حافظ على أمان أجهزتك

يقدم هذا المصدر بعض الخطوات العملية الأولى التي تساعدك على تأمين أجهزتك ضد الأشكال الشائعة لتتبع الأجهزة، كما يحتوي على إجراءات مثل إيقاف تشغيل تقنيتي Bluetooth وWiFi، وإيقاف تشغيل مشاركة الموقع، وإعادة تسمية جهازك، والتحقق من وجود برامج تجسس، والتحقق من أذونات التطبيقات، وإجراء إعادة ضبط المصنع.

هذه نصائح عامة حول كيفية الحفاظ على أمان أجهزتك. قد تختلف الخطوات المحددة باختلاف الأجهزة وقد تتغير بمرور الوقت.

على أجهزة iPhone وiPad، يمكنك عادةً العثور على الإعداد من خلال الضغط على "الإعدادات" على الشاشة الرئيسية، ثم السحب لأسفل لإظهار شريط البحث. (للحصول على المساعدة، يُرجى الاطلاع على .(http://tiny.cc/iphonesearch

على أجهزة Android، اسحب لأعلى من الشاشة الرئيسية: سيظهر شريط بحث برسالة "ابحث في هاتفك والمزيد". اكتب الإعداد الذي تبحث عنه في شريط البحث.

إيقاف تشغيل Bluetooth وWiFi في حال عدم استخدامهما

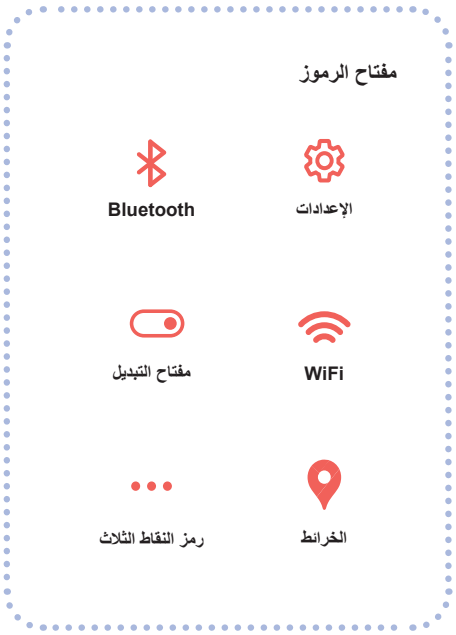
تجعل تقنيتا Bluetooth وWiFi جهازك مرئيًا للأجهزة الأخرى. إن لم تكن بحاجة إلى استخدامهما، فقم بإيقاف تشغيلهما، وذلك بالانتقال إلى **الإعدادات** أو بالضغط على رمزي **Bluetooth** و**WiFi**.

يمكنك أيضًا الانتقال إلى إعدادات Bluetooth (**الإعدادات** > **Bluetooth**) والبحث عن أي أجهزة مقترنة بهاتفك. إذا كان هناك أي جهاز مقترن بهاتفك لا تعرفه، فقم بإلغاء إقرانه.

إيقاف تشغيل مشاركة الموقع

لا تزال ميزة مشاركة الموقع تعمل حتى بعد إغلاق هاتفك وكذلك عدد من التطبيقات مثل تطبيق "العثور على هاتفي"، لذلك عليك إيقاف تشغيلها من الإعدادات. على أجهزة iPhone، افتح **الإعدادات** > الخصوصية > خدمات الموقع، أو ابحث عن "خدمات الموقع"، وقم بإيقاف تشغيل مشاركة الموقع.

على أجهزة Android، افتح تطبيق **الخرائط**، واضغط على صورة ملفك الشخصي ثم مشاركة الموقع. اضغط على صورة الملف الشخصي لأي شخص لا ينبغي *له* رؤية موقعك، ثم اضغط على "إيقاف".



حافظ على أمان أجهزتك

إعادة تسمية أجهزتك

حتى لو لم تغيّر اسم هاتفك مطلقًا، فلا يزال يحمل اسمًا يحدده. على أجهزة iPhone، اضغط على **الإعدادات** > "عام" > "حول" > "الاسم"، أو ابحث عن "الاسم"، ثم أدخل اسمًا جديدًا واضغط على "تم".

على أجهزة Android، اضغط على **الإعدادات** > "حول الهاتف" > "اسم الجهاز"، أو ابحث عن "الاسم"، ثم أدخل الاسم الجديد واضغط على "موافق".

التحقق من وجود برامج تجسس

"برامج التجسس" تعني التطبيقات التي تسمح لشخص آخر بالتجسس على جهازك. تحقق لمعرفة ما إذا كان هاتفك يحتوي على أي تطبيقات غير معروفة بالنسبة لك. على أجهزة iPhone، اسحب لليمين على الشاشة الرئيسية حتى تظهر لك "مكتبة التطبيقات".

اضغط على مربع البحث الموجود أعلى الشاشة، ثم قم بالتمرير عبر قائمة التطبيقات وإزالة أي تطبيق لا تعرفه.

على أجهزة Android، انتقل إلى **الإعدادات** > "التطبيقات والإشعارات" > "عرض جميع التطبيقات"، أو ابحث عن "التطبيقات".

هناك أيضًا تطبيقات يمكنك استخدامها لهذا الغرض، مثل *Certo* و*Incognito*، والتي تُجري فحصًا لأجهزتك بحثًا عن برامج التجسس، ولكن يجب أن تعلم أن هناك دائمًا احتمال أن تظل برامج التجسس موجودة على هاتفك.

التحقق من أذونات التطبيقات

يمكنك أيضًا عدم السماح لأي تطبيق بجمع أو مشاركة أي بيانات تخصّك مثل موقعك. على أجهزة iPhone، اضغط على **النقاط الثلاث** > "الخصوصية والأمان" > "تقرير خصوصية التطبيق"، لمعرفة البيانات التي يشاركها كل تطبيق، أو ابحث عن "تقرير الخصوصية". اضغط على كل تطبيق لتغيير الإعدادات.

مفتاح الرموز


الإعدادات

رمز النقاط الثلاث

مفتاح التبديل

على أجهزة Android، قم بتنزيل تطبيق *DuckDuckGo* من متجر Play ثم افتحه. اضغط على **الإعدادات** > "حماية تتبع التطبيقات"، ثم قم بتحريك **مفتاح التبديل** إلى اليمين.

إجراء إعادة ضبط المصنع

إذا نفّذْت جميع الإجراءات الأخرى ولا تزال تظن أن هناك من يتعقب هاتفك، فيمكنك إجراء إعادة ضبط المصنع. ولكن هذا الإجراء سيؤدي إلى حذف جميع البيانات، بما فيها أي دليل موجود على هاتفك. إن أجريت إعادة ضبط المصنع لهاتفك، فلن تتمكن من استعادة البيانات مرة أخرى من نسخة احتياطية محفوظة، لأنك بذلك قد تُعيد تحميل كل ما كان يتتبعك، لذا عليك أن تبدأ من جديد تمامًا.

إذا كنت متأكدًا من رغبتك في القيام بهذا الإجراء، على أجهزة iPhone، فيمكنك الضغط على **الإعدادات** > "عام" > "نقل أو إعادة تعيين iPhone"، ثم "مسح جميع المحتويات والإعدادات". يمكنك أيضًا البحث عن "إعادة تعيين" للعثور على هذا الإعداد.

إذا كان لديك جهاز iPhone، فيمكنك أيضًا تشغيل "نمط المنع"، الذي يحميك من معظم أنواع برامج التجسس. كما أنه يحدُّ من معدل استخدامك لتطبيقات مثل "فيس تايم" و"سفاري". راجع https://support.apple.com/en-ca/HT212650 لمعرفة المزيد حول "نمط المنع".

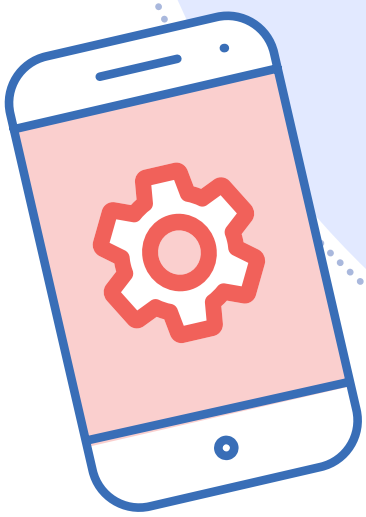
على أجهزة Android، ابدأ بالانتقال إلى **الإعدادات**، ثم ابحث عن "إعادة ضبط". ابحث عن نتيجة مثل "إعادة ضبط المصنع" أو "مسح جميع البيانات" واضغط عليها.

Financial contribution from

Public Health Agency of Canada
Agence de la santé publique du Canada

احرص على التواصل بشكل آمن

يقدّم هذا المصدر بعض الخطوات العملية الأولى للتواصل بأمان عبر الإنترنت لتجنب الأشكال الشائعة للتتبع عبر الإنترنت، كما يحتوي على إجراءات، مثل تسجيل الخروج من الحساب وإيقاف تشغيل مشاركة الموقع ومراجعة إعدادات الخصوصية وتغيير كلمة السر.



هذه نصائح عامة حول كيفية الحفاظ على أمان أجهزتك. قد تختلف الخطوات المحددة باختلاف الأجهزة وقد تتغير بمرور الوقت.

على أجهزة iPhone وiPad، يمكنك عادةً العثور على الإعداد من خلال الضغط على "الإعدادات" على الشاشة الرئيسية، ثم السحب لأسفل لإظهار شريط البحث. (للحصول على المساعدة، يُرجى الاطلاع على http://tiny.cc/iphonesearch.).

على أجهزة Android، اسحب لأعلى من الشاشة الرئيسية: سيظهر شريط بحث برسالة "ابحث في هاتفك والمزيد". اكتب الإعداد الذي تبحث عنه في شريط البحث.

تسجيل الخروج من جميع الحسابات

ربما قمت بتسجيل الدخول إلى بعض التطبيقات على أكثر من جهاز واحد. إليك كيفية تسجيل الخروج من كل مكان على Facebook: اضغط على **النقاط الثلاث الأفقية** ثم **الإعدادات**، ثم "كلمة السر والأمان"، ثم "مركز الحسابات". اضغط على "كلمة السر والأمان" ثم "الأماكن التي سجلت الدخول منها".

سترى الآن جميع حساباتك على *Facebook* أو *Instagram* أو *WhatsApp*. اضغط على كل جهاز لمعرفة الأجهزة التي قمت بتسجيل الدخول إليها، ثم اضغط على "تسجيل الخروج" من كل جهاز ليس هاتفك.

احرص على التواصل بشكل آمن

إيقاف تشغيل مشاركة الموقع على مواقع التواصل الاجتماعي

يعد هذا إجراءً مهمًا إذا كنت تستخدم *Snapchat*، والذي يعرض موقعك على الخريطة. للقيام بذلك، افتح *Snapchat* واضغط على رمز ملفك الشخصي. بعد ذلك، اضغط على **النقاط الثلاث العمودية** في أعلى اليمين ثم مرّر لأسفل إلى قسم "من يستطيع...". إذا ضغطت على "رؤية موقعي"، فستظهر نافذة منبثقة برسالة "وضع الشبح". قم **بالتبديل** إلى "وضع التشغيل".

على *Facebook* أو *Instagram*، يمكنك إيقاف تشغيل الموقع من خلال الضغط على **الإعدادات** > "الخصوصية" > "خدمات الموقع" ثم الضغط على **مفتاح التبديل** المجاور له. تضع معظم الشبكات الاجتماعية الأخرى هذا الخيار في أماكن مماثلة ضمن إعدادات مثل "الخصوصية" أو "الأمان".

مراجعة إعدادات الخصوصية

تحتوي جميع حسابات شبكات التواصل الاجتماعي الخاصة بك على إعدادات الخصوصية، والتي يمكنك الوصول إليها عادةً عن طريق الضغط على **الإعدادات** ثم خيار مثل "الخصوصية" أو "الخصوصية والأمان" أو "الجمهور". تأكد من ضبط هذا الإعداد لعرض ما تنشره للأصدقاء فقط.

تغيير كلمات السر على حسابات التخزين السحابي

إذا كنت تستخدم أي وحدة تخزين سحابية لصورك أو مقاطع الفيديو الخاصة بك، مثل *iCloud* أو *Google Drive*، فتأكد من تغيير كلمة السر حتى لا يتمكن أي شخص آخر من الوصول إليها.

Financial contribution from

Public Health Agency of Canada | Agence de la santé publique du Canada

تصفّح بأمان

يقدّم هذا المصدر بعض الخطوات العملية الأولى للتصفّح بأمان عبر الإنترنت لتجنب الأشكال الشائعة للتتبع عبر الإنترنت، كما يحتوي على إجراءات مثل: استخدام متصفّحات تركز على الخصوصية والتصفّح الخاص/المتخفي ومسح السجل وتسجيل الدخول باستخدام عناوين بريد إلكتروني مجهولة وكلمات سر قوية.

هذه نصائح عامة حول كيفية الحفاظ على أمان أجهزتك.
قد تختلف الخطوات المحددة باختلاف الأجهزة وقد تتغير بمرور الوقت.

على أجهزة iPhone وiPad، يمكنك عادةً العثور على الإعداد من خلال الضغط على "الإعدادات" على الشاشة الرئيسية، ثم السحب لأسفل لإظهار شريط البحث. (للحصول على المساعدة، يُرجى الاطلاع على .(http://tiny.cc/iphonesearch

على أجهزة Android، اسحب لأعلى من الشاشة الرئيسية: سيظهر شريط بحث برسالة "ابحث في هاتفك والمزيد". اكتب الإعداد الذي تبحث عنه في شريط البحث.

استخدام متصفّح يركز على الخصوصية

توجد متصفّحات مصمّمة لمراعاة الخصوصية مثل *Firefox* و*DuckDuckGo*، لذا فهي تتعقبك بأقل قدر ممكن. حاول استخدام أحدها بدلًا من المتصفّح الذي يأتي مثبّتًا على جهازك.

التصفّح الخاص أو المتخفي

تحتوي معظم المتصفّحات على وضع **تصفّح خاص** أو **متخفي**. يمنع هذا الوضع المتصفّح نفسه من تسجيل المواقع التي زرتها، لكنه لا يمنع تلك المواقع (أو مزود خدمة الإنترنت لديك، أو التطبيقات الأخرى على جهازك) من تسجيل ما تفعله.

مفتاح الرموز

الإعدادات

وضع التصفّح الخاص أو المتخفي

تصفّح بأمان

مسح سجلك

ابحث عن "السجل". إذا كان لديك حساب *Google*، فيمكنك أيضًا مسح سجل *Google* و*YouTube* الخاص بك. انتقل إلى **myactivity.google.com** وقم بإيقاف تشغيل "نشاط الويب والتطبيقات" و"سجل المواقع" و"سجل YouTube".

لمسح سجل المتصفّح الخاص بك على "سفاري"، اضغط على **الإعدادات** ثم "سفاري" > "مسح سجل التاريخ وبيانات الموقع"، أو ابحث عن "بيانات مواقع الويب".

تسجيل الدخول باستخدام بريد إلكتروني مجهول

تتطلب العديد من مواقع الويب والخدمات تقديم عنوان بريد إلكتروني للتسجيل. إذا لم تكن بحاجة إلى النقر فوق رابط التحقق، فيمكنك استخدام عنوان بريد إلكتروني مزيف تم إنشاؤه على **Sharklasers.com**.

يمكنك أيضًا إنشاء عنوان *Protonmail* مجاني وخاص وآمن حتى لا تضطر إلى استخدام عنوان قد يتعرف عليه شخص آخر.

استخدام كلمات سر قوية

يمكنك إنشاء كلمة سر قوية من خلال البدء بعبارة سهلة التذكر (مثل "I like bananas") ثم تحويل بعض الحروف إلى أرقام أو أحرف (مثل العلامات النجمية أو علامات التعجب لتصبح !L1keBan@nas).

لكن لا تستخدم كلمة السر نفسها لحسابات مختلفة. من المهم بشكل خاص استخدام كلمة سر قوية مختلفة لحساب بريدك الإلكتروني الرئيسي، حيث سيتم إرسال رسائل البريد الإلكتروني الخاصة باسترداد الحساب هناك. يمكنك أيضًا استخدام مدير كلمات السر مثل *1Password*. إذا قمت بذلك، فتأكد من أن كلمة السر التي تستخدمها قوية ومختلفة عن جميع كلمات السر الأخرى.

Financial contribution from

Public Health Agency of Canada | Agence de la santé publique du Canada