# تكلّم بأمان

# SpeakSafe

كتيّب للعاملين في مجال الإعلام
من أجل استخدام الإنترنت والهاتف الجوال بأمان

Media Workers' Toolkit for
Safer Online and Mobile Practices

Internews
Local voices. Global change.

تُرجِم هذا الدليل ونُشِر بإذنٍ من المؤلف والناشر.

جميع حقوق الطبع والنشر الخاصة بالنسخة الإنكليزية محفوظة لمنظمة «إنترنيوز» (Internews).
جميع حقوق الطبع والنشر الخاصة بالنسخة العربية محفوظة للمعهد الديمقراطي الوطني (NDI) ومنظمة «إنترنيوز» (Internews).

لا يجوز نشر أيّ جزء من هذا الكتاب، أو اختزال مادته بطريقة الاسترجاع، أو نقله في أي شكل من الأشكال أو بأية وسيلة من الوسائل، سواء كانت إلكترونية أو ميكانيكية أو بالتصوير أو بالتسجيل أو خلاف ذلك، إلا بإذن خطي مسبق من الناشر.

صدرت النسخة العربية في لبنان، ٢٠١٣.

لمزيد من المعلومات، يُرجى الاتصال بالمعهد الديمقراطي الوطني على العنوان:

Massachusetts, NW 455
Washington, DC 20001
الهاتف: 5500-728-202
الفاكس: 5520-728-202
الموقع الالكتروني: www.ndi.org

المعهد الديمقراطي الوطني للشؤون الدولية (NDI) هو منظمة غير ربحية، تعمل في سبيل توطيد الديمقراطية ونشرها على نطاق واسع في العالم. يوفر المعهدُ المساعدةَ العملية للقادة المدنيين والسياسيين، من أجل تنمية القيم والممارسات والمؤسسات الديمقراطية، مستعيناً بشبكة عالمية من الخبراء المتطوعين. ويتعاون أيضاً مع دعاة الديمقراطية في كل أنحاء العالم، بهدف بناء المنظمات السياسية والمدنية، وصون نزاهة الانتخابات، بالإضافة إلى توسيع مشاركة المواطنين، وتعزيز الشفافية والمساءلة في مؤسسات الحكم.

ترجمة ناتالي سليمان، تصميم طباعي مارك رشدان.

الرجاء إرسال أي تعليق أو سؤال حول ترجمة هذا الكتاب إلى البريد الإلكتروني: arabicpublications@ndi.org

## كلمة شكر وتقدير

تُحدِث الأدوات الرقمية والإلكترونية تغييرات جذرية في طريقة عمل الإعلاميين، مواطنين ومحترفين، للحصول على المعلومات، واستخدامها، وإنتاجها، وتبادلها. أكان الصحافيون ومنتجو المواد الإعلامية يبحثون عن الأخبار باستخدام جهاز كمبيوتر مشترك ضمن مكاتب التحرير على طول الحدود الباكستانية-الأفغانية، أو يتحادثون عبر الخليوي مع أحد معارفهم في مخيّمات اللاجئين في أفريقيا، فلا يكفي أن يحسنوا استخدام هذه الأجهزة وحسب، بل يجب أن يعرفوا كيف يحمون أنفسهم ومصادر المعلومات التي يستندون إليها.

يتوجّه مشروع «تكلّم بأمان» إلى الصحافيين والإعلاميين العاملين في قطاع المعلومات. وقد تيسّر إنتاجه بفضل برنامج «إنترنيوز» العالمي لحقوق الإنسان، الذي يعمل على تعزيز قدرة الإعلاميين على الإخبار بأمانٍ عن قضايا حقوق الإنسان.

إعداد وإنتاج: مانيشا آرييل
بحث وتأليف: سام تانيسون
تدقيق: جيني هولم
رسومات وصور: آشلي لوو
تصميم طباعي: شركة سيترين سكاي ديزاين Citrine Sky Design
تنسيق الإنتاج: إيريكا هاجر

تشكر منظمة «إنترنيوز» كريستين باتش على النصائح التي قدّمتها حول محتوى الكتيّب، وجوش ماكليدر وسفلتانا كيمايفا ودجاميليا عبد الرحمانوفا على الدعم المعنوي والإداري الذي قدّموه، إضافة إلى دعم البرنامج في مرحلة إنتاج الكتيّب.

ساهم في تنقيح هذا الكتيّب مستشارو الإبداع والابتكار والفريق التقني في المنظمة. كما تشاورنا حوله مع عددٍ من مدراء البرامج في البلدان التي تعمل فيها إنترنيوز، ومع منظمات شريكة من كل أقطار العالم، تتشارك معها المهمة ذاتها. فلا تزال جهودكم وخبراتكم وتعاليمكم وآراؤكم تغني عمل المنظمة، التي تشكركم جميعاً على دعمكم لها.

صحيحٌ أنّ مشروع «تكلّم بأمان» يعود إلى منظمة إنترنيوز، ولكنه يستند إلى جملة مواد تعليمية وتدريبية من إنتاج منظمات تعمل في مجال أمن الهاتف الجوّال والإنترنت، والأمن الرقمي، وشؤون الإعلام وحقوق الإنسان. لقد أوردنا قائمة بالروابط التي تقود إلى هذه الموارد ضمن الفصل الذي يحمل عنوان «روابط الأمن الرقمي». أما هذا الكتيّب، فيتوافر عبر الموقع الإلكتروني: www.speaksafe.internews.org

**حقوق الطبع والنشر لمنظمة "إنترنيوز"، ٢٠١٢**
يخضع هذا الكتيّب لرخصة المشاع الإبداعي للمصنَّفات الفكرية غير التجارية، الإصدار (CC BY-NC 3.0)، التي تجيز استخدام وتبادل الكتيّب لأغراض تعليمية، غير تجارية، وغير ربحية، على أن يُنسَب إلى «إنرتنيوز». يحقّ لمستخدميه أن يقوموا بتعديل محتوياته أو نشرها ضمن الشروط المنصوص عليها في الرخصة.

يصلح اعتماد هذا الكتيّب كمرجع، علماً أنّ المنظمة لا تتحمّل أي مسؤولية عن أمن وسلامة الأشخاص الذين يستخدمونه بصفتهم الشخصية أو المهنية.

Internews
Local voices. Global change.

# فهرس المحتويات

## ملاحظات

# المقدّمة

بات أسهل علينا اليوم، وأكثر من ذي قبل، أن نخبر الآخرين من نحن، وأين نتواجد، ومن نعرف. فقد ساهمت التكنولوجيا الرقمية في توسيع دائرة الأدوات المدرجة ضمن كتيّب العاملين في مجال الإعلام، مسهّلةً عمل الصحفي الاستقصائي، والمواطن المراسل، وسواهما من الأشخاص الذين ينقلون الأخبار والمعلومات. بتنا اليوم ننقل دفتر العناوين باستخدام بطاقة SIM، ونتواصل مع مصادر معلوماتنا باستخدام خدمة الرسائل القصيرة، ونبحث عن أخبارنا عبر محركات البحث ومواقع ويكي، ونجري مقابلات باستخدام خدمات الدردشة بالصوت والصورة، ونرسل تقاريرنا الإخبارية عبر البريد الإلكتروني، ونوصل أصواتنا كما أصوات الآخرين عبر المواقع الإلكترونية، وشبكات التواصل الاجتماعي، والمدونات.

لكنّنا قد نكشف معلومات عن أنفسنا أكثر من اللازم أو المراد. فلا يصعب إطلاقاً رصد محادثاتنا عبر الجوّال، ومكان وجودنا حينما نحمل هواتفنا؛ لا بل بإمكان العاملين لدى مزودي خدمة الإنترنت المحلية، أو لدى مقاهي الإنترنت التي نقصدها، الاطّلاع على مضمون الرسائل الإلكترونية التي نتبادلها عبر خدمات التواصل الشائعة، كخدمتي ياهو! أو هوتمايل. فضلاً عن ذلك، يسهل على الآخرين متابعة النشاطات التي نقوم بها عبر موقع فايسبوك أو أي مواقع إلكترونية أخرى، حينما نتصل بالشبكة اللاسلكية العامة عبر نقاط وصول غير مشفّرة.

صحيحٌ أنّ العصر الرقمي أدخل إلى حياتنا أدوات مبتكرة، تزيد من قدرتنا الإنتاجية، ولكنها تعرّضنا وتعرّض أعمالنا ومصادرنا، في المقابل، لمخاطر متزايدة.

لسنوات خَلَت، كان مفهوم أمن المعلومات يعني بالنسبة إلى الصحافيين اتخاذ بعض الخطوات للتأكّد من أنّ لا أحد يستمع إلى مخابراتهم الهاتفية. أما اليوم، وقد اعتمدنا الأدوات الرقمية لتحسين قدراتنا، فلا بد من التنبّه إلى التهديدات التي تواكبها على مستوى الخصوصية. ففي بعض البلدان، تطلب السلطات من مزودي خدمة الإنترنت حجب بعض المواقع الإلكترونية، وإطلاعها على سجّل محادثات المراسلين والمدونين، ورصد ما يُنشَر على شبكات التواصل الاجتماعي والمنتديات. وهكذا، أخذت برامج المراقبة تظهر على شكل ملفات مرفقة بالبريد الإلكتروني للوصول إلى أجهزة الكمبيوتر الخاصة وشبكات المكاتب.

ليست أعمال التنصّت حكراً على أهل السلطة وحسب، لأنّ عصابات الجريمة المنظّمة والقراصنة الذين يعملون لحسابهم الخاص يتسلّلون أيضاً إلى أجهزة الصحافيين، من خلال الشبكات اللاسلكية غير الآمنة وسواها من المواقع المضيفة. وفي مثال بارز ظهر مؤخّراً، كشف مات هونين، كاتب سابق لدى موقع جيزمودو ومجلة وايرد أنّ قراصنة استغلّوا سياسة استعادة كلمة السر الضعيفة لدى شركة آبل وموقع أمازون، من أجل الوصول إلى حسابات كانت موصولةً بأجهزته الخاصة، وعدة خدمات إلكترونية. فتمكّنوا، عن بعد، من حذف جميع البيانات المحفوظة في هاتفه الذكي، وجهازه اللوحي، وجهازه المحمول، وكذلك أي معلومات كان قد احتفظ بنسخة احتياطية عنها عبر الإنترنت. وقد فعلوا ذلك بعد أن نجحوا في اختراق حسابيه على موقعي جي مايل وتويتر. (يمكن الاطّلاع على ما جرى مع مات، في مجلة وايرد، حيث رواها بوضوح).

(ولهذه الغاية، ستُستخدم عبارة «قرصان الكمبيوتر» كثيراً للدلالة على شخص ينوى الإساءة إلى موقع إلكتروني، أو خدمة معيّنة، أو أي شخص. ولكننا لا ننكر في المقابل وجود عدد كبير من «القراصنة ذوي القبعات البيضاء»، وهم أشخاص لا يبغون إلا إتقان استخدام بعض التقنيات، موظّفين مهاراتهم ومعارفهم لمساعدة الآخرين. إنما، في الوقت الحاضر، تشير عبارة «قرصان الكمبيوتر» المتداولة عموماً في الصحف الشائعة إلى فئة «القبعات السوداء»، وهو المصطلح الذي تبّنيناه عرفاً وفقاً لمقتضيات هذا الكتيّب).

بصفتهم أشخاصاً يبحثون عن المعلومات، وينتجون مواد إعلامية حول قضايا اجتماعية وسياسية هامة، وينشرون وقائع وأفكاراً وآراء من خلال الوسائل الرقمية، من الضروري أن يكون الصحافيون والمدونون على معرفةٍ بالظروف الاجتماعية السياسية التي يعملون فيها. كما يجدر بهم أن يتفهّموا مصالح الهيئات (الحكومات، مجموعات الجريمة المنظّمة، وما شابهها) التي ترغب في الحدّ من وصول المواطنين إلى المعلومات، متخذةً خطوات حاسمة لحجبها، وأن يعاينوا قدراتها التكنولوجية. أخيراً، يتعيّن عليهم اتخاذ القرارت

الحكيمة والتدابير اللازمة لحماية أنفسهم (والمصادر التي يستندون إليها في مضمار عملهم)، وتأمين أمنهم الرقمي.

يُطلِع هذا الكتيّب المراسلين والصحافيين والمدونين والعاملين في مجال الإعلام على ممارسات بسيطة، إنما فعّالة، للتحكّم بمعلوماتهم واتصالاتهم الهامة باستمرار. كما يطلعهم على عدة مصادر ممتازة متوافرة عبر الإنترنت، تزوّدهم بمعلومات ودروس خصوصية وبرمجيات إضافية.

## كيفية ترتيب المعلومات

يفترَض بهذا الكتيّب أن يكون مفيداً لأي شخصٍ، أكان يستخدم جهازه الخاص، أو جهاز كمبيوتر مشترك (في مكتب التحرير، أو مقاهي الإنترنت، أو نادي الصحافة)، أو ينجز معظم أعماله باستخدام هاتف ذكي. فقد اخترنا مواضيع متنوعة من عدة مصادر متوافرة عبر الإنترنت، موزعين الحلول إلى ثلاث فئات:

- **المبادئ الأساسية** – العلاجات الضرورية/الملحّة، التي ننصحك بتطبيق معظمها على الفور.
- **بعض التقنيات المتطورة** – الأكثر تطوراً نوعاً ما، وإنما يُستحسن الإلمام بها.
- **مصادر ومراجع إضافية** – مواد ذات صلة، متوافرة مجاناً عبر الإنترنت، تجد فيها شروحات معمّقة ومعلومات موسّعة حول مواضيع معيّنة.

يضمّ كل موضوع قائمة مرجعية بالنشاطات التي يُطلَب منك الشروع بتنفيذها، وتساعدك في تحديد التقدم الذي تحرزه. صحيحٌ أنها لا تتضمّن كل الحلول الممكنة لمواجهة تحديات معيّنة، ولكنها تتناول جملة وسائل معهودة لمعالجة المشاكل التي تبرز اليوم.

## بعض الفرضيات

مع أنّ هذا الكتيّب يتضمّن فقرات لمعالجة فيروسات الكمبيوتر ومشكلة الشبكات المعرّضة للاختراق، تنطلق غالبية التوصيات الصادرة عنه من فرضية خلو جهازك من أي إصابة.

نقرّ بأنّ نظامي التشغيل ماك ولينكس يلقيان شعبية متزايدة، إلا أنّ غالبية أجهزة الكمبيوتر الخاصة المنتشرة في العالم ما زالت تعتمد نظام ويندوز، مع استمرار عدد كبير من منتجي وناشري المحتويات باستخدامها. لذا، يركّز هذا الكتيّب على نظام ويندوز، وتطبيقات ويندوز، على أمل أن نزوّد مستخدمي نظامي ماك ولينكس بمعلومات مماثلة في المستقبل.

## ليس إلا مدخلاً إلى مبتكرات الأمن الرقمي

يشهد عالم التكنولوجيا كل يوم تطورات هائلة، كما يتعرض لتهديدات جديدة. (إذ يبرز كل أسبوع أكثر من ٢٠٠٠ فيروس جديد، بحسب تقدير شركة سايمنتك التي أنشأت برنامج نورتن المعروف المضاد للفيروسات).

يصلح هذا الكتيّب، الصادر في تشرين الأول/أكتوبر ٢٠١٢، والمحدّث في كانون الأول/ديسمبر ٢٠١٢، مدخلاً إلى موضوع أمن المعلومات، ودليلاً لعدة مصادر تتوافر مجاناً عبر الإنترنت. الرجاء أن تبحث عن آخر المعلومات حول هذا الكتيّب وأبرز المواقع الإلكترونية في الفصل المخصص للمصادر الإضافية.

## قبل أن تنقر...

يتضمّن هذا الكتيّب روابط تقود مباشرة إلى مصادر وتطبيقات عبر الويب. نأمل أن تكون مفيدة للصحافيين والمدونين في مضمار عملهم. ولكن، حذارِ أن تستخدم شبكات غير آمنة لزيارة بعض هذه المواقع، لئلا تصبح نشاطاتك مكشوفةً أمام المسؤولين عن شبكات مكتبك، أو جيرانك، أو مزودي خدمة الإنترنت). الرجاء أن تقرأ القسم المتعلق **بالتصفح الآمن، ورصد مشاكل الوصول ومعالجتها**، إذا كنت مهتماً بمعرفة الانعكاسات السلبية المترتبة عليك، أو على منظمتك، جراء زيارة هذه المواقع.

# ١: تحكّم بأمن حاسوبك

## حماية حاسوبك من الفيروسات وسواها من البرمجيات الخبيثة

إنّ الاتصال بشبكة الإنترنت من جهازك من دون الحماية اللازمة هو أشبه بمن يترك باب داره مشرّعاً أمام دخول أي شخص من دون حسيب أو رقيب. وقد بيّنت الدراسات أنّ الجهاز غير الخاضع للحماية أو غير المحصّن يصبح عرضةً للإصابة في غضون دقائق. وللتسلّل من قبل غرباء عند الاتصال بالإنترنت. وها هي الهواتف الذكية بدأت تواجه اليوم تحديات مماثلة.

إذا كانت الفيروسات وسواها من البرمجيات الخبيثة (وهي برمجيات «مضرّة» تهدف إلى اختراق حاسوبك، أو التجسس على نشاطاتك، أو إفساد يومك بكل بساطة) تثير لنا جميعاً مشاكل مشتركة، فعواقبها تكون أخطر على الصحافيين والمدونين تحديداً.

فمن شأن أي فيروس أن يشلّ قدرتك على العمل ونشر الأخبار في أبسط الأحوال، بحيث يتعذّر عليك الوصول إلى برامجك وملفاتك بشكل مؤقت. ولا يعود بإمكانك، نتيجة ذلك، إيصال الخبر إلى رئيس التحرير في الوقت المناسب، أو البحث عن مقالة معيّنة، أو تحديد موعد مقابلة عبر الإنترنت.

لا بل قد يرتّب أي فيروس عواقب أخطر بكثير، إذ تبعاً لنوعه، قد تفقد نهائياً كل العمل الذي أنجزته، ضمن إطار مشروعك الحالي وما سبقه من جهود؛ أو لا تعود قادراً على الوصول إلى بريدك الإلكتروني أو حساباتك على مواقع الدردشة، وما تحويه من محادثات سرية. لا بل يجوز أن تفقد قائمة الاتصالات، التي أمضيت سنوات في إعدادها، واضعاً ربما معارفك الأكثر تكتماً وعرضةً للهجمات في دائرة الخطر.

لا بل قد تسمح بعض البرمجيات الخبيثة إلى شخص غريب مراقبة نشاطاتك عبر الإنترنت، أو الاطلاع على كلمات السر لحساباتٍ كان يخال إليك أنها سرية.

يستعرض هذا الفصل بعض الخطوات التي تتخذها من أجل تحصين حاسوبك ضد الفيروسات وما شابهها من برمجيات خبيثة.

### حدِّث التطبيقات التي تستخدمها لمكافحة الفيروسات

تخوّلك غالبية التطبيقات المدفوعة لمكافحة الفيروسات أن تقوم بتحديثات لمدة سنة قبل انتهاء مدة صلاحيتها. بعد ذلك، لا يتوقف العمل بهذه التطبيقات، إنما لا تعود قابلة للتحديث. عند انتهاء صلاحية رخصتك، يبقى أمامك إما أن تشتري آخر إصدار من البرنامج، أو، في المقابل، أن تنزّل تطبيقاً مجانياً مضاداً للفيروسات.

## المبادئ الأساسية

### زوّد نفسك ببرامج مضادة للفيروسات

لا يصعب على أي شخص الإفادة بانتظام من تثبيت وتحديث التطبيقات المضادة للفيروسات بانتظام، أياً كان نظام التشغيل الذي يعتمده. لا تسهم هذه التطبيقات في استئصال البرمجيات الخبيثة من حاسوبك وحسب، بل تساعد أيضاً على حماية أجهزة أصدقائك وزملائك. (إذا لم يضرب الفيروس نظام التشغيل الخاص بك، هذا لا يعني بالضرورة أنك لن تنقل العدوى إلى جهاز زميل لك تتبادل معه ملفاً خبيثاً).

إستخدم مزيجاً من الأدوات لحماية حاسوبك:

- تطبيق لمكافحة الفيروسات. لا يحمي الحاسوب من أي إصابة وحسب، بل يساعد أيضاً في استئصال الفيروس من حاسوبك إذا كان مصاباً.
- برنامج لمكافحة التجسس. يستطلع التطبيقات وملفات الكوكيز التي تكشف معلومات عنك وعن عادات تصفحك عبر الإنترنت.
- أداة فحص البرمجيات الخبيثة التي ترصد وتزيل البرمجيات الخبيثة التي تسيء إلى جهازك أو تستحوذ على معلوماتك السرية. يسود الاعتقاد لدى شريحة واسعة من الناس بأنّ برنامج مكافحة الفيروس الذي تشتريه هو أفضل من البرامج المجانية، علماً أنّ عدة أدوات مجانية لمكافحة الملفات الخبيثة تلقى استحساناً ويوصي بها الصحافيون المعنيون بشؤون التكنولوجيا. ومن الأدوات الممكن النظر فيها، نذكر الآتي:
  - «آي في جي»؛
  - «أفاست!»؛
  - «أفيرا».

## حدِّث كل المكونات

غالباً ما تفتك الفيروسات بالبرمجيات التي لم تعد صالحة للاستعمال. لذا، من الضروري مثلاً أن تخضع تطبيقات مكافحة الفيروسات لتحديثات منتظمة، وإلا قد تعجز عن صدّ هجمات فيروسات جديدة على حاسوبك. من هنا أهمية السهر باستمرار على تحديث جهاز التشغيل الذي تعتمده. تجدر الإشارة إلى أنّ شركة مايكروسوفت تؤمّن تحديثات الأمان لجميع إصدارات نظام ويندوز، **أكانت أصلية أم غير أصلية**، لذا يُنصَح المستخدمون بشدة الإفادة منها.

إحرص على تشغيل ميزة التحديثات التلقائية لنظام ويندوز على حاسوبك:

- تحقّق من وضعية تحديثات ويندوز: أنقر على خانة «النظام والأمن» في لوحة التحكّم، ثمّ اختَر ميزة «تفعيل/تعطيل التحديث التلقائي»، ضمن تحديثات ويندوز.

لهذا السبب، فإنّ المواظبة على تحديث التطبيقات الأخرى يسهم في منع حصول أي خروقات أمنية.

يجوز لك أن تفحص يدوياً برامج تحديث التطبيقات، بزيارة المواقع الإلكترونية العائدة إلى مطوري البرمجيات، أو باستخدام أحد التطبيقات الشبيهة بتطبيق "**سيكونيا بي إس آي**" لفحص برامج المستخدم الخاصة. (يزوّدك هذا التطبيق أيضاً برابط يقودك إلى موقع الشركة المصمّمة، عند توافره).

- نزِّل «سيكونيا بي إس آي»

## شغِّل جدار الحماية

عند الاتصال بشبكة الإنترنت، إن بواسطة الكابل أو لاسلكياً أوعبر الهاتف، لا ندرك بالطبع أننا نعرض جهاز الكمبيوتر أو الجهاز الجوّال الذي نستخدمه إلى مخاطر لا نراها بأمّ العين. فقد صُمِّمت الفيروسات المعروفة بالديدان مثلاً، للعثور تلقائياً على أجهزة تضربها وتفتك بها. وما إن تصيب أول هدف بنجاح حتى تسعى جاهدةً على الفور إلى إصابة جهاز آخر متّصل بالشبكة ذاتها للانقضاض عليه. وبالتالي، يرى موقع «إنترنت ستورم سنتر» التابع لمعهد «إس آي إن آس»، الذي يعمل خصيصاً على تعقّب قدرة الديدان والبرمجيات الخبيثة الأخرى الناشطة عبر الويب، حالياً أنّ أي جهاز ويندوز غير محصّن، أي لم يجرِ سدّ ثغراته الأمنية ولا ينعم بجدار حماية، يمكن أن يصاب بفيروس في غضون خمس دقائق عند اتصاله بالشبكة. (يمكن أن تتعقّب بنفسك معدل «وقت الصمود» باستخدام خدمة «وقت الصمود»).

يمنع جدار الحماية الديدان من التسلل إلى الأجهزة التي تستخدمها لإعداد التقارير، والمراسلات، والمهام الضرورية الأخرى. فيقف حاجزاً في وجه الديدان ويتصدى لكل التعديات الأخرى، عن طريق اعتراض حركة مرور البيانات التي لم تطلب الحصول عليها أو تأذن بها تحديداً. (أحياناً، تعمد الحكومات، كما مزوّدو خدمات الإنترنت، إلى استخدام جدران الحماية من أجل منع المستخدمين من الوصول إلى مواقع محددة، إلا أنّ الجدران التي نشير إليها في معرض هذا الكتيّب هي تلك التي تمنع البيانات غير المرغوب فيها من دخول حاسوبك أو هاتفك الجوّال).

عند اتصالك بالإنترنت من خلال جهاز التوجيه اللاسلكي، تكون مزوّداً أصلاً بجهاز حماية في حاسوبك، وهوعبارة عن فلتر يحجب حركة المرور الوافدة من دون استئذانك.

إلا أنّ برامج الحماية التي تضيفها إلى حاسوبك أو هاتفك الذكي تؤمّن لك حماية زائدة ضد كل الخروقات المحتملة. أما أجهزة الكومبيوتر العاملة على نظام ويندوز فتأتي مزوّدة بجدار حماية، يُعرَف بجدار حماية ويندوز، وهو كل ما تحتاجه من أجل صدّ معظم الاختراقات، وتنبيهك إلى التطبيقات التي تحاول الاتصال بالإنترنت من دون إذنك.

- تأكّد من تشغيل جدار الحماية في جهازك: أنقر على خانة «النظام والأمن» في لوحة التحكّم، ثمّ، اختَر «تحقّق من وضعية جدار الحماية» ضمن جدار حماية ويندوز.

- يُطلِعك الموقع الخاص بـ«عُدّة الأمان، أدوات وممارسات للأمان الرقمي» على خيارات مجانية بديلة لجدار حماية ويندوز، وتتضمّن بعض الميزات الإضافية، على مثال لوحة التحكّم التي تسمح لك برصد جميع اتصالاتك.

### كن سبّاقاً

إلا أنّ سلوكياتك وتصرفاتك تبقى سبيلك الأفضل للاتقاء من البرمجيات الخبيثة. لذا، لا يضيرك أن تكتسب بعض العادات المفيدة:

- إحرص على تنزيل التطبيقات من مواقعها الرسمية مباشرة، أو من مواقع تنزيل برامج الكمبيوتر التي تضع البرمجيات الخبيثة موضع اختبار، كمواقع «فايلهيبو»، أو «سوفتبيديا»، أو «داونلود دوت كوم».
- لا تنقر أبداً على الروابط الواردة ضمن رسائل البريد الإلكتروني: بل انسخها وألصقها مباشرةً في شريط العنوان ضمن متصفحك.
- لا تفتح الملف المرفق ببريدك الإلكتروني، إلا إذا كنت واثقاً من مصدره. أما إذا كنت مرتاباً بشأن ملف مرفق سبق لك أن نزّلته، وأنت غير مزوّد بتطبيق مضادة للفيروسات يفحص صندوق بريدك تلقائياً، فما عليك سوى أن تفحصه يدوياً.

## إلتزم بتطبيق واحد لمكافحة الفيروسات

إذا كان تطبيق واحد لمكافحة الفيروسات يفيدك، فلا ضير من استخدام اثنين، صحيح؟ لا، هذا غير صحيح. لأنّ تطبيقات مكافحة الفيروسات تستلزم عادةً الوصول بطريقة خاصة إلى نظام التشغيل في جهازك. وبالتالي، فقد يختلط الأمر على بعض هذه التطبيقات، التي قد تحسب بنات جنسها... فيروسات! إذا صادَفتها في نظام التشغيل. كما يجوز أن يمنع أي تطبيق تطبيقاً آخر من رؤية جميع الملفات الموجودة في جهازك.

- لا تنزّل البرمجيات المقرصَنَة، قد تكون غير مكلفة وإنما تأتيك بعلّات إضافية أنت بغنىً عنها، كالبرمجيات الخبيثة! لذلك أبحث عن برمجيات بديلة مجانية، لكن أصلية، لما تحتاج إليه. وفي هذا الإطار، ينصحك الموقع الإلكتروني «ألترنتيف تو» باستعمال تطبيقات مجانية، تتماشى مع نظام التشغيل الذي تعتمده، والمهام التي أنت بصدد إنجازها. كما يقدّم الموقع «أوزالت» خدمات مماثلة، مركّزاً على برمجيات مفتوحة المصدر.

## إذا لم تكن مزوّداً بالحزمة المكتبية "مايكروسوفت أوفيس"...

إذا لم تعتمد تطبيقات مايكروسوفت وورد وإكسيل وتطبيقات أخرى من هذا البرنامج، يتوافر عدد كبير من التطبيقات البديلة المجانية، على مثال حزمتي تاكست إيديت وآبي وورد، الصالح استعمالهما كتطبيق واحد، على شاكلة حزمة وورد. أما التطبيقات الأخرى، كحزمتي أوبن أوفيس ولايبر أوفيس، فتوفّران سلسلة كاملة من البرامج المكتبية.

### إذا كنت تستخدم جهاز كمبيوتر مشتركاً:

إذا كنت تستخدم جهاز كمبيوتر مشتركاً في مكتب التحرير، فمن الضروري أن تزوّد الجهاز بتطبيق لمكافحة الفيروسات، أي التطبيق الذي برمجته لحماية جميع المستخدمين، بما أنّ سلوكيات شخص واحد قد تؤثّر على سلامة الجهاز المستخدَم من الجميع.

إذا كنت تكتب مقالتك أو مدونتك في مقهى إنترنت عام، لا تتّكل على سلامة الأجهزة المستخدمة فيها، بل افترض أنها مصابة بفيروسات خبيثة. فإذا كنت تخشى إمكانية انتقال العدوى إلى الملفات التي تنزّلها من مكان عملك، ما عليك سوى أن تتحقّق منها بواسطة تطبيقات محمولة لمكافحة الفيرسات، كفاحص مايكروسوفت للتحقق من سلامة الجهاز أو برامج الفحص المتوافرة مجاناً عبر الإنترنت، كبرنامجي «هاوس كول» أو بيت ديفندر» من شركة «ترند مايكرو».

- تفحّص حاسوبك الآن ببرنامج «هاوس كول»:
- تفحّص حاسوبك الآن ببرنامج «بيت ديفندر»:
- زر صفحة مايكروسوفت حول برامج فحص الأجهزة للتحقق من سلامتها.

## بعض التقنيات المتطورة

تتوافر وسائل أخرى لحماية جهازك، أكثر تعقيداً نوعاً ما، إنما أجدى نفعاً.

### عطّل وظيفة التشغيل التلقائي في نظام ويندوز

هل أصيب جهاز الكمبيوتر الموضوع في خدمتك في مركز العمل بفيروس أو ما شابه، نتيجة استخدام شريحة الذاكرة «يو آس بي»، أو الأقراص المدمجة؟ قد تبدأ رسائل تنبيهية بالظهور فجأة أمامك وأنت تنسخ صورة وصلتك للتو من المكتب الميداني. كما يمكن أن تنتقل بعض البرمجيات الخبيثة من جهاز مصاب إلى جهاز شخصي من خلال وظيفة التشغيل التلقائي، وهي عبارة عن ميزة

## نزّل بعض نسخ ويندوز الحديثة

إذا كنت واحداً ممّن لا يزالون يعتمدون نسخة ويندوز «آكس بي»، قد آن لك ربما الارتقاء إلى نسخة ويندوز ٧ أو ٨. رغم تقديرات تشير إلى استمرار أكثر من ٤٠٪ من الأجهزة الشخصية الموصولة بالإنترنت باعتماد هذه النسخة. كما أعلنت الشركة أيضاً أنها لن تواصل تقديم دعمها إلى نسخة «آكس بي» بعد ٨ نيسان/أبريل ٢٠١٤، بما يعني أنّ مستخدمي هذه النسخة لن يحظوا بتحديثات أمنية بعد هذا التاريخ.

تطلق آلياً بعض التطبيقات الملائمة لحاجاتنا، ولكنها في المقابل تسمح لبعض البرمجيات الخبيثة بأن تفعل فعلها قبل أن تعرف حتى بوجودها. لذلك، تشرح شركة مايكروسوفت إلى المستخدم كيف يعطّل يدوياً وظيفة التشغيل التلقائي في جميع إصدارات ويندوز منذ صدور نسخة ويندوز «آكس بي»، وتستعرض أدوات إلكترونية من أجل تشغيل الميزة أو إيقاف تشغيلها:

- تعطيل ميزة التشغيل التلقائي؛
- إطلاق ميزة التشغيل التلقائي.

### إغلاق المنافذ

صحيحٌ أنك لا ترى هذه المنافذ، ولكنّ لحاسوبك منافذ تخوّله التواصل مع العالم الخارجي. يصل عددها إلى ٦٥ ٥٣٥ تحديداً. بعض هذه المنافذ يُستخدَم للبريد الإلكتروني، وبعضها الآخر لتصفح الويب، وبعضها للمحادثات عبر الإنترنت، وما شابهها من استعمالات. وبالتالي، قد تسمح هذه المنافذ المفتوحة، شأنها شأن أي نوافذ مشرّعة في دارك، بدخول ضيوف لم تتفضّل بدعوتهم، ما يعلّل رغبتك ربما بأن يغلق جهازك أي منافذ لا تستخدمها حالياً. يمكنك أن تتحقّق من وجود أي منافذ مفتوحة في جهازك بواسطة أداة تُدعى «شيلدز آب» متوافرة عبر الإنترنت. ويعتبر هذا الموقع المتخصص إلى حدّ كبير في تحصين أمن أجهزة الكمبيوتر الشخصية، أيضاً، مصدراً مفيداً للمعلومات المتعلقة بأمن الإنترنت.

- تأكّد من خلو جهازك من منافذ مفتوحة، تكون مكشوفة أمام القراصنة.

### إحصل على النسخ المرخّصة

إذا قررت شراء برمجيات مضادة للفيروسات، تأكّد من الحصول على نسخة مرخّصة. ومن أنّ التطبيقات (لا قائمة الفيروسات فقط) ما زالت سارية المفعول، لأنّ النسخة المقرصنة أو «المزوّرة» ليست آمنة.

### إستخدم نسخة يمكنك التصرف بها لنظام التشغيل

إذا أمضيت شخصياً أو أمضى زملاؤك (إذا كنت محظوظاً كفاية لتنعم بهم) في قسم المعلوماتية ساعات ساعات على إعادة تنزيل نظام التشغيل والبرامج، بسبب فيروسات ضربت جهازك أو مشاكل أخرى في البرمجيات، فلمَ لا تفكّر في استخدام آلة افتراضية، وهي عبارة عن نسخة مؤقتة لبرنامجك يمكنك التخلص منها متى بدأت تفسد.

تشيع الآلة الافتراضية بيئة محصّنة، لا تسمح بالوصول إلى كل مكوّنات جهازك، وتحدّ حجم الأضرار الناجمة عن أي فيروسات أو برمجيات خبيثة أخرى. فإذا فتحت ملفّاً مشبوهاً في ظل هذه البيئة مثلاً، يجوز أن يفسد نظام التشغيل الافتراضي الذي تستخدمه، من دون الإساءة على الأرجح إلى جهازك «الحقيقي». عندئذٍ، يسعك أن تستأصل نظام التشغيل المصاب بفيروس، وأن تعاود العمل باستخدام آلة افتراضية جديدة (إذا افترضنا أنك احتفظت بنسخة جاهزة للاستعمال!).

تحتمل نسخة ويندوز ٧ هذا النوع من البيئة الافتراضية، مزوّدةً بميزة داخلية تُعرَف بالجهاز الشخصي الافتراضي، مع أنّ الأشخاص غير الملمّين بالآلات الافتراضية قد يرغبون في أن يجرّبوا تطبيق «فيرتشوول بوكس»، السهل الاستعمال، والعامل أيضاً على نظام ويندوز «آكس بي».

- يمكن أن يطّلع مستخدمو نظام ويندوز ٧ على مزيد من المعلومات حول الجهاز الشخصي الافتراضي
- قد ترغب في اختبار تطبيق «فيرتشوول بوكس»، إذا كنت غير ملمّ بالآلات الافتراضية أو لا تستخدم نظام ويندوز ٧
- إذا كنت تودّ أن تعرف المزيد عن الآلات الافتراضية بوجهٍ عام، يمكنك العثور على مقالة مطوّلة عن هذا الموضوع في موقع Wikipedia.org.

### إحتفظ بـ"نسخة" عن محرّك القرص الصلب أو نظام التشغيل

إذا كنت تتمنّى أحياناً، عندما تسوء الأحوال، لو أنك تستطيع العودة بالزمن إلى الوراء، لتعود الأحوال إلى ما كانت عليه، فلن يصعب عليك أن تحقق هذه الأمنية بفضل جهاز الكمبيوتر الشخصي.

يسعك أن تحتفظ بصورة، أي نسخة، عن نظام التشغيل في جهازك متى كان سليماً معافىً، بحيث يتسنّى لك أن تعيد الأوضاع إلى طبيعتها إثر إصابته بفيروس. وبما أنّ نظام ويندوز يتمتع بميزة «النسخ الاحتياطي والاستعادة»، فما عليك سوى أن:

- تذهب إلى لوحة التحكّم، وتنقر ضمن خانة النظام والأمن على زر «إحتفظ بنسخة احتياطية عن جهازك».
- تختار من مجموعة الخيارات المتاحة عن شمالك، خيار «إحتفظ بنسخة عن نظام التشغيل»، الأمر الذي يسمح لك أن تخزّن ملفات وإعدادات ويندوز الحالية، وكذلك برامجك، في قرص صلب خارجي أو في سلسلة أقراص رقمية «دي في دي».
- تقدمّ شركة ميكروسوفت شروحات مفصّلة حول آلية تخزين بيانات نظام ويندوز وإعداداته.

إذا اخترت أن تحتفظ بنسخة طبق الأصل عن كل مخزون القرص الصلب، ضمن إطار ما يُعرَف أحياناً بـ«استنساخ» القرص، يمكنك الاستعانة بعدة برامج مجانية للنسخ الاحتياطي، لعلّ أسهلها استعمالاً على الإطلاق هو برنامج «إيزوس تودو للنسخ الاحتياطي».

- يمكنك تنزيل برنامج «إيزوس تودو للنسخ الاحتياطي».

### عند إصابة جهازك بفيروس:

لعلّ المنطق السليم العام يقول بأنّ السبيل الأوحد لحماية جهازك الشخصي أو هاتفك الجوّال فعلياً من الإصابة بأي فيروس أو برنامج خبيث تكمن بعدم استخدامه.

لسوء الحظ أنّ هذا الحلّ ليس عملياً بالنسبة إلى الصحافيين والمدونين، الذين يتلقّون بالطبع ملفات ومراسلات من مصادر معلوماتهم غير الواعية ربما لأهمية حماية أمنها. لذا، في حال وقع المحظور، ما عليك سوى أن تراجع قائمة التوصيات المتعلقة بطريقة معالجة الأجهزة الشخصية المصابة بفيروسات.

## مصادر ومراجع إضافية

### دليل عُدّة الأمان: أدوات وممارسات للأمان الرقمي، صادر عن منظمة "تاكتكل تكنولوجي كولكتيف" Tactical Technology Collective، ومؤسسة "فرونت لاين ديفندرز" Front Line Defenders

- «حماية جهازك من البرامج الخبيثة والقراصنة» - يستعرض هذا الدليل خطوةً خطوة:
  - «أفاست» مضاد للفيروسات؛
  - «سبايبوت» للكشف عن البرمجيات التجسسية وإبادتها؛
  - جدار النار كومودو؛
- دليل الاستمرارية الرقمية: الكمبيوتر.

### نصائح غوغل لتصفح الإنترنت بأمان

- التصيّد الإلكتروني؛
- البرمجيات الخبيثة.

## قائمة مرجعية لوسائل الحماية الأساسية

### الاتقاء من البرمجيات الخبيثة

**عند استخدام جهاز كمبيوتر شخصي:**

- ونزّل وثبّت تطبيقاً واحداً من كل فئة من الفئات التالية:

**تطبيقات لمكافحة الفيروسات**

- «آي في جي»؛
- «أفاست!»؛
- «أفيرا».

**تطبيقات لمكافحة برامج التجسس**

- «سوبر أنتي سبايوير»؛
- «سبايبوت» للكشف والإبادة؛
- «أدوير».

**فاحص/مزيل البرمجيات الخبيثة**

- برنامج الحماية «مالوير بايتس»؛
- برنامج «هاوس كول» من شركة «ترند مايكرو»؛
- برنامج مايكروسوفت لفحص الجهاز والتحقق من سلامته.

- حدِّث التطبيقات التي نزّلتها.
- أجرِ فحصاً كاملاً.

**عند استخدام جهاز كمبيوتر مشترك:**

- تأكّد من حماية حاسوبك بتطبيق مضاد للفيروسات، يخضع للتحديث.
- إذا كنت تستخدم جهازاً مشتركاً في مكتب التحرير، أدرس مع مدير المكتب إمكانية إضافة تطبيقات لمكافحة الفيروسات، والحماية من البرمجيات الخبيثة، في حال عدم توافرها.

### نزّل مرة، إستخدم مرتين (أو أكثر)

إذا كنت تعمل في مكتب تحرير، من الأرجح أن تجد حولك عدة أجهزة كمبيوتر شخصية، قلّما تخضع للتحديث. لذلك، من شأن تحميل بعض التحديثات من حينٍ إلى آخر، وتنزيلها على جميع أجهزة الكبيوتر التي تعتمد على نظام التشغيل ذاته، أن يسمح لك بتوفير الوقت ونطاق الحزمة. لهذه الغاية، يمكنك الاستعانة بتطبيق wsuoffline.net.

## إيّاك أن تثق بدخيل

يجب أن تفحص دوماً أقراص التخزين الصغيرة الحجم، والأقراص الصلبة الخارجية، والأقراص المدمجة، وأقراص الفيديو الرقمية للكشف عن البرمجيات الخبيثة

- إذا كنت تعمل أو تكتب مدونتك في مقهى إنترنت، زوّد نفسك ببرامج حماية خاصة (بتخزين إسطوانة الإنقاذ من برنامج «آي في جي» وفاحص مايكروسوفت ضمن شريحة ذاكرة للتحقق من خلوّ أجهزة الكمبيوتر في الأماكن العامة من البرمجيات الخبيثة)، أو شغّل أحد محركات الفحص المتوافرة عبر الإنترنت، مثل «هاوس كول» أو «بيت ديفندر» من شركة «ترند مايكرو».

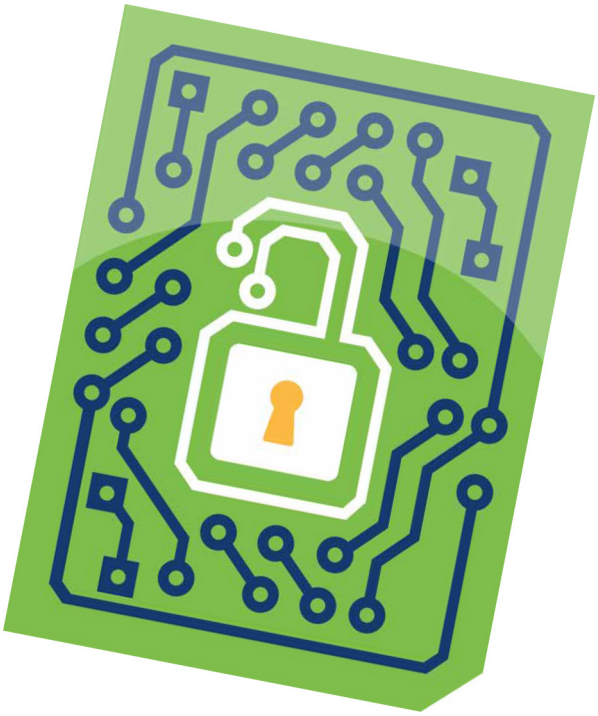
### حدِّث كل المكونات

- حدّث نظام التشغيل، واسمح ضمن نظام ويندوز بتفعيل ميزة التحديثات التلقائية.
- شغّل تلقائياً تطبيقات مكافحة الفيروسات وسواها من التطبيقات المضادة للبرمجيات الخبيثة.
- زر الصفحات الرئيسية للبرامج التي نزّلتها، حرصاً على استخدام آخر إصداراتها، أو ادرس إمكانية استخدام تطبيق «سيكونيا بي إس آي».
- حدّد إشعارات تنبيهية للاستعلام عن التحديثات الجديدة.

### شغِّل جدار الحماية

- تثبّت من أنّ جدار الحماية الموجود في جهازك هو في وضعية التشغيل.
- إذا كنت ترغب في الحصول على مزيد من الحماية، نزّل برنامجاً إضافياً، كبرنامج «كومودو» المجاني. وللاستعلام عن هذا البرنامج، يمكنك العودة إلى دليل يشرح لك خطوةً خطوة كيفية استخدامه لدى الموقع الإلكتروني «عُدّة الأمان»، الذي تديره منظمة «تاكتكل تكنولوجي كولكتيف»، ومؤسسة «فرونت لاين ديفندرز».

## ملاحظات



# ٢: حماية بياناتك

## حماية حاسوبك الشخصي أو هاتفك الذكي من الفيروسات وسواها من البرمجيات الخبيثة

تعتبر قائمة الاتصال، كما الأبحاث الحالية وأرشيف المقالات والصور، من أغلى ما يحتفظ به الصحافي ضمن مقتنياته. لكنّ هذه المواد تجذب أيضاً منافسيه أو أي شخص آخر قد يرغب في معرفة مصادره السرية، أو الكشف عن الأبحاث التي قام بها لمشروعه القادم.

لكنّ فقدان هذه المواد القيّمة هو أشبه بالكارثة. فماذا يصيبك مثلاً إذا اختفت فجأةً الملاحظات التي عملت على تجميعها من عدة مقابلات على مدار شهر، من دون أن تحفظها في نسخة احتياطية؟ هذا يعني بكل بساطة بالنسبة إلى عدة أشخاص العودة إلى نقطة الصفر.

إليك بعض الوسائل اللازمة لحماية أعمالك ومصادرك:

## المبادئ الأساسية

### إبدأ بتحصين نفسك بكلمة سر قوية

تكون الأقفال عديمة الفائدة تقريباً إذا كانت سهلة الاختراق. والأمر سيّان بالنسبة إلى كلمة السر. فإذا اعتمدت «كلمة سر»، أو إسم المستخدم، ككلمة سر، فسيسهل على أيٍّ كان أن يفتح هذا القفل، مخترقاً البيانات والحسابات التي تحاول حمايتها، من دون أي عناء.

تستعرض منظمة «تاكتكل تكنولوجي كولكتيف» قائمة ممتازة بالتوصيات المفيدة لإنشاء كلمة سرّ قوية، بما في ذلك:

- فلتكن طويلة.
- فلتكن معقّدة (راجع قائمة أفضل ٢٥ كلمة سر).
- يُستحسَن ألاّ تكون شخصية (قلما تكون العبارة التي تأخذها من كتابك المفضّل محصّنةً إذا كان الجميع على علمٍ بقراءاتك الأدبية المفضّلة!).
- لا تستخدم كلمة السر ذاتها لأكثر من حساب.

من قبيل التسلية، يمكنك أن تختبر عدة كلمات سرّ باستخدام أداة فحص كلمات السر من مايكروسوفت. فترى بأم عينيك كيف تؤثّر إضافة بعض الأحرف الكبيرة، أو الأرقام، أو الرموز الخاصة على طول كلمة السر. (ولكن، عند استخدام أداة الفحص هذه، شأنها شأن أي أداة أخرى متوافرة عبر الإنترنت، لا يجدر بك بالطبع أن تختبر كلمات السر التي تنوي استخدامها فعلياً).

- تحقّق من مدى تأثير طول كلمة السر، والمقومات الأخرى التي تدخل في بنيتها، على قوتها باستخدام أداة فحص كلمة السر من مايكروسوفت.
- إطّلع على نصائح إضافية بشأن كلمات السر من موقع «عُدّة الأمان».

### إحفظ كلمات السر بمكان آمن

باستطاعتك أن تحمي قائمة كلمات السر الخاصة بك... بكلمة سر. قد تبدو لك هذه الحيلة سخيفة في بادئ الأمر، إنما لا تخلو من فوائد حقيقية، أقلّها أنها لا تلزمك إلاّ بتذكّر كلمة سر واحدة، وهي التي تستخدمها لإقفال وفتح قائمتك المحميّة. وبالتالي، عوض أن تحتفظ بكلمات السر في ملف خاص، أو تدوّنها في ورقة تتركها على مكتبك مثلاً، فلِمَ لا تودعها في «خَزْنة كلمات السر» التي تحمي قائمتك بشيفرة معيّنة، في حال فقدتها أو أضعتها.

تتوافر عدة خزنات لحفظ كلمات السر، نذكر منها برنامج «كي باس» المجاني. ويتميّز هذا البرنامج، الذي يُحفَظ ضمن شريحة ذاكرة «يو آس بي»، ببعض الخصائص الإضافية، إذ يسمح لك أن تشفّر قائمتك بكلمة سر رئيسية وبملف مفتاح (وهو ملف يجب أن يكون متوافراً على جهاز الكمبيوتر الشخصي لقبول كلمة السر).

- نزّل برنامج «كي باس»
- يزوّدك موقع «عُدّة الأمان»، الذي تديره منظمة «تاكتكل تكنولوجي كولكتيف» ومؤسسة «فرونت لاين ديفندرز»، بدروس خصوصية لاستخدام برنامج «كي باس».

## هل هذه كلمة سرك؟

قائمة بكلمات السرّ الخمس والعشرين الأكثر شيوعاً:

1. password
2. 123456
3. 12345678
4. abc123
5. qwerty
6. monkey
7. letmein
8. dragon
9. 111111
10. baseball
11. iloveyou
12. trustno1
13. 1234567
14. sunshine
15. master
16. 123123
17. welcome
18. shadow
19. ashley
20. football
21. jesus
22. michael
23. ninja
24. mustang
25. password1

المصدر: www.splashdata.com

### حماية بياناتك بمفتاح التشفير

إنّ كلمة السر الخاصة بحساب المستخدم، وهي الكلمة التي يُطلَب منك تسجيلها في شاشة الترحيب لنظام ويندوز، تشكّل وسيلة مؤاتية لمنع أي شخص قادر فعلياً على استخدام حاسوبك من تعديل إعداداتك من دون إذنك، إنما لا تمنعه من العبث بملفاتك. لهذا السبب، قد ترغب بتشفير كامل المحركات لتمويه محتويات ملفاتك.

يمكّنك تطبيق "**بت لوكر**"، المتوافر في نسختي ويندوز فيستا وويندوز ٧، إنتربرايز وآلتميت، أن تقفل الجهاز الشخصي الذي تستخدمه في مضمار عملك الإخباري، وكذلك الأقراص الصلبة الخارجية، كتلك التي قد تستخدمها لحفظ نسخة احتياطية عن ملفاتك.

- إذا كنت تملك أصلاً نسخة متطابقة من ويندوز، بإمكانك أن تشغّل تطبيق «بت لوكر» في لوحة التحكّم، من خلال النقر على أيقونة «النظام والأمن»، ثمّ «تشفير محرّكات الأقراص بواسطة بت لوكر».

أما في حال عدم توافر نسخة متطابقة من ويندوز، فيبقى بإمكانك، أنت وزملائك، تأمين حماية كامل محركات الأقراص، باستخدام التطبيق المجاني المعروف بإسم "**تروكريبت**". ليس هذا الأخير ببساطة تطبيق «بت لوكر»، إنما يأتي مزوّداً بخيارات إضافية: تحمله معك أينما ذهبت إذ يعمل على وسائط تخزين محمولة؛ يمكن استخدامه لتشفير القرص الصلب أو أحد ملفاتك؛ كما يسمح لك بحماية ملفاتك بكلمة سر، أو ملف مفتاح، أو كلاهما.

- نزّل برنامج «تروكريبت».
- يزوّدك مطوّرو البرامج بدروس خصوصية لاستخدام برنامج «تروكريبت».

## إزالة نُسَخ الملفات غير المرغوب فيها

حين تفتح، أو تفكّ شيفرة، أحد الملفات الموجودة في جهازك الشخصي، يبقى هذا الملف متوافراً على جهازك على شكل ملف «مؤقّت». في هذه الحالة، يجوز أن تستخدم أدوات، كبرنامج «سيكلينر»، لمحو هذه النسخ غير المحمية (وغير المرغوب فيها).

### إذا كنت تستخدم جهازاً مشتركاً:

قد يتمكّن مدراء الشبكات في مكاتب التحرير أو مقاهي الإنترنت العامة من نسخ محتويات أي شريحة ذاكرة أو أجهزة أخرى تكون بحوزتك من دون علمك، تبعاً لقدرتهم على الوصول إلى أجهزة الكمبيوتر الموصولة بالشبكات. لذا، أدرس إمكانية استخدام تطبيق «تروكريبت» لحماية الملفات المحفوظة في جهازك، إنما لا تنسَ أنه يسهل على هؤلاء المدراء أيضاً الاطّلاع على ملفاتك، عند فكّ شيفرتها. لذا، من الأوفق لك أن تكون على معرفة بسياساتهم وممارساتهم.

إذا كنت تستخدم جهاز كمبيوتر مشتركاً، إحرص على عدم مشاركة الملفات الموجوة في جهازك مع أجهزة أخرى موصولة بالشبكة، إنما غير خاضعة لرقابة المدراء: أنقر على الملف بزر الفأرة الأيمن، ثمّ اختَر علامة التبويب الدالة على المشاركة، للتحقّق مما

إذا كانت محتويات الملف متوافرة لأجهزة أخرى (كأجهزة كمبيوتر محمولة يستخدمها المراسلون أو المدوّنون) موصولة بالشبكة ذاتها.

- إطّلع على ميزة تبادل الملفات لدى موقع الدعم الخاص بنظام ويندوز لدى شركة مايكروسوفت.

## إحتفظ بنسخة احتياطية عن كل بياناتك

إنّ الفيروسات، وانقطاع التيار الكهربائي، وتعطّل الأجهزة، والسرقة، وما شابهها تشكّل بمجملها تهديداً لبياناتك. لذا من المهم أن تحتفظ بنسخ محميّة عن كل أعمالك، وقائمة الاتصال بمعارفك، وكل البيانات الضرورية لإنجاز مهامك الصحفية.

تتوافر عدة وسائل للاحتفاظ بنسخة احتياطية عن الملفات (لعلّ أفضلها هي الوسيلة التي تعتمدها حالياً!). أياً كانت الوسيلة التي تلجأ إليها، إعمل بالتوجيهات التالية:

- إحتفظ بنسختين احتياطتين عن بياناتك، واحدة في متناول يدك، على أجهزة أو وسائط تخزين خارجية (قرص مدمج، قرص دي في دي) و...
- وأخرى في مكان آخر، لدى أحد الأصدقاء، أو «على السحابة» (باللجوء إلى خدمة تبادل الملفات عبر الإنترنت أو خدمة تخزين النسخ الاحتياطية). لكن، حذارِ الاتّكال فقط على خدمة التخزين السحابي، لأنك إذا عجزت عن الدخول إلى حسابك عبر الإنترنت، فلن تعود قادراً على الوصول إلى نسخك الاحتياطية.
- قم دورياً بالنسخ الاحتياطي، واضبطه تلقائياً إن أمكن، ولا ضير من أن يكون بوتيرة أسبوعية.
- إحمِ المحفوظات الاحتياطية بشيفرة خاصة، وكلمة سر قوية.

### إحتفظ بنسخة احتياطية عن نسختك الاحتياطية

تؤمّن عدة خدمات متوافرة عبر الإنترنت، كخدمة «دروب بوكس» و«موزي»، تخزيناً محدوداً بشكل مجاني. إنما يُستحسن أيضاً أن تحتفظ بنسخة عن ملفاتك خارج الشبكة، وأن تحمي محفوظاتك الاحتياطية عبر الشبكة أو في قرص خارجي بشيفرة خاصة.

إحرص على مراعاة هذه المبادئ، حتى ولو كان مكتب التحرير حيث تعمل مزوّداً بنظام تلقائي للنسخ الاحتياطي لحسن حظك، إذ سرعان ما يتعذّر عليك الوصول إلى نسخك الاحتياطية نتيجة أي تغيّر مفاجئ في التيار الكهربائي، أو فيضانات، أو حرائق، أو مصادرة من قبل السلطات.

## بعض الوسائل الشائعة للاحتفاظ بنسخة احتياطية عن جهازك الشخصي:

١. يمكن أن تسحب وتسقط بعض الملفات في قرص خارجي، مع الحرص على أن يكون القرص، أو الملفات الموجودة في القرص، مشفّراً ومحميّاً بكلمة سر. إذا لم تكن أكيداً من طريقة تشفير قرصك الخارجي أوالملفات التي تودّ إيداعها في القرص، عُد إلى الفقرة الواردة أعلاه حول «حماية بياناتك بمفتاح التشفير»، أو زُر موقع «عُدّة الأمان» لمعرفة المزيد عن برنامج «تروكريبت».

٢. يجوز لمستخدمي نظام ويندوز ٧ أن يفيدوا من ميزة «النسخ الاحتياطي والاستعادة»، لنقل ملفات من أماكن التخزين الأكثر شيوعاً (كـ«ملفاتي») إلى مكان تخزين آخر كقرص خارجي، أو قرص دي في دي، أو قرص موصول بشبكة، مع الحرص مجدداً على أن يكون هذا الأخير محصّناً بكلمة سر.

٣. أما الأشخاص الذين يستخدمون إصدارات أخرى من نظام ويندوز، أو يودون التحكّم أكثر بنسخهم الاحتياطية، فبوسعهم تحميل تطبيق مجاني لهذه الغاية، كتطبيق **كوبيان للمحفوظات الاحتياطية** الذي ينصح به الجميع. ويتضمّن هذا الأخير ميزة تشفير وجدولة تلقائية، بحيث لا تعود مضطراً إلى تذكير نفسك بمواعيد تحديث نسخك.
   - لاستخدام ميزة النسخ الاحتياطي للمرة الأولى في نظام ويندوز ٧، إفتح لوحة التحكّم، وانقر على أيقونة «النظام والأمن»، ثم «النسخ الاحتياطي والاستعادة».
   - نزّل تطبيق **كوبيان للمحفوظات الاحتياطية**.
   - زر الدروس الخصوصية المتوافرة عبر موقعي منظمة «تاكتكل تكنولوجي كولكتيف»، ومؤسسة «فرونت لاين ديفندرز».

### لا تحمي مجمل التدابير الوقائية جميع بياناتك بالقدر ذاته

تساعد خاصية استعادة النظام في نظام ويندوز على استرداد ملفات نظام التشغيل، فيما تحمي كلمة سر حساب المستخدم إعداداتك. لكنّ كلا الوظيفتين لا تسمحان بحماية بياناتك من السرقة، أو المصادرة، أو أي تهديدات أخرى.

## أزِل التفاصيل غير اللازمة من ملفات "أوفيس"

تتضمّن وثائق «مايكروسوف أوفيس»، كملفات «وورد وآكسيل»، معلومات عمّن أنشأ الملف، عمّن قرأه أو نقّحه آخر مرة، إلى جانب

تفاصيل إضافية. إذا كنت لا تودّ إدراج هذا النوع من المعلومات ضمن وثائقك، رغبةً منك ربما في حماية المصدر الذي شاركك بتقرير، غير مدركٍ أنه يخلّف وراءه مساراً افتراضياً. فالأجدى بك أن تطلب من إصدار أوفيس ٢٠١٠، والإصدارات الأحدث، إزالة قسم كبير من هذه المعلومات التي تدلّ على هوية صاحبها.

- حين تكون الوثيقة مفتوحة، أختَر «ملف» في القائمة الرئيسية، ثم «معلومات». ثم إبحث عن فقرة «أعِدّ للتبادل»، واختَر أيقونة «تحقّق من المواضيع». عندئذٍ، تتيح لك ميزة فحص الوثيقة التفتيش عن معلومات شخصية وتعليقات، وحتى عن محتويات غير ظاهرة، فيها، تمهيداً لمحوها.

## بعض التقنيات المتطورة

### عطِّل وظيفتي المساعدة عن بعد والوصول إلى الجهاز عن بعد

يسمح لك نظام ويندوز الحصول على مساعدة تقنية عبر الإنترنت من أشخاص متواجدين في مواقع بعيدة، عندما يصاب جهازك بمكروه. لكن، بما أنّ هذه الميزات هي عرضة للاستغلال، إحرص على تعطيلها افتراضياً (يمكن أن تعيد تشغيلها لاحقاً، عند الحاجة) حتى لا تسهّل على أحد الوصول إلى جهازك الشخصي من دون انتباه:

- إختَر خانة «النظام والأمن»، في لوحة التحكّم، ثم انقر على خانة «إسمح بالوصول عن بعد» في إمدادات النظام، للتحقّق من وضعك الحالي. ثمّ، إزل الإشارة من مربّع «إسمح الاتصال بالكمبيوتر للمساعدة عن بعد»، وانقر في ما بعد على زر الاختيار «لا تسمح الاتصال بهذا الكمبيوتر».

### إحفظ الملفات في "مجلّد مخفي"

يتيح لك برنامج «تروكريبت» أن تحمي بعض بياناتك في قسم مخفي من مجلداتك المشفّرة، فلا يتسنّى لأحد رؤية الملفات الموجودة في هذا القسم إذا اضطررت إلى الكشف عن كلمة السر. إلا أنّ إنشاء المجلّد الخفي هو أمر دقيق للغاية، باعتبار أنّ الشخص الذي يجهل آلية استعماله قد ينتهي به الأمر إلى محو البيانات المحفوظة فيه بطريقة عرضية. لهذا السبب، يجدر بك أن تطّلع على الشروحات والتعليمات الخاصة المقدّمة أدناه قبل أن تجازف باستخدام هذه الوسيلة لحفظ صورك، أو مقابلاتك المسجّلة، أو المواد الأخرى الضرورية لأعمالك.

- إقرأ هذه الشروحات حول المجلدات المخفية لدى موقع «تروكريبت».
- إتّبع الدروس الخصوصية خطوة خطوة لدى موقع «عُدّة الأمان».

### إحتفظ بـ"نسخة طبق الأصل" عن القرص الصلب في جهازك

إذا كنت تريد أن تحتفظ بنسخة احتياطية عن كل ما ينطوي عليه جهازك، وصولاً إلى إعدادات نظام التشغيل الذي تعتمده، فبإمكانك أن تأخذ نسخة طبق الأصل عن كامل محتويات القرص الصلب. ولا تنعدم برامج النسخ الاحتياطي التي تدرج هذه الميزة ضمن تطبيقاتها، لكنّ أفضلها على الإطلاق يتجلّى في برنامج «إيزوس تودو» للنسخ الاحتياطي، المعروف بسهولة استخدامه وميزاته.

- نزّل برنامج «إيزوس تودو» للنسخ الاحتياطي.

## مصادر ومراجع إضافية

**كلمات السر:**

- كيفية وضع كلمات سر آمنة وحفظها (عُدّة الأمان).
- دليل يشرح خطوة خطوة آلية استخدام أداة «كي باس» (عُدّة الأمان).

**التشفير:**

- كيفية حفظ سرية البيانات الحسّاسة على جهازك (عُدّة الأمان).
- إستخدام برنامج «تروكريبت» (عُدّة الأمان).

**النسخ الاحتياطي:**

- كيفية استخدام أداة «كوبيان» للمحفوظات الاحتياطية على جهازك (عُدّة الأمان).

## قائمة مرجعية لحماية البيانات

### أنشئ كلمات سر قوية:

**عند استخدام جهاز شخصي:**

- إقرأ التوصيات الصادرة عن منظمة «تاكتكل تكنولوجي كولكتيف»، ومؤسسة «فرونت لاين ديفندرز» بشأن إنشاء كلمات سر قوية.
- نزّل برنامج «كي باس» وأنشئ قاعدة بيانات جديدة ، محكماً حمايتها بكلمة سر قوية.
- أحِل كلمات السر التي تنشئها إلى «كي باس»، واعمد إلى تحديثها من حينٍ لآخر، سعياً إلى تعزيز قوتها.
- إحرص على أن تشمل ضمن خطة النسخ الاحتياطي قاعدة البيانات المتعلقة بكلمات السر.

### شفّر بياناتك الحساسة:

**عند استخدام جهاز شخصي:**

- لتشفّر القرص الصلب في جهازك، تأكّد من أنّ نسخة ويندوز

التي تستخدمها تحتمل أصلاً هذه الميزة من برنامج «بت لوكر». وإلا نزّل برنامج «تروكريبت». واقرأ الدروس الخصوصية الوارادة في الموقع الإلكتروني.

- لإنشاء مجلدات مشفّرة (لا كامل القرص الصلب) أو مجلدات مخفية، نزّل برنامج «تروكريبت».
- قبل أن تبدأ بتشفير القرص الصلب، أنسخ جميع بياناتك على جهاز خارجي.
- إبحث عن دروس خصوصية لوسيلة التشفير ال لك:
  ١. «بت لوكر» في نظام ويندوز.
  ٢. «تروكريبت».

## أبقِها سرية، أبقِها آمنة

لا ضير من تبادل البيانات مع الآخرين. ولكنّ كلمة السر لا تبقى سراً إذا تشاركتها مع الآخرين. لذا، إحمِ كلمة السر حمايتك لمقتنياتك الثمينة.

**عند استخدام جهاز كمبيوتر مشترك:**

- لنفترض أنه لا يؤذَن لك بتثبيت برمجيات معيّنة على جهاز شخصي تتشارك به مع مستخدم آخر، فلا شيء يمنعك من أن تحمل معك برنامج تشفير: لذلك، نزّل برنامج «تروكريبت»، وافتح ملف التثبيت، مختاراً «إستخرج» عوض «ثبّت» من أجل تخزين البرنامج في شريحة ذاكرة «يو آس بي».
- إقرأ التعليمات لمعرفة كيفية استعمال «تروكريبت».

### إحتفظ بنسخة احتياطية عن بياناتك

من شأن تشفير البيانات المحفوظة في جهازك أو هاتفك الذكي أن يمنع الآخرين من الاطلاع عليها.

**عند استخدام جهاز شخصي:**

- حدّد البيانات التي تريد أن تودعها في نسخة احتياطية. هل تريد أن تنسخ كل شيء، بما في ذلك نظام التشغيل وبرامجك؟ أو تكتفي بنسخ بياناتك، أي ملفاتك ورسائلك الإلكترونية وصورك....؟
- زوِّد نفسك بقرص صلب خارجي يتميّز بسِعَة تخزين كافية لاستيعاب البيانات التي تنوي إيداعها في نسخة احتياطية.
- إختَر وسيلة محددة للنسخ الاحتياطي (باستخدام تطبيق طرف ثالث، كتطبيق «كوبيان» للنسخ الاحتياطي، مثلاً).
- إذا كانت الوسيلة التي تستخدمها للنسخ الاحتياطي الأولي لا توفّر لك ميزة التشفير، إعمل على تشفير جهازك الخارجي بواسطة تطبيقَيْ «بت لوكر» أو «تروكريبت»، بحيث لا يقوى أحد على اختراق بياناتك عند فقدان الجهاز أو تعرّضه للسرقة.
- حدّد وسيلة النسخ الاحتياطي الثاني. هل تستعين بجهاز خارجي آخر أو بإحدى خدمات الإنترنت؟
- إذا كنت تعتمد النسخ الاحتياطي اليدوي، من دون الاستعانة بتطبيق متخصص، لا تنسَ أن تحدد إشعارات تنبيهية للنسخ الدوري، كتدبير روتيني ليس إلاّ.

## لا تحتفظ بنسخ احتياطية في جهازك الشخصي

لا تحتفظ بنسخ احتياطية عن ملفاتك في قسم آخر من جهازك، لأنك ستفقد البيانات الأصلية والمنسوخة إذا سُرق جهازك أو تعطّلت معدّاته.

# ٣: البريد الإلكتروني الآمن

## إستخدام بروتوكول آمن وخدمة آمنة للبريد الإلكتروني، حمايةً لخصوصية مكالماتك

لعلّ إرسال بريد إلكتروني هو أشبه بإرسال رسالة عبر خدمة البريد العادي من دون إيداعه في ظرف مختوم، مما يسمح لأي شخص ينقل الرسالة ضن أروقة المكتب البريدي أن يقرأ مضمونها. فشبكة الإنترنت، كما الشركات المزوّدة خدمة الإنترنت، والأطراف الفاعلة الأخرى ضمن الشبكة، «تحتفظ بنسخة عن» الرسالة التي كتبتها، وقد تقرّر الاطّلاع عليها.

وما العمل إذاً؟ فمعظم المراسلات الشخصية المتبادلة قد لا تهمّ إلا صاحبي العلاقة. لكنّ المراسلات المتعلقة بعملك قد تتضمّن معلومات يُستحسَن ألا تتقاسمها مع شركات تزويد خدمة الإنترنت أو السلطات التي تتحكّم بها. فقد تكون بصدد إرسال آخر مقالة إلى رئيس التحرير، أو تجري مقابلة عبر البريد الإلكتروني مع أحد الناشطين في مجال حقوق الإنسان، حيث يدلي هذا الأخير بتعليقات، قد تكون هامة لشرح الظروف المحيطة بالخبر، إنما توقعه في ورطة كبيرة.

في أيّ حال، كثيرة هي الأسباب التي تدفعك إلى منع أي شخص من الاطّلاع على رسائلك الإلكترونية عدا الشخص الذي تراسله. وتطالعك في ما يلي عدد من الخطوات البسيطة التي تتخذها لتحصين أمن بريدك الإلكتروني:

## المبادئ الأساسية

### إستخدم بروتوكول النقل الآمن "آتش تي تي بي آس"

إذا كنت تستخدم خدمة مجانية للبريد الإلكتروني، ومتاحة للجميع عبر الإنترنت، مثل «جيمايل» أو «هوتمايل»، تأكّد من أنّ هذه الخدمة تؤمّن الاتصالات بين جهازك الشخصي وخادم البريد بموجب هذا البروتوكول. يُشار إلى أنّ كلا الموقعين يتمتع بهذه الميزة، لكنّ موقع «هوتمايل» يمنح لمستخدميه خيار تشغيلها يدوياً في إعداداتهم. إذا كانت مؤسستك الإخبارية أو الطباعية تملك خدمة خاصة بها للبريد الإلكتروني، إسأل المدير المسؤول عن هذه الخدمة كيف يضمن أمن الاتصالات الواردة إلى خادم البريد).

### يعمل بروتوكول "إتش تي تي بي آس" في الاتجاهين

صحيحٌ أنّ الاتصال عبر بروتوكول «آتش تي تي بي آس» يحمي البريد الإلكتروني وهو في طريقه إلى مزوّد خدمة البريد. لكنّ الشخص الذي يتلقى البريد يجب أن يستخدم هذا البروتوكول أيضاً لتأمين الحماية ذاتها عند قراءته.

إذا كنت تتلقى بريدك عبر متصفح معيّن، فلعل أسهل طريقة للتأكد من أنك تستخدم بروتوكولاً آمناً في معرض اتصالك هو أن تخزّن في ذاكرة الكمبيوتر كامل العنوان البريدي (مثلاً https://www.somemailservice.com). أما إذا كانت خدمة البريد التي تعتمدها تعمل بموجب هذا البروتوكول، فلا تخشى أن تفقد فجأة الاتصال عبر هذا البروتوكول بعد تسجيل دخولك.

من شأن الاتصال عبر بروتوكول «آتش تي تي بي آس» أن ينشئ قناة مشفّرة بينك وبين خادم الموقع الإلكتروني (أي الكمبيوتر المقابل الذي «يستضيف» الموقع). فيكون اتصالك بأحد المواقع من خلال

هذا البروتوكول، كمن يتكلم مع صديق عبر أنبوب، بحيث لا يتسنّى لمن هم في الجوار الاستماع إلى ما يجري بينكما من حديث. لكن، من الضروري أن تتذكّر بأنّ هذا البروتوكول لا يؤمّن لك حماية كاملة، بما أنه سيكون متاحاً لمزودي خدمة الإنترنت الاطّلاع على هويتك وأصدقائك، وكذلك على موضوع أي رسالة تبعث بها.

يمكنك أن تتحقّق على الفور مما إذا كانت خدمة البريد الإلكتروني تستخدم وسائل اتصال آمنة: سجّل دخولك إلى حسابك، وتحقق ضمن صندوق بريدك من عنوان الصفحة في الخانة المخصصة في أعلى المتصفح. فإذا كانت تبدأ بـ«آتش تي بي آس» فهذا يعني أنك تستخدم نظاماً آمناً لنقل المعلومات. وإلا... سجّل اشتراكك في حساب مجاني يوفّر لك اتصالات آمنة.

## العلامات المرجعية: بسيطة إنما وسيلة دفاع قوية

إذا كنت تتلقى بريدك عبر متصفح معيّن، فلعل أسهل طريقة للتأكد من أنك تستخدم بروتوكولاً آمناً في معرض اتصالك هو أن تخزّن في ذاكرة الكمبيوتر كامل عنوان الصفحة أو الموقع (مثلاً https://www.somemailservice.com)). أما إذا كانت خدمة البريد التي تعتمدها تعمل بموجب هذا البروتوكول، فلا تخشى أن تفقد فجأة الاتصال عبر هذا البروتوكول بعد تسجيل دخولك.

مجدداً، من المفترض أن تكون متصلاً تلقائياً عبر بروتوكول النقل الآمن إذا كنت تستخدم موقع «جيمايل» للبريد الإلكتروني. أما إذا كنت تستخدم موقع «هوتمايل» أو حساب Live.com، فلا شيء يمنعك من أن تزوّد نفسك بحماية «آتش تي بي آس»، باتّباع التعليمات الواردة على موقع مايكروسوفت تحت عنوان «تعاطَ بجدية مع المسائل الأمنية»:

١. عند استخدام موقع «هوتمايل»، أنقر على **خيارات**، ثم على **مزيد من الخيارات**. وضمن خانة **إدارة حسابك**، إضغط على **تفاصيل عن الحساب**. قد يُطلب منك أن تدخل كلمة السر.
٢. ضمن خانة **خيارات أخرى**، أنقر على "**إتصل من خلال آتش تي بي آس**"، ثم على "**إستخدم آتش تي بي آس تلقائياً**"، وأخيراً على «إحفظ».

### إستخدم برنامج عميل للبريد الإلكتروني

يمكنك أن تضبط تطبيقات البريد الإلكتروني، كتطبيقي «أوتلوك» أو «ثندربرد»، للاتصال تلقائياً من خلال نظام آمن لنقل المعلومات.

عدا ذلك، تؤمّن لك هذه التطبيقات أيضاً بعض الحماية، إذ لا تفقد معها بريدك الإلكتروني نهائياً عند تعرض حسابك للاختراق، بما أنها تحتفظ بنسخة عنها مباشرة في جهازك الشخصي أو شريحة الذاكرة. أما تطبيق «ثندربرد» فيضبط عادةً حسابات البريد الإلكتروني الجديدة بموجب نظام آمن لنقل المعلومات، عند توافر اتصال آمن، إلى جانب قدرتك على ضبط إعداداتك يدوياً.

- تعلّم كيف تضبط حساب بريدك الإلكتروني للاتصال بموجب نظام آمن لنقل المعلومات، عند استخدام تطبيق «ثندربرد».

### أنت لا تبعث برسالة وحسب

عندما ترسل رسالة إلكترونية إلى أحد مصادرك أو مدير التحرير أو أي شخص آخر، إنما ترفقها بمعلومات إضافية من دون أن تلحظ ذلك. وهي معلومات قد تكشف عنك، وعن مضمون رسالتك، أكثر مما تريد. إذ تفصح رسالتك عمّا أوردته في خانة العنوان، حتى ولو كان مضمونها مشفّراً. (إقرأ المزيد حول هذا الموضوع ضمن فقرة **بعض التقنيات المتطورة** أدناه). وكذلك تحتوي كل رسالة تبعث بها على معلومات ضمن خانة العنوان، إذ تكشف عن المسار الذي سلكته عبر الإنترنت، وهي في طريقها إلى المستلم، أو العنوان الأصلي الذي أرسلها. في بعض الحالات، قد يكون ذلك مفيداً، عندما تود مثلاً أن تتحقق مما إذا صديق قد بعث إليك برسالة مشبوهة. وقد يشير من جهة أخرى إلى رسائلك الخاصة التي يتم اعتراضها. إليك بعض الخطوات التي تسمح لك أن تستعرض عنوان البريد في موقع «جيمايل»:

١. سجّل دخولك إلى حسابك، وتوجّه إلى صندوق بريدك؛
٢. إختَر أي رسالة، وافتحها؛
٣. في خانة «أنظر القائمة المنسدلة»، إختَر «أظهر العنوان الأصلي»؛
٤. سيطالعك الآن العنوان.

## كلمات السر يمكن أن تكون نقطة ضعفك

لعلّ كلمة السر الضعيفة هي أسهل سبيل لاختراق حساب بريدك، كما تبيّن، للأسف الشديد، لعدد من السياسيين في السنوات الأخيرة. لذا، تذكّر أن تختار كلمة سر طويلة ومعقدة، لا يسهل التكهنّ بها.

بناءً على ذلك، قد تود أن تختبر شبكة تور أو شبكة افتراضية خاصة (راجع الفصل المتعلق بالتصفح الآمن للحصول على معلومات إضافية حول هذين البرمجيتين)، لإخفاء موقعك وعنوان بروتوكول الإنترنت (العنوان المرتبط بجهازك الخاص أو نقطة وصولك).

## فكّر قبل أن تفتح الروابط، ترد أو تنقر عليها

قد تصلك ذات يوم رسالة موجزة يخال إليك أنها من أحد زملائك في العمل، أو زملائك المدونين، يخبرك فيها أنه تعرّض للسرقة وهو في زيارة إلى الخارج، طالباً منك أن ترسل إليه مبلغاً من المال على الفور. أو قد تردك رسالة يخال إليك أنها من الشركة التي تزوّدك بخدمة الإنترنت، تنبئك فيها بأنّ حسابك سيتعرّض للإقفال ما لم تؤكّد كلمة السر التي تستخدمها. هذا النوع من الهجمات، التي تأتيك من بريد يبدو لك في الظاهر حقيقياً، ويدفعك إلى القيام بعمل ما (كالإفصاح عن كلمة السر أو إرسال مبلغ مالي) يُعرَف بالتصيّد الإلكتروني، وبات شائعاً اليوم حتى أصبح جزءاً من الألاعيب التي تعبث في الخفاء بصندوق بريدنا.

إلا أنّ لهذه الظاهرة مخاطر حقيقية، باعتبار أنّ البريد المرسل لهذا الغرض يكون مكتوباً في بعض الحالات بعناية فائقة لاستهداف منظمات وأشخاص معيّنين، فيسمى بالتالي التصيّد بالرمح (التصيّد الهادف). ففي أيار/مايو ٢٠١١، أعلنت شركة غوغل أنها رصدت حملة واسعة من الرسائل الإلكترونية التي كان يتلقاها مئات الأشخاص في المؤسسات الحكومية والمنظمات غير الحكومية، من أصدقائهم أو زملائهم بحسب ظنّهم. إنما تبيّن لهم في الواقع أنّ هذه الرسائل كانت تَردهم من قراصنة ضمّنوها روابط تقودهم إلى خوادم متواجدة في بلدان أخرى، بهدف الوصول إلى أي بيانات تقع في مصيدتهم. من الضروري للصحافي، بحكم وظيفته، أن يتنبّه إلى أنّ هذا النوع من الهجمات يستهدفه خصيصاً، لذا لا يضيره البتة أن يتوخّى الحذر عند تصفّح البريد الوارد إليه:

**لا تنقر على الروابط الواردة ضمن البريد:** فالروابط غير المشبوهة في الظاهر قد ترسلك إلى عنوان مختلف عن العنوان المبيّن، أو تنتهي بنقل فيروس إلى جهازك الشخصي. لذا، حين يزوّدك أحدهم برابط يبدو لك عادياً للوهلة الأولى، من الأوفق لك أن تنسخ العنوان وتلصقه في متصفحك.

**لا تفتح الملفات المرفقة ببريدك:** لأنّ هذه الملفات، التي تَرِد على شكل صور أو وثائق، قد تحمل معها فيروسات تستقر في جهازك حين تنقر عليها مرتين. إذا كنت تعرف المرسل وتتوقّع استلامها، فاحرص على أن يقوم التطبيق المضاد للفيروسات الذي تستخدمه بمسح الملفات المرفقة قبل فتحها. ولكن، إيّاك أن تفتح الملفات المرفقة التي تردك من شخص لا تعرفه.

**عطّل وظيفة الصور:** لأنّ الصور الواردة ضمن البريد تتضمّن أحياناً روابط مخفية تصلك بمواقع إلكترونية أو أجهزة كمبيوتر متواجدة في أمكنة أخرى، بحيث تترتّب عليك عواقب أخرى بمجرد أن تفتح بريدك، كأن تنزّل عن غير قصد بعض الرموز المتعلقة بجهازك. فمن شأن تعطيل وظيفة تحميل الصور في بريدك أن تقلّص إمكانية تعرضك لهذا النوع من الهجمات.

- تعلّم كيف تعطّل وظيفة الصور في خدمة «جيمايل»؛
- تعلّم كيف تحجب الصور في خدمة «أوتلوك»؛
- تعلّم كيف تفعّل وظيفة التحقق بخطوتين لحساب غوغل الذي تستخدمه.

## أنشئ حساباً مجهول الهوية لأغراض العمل

قد ترغب في الاحتفاظ بحساب منفصل للبريد الإلكتروني، لا يُستدّل منه إلى اسمك الحقيقي، أو عنوانك، أو رقم هاتفك الجوّال، أو أي معلومات أخرى تعرّف عنك، ويسهم بالتالي في الحفاظ على خصوصيتك حينما تعمل على مشروع حسّاس. كما يقلّص حجم الأضرار التي تحلّ ببريدك وقائمة اتصالاتك عند اختراقهما (والعكس صحيح).

## تأكّد من أنك لا تحيل بريدك إلى شخص آخر

كثيرة هي حسابات البريد، بما فيها حسابات خدمة «جيمايل»، التي تسمح لك اليوم أن تحيل تلقائياً نسخةً عن مراسلاتك إلى عنوان بريدي آخر. تثبت هذه التقنية فائدتها بالنسبة إلى الصحافيين الذين قد يضطرون إلى تشغيل أكثر من حساب. ولكن، إذا تمكّن أحدهم من الوصول إلى حساب بريدك الإلكتروني، فبإمكانه أن يضيف عنوانه البريدي إلى قائمة الأشخاص الذين تحيل إليهم رسائلك، وأن يستلم نسخ عن رسائلك، من دون الحاجة إلى دخول حسابك مجدداً. لذا، تحقق دوماً من إعدادات حسابك للتأكّد من أنّ أحداً لم يضِف صندوقه البريدي إلى صندوقك.

- تعلّم كيف تتحقق من وضعية إعدادات الإحالة في جهازك.

## راجع أنشطة حسابك

تسمح لك بعض خدمات البريد عبر الإنترنت، كخدمة «جيمايل»، أن تراجع أنشطة حسابك، فتعرف بالضبط متى وأين كان موضع استخدام.

- تعلّم كيف تطّلع على آخر أنشطة حسابك في موقع «جيمايل».

## لا تربط الحسابات بعضها ببعض

تخوّلك بعض خدمات الإنترنت اليوم أن تستخدم بيانات الدخول الخاصة بخدمة موقع شريك لتسجيل دخولك، كأن تستخدم مثلاً بيانات حساب بريدي «لفكّ شيفرة» حساب إحدى شبكات التواصل الاجتماعي، مما يمكّنك من تتبّع آخر الأخبار المتعلقة بخدمة معيّنة

عن طريق استخدام خدمة أخرى. لا شكّ أنّ هذه التقنية تناسبك إلى حد كبير، خاصةً إذا كنت تريد أن تنشر أخباراً، ثم تعمل على ترويجها عبر شبكات التواصل الاجتماعي. ولكنها تعني في المقابل أنّ أي شخص يستحصل على كلمة سر أحد الحسابين، قد يستولي فجأةً، وبلمح البصر، على كلمة السر الأخرى.

## إعتمد أدوات تعريف قوية

تتيح لك بعض خدمات الإنترنت أن تحمي حسابك بالمزج بين عدة معلومات، على شكل كلمة سر ورمز ترسلهما مثلاً إلى هاتفك الجوال. مما يعني أنّ الشخص الذي يحاول اختراق حسابك يحتاج إلى هاتين المعلومتين لتحقيق مبتغاه. لحسن الحظ أنّ هذا النوع من الحماية الإضافية راح يلقى رواجاً واسعاً، باعتبار أنّ موقعي «فايسبوك» و«دروب بوكس»، إلى جانب خدمات أخرى، صارا يوفّران هذه الميزة بين الخيارات المتاحة. وبالتالي، يمكن أن تفعّل حماية حسابك في موقع «جيمايل»، مثلاً، بضبط إعدادات حساب غوغل.

## عند استخدام جهاز مشترك

إذا كنت تستخدم جهازاً مشتركاً في مكتب التحرير أو مقهى الإنترنت، يكمن التحدي الأكبر بالنسبة إليك في الحفاظ على خصوصية اتصالاتك. ففي هذه الحال، إضافة إلى المخاطر التي تلحظها ضمن البيئة المحيطة بك، تبرز مخاطر أخرى قد تغفل عنها، مثل راصد لوحة المفاتيح، وهو نوع من البرمجيات الخبيثة التي تسجّل كل ما يُكتب بلوحة المفاتيح، أو أي برمجيات خبيثة أخرى.

لهذا السبب، فليكن بحوزتك متصفح محمول مزوّد بوظائف إضافية للحماية (راجع الفصل المتعلق بالتصفح الآمن لمزيد من المعلومات حول هذه الوظائف) أو متصفح يشكّل جزءاً من حزمة إخفاء الهوية، على شاكلة حزمة متصفح تور. إلى ذلك، تبرز أيضاً إمكانية تشغيل أي برنامج محمول لفحص البرمجيات الخبيثة، كبرنامج مايكروسوفت لفحص أمن الجهاز أو برنامج «كومودو» لإزالة الفيروسات والملفات الضارة، من شريحة ذاكرة لرصد المخاطر المعهودة. ولكن، تنبّه إلى أنّ أي أدوات أخرى، أو حتى برمجيات مشروعة لإدارة الشبكات، قد تعرّض اتصالاتك للخطر، من دون التعرّف عليها كبرمجيات خبيثة.

# ٤: التصفّح الآمن

**تزويد متصفحك بميزات إضافية لتحصين أمنك، وتعزيز خصوصية اتصالك بالمواقع الإلكترونية.**


تشكّل شبكة الإنترنت سلاحاً قوياً بيد الصحافيين، والأشخاص الذين يتواصلون معهم. ولكن، يجدر بهم أن يتقنوا استخدامها تجنّباً لأي مشاكل قد تثيرها، شأنها شأن أي أداة أخرى.

يجوز أن يُصاب متصفحك أو جهازك الشخصي بفيروس من دون أن تنقر على أي روابط في الصفحة. فمن شأن زيارة أي موقع بهدف إجراء الأبحاث أو قراءة بريدك من خلال وسيلة اتصال غير آمنة، قادرة على أن تراقب نشاطاتك عن كثب، أن تسمح لأي شخص في الاستحصال على معلومات عن عاداتك وموقعك. فكما ذكرنا في الفصل المتعلق بالبريد الآمن، من الأوفق الاتصال بمواقع الإنترنت من خلال بروتوكول «آتش تي تي بي آس»، عوض الاتصال بها عبر بروتوكول «آتش تي تي بي» العادي، تعزيزاً لأمنك.

فهذه الخطوات تساعد بالطبع على تحصين أمنك، عند استخدام متصفحك.

**(إذا أردت أن تتصفح أي موقع من دون الكشف عن هويتك، أحرص على الاطّلاع على بعض التقنيات المتطورة وفقرة المصادر والمراجع الإضافية).**

## المبادئ الأساسية

### إستخدم متصفح آمن

قد تدخل الشركات في نقاش حول متصفح الإنترنت الأكثر أماناً، ولكنّ الأكيد أنّ «فايرفوكس» ينعم بأكبر قدر من الملحقات الإضافية لخدمات الأمن والحفاظ على الخصوصية.

### حماية نتائج أبحاثك

يتمكّن بعض محركات البحث من حماية نتائج أبحاثك بفضل الاتصال عبر بروتوكول «آتش تي تي بي آس» الآمن. تجدر الإشارة إلى أنّ موقعي غوغل و«داك داك غو دوت كوم» يوفّران هذه الميزة. ناهيك عن أنّ هذا الأخير ينتهج سياسة عدم تعقّب سجل البحث الذي يقوم به مستخدموه.

أما الملحقات فهي تطبيقات بسيطة تزوّد المتصفح بميزات جديدة. ويشمل متصفح «فايرفوكس» بعض الملحقات الأكثر فائدةً:

- «نوسكريبت»: يمنع صفحات الإنترنت من تنزيل تطبيقات أو إطلاق أي برنامج على جهازك الشخصي من دون علمك.
- «آتش تي تي بي آس إيفريوير»: يُطلِع هذا التطبيق المستخدمين تلقائياً على إصدارات المواقع التي تستخدم هذا البروتوكول، وهي الإصدارات التي يكون فيها الاتصال بين الجهاز الشخصي أو الهاتف والموقع مشفّراً. صحيحٌ أنّ قائمة المواقع التي تنطبق عليها هذه التطبيقات الإضافية هي محدودة، ولكنها تشمل عدداً كبيراً من المواقع المعروفة.
- «آتش تي تي بي آس فايندر»: يسمح هذا التطبيق للمستخدمين إدراج مواقع إضافية ضمن قائمة «آتش تي تي بي آس إيفريوير» للمواقع المحمية.
- «بيتر برايفيسي»: يحذف هذا التطبيق «ملفات الكوكيز» الموجودة في متصفحك منذ أمد طويل، والمحتمل استخدامها لتعقّب نشاطاتك.

- «دبليو أو تي (ويب أوف تراست)»: يصنّف المواقع من حيث مراعاتها للخصوصية وإيحائها بالثقة، إستناداً إلى أصوات مستخدمي المواقع الأخرى.
- «برسبكتيفز»: يتحقق من صحة شهادة النظام الآمن لنقل المعلومات التي تعتمدها مواقع آمنة، رصداً للشهادات المحتمل أن تكون مزيّفة.

تجد على موقع «موزيلا» مزيداً من التطبيقات الملحقة لتدعيم الخصوصية والأمن.

هل أستخدم كروم؟ يمكنك أن تجد أيضاً بعض الملحقات الأمنية لدى متصفح غوغل، بما فيها تطبيقات «آتش تي تي بي آس إيفريوير»، و«برسبكتيفز»، و«دبليو أو تي».

## تحقق من إعداداتك الأمنية

تحفظ برامج التصفح في ذاكرتها الكثير عنك وعن عاداتك، ما لم تطلب منها خلاف ذلك. وبحكم مهنتك كصحافي، قد يكون لهذه المعلومات أهمية بالغة، خاصةً إذا كان عملك يؤثّر على شركات ضخمة أو أشخاص نافذين في الحكم. لذا، بإمكانك أن تقلّص قدر المستطاع المعلومات التي يتذكرها متصفح «فايرفوكس»، تفادياً لمشاكل الرقابة المعهودة، عن طريق إضافة بعض أدوات الحماية الأخرى ضمن لوحة الخيارات. فابدأ باختيار أيقونة الأدوات في القائمة المستعرضة، ثم «خيارات»:

في باب الأمن:

- إختر المربّع نبّهني عندما يحاول أي موقع تنزيل تطبيق ملحق، وكذلك المربّع المخصص لحجب مواقع الهجوم، وحجب المواقع المزيّفة.
- عطّل خيار المربّع الذي يسمح بتذكّر كلمات السر المحددة للمواقع.

في باب الخصوصية:

- إختَر المربّع أعلِم المواقع الإلكترونية أنني لا أريد تعقّب نشاطاتي، مستخدماً وضعية التصفّح الخاص على الدوام.

## إستخدم شبكة إفتراضية خاصة

تشكّل الشبكة الافتراضية الخاصة قناة تربط بين جهازك الشخصي وخادم موجود في بلد آخر؛ مما يمنحك مزيداً من الخصوصية عندما تتصفّح شبكة الإنترنت، أو تبحث عن مقالات، أو تجري مقابلات عبر الإنترنت. (إلا أنها لا تمنع الشركة المسؤولة عن إدارة هذه الشبكة الافتراضية الخاصة من الاطّلاع على المحتويات التي تتناقلها مع المواقع الإلكترونية. لهذا السبب، تبقى بحاجة إلى الاتصال بموقع يعتمد بروتوكول «آتش تي تي بي آس»! كما لا تمنع مدير الشبكة من الاحتفاظ بقائمة المستخدمين والمواقع التي يزورونها).

### هل ملفات "الكوكيز" مفيدة أو مضرّة؟

إنّ ملفات «كوكي»، أي علامات التبويب التي تدرجها المواقع ضمن متصفحك، لمساعدتها على تذكّرك أو تعقّبك وأنت تتنقّل عبر شبكة الإنترنت، ليست مفيدة ولا مضرّة في الواقع.

لا بل يُعتبر بعضها مفيداً، كالملفات التي تسمح لك مثلاً الانتقال من قسم في موقع تسجل دخولك إليه إلى موقع آخر، من دون الاضطرار إلى إعادة كتابة كلمة السر في كل صفحة (هل حدث لك أن سجّلت دخولك إلى موقع «جيميل»، ثم فتحت روزنامة غوغل من الحساب ذاته، من دون أن تضطر إلى تسجيل الدخول مجدداً؟). إلا أنّ ملفات أخرى قد تُستغلّ لتعقّب المواقع التي زرتها، وتبادل هذه المعلومات مع شخص يودّ استخدامها ضدك أو الإساءة إليك.

يتيح لك بعض المتصفحات أن تختار بنفسك احتفاظ المواقع، أو عدم احتفاظها، بملفات «الكوكي». وفي هذا الإطار، يخوّلك غوغل كروم مثلاً أن «تمنع تثبيت ملفات كوكيز لطرف ثالث» ضمن إعدادات محتوياته، مما يحول دون تنزيل بعض الملفات التي قد تنطوي عليها الدعايات. لتشغيل هذه الميزة، أمتب «كروم://إعدادات/محتويات» ضمن شريط عنوان غوغل كروم.

بدأت بعض المتصفحات مؤخراً إدراج خيار إضافي «لا تتعقّب» ضمن إعدادات الخصوصية (على مثال متصفح «فايرفوكس» الذي يوفّر هذا الخيار ضمن مربّع في أعلى إعدادات الخصوصية).

توفّر بعض الشبكات الافتراضية الخاصة خدمات معيّنة مجانية، بما فيها:

- «بي سايفون ٣»، برنامج عميل لشبكة افتراضية خاصة قائم بذاته، يمكنك تشغيله من شريحة ذاكرة على جهازك، ويقوم بالتحديث التلقائي بفضل إدراج عناوين بروتوكولات جديدة للخوادم ضمن خدمة «بي سايفون».
- الشبكة الافتراضية الخاصة «رايز أب» تتوافر لأي مستخدم

يملك حساباً مجانياً في البريد الإلكتروني RisepUp.net، ويمكن الوصول إليها من خلال تطبيق للشبكات الافتراضية الخاصة، كالشبكة الافتراضية الخاصة المفتوحة، علماً أنّ هذه الأخيرة تتوافر أيضاً على شكل تطبيق محمول.

- «هوت سبوت شيلد»، تطبيق مدعوم بالدعايات، يمكن تنزيله على جهاز الكمبيوتر الخاص مباشرة.

من الضروري التنبّه إلى أنّ **الشبكات الافتراضية الخاصة لا تخفي هوية المستخدم**. فعند اتصالك بهذه الخدمة، يحصل المسؤولون عنها على معلومات تتعلق بك بقدر المعلومات التي يحصل عليها مزوّدو خدمة الإنترنت، بما في ذلك المواقع التي تزورها.

- وسّع معرفتك بتطبيق «بي سايفون ٣»، وهو الحلّ المجاني للشبكات الافتراضية الخاصة، عن طريق إرسال رسالة فارغة إلى عنوان البريد get@psiphon3.com.
- إتّبع التعليمات الصادرة عن موقع RisepUp.net بشأن ضبط خدمة «رايز أب» للشبكات الافتراضية الخاصة.
- نزّل تطبيق هوت سبوت شيلد.

## إستخدم النقاط الساخنة لنظام الاتصال اللاسلكي واي فاي مع وسيلة اتصال محمية

إذا كنت تستخدم تقنية واي فاي للاتصال بشبكة الإنترنت، سواء في مكان عام أو مكتب التحرير، تأكّد من أنّ الاتصال اللاسلكي بجهاز التوجيه يخضع لحماية التشفير بموجب بروتوكول الوصول المحمي للشبكة اللاسلكية أو بروتوكول الوصول المحمي ٢ (علماً أنّ هذا الأخير هو الأفضل)، وتجنّب الأماكن التي تعتمد الخصوصية المتكافئة للاتصال اللاسلكي، أو التي لا توفّر أي وسيلة تشفير إطلاقاً.

عندما تفتح أي متصفح في مكان اتصال عام، تطالعك للوهلة الأولى صفحة إلكترونية تطلب منك تسجيل كلمة السر. قد لا يبدو لك هذا التدبير مثيراً للريبة، إنما يدلّ فقط على أنّ صاحب المكان يريد أن يراقب كل من له وصول إلى شبكة اتصالاته. لكنّ اتصالك بجهاز التوجيه، لسوء الحظ، لا يحظى بأي حماية.

للتأكّد مما إذا اتصالك بنقطة الوصول إلى خدمة واي فاي محمياً، ما عليك سوى أن تنقر بالزر الأيمن على أيقونة الشبكة، البادية في الزاوية اليمنى السفلى من الشاشة، ووجّه مؤشر الفأرة إلى إسم الشبكة، فيطلعك النص الذي يبرز أمامك إذا كانت وسيلة الاتصال محمية، وشكل الحماية التي تحظى بها. كما يمكنك أن تستخدم برنامجاً مجانياً مثل «إينسايدر» للحصول على معلومات أكثر تفصيلاً عن شبكات الاتصال المتوافرة ضمن منطقتك. **من هنا يجدر بك أن تتصل بمواقعك المفضلة من خلال بروتوكول "آتش تي تي بي آس"، أو أن تستخدم الشبكات الافتراضية الخاصة، ولو كنت تستخدم نقطة ساخنة محمية**. ولكن، تنبّه إلى أنّ هذه الشبكات الافتراضية تحمي اتصالاتك محلياً، إنما لا تستطيع أن تمنع أي شخص يشغّلها من الاطلاع على النشاطات التي تقوم بها على موقع لا يعتمد البروتوكول المذكور.

### إلى أي درجة تحفظ وضعية التصفح الخاص خصوصيتك؟

هل تلتزم وضعية التصفّح الخاص بمعايير الخصوصية؟ تسمح لك غالبية المتصفحات أن تمنع المتصفح نفسه من الاحتفاظ في ذاكرته بنشاطات التصفح أو التحميل أو البحث التي قمت بها. ولكنها لا تخوّلك أن تحافظ على خصوصيتك عبر الإنترنت، باعتبار أنّ مقدّمة خدمة الإنترنت والمسؤولون عن المواقع التي تزورها يكونون على علمٍ بمكانك وأعمالك، ما لم تتخذ الخطوات الكفيلة بحماية اتصالك، واستخدام أداة لإخفاء هويتك.

- برنامج «إنسايدر» هو أداة مجانية تعرض معلومات عن نقاط الاتصال الساخنة بنظام واي فاي ضمن منطقتك.

### عند استخدام جهاز مشترك:

- إذا كنت تستخدم جهازاً مشتركاً في مكتب التحرير أو مقهى الإنترنت، قد يصعب عليك أن تتصفّح المواقع تحت جناح السرية، إذ، إلى جانب التحديات الناشئة عن البيئة المحيطة بك بحدّ ذاتها، يجوز أن يتعرّض جهازك للاختراق من قبل برمجيات خبيثة، أو من قبل برمجيات تتعقّب سلوكيات الموظفين في بعض المؤسسات.
- صحيحٌ أنك لا تضمن الحصول على سرية تامة، ولكن بإمكانك أن تتخذ بضع خطوات لتعزيز حمايتك. فعلى سبيل المثال، بإمكانك أن تنزّل من شريحة ذاكرة برنامجاً محمولاً لفحص البرمجيات الخبيثة، كبرنامج مايكروسوفت لفحص أمن جهازك أو برنامج كومودو لإزالة الفيروسات، بحثاً عن أي برمجيات خبيثة قبل أن تبدأ بالتصفح. ولكن، تنبّه دوماً إلى أنّ البرمجيات المرخّصة لإدارة الأجهزة الشخصية التي تتعقّب نشاطاتك، قد لا يتمّ التعرّف عليها كبرمجيات خبيثة.
- يجدر بك أن تستعين بشبكة افتراضية خاصة محمولة، وبمتصفح محمول، يتمتعان بتطبيقات إضافية لحفظ الأمن. ومن هذا القبيل، يجوز أن تسمح لك حزمة متصفح تور، التي تأتي أيضاً على شكل نسخة محمولة، بالحصول على بعض الخصوصية المحلية وإخفاء هويتك عبر المواقع التي تزورها.

### عند استخدام هواتف ذكية:

- يشغّل الهاتف الجوّال نسخاً خاصة من المتصفحات المعدّة خصيصاً لمنصاته، علماً أنّ النسخ قد لا تتضمّن متصفح فايرفوكس أو تحتمل الملحقات المذكورة أعلاه.
- عند استخدام هاتف يعمل على نظام أندرويد، يتسنّى لك أصلاً الاستفادة من بعض ميزات الخصوصية التي يوفّرها تطبيق «أوربوت» من مشروع «غارديان».

## لا تستعجل فتح الوثائق

ينصح فريق برنامج «تور» المستخدم الإحجام عن فتح الوثائق المحمّلة، وهو ما يزال موصولاً بالإنترنت، إذ قد يعمد حاسوبك، في هذه الحالة، وعن غير قصد، إلى تسريب معلومات عن الجهاز وعنك.

## الفارق بين الشبكة الافتراضية الخاصة وشبكة تور

ما الفرق بين الشبكة الافتراضية الخاصة وشبكة تور؟ تقوم الشبكة الافتراضية بتشفير الاتصال القائم بين جهازك وخادم الشبكة، الموجود ربما في بلد آخر، بحيث يتعذّر على المستخدمين ضمن حدود منطقتك المباشرة، كمزوّد خدمة الإنترنت أو الشخص الذي يتصل بتقنية واي فاي عبر نقطة اتصال غير محمية، الاستحصال على معلومات شخصية عنك، فيما يتسنّى للشخص الذي يعمل على شبكة افتراضية خاصة معرفة مصدر اتصالك، وعنوان بروتوكول الإنترنت، والمواقع التي تزورها، وكذلك مضمون ما تكتب وتقرأ، عند اتصالك من بريد غير محمي.

أما الاتصال عبر شبكة تور (نظام التوجيه البصلي)، وخلافاً للشبكة الافتراضية، فيكون أشبه باستعمال ثلاث شبكات افتراضية مترابطة ضمن سلسلة، حيث لا تعلم كل شبكة إلا «بالحلقة» التي تسبقها أو تليها مباشرة ضمن هذه السلسلة. وبالتالي، فإنّ الخادم الأول يعرف أنك موصول بالإنترنت، من دون أن يستدلّ إلى المواقع التي تزورها، فيما يعرف الخادم الأخير أنّ أحد المستخدمين يزور موقعاً معيّناً، إنما يتعذّر عليه معرفة هويته.

راجع التعليمات المتوافرة عبر موقع منظمة «موبايل أكتيف» بشأن تصفّح الإنترنت بكل سرية من خلال استخدام تطبيق «أوربوت».

## بعض التقنيات المتطورة

### إستخدم شبكة تور لإخفاء موقعك

تخفي شبكة تور (نظام التوجيه البصلي) اتصالك بالإنترنت بواسطة ثلاث طبقات من التشفير، ثم تنزعها، الواحدة تلو الأخرى، قبل أن تقودك إلى الموقع الإلكتروني الذي ترغب في زيارته. وبالتالي، يتسنّى لهذه الشبكة، من خلال «المحطات القصيرة» الإضافية التي توفّرها في رحلتك عبر الإنترنت، أن تحجب المواقع التي تزورها عن أنظار مزوّد خدمة الإنترنت المحلي، فيما تخفي أيضاً مكانك الفعلي عن المواقع التي تزورها.

أما فوائدها الثانوية فتكمن في أنها قد تتيح لك الوصول إلى المواقع التي تكون محجوبةً عادةً ضمن منطقة تواجدك، عند استخدام حزمة متصفح تور، التي تتضمّن نسخة محمولة للمتصفح، مضبوطة مسبقاً لضمان لحسن استخدامها.

إذا كنت تريد الإفادة من حماية «تور» ضمن نطاق خدمات الإنترنت الأخرى، كخدمتي الرسائل القصيرة أو البريد الإلكتروني، فاقرأ المعلومات الواردة في موقع مصممي الشبكة قبل استخدامها. ولكنك لن تجني أي إفادة منها ما لم تحسن ضبط تطبيقك لتشغيل هذه الخدمات، على حدّ ما يشددون عليه. كما ينصح مطوّرو شبكة «تور» بعدم تنزيل ملحقات إضافية على متصفحهم المحمول، (إذ يأتي المتصفح عادةً مزوّداً بتطبيقات ملحقة مثل «آتش تي تي بي آس إيفريوير» و«نوسكريبت» المثبتة مسبقاً).

### إستخدم خدمة "أوبن دي آن آس" أو "بابلك دي آن آس" من غوغل

نظام إسم النطاق هو بمثابة فهرس الإنترنت. فهو يحفظ إسم النطاق الذي تسجّله، مثل «yahoo.com»، ويترجمه إلى عناوين محددة للغاية، ومرقّمة على الشكل الآتي: «١٤٠. ٣٨. ٣٠. ٧٢»، مما يسمح لمتصفحك أن يجد في المكان ذاته الخادم اللازم للعثور على الموقع الذي تريده تحديداً.

## إذا كانت خدمة الاتصال بطيئة

بما أنّ شبكة تور يتمّ تشغيلها عبر عدة خوادم متسلسلة، فقد يتسبّب ذلك بإبطاء تصفحك عبر الإنترنت. لذا، فلتحصر دوماً استعمال تور بالأعمال الحساسة، فيما تستعمل خدمة الاتصالات العادية للأعمال المعهودة.

تعتمد شبكة الإنترنت، لتضمن حسن عملها، على نظام إسم النطاق الذي يلقى ثقة كبيرة لدى المستخدمين.

لسوء الحظ أنّ خادم نظام إسم النطاق قد يتعرض أحياناً للقرصنة، أو تُعاد كتابة دليل العناوين بهدف حجب بعض المواقع أو إرسال المستخدمين إلى نسخ مزوّرة من صفحات الويب التي كانوا يتوقعونها.

إنّ خدمتي «أوبن دي آن آس» و«بابلك دي آن آس» من غوغل المجانيتين حققتا كلاهما نجاحاً كبيراً في حماية خوادمها، عدا عن أنهما لا تحجبان المواقع الإلكترونية (مع أنّ الخدمة الأولى توفّر للأهل خيار حجب بعض المحتويات).

- إقرأ التعليمات بشأن التحوّل إلى خدمة «أوبن دي آن آس».
- إقرأ التعليمات بشأن التحوّل إلى خدمة «بابلك دي آن آس».

### سبب آخر لاعتماد بروتوكول "آتش تي تي بي آس"

عندما يحاول حاسوبك الاتصال بموقع إلكتروني عبر بروتوكول «آتش تي تي بي آس»، سيعمد متصفحك في خطوة أولى إلى التحقق من شهادة النظام الآمن لنقل المعلومات، وهي بمثابة بطاقة الهوية المطلوبة لاستكمال الاتصال. فإذا بدت الشهادة غير صالحة، ستتلقّى تنبيهاً من متصفحك، ما كنت لتتلقّاه نتيجة اتصال عادي بالموقع ذاته عبر البروتوكول المذكور.

## مصادر ومراجع إضافية

### "فرونت لاين دفيندرز" و"تاكتكل تكنولوجي"

- فيديو: دليل «أونو» للتصفح الآمن
- كيف تحافظ على المجهولية وتتجاوز الرقابة على الإنترنت

### كيف تتجاوز الرقابة على الإنترنت

- كيف تتجاوز الرقابة على الإنترنت

### مراسلون بلا حدود

- كتيّب للمدونين والمعارضين الناشطين عبر الإنترنت
- تقرير ٢٠١٢ حول «أعداء الإنترنت»

### نصائح غوغل لحفظ السلامة عبر الإنترنت

- الشبكات الآمنة

### مؤسسة الحدود الإلكترونية

- آليات التدوين الآمن (بشأن العمل أو أي موضوع آخر)
- نزّل التطبيق الملحق «آتش تي تي بي آس إيفريوير» لمتصفحي «فايرفوكس» أو «كروم»

### صفحة ويكي حول الرقابة على الإنترنت

- آليات الحجب وكيفية تجاوزها

### (التطبيقات الإضافية) لمتصفح "موزيلا دوت أورغ"

- «نوسكريبت»
- «دبليو أو تي»
- «برسبكتيفز»
- «آتش تي تي بي آس فايندر»

### شبكة الأصوات العالمية

- التدوين المجهول الهوية باستخدام برنامجي «وورد بريس» و«تور»

### منظمة موبايل أكتيف

- إخفاء الهوية عبر الهاتف الجوّال والتحايل على أساليب الرقابة: كيف السبيل لتصفّح الإنترنت بسرية من هاتفك الجوّال.
- دليل المستخدم إلى «أوربوت»: تصفّح شبكة تور على هاتفك الجوّال من دون الكشف عن هويتك.

## قائمة مرجعية للتصفح الآمن

### عند استخدام جهاز كمبيوتر شخصي:

- إستخدم «فايرفوكس».
- نزّل تطبيقات ملحقة لحماية الخصوصية والأمن.
- غيّر إعدادات المتصفح، منعاً لتسجيل معلومات لا تحتاج إليها أو تريدها.
- عزّز خصوصيتك المحلية باستخدام شبكة إفتراضية خاصة مجانية، أو حزمة متصفح تور لمزيد من السرية.
- إستخدم تطبيق «أوبن دي آن آس» أو «بابلك دي آن آس» من غوغل، منعاً لتوجيهك نحو مواقع إلكترونية وهمية.

### عند استخدام جهاز كمبيوتر مشترك:

- تحقّق من خلو الجهاز المشترك من أي برمجيات خبيثة.
- إستخدم نسخة محمولة من الشبكة الافتراضية الخاصة والمتصفح، أو استخدم حزمة متصفح تور.

### عند استخدام هواتف ذكية:

- تحرَّ عن المتصفحات المتطابقة مع هاتفك، وعن التطبيقات الإضافية المتوافرة، عند توافرها.
- إذا كنت تستخدم هاتف يعمل على نظام أندرويد، قد تكون أصلاً قادراً على الاستفادة من بعض ميزات الخصوصية التي يقدّمها تطبيق مشروع «غارديان».

# ٥: شبكة واي فاي آمنة

**الاتصال اللاسلكي بجهاز التوجيه بمأمن عن المتنصّتين وسواهم من "العابثين".**

تتيح نقاط الوصول اللاسلكية العامة إلى الصحافيين إنجاز أعمالهم أينما وجدوا، سواء أكانوا في مقهى أو فندق أو مدرسة أو مطار. ولكنهم قلّما يحظون بالحماية اللازمة التي يؤمّنها لهم نظام التشفير، مما يجعلهم لقمة سائغة للقراصنة وسواهم من الأشخاص الذين يطمعون برصد تحركات المستخدمين غير المحميين، أي البيّنات/البيانات المتدفقة ذهاباً وإياباً من الإنترنت، والتي قد تشمل بريدك الإلكتروني وما تنشره عبر فايسبوك، وتغريداتك.

وكان مطوّر البرامج، إيرك باتلر، من لفت الانتباه إلى هذا الأمر في أواخر العام ٢٠١٠، حين أصدر تطبيقاً إضافياً مجاناً من «فايرفوكس»، يُدعى «فايرشيب»، يسهّل على أي شخص يملك جهاز كمبيوتر محمولاً أن يستولي على حساب الفايسبوك الخاص بك، أو على جلسة تويتر بعد أن تسجّل دخولك، ثم يقرأ رسائلك الخاصة، وينشر تحديثات منتحلاً هويتك. وقد سُجِّل تنزيل هذا التطبيق الإضافي أكثر من مليوني مرة منذ أن وُضِع قيد الاستعمال.

(لحسن الحظ أنّ الاتصال بالمواقع الإلكترونية بواسطة نظام واي فاي يبعد شبح هذا التهديد. راجع الفصل المتعلق بالتصفح الآمن للاستعلام أكثر عن هذا الموضوع، وعن وسائل أخرى لحماية اتصالاتك في الأماكن العامة).

إذا كنت موصولاً بشبكة واي فاي في مكتب التحرير، يُستحسن أن تكون محميّة أصلاً ببروتوكول الوصول المحمي أو بروتوكول الوصول المحمي ٢ للتشفير، منعاً للغرباء من اختراقها. ولكن، إذا لم يكن جهاز التوجيه الذي تستخدمه «محصّناً» بما يكفي لصدّ الهجمات، خصّص بضع دقائق لتعديل الإعدادات المبدئية.

## ليست المسألة مسألة إسم

يعمد بعض الأشخاص إلى إطلاق تسميات مخيفة على جهاز التوجيه (مثل «ضع فيروسك المجاني هنا») منعاً للأشخاص غير المرغوب فيهم من استخدامه. ولكنك لا تنوي بالطبع الاتكال على هذه الحيلة للحصول على الحماية.

## المبادئ الأساسية

### غيّر كلمة السر الموضوعة من قبل مدير الجهاز

تأتي غالبية أجهزة التوجيه، مصحوبة بكلمة سر مضبوطة أصلاً، عند استلامها، وهي كلمة السر التي يُطلب منك إدراجها قبل أن تتمكّن من تعديل أبسط الإعدادات. لا ضير من ذلك. ولكنّ المشكلة تكمن في أن معظم كلمات السر الافتراضية يسهل تخمينها. (إذا كان هذا الموضوع يثير فضولك، بادر إلى مقارنة كلمات السر الافتراضية المستخدمة لعدة أجهزة توجيه).

منعاً لأي شخص قادر على الوصول مباشرة إلى جهاز التوجيه من تغيير إعداداتك، يتعيّن عليك أن تحصّن كلمة السر بكلمة أقوى. يأتي جهاز التوجيه مع دليل المستخدم الذي يشرح كيفية الوصول مباشرة إلى إعداداته من خلال المتصفح، عبر كابل الإيثرنت عادةً. وإلاّ يمكنك أن تنزّل نسخة إلكترونية عن هذا الدليل من موقع الشركة المصنّعة للإفادة من إرشاداته وتوجيهاته.

قبل الغوص في هذه المسألة، من الأوفق أن تدرج عنوان بروتوكول الإنترنت الافتراضي الخاص بجهاز التوجيه ( الذي يأتي عادةً على

هذا الشكل ١. ١١. ١٦٨. ١٩٢ أو ١. ١١. ١٦٨. ١٩٢)، وكذلك إسم المستخدم وكلمة السر الافتراضيين العائدين إلى مدير الجهاز، إذا أردت إعادة ضبط الجهاز، والإقلاع به مجدداً في وقت لاحق.

ما إن تربط حاسوبك بجهاز التوجيه، وتسجّل دخولك إلى لوحة التحكّم، أي المنطقة التي تتيح لك التحكّم بطريقة عمله، ستصطدم على الأرجح بعدد كبير من الروابط والأزرار وعلامات التبويب، المفترض أن تختار منها ما يلزمك. سيسديك دليل المستخدم نصائح عملية في هذه المرحلة بالذات. ولكن إذا تعذّر عليك إيجاده، فلن يصعب عليك الاطلاع على الضوابط اللازمة لإعادة تعيين كلمة السر الخاصة بالجهاز ضمن أي خانة مخصصة للإدارة.

- إحصل على نصائح إضافية حول كيفية إنشاء كلمات سر قوية من موقع «عُدّة الأمان».

## عطّل تشغيل ميزة التشفير

لا يجدر بك أن تستخدم نقاط الوصول التي توفّر التشفير بين حاسوبك وجهاز التوجيه إلا لحماية بياناتك من المتنصتين المتواجدين ضمن حدود منطقتك المباشرة.

للتأكد من تشغيل خدمة التشفير، عليك أن تتّبع أولاً الخطوات المشار إليها أعلاه لتسجيل دخولك إلى إعدادات جهاز التوجيه الخاص بك، ثم إبحث عن إعدادات الأمان للشبكة اللاسلكية، علماً أنّ موقع هذه الإعدادات يبقى رهناً بالشركة المصنّعة لوحدة التشغيل الخاصة بك. عند فتح إعدادات الأمان، إختَر بروتوكول الوصول المحمي أو بروتوكول الوصول المحمي ٢ من مجمل أنواع التشفير المتوافرة في القائمة (مع الإشارة إلى أنّ بروتوكول الوصول المحمي ٢ هو أقوى، مع أنه لا ينطبق على جميع أجهزة التوجيه القديمة)، واعتمد كلمة سر قوية، أي كلمة تكون طويلة ومعقدة، يصعب تخمينها.

- إحصل على نصائح إضافية حول كيفية إنشاء كلما سر قوية من موقع «عُدّة الأمان».

## عطّل تشغيل الوضعية المحمية لشبكة واي فاي

قلما يراعي مصنّعو التكنولوجيا تسهيل التقنيات الأمنية على المستخدم العادي. لهذا السبب، رحّب كثيرون بالتغيير الذي طرأ مع بروز الوضعية المحمية لشبكة واي فاي، وهي عبارة عن نظام يتيح لك تبادل كلمة السر مع حاسوبك بمجرد الضغط على زر خارج جهاز التوجيه. ولكن، في أواخر العام ٢٠١١، كشفت الشركات المصنّعة عن أنّ تشغيل هذه الميزة في جهازك تدفع شبكتك إلى «الإفصاح عن» كلمة السر المشفّرة إلى شخص يخترق الشبكة، حتى ولو لم تكن تستخدمها.

وفي هذا السياق، استحدثت شركة «تاكتكل نتوورك سوليوشنز» أداة مجانية للقرصنة، تحت إسم «ريفير»، لتبيان هشاشة هذه التقنية. وأفادت بأنّ هذه الأداة ستتمكّن من الكشف عن كلمة سر مشفّرة بموجب بروتوكول الوصول المحمي/بروتوكول الوصول المحمي ٢» في غضون ٤-١٠ ساعات، تبعاً (لجهاز التوجيه المستخدَم). أما عملياً، فيعوزك نصف هذا الوقت لتخمين رمز التعريف الشخصي الصحيح للوضعية المحمية واستعادة عبارة المرور».

لذا عطّل هذه الميزة في لوحة التحكّم بجهاز التوجيه، لصدّ هجوم المتسللين على مفتاح التشفير.

## عطّل ميزة الشبكات العريضة الإقليمية، أو الشبكات اللاسلكية المحلية، أو الإدارة عن بعد

تأتي غالبية أجهزة التوجيه مضبوطة تلقائياً بما يسمح لأحدهم أن يكون موصولاً بها عن بعد، كخبير الدعم التقني لدى شركة تزويد خدمة الإنترنت الذي قد يرغب في مساعدتك على تشغيل جهازك. ولكن، بما أنّ جهازك غير قادر على التمييز بين أصحاب النوايا الحسنة والسيئة لسوء الحظ، فمن الأوفق لك، وبكل بساطة، أن تعطّل هذه الميزة.

تمنحك بعض أجهزة التوجيه اليوم إمكانية تعطيل ما يُعرَف بميزة إدارة الشبكة اللاسلكية المحلية (أو الشبكة العريضة الإقليمية)، فلا تعود تسمح لأي شخص الوصول إلى إعداداتها ما لم يكن موصولاً بها مباشرة عبر كابل إيثرنت.

### جهاز التوجيه المخفي ليس حقاً مخفياً

يجوز أن تخفي جهاز التوجيه الخاص بك عن جارك بمنعه من نشر إسم التعريف بالشبكة (إسمه)، ولكن يتعذّر عليك إخفاءه على كل من يشغّل «إنسايدر»، برنامج فحص شبكة واي فاي، أو أي خدمة مجانية أخرى من واي فاي. وبالتالي، لا تعتمد على هذه الحيلة لتحصين أمنك.

## عطّل تقنية التوصيل والتشغيل العالمية

هي ميزة مريحة متوافرة في معظم أجهزة التوجيه التي تسمح لبعض الأجهزة الأخرى الموصولة بشبكتك أن تتحكّم ببعض الإعدادات، من دون أن تتطلب منك إجراء التعديلات يدوياً. فمنصات ألعاب الفيديو وآلات الطبع تستخدم هذه التقنية أحياناً، لتطلب من جهاز التوجيه القبول باتصالات قد يرفضها عادةً عندما تَرِد من

الإنترنت. من هنا، تشكّل هذه الميزة على الأرجح منفذاً إلى شبكتك قد لا ترغب في إبقائه مشرّعاً. لذا، إكتفِ بتعطيلها ولن تشعر بالفرق.

## بعض التقنيات المتطورة

### فلترة عناوين ماك (بروتوكول التحكّم بالوصول إلى الوسائط)

إذا كانت كلمة السر وحدها لا تكفيك لتقييد الوصول إلى شبكتك، يمكنك أيضاً أن تحدد لجهاز التوجيه الأجهزة الأخرى المصرّح لها باستخدامه. وبهذه الطريقة، ستحجب عنه أي أجهزة لا تحظى بإذن صريح منك، حتى ولو كانت تملك مفتاح التشفير الخاص بجهازك.

أين يكمن السر؟ يتفرّد كل جهاز كمبيوتر وهاتف جوّال بعنوان ماك، وهو عبارة عن بطاقة التعريف التي يحملها أينما كان، لتمييزه عن الأجهزة الأخرى. وبالتالي، ستجد ضمن لوحة التحكّم في جهاز التوجيه قسماً مخصصاً لفلترة عناوين ماك التي تتيح لك الاحتفاظ بقائمة عنها، ويمكّن هذا الجهاز لاحقاً من التعرف على الأجهزة المسموح لها الانضمام إلى الشبكة، بينما يحجب مبدئياً الأجهزة غير المدرجة ضمن القائمة المذكورة.

**تنبيه:** إذا كان هذا النوع من الفلترة يساعدك على التحكّم بالوصول إلى شبكتك، مع ما يواكبه من إجراءات السلامة، فمن الضروري التنبّه إلى أنّ **فلترة عناوين ماك لا يغنيك إطلاقاً عن وسائل الحماية بكلمات السر، والتشفير، أو أي إجراءات أخرى تتخذها لسلامة شبكتك**. فعملية الفلترة بحد ذاتها، لا توفّر أي حماية على شاكلة تشفير الاتصال بين حاسوبك أو الهاتف الجوّال وجهاز التوجيه، ناهيك عن إمكانية تقليد هذا العنوان، ولو لم يكن ذلك بالأمر اليسير.

## ملاحظات

- هل تريد أن تعرف عنوان ماك الخاص بك؟ إستعلم عن الوسائل الكفيلة بمساعدتك في هذه المقالة على موقع ويكي wikihow.com.

## قائمة مرجعية آمنة لشبكة واي فاي

### عند استخدام جهاز التوجيه الخاص بك:

- غيّر كلمة السر التي وضعها مدير الجهاز (مستخدماً كلمة سر قوية!).
- شغّل ميزة التشفير بموجب بروتوكول الوصول المحمي إلى شبكة واي فاي وبروتوكول الوصول المحمي ٢ (علماً أنّ بروتوكول الوصول المحمي ٢ هو الأفضل).
- عطّل تشغيل:
  - الوضعية المحمية لشبكة واي فاي؛
  - شبكة الاتصال الإقليمية/إدارة الويب؛
  - تقنية التوصيل والتشغيل العالمية.

### تقوية جهاز التوجيه

إذا كان جهازك لا يوفّر الميزات المشار إليها في هذا الفصل، وتودّ تدعيمه، فلا يزال بإمكانك «تقويته» باستخدام برمجيات مجانية، ومفتوحة المصدر، كـ«دي دي دبليو آر تي» أو «توميتو». لذا، ننصحك أن تتحقق من الموقعين الخاصين بهما لمعرفة إذا كانا متطابقين مع جهازك.


# ٦: الاتصال الآمن عبر الدردشة والمكالمات الصوتية

**الحفاظ على خصوصية المراسلات الفورية، والدردشة، والمقابلات.**

إنّ التحادث عبر برنامج غير محمي للمراسلات أو المحادثات الفورية هو أشبه بتبادل الحديث مع صديق عبر مكبّر الصوت في مكتب التحرير. فقد لا يعرف زملاؤك الجالسون في جوارك رقم الهاتف الذي طلبته، أو الشخص الذي تتحدث معه، إنما يتابعون حديثك بالتفصيل. الأمر سيّان عبر الإنترنت. إذ بإمكان أي شخص يعمل لدى مزوّد خدمة الإنترنت أن يطّلع على مضمون الحديث الذي تتبادله مع رئيس التحرير أو مصدر معلوماتك عبر شبكاته، وأن يسجّله للاطلاع عليه لاحقاً. وإن كان لا يعرف إسم المستخدم وكلمة المرور اللذين تعتمدهما لتطبيق الدردشة، لكنّك قد تكون أشدّ اهتماماً بالحفاظ على خصوصية مقابلاتك نظراً إلى عملك الصحفي. لذا، نستعرض في ما يلي بعض الوسائل الكفيلة بتعزيز خصوصية اتصالاتك المباشرة.

## المبادئ الأساسية

### إستخدم بروتوكول "إتش تي تي بي آس"

عندما تدردش عبر متصفحك باستخدام ميزة الدردشة في غوغل مثلاً، قد تعتمد أصلاً على بروتوكول «إتش تي تي بي آس»، بما يدلّ على أنّ اتصالك بخادم غوغل يخضع للتشفير (رغم اطّلاع غوغل بالطبع على مضمون ما تقول أو تكتب).

لكنّ المفارقة تكمن في أنّ تطبيقات كثيرة للرسائل الفورية توفّر لك اتصالاً آمناً عند تسجيل دخولك فقط، لا أثناء الدردشة.

### الأوسع انتشاراً ليس دوماً الأفضل

إنّ شيوع استخدام تطبيق معيّن بين أوساط أصدقائك لا يعني بالضرورة أنه آمن، لأنّ شعبية التطبيق قد تجعل منه في الواقع هدفاً أهمّ في نظر المهاجمين الانتهازيين. لذا، يجدر مثلاً بمستخدمي سكايب، المقدّرة أعدادهم بعشرات الملايين، عدم الركون إلى استخدام إصدارات من هذا التطبيق معرّضة للاختراق (كميزة توم سكايب في الصين)، وامتدادات مزوّرة لبرنامج سكايب، كأداة «تشفير سكايب» الموزّعة في سوريا، وسواها من البرمجيات الخبيثة التي تنجح في التسلل إلى قائمة اتصالات أي مستخدم، والانتقال منها إلى أي جهاز كمبيوتر آخر. أما الخيار البديل المفتوح المصدر، مثل برنامج بدْجِن (المشار إليه أدناه)، فيجوز أن يكون مستهدفاً بدرجة أقل، وأن يمنح في الوقت ذاته خبراء الأمن فرصة التأكيد على أنّ التطبيق يفعل بالضبط ما يُطلّب منه.

### إستخدم تطبيق بدجِن المزوّد بخدمة التراسل الفوري الآمن

إنّ تطبيق بدجن هو تطبيق مجاني يسمح لك أن تجمع عدة حسابات، بما فيها حسابات «فايسبوك»، «ياهو ماسنجر» و«إم إس إن ماسنجر»، وغوغل، في مكان واحد. يفيدك هذا البرنامج بالذات إذا كنت تلقى صعوبة في متابعة الأشخاص الموصولين بالشبكة. لكنّ مستخدمي هذا البرنامج يسعهم أيضاً تنزيل أداة إضافية تُعرَف بالتراسل الفوري الآمن الذي يضمن الاتصال الآمن والموثوق في ما بينهم. فيتيح لك هذا التطبيق المزوّد بخدمة التراسل الفوري الآمن، عند حسن ضبطه، تشفير مضمون الرسائل الفورية قبل إرسالها عبر الإنترنت، ولا يسمح بفك شيفرتها إلا عند استلامها من قبل جهاز كمبيوتر (مفترض أن يعود لأحد مصادر معلوماتك أو صديق لك) ومأذون له وحده أن يقرأ الرسائل. صحيحٌ أنّ هذا التطبيق يتطلب منك جهداً أكبر بقليل من الجهد المطلوب للتحادث عبر متصفحك، لكنه يحصّن أمنك إلى حد كبير، لأنه يشلّ قدرة الجميع، حتى مزوّد خدمة الدردشة، على قراءة مراسيلك.

لغاية إصدار هذا الدليل، كان برنامج بدجن يكتفي بتوفير خدمة الرسائل الفورية، لا خدمة الاتصالات الصوتية. وقد أفادت تقارير بأنّ شركة غوغل تعتزم في المستقبل إضافة ميزة التشفير إلى تطبيق «غوغل توك».

- نزّل تطبيق بدجن
- نزّل الأداة الإضافية للتراسل الفوري الآمن
- ثمّ إتّبع الشروحات المقدمة خطوة خطوة على موقع «عُدّة الأمان» للبدء باستعمال برنامج بدجن وميزة التراسل الفوري الآمن.

### عند استخدام جهاز كمبيوتر مشترك:

يُتاح لك أن تنزّل نسخة محمولة من برنامج بدجن من موقع PortableApps.com، أو أي نسخة مشابهة من مطوّري البرامج الذي ثبّتوا ميزة التراسل الفوري السري مسبقاً، فتحملها معك أينما كان، وتخوّلك تشفير رسائلك الفورية على الدوام.

ولكن، كن متيقظّاً عند تحميل أي تطبيق إلى شريحة الذاكرة التي تحتضن كلمات السر الخاصة بك، لأنّ فقدان هذه الشريحة سيعرّض حساباتك للخطر. لذا، إذا كنت تنوي استخدام تطبيق بدجن المحمول لحماية حسابات الدردشة، إقرأ المعلومات المتعلقة باستخدام برنامج «تروكريبت» لحماية بياناتك على شريحة الذاكرة بمفتاح التشفير.

- نزّل النسخة المحمولة من تطبيق بدجن مع خدمة التراسل الفوري الآمن المثبّت مسبقاً.
- تعرّف على مزيد من التطبيقات المحمولة.

### محو سجل الدردشة

يحتفظ تطبيق سكايب، وسواه من تطبيقات المراسلات الفورية، بسجل دردشاتك على خادمه بموجب الضبط المبدئي. قد ترغب في تعطيل هذه الميزة لحماية محادثاتك واتصالاتك في وجه أي شخص قد يحاول اختراق حسابك في المستقبل. لكنّ إيقاف العمل بهذه الميزة لا يحول بالطبع دون تسجيل محادثاتك التي تجريها عبر وسيلة اتصال غير آمنة، أو التقاطها بوسائل أخرى، كالبرمجيات الخبيثة.

إذا كان التطبيق الذي تستخدمه يوفّر ميزة عرض الفيديو، فالأوفق أن تتحقق ما إذا كنت تأذن باستخدام شاشة حاسوبك أو بثّ صورة فيديو بصورة تلقائية. تجد هذه الضوابط في موقع سكايب تحت خانة الخصوصية ضمن لوحة الخيارات.

## تقنيات متطورة

### إستخدم شبكة تور

يمكنك أن تثبّت تطبيق بدجن للاتصال بالإنترنت عبر شبكة تور، توخياً لمزيد من الخصوصية، رغم ما أعلنه الفريق القيّم على تطوير مشروع تور عن احتمال تسريب بعض المعلومات عن هويتك من خلال تسجيل الدخول وكلمة السر.

- تعلّم كيف تضبط تطبيق بدجن للاتصال عبر شبكة تور المتوافر على موقع المشروع (ما إن تفتح الصفحة، إستعرضها نزولاً إلى أن تقع على مدخل إلى تطبيق بدجن).

### تسجيل الدخول ليس دليل حماية

صحيحٌ أنّ معظم برامج التراسل الفوري تحمي إسم المستخدم وكلمة السر عند تسجيل الدخول، ولكنّ أكثرها لا يحمي محادثاتك.

## مصادر ومراجع إضافية

### منظمتا "فرونت لاين ديفندرز" و"تاكتكل تكنولوجي كوليكتف"

- كيف تحافظ على خصوصية اتصالاتك عبر الإنترنت.
- إستخدام برنامج بدجن مع ميزة التراسل الفوري الآمن.
- دليل الاستمرارية في العالم الرقمي (لأجهزة الكمبيوتر).
- دليل الاستمرارية في العالم الرقمي (للهواتف الجوّالة).
- الأمن المحمول.

### مؤسسة الحدود الإلكترونية

- بروتوكول «إتش تي تي بي آس إيفريوير».

### منظمة موبايل أكتيف

- إضمن خصوصية محادثاتك على نظام أندرويد: دليل المستخدم لتطبيق «جيبربوت».

### سكايب

- مدونة الحفاظ على أمنك عبر سكايب.

# قائمة مرجعية للدردشة والمكالمات الصوتية

## عند استخدام جهاز كمبيوتر خاص:

- نزّل وثبّت «بدجن».
- نزّل وثبّت الوظيفة الإضافية لتطبيق التراسل الفوري الآمن.
- إقرأ التعليمات المتعلقة بإضافة حساب.
- إتبع الدروس الخصوصية المتوافرة عبر موقع «عُدّة الأمان» حول سبل تأمين حماية الدردشة مع أصدقائك.
- إستعلم عن الإعدادات التي يمكنك استخدامها مع برنامجي بدجن وتور إذا كنت ترغب في الحفاظ على خصوصية محادثاتك أثناء الدردشة.

## عند استخدام جهاز كمبيوتر مشترك:

- نزّل النسخة المحمولة من «بدجن»، وثبّتها في شريحة الذاكرة.
- نزّل وثبّت الوظيفة الإضافية لتطبيق التراسل الفوري الآمن من برنامج «بدجن» المحمول.
- إقرأ التعليمات المتعلقة بزيادة حساب.
- إتبع الدروس الخصوصية المتوافرة عبر موقع «عُدّة الأمان» حول سبل تأمين حماية الدردشة مع أصدقائك.
- إذا كنت ترغب في إخفاء هويتك أثناء الدردشة، نزّل حزمة متصفح تور، ثمّ استعلم عن الإعدادات الواجب تعديلها في «بدجن»، لتستخدم شبكة تور.


# ٧: رصد مشاكل الوصول ومعالجتها

**التحايل على الحواجز المعهودة التي تصطدم بها عندما تحاول الوصول إلى مواقع ضرورية لعملك.**

كم مرة شعرت بالانزعاح لعدم قدرتك على الوصول إلى بعض المواقع الضرورية لصياغة خبرك عند إجراء أبحاث مكثّفة حوله عبر الإنترنت. ولعلّ ذلك يعود إلى عدة أسباب. تفرض المؤسسات الإعلامية في عدة بلدان قيوداً على بعض المحتويات بحسب المواقع الجغرافية لأسباب تجارية؛ كما يجوز أن يحجب مزوّدو خدمة الإنترنت مواقع عدد من منافسيهم أو المواقع التي تنشر محتويات للراشدين (فيما يمتنع أقرانهم في البلد ذاته عن ذلك)؛ أما الحكومات، فقد تحجب من جهتها بعض المواقع لأسباب ثقافية أو سياسية.

أياً كانت هذه الأسباب، فما زالت أمامك خيارات تخوّلك الوصول إلى مواقع ومحتويات محجوبة، لتوسيع معرفتك بموضوع بحثك. يمكنك الاطّلاع بشكل معمّق على هذه الوسائل (إضافة إلى بعض الشروحات السهلة حول آلية عمل كلٍّ منها) على الموقع الخاص بكيفية تجاوز الرقابة عبر الإنترنت. ولكن، إليك في ما يلي بعض النقاط البارزة.

## المبادئ الأساسية

### أولاً، تنبيه هام

حاول أن تستعلم عن أسباب حجب الموقع قبل زيارته. فقد تحظّر بعض البلدان زيارة مواقع معيّنة بموجب القانون، مما يرتّب عليك وعلى المؤسسة الإخبارية التي تعمل لديها عواقب وخيمة عند انتهاك القانون. لذا، إذا كنت بحاجة إلى استخدام موقع ضمن منطقتك تعرف سلفاً أنه محظور، فلا تحاول الوصول إليه من نقطة اتصال مرتبطة بك، إذ يجوز أن يكون الموقع خاضعاً للمراقبة، وأن يقوم أحدهم بتسجيل عناوين الأشخاص الذين يحاولون الوصول إليه.

### إطّلع على القوانين

من الضروري لك أن تكون مطّلعاً على القوانين السارية في بلدك حينما تصطدم بمواقع إلكترونية محجوبة. وذلك للتأكّد مما إذا كانت محتوياتها خاضعة للحظر. لا نسديك هذه النصيحة إلا من قبيل تسهيل عملك كصحافي.

### إستخدم خادم وكيل (بروكسي) آمن

إذا كنت تعيش ضمن منطقة غالباً ما تتعرض فيها المواقع الإلكترونية للحظر، قد تكون قد سمعت مسبقاً عن خوادم وكيلة، وهي خدمة قادرة على «رفع الحظر» عن موقع معيّن، حين تتصل من خلالها بالإنترنت. تجدر الإشارة إلى أنّ غالبية الخوادم الوكيلة تعمل عبر الإنترنت، أي أنها خدمات تعمل عبر متصفحك ولا يلزمك أي تطبيق خاص للحصول عليها. ورغم كونها خدمات مجانية، فالأجدى بك أن تأخذ بعين الاعتبار بعض المبادئ التوجيهية عند استخدامها:

- لا تستخدم إلا خوادم وكيلة تعمل بموجب بروتوكول «إتش تي تي بي آس» (لأنّ استخدام الخادم الذي يوفّر الاتصال بواسطة بروتوكول «إتش تي تي بي» يتسبّب لك بمشاكل كارثية، باعتبار أنّ نشاطاتك عبر الشبكة لن تخفى أبداً على الشركة المحلية التي تقدم لك خدمة الإنترنت، أو على أي شخص آخر يترقّب تحركاتك).
- لا تنطلق من فرضية أنّ الخادم الوكيل يريد حماية خصوصيتك، بل إعلم أنّ الاتصال بهذا الخادم عبر بروتوكول «إتش تي تي بي آس» لا يكون آمناً إلا بين حاسوبك والخادم. ولكن بعد هذه

النقطة، قد لا تعود حركة زوارك وبياناتك خاضعة للتشفير إذ يتسنّى للفريق المسؤول عن هذه الخدمة متابعة تفاصيلها.

- لا تزوّد الخادم الوكيل بمعلومات شخصية أو تعرّف عن هويتك عندما تسجّل اشتراكك، لأنّ هذه الخدمة تعتمد سياسات مغايرة للحفاظ على الخصوصية؛ فضلاً عن ذلك، يجمع بعضها بيانات معيّنة، كعادات المستخدم أو عناوين البريد الإلكتروني، التي يبيعونها تحصيلاً للمداخيل.

يعتبر برنامج «بي سايفون» خدمة مجانية من خدمات الخوادم الوكيلة التي لا تتطلب من المستخدم إلا أن يتذكّر عنوان بروتوكول الإنترنت. ولكن، نظراً إلى شعبيتها، حُجِب خوادم «بي سايفون» أحياناً في البلدان التي تفرض حظراً على بعض المواقع الإلكترونية. لهذا السبب، تزوّدك هذه الخدمة بعناوين محدّثة للخوادم عندما تسجّل اشتراكك فيها للمرة الأولى. وقد تلبّي رغبتك في استخدام حساب للبريد الإلكتروني يخفي هويتك عند التراسل عبر الخوادم الوكيلة، والشبكات الافتراضية الخاصة، وما شابهها من أدوات.

### إستخدم الروابط المخزّنة

عند استخدامك غوغل كمحرك بحث، قد تقع على روابط «مخزّنة» إلى جانب بعض النتائج التي تتوصّل إليها. لكنّ النسخة المخزّنة من الصفحات ليست متاحة مباشرة، بل هي مجرد صورة للصفحة، يجري تخزينها على خادم غوغل للمساعدة في تسريع نتائج البحث. كما يجد المستخدم في هذه الروابط فائدة أخرى تكمن في أنّ الصفحة المخزّنة لا تحجب أحياناً حتى ولو حجب نطاق الموقع الفعلي.

### إستخدم الشبكة الافتراضية الخاصة أو شبكة تور

عندما يتعذّر عليك الوصول إلى موقع معيّن في بلدك لأي سبب من الأسباب، فقد يتيسّر لك الوصول إليه من خلال الاتصال الآمن بشبكة افتراضية خاصة أو عبر شبكة تور.

أحياناً، يكون الاتصال عبر الشبكة الافتراضية أسرع من الاتصال عبر شبكة تور. ولكن تذكّر أنّ الشبكة الافتراضية لا تضمن لك إخفاء الهوية، لأنّ مديرها كان ليعرف عنك قدر ما يعرف مزوّد خدمة الإنترنت لو لم تكن تستخدمها إطلاقاً.

- تعلّم كيفية استخدام برنامج «بي سايفون ٣»، الخدمة المجانية للشبكة الافتراضية الخاصة، من خلال إرسال بريد إلكتروني فارغ إلى العنوان get@psiphon3.com.
- إستعلم عن تطبيق الشبكة الافتراضية الخاصة والمفتوحة، وهو أيضاً تطبيق مجاني.
- نزّل حزمة متصفح تور.

## إخفِ الهوية من دون عناء

«تايلز» هو نظام تشغيل مستقل، ومتصفح، وبرنامج عميل للدردشة، يتمّ ضبطه مسبقاً لاستخدام شبكة تور القادرة على إخفاء الهوية، ويجوز تشغيله من قرص مدمج أو شريحة ذاكرة.

### إستخدم قارئ الخلاصات "آر إس إس"

قد يُتاح لتقنيات قراءة الخلاصات «آر إس إس» والتطبيقات الأخرى، التي تستمدّ محتوياتها من مواقع متعددة، كتطبيقي «أي كورنت» أو «غوغل نيوز»، أن تستعرض أخباراً أو صوراً أو محتويات أخرى من مواقع محظورة، لأنها ليست، بدورها، محظورة.

- إستعلم عن طريقة إضافة مواضيع إلى «غوغل نيوز».
- تعلّم كيفية البدء باستعمال قارئ غوغل.
- تعلّم كيفية استخدام خدمة الإنترنت «أي كورنت» التي تزوّدك أيضاً بخلاصات عن الأخبار الواردة عبر البريد الإلكتروني.

## تعرّف على سياسات الخصوصية

تتّبع الخوادم الوكيلة وخدمات الشبكات الافتراضية الخاصة سياسات خصوصية واضحة. يجدر بك أن تخصص لها بعض الوقت لتطّلع عليها. فقد يتبيّن لك أنها تتبادل رسائلك الإلكترونية أو معلومات مختلفة عنك مع شركات أخرى لأغراض تجارية.

### عند استخدام جهاز كمبيوتر مشترك:

كما أشرنا في الفصل المتعلق بالتصفح الآمن، يمكنك أن تستعين بالنسخة المحمولة من حزمة متصفح تور للحفاظ على سرية تصفحك، عند استخدام جهاز كمبيوتر مشترك في مكتب التحرير أو مقهى محلي للإنترنت. فإذا نجحت في إعادة إقلاع جهاز الكمبيوتر المشترك من دون فقدان الاتصال بشبكة الإنترنت، يُستحسن ربما أن تجرّب استخدام نظام «تايلز»، وهو أداة محمولة تزوّدك بنظام تشغيل ومتصفح وبرنامج عميل للتراسل الفوري، ومعدة سلفاً للعمل على شبكة تور (المشغّلة افتراضياً).

أما إذا كنت تملك أصلاً حساباً لدى خدمة الشبكات الافتراضية الخاصة، كخدمة شبكة RiseUp.net المجانية، فقد يتسنّى لك أن تستخدم النسخة المحمولة من الشبكة الافتراضية الخاصة المفتوحة. ولكن، لحسن تشغيلها، قد تكون أيضاً بحاجة إلى حساب مستخدم يوفّر لك امتيازات مدير الحساب إزاء الجهاز الذي تستخدمه. ولا تغفل أيضاً عن أنّ الشبكات الافتراضية الخاصة،

كالخوادم الوكيلة الآمنة، ليست معدّة لإخفاء هويتك عبر الإنترنت، حتى ولو كانت قادرة على حماية طبيعة النشاطات التي تقوم بها عن مزوّد خدمة الإنترنت المحلي الذي تتعامل معه.

- إحصل على حزمة متصفح تور.
- إطّلع على نظام «تايلز».
- إحصل على نسخة محمولة من الشبكة الافتراضية الخاصة المفتوحة.
- إطّلع على تطبيقات محمولة لحماية الأمن.

## تقنيات متطورة

تتوافر قائمة وشروحات موسّعة حول أدوات التحايل، أي التطبيقات التي تساعد المستخدم على تجاوز جدران النار، لدى الموقع «كيف تتجاوز الرقابة على الإنترنت».

## مصادر ومراجع إضافية

### موقع: كيف تتجاوز الرقابة على الإنترنت

- دليل لانطلاقة سريعة (بنسخة بي دي أف)؛
- حِيَل بسيطة؛
- كتيّب عملي (بنسخة بي دي أف).

### «فرونت لاين ديفندرز» و«تاكتكل تكنولوجي كولكتيف»

- كيف تخفي هويتك وتتجاوز الرقابة على الإنترنت.

### مراسلون بلا حدود

- كتيّب للمدونين والمعارضين الناشطين عبر الإنترنت.

### مؤسسة الحدود الإلكترونية

- آليات التدوين الآمن (بشأن العمل أو أي موضوع آخر).

### الأصوات العالمية

- التدوين المجهول الهوية باستخدام برنامجي «وورد بريس» و«تور».

### صفحة ويكي حول الرقابة على الإنترنت

- خطوات لتجاوز الرقابة على الإنترنت

### موبايل أكتيف

- كيف تتصفّح الإنترنت عبر هاتفك من دون الكشف عن هويتك.

## القائمة المرجعية لرصد مشاكل الوصول ومعالجتها

### عند استخدام جهاز كمبيوتر خاص:

- إذا كنت ترغب في إخفاء هويتك عند تصفح مواقع الإنترنت، وكذلك الوصول إلى المحتويات التي تكون محجوبة، نزّل حزمة متصفح تور.
- إذا كانت شبكة تور محجوبة في منطقتك، فحاول أن تستخدم جسر تور أو أي تطبيق مجاني للشبكات الافتراضية الخاصة.
- إذا ارتايت أن تستخدم شبكة افتراضية خاصة، إقرأ التعليمات المتعلقة بحسن استخدامها أو ضبطها:
  - Riseup.net؛
  - «بي سايفون ٣»؛
  - «هوت سبوت شيلد».

### عند استخدام جهاز كمبيوتر مشترك:

- إذا كنت ترغب في إخفاء هويتك عند تصفح مواقع الإنترنت، وكذلك الوصول إلى المحتويات التي تكون محجوبة، نزّل حزمة متصفح تور.
- إذا كانت شبكة تور محجوبة في منطقتك، فحاول أن تستخدم جسر تور أو أي تطبيق محمول من الشبكات الافتراضية الخاصة.
- إذا ارتايت أن تستخدم نسخة محمولة من الشبكات الافتراضية الخاصة، إقرأ التعليمات المتعلقة بحسن استخدامها أو ضبطها:
  - Riseup.net (ستحتاج أيضاً إلى شبكة افتراضية خاصة مفتوحة المصدر)؛
  - «بي سايفون ٣».

## ملاحظات

# ٨: التشبيك والتدوين الآمنان عبر مواقع التواصل الاجتماعي


**التحقق من المحتويات التي تتبادلها عبر شبكات التواصل الاجتماعي والمدونات.**

أصبحت مواقع فايسبوك وتويتر وشبكات التواصل الاجتماعي الأخرى تشكّل سلاحاً قوياً بين أيدي الصحافيين، إذ أخذت المؤسسات الإعلامية تستعين بها لتقصي المعلومات، أو البحث عن مصادر أو شهود للاتصال بهم، أو استقطاب ملاحظات وتعليقات الجمهور، أو استدرار آراء من مصادر معلومات جماعية، أو نشر محتوياتها.

لكنّ خدمة «نشر التدوينات المصغّرة» هذه، شأنها شأن أي وسيلة هامة للتعبير عن الآراء، قد تخضع للمراقبة، فترتّب عليك أو على مصادرك عواقب جمّة. قد يتسنّى لكل من يخترق حسابك مثلاً أن:

- ينسخ قائمة اتصالاتك.
- ينشر محتويات مزورة، كالتدوينات التي تبدو وكأنها صادرة عنك، إنما تشوّه سمعتك وتسيء إلى منظمتك في الواقع.
- يرصد مدونة «مجهولة الهوية» (أو مدونة منشورة تحت إسم مستعار)، من خلال الخدمات الأقل حفاظاً على السرية أو العناوين البريدية التي تكون قد ربطتها بتلك المدونة.

لا بل باستطاعة أي شخص أن يحدد مكانك حينما تُقدِم على تحديث تدويناتك بواسطة أداة مجانية مثل «كريبي»، حتى من دون الحصول على حسابك. لذا، قد تساعدك التوصيات التالية في تحصين أمنك عند استخدام مواقع التواصل الاجتماعي.

### فايسبوك يرصد التغييرات

يرصد موق فايسبوك عاداتك عبر الإنترنت، ويطلب منك أن تثبت هويتك عندما يشتبه بوجود تغييرات جذرية، غير اعتيادية، على موقعك.

## المبادئ الأساسية

### إستخدم بروتوكول "إتش تي تي بي آس" للنقل الآمن

عند الاتصال بإحدى شبكات التواصل الاجتماعي كفايسبوك، يتعيّن عليك دوماً أن تتحقق من أنك وصلت إلى الصفحة المتوقعة، ومن أنها تحظى بحماية البروتوكول المذكور. أما إذا كنت قد نزّلت التطبيق الإضافي المعروف بـ«برسبكتيفز» في متصفحك، فالأوفق لك أن تتأكد من صحة بيانات اعتماد الموقع، وسلامتها. (راجع الفصل المتعلق **بالتصفح الآمن** للحصول على مزيد من المعلومات حول التطبيق المذكور، وما شابهه من تطبيقات ملحقة لتحصين الأمن).

يراعي بعض المواقع بروتوكول «إتش تي تي بي آس» طيلة فترة الاتصال، مما يمنع مزوّد خدمة الإنترنت، كما الأشخاص الذين يتشاركون الشبكة ذاتها، من رصد التدوينات التي تنشرها أو

المحادثات التي تتبادلها أثناء اتصالك. وبالتالي، يمكّنك موقعا فايسبوك وتويتر، كلاهما، من تشغيل هذه الميزة ضمن إعدادات حسابيهما.

- تعلّم كيفية تشغيل بروتوكول «إتش تي تي بي آس» في موقع تويتر.
- تعلّم كيفية تشغيل بروتوكول «إتش تي تي بي آس» في موقع فايسبوك.

## إستخدم كلمة سر قوية

كما هي الحال مع أي خدمة من خدمات الإنترنت، يجدر بك أن تتبّع التوصيات الصادرة بشأن إنشاء كلمة السر أو إعداد خطة لاستعادة كلمة السر الموضوعة لأي شبكة اجتماعية. يشغل هذا الموضوع حيّزاً هاماً لدى المؤسسات الإخبارية التي تستخدم فايسبوك وتويتر للتفاعل مع جمهورها، بما أنّ فقدان السيطرة على أحد الحسابات قد يسيء إلى سمعتها بعد أن عملت جاهدة لكسبها وتعزيزها.

- راجع التوصيات الواردة في موقع «عُدّة الأمان» حول إنشاء كلمة سر قوية.

## إستخدم شبكة افتراضية خاصة أو شبكة تور

تعزّز الشبكة الافتراضية الخاصة خصوصيتك عند تصفّح مواقع الإنترنت، وكذلك عند استخدام شبكات التواصل الاجتماعي. ولكن، يجدر التذكير بأنّ هذه الشبكة لا تؤمّن حمايتك إلا على مستوى الاتصال القائم بينك وبين مزود هذه الخدمة، فيما تخفي حزمة متصفح تور هويتك على مستوى الاتصال القائم بين جهازك والموقع الإلكتروني الذي تحاول الوصول إليه. في أي حال، يبقى عليك التأكد من أن اتصالك بالموقع يجري بموجب بروتوكول «إتش تي تي بي آس»، منعاً من تبادل تدويناتك عن غير قصد مع أشخاص يستخدمون شبكة «تور».

- نزّل آخر إصدار من حزمة متصفح تور.
- إستعلم عن تطبيق «بي سايفون ٣»، وهو خدمة مجانية للشبكات الافتراضية الخاصة، من خلال إرسال بريد إلكتروني فارغ إلى get@psiphon3.com.

## تشغيل ميزة التحقق بواسطة عاملين

قد يوفّر لك موقع التواصل الاجتماعي أو الموقع المضيف لتدويناتك خيار حماية حسابك بتقنية لا تقتصر على إسم المستخدم وكلمة السر اللازمين لتسجيل الدخول. فيخوّلك موقع فايسبوك مثلاً أن تحمي حسابك برمز يرسله إلى هاتفك الجوّال (تجده تحت خانة حساب/إعدادات الحساب/الهاتف الجوّال). لذا تأكّد ما إذا كانت مواقع التواصل الاجتماعي التي تستخدمها توفّر لك ميزة مماثلة.

- تعلّم كيف تضيف ميزة التحقق بعاملين إلى حساب فايسبوك.
- أضِف ميزة التحقق بعاملين إلى جميع حسابات غوغل.

## إخفاء الهوية باستمرار

قام مراسلون بلا حدود ومؤسسة الحدود الإلكترونية بإصدار كتيّبات تتضمّن نصائح للمدونين، بما في ذلك كيفية نشر المدونات من دون الكشف عن هويتهم. تعتبر هذه العادة مفيدة أيضاً بالنسبة إلى الصحافيين الذين يرغبون، ولأي سبب من الأسباب، في حماية هويتهم عند نشر أخبارهم عبر الإنترنت:

- إحصل على «كتيّب للمدونين والمعارضين الناشطين عبر الإنترنت» الصادر عن منظمة «مراسلون بلا حدود».
- إطّلع على «آليات التدوين الآمن (بشأن العمل أو أي موضوع آخر)» لدى مؤسسة الحدود الإلكترونية.

## كن حريصاً على البيانات التي تتبادلها

تتغيّر سياسات الخصوصية التي ترعاها مواقع التواصل الاجتماعي باستمرار. فيصيبك العجب حين ترى أحياناً أنّ المعلومات التي كانت محصورة بحلقة ضيقة من الأشخاص الذين دعوتهم البارحة لتقاسمها، باتت فجأة في متناول جمهور عريض اليوم.

### أين كنت؟

عندما تنشر تدوينة عبر شبكات التواصل الاجتماعي، فأنت لا تقتصر على تبادل أفكارك أو تقرير إخباري سريع وحسب، بل قد تضع في متناول المستخدمين معلومات إضافية حول مكان تواجدك. فعلى سبيل المثال، يسمح التطبيق المجاني «كربي» لأي شخص أن يطبع في موقعي تويتر وفليكر إسم المستخدم، للتحري عن مصدر تحميل التغريدات أو الصور.

إضافة إلى ذلك، أخذت الشبكات تتدخل وتدقق أكثر في المحتويات التي تنشرها، عن حسن نية في أغلب الأحيان. فقد تبنّى موقع فايسبوك مثلاً عادة رصد الكلمات والجمل المفاتيح التي ترِد في المحادثات والتدوينات، للكشف عن النشاطات غير المشروعة التي قد تعرّض بعض الأعضاء للخطر. لذا، يستحسن أن تكون على علم بسياسة الخصوصية لدى شبكة التواصل الاجتماعي التي تستخدمها، لمعرفة طبيعة المعلومات التي تتبادلها هذه الأخيرة عن حسابك ومعارفك مع الغرباء.

- تنبّه إلى المعلومات المحتمل أن تتبادلها مع الآخرين من دون وعي منك، عند استخدام شبكات التواصل الاجتماعي.

وفي السياق ذاته، إعلم أنك، عندما تكتب أو تنشر أي محتويات عبر مدونة أو صفحة إحدى شبكات التواصل الاجتماعي غير المربوطة بهويتك الفعلية، إنما تلفت انتباه الأشخاص أيضاً إلى الأخبار التي تتابعها ضمن منطقتك المحلية. ففي المكسيك، تغربل عصابات المخدرات التدوينات المنشورة عبر صفحات الفايسبوك، بهدف تعقّب وقتل المواطنين الصحافيين الذين يبلّغون عن حوادث إطلاق النار في البلدات الصغرى.

## مصادر ومراجع إضافية

### "فرونت لاين ديفندر" و"تاكتكل تكنولوجي كولكتيف"

- كيف تحمي نفسك وبياناتك عند استخدام مواقع التواصل الاجتماعي.
- الأمن المحمول.

### مركز فايسبوك للسلامة

- أدوات حفظ السلامة على فايسبوك.

## قائمة مرجعية لتحصين أمن شبكات التواصل الاجتماعي

### عند استخدام جهاز كمبيوتر خاص:

- إبدأ بقراءة التوصيات الصادرة عن منظمة «مراسلون بلا حدود» ومؤسسة الحدود الإلكترونية للتدوين الآمن، والتي تفيدك أيضاً في استخدام مواقع التواصل الاجتماعي.
- أكنت تستخدم حساباً سابقاً أو حساباً جديداً، إحرص على استعمال كلمة سر قوية. إحصل على معلومات إضافية حول إنشاء كلمات السر القوية من موقع «عُدّة الأمان» لمنظمة «فرونت لاين ديفندرز».
- شغّل ميزة الاتصال بمواقع التواصل الاجتماعي عبر بروتوكول «إتش تي تي بي آس»، عند توافرها. يوفّر موقعا فايسبوك وتويتر كلاهما هذه الميزة ضمن إعدادات الحساب.
- إستخدم شبكة افتراضية خاصة أو شبكة «تور» لتعزيز خصوصيتك.

### عند استخدام جهاز كمبيوتر مشترك:

- إستخدم شبكة افتراضية خاصة ومتصفح محمولين أو حزمة متصفح تور.
- إفحص الجهاز المشترك بحثاً عن برمجيات خبيثة قد تسجّل نشاطاتك.
- بعد نشر التدوينات، شغّل تطبيق «سيكلينر» المحمول لمحو آثار نشاطاتك، كسجل تصفحك والملفات المؤقتة الموجودة في جهازك الخاص.

### عند استخدام هواتف ذكية:

- إقرأ أدلة المستخدم الصادرة عن منظمة «موبايل أكتيف» بشأن:
  - إستخدام شبكة تور على هاتفك.
  - إستخدام آمن للفايسبوك.
  - إستخدام آمن لتويتر.

## ملاحظات

# ٩: أحذف بياناتك كلياً

## الحرص على أن تحذف كلياً الملفات التي لا تريد الاحتفاظ بها في جهاز الكمبيوتر الخاص أو الهاتف الذكي

هل تعلم أنك قد لا تتخلّص نهائياً من مقالة أو صورة أو مقاطع مقابلة عندما تحذفها من جهازك الخاص؟

هذا صحيح. فحينما تفرغ سلة المحذوفات في نظام ويندوز، مثلاً، فكأنك تقول لحاسوبك لا بأس إن طمرنا البيانات القديمة ببيانات جديدة. وإلى حين القيام بذلك، فقد يتستّى لك، أو لسواك، أن يستردّ البيانات التي ظننت أنك تخلصت منها نهائياً.

يصحّ هذا القول أيضاً في شرائح الذاكرة أو الهواتف الجوالة. فإذا حذفت من دون انتباه صورة محفوظة في هاتفك (أو إذا أرغمك أحدهم على حذفها)، فقد يتستّى لك أن تسترد الصورة/البيانات في مرحلة لاحقة، باستخدام برنامج «ريكوفا» أو أي تطبيق مجاني آخر لاستعادة الملفات المحذوفة.

تعمل البرامج المشابهة لـريكوفا» على البحث في القرص الصلب عن البيانات التي «حُذِفت» منه، لإعادة تجميعها. وبقدر ما تفيدك هذه البرامج في استعادة صورة هامة حذفتها عن غير قصد من شريحة الذاكرة «آس دي» (شريحة الذاكرة الرقمية الخاصة بالكاميرا)، وأنت بأمس الحاجة إليها، تثير قلقك لكثرة الملفات التي تخزّنها على حاسوبك أو هاتفك أو شريحة الذاكرة من دون علمك.

قد تشمل هذه الملفات بالطبع أي بيانات تخطر على بالك، كملاحظات حول مقابلات أجريتها أو عناوين المصادر التي تستمد منها معلوماتك أو رسائل إلكترونية قديمة. ولكن، عند تعرض جهازك للمصادرة أو السرقة، ثمة احتمال كبير بأن يعمد الأشخاص المعنيون إلى استخدام برنامج يمسح القرص الصلب مسحاً، بحثاً عن البيانات المذكورة. أذا كنت لا تصدق، فما عليك سوى أن تنزّل برنامج «ريكوفا» لمعرفة ما قد يكون خافياً في زوايا حاسوبك العامل بنظام ويندوز في الوقت الحاضر.

- نزّل برنامج «ريكوفا» للتحري عن البيانات «المحذوفة» من حاسوبك أو جهازك.

### إمحِ قبل المنحِ

إذا كنت تنوي بيع، أو وهب، أو إقراض حاسوبك القديم، فيجدر بك أن تمسح القرص الصلب مسحاً كاملاً حفظاً لأمنك. ماحياً كل مخلفاتك. لعلّ خير أداة مجانية تساعدك في إنجاز هذه المهمة تتمثّل في برنامج «داريكس بوت ونيوك».

## المبادئ الأساسية

### إستخدم تطبيق "إريسر"

لا تكتفي بعض التطبيقات المجانية، كتطبيق «إريسر»، بحذف الملف وحسب، إنما تكتب فوقها على الفور بيانات عشوائية، مؤلفة من رقمي واحد وصفر، مما يجعل من الصعب جداً استردادها. لا شك أنّ وسيلة الحذف هذه تستغرق وقتاً أطول من إفراغ سلة المحذوفات، ولكنها تستحق العناء، خاصةً بالنسبة إلى مصادرك السرية التي تتوقف سلامتها على شدة تكتمك.

- نزّل تطبيق «إريسر» لتتمكّن من حذف الملفات الحساسة نهائياً.
- تعلّم كيفية استخدام تطبيق «إريسر» بالرجوع إلى موقع «عُدّة الأمان».

### إستخدم تطبيق "سيكلينر"

ينجح تطبيق «سيكلينر» في محو الآثار المعهودة التي تخلّفها وراءك على جهازك الخاص، كسجل تصفحك عبر الإنترنت، ما يعلّل أهميته البالغة بالنسبة إلى كل شخص يستخدم جهاز كمبيوتر مشترك في مكتب التحرير، أو ينشر تدويناته من مقاهي الإنترنت العامة. ولكن، يمكنه أن يعتمد أيضاً وسيلة حذف مماثلة لتلك التي يعتمدها تطبيق «إريسر»، عندما ينظّف ذاكرة التخزين المؤقت، وما عداها من المخلفات الإلكترونية.

- نزّل تطبيق «سيكلينر» لتتمكّن من حذف الملفات الموجودة في سلة المحذوفات، وسواها من الملفات المخزّنة مؤقتاً بشكل نهائي.
- تعلّم كيفية تشغيل تطبيق «سيكلينر» لحذف الملفات بشكل آمن من موقع «عُدّة الأمان»، الدليل الصادر عن منظمتي «فرونت لاين ديفندز» و«تاكتكل تكنولوجي كولكتيف».

### محو الملفات المحفوظة في أقراص التخزين، والأقراص الصلبة الجامدة، وشرائح الذاكرة

إنّ أقراص التخزين، بما فيها الأقراص الصلبة الجامدة، وشرائح الذاكرة لا تخزّن أو تمحو البيانات على طريقة الأقراص الصلبة العادية. فإذا أردت أن تمحو محتويات القرص الصلب الجامد، إحرص على استخدام أداة آمنة لهذه الغاية، تحصل عليها من موقع الشركة المصنّعة. ولن تضمن نجاح عملية المحو إلا بعد أن تتأكد من أنّ برنامج «ريكوفا» قضى نهائياً على بياناتك.

### كن سبّاقاً!

حسناً، لا ندّعي أنّ هذه التقنية هي المثلى لحذف الملفات، مع الإشارة بالطبع إلى أنّ ما تنشره عبر الإنترنت يبقى مخزّناً في الشبكة، وتعجز على الأرجح عن محوه.

- تقوم مكتبة الكونغرس الأميركي حالياً بأرشفة كل تغريدة تنشر على موقع تويتر، وتحفظها للأجيال القادمة.
- يحتفظ أرشيف الإنترنت، الذي انطلق العمل به في العام ١٩٩٦، بمئات آلاف المواقع، والملفات الصوتية، ومقاطع الفيديو، والكتب ذات الملكية العامة.
- يحتفظ موقع غوغل بنسخة عن كل صفحة من صفحات محركات البحث التي يسجّلها على خوادمه، ما يسمح للمستخدمين الاطلاع عليها حتى بعد زوال الموقع الذي تعود إليه.

تنبّه إلى أنّ مفهوم الخلود، أقله عبر الإنترنت، هو حقيقة ثابتة في عالم اليوم، إنما لا داعٍ إلى ممارسة الرقابة الذاتية على أعمالك بفعل هذا الواقع.

### عند استخدام جهاز كمبيوتر مشترك:

يمكنك استخدام نسخة محمولة من تطبيقي «إريسر» أو «سيكلينر»، مخزّنة ضمن شريحة ذاكرة، بحيث لا تخلّف وراءك سهواً «أي أثر» لأعمالك على جهاز الكمبيوتر. كما تتوافر أيضاً نسخة محمولة من برنامج «ريكوفا»، في حال اختفاء ملف معيّن من شريحة الذاكرة بطريقة مفاجئة.

- إحتفظ دوماً بنسخة محمولة من «إريسر» في شريحة ذاكرة.
- نزّل نسخة محمولة من «سيكلينر» لمحو آثار نشاطاتك عبر الإنترنت، والملفات المخزّنة مؤقتاً، والملفات الموجودة في سلة المحذوفات نهائياً.
- نزّل نسخة محمولة من «ريكوفا» لاستعادة الملفات التي حذفتها من دون انتباه.
- إطّلع على تطبيقات محمولة أخرى لحفظ أمنك.

## مصادر ومراجع إضافية

### "فرونت لاين ديفندرز" و"تاكتكل تكنولوجي كولكتيف"

- فيديو: دليل «أونو» لمحو الآثار التي تخلّفها وراءنا.
- كيف تستعيد البيانات بعد فقدانها.
- كيف تقضي على معلومات حساسة.
- كيف تستخدم برنامج «ريكوفا».
- كيف تستخدم نسخة محمولة من تطبيق «إريسر».

### "موبايل أكتيف"

- أدوات متحركة للنسخ الاحتياطي، وحذف البيانات، ومحو البيانات عن بعد.

### إزالة الآثار نهائياً

إذا استخدمت برنامج «إريسر» أو أي برنامج آخر للحذف الآمن، قد يمنحك أيضاً الخيار بأن تكتب فوق بياناتك المحذوفة لغاية ٣٥ مرة. قد يبدو لك الأمر مبالغاً فيه، (وسيستغرق بلا شك وقتاً أطول من احتمال الثلاث مرات، الذي ينصح بها معظم الخبراء، تفادياً لاستخدام وسائل استعادة البيانات الأكثر شيوعاً اليوم). ولكن، ماذا عن الوسائل المستقبلية؟

## قائمة مرجعية للحذف الآمن

### عند استخدام جهاز كمبيوتر خاص:

- نزّل وثبّت برنامج «إريسر». في قائمة الإعدادات، حدّد للبرنامج عدد المرات التي تريد أن يستخدمها عند حذف ملف منفرد (العدد المبدئي هو ٣٥)، أو عند الكتابة فوق البيانات القديمة المحذوفة التي قد تبقى مخفيّة ضمن المساحة الشاغرة من القرص الصلب (ثلاث مرات).
- قم بحملة تنظيف. لهذه الغاية، أطلق برنامج «إريسر» (سيتعيّن على مستخدم نظام ويندوز ٧ أن يشغّله بصفته مديراً لإتمام هذه المهمة)، ثم انقر على القائمة المستعرضة لجدول «إريسر»، واختر «مهمة جديدة». في النافذة المنبثقة، أنقر على زر «أضِف بيانات»، فاختَر خانة «مساحة القرص غير المستخدَمة»، وانقر على زر «نعم». يجب أن تطالعك الآن المهمة في نافذة برنامج «إريسر» الرئيسية. أنقر عليها بالزر الأيمن، واختَر «شغّل الآن». فمن شأن هذه التقنية أن تمحو أي ملفات قديمة حُذفت في السابق إنما قد لا تزال مخبّأة في القرص الصلب.
- نزّل وثبّت برنامج «سيكلينر». في خانة الخيارات، إختَر إعدادات، ثم شغّل «حذف آمن للملفات». حدّد عدد المرات التي تريد أن يطمس فيها «سيكلينر» البيانات المحذوفة. لا شك أنّ زيادة عدد المرات يطيل عملية الطمس، ولكنها تبقى الطريقة الأسلم.

### عند استخدام جهاز كمبيوتر مشترك:

- نزّل نسخة محمولة من برنامجي «سيكلينر» و«إريسر»، وثبّتهما في شريحة ذاكرة، لتتمكّن من حذف ملفاتك بشكل آمن عند استخدام كمبيوتر مشترك.

### ما إن تفقده، لا تستخدمه

تزيد حظوظك في استعادة البيانات من القرص بالامتناع عن استخدامه حالما تفقد البيانات. فقد تطمس البيانات القديمة التي تريد استعادتها ببيانات جديدة عند استخدامه.

# ١٠: مراعاة مخاطر تبادل البيانات عبر الإنترنت

## إستخدام خدمات تبادل الملفات، مثل خدمة دروب بوكس، بشكل آمن.

تمثّلت إحدى أهم الصرعات المفيدة التي شهدها عالم الإنترنت بخطوة الانتقال إلى الحوسبة السحابية، من خلال إيداع البيانات ضمن خوادم عامة، تسهّل عليك تبادلها مع أشخاص آخرين، أو تخزينها لاستعمالاتك الشخصية. وبفضل هذه التقنية، ما عاد الصحافيون الذين يلاحقون أخبارهم من عدة مواقع، أو يستخدمون عدة أجهزة لهذه الغاية، بحاجة إلى اصطحاب ملفاتهم أينما ذهبوا، بعد أن تيسّر لهم حفظها جميعاً في السحابة. كما أصبح اليوم التعاون في مسائل معيّنة، والذي كان يستلزم سابقاً الاستعانة بخوادم متطورة وتحمّل مشقات تقنية جمّة، بمنتهى السهولة، لدرجة تدفعنا إلى التساؤل كيف لم يفكّر أحد من قبل بهذه الحلول.

لا أحد ينكر فوائد هذه التقنيات المستحدثة: فالخدمات المتوافرة حالياً، كخدمة غوغل دوكس أو ملفات غوغل، تتيح لأي مجموعة الوصول إلى الملفات ذاتها عبر الإنترنت، والتعاون في ما بينها، وتجنّب الأخذ والرد في المراسلات. في الواقع، توفّر خدمات تبادل الملفات، كخدمة «دروب بوكس»، وسيلة مجانية أو غير مكلفة، للاحتفاظ بنسخة احتياطية عن ملفاتك في مكان بعيد.

لكنّ تبادل المعلومات عبر الإنترنت لا يخلو أيضاً من مخاطر الكشف عن نشاطاتك وأعمالك. لذا، يتعيّن عليك التنبّه إليها إذا كنت تريد استخدام هذه الخدمات بشكل مدروس.

على سبيل المثال، لا يبقى المجلد المتبادَل عبر الإنترنت «مراعياً للخصوصية» إلا بقدر ما يحمي الأعضاء المعنيون به كلمات السر، ويتحكّمون بحواسيبهم، وإلا انكشف النقاب عن عناوين جميع مستخدمي المجلد المشترك، وكذلك عن محتوياته، حتى ولو حافظ الملف على طابع الخصوصية. فمن غير المستبعد أن يطّلع على محتوياته العاملون لدى شركات تزويد خدمة الإنترنت أو الأشخاص المتاح لهم الوصول إلى خوادمها.

يجوز أيضاً لمستخدمي الهاتف الجوّال أن يفصحوا من حيث لا يدرون عن أماكن تواجدهم ومعلومات تعرّف عنهم، عند استخدام خدمات التبادل عبر الإنترنت، كتلك التي تسمح لهم مثلاً أن ينشروا تعليقات مقتضبة عبر صفحات الإنترنت من خلال خدمة الرسائل النصية.

لا يخلو التخزين السحابي من بعض الشوائب. فقد شرح مات هونان مؤخراً، في مقالة نشرها في مجلة «وايرد»، كيف تمكّن بعض القراصنة من اختراق حسابه السحابي، واستغلال ذلك لحذف بيانات موجودة في جهازه المحمول، وأجهزة الهاتف الموصولة به. إلى جانب هذه الظاهرة، قد يضطر مزوّدو الخدمات السحابية إلى الامتثال لأوامر سلطات إنفاذ القوانين في بلدانهم، وإطلاعهم على ملفات المستخدمين.

### أمن خدمة "دروب وكس"

تؤمّن خدمة «دروب بوكس» الاتصال بين حاسوبك وخوادمها بموجب بروتوكول «إتش تي تي بي آس»، وتشفّر ملفاتك فور تحميلها، مع أنّ الشركة لا تنكر اطّلاعها فعلياً على كلمة السر التي تعتمدها. كما توفّر اليوم ميزة التثبّت بخطوتين، التي يستطيع المستخدمون تشغيلها بواسطة إعدادات حساباتهم.

## المبادئ الأساسية

### إستخدم بروتوكول "إتش تي تي بي آس"

تفرض خدمتا «دروب بوكس» و«غوغل درايف» وما عداها من خدمات لتبادل الملفات الاتصال بموجب البروتوكول المذكور مبدئياً. لذا، إحرص على أن تكون الخدمة التي تختارها عبر الإنترنت مراعية للمبدأ ذاته، حتى تحمي حركة البيانات المتبادلة بينها وبين حاسوبك.

### تحقق ممن له حق الوصول

إذا كنت تدير أو «تملك» مجلداً مشتركاً، خصّص بعض الوقت لاستعراض الأشخاص الذين لهم حق الاطلاع عليه. هل ما زال الجميع بحاجة للوصول إلى مجمل ملفاتك؟ وإذا كان الملف يتعلق بتحقيق نشرته المؤسسة الإعلامية التي تعمل لديها العام الماضي، مثلاً، هل يجب أن يبقى متوافراً عبر الإنترنت؟ إذاً، لا تغفل عن مراجعة الحالات التي تسمح فيها الوصول إلى ملفاتك كل بضعة أشهر، ولا تستبعد أيضاً إمكانية القيام «بحملة تنظيفات» للتأكيد على رغبتك في عدم سحب الملفات المتاحة حالياً عبر الإنترنت.

### إستخدم التشفير

تشفّر خدمة «دروب بوكس» ملفاتك بعد تحميلها، ولكنها تحتفظ بمفتاح التشفير (كلمة السر) في حال طلبت منها سلطات إنفاذ القوانين الإطلاع على بيانات المستخدمين.

يقوم بعض الخدمات، كخدمة «سبايدرأوك»، بتشفير بياناتك الموجودة في حاسوبك قبل تحميلها من دون الاحتفاظ بكلمة السر، وهي تقنية تمنع الشركة من الكشف عن بياناتك، حتى بموجب أمر المحكمة.

إلا أنّ الأهم هو ألا تعتمد على خدمة تبادل الملفات وحدها لحماية خصوصيتك، بل احرص على تشفير بياناتك قبل تحميلها إذا كانت حساسة. ولهذا السبب، خير لك أن تستعين بتطبيق «تروكريبت» المجاني، إحدى الوسائل الناجعة لتشفير المجلدات التي تنوي تحميلها إلى خدمة تبادل الملفات.

### إحمِ ملفاتك المخزّنة في السحابة

يمكنك استخدام برنامج تشفير، كـ«تروكريبت» المتوافر على (www.truecrypt.org)، لحماية الملفات التي تنوي تخزينها عبر السحابة بكلمة سر.

### إستخدم شبكة افتراضية خاصة أو شبكة "تور"

إذا اخترت الوصول إلى «دروب بوكس» أو أي خدمة أخرى لتبادل الملفات، **من خلال متصفح**، قد ترتئي استخدام شبكة افتراضية خاصة أو شبكة «تور»، لعدم الكشف عن عاداتك عبر الإنترنت أمام الجميع. ولكن، تنبّه إلى ضرورة الاتصال دوماً عبر بروتوكول «إتش تي تي بي آس» بالخدمة التي تستخدمها، إلا إذا كنت تودّ فعلاً أن تطلع العاملين لدى الشبكة الافتراضية أو أحد العاملين في شبكة «تور» على نشاطاتك.

### عند استخدام جهاز كمبيوتر مشترك:

فيما يستمر العمل على تطوير نسخات محمولة من أداة «دروب بوكس»، قد يكون من الأفضل لك أن تستحصل على هذه الخدمة باستخدام متصفح محمول تتحكّم به.

تنطبق هذه التوصية أيضاً على جميع خدمات الإنترنت لتبادل الملفات. فإذا كنت لا تستخدم حزمة متصفح تور التي تأتي ضمن متصفح محمول، يُتاح لك أن:

- تنزّل النسخة المحمولة من متصفح «فايرفوكس».
- تستعلم عن التطبيقات الملحقة التي تحسّن مستوى الخصوصية عندما تستخدم متصفح «فايرفوكس».
- تنزّل آخر إصدار من حزمة متصفح تور من موقع Torproject.org لزيادة خصوصيتك وإخفاء هويتك محلياً عبر المواقع التي تزورها، إذا كنت تريد إخفاء هويتك.
- تتأكّد من أنّ الخدمة التي تستخدمها تؤمّن اتصالاً آمناً بخوادمها، لجهة اعتمادها مثلاً على بروتوكول «إتش تي تي بي آس» (النظام الآمن لنقل المعلومات).

### لا تعتمد كلمة سر يسهل خرقها

إحرص على حماية كلمات السر التي تعتمدها لخدمات تبادل الملفات المحفوظة في هاتفك الجوّال، أو لا تدعها على قصاصة ورق ملصقة بمكان ما على مكتبك أو شاشة حاسوبك!

### تبادل الملفات مع إخفاء الهوية

تعتبر خدمات تبادل الملفات بالطبع من أهم الأدوات التي تسهّل تعاونك مع الزملاء حول المشاريع التي تنفّذونها. ولكنك قد ترغب في تزويد مصادرك بوسيلة تخوّلهم أن يرسلوا إليك معلومات من دون الكشف عن هويتهم، فتكون أشبه بصندوق البريد الميت (السري)، الذي تتلقّى منه النصائح وما عداها من معلومات من دون أن تفصح عن هوية مصادرها.

إنّ سوء سمعة موقع ويكيليكس دفع بعض مطوري البرامج إلى البحث عن وسائل لإنشاء خدمات مماثلة للمخبرين، بما فيها

برنامجي «غلوبلليكس و»جيتوريوس». وفي إطار منفصل، حاول موقع Tor2web.org أن يتيح للمستخدمين نشر محتوياتهم عبر الإنترنت من دون الكشف عن هويتهم.

تتوافر للمخبرين على موقع LeakDirectory.org. قائمة لا يُستهان بها بالخدمات المتوافرة لصناديق البريد الميتة، أي الخدمات التي تخوّلك تحميل وإرسال ملفات إلى شخص آخر يستلمها لاحقاً، من دون أن تحفظها سجلات الخادم.

## مصادر ومراجع إضافية

- إحصل من موقع DrawingByNumbers.org على توصيات إضافية حول الاعتبارات التي يجب أن تأخذها بعين الاعتبار عند تبادل محتويات مع الآخرين.
- كتيّب للمدونين والمعارضين الناشطين عبر الإنترنت (مراسلون بلا حدود).
- آليات التدوين الآمن (مؤسسة الحدود الإلكترونية).
- التدوين المجهول الهوية باستخدام برنامجي «وورد بريس» و»تور» (الأصوات العالمية).
- الأمن المحمول (عُدّة الأمان).

## قائمة مرجعية حول استخدام آمن لنظام السحابة

### عند استخدام جهاز كمبيوتر خاص:

- إبدأ بقراءة التوصيات الصادرة عن «مراسلون بلا حدود»، ومؤسسة الحدود الإلكترونية، للتدوين الآمن. قد يصلح التنبّه إلى المحاذير ذاتها عند إنشاء حسابات لدى خدمات تبادل الملفات.
- أكنت تستخدم حساباً قديماً أو تنشئ حساباً جديداً، إحرص في كلتا الحالتين على اختيار كلمة سر قوية. يمكنك الحصول على معلومات إضافية حول إنشاء كلمات السر القوية من دليل «عُدّة الأمان» الصادر عن «فرونت لاين ديفندرز» و»تاكتكل تكنولوجي كولكتيف».
- تحقق من الموقع الخاص بخدمة تبادل الملفات التي تستخدمها، للتثبّت من أنه يوفّر الاتصال (عبر بروتوكول «إتش تي بي آس» مثلاً). أما إذا كانت خدمتك لا تؤمّن لك الاتصال الآمن، فاختر خدمة أخرى أكثر أماناً.
- إذا كنت تريد أن تستخدم خدمة تبادل الملفات، عبر شبكة افتراضية خاصة أو شبكة «تور»، فقد تكون مضطراً إلى ضبط تطبيقك لاستخدام هذه الخدمات.

### عند استخدام جهاز كمبيوتر مشترك:

- يمكنك دوماً الاستعانة بخدمة تبادل الملفات عبر متصفح، عند استخدام جهاز كمبيوتر مشترك. لذا، إتّبع أفضل الممارسات المرعية لإنشاء كلمات السر، باختيار كلمة سر قوية، من دون أن تخزّنها على جهاز كمبيوتر خاص، وبحذف ملفاتك المؤقتة بواسطة أداة «سيكلينر»، عند الانتهاء من استعمالها.
- تثبّت من أنّ خدمة تبادل الملفات عبر الإنترنت تفرض الاتصال الآمن عبر بروتوكول «إتش تي بي آس».
- تحقق من خلو جهاز الكمبيوتر المشترك من برمجيات خبيثة قد تسجّل نشاطاتك.
- إذا كنت بحاجة لمزيد من الخصوصية، أو إذا كانت خدمات تبادل الملفات محظورة ضمن منطقتك، فيجوز لك أن تستخدم نسخة محمولة من الشبكة الافتراضية الخاصة أو المتصفح أو حزمة متصفح «تور» للاستفادة منها.

## ملاحظات

# ١١: الهواتف الجوالة الآمنة

## إستخدم هاتفك الجوال بشكلٍ آمن لإنجاز مهام متعدّدة

لما كانت الهواتف الذكية قد ازدادت عدداً وتطوّراً، والشبكات التي تعتمد عليها ازدادت انتشاراً، فقد اتخذها الناس، بدون تردّد، أداةً للعمل. فلا يخفى على أحد أنّ هواتفنا اليوم، تنجز الكثير من المهام التي كان الكمبيوتر الثابت ينجزها في السابق: فهي تتيح لنا نشر أفكارنا على الشبكات الاجتماعية، وتصفّح البريد الإلكتروني، وتعديل الصور أو المقاطع الصوتية، وإجراء الأبحاث عبر الإنترنت، كلّ ذلك بكفّ اليد. بالفعل، ليس من أجهزة أخرى تساعد هذا الكمّ من الأشخاص في مختلف الأماكن على الوصول إلى المزيد من المعلومات. وإضافة إلى كل ما تقدّم، تجيز لنا هذه الهواتف إجراء الاتصالات أيضاً!

لكن من الضروري أن نفهم أنّ الوصول إلى المعلومات يتمّ بشكلٍ متبادل: فمبقدور هاتفك، بما يحويه من أسماء وسجل بأحدث المكالمات والرسائل القصيرة، لا بل حتى سجل نشاطاتك الإلكترونية وموقعك الجغرافي، أن يزوّد شخصاً غريباً بمعلومات كثيرة عن حياتك الشخصية والمهنية، ربّما أكثر مما كنتَ تقصد في المقام الأول.

في الوقت نفسه، قد تحتفظ شركات تزويد خدمة الهواتف الخليوية بمجموعة من البيانات المتعلقة بالزبائن، سواء لإعداد الفواتير الخاصة بهم أم لأغراض أخرى، كموقعهم الجغرافي، والرسائل القصيرة التي أرسلوها، ومتى أرسلوها، ومتى أجريت الاتصالات، وهكذا دواليك.

وتبعاً للشركة التي تقدّم الخدمة، يمكن أن يتمّ تبادل هذه المعلومات مع شركات أخرى. فلما كانت هذه الشركات تخضع لقوانين الدول التي تعمل فيها، فمن الممكن تبادل هذه المعلومات نفسها مع السلطات، وبالتالي مع سلطات الحكومات الأخرى التي أبرمت معها اتفاقات. (للمزيد من المعلومات عن طريقة عمل الهواتف الجوّالة، وأبرز المخاطر المرتبطة بها، يمكن الاطلاع على كتيّب «الأجهزة الخليوية والأمن» الصادر عن منظمة «تاكتكل تكنولوجي كولكتيف».

### حصّن أمن هاتفك

يجب أن تحمي هاتفك الذكي بكلمة سر قوية، على الدوام، كي تحمي البيانات الموجودة فيه في حال فقدته أو سُرق منك.

مع أنك تستطيع حماية البيانات الموجودة في هاتفك، إضافةً إلى بعض النشاطات الإلكترونية، وفق طرق مبيّنة أدناه، لكن لا بدّ من أن تتذكّر أنّ الاتصالات التي تجريها عبر الهاتف، إضافةً إلى الرسائل القصيرة ستكون مكشوفةً لدى شركة خدمة الهاتف أو أيّ شخص آخر يملك المعدّات أو المهارات اللازمة للاطلاع عليها.

### تمتلك به

من أهم ميزات الهواتف المحمولة حجمها: فهي تقدّم الكثير من المعلومات ضمن حجمٍ ملائم. لكن من السهل أيضاً فقدان الهواتف بسبب حجمها هذا، لا بل إنّ هذا الأمر يجعلها عرضةً للسرقة والمصادرة منك أيضاً. فحذار! لقد قدّرت إحدى الشركات المتخصصة في أمن المحمول «قيمة الهواتف المحمولة التي يفقدها مستخدمو «لوك آوت» وحدهم بسبعة ملايين دولار يومياً». من هنا، إنّ التمسّك بهاتفك وعدم إبعاده عن ناظريك يعتبر من الأولويات.

## حصّنه بكلمة سر يصعب اختراقها

في قسم «حماية بياناتك»، راجعنا فوائد استخدام كلمات السر القوية للحفاظ على سرية المعلومات الموجودة ضمن جهازك. وينطبق الأمر نفسه على الهواتف المحمولة.

فلا يخفى عليك أنّ العديد من أنظمة تشغيل الهاتف، مثل «أندرويد» و«بلاكبيري» و«آي. أو. إس. آبل» تسمح لك بوضع كلمة سر تفوق الأربعة أرقام، كما تتضمّن مزيجاً من الأرقام والرموز والعلامات الخاصة. (زر الموقع الإلكتروني للشركة المصنّعة للاطلاع على التوجيهات الملائمة).

فضلاً عن ذلك، تتضمّن بعض الهواتف، مثل «بلاكبيري» والهواتف المزوّدة بخدمة «أندرويد ٤» أو ما يفوقها مستوىً، ميزة تشفيرٍ مضمّنة للبيانات الموجودة في الهاتف، مما يضاعف من معايير الحماية لا سيّما إذا تمكّن أحدهم من الوصول إلى هاتفك فعلياً. أما إذا كنتَ تستخدم الآيفون، فمن الممكن تحميل تطبيقات طرف ثالث، مثل «ويكر»، لتأمين هذا النوع من الحماية أيضاً. زر الموقع الإلكتروني للشركة المصنّعة للهاتف والتطبيقات الخاصة بالتشفير المتوفّرة لنموذج الهاتف الذي تعتمده.

- للحصول على المزيد من النصائح عن إنشاء كلمات السر القوية، زر الموقع الإلكتروني «عدّة الأمان».

### قلّص من محاولات فتح القفل

بعض الهواتف الذاتية تُقفَل بشكلٍ تلقائيّ عند طباعة عبارات السر غير المناسبة أكثر من مرة. إقرأ التوجيهات الخاصة بالنموذج الذي تستخدمه، لتتبيّن إن كانت هذه الميزة متاحة لك.

## ضع البيانات في المتناول

إذا كنتَ خائفاً من أن تتمّ مصادرة هاتفك منك في أيّ وقت كان، رغم ما تتّخذه من احتياطات، لعلّه من الأفضل أن تحتفظ بالبيانات الحسّاسة، كجهات الاتصال والصور، على شريحة الذاكرة (مثل «مايكرو آس دي») بحيث يمكن فصلها عن الهاتف والتخلّص منها بسهولة.

لكن لا تتضمّن كل الهواتف ميزة الاستعانة بشرائح الذاكرة. في هذه الحالة، فكّر في حفظ البيانات الأكثر حساسيةً على بطاقة السيم التي يمكن استخراجها من الهاتف وإتلافها إذا دعت الحاجة، وإن لم تتمّ العملية بالسرعة المطلوبة.

## إحفظ النسخ الاحتياطية واحمها

كما هو مبيّن في فقرة «إحفظ بياناتك» أعلاه، يجب أن تحتفظ دوماً بأكثر من نسخة عن بياناتك، إحداها في متناولك وأخرى مخبّأة في مكان آخر، للوقاية من الكوارث الطبيعية وتلك التي يفتعلها الإنسان.

بعض شركات تصنيع الهاتف توفّر برنامجاً احتياطياً يحفظ البيانات بالتزامن مع حاسوبك الشخصي، كما يشفّرها في الوقت نفسه. إذا لم يكن هاتفك يتضمّن تطبيقاً خاصاً يسمح بالتشفير، سيبقى بإمكانك حماية نسخك الاحتياطية من خلال حفظها ضمن ملف مشفّر على الحاسوب أو على محرّك أقراص خارجي بواسطة تطبيق شبيه بـ«تروكريبت».

تماماً كما في الكمبيوتر، يمكنك الاعتماد على الروزنامات أو غيرها من الأساليب لتنبيهك إلى تحديث نسخك الاحتياطية بشكلٍ منتظم.

- إحصل على مزيد من المعلومات عن «تروكريبت» على الموقع الإلكتروني لمصنّع البرنامج.
- زر الموقع الإلكتروني «عدّة الأمان» للتدرّب على استخدام برنامج «تروكريبت».

## إجعل اتصالاتك أكثر خصوصية

طوّر مشروع «غارديان» مجموعة ثلاثية من التطبيقات التي تحفظ الخصوصية لمستخدمي «أندرويد»- وهي «أوربوت»، «أورويب»، و«جيبربوت»- وتؤمّن درجةً عاليةً من السرية للأشخاص الذين يستخدمون هاتف أندرويد لتصفّح الإنترنت أو للدردشة.

في حال تصفّح الإنترنت، يقدّم «أوربوت» و«أورويب» ميزةً إضافية هي السماح بزيارة بعض المواقع الإلكترونية التي ما كانت متوفّرة من خلال متصفّح عادي. في هذا الإطار، يُرجى الاطلاع على الفصل المتعلق برصد مشاكل الوصول إلى المواقع ومعالجتها، لفهم بعض القضايا المحيطة بهذا الموضوع.

تماماً كما تطبيق «بدجن» (المزوّد بوظيفة إضافية للتراسل الفوري الآمن) الذي تمّ التطرّق إليه في الفصل المتعلق بـ«الاتصال الآمن عبر الدردشة والمكالمات الصوتية»، يتيح تطبيق «جيبربوت» للتراسل الفوري للمستخدمَين اللذين «يتثبّتان» من بعضهما بأن يدردشا بلغةٍ مشفّرة، بحيث لا يكون نص الدردشة متاحاً أمام شركة تزويد الخدمة، أو جهات أخرى تقف ما بين الاثنين. أما بالنسبة للآيفون، فبإمكان «ويكر» أن يشفّر محتويات الرسائل الفورية المرسلة إلى مستخدمين آخرين ضمن البرنامج نفسه، إلا أنه لا يزوّد المستخدم

بالسرية. وبينما كان «البلاكبيري» الرائد في تأمين خدمة الدردشة المشفّرة، انتشرت بعض المخاوف بشأن سياساته ومشاركته في بعض مشاريع المراقبة.

- تعلّم كيف تستخدم «جيبربوت» ضمن دروس تعليمية عبر موقع «موبايل أكتيف».
- إحصل على المزيد من المعلومات عن «جيبربوت» عبر مشروع «غارديان».
- إقرأ التعليمات الواردة على موقع «موبايل آكتيف» بشأن تصفّح الإنترنت بسرية من خلال برنامج «أوربوت».

سهّلت بعض خدمات الويب، مثل «فايسبوك» و«تويتر»، على المستخدمين الوصول إليها، من خلال تحميل تطبيقات صغيرة خاصة بها على هواتفهم الذكية، مع أنّ الحفاظ على الخصوصية قد لا يكون همّها الرئيسي. في هذا الإطار، تقدّم «موبايل آكتيف» بعض التوصيات السهلة التي تمكّننا من استخدام كل خدمة بمزيدٍ من الأمان:

- تعلّم كيف تستعمل «فايسبوك» بمزيدٍ من الأمان.
- تعلّم كيف تستعمل «تويتر» بمزيدٍ من الأمان.

## تنبّه لما تقوم بتنزيله وللمعلومات التي تملك التطبيقات حق الوصول إليها

قبل أن تنزّل تطبيقاً على هاتفك المحمول، تأكّد إذا كنتَ تحتاج لهذا التطبيق فعلاً، وإن كان هذا التطبيق هو ما تبحث عنه فعلاً، وتأكّد من أنه لا يشترط الاطلاع على معلوماتك الشخصية بما يتجاوز الحدود المقبولة.

تماماً كما تفعل عند تنزيل تطبيقٍ على كمبيوتر، راجع ملاحظات المستخدمين السابقين وتعليقاتهم، فضلاً عن مراجع أخرى قبل تنزيل أيّ تطبيق على هاتفك.

## نزّل دروع حماية

صحيحٌ أنّ مستخدمي الهواتف المحمولة ما زالوا غير معتادين على تلقّي الفيروسات والبرمجيات الخبيثة، إلا أنّ هذه الأخيرة باتت أكثر انتشاراً مع انتشار الهواتف الذكية. وقد أصبحت معظم الشركات المكافحة للفيروسات ترفق جدار حماية بتطبيقاتها المعدّة للتنزيل على الهواتف المحمولة، رغم أنّ هذه البرامج لا تكون مجانية في بعض الأحيان. أما هواتف «أندرويد» التي تقبل أيّ نظام تشغيل أكبر من ٤,٠، فتتضمّن ميزة تشفير. يكفي أن تنتقل إلى إعدادات -> الأمن وإقفال الشاشة للانطلاق. بالنسبة للإصدارات الأولية من «أندرويد»، يمكن الاستعانة بـ «دروبد وول»، المتوفّر في سوق «غوغل بلاي»، لكنّ تنزيله قد يكون صعباً لأنه يشترط الحصول على امتيازات المستخدم الأساس عند الدخول إلى هاتفك.

- يمكن الاطلاع على المزيد من المعلومات عن «دروبد وول» على الموقع الإلكتروني للشركة المصنّعة.

## ماذا لو وقع المحظور؟

**لقد أُخذ مني هاتفي!**

إذا سُرق منك هاتفك، أو تمّت مصادرته، فلن يكون بمقدورك فعل الكثير إلا في حال كنتَ قد اتخذتَ خطواتٍ معيّنة قبل فقدان الهاتف:

- إذا كنتَ قد ضبطتَ هاتفك بحيث تستفيد من ميزة المسح عن بعد، إستعملها في الحال. فيتيح لك ذلك إرسال رمز إلى هاتفك يطلب من الجهاز محو كلّ البيانات الموجودة على هاتفك.
- غيّر كلمات السر لكل الحسابات التي تستعملها على الهاتف أيضاً، مثل البريد الإلكتروني وحسابات فايسبوك وتويتر.
- راجع نتائج التقييم الأولي للمخاطر: إذا حاول أحدهم فكّ تشفير المعلومات على هاتفك، أو استطلاع قوائم الاتصال الواردة فيه، أو سجلّ المكالمات، أو الرسائل القصيرة، أو أيّ بيانات أخرى، من سيكون بخطر، كيف، وإلى أيّ مدى.
- بلّغ الأشخاص الذين قد يتضررون نتيجة فقدان هاتفك.

**أعتقد أنّ أحدهم يسجّل مكالماتي!**

إذا كنتَ تعتقد أنك تتعرض للتنصّت وأنّ مكالماتك مسجّلة، يمكنك اتخاذ بضع خطوات لمعالجة الوضع بشكلٍ مؤقّت:

- أولاً، راجع توصيات «موبايل آكتيف» لمعالجة مسألة المراقبة، فضلاً عن توصيات «عُدّة الأمان» للاطلاع على أفضل الممارسات لضمان أمن الهواتف.
- أطفئ الهاتف المعرّض للخطر وانزع عنه البطارية.
- إشترِ جهازاً آخر و«بطاقة سيم» جديدة (من الضروري أن تبتاع كلا الغرضَين، بما أنّ كلاً منهما يملك رقم تعريف خاصاً به. فمجرّد استبدال «بطاقة السيم» لن يزوّدك بهوية جديدة إذا لم يكن الهاتف جديداً بدوره).
- قبل أن تركّب البطارية في الهاتف الجديد: تنبّه إلى إمكانية تعقّب موقع الهاتف سواء كنتَ تستعمله أم لا، وسواء كان الهاتف مغلقاً أم شغّالاً. لذا، إنّ نقل الهاتف معك إلى منزل أو مكان العمل سيربط الهاتف الجديد بهذه المواقع.
- لا تركّب البطارية في الخارج إلا إذا كنتَ تنوي إجراء المكالمات. بعد أن تنهي المكالمة، إنزع البطارية من جديد. لعلّه من الأفضل

تنبيه زملائك وأصدقائك إلى أنّ هاتفك سيكون متاحاً في ساعاتٍ محدّدة فقط. واحرص على ألا تكون في المنزل أو في مكان العمل خلال تلك الساعات.

- إشترِ بطاقة «آس دي» جديدة.
- إنسخ قوائم الاتصال من بطاقتك الرقمية القديمة إلى البطاقة الجديدة، بواسطة جهاز الكمبيوتر، من دون أن تنقل التطبيقات.

## مصادر ومراجع إضافية:

**"موبايل آكتيف":**

- دليل المستخدم إلى «أوربوت»- تصفّح الإنترنت على هاتفك الجوّال بواسطة متصفّح «تور» للخصوصية؛
- «فايسبوك» أكثر أماناً؛
- «تويتر» أكثر أماناً؛
- أدوات الهاتف الجوّال للنسخ الاحتياطي، وحذف البيانات، ومحوها عن بعد.

**عُدّة الأمان:**

- كيفية استخدام الهواتف الجوّالة بأكبر قدر ممكن من الأمن.

## قائمة مرجعية لاستخدام الجوال بأمان أكبر

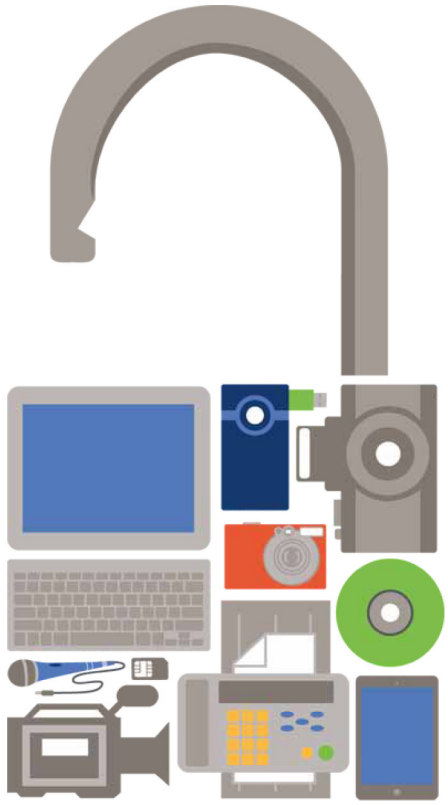
أقفل هاتفك بواسطة كلمة سرّ أو رقم تعريف شخصي. إذا كان هاتفك يتيح لك استخدام كلمة سرّ تفوق الأربعة أرقام، إستفد من هذه الميزة. عوّد نفسك على إبقاء الهاتف مقفلاً عندما لا تستخدمه.

إذا كان هاتفك يقدّم ميزة تشفير مدمجة، على غرار هواتف «البلاكبيري» و«الأندرويد»، تأكّد من أنك تستفيد من هذه الميزة. إذا كنت تملك هاتف «آيفون»، يمكنك تحميل تطبيق خارجي مثل «ويكر» للاستفادة من الخدمة نفسها.

جديرٌ بالذكر أنّ بعض الهواتف الذكية تُقفل تلقائياً عند طباعة عبارة مرور غير صحيحة عدّة مرات. إقرأ الإرشادات المرفقة بهاتفك لتعرف إن كان يوفّر لك هذه الميزة.

إختر طريقة لحفظ نسخة احتياطية عن البيانات الموجودة في هاتفك. حاول أن تحفظ بياناتك بشكلٍ منتظم وتحميها من خلال تشفيرها.

# ١٢: تطبيق معايير "السلامة أولاً" على التقنيات الأخرى



**تعنى الأجهزة غير الذكية كفاية، كأجهزة الفاكس والكاميرا، بالمسائل الأمنية أيضاً.**

كلما أصبحت أكثر وعياً للتحديات الأمنية التي تواجهها عبر الإنترنت، وأخذت تكتسب عادات جديدة تحفظ النشاطات التي تقوم بها كصحافي أو مدوّن، قد تفكّر في تطبيق المعارف المكتسبة على تقنيات أخرى تستخدمها إلى جانب جهاز الكمبيوتر أو الهاتف الذكي. إليك في ما يلي بضع أمثلة:

## إستخدام الفاكس

يجدر بالصحافيين الذين يستخدمون جهاز الفاكس أن يراعوا الاعتبارات التالية:

- إذا طُلِب منك أن تزوّد رئيس التحرير أو المصدر الذي تتعامل معه بإسمك أو عنوانك، عند إرسال فاكس، زودهما باسم مستعار تتفقان عليه مسبقاً.
- إستعِد الصفحات بعد أن ترسلها بالفاكس. إياك أن تنساها في المتجر الذي أرسلتها منه.

## الصور والفيديو

لا تقتصر الصور الرقمية التي تلتقطها على الصورة التي تطبعها، إذ تنطوي على معلومات إضافية. في الواقع تتضمّن بيانات التعريف، أي المعلومات التي تشتمل عليها تلقائياً كل صورة، التاريخ والوقت مطبوعين، ونوع الكاميرا المستخدمة، وفي أغلب الأحيان، الموقع الذي التقطت فيه الصورة بفضل نظام تحديد المواقع العالمي. وقد تتضمّن ملفات الفيديو أيضاً بيانات وصفية. لكنّ بعض التطبيقات، على شاكلة «إيرفانفيو»، يساعدك على استعراض وحذف هذا النوع من المعلومات من حاسوبك.

إذا كنت تخشى أن تسهّل إحدى الصور أو ملفات الفيديو التي تنوي نشرها اقتفاء أثرك، فعليك أن تتعلّم كيفية إزالة هذه المعلومات، ثم تحميل المواد المذكورة بأمان. كما يجدر بمستخدمي هاتف أندرويد الاستعلام عن تطبيق «أوبسكيورا كام» الذي طوّره مشروع «غارديان» وموقع Witness.org . يسمح هذا الأخير للمستخدمين إخفاء بعض عناصر الصورة، باستخدام الكاميرا وحدها.

### المعلومات الكامنة وراء الصورة

إنّ برنامج «إيرفانفيو» هو أداة شائعة الاستعمال ومجانية تبيّن لك المعلومات «المخفية» التي قد تشتمل عليها صورك.

إليك بعض المراجع الإضافية:

- تعلّم من منظمة «موبايل آكتيف» كيف تمحو من صورك المعلومات الدالة على مكان تواجدك.
- إستعلم عن الوظائف الإضافية ضمن برنامج «إيرفانفيو» لتشغيل الفيديو.
- إحصل على نصائح مفيدة من شركة «سمول وورلد نيو» حول كيفية إنتاج مواد إعلامية بشكل آمن.
- إستعلم عن تطبيق «أبسكيورا كام» لنظام أندرويد، أو...
- نزّل «أبسكيورا كام» من سوق «غوغل بلاي».

## الكاميرا والمايكروفون في جهاز الكمبيوتر الخاص

في مطلع العام ٢٠٠٩، اكتشف الباحثون فيروساً من فصيلة

أحصنة طروادة أسموه «غوست نت». يسمح هذا الفيروس للقراصنة، على سبيل التعداد لا الحصر، التحكّم عن بعد بأجهزة الكاميرا والمايكروفون الموصولة بأجهزة الكمبيوتر المصابة بفيروس، تمهيداً لاستخدامها على الأرجح لأغراض التجسس. وقد تمّ رصد هذا الفيروس في أكثر من ١٠٠ بلد.

وفي شباط/فبراير ٢٠١٢، لوحِظ وجود خلل في كاميرا الويب ذات العلامة التجارية «تراندنت»، يخوّل مستخدمي الإنترنت الاطلاع على التلقيمات «الخاصة» بآلاف الأشخاص الذي يستخدمون هذه الأجهزة، بعد رصدها.

أين المغزى في ذلك؟ قد تكون الكاميرا أو المايكروفون الموصولين بحاسوبك في وضعية التشغيل من دون علمك. وبغض النظر عن رأيك في هذا الموضوع، فاعلم أنّ نظام ويندوز يتيح لك إلغاء تثبيت البرنامج الذي يربط الكاميرا والمايكروفون بحاسوبك المحمول، بهدف إبطال تشغيلهما بالدرجة الأولى. لهذا الغرض، إذهب إلى أيقونة البداية و«مدير الجهاز»، بحثاً عن أجهزتك ضمن الأجهزة المدرجة في القائمة، ثم أنقر عليها بالزر الأيمن، واختر خيار إلغاء تثبيتها من بين الخيارات المتاحة لك). وإلا يمكنك بالطبع اللجوء إلى عادة درجت قديماً وهي تغطية العدسة بشريط.

## ملفات بودكاست حول الأمن عبر الإنترنت

يمكنك أن تحصل على مزيد من المعلومات حول الثغرات الأمنية والتهديدات اليومية عبر الإنترنت من ملفات بودكاست، كـ«سيكيوريتي ناو!» و«إنترنت ستورم سنتر» التابع لمعهد التكنولوجيا «آس آي آن آس».

## ملاحظات

# ١٣: ما العمل لو...

## الإسعافات الأولية لجهاز كمبيوتر مصاب، وحساب مخترَق، وحالات طارئة أخرى.

عندما صُمِّمت شبكات الإنترنت والهاتف لم تكن الثغرات الأمنية مأخوذة في الحسبان. فصعُب على المستخدم تجنّب المخاطر التي تحيط بأجهزته، حتى في ظل التدابير الاحترازية التي يتخذها. إليك في ما يلي بعض الخطوات الواجب اتباعها عند وقوع المحظور:

### إذا أصيب حاسوبك بفيروس!

- حدِّث التطبيقات التي تستخدمها لمكافحة البرمجيات الخبيثة.
- أفصل جهازك عن الشبكة.
- أعِد تشغيل جهاز الكمبيوتر وفق الوضعية الآمنة (في معظم أجهزة الكمبيوتر، تدخل الوضعية الآمنة من خلال النقر على زر إف ٨ عند إعادة إقلاع الحاسوب. ولكن يستحسن أن تعود إلى دليل المستخدم لمعرفة كيفية تشغيل هذه الوضعية في نوع الجهاز الذي تستخدمه).
- أفحص الكمبيوتر، مع الحرص على اختيار خانة «الفحص الكامل». (قد لا تعمل بعض التطبيقات المضادة للبرمجيات الخبيثة وفق الوضعية الآمنة، لذا إبدأ بالتطبيقات التي تفعل. ثم أعِد إقلاع الكمبيوتر بشكل عادي من أجل تشغيل تطبيقات الفحص بفضل البرامج المتبقية).
- إذا نلت شهادة صحية خالية من أي عيوب، أو عثرت على برمجيات خبيثة ثم أزلتها، لا تتردد في استشارة رأي آخر:
  - شغّل إحدى برامج الفحص عبر الإنترنت، كبرنامج «هاوس كول»، أو...
  - شغّل أداة فحص من خارج الشبكة، كبرنامج مايكروسوفت لفحص الكمبيوتر، أو قرص الإنقاذ من شركة «آي في جي»، أو برنامج «كومودو» لأساسيات التنظيف.
  - إذا كنت تستخدم نظام ويندوز، أدرس إمكانية تشغيل أداة التشخيص «هايجاك ذيس» للكشف عن جميع الآليات العاملة على جهازك. وبما أنّ هذا البرنامج لا يميّز بين الآليات «الجيدة» و«السيئة»، فحريٌّ بك أن تنشر النتائج التي توصلت إليها عبر أحد المنتديات، أو أن تستعين بأداة إلكترونية، كبرنامج «هايجاك ذيس»، لمساعدتك على فهم ما تراه قبل أن تحذف أي ملفات.
- إذا لم تتخلّص من الفيروس، فيجدر بك أن تفكّر في...
- العودة إلى «صورة» أخذتها سابقاً عن القرص الصلب في حاسوبك - راجع الفصل المتعلق بالنسخ الاحتياطي للاطلاع على هذه الآلية.
- محو محتويات القرص الصلب ببرنامج متخصص كبرنامج «داريكس بوت ونيوك»، ثم إعادة تثبيت نظام التشغيل والبرامج التي تستخدمها.

### هل يخلو جهازك حقاً من البرمجيات الخبيثة؟

عند إصابة جهازك بفيروس، سيصعب عليك جداً أن تجزم إذا كان خالياً من البرمجيات الخبيثة، حتى ولو كان التطبيق الذي تستخدمه لمكافحة الفيروسات يثبت هذا الواقع. فغالباً ما يملي القراصنة على فيروساتهم تجنّب أدوات الرصد، وهي تنجح في ذلك. لذا، قد تضطر إلى محو محتويات القرص الصلب ثم إعادة تثبيت نظام التشغيل والبرامج.

## حاسوبي يجد صعوبة في الإقلاع!

إذا كان حاسوبك يقلع بصعوبة أو يتعطّل باستمرار في مرحلة الإقلاع، فقد يعود ذلك إلى عدة أسباب، وتحتاج إلى خبير لإصلاح الكمبيوتر.

في حال صادفتك مشاكل مماثلة:

- عد إلى النُسَخ الاحتياطية التي تسمح لك مواصلة عملك باستخدام جهاز آخر، عند الضرورة، بانتظار الانتهاء من إصلاح الكمبيوتر.
- إبقَ بجانب الشخص الذي يساعد في إصلاح جهازك: إنها لفرصة مؤاتية أن تتعلّم كيف يشخّص الخبراء المشاكل، ناهيك عن ضرورة أن تمنع هذا الشخص من الاستيلاء على القرص الصلب في جهازك واستبداله بآخر من دون علمك أو إذنك.
- إياك أن تترك جهازك في أي متجر ما لم تنتزع منه القرص الصلب أولاً.
- إذا دعت الحاجة إلى استبدال القرص الصلب، فاحرص على أن يُستبدَل بحضورك، وأن تحتفظ بالقرص القديم. وإذا اقتضى الأمر نقل البيانات من القرص القديم إلى القرص الجديد، فليكن ذلك بحضورك أيضاً، مع الحرص على أن تُنسَخ البيانات من الجهاز الذي جرى إصلاحه، لا من جهاز ثالث في المتجر.
- إذا اضطررت إلى الاستعانة بشخص لاستعادة البيانات من القرص الصلب في جهازك، فليكن ذلك بحضورك، لأنّ إيداع القرص الصلب في المتجر ليس خياراً مستحباً.

### بلّغ عن الهجمات الإلكترونية

هل تعرضت يوماً لهجوماً إلكترونياً؟ يمكنك الاتصال بـ«مراسلون بلا حدود» للتبليغ عما جرى.

## ثمة من يستغل حسابي!

إذا رصدت نشاطات مشبوهة في حسابات البريد الإلكتروني أو مواقع التواصل العائدة إليك، وأنت مستمر في استخدامها، يجدر بك أن:

- تؤكّد في الإعدادات أنّ جميع العناوين البريدية أو الأرقام الخلوية المرتبطة بالحساب تخصّك.
- تغيّر كلمة السر وأسئلة الأمان، تبعاً للتوجيهات الموصى بها.
- تتعلّم كيف تؤمّن حماية إضافية لحسابك من خلال آلية التثبّت بخطوتين.
- إذا ما عدت قادراً على استخدام حساباتك، يجدر بك أن:
- تتصل بفريق الدعم لدى مزوّد خدمة البريد الإلكتروني، وإبلاغه بشكوكك حيال استيلاء أحدهم على حسابك، طالباً منه تزويدك بالخطوات اللازمة لإعادة ضبط كلمة السر.
- تستبدل حسابك بحساب آخر، محصّناً بكلمة سر وأسئلة أمان جديدة، تبعاً لتوجيهات صادرة في فصول أخرى من هذا الدليل.
- إذا عجز مزوّد الخدمة عن مساعدتك في استعادة حسابك، فأعلم أصدقاءك وزملاءك بأنك تشتبه بوجود من يستغلّ حسابك، طالباً منهم عدم الرد على الرسائل الإلكترونية أو أي رسائل أخرى تَردهم من الحساب، ولفت انتباهك إلى أي نشاطات مشبوهة يرصدونها. ثم اعرض عليهم أن تقدّم ما يثبت هويتك الحالية عبر الهاتف أو سكايب أو شخصياً، إذ كيف لهم في النهاية أن يتعرّفوا عليك فعلياً لولا ذلك؟
- تنسخ قائمة الاتصال من الحساب المخترَق، باستخدام آخر نسخة احتياطية لبريدك الإلكتروني.
- تنقل بريدك الإلكتروني خارج الشبكة من البريد المخترَق إلى صندوق البريد الجديد. إذا كنت تستخدم برنامج عميل لإدارة البريد الإلكتروني كبرنامج «ثندربرد».

## ملاحظات

# مسرد بأهم المصطلحات المستخدَمة

تيسّر إعداد المسرد التالي للمصطلحات التقنية، جزئياً، بفضل رخصة المشاع الإبداعي للمصنّفات الفكرية غير التجارية، تحت إصدار (CC BY-NC ٣,٠)، من موقع «عُدّة الأمان»، العائد إلى كل من منظمة «تاكتكل تكنولوجي كولكتيف» و«فرونت لاين ديفندرز».

في ما يلي تعريف ببعض المصطلحات التقنية التي قد تصادفك في هذا الدليل:

- **إريسر** – أداة تحذف بشكلٍ آمنٍ ونهائي المعلومات من الكمبيوتر أو من جهاز التخزين القابل نقله.
- **أنديليت بلاس** – أداة من البرمجيات المجانية يمكنها أحياناً استعادة المعلومات التي حذفتها عن طريق الخطأ.
- **اسم النطاق** – العنوان، بالكلمات، الخاص بموقع إلكتروني أو خدمة إنترنت؛ مثلاً security.ngoinabox.org
- **أفاست** – أداة مجانية لمكافحة الفيروسات.
- **إقلاع** – عملية تشغيل الكمبيوتر.
- **أوبن دي إن إس** – خدمة مجانية (للأفراد) تستبدل خدمة دي إن إس التي يقدّمها مزوّد خدمة الإنترنت للمستخدم بخدمة أخرى أكثر تنظيماً. تساعد في حماية المستخدم من هجمات «الرجل في الوسط» في حال كان المخترقون أو سواهم يسيئون استخدام جداول التوجيه المحلية لنظام اسم النطاق.
- **إينغمايل** – خدمة إضافية على برنامج ثندربيرد للبريد الإلكتروني تسمح له بإرسال وتلقي الرسائل الإلكترونية المشفّرة والموقعة توقيعاً رقمياً.
- **برمجيات مجانية** – تتضمّن البرمجيات المجانية إنما الخاضعة لقيود قانونية أو تقنية تمنع المستخدمين من الوصول إلى رمز المصدر المستخدم لابتكارها.
- **برمجيات مجانية ومفتوحة المصدر** – تتوافر هذه الأسرة من البرمجيات مجاناً ولا قيود قانونية عليها تمنع المستخدم من اختبارها، وتبادلها، أو تعديلها.
- **بت لوكر** – تطبيق معتمد في نسختي «إنتربرايز» و«ألتيمت» من «ويندوز فيستا» و«ويندوز ٧»، سهل الاستخدام ولا يقفل على الكمبيوتر فحسب بل على محرّكات الأقراص الصلبة - كتلك التي قد تستخدمها لحفظ نسخة احتياطية عن بياناتك.
- **بدجن** – برمجيات مجانية ومفتوحة المصدر للرسائل الفورية، تدعم وظيفة إضافية للتشفير معروفة بالتراسل الفوري الآمن.
- **البرمجيات الخبيثة** – مصطلح عام لجميع البرمجيات الخبيثة، بما في ذلك الفيروسات، والبرمجيات التجسّسية، وأحصنة طروادة، وما شابهها من تهديدات.
- **البرمجيات المسجّلة** – نقيض البرمجيات المجانية والمفتوحة المصدر. هذه التطبيقات هي عادةً تجارية ولكن تتوافر أحياناً بصورة مجانية وفق رخصة خاضعة لشروط.
- **برنامج كوبيان للنسخ الاحتياطي** – أداة مجانية ومفتوحة المصدر للنسخ الاحتياطي. اتّخذت آخر إصدارات كوبيان شكل برمجية مجانية ذات مصادر مغلقة، فيما صدرت النسخ السابقة منه على شكل برمجية مجانية ومفتوحة المصدر.
- **بطاقة السيم** – بطاقة صغيرة قابلة للإزالة يمكن إدخالها في الهاتف المحمول بهدف توفير خدمات إحدى شركات الهواتف المحمولة. يمكن لبطاقات السيم أيضاً أن تخزّن أرقام الهواتف والرسائل القصيرة.
- **بلوتوث** – مقياس مادي للاتصالات اللاسلكية يفيد في تبادل البيانات على مسافات قصيرة من الأجهزة الثابتة والمحمولة. يستخدم البلوتوث تقنيات الإرسال الإذاعية ذات الموجات القصيرة.
- **بيسفاير** – يتلقى المشتركون في هذه الخدمة المجانية رسائل إلكترونية تتضمّن لائحةً محدثةً عن الخوادم الوكيلة، التي يمكن استخدامها لتجاوز رقابة الإنترنت.
- **التحايل** – تجاوز فلاتر الإنترنت للوصول إلى المواقع المحجوبة وغيرها من خدمات الإنترنت.
- **التراسل الفوري الآمن** – وظيفة إضافية للتشفير ضمن برنامج بدجن للرسائل الفورية.
- **تروكريبت** – أداة للتشفير من البرمجيات المجانية والمفتوحة المصدر تسمح لك بتخزين المعلومات الحساسة على نحوٍ آمن.
- **التصيد** – تصميم مواقع إلكترونية مزيّفة أو بريد إلكتروني مزيّف لتضليل مستخدمي الإنترنت وحضّهم على التفاعل مع المحتوى. يُستخدم في أغلب الأحيان من أجل الاستيلاء على كلمات السر والبيانات المالية.
- **التصيد بالحربة** – عملية تصميم موقع أو بريد إلكتروني مزيّف

بحيث يبدو حقيقياً بالنسبة إلى فردٍ معيّن أو مجموعة صغيرة.

- **تطبيقات جافا** – برامج صغيرة تجري تحت أنظمة تشغيلية عدة وذات برامج متعارضة. تستخدم في أغلب الأحيان لتوفير وظائف محسّنة ضمن صفحات الويب.
- **التطبيقات المحمولة** – البرامج التي تشغّل من جهاز محمول كذاكرة فلاش أو شريحة الذاكرة، ولا يُشترَط تثبيتها بموجب نظام تشغيل الكمبيوتر الشخصي.
- **التشفير** – هي طريقة تُستخدم فيها الرياضيات الذكية لتشفير المعلومات أو مزجها، بحيث لا يفكّ الشيفرة ويقرأ محتواها إلا من كان يملك كلمة السر أو مفتاح الشيفرة مثلاً.
- **التعمية بالإخفاء** – الوسيلة المعتمدة لإخفاء المعلومات الحساسة بحيث تبدو مختلفة، لعدم لفت الانتباه غير المرغوب إليها.
- **التهديد المادي** – في هذا السياق، أي تهديد يطال معلوماتك الحسّاسة، ويسفر عن وصول أشخاص آخرين بشكل مباشر إلى تجهيزات الكمبيوتر الخاصة بك، أو عن أي مخاطر مادية أخرى، كالكسر، أو الحوادث أو الكوارث الطبيعية.
- **تور** – أداة لإخفاء الهوية تسمح لك بتجاوز الرقابة على الإنترنت وإخفاء المواقع الإلكترونية وخدمات الإنترنت التي تزورها عن أي شخص قد يتولى مراقبة الاتصال بالإنترنت، مع إخفاء الموقع الخاص بك من هذه المواقع الإلكترونية.
- **التوقيع الرقمي**- إستخدام التشفير بطريقة تثبت إرسال ملف معيّن أو رسالة معيّنة من قبل الشخص الذي يدّعي إرسالها.
- **ثندربرد** – برنامج بريد إلكتروني من البرمجيات المجانية والمفتوحة المصدر يتضمّن عدداً من الخصائص الأمنية بما في ذلك الدعم لإضافة تشفير «إينيغمايل».
- **جدار النار** – أداة تحمي الكمبيوتر من وسائل الاتصال غير الموثوق بها إلى أو من الشبكات المحلية والإنترنت.
- **جدار النار كومودو** – أداة حماية من البرمجيات المجانية.
- **روابط البيانات دون الحمراء** – معيار للتواصل المادي اللاسلكي لتبادل البيانات عبر مسافات قصيرة باستخدام أشعة الضوء ما دون الحمراء، تستبدل روابط البيانات ما دون الحمراء بتقنية البلوتوث في الأجهزة الحديثة.
- **جنو/لينكس** – برنامج يشتغل بحسب البرمجيات المجانية والمفتوحة المصدر، ويوفّر بديلاً عن مايكروسوفت ويندوز.
- **جهاز التوجيه** – جهاز لربط الشبكات، يسمح لأجهزة الكمبيوتر الاتصال بشبكاتها المحلية، ومن خلال مختلف الشبكات المحلية الاتصال بالإنترنت. فتقوم الأزرار والمداخل والمحاور بمهام مشابهة، شأنها شأن نقاط الاتصال بالنسبة إلى أجهزة الكمبيوتر المجهّزة لاستخدامها.
- **الجهاز المساعد للذاكرة** – خدعة بسيطة تساعدك على تذكّر كلمات السر المعقدة.
- **راصد لوحة المفاتيح** – أحد أنواع البرمجيات التجسّسية تسجّل المفاتيح التي طبعتها على لوحة مفاتيح الحاسوب وتقوم بإرسال المعلومات إلى طرف ثالث. تستخدم هذه البرمجيات في أغلب الأحيان لسرقة البريد الإلكتروني وغير ذلك من كلمات السر.
- **ريفر** – أداة هجوم مصمّمة لتحطيم مفتاح التشفير المستخدَم في ظل الوضعية المحمية عبر شبكة واي فاي.
- **حارق الأقراص المدمجة** – محرّك أقراص مدمجة للكمبيوتر يمكن بواسطته كتابة البيانات على الأقراص المدمجة الفارغة. ومن الممكن لحارق أقراص الـ«دي في دي» أن يقوم بالمثل. أما معيد الكتابة على الأقراص المدمجة وأقراص الـ«دي في دي» فيمكنه حذف المعلومات وإعادة كتابتها غير مرّة على معيد الكتابة نفسه.
- **الخادم** – كمبيوتر يبقى متصلاً بالإنترنت بهدف توفير بعض الخدمات كاستضافة صفحة على الإنترنت أو إرسال أو استقبال البريد الإلكتروني إلى أجهزة كمبيوتر أخرى.
- **خادم وكيل** – خدمة وسيطة تسمح بتمرير بعض أو جميع أشكال التواصل عبر الإنترنت، ويمكن استخدامها لتجاوز الرقابة على الإنترنت. يمكن أن يكون خادم بروكسي عاماً أو قد يكون بإمكانك تسجيل الدخول للوصول إليه بواسطة اسم مستخدم أو كلمة سر. بعض الخوادم الوكيلة تتسم بالأمان، ما يعني أنها تستخدم التشفير لحماية خصوصية المعلومات التي تمرّ بين جهاز الكمبيوتر وخدمات الإنترنت التي تتصل بها من خلال هذا الخادم.
- **رايز أب** – خدمة بريد إلكتروني يشغّله الناشطون تلبيةً لأغراضهم، ويمكن الوصول إليه بأمان إما من خلال البريد الإلكتروني أو باستخدام برنامج عميل للبريد الإلكتروني الضيف مثل موزيلا ثندربيرد.
- **رمز المصدر** – الرمز الكامن، الذي يكتبه واضعو برامج الكمبيوتر الذي يسمح بابتكار البرمجيات. إنّ رمز المصدر الخاص بأداة معينة يكشف عن طريقة عملها وما إذا كانت غير آمنة أو خبيثة.
- **سبايبوت** – أداة مجانية لمكافحة البرمجيات الخبيثة، تمسح وتزيل وتساعد في حماية الكمبيوتر من البرمجيات التجسّسية.
- **سكايب** – أداة مجانية لنقل الصوت عبر بروتوكول الإنترنت، تتيح لك التحدث مع سائر مستخدمي سكايب مجاناً والاتصال بأرقام الهاتف لقاء رسم معين. يؤكّد مطوّرو هذه الخدمة أنّ المكالمات بين مستخدمي سكايب مشفّرة من جانبٍ لآخر.
- **سياسة الأمن** - وثيقة خطية تصف كيف يمكن لمنظمتك أن تحمي نفسها من تهديدات مختلفة، وتتضمّن لائحة بالخطوات التي يقتضي اتخاذها في حال وقوع حالات طارئة.

- **سيكلينر** – أداة مجانية تزيل الملفات المؤقتة والآثار الحساسة على محرّك القرص الصلب، ببرامج استخدمتها مؤخراً وبنظام تشغيل «ويندوز» نفسه.
- **شهادة أمنية** – هي وسيلة تتيح للمواقع الإلكترونية الآمنة وغيرها من خدمات الإنترنت أن تثبت عن طريق التشفير أنها صاحبة الهوية المزعومة. ولكن، ليتمكّن متصفّحك من قبول الشهادة الأمنية كشهادة صالحة، يجب أن تحصل خدمة الإنترنت على توقيع رقمي من منظمة موثوق بها لقاء مبلغ من المال. وبما أنّ هذا التدبير يرتّب على مشغّلي الخدمات كلفة لا رغبة أو طاقة لهم على تحمّلها، فقد ترصد أحياناً وجود خلل في شهادة أمنية عند زيارة خدمة صالحة.
- **طبقة المنافذ الآمنة** – تكنولوجيا تتيح لك المحافظة على اتصال آمن ومشفّر بين جهاز الكمبيوتر الخاص بك وبعض المواقع الإلكترونية وخدمات الإنترنت التي تستخدمها. عندما تتصل بأحد المواقع الإلكترونية من خلال طبقة المنافذ الآمنة، يبدأ عنوان الموقع الإلكتروني بـ«إتش تي تي بي آس» عوضاً عن «إتش تي تي بي».
- **عنوان بروتوكول الإنترنت (عنوان أي بي)** – رمز خاص يعرّف بجهاز الكمبيوتر الخاص بك عند اتصاله بالإنترنت.
- **عنوان ماك** – عنوان التحكّم بالوصول إلى الإعلام هو عبارة عن رقم تعريف فريد يرتبط بأجهزة الكمبيوتر الفردية، والهواتف الذكية، وما شابهها من أجهزة. وفيما تكون هذه العناوين مشفّرةً في الجهاز، يُتاح للمستخدمين تزييف عنوان ماك وبالتالي إبرازه على آلة أخرى.
- **قاعدة بيانات كلمة السر الآمنة** – أداة يمكنها تشفير وتخزين كلمات السر الخاصة بك باستخدام كلمة سر رئيسية واحدة.
- **فايرشيب** – تطبيق معروف ملحق بمتصفّح فايرفوكس، طوّره إريك باتلر ويتيح للمستخدمين اختراق الجلسات المفتوحة لعديد من المواقع الإلكترونية الشائعة الاستعمال عبر شبكات الاتصال غير المشفّرة.
- **فايرفوكس** – متصفّح معروف لشبكة الإنترنت يوفّر بديلاً عن متصفّح مايكروسوفت إنترنت إكسبلورر.
- **فلترة عناوين ماك** – إنّ وسيلة التحكم بشبكتك من خلال عناوين ماك الخاصة بالأجهزة الفردية لا تشفّر أو، بشكل آخر، تحمي البيانات المتبادلة بين الكمبيوتر وجهاز التوجيه.
- **القائمة السوداء** – قائمة بالمواقع الإلكترونية وغيرها من خدمات الإنترنت المحجوبة التي لا يمكن الوصول إليها بسبب سياسة الخصوصية المقيّدة.
- **القرص المدمج الحي** – قرص مدمج يتيح لجهاز الكمبيوتر تشغيل نظام مختلف بشكلٍ مؤقت.
- **الكابل الأمني** – كابل للقفل يمكن استخدامه لحفظ أمن الحاسوب المحمول أو غيره من التجهيزات، بما في ذلك المحرك الصلب وبعض أجهزة الكمبيوتر المثّبتة إلى جدار أو مكتب، منعاً لإزالته.
- **كلام وين** – برمجية مجانية ومفتوحة المصدر من ويندوز لمكافحة الفيروسات.
- **كي باس**- برمجية مجانية على شكل قاعدة بيانات من كلمات السر الآمنة.
- **المخترق** – يُقصَد به في هذا السياق، كل من يرتكب جريمة حاسوبية، محاولاً الوصول إلى معلوماتك الحساسة أو الاستيلاء على حاسوبك عن بعد.
- **مزود خدمة الإنترنت** – الشركة أو المنظمة التي تزوّدك برابط أساسي يصلك بشبكة الإنترنت. لكنّ عدة حكومات تُحكِم سيطرتها على الإنترنت بممارسة أعمال الفلترة والمراقبة مثلاً، عن طريق مزوّدي خدمات الإنترنت العاملين ضمن بلدانها.
- **ملف المقايضة** – ملف على الكمبيوتر تحفظ فيه المعلومات، والبعض منها معلومات حساسة، من وقتٍ لآخر من أجل تحسين الأداء.
- **ملفات الكوكيز** – ملفات صغيرة يحفظها المتصفّح على الكمبيوتر ويمكن استخدامها لحفظ المعلومات أو لتعريفك على موقع إلكتروني معيّن.
- **النظام الأساسي للمدخلات/المخرجات** – المستوى الأول والأكثر عمقاً من البرامج على الكمبيوتر. يتيح لك هذا النظام تحديد الخيارات التفضيلية المتقدمة الخاصة بمعدات الكمبيوتر، بما في ذلك كلمة السر المناسبة للإقلاع.
- **نظام اسم النطاق** – شبكة من الخوادم التي يطلق عليها أحياناً اسم السجل أو دفتر الهاتف الخاص بالإنترنت. يترجم أسماء النطاقات بشكل عناوين بروتوكول الإنترنت.
- **نظام تحديد المواقع العالمي** – نظام تصفّح فضائي عالمي يحدّد المعلومات الخاصة بالمكان والزمان في جميع الأحوال الجوية وفي أي مكان على الكرة الأرضية أو على مقربة منها، حيث لا يكون هناك تقريباً أي عائق أمام رؤية السماء.
- **نوسكريبت** – تطبيق أمني ملحق بمتصفّح فايرفوكس، يحميك من البرمجيات الخبيثة التي قد تكون موجودة في صفحات الويب غير المألوفة.

# بعض الروابط الإلكترونية حول الأمن الرقمي

## ١. تحكّم بأمن حاسوبك

### المبادئ الأساسية

secunia.com/products/consumer/psi/download_psi/

isc.sans.edu/

isc.sans.edu/survivaltime.html

security.ngoinabox.org/en/comodofirewall_main

alternativeto.net/

www.osalt.com/

housecall.trendmicro.com/

www.bitdefender.com/scanner/online/free.html

www.microsoft.com/security/scanner/en-us/default.aspx

### بعض التقنيات المتطورة

go.microsoft.com/?linkid=9741395

go.microsoft.com/?linkid=9743275

www.grc.com/x/ne.dll?bh0bkyd2

www.microsoft.com/windows/virtual-pc/default.aspx

www.virtualbox.org/

en.wikipedia.org/wiki/Virtual_machines

windows.microsoft.com/en-US/windows7/products/features/backup-and-restore

www.todo-backup.com/

security.ngoinabox.org/en/chapter-1

security.ngoinabox.org/en/avast_main

security.ngoinabox.org/en/spybot_main

security.ngoinabox.org/en/comodofirewall_main

survival.tacticaltech.org/computer

www.google.com/goodtoknow/online-safety/phishing/

www.google.com/goodtoknow/online-safety/malware/

### القائمة المرجعية الأساسية للحماية

support.microsoft.com/kb/306525

http://support.microsoft.com/kb/306525

security.ngoinabox.org/en/comodofirewall_main

## ٢. حماية بياناتك

### المبادئ الأساسية

www.splashdata.com/press/PR111121.htm

www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

security.ngoinabox.org/en/chapter-3

keepass.info/download.html

security.ngoinabox.org/en/using_keepass

www.truecrypt.org/download

www.truecrypt.org/docs/?s=tutorial

windows.microsoft.com/en-US/windows-vista/File-sharing-essentials

securityinabox.org/en/truecrypt_main

windows.microsoft.com/en-US/windows7/products/features/backup-and-restore

www.cobiansoft.com/index.htm

security.ngoinabox.org/en/cobian_howtobackup

### بعض التقنيات المتطورة

www.truecrypt.org/docs/?s=tutorial

security.ngoinabox.org/en/truecrypt_main

www.todo-backup.com/download/

security.ngoinabox.org/en/chapter-3

security.ngoinabox.org/en/keepass_main

security.ngoinabox.org/en/chapter-4

security.ngoinabox.org/en/truecrypt_main

security.ngoinabox.org/en/cobian_main

## ٣. البريد الإلكتروني الآمن

### المبادئ الأساسية

windows.microsoft.com/en-us/hotmail/security?T1=t2

support.mozillamessaging.com/en-US/kb/manual-account-configuration?s=configure+ssl&as=s

www.ehow.com/how_8223091_turn-off-images-gmail.html

office.microsoft.com/en-us/outlook-help/block-or-unblock-automatic-picture-downloads-in-email-messages-

HP010355038.aspx

support.google.com/accounts/bin/answer.py?hl=en&answer=180744

www.microsoft.com/security/scanner/en-us/default.aspx

www.comodo.com/business-security/network-protection/cleaning_essentials.php?track=2745&key5sk1=87df603f01aaa e03acc1a bf058bb1bac233a524e&key5sk2=2128&key5sk3=1334043298000&key5sk10=2005&key5sk11=133404329800 0&key5sk12=-

2745 &key5sk13=1334043308000&key6sk1=&key6sk2=CH1801025162&key6sk3=7&key6sk4=en-us&key6sk5=TH&key6sk6

.w.comodo.com%252F&key6sk8=112202&key6sk9=19201080&key6sk10=true&k ey6sk11=298cde2eecbc5eb69d3ae735 aa2be8f85261fba7&key7sk1=72&key1sk1=dt&key1sk2=https%253A%252F%252Fwww. comodo.com%252F

## ٤. التصفّح الآمن

### المبادئ الأساسية

addons.mozilla.org/EN-US/firefox/addon/noscript/?src=cb-dl-mostpopular

www.eff.org/https-everywhere

addons.mozilla.org/EN-US/firefox/addon/https-finder/?src=ss

addons.mozilla.org/EN-US/firefox/addon/betterprivacy/?src=search

addons.mozilla.org/EN-US/firefox/addon/wot-safe-browsing-tool/?src=search

addons.mozilla.org/EN-US/firefox/addon/perspectives/?src=search

addons.mozilla.org/en-US/firefox/extensions/privacy-security/

www.eff.org/https-everywhere

chrome.google.com/webstore/detail/lnppfgdnjafeikakadfopejdpglpiahn?utm_source=chrome-ntp-icon

chrome.google.com/webstore/detail/bhmmomiinigofkjcapegjjndpbikblnp?utm_source=chrome-ntp-iconwe.riseup.net/

riseuphelp+en/openvpn-windows

hotspotshield.com/

www.metageek.net/products/inssider/

www.microsoft.com/security/scanner/en-us/default.aspx

www.comodo.com/business-security/network-protection/cleaning_essentials.php?key5sk1=5ed0a3d8f28d25396377d3 d33ba64

68b64cea749&key5sk2=2128&key5sk3=1338810504000&key5sk4=2720&key5sk5=1338810511000&key5sk6=2720&key5 sk7=1338810532000&key6sk1=&key6sk2=C

www.mobileactive.org/howtos/user-guide-to-orbot

### بعض التقنيات المتطورة

208.69.38.205/

developers.google.com/speed/public-dns/docs/using

onorobot.org/en/episode_4

security.ngoinabox.org/en/chapter-8

www.howtobypassinternetcensorship.org/

en.rsf.org/spip.php?page=article&id_article=33844

en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html

www.google.com/goodtoknow/online-safety/safe-networks/

www.eff.org/wp/blog-safely

www.eff.org/https-everywhere

en.cship.org/wiki/Main_Page addons.mozilla.org/en-US/firefox/addon/noscript/?src=ss

addons.mozilla.org/en-US/firefox/addon/wot-safe-browsing-tool/?src=search

addons.mozilla.org/en-US/firefox/addon/perspectives/?src=search

addons.mozilla.org/en-US/firefox/addon/https-finder/?src=search

advocacy.globalvoicesonline.org/projects/guide/

www.mobileactive.org/howtos/mobile-anonymity

www.mobileactive.org/howtos/user-guide-to-orbot

## ٥. شبكة واي فاي آمنة

### المبادئ الأساسية

www.routerpasswords.com/

security.ngoinabox.org/en/chapter-3

security.ngoinabox.org/en/chapter-3

### بعض التقنيات المتطورة

www.wikihow.com/Find-the-MAC-Address-of-Your-Computer

## ٦. الاتصال الآمن عبر الدردشة والمكالمات الصوتية

### المبادئ الأساسية

www.pidgin.im/download/windows/

www.cypherpunks.ca/otr/index.php#downloads

security.ngoinabox.org/en/using_pidgin

portableapps.com/apps/internet/pidgin_portable

sourceforge.net/projects/portableapps/files/Pidgin-OTR%20Portable/Pidgin-OTR%20Portable%203.2%20Rev%202/

security.ngoinabox.org/en/portable_security

### بعض التقنيات المتطورة

trac.torproject.org/projects/tor/wiki/doc/TorifyHOWTO/InstantMessaging

### مصادر ومراجع إضافية

security.ngoinabox.org/en/chapter-7
security.ngoinabox.org/en/pidgin_main
survival.tacticaltech.org/computer
survival.tacticaltech.org/mobile
security.ngoinabox.org/en/portable_security
www.eff.org/https-everywhere
www.mobileactive.org/howtos/off-the-record-messaging
blogs.skype.com/security/

## ٧. رصد مشاكل الوصول ومعالجتها

### المبادئ الأساسية

www.howtobypassinternetcensorship.org/
tails.boum.org/
openvpn.net/index.php/open-source/overview.html
www.torproject.org/download/download.html.en
support.google.com/news/bin/answerpy?hl=en&answer=1146405
support.google.com/reader/bin/answerpy?hl=en&answer=113517
www.icurrent.com/about
www.torproject.org/projects/torbrowser.html.en
tails.boum.org/
sourceforge.net/projects/ovpnp/files/
security.ngoinabox.org/en/portable_security

### بعض التقنيات المتطورة

www.howtobypassinternetcensorship.org/
www.howtobypassinternetcensorship.org/files/bypass-internet-censorship-quickstart.pdf
flossmanuals.net/bypassing-censorship/ch010_simple-tricks/
www.howtobypassinternetcensorship.org/files/bypassing-censorship.pdf
security.ngoinabox.org/en/chapter-8
en.rsf.org/spip.php?page=article&id_article=33844
www.eff.org/wp/blog-safely
advocacy.globalvoicesonline.org/2011/06/21/anonymous-blogging-with-wordpress-and-tor-guide-in-spanish/
en.cship.org/wiki/Main_Page
www.mobileactive.org/howtos/mobile-anonymity

## ٨. التشبيك والتدوين الآمنان عبر مواقع التواصل الاجتماعي

### المبادئ الأساسية

support.twitter.com/groups/31-twitter-basics/topics/113-online-safety/articles/481955-how-to-enable-https

security.ngoinabox.org/en/chapter_3_1

www.torproject.org/projects/torbrowser.html.en

www.facebook.com/note.php?note_id=10150172618258920&comments

support.google.com/accounts/bin/answer.py?hl=en&answer=180744

en.rsf.org/spip.php?page=article&id_article=33844

www.eff.org/wp/blog-safely

security.ngoinabox.org/en/chapter-10

dev.mobileactive.org/howtos/safer-facebook

mobileactive.org/howtos/safer-twitter

### مصادر ومراجع إضافية

security.ngoinabox.org/en/chapter-10

security.ngoinabox.org/en/portable_security

www.facebook.com/safety/tools/

## ٩. أحذف بياناتك كلياً

### المبادئ الأساسية

www.piriform.com/recuva/download/standard

eraser.heidi.ie/download.php

security.ngoinabox.org/en/eraser_main

www.piriform.com/ccleaner/download/standard

security.ngoinabox.org/en/settingup_ccleaner

portableapps.com/apps/utilities/eraser_portable

www.piriform.com/ccleaner/download/portable

www.piriform.com/recuva/download/portable

security.ngoinabox.org/en/portable_security

### مصادر ومراجع إضافية

onorobot.org/en/episode_1

security.ngoinabox.org/en/chapter-5

security.ngoinabox.org/en/chapter-6

security.ngoinabox.org/en/recuva_main

security.ngoinabox.org/en/eraser_portable

www.mobileactive.org/howtos/mobile-backups-data-deletion-remote-wipe

## ١٠. مراعاة مخاطر تبادل البيانات عبر الإنترنت

### المبادئ الأساسية

www.dropbox.com/

drive.google.com/

portableapps.com/apps/internet/firefox_portable

www.torproject.org/

leakdirectory.org/index.php/Leak_Site_Directory

### مصادر ومراجع إضافية

drawingbynumbers.org/what-can-you-do-about-these-risks

en.rsf.org/spip.php?page=article&id_article=33844

www.eff.org/wp/blog-safely

advocacy.globalvoicesonline.org/projects/guide/

security.ngoinabox.org/en/portable_security

## ١١. الهواتف الجوالة الآمنة

### المبادئ الأساسية

safermobile.org/resource/mobile-security-survival-guide-for-journalists/#mobile-network-awareness-title

security.ngoinabox.org/en/chapter_9_1

www.mylookout.com/news-mobile-security/lookout-lost-phones-30-billion

security.ngoinabox.org/en/chapter-3

www.truecrypt.org/

securityinabox.org/en/truecrypt_main

itunes.apple.com/us/app/wickr-secure-im-multimedia/id528962154?mt=8

mobileactive.org/mobile-tools/gibberbot

guardianproject.info/apps/gibber/

www.mobileactive.org/howtos/user-guide-to-orbot

dev.mobileactive.org/howtos/safer-facebook

mobileactive.org/howtos/safer-twitter

code.google.com/p/droidwall/

mobileactive.org/howtos/mobile-surveillance-primer

securityinabox.org/en/chapter_9_2_1

### مصادر ومراجع إضافية

www.mobileactive.org/howtos/user-guide-to-orbot

mobileactive.org/howtos/safer-facebook

mobileactive.org/howtos/safer-twitter

www.mobileactive.org/howtos/mobile-backups-data-deletion-remote-wipe

securityinabox.org/en/chapter-9

## ١٢. تطبيق معايير "السلامة أولاً" على التقنيات الأخرى

### المبادئ الأساسية

mobileactive.org/howtos/safer-photos-how-remove-location-information-mobile-images

www.irfanview.com/plugins.htm

smallworldnews.tv/guide/

guardianproject.info/apps/securecam/

market.android.com/details?id=org.witness.sscphase1&feature=search_result

## مسرد المصطلحات

creativecommons.org/licenses/by-sa/3.0/

security.ngoinabox.org

## ملاحظات

## ملاحظات

www.speaksafe.internews.org

Internews
Local voices. Global change.