر في أكتوبر 2019، فإن العراق ضمن قائمة 29 دولة تعاني فيها قطاعات الاتصالات من ثغرة تزيد من تعرضها لهجمات Simjacker. تحتوي بعض بطاقات SIM على تطبيق Java صغير مثبت مسبقًا يسمى S@T Browser ، والذي، إذا تم تكوينه بشكل غير صحيح، يمكنه فتح بطاقة SIM لأوامر ضارة من المهاجمين والمحتالين والرقابة الذين يرغبون في الوصول إلى محتوى هاتف المستخدم. انظر ZDNet، هذه هي 29 دولة عرضة لهجمات Simjacker، 11 أكتوبر 2019، متاح على: https://www.zdnet.com/article/these-are-the-29-countries-vulnerable-to-simjacker-attacks/

04

تخلص من البرامج الضارةMalware



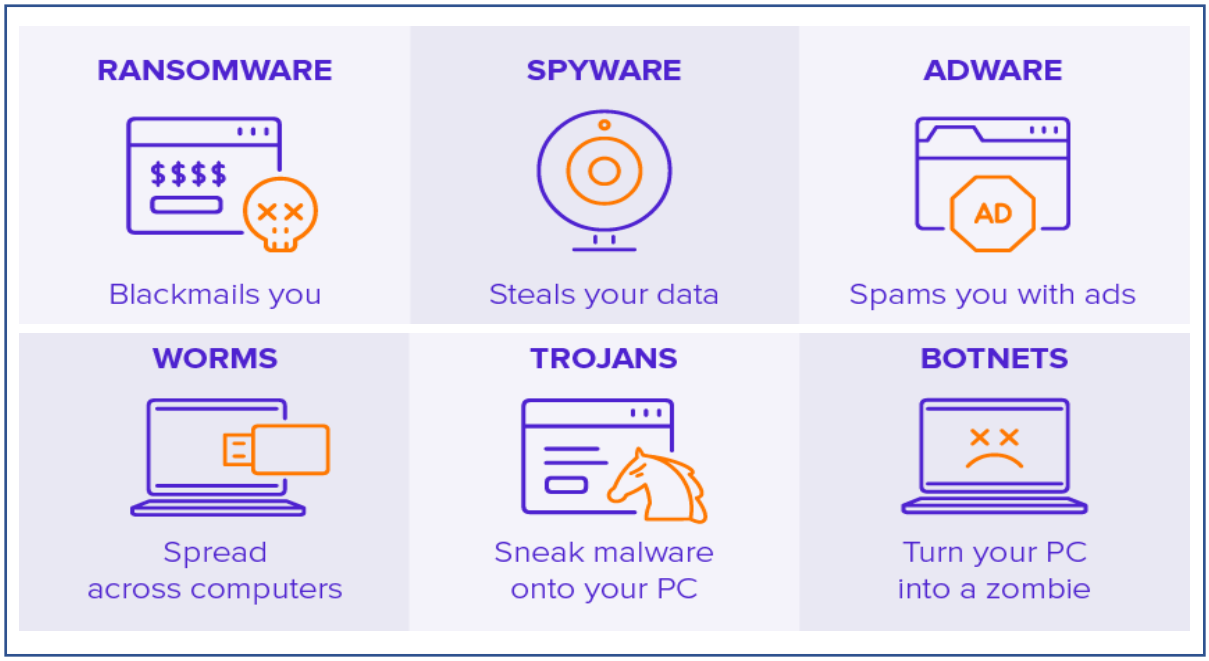
ما هي البرامج الضارة؟

البرامج الضارة، أو "Malware"، هي مصطلح يصف البرامج المصممة بقصد إتلاف الأجهزة أو أنظمة التشغيل أو الشبكات أو استغلالها أو تعطيلها. ويتم استخدامها لسرقة البيانات أو الحصول على وصول غير مصرح به أو تعطيل بعض أو كل الوظائف أو إتلاف الأجهزة أو أي شبكات ذات صلة.

تشكل "الفيروسات" جزءاً صغيراً فقط من عائلة البرامج الضارة، بينما قد تتسلل أنواع أخرى من البرامج الضارة الأكثر ضرراً إلى الأجهزة وتصيبها أثناء استخدام الإنترنت.

تتطلب عملية التخلص من البرامج الضارة خطوات وقائية مستمرة. يتيح إنشاء حواجز أمام العدوى واختراق البرامج الضارة للمستخدمين القضاء على التهديدات قبل دخولها إلى أجهزتهم.

هناك أنواع عديدة من البرامج الضارة، بما في ذلك أحصنة طروادة والديدان وبرامج الفدية وبرامج الإعلانات المتسللة وبرامج التجسس وغيرها.

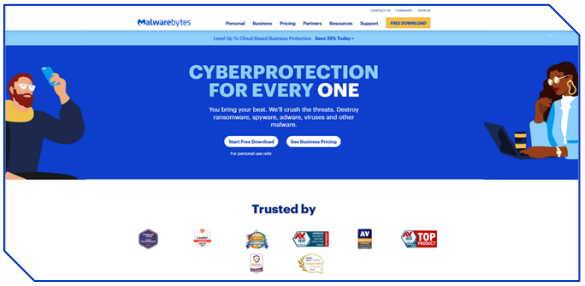


كيفية حماية الأجهزة من البرامج الضارة

يجب اتباع الخطوات التالية لحماية الأجهزة من البرامج الضارة:

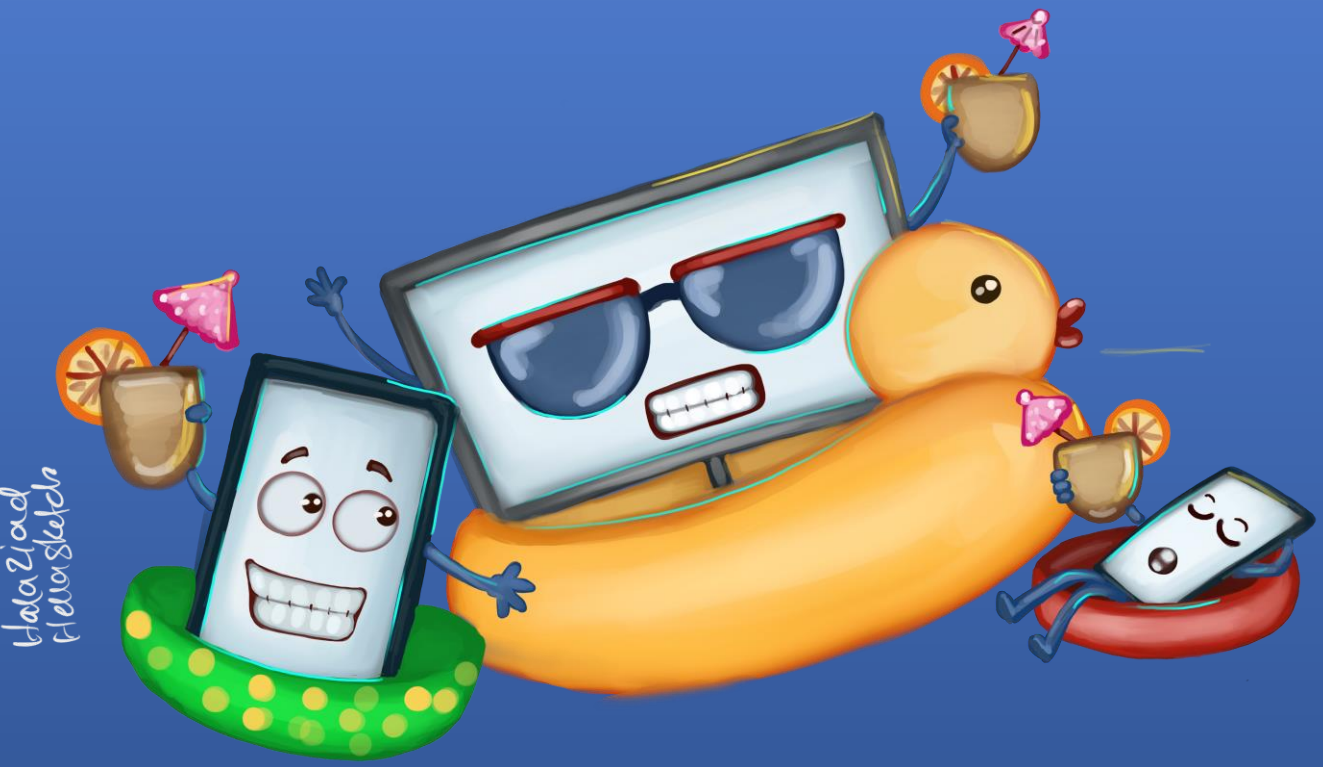
1. قم بتثبيت برنامج موثوق لاكتشاف نقطة النهاية والاستجابة (EDR) على كل جهاز يعمل بنظام ويندوز أو Mac أو Linux أو iOS أو Android، بما في ذلك جميع أجهزة الكمبيوتر والهواتف المحمولة. لاحظ أنه يجب تثبيت برنامج EDR واحد فقط.
2. قم بتنزيل البرامج والتطبيقات من مواقعها الرسمية فقط.
3. قم بتحديث أنظمة التشغيل والتطبيقات الخاصة بكل جهاز بشكل منتظم.
4. تجنب استخدام شبكات Wi-Fi العامة و / أو غير الآمنة بدون الحماية المناسبة (مثل استخدام شبكة افتراضية خاصة VPN).
5. لا تضغط على روابط من الغرباء أو رسائل البريد الإلكتروني أو الرسائل المشبوهة حتى لو كانت من جهات اتصال معروفة.
6. تجنب مشاركة المعلومات الشخصية.
7. استخدم متصفحاً آمناً أثناء تصفح الإنترنت.
8. قم بتثبيت الوظائف الإضافية للأمان الموصى بها للمتصفح.

يعتبر برنامجي Malwarebytes و Avira من برامج EDR الآمنة وقت النشر (بكلتا إصداريهما المجاني والمدفوع).



05

تصفح الانترنت بأمان



تصفح الإنترنت بأمان

تبدأ المخاطر التي يتعرض لها المستخدمون عندما يتصل الكمبيوتر أو الهاتف بالإنترنت ويبدأ المستخدم في البحث أو التواصل مع الآخرين.

لزيادة الأمان، استخدم أدوات آمنة للوصول إلى الإنترنت. يساعد هذا في منع مقدمي الخدمة أو السلطات أو المتسللين من مراقبة نشاط المستخدمين.

تأمين جهاز التوجيه الخاص بك

تتضمن الخطوة الأولى تأمين نقطة اتصال Wi-Fi في المنزل أو في العمل عن طريق تغيير إعدادات جهاز التوجيه. اطلب المساعدة الفنية لهذه الخطوات إذا كانت غير مألوفة[4].

1. قم بتغيير اسم المستخدم وكلمة المرور لحساب مسؤول جهاز التوجيه.
2. قم بتغيير عنوان IP الخاص بجهاز التوجيه.
3. استخدم كلمة مرور قوية وخاصة لشبكة Wi-Fi.
4. اضبط إعدادات التشفير واختر WPA2-PSK (AES)
5. قم بتحديث البرنامج الثابت لجهاز التوجيه.
6. قم بإخفاء اسم شبكة Wi-Fi.

استخدام نقاط اتصال Wi-Fi العامة

عادة ما تكون شبكات Wi-Fi العامة (في المقاهي والمتاجر ومراكز التسوق والفنادق والمطارات ووسائل النقل العام والمطاعم وما إلى ذلك) ضعيفة في الأمان ويمكن أن تشكل تهديدات خطيرة للمستخدم، بما في ذلك:

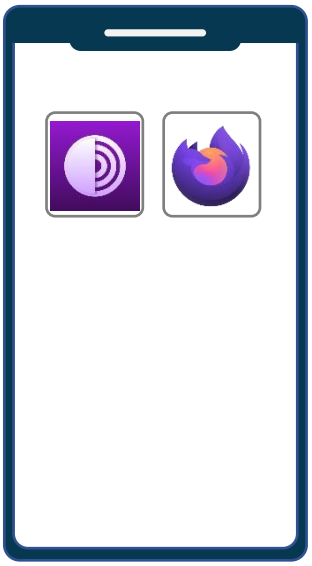
[4] للحصول على معلومات أساسية حول كيفية تهيئة جهاز التوجيه، يرجى الاطلاع على مشروع Security in a Box "الحماية من البرامج الضارة: تأمين جهاز التوجيه الخاص بك،" المتاح هنا: https://securityinabox.org/en/phones-and-computers/malware/

1. **تهديد اكتشاف الحزم:** يقوم المهاجمون (المتسللون) بمراقبة واعتراض البيانات المرسلة أو المستلمة غير المشفرة المنقولة عبر شبكات غير محمية.
2. **هجمات الرجل في المنتصف:** يتسلل المهاجمون إلى نقطة اتصال Wi-Fi الضعيفة لتكون جزءاً من الاتصال بين الضحية المستهدفة ونقطة الاتصال، لاعتراض البيانات أثناء النقل وتعديلها أحياناً.
3. **شبكات Wi-Fi الخادعة:** يقوم المهاجمون بإنشاء وإعداد نقطة اتصال مجانية ومفتوحة للجمهور للاتصال، مما يجعلها ممراً لجمع بيانات المستخدم.

احمِ نفسك عند استخدام شبكة Wi-Fi العامة

اتبع هذه الإرشادات لحماية المعلومات الشخصية من المهاجمين أثناء استخدام نقاط الاتصال العامة:

- تجنب استخدام نقاط الاتصال المحمولة Hotspot غير المعروفة / غير الآمنة أو الإنترنت العام كلما أمكن ذلك.
- إذا كنت تستخدم شبكة عامة، فتأكد من تمكين المصادقة متعددة العوامل لجميع الحسابات قبل الاستخدام.
- استخدم جدار حماية. تتضمن معظم أنظمة التشغيل هذه الخدمة، كما هو الحال مع برامج مكافحة البرامج الضارة / اكتشاف نقاط النهاية والاستجابة لها. تشمل التطبيقات التي تعتبر آمنة وقت تقديم الطلب ما يلي:
  - Avira
  - Comodo
  - GlassWire
- استخدم خدمة VPN لتشفير اتصال الإنترنت والحفاظ على خصوصية النشاط عبر الإنترنت على أي شبكة. تشمل الشبكات الافتراضية الخاصة التي تعتبر آمنة وقت النشر ما يلي:



- Psiphon
- TunnelBear
- Riseup

استخدم متصفحات آمنة

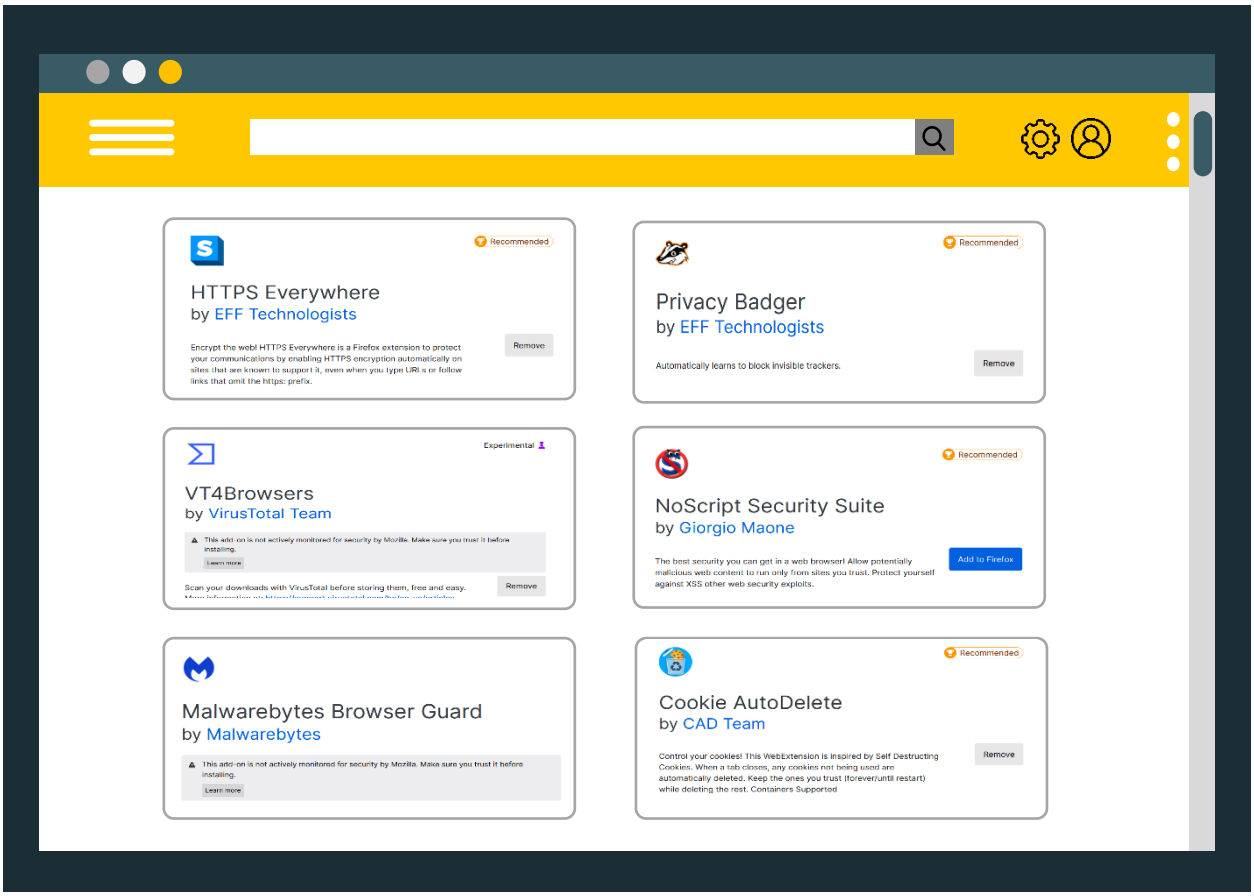
المتصفحات هي البوابة الرئيسية للوصول إلى الإنترنت، وبالتالي تلعب دوراً مهماً في الأمان عبر الإنترنت. من الضروري اختيار متصفح آمن من حيث الحماية من السرقة أو انتهاكات خصوصية البيانات.

تتضمن المتصفحات التي تعتبر آمنة وقت النشر ما يلي:

يعد متصفح Tor المتوفر على أجهزة الكمبيوتر وهواتف (Android) أحد أفضل المتصفحات المتاحة للحفاظ على الأمان والخصوصية وإخفاء الهوية. قد يختار النشطاء والصحفيون الذين يعملون في بيئات بها مخاطر أمنية، كما هو الحال في العراق، استخدام Tor بسبب أمانه المشددة.

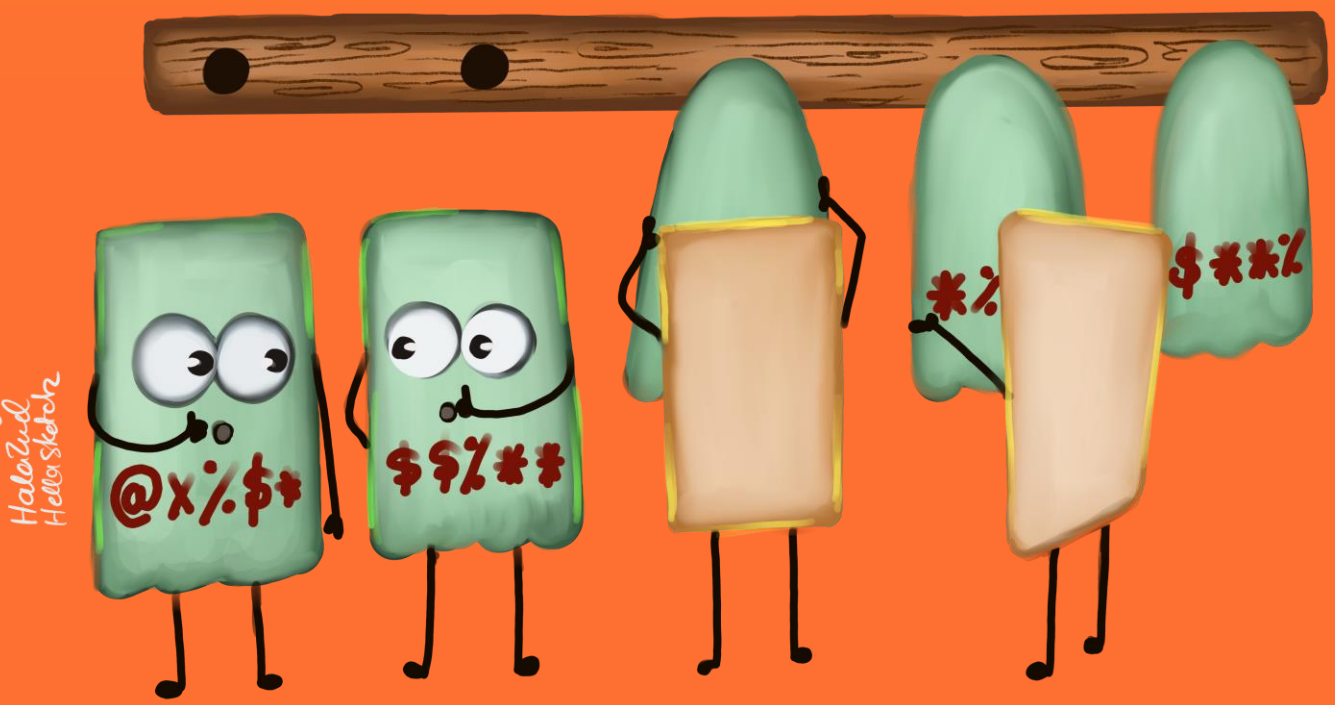
تتضمن المتصفحات الأخرى التي تعتبر آمنة وقت النشر ما يلي:

- HTTPS Everywhere
- Virus Total
- Ghostery
- Malwarebytes
- Cookie AutoDelete
- NoScript
- Privacy Badger


Recommended
HTTPS Everywhere
by EFF Technologists
Encrypt the web! HTTPS Everywhere is a Firefox extension to protect your communications by enabling HTTPS encryption automatically on sites that are known to support it, even when you type URLs or follow links that omit the https: prefix.
Remove
Recommended
Privacy Badger
by EFF Technologists
Automatically learns to block invisible trackers.
Remove
Experimental
VT4Browsers
by VirusTotal Team
This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.
Learn more
Scan your downloads with VirusTotal before storing them, free and easy.
Remove
Recommended
NoScript Security Suite
by Giorgio Maone
The best security you can get in a web browser! Allow potentially malicious web content to run only from sites you trust. Protect yourself against XSS other web security exploits.
Add to Firefox
Malwarebytes Browser Guard
by Malwarebytes
This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing.
Learn more
Recommended
Cookie AutoDelete
by CAD Team
Control your cookies! This WebExtension is inspired by Self Destructing Cookies. When a tab closes, any cookies not being used are automatically deleted. Keep the ones you trust (forever/until restart) while deleting the rest. Containers Supported
Remove

06

كل شيء عن التشفير



كل شيء عن التشفير

ما هو "التشفير؟"

بشكل أساسي، التشفير هو عملية تحويل البيانات من تنسيق قابل للقراءة إلى رمز سري لا يمكن "إلغاء قفله" إلا من قبل المستخدمين الذين يمتلكون "المفتاح" السري أو كلمة المرور.

للتشفير ست فوائد:

- يساعد في الحفاظ على تكامل البيانات والخصوصية.
- يساعد المنظمات على الامتثال للوائح الخصوصية والأمن.
- يحمي البيانات لأنها تنتقل عبر الأجهزة.
- يساعد المنظمات على تأمين المكاتب.
- يحمي الملكية الفكرية.
- يحمي البيانات أثناء نقلها إلى التخزين السحابي.

يمكن استخدام التشفير من أجل:

1. حفظ الصور ومقاطع الفيديو والبيانات على الأجهزة.
2. مشاركة الملفات والمستندات.
3. إرسال رسائل البريد الإلكتروني بشكل خاص.
4. تخزين الملفات باستخدام الخدمات السحابية.
5. التواصل عبر الرسائل أو المكالمات.

تواصل بأمان

ما هو "الاتصال الآمن"؟

الاتصال الآمن هو عملية تشفير اتصالات المستخدم باستخدام واحد أو أكثر من بروتوكولات الأمان لضمان تدفق البيانات بين المرسل والمستلم دون الوصول إلى طرف ثالث. يعمل التشفير على تحويل النص العادي إلى نوع من الشفرات السرية لا يستطيع الآخرون قراءته، حتى لو اعترضوه قبل أن يصل إلى المستلمين المقصودين. عندما تصل الرسالة إلى مستلميها، سيستخدم كل من أجهزتهم مفتاحه الخاص لفك رموز المعلومات مرة أخرى إلى نص عادي يمكن قراءته.

إذا لم يتم تشفير الاتصال، يمكن للحكومات والمجموعات والأفراد ذوي الخلفيات التقنية الاستماع إلى الاتصال أو قراءته والوصول إلى محتواه واعتراضه وتعديله وزرع البرامج الضارة وفتح الأبواب الخلفية داخل النظام لنقل البيانات من وإلى الجهاز.

معايير الأمان

يوصى بالمعايير التالية لاختيار برامج وتطبيقات الاتصال، لضمان خلو الاتصالات من التنصت والتجسس والوصول غير المصرح به إلى المعلومات الشخصية.

- **يجب تشفير الاتصال بين المرسل والمتلقي**، باستخدام التشفير من طرف إلى طرف (E2EE)، حتى لا تتمكن الشركة أو مزود الخدمة من الوصول إلى محتوى الرسائل. يتم إصدار الرسائل من قبل المرسل مشفرة ولا يتم فك تشفيرها حتى تصل إلى جهاز المستلم.

- **لا يوجد تتبع**، مما يعني أن الشركة التي أنتجت التطبيق لا تتبع معلومات الاتصال أو تجمع بيانات المستخدم. تجمع معظم الشركات التجارية معلومات حول المستخدم وتبيعها لشركات أو دول أخرى، مثل شركات الإعلان والتسويق.

- **يجب أن يكون التطبيق أو البرنامج مفتوح المصدر**، كما تمت مناقشته أعلاه. توفر البرمجيات مفتوحة المصدر كود التطبيقات والبرامج للفنيين لتقييم واكتشاف نقاط الضعف. تسمح التعليمات البرمجية مفتوحة المصدر أيضاً بمراجعة ما إذا كانت الشركة المنتجة تجمع معلومات وبيانات المستخدم.

- **يجب أن تتوفر ميزة إخفاء الهوية**، مما يعني أن البرنامج أو التطبيق يمكنه إخفاء المعلومات الشخصية للمستخدم (الاسم ورقم الهاتف والبريد الإلكتروني والموقع الجغرافي ومعرف الجهاز) حتى أثناء إرسال واستقبال الرسائل والمكالمات الصوتية وإرسال واستقبال المرفقات (بما في ذلك doc. و pdf. و jpeg. و mp3. وما إلى ذلك).

يتساءل العديد من المستخدمين عما إذا كانت التطبيقات الشائعة، بما في ذلك Facebook Messenger و Viber و Telegram و WhatsApp وغيرها، تفي بالمعايير المذكورة أعلاه. تشير مراجعة تقارير الشفافية التي تنتجها الشركات بشكل دوري وتقييمات من قبل فنيي الأمن إلى أن هذه التطبيقات للأسف تلتزم ببعض المعايير المذكورة أعلاه، لكنها غالباً لا تلبيها جميعاً.

توصيات لتطبيقات الاتصالات الآمنة

- Wire: هذا التطبيق يفي بالمعايير المذكورة أعلاه، مع واجهة مستخدم سهلة. وهي متوفرة للهواتف وأجهزة الكمبيوتر. لا يلزم تثبيته كبرنامج أو تطبيق - يمكن استخدامه داخل المتصفح كملحق.
- Signal: يعتبر تطبيق Signal Private Messenger على نطاق واسع أحد أكثر التطبيقات أمانًا للحفاظ على الخصوصية ويلتزم بجميع المعايير المذكورة أعلاه باستثناء

واحد: إخفاء الهوية. يتطلب تطبيق Signal رقم هاتف لتنشيطه؛ ومع ذلك، لا يتتبع Signal المعلومات ولا يجمع معلومات المستخدمين.

- Jitsi: جيتسي ميت هي منصة لإجراء الاتصالات أو عقد اجتماعات عبر الإنترنت. وتتمثل ميزته مقارنة ببرامج الاجتماعات الأخرى المستندة إلى الويب في أنه ينشئ قناة مشفرة للاتصالات، ويحافظ على إخفاء الهوية. ليس من الضروري إنشاء حساب أو إدخال أي تفاصيل شخصية. يمكن للمستخدمين زيارة موقع الويب عبر متصفح، وفتح محادثة، ومشاركة الرابط مع أي شخص يريدون دعوته إلى المحادثة. يمكن تثبيت تطبيق جيتسي على أجهزة الكمبيوتر والهواتف المحمولة.
- OnionShare: لإرسال ملفات ومعلومات كبيرة أو حساسة إلى الأشخاص أو المؤسسات أو منظمات المجتمع المدني، فإن أفضل خيار هو استخدام OnionShare. يستخدم OnionShare خاصية Onion Routing "التوجيه البصلي" في شبكة Tor لنقل المعلومات، مما يجعله آمن جداً ومثالي للمدافعين عن حقوق الإنسان. يحتوي OnionShare على واجهة بسيطة وسهلة الاستخدام، مع إصدارات متعددة لأنظمة تشغيل ويندوز و Mac و Linux. يشتمل البرنامج أيضاً على منصة دردشة تدعم إخفاء الهوية.
- Tresorit: تقوم هذه الخدمة أيضاً بتشفير المعلومات من طرف إلى طرف. وتحتوي على واجهة بسيطة وتحافظ على أمان المعلومات وتشفيرها أثناء الإرسال.

كيفية إرسال رسائل بريد إلكتروني آمنة (مشفرة) باستخدام PGP

أفضل طريقة لضمان أمان رسائل البريد الإلكتروني هي تشفيرها باستخدام "PGP" وتعني PGP "خصوصية جيدة جداً". وهو نظام تشفير يستخدم لإرسال رسائل بريد إلكتروني مشفرة وتشفير الملفات الحساسة. يقوم PGP بتشفير رسائل البريد الإلكتروني ومرفقاتها لزيادة سرية الاتصال عن طريق إنشاء زوج من المفاتيح الخاصة والعامة اللازمة "لفتح" المعلومات.

لسوء الحظ، فإن ما يسمى بأنظمة البريد الإلكتروني "الآمنة" الشائعة، لا تستخدم التشفير الكامل من طرف إلى طرف، وبالتالي يمكن أن تعرض المستخدم للمخاطر. يوصي الخبراء دائمًا باستخدام تشفير PGP لرسائل البريد الإلكتروني، واستخدام مثل ProtonMail و Tutanota من الخيارات الممتازة.

ملاحظة: لا يمكن استخدام PGP إلا عندما يستخدم كل من المرسل والمتلقي تطبيقات أو برامج مخصصة لتشفير وفك تشفير الرسائل. هناك العديد من البرامج والتطبيقات التي تستخدم معيار OpenPGP، لذلك لا يحتاج كل مستخدم إلى استخدام نفس البرنامج تماماً؛ ومع ذلك، يجب أن تكون مجهزة "لتبادل المفاتيح." تواصل مع جهات الاتصال حول أفضل طريقة لإنشاء اتصالات آمنة قبل محاولة إرسال رسائل بريد إلكتروني مشفرة.

Mailvelope هو برنامج موصى به يمكن استخدامه مع موفري بريد الويب المشهورين مثل Hotmail و Outlook و Gmail و Yahoo. ويمكن إضافته كملحق لمتصفحات مثل Google Chrome و Firefox. يقوم بإنشاء زوج المفاتيح العام والخاص الضروري، ثم يشارك المفتاح العام مع مستخدمين آخرين لإضافته.

ب. احفظ المعلومات وقم بخزنها بشكل آمن

لا يجب على المستخدمين تشفير المعلومات التي يشاركونها مع الآخرين فحسب، بل يجب عليهم أيضاً تشفير معلوماتهم الخاصة لتخزينها بشكل آمن. يوفر هذا القسم دليلاً للطرق المختلفة التي يمكن من خلالها استخدام التشفير لتخزين البيانات على أجهزة المستخدم وفي السحابة.

حفظ الصور ومقاطع الفيديو والبيانات على جهاز:

يعد Tella مثالاً لتطبيق يساعد في الحفاظ على البيانات أكثر أماناً. يتم استخدامه من قبل النشطاء والمدافعين عن حقوق الإنسان ومنظمات المجتمع المدني ووسائل الإعلام والمتخصصين في العمل الإنساني والتوثيق. إنه متاح حالياً لأجهزة Android فقط، ولكن إصدار iOS قيد التطوير.

- هو سهل الاستخدام، بواجهة بسيطة.
- يقوم المستخدمون بقفل التطبيق عبر "طريقة النمط" عن طريق إنشاء شكل.
- يمكن للمستخدمين تغيير ايقونة التطبيق وبالتالي لا يمكن التعرف عليه.
- يتميز بخاصية "الحذف السريع" لمسح البيانات في حالة تعرض المستخدم لخطر الاستيلاء على هاتفه.
- يمكن حذف التطبيق نفسه نهائيًا في حالات الخطر المباشر.

تشفير الملفات وتخزينها باستخدام الخدمات السحابية:

على الرغم من أن العديد من الأشخاص يقومون بحفظ ملفاتهم الحساسة وتخزينها على أجهزة الكمبيوتر الخاصة بهم أو في محركات أقراص صلبة خارجية (دون تشفيرها)، فإن هذا الأسلوب ينطوي على مخاطرة. في حالة حدوث وصول غير مصرح به، يمكن الاستيلاء على هذه الأجهزة وفك تشفيرها، أو يمكن للأفراد إجبار المستخدم على فتح التشفير.

من المهم جداً عدم ترك معلومات حساسة على الأجهزة، لأن هذا قد يعرض المستخدم للخطر سواء عبر الإنترنت أو في وضع عدم الاتصال. يضمن تخزين المعلومات بأمان في السحابة عدم تمكن الجهات الخارجية غير المصرح لها من الوصول إلى المعلومات الحساسة. يجب على المستخدمين تجنب ترك آثار البيانات على الأجهزة التي قد تسبب مشاكل أمنية.

"الخدمات السحابية" هي منصات أو برامج بنية تحتية يستضيفها موفرو الطرف الثالث ويتم إتاحتها للمستخدمين عبر الإنترنت. يوصى بالخدمات السحابية الآمنة التالية لتخزين المعلومات الحساسة دون ترك آثار مادية:

- Mega
- pCloud

ومع ذلك، فانه لا يزال من المهم تشفير البيانات قبل تحميلها على السحابة.

برامج التشفير:

VeraCrypt : في وقت النشر، يعتبر VeraCrypt برنامجاً آمناً مفتوح المصدر يقوم بتشفير البيانات وحفظ الملفات على كمبيوتر المستخدم. يمكن للمستخدم فقط عرض البيانات باستخدام مفتاح لفك تشفيرها. يمكن لـ VeraCrypt تشفير البيانات والملفات والمجلدات، ولكن يمكنه أيضاً تشفير وحدات التخزين الخارجية بالكامل مثل محركات أقراص USB المحمولة أو محركات الأقراص الثابتة أو أجزاء من محركات الأقراص الثابتة. يمكن استخدامه على أنظمة ويندوز و Mac و Linux.

07

محو البيانات بأمان

محو البيانات بأمان

عندما يقوم المستخدم "بحذف" البيانات من جهاز كمبيوتر أو هاتف ذكي أو كاميرا رقمية أو جهاز آخر، فإن البيانات لا يتم إتلافها فعلياً. يؤدي الحذف ببساطة إلى "إخفاء" البيانات عن المستخدم ولكنه لا يمحيها من الجهاز.

يصف هذا القسم كيفية محو البيانات بشكل آمن ودائم، ويغطي المصطلحات الأساسية المرتبطة بفحص الأمان، وكيفية إجراء العملية، والبرامج والتطبيقات الآمنة التي يمكن استخدامها لمحو المعلومات بحيث لا يمكن استعادتها.

من المهم فهم الفرق بين هذه المصطلحات الأساسية:

طمس المعلومات Wipe

عندما تطمس قرصًا صلبًا أو أي جهاز تخزين آخر، فإنك تمسح كل شيء موجود عليه حاليًا، بالإضافة إلى أي شيء قمت بحذفه مسبقًا والذي قد لا يزال موجودًا.

مزق المعلومات اربا اربا Shred

عندما تقوم بتمزيق جزء من البيانات، عادة ما يكون ملفًا أو مجلدًا واحدًا أو أكثر ، فإنك تمسح كل ما حددته ، وفقط تلك العناصر.

بعبارات أخرى:

حذف: "أخفيني ، ولكن سأكون هنا إذا كنت تريد استعادتي حقاً"

محو: "هل أنت متأكد؟ لن تراني مرة أخرى"!

إزالة: "سأقوم بمسح كل شيء"

تقطيع: "سأمسح هذا وهذا فقط"

الأسئلة الشائعة :

هل يعني حذف الملفات من سطح المكتب وإفراغ "سلة المهملات" أن الملفات تتم إزالتها نهائياً وبشكل لا رجعة فيه من الكمبيوتر أو الهاتف الذكي؟

كلا. يؤدي حذف البيانات وإفراغ سلة المهملات إلى تحديد المساحة على أنها "متوفرة،" ولكن حتى تتم الكتابة فوق "المساحة المتاحة" بمعلومات جديدة، فلا يزال من الممكن استعادة البيانات الأساسية.

هل تؤدي إعادة تهيئة محرك الأقراص الثابتة إلى إزالة البيانات بشكل دائم ولا رجعة فيه؟

كلا. تعد إعادة التنسيق طريقة رائعة "لحذف" البيانات - وليس "محوها!" تحدد عملية إعادة التهيئة كل المساحة الموجودة على الجهاز على أنها "متوفرة؛" ومع ذلك، لا يزال من الممكن استعادة البيانات الأساسية حتى تتم كتابتها بمعلومات جديدة. هذه عملية مقبولة إذا كان المستخدم نفسه يخطط لإعادة استخدام محرك الأقراص، ولكنه لا يلغي المعلومات الحساسة تلقائياً.

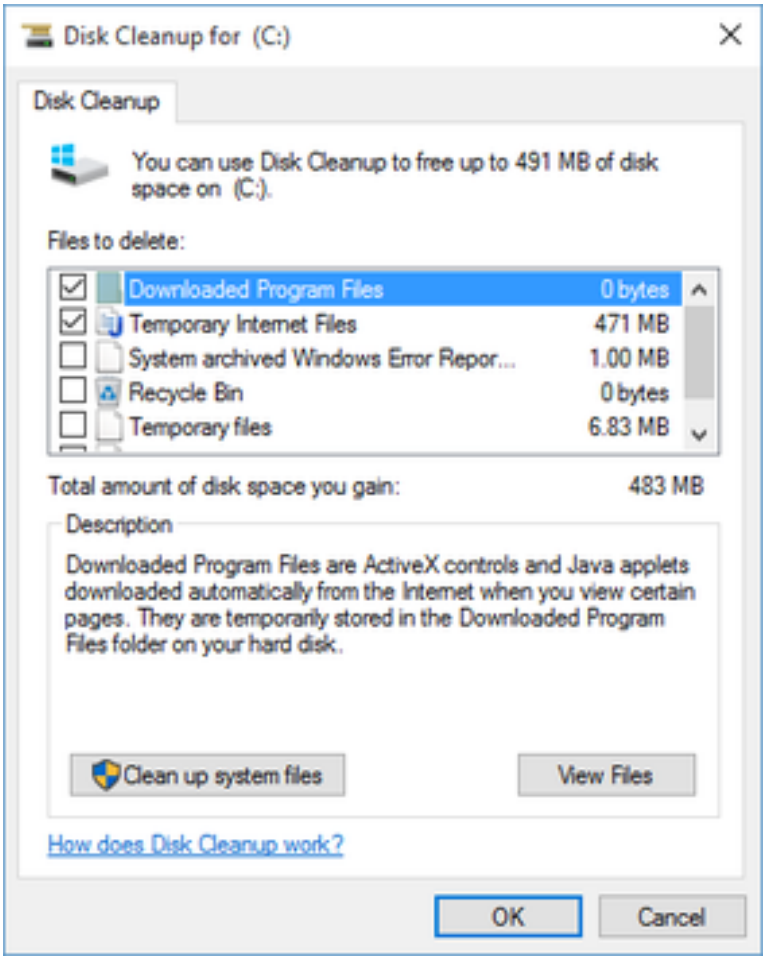
تتحسن تقنيات استعادة الملفات المحذوفة كل يوم، ويمكن استرداد العديد من أنواع الملفات التي من المفترض أنها "محذوفة" (الصور والمستندات ومقاطع الفيديو وما إلى ذلك). يضمن مسح القرص أو تمزيقه أن المساحة "المتاحة" التي تم إنشاؤها عن طريق الحذف البسيط قد تم استبدالها، مما يجعل البيانات الأساسية غير قابلة للاسترداد.

من أكثر الأخطاء شيوعاً في العراق بيع الأجهزة المستعملة لطرف آخر دون مسح البيانات الأساسية بالكامل. وقد تسبب هذا في العديد من المشكلات والدعاوى القضائية عندما تم استرداد معلومات يعتقد المستخدم السابق أنه تم محوها. أفضل نصيحة هي عدم شراء أو بيع الأجهزة المستعملة.

كيفية تنظيف الأجهزة:

لتنظيف جهاز كمبيوتر يعمل بنظام ويندوز (حذف الملفات المؤقتة وتنظيف ملفات النظام)، استخدم أداة تنظيف القرص **Disk Cleanup tool** الخاصة بالنظام على النحو التالي:

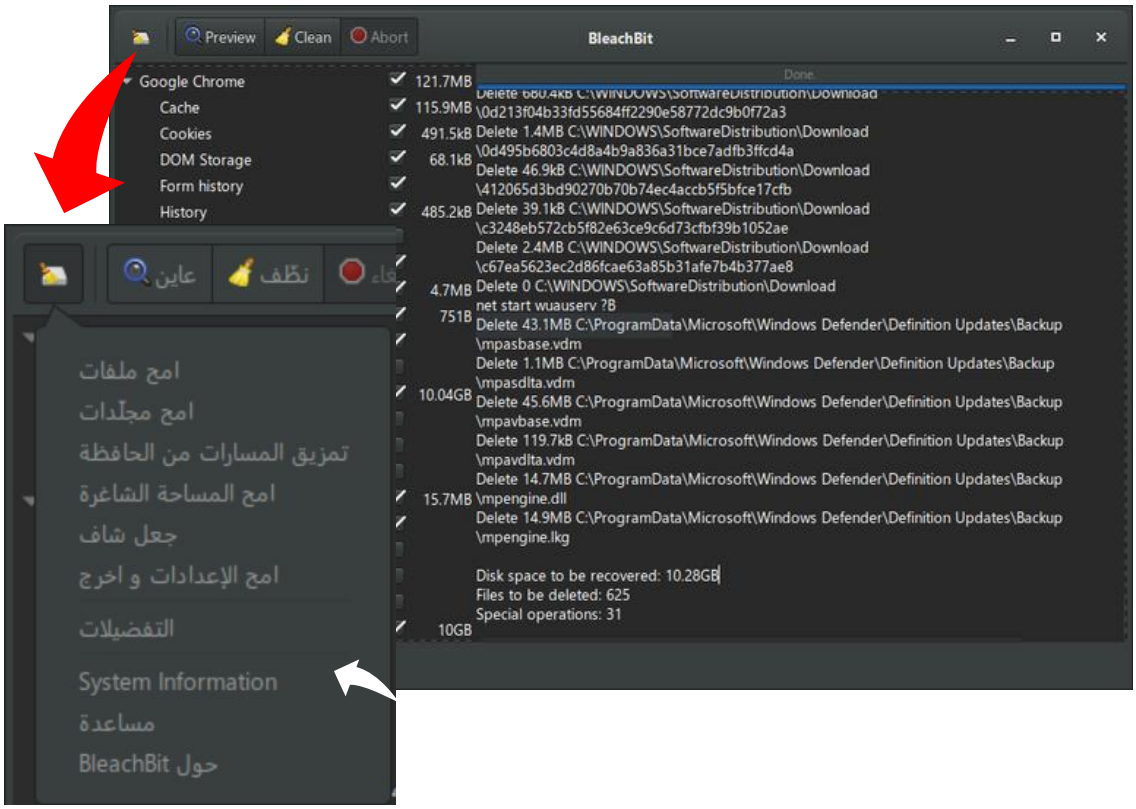
- انتقل إلى قائمة **ابدأ Start Menu** ، ثم جميع البرامج **All Programs** ، ثم أدوات النظام **System Tools** ، ثم حدد " تنظيف القرص **Disk Cleanup** " (أو اكتب "تنظيف القرص" في مربع البحث، والذي سيفتح موقع التطبيق).



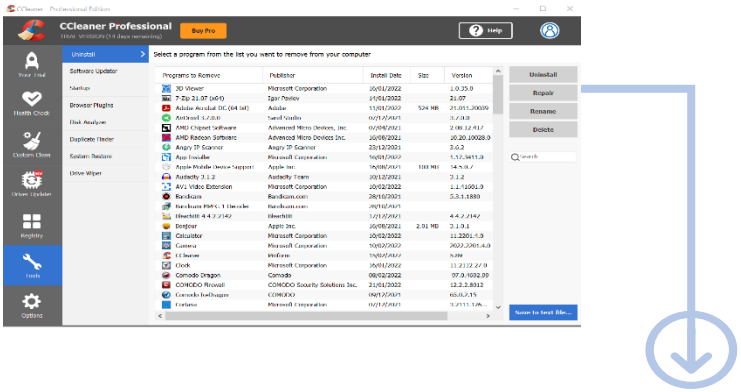
كيفية محو البيانات أو مسحها نهائياً:

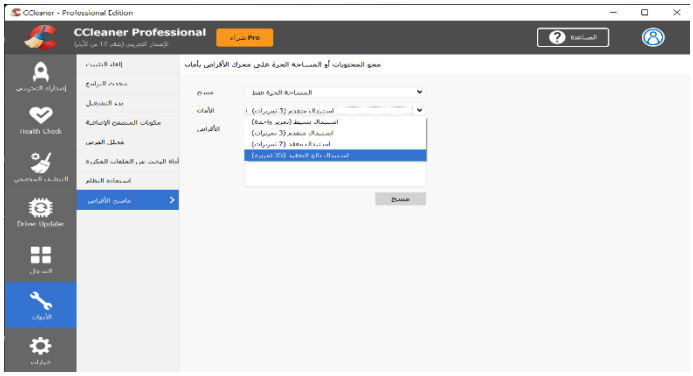
يتضمن أحد أهم أجزاء محو البيانات محو الطبقات الأساسية من المعلومات والكتابة عليها ببيانات جديدة. هذا يمنع إمكانية استعادة البيانات بشكل دائم.

BleachBit : يمكن استخدام هذا البرنامج المجاني مفتوح المصدر على أجهزة ويندوز و Linux لمحو الملفات والمجلدات والمساحة الخالية ومحو الإعدادات وتقطيع المسارات من الحافظة.

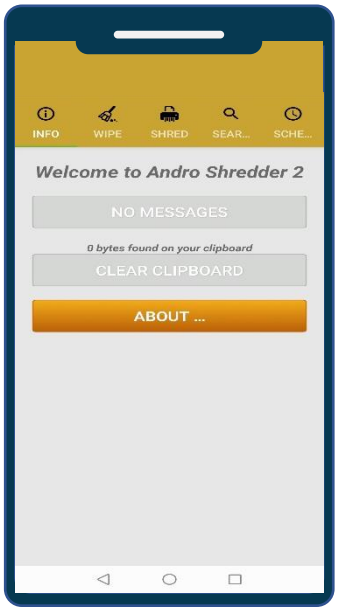


CCleaner برنامج لإزالة ومحو المعلومات. يمكن أن يوفر حماية الخصوصية القياسية والتنظيف القياسي والتحديثات المنتظمة للنظام والبرامج وإجراء فحوصات صحة الكمبيوتر وتنظيف سجل التصفح والحفاظ على خصوصيته ويكشف ويزيل متتبعات الإنترنت ويمنع الجهاز من نفاذ المساحة.





Andro Shredder : تطبيق لهواتف Android لمحو المعلومات وتقطيعها ومسحها وتحرير مساحة.



08

منع التصيد الاحتيالي

منع التصيد الاحتيالي

"التصيد الاحتيالي،" المعروف أيضاً باسم الاحتيال الإلكتروني أو الإغراء الإلكتروني أو السرقة الإلكترونية، هو عبارة عن مجموعة من التكتيكات والتقنيات المستخدمة لسرقة أو الحصول على المعلومات الشخصية وكلمات المرور والمعلومات التجارية والحسابات المالية وما إلى ذلك.
يعد التصيد الاحتيالي أحد أكثر الطرق شيوعاً لاستهداف المستخدمين، كما أن منع التصيد الاحتيالي هو أحد أسهل الطرق التي يمكن للمستخدمين من خلالها حماية أنفسهم من أن يصبحوا ضحية.
بعبارات بسيطة، يستغل المهاجم المستخدم من خلال عملية خادعة أو يستخدم تقنيات الهندسة الاجتماعية لتشجيع الضحية أو إجبارها على الاستجابة لطلب المهاجم. عادة ما يتضمن الطلب إقناع المستخدم بما يلي:

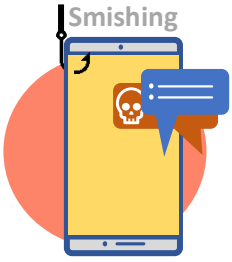
- انقر فوق الرابط
- تبادل المعلومات
- امنح أذونات
- تنزيل الملفات المصابة بالبرامج الضارة

عادة ما ينتظر المهاجم أن يرتكب الهدف خطأ، ثم يمكنه الحصول على معلومات الضحية والوصول إلى حساباته.
أنواع التصيد
هناك العديد من **أنواع التصيد الاحتيالي**، بما في ذلك:

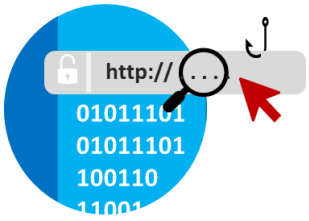
التصيد بالرمح Spear phishing: أسلوب متطور يستهدف شخصاً معيناً أو مجموعة معينة. يجمع المهاجم معلومات عن الضحية ثم يستخدمها لصياغة رسالة تبدو حقيقية. يتم إجراء هذا النوع من التصيد بشكل عام من خلال رسائل البريد الإلكتروني التي تستهدف الضحية.

صيد الحيتان Whaling: أسلوب التصيد بالرمح الذي يستهدف بشكل خاص الأشخاص المؤثرين والأقوياء داخل الشركات أو المنظمات.

تزوير العناوين Pharming: نوع من الاحتيال يقوم فيه المهاجم بتوجيه الضحية من موقع رئيسي / حسن السمعة إلى موقع مزيف آخر أو موقع تم اختراقه ببرامج ضارة. يمكن اعتراض معلومات الضحية عند دخوله الى الموقع.



تزوير الرسائل النصية Smishing: استخدام الرسائل النصية القصيرة للاحتيال على الضحية من خلال مطالبتهم بالكشف عن معلومات حول الحسابات أو الحصول على أرقام مصادقة متعددة العوامل أو تنزيل برامج ضارة على جهاز الضحية.



تصيد محرك البحث Search engine phishing: يقوم المهاجم بإنشاء موقع على شبكة الإنترنت، ويضعه على محركات البحث أو وسائل التواصل الاجتماعي، ويعرض السلع بأسعار رخيصة، مما يغري الضحية بالدفع مقابل منتج. ثم يُدخِل الضحية معلومات حسابه المصرفي لتتم سرقتها واستخدامها.

6. التصيد الصوتي Voice phishing: يستخدم المهاجم مكالمة هاتفية صوتية لخداع الضحية للاعتقاد بأن المتصل من جهة رسمية من أجل الحصول على المعلومات التي يريدها من الضحية.

كيف تحمي نفسك من التصيد الرقمي

يجب على جميع المستخدمين توخي الحذر الشديد واتباع هذه النصائح:

1- **لا تشارك أبداً معلومات حساسة أو شخصية مع الآخرين**، ولا تنشرها أبداً على وسائل التواصل الاجتماعي تحت أي ظرف من الظروف.

2- **لا تستجيب تحت أي ظرف من الظروف للتهديدات** التي تتلقاها عبر الرسائل أو رسائل البريد الإلكتروني أو مواقع التواصل الاجتماعي. لا تتفاعل بأي شكل من الأشكال مع المهددين.

3- **لا تفتح الروابط المستلمة**، حتى من جهات الاتصال القريبة، دون التحقق منها أولاً.

أ- استخدم Virus Total للتحقق من الروابط والملفات. لا تنقر على الروابط فور استلامها - انسخ الرابط وافتح الموقع والصق الرابط في نافذة "روابط URL" وانقر على "إدخال." إذا كانت النتيجة، فسيكون الرابط خالياً من البرامج الضارة. لا تنقر على الرابط مباشرة - انسخه والصقه في المتصفح. إذا كان الرابط عبارة عن رابط محتوى اعتيادي، فسيظهر المحتوى في المتصفح.

4- **تأكد من أن المواقع التي تدخل إليها بها شهادة أمان وأن الرابط يبدأ بـ ."https://" رمز القفل بجوار عنوان URL في شريط عنوان المتصفح يعني أن طبقة المقابس الآمنة** تحمي موقع الويب الذي يزوره المستخدم. تحافظ طبقة المقابس الآمنة على اتصالات الإنترنت آمنة وتمنع المستخدمين غير المصرح لهم من قراءة أو تعديل المعلومات المنقولة بين نظامين.

5- **تحقق من العنوان أو رقم الهاتف لرسائل البريد الإلكتروني والرسائل النصية القصيرة**. غالباً ما يخفي المهاجمون العناوين لجعلها تبدو مشابهة لجهات الاتصال ذات السمعة الطيبة، ولكن عند الفحص الدقيق، فإنها لا تتطابق مع موقع الويب أو الشخص الذي يتظاهرون به.

6- **جميع الخدمات التي اشتركت فيها لمعرفة اسمك،** وستتضمن اتصالاتها لك اسمك. أي رسالة تظهر على أنها "إلى مشتركنا العزيز" أو "عميلنا العزيز" أو ما شابه ذلك قد تكون رسالة احتيالية: احرص على التعامل معها.

7- **أي هدية أو جائزة تتلقاها تكون احتيالية إذا لم تكن قد شاركت في مسابقة أو مسابقة**. لا تتفاعل معها.

٨- **إذا تلقيت بريداً إلكترونياً أو أي اتصال آخر يطلب معلومات حساسة، فاتصل بالمرسل مباشرةً** عبر طريقة مختلفة للاستعلام عن الرسالة.

٩- **إحمِ الأجهزة ببرامج أمن الإنترنت وبرامج مكافحة البرامج الضارة،** ولا تقم بتثبيت البرامج المقرصنة.

١٠- قم **بتمكين التحقق من خطوتين** على جميع الحسابات.

09

المراجع وقراءات أخرى

لمزيد من المعلومات والموارد والتحديثات الجارية، راجع الموارد التالية:

1. **الحماية الرقمية** (عربي) - معلومات أمنية وأدلة تدريبية وأدوات موصى بها باللغة العربية.
2. **Security-in-a-Box** (باللغتين العربية والإنجليزية) - معلومات حول الأمن الرقمي وأدلة تدريبية وموارد الأخرى.
3. **FrontLine Defenders** (باللغتين العربية والإنجليزية) - معلومات ودعم بشأن المخاطر الرقمية وغيرها من المخاطر الأمنية للمدافعين عن حقوق الإنسان.
4. **سلامة تك** (عربي) - أخبار الأمن الرقمي، مصادر التعلم الذاتي، الدعم الفني، التدريب والمساعدة العاجلة.
5. **لجنة حماية الصحفيين** (عربي وإنجليزي) - حقيبة السلامة الرقمية للصحفيين.
6. **الدفاع عن النفس ضد المراقبة** (باللغتين العربية والإنجليزية): نصائح وأدوات وإرشادات لاتصالات أكثر أماناً عبر الإنترنت، تديرها مؤسسة Electronic Frontier Foundation.
7. **Cyber Kurds** (باللغة الكردية) - معلومات باللغة الكردية عن الأمن الرقمي.
8. **Rory Peck Trust** (باللغتين العربية والإنجليزية) - منظمة غير حكومية مكرسة لسلامة ودعم ورفاهية الصحفيين المستقلين.
9. **Safe Sisters** (الإنجليزية) - برنامج زمالة وموارد تستهدف بشكل خاص المدافعات عن حقوق الإنسان والصحفيات أو العاملات في مجال الإعلام والناشطات للتدريب على تحديات الأمن الرقمي.

10

مسرد مصطلحات
الأمن السيبراني

مسرد مصطلحات الأمن السيبراني

ما لم يُذكر خلاف ذلك، يمكن العثور على التعريفات الواردة أدناه في قاعدة بيانات مصطلحات الأمم المتحدة (UNTERM)، المتاحة هنا.

- **برامج الإعلانات المتسللة:** نوع من تطبيقات البرامج التي تعرض إعلانات من نوع ما أثناء تشغيلها. في بعض الأحيان، سيقدم المطورون نسخة "مجانية" من برامجهم بشرط أن يكون عليك مشاهدة الإعلانات، ويتقاضون أجراً من خلال عدد الأشخاص الذين ينقرون على الإعلانات. غالباً ما توجد أيضاً نسخة مدفوعة من نفس البرنامج خالية من الإعلانات.
- **ذاكرة التخزين المؤقت:** منطقة تخزين مؤقتة حيث يمكن تخزين البيانات التي يتم الوصول إليها بشكل متكرر للوصول السريع.
- **برنامج مقرصن**: "الكراك" هو برنامج مصمم لتنشيط أو تسجيل أو تمديد الفترة التجريبية لبرنامج احتكاري يتطلب عادةً رقماً تسلسلياً لمنع القرصنة والاستخدام غير المصرح به. دائماً ما يكون استخدام "الكراك" للوصول إلى البرامج أمراً غير قانوني[5].
- **تقنية التشفير:** تمكن المستخدم من حماية البيانات المحفوظة على محركات أقراص USB أو الأجهزة المحمولة أو أقراص الفلاش أو محركات القلم أو الأقراص المضغوطة أو الأقراص الثابتة. لا يمكن قراءة المستند المشفر أو عرضه من قبل المستلمين غير المقصودين، حتى لو كان لديهم المستند نفسه.
- **التشفير من طرف إلى طرف (E2EE):** تطبيق التشفير على أدوات وخدمات الاتصال، بحيث لا يتمكن سوى مستخدمي الأداة أو الخدمة من الوصول إلى الرسائل ذات النص العادي. يتم نشر العديد من أشكال التشفير من قبل موفري الخدمة لتأمين الاتصالات بطريقة تمنع وصول طرف ثالث غير مصرح به، ولكن لا يزال بإمكان مزود الخدمة الذي يقوم بتطبيقه الوصول إلى بيانات المستخدم ذات الصلة.

[5] انظر قرصنة البرامج - ويكيبيديا

- **جدار الحماية:** جدار الحماية هو نظام مصمم لمنع الوصول غير المصرح به إلى شبكة خاصة أو منها. يمكن تنفيذ جدران الحماية في كل من الأجهزة والبرامج، أو مزيج من كليهما.
- **عنوان IP**: رقم فريد تستخدمه أجهزة تقنية المعلومات للتعرف والتواصل مع بعضها البعض على شبكة الكمبيوتر باستخدام معيار بروتوكول الإنترنت (IP). أي جهاز يشارك في الشبكة - على سبيل المثال أجهزة التوجيه وأجهزة الكمبيوتر والطابعات وأجهزة الفاكس عبر الإنترنت - يجب أن يكون له عنوان فريد خاص به. يمكن اعتباره معادلاً لعنوان شارع أو رقم هاتف لجهاز كمبيوتر أو جهاز شبكة آخر على الإنترنت. مثلما يحدد كل عنوان شارع ورقم هاتف بشكل فريد مبنى أو هاتف، يمكن لعنوان IP أن يحدد بشكل فريد جهاز كمبيوتر معين أو جهاز شبكة آخر على الشبكة.
- **Keylogger:** أداة تسجل نشاط المستخدم، مثل ضغطات المفاتيح، ويمكنها إرسال هذه المعلومات إلى مهاجم باستخدام البريد الإلكتروني أو طرق أخرى.
- **البرامج الضارة:** برامج مصممة لاختراق نظام الكمبيوتر أو إتلافه دون موافقة مستنيرة من المالك. يعتبر البرنامج برنامجاً ضاراً استناداً إلى النية المتصورة لمنشئ المحتوى بدلاً من أي ميزات معينة. ويشمل فيروسات الكمبيوتر والديدان وأحصنة طروادة وبرامج التجسس والبرامج الإعلانية غير النزيهة وغيرها من البرامج الضارة وغير المرغوب فيها. وهي مزيج من الكلمتين "برمجيات" و "ضارة".
- **توجيه البصلة:** الأساس التكنولوجي لشبكة Tor. الاسم مشتق من البنية الشبيهة بالبصل لنظام التشفير المستخدم، والذي يتم تأمينه عدة مرات عبر عدة طبقات. الهدف من توجيه البصل هو استخدام الإنترنت بأكبر قدر ممكن من الخصوصية، وتوجيه حركة المرور عبر خوادم متعددة وتشفيرها في كل خطوة6.

[6] لمزيد من المعلومات، راجع مشروع Tor على https://www.torproject.org

- **البرمجيات مفتوحة المصدر:** هذا مصطلح عام للبرامج (التطبيقات وبرامج النظام) حيث تكون شفرة المصدر متاحة بشكل مفتوح لأي مستخدم؛ برنامج يمكن استخدامه ونسخه ودراسته وتعديله وإعادة توزيعه دون قيود.
- **PGP:** يرمز PGP إلى "Pretty Good Privacy" أو "خصوصية جيدة جداً،" وهو برنامج لتشفير مفتاح عام غير متماثل قادر على ضمان سرية ومصداقية الاتصالات الإلكترونية.
- **التصيد الاحتيالي:** تكتيك لارتكاب الاحتيال عبر الإنترنت وسرقة الهوية. على سبيل المثال، يرسل "المحتال" بريداً إلكترونياً يمثل طلباً تجارياً مشروعاً - على سبيل المثال، من أحد البنوك يطلب من العملاء التحقق من البيانات المالية. يتضمن البريد الإلكتروني رابطاً يزعم أنه ينتقل إلى موقع ويب مصرفي شرعي. ومع ذلك، فإن الموقع مزيف وعندما يكتب الضحية أرقام الحسابات أو كلمات المرور أو غيرها من المعلومات الحساسة، يتم التقاط هذه البيانات واستخدامها لاحقاً من قبل المخادع لارتكاب الاحتيال.
- **برامج الفدية:** نوع من البرامج المصممة للوصول إلى نظام الكمبيوتر حتى يتم دفع مبلغ من المال. تقوم بعض أشكال برامج الفدية بتشفير الملفات على محرك الأقراص الثابتة (المعروف أيضاً باسم الابتزاز الفيروسي المشفر)، بينما قد بعضها بإغلاق النظام ببساطة وعرض الرسائل التي تقوم بإقناع الضحية بالدفع.
- **برامج التجسس:** برامج الكمبيوتر التي تجمع معلومات شخصية عن المستخدمين دون موافقتهم المستنيرة. يتم تسجيل المعلومات الشخصية سراً باستخدام مجموعة متنوعة من التقنيات، بما في ذلك تسجيل ضغطات المفاتيح وتسجيل محفوظات تصفح الويب على الإنترنت ومسح المستندات ضوئياً على القرص الصلب للكمبيوتر.
- **حصان طروادة:** برنامج يبدو شرعياً ولكنه يقوم ببعض الأنشطة غير المشروعة عند تشغيله. يمكن استخدامه لتحديد موقع معلومات كلمة المرور أو جعل النظام أكثر عرضة للإدخال المستقبلي أو ببساطة تدمير البرامج والبيانات المخزنة للمستخدم. حصان طروادة يشبه الفيروس، إلا أنه لا يكرر نفسه.

- **VPN:** "الشبكة الخاصة الافتراضية" هي شبكة توفر مساراً خاضعاً للرقابة عبر الإنترنت لا يمكن الوصول إليه إلا للمستخدمين المصرح لهم، والتي يمكن أن تنتقل عبرها البيانات المصرح بها فقط.
- **الديدان:** مصطلح كمبيوتر يشير إلى البرامج الطفيلية الخبيثة، المشابهة للفيروسات، والتي تتكاثر وتنتشر عبر الشبكات بحثاً عن الأجهزة المعرضة للإصابة. على عكس الفيروسات، لا تصيب الفيروسات المتنقلة ملفات برامج الكمبيوتر الأخرى. يمكن للديدان إنشاء نسخ على نفس الكمبيوتر، أو يمكنها إرسال النسخ إلى أجهزة كمبيوتر أخرى عبر الشبكة.

فريق العمل

حيدر حمزوز	المنسق العام
آسو وهاب	الإعداد والتصميم البصري
هالة زياد	الرسومات
محمد عبدالله	المراجع اللغوي للنص العربي

Human Rights Office
United Nation Assistance Mission for Iraq
(UNAMI)
بعثة الأمم المتحدة لمساعدة العراق
(يونامي)

INSM
الشبكة العراقية
للإعلام المجتمعي

الحماية عبر الإنترنت والأمن الرقمي

دليل المستخدم للمدافعين عن حقوق الإنسان

2022