Workshop 04 - Social Media and Online Safety

SLQ Wiki Fabrication Lab 2024/07/27 12:19

Workshop 04 – Social Media and Online Safety

هنا سوف:

1. نقوم بتأمين أجهزتك والربط والمتصفح والحسابات
2. نتعرف على الأحوال الخطرة
3. نفهم الخصوصية على الإنترنت

نقوم بتأمين أجهزتك

الكمبيوتر

* **قم بتثبيت البرامج المعروفة فقط.** قم بالبحث أولاً (خاصة إذا كانت البرامج مجانية). * **استخدم كلمات مرور آمنة** واقفل جهازك عند عدم استخدامه. * **لا تتركه دون رقابة في الأماكن العامة.** حتى لو تم قفله، يمكن سرقته. * **حافظ على تحديث البرامج** ـ تعمل تصحيحات الأمان على تقليل نقاط الضعف.

قم بتثبيت جدار حماية. إنه حاجز بين جهاز الكمبيوتر الخاص بك والآخرين. يمكنك رفض/السماح بمحاولات الدخول.

قم بتثبيت برامج مكافحة الفيروسات (**وبرامج مكافحة التجسس إذا لم تكن مدرجة بالفعل**). من أمثلة الفيروسات والبرامج الضارة:

- مسجلات المفاتيح Keyloggers (تسجل نقرات المفاتيح)
- رانسوم وير Ransomware (يحتجز نظامك أو تفاصيلك كرهينة)
- الديدان Worms (فيروسات تنسخ نفسها لإصابة الأجهزة الأخرى)

- أحصنة طروادة Trojan Horses (البرامج التي تضلل بشأن النوايا الخبيثة)
- الجذور الخفية Rootkits (توفر دخولاً غير مصرح به للنظام)

الهاتف

استخدم **كلمة مرور أو رقم تعريف شخصي أو بيانات مقاييس حيوية** لقفل جهازك عند عدم استخدامه. ضع في اعتبارك تشغيل خاصية قفل الجهاز بعد فترة زمنية محددة دون استخدام.

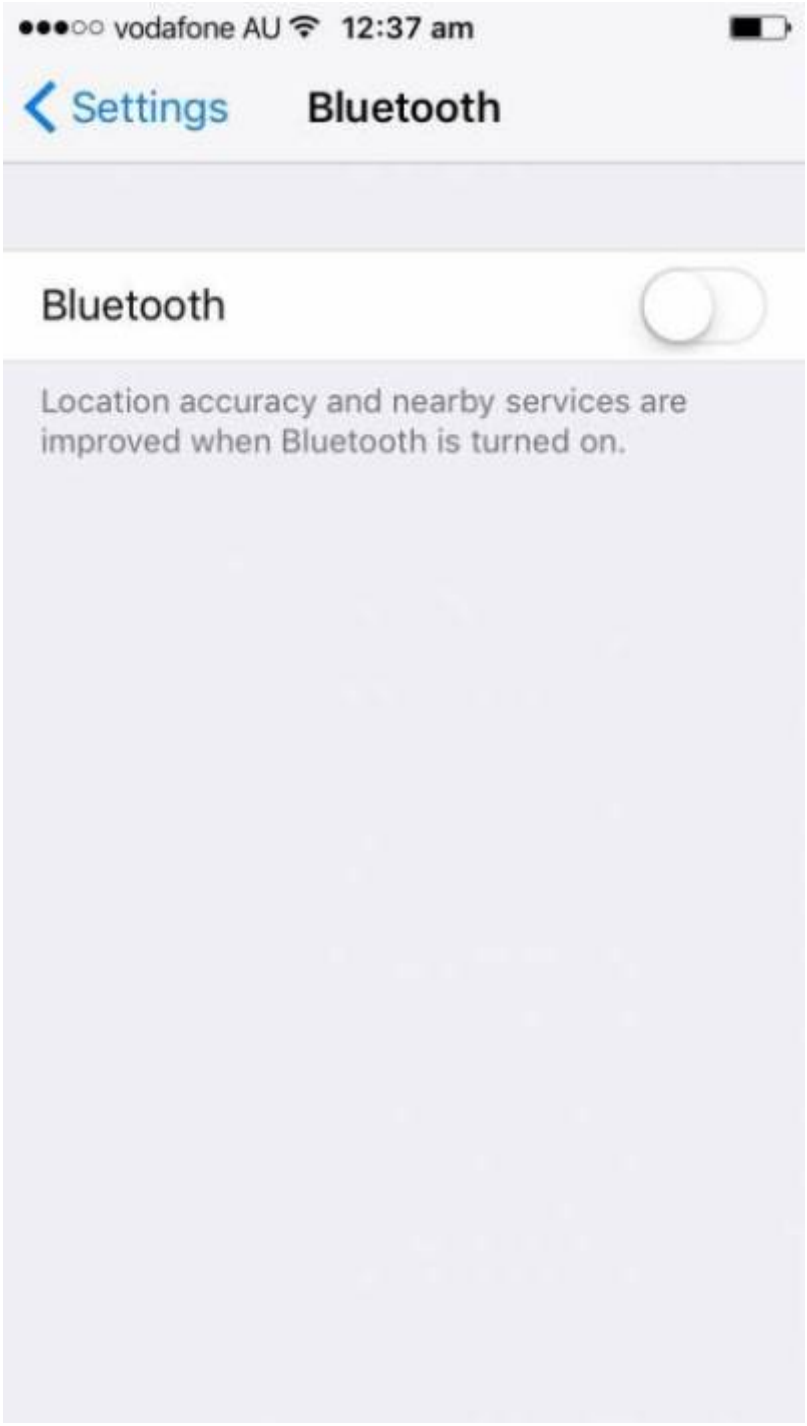
لا تتركه دون رقابة في الأماكن العامة. حتى لو تم قفله، يمكن سرقته. لا تقرضه للآخرين إلّا عند الحاجة، ولا تتركه بعيدًا عن عينيك إذا فعلت ذلك.

حافظ على تحديث البرامج ـ تعمل تصحيحات الأمان على تقليل نقاط الضعف.

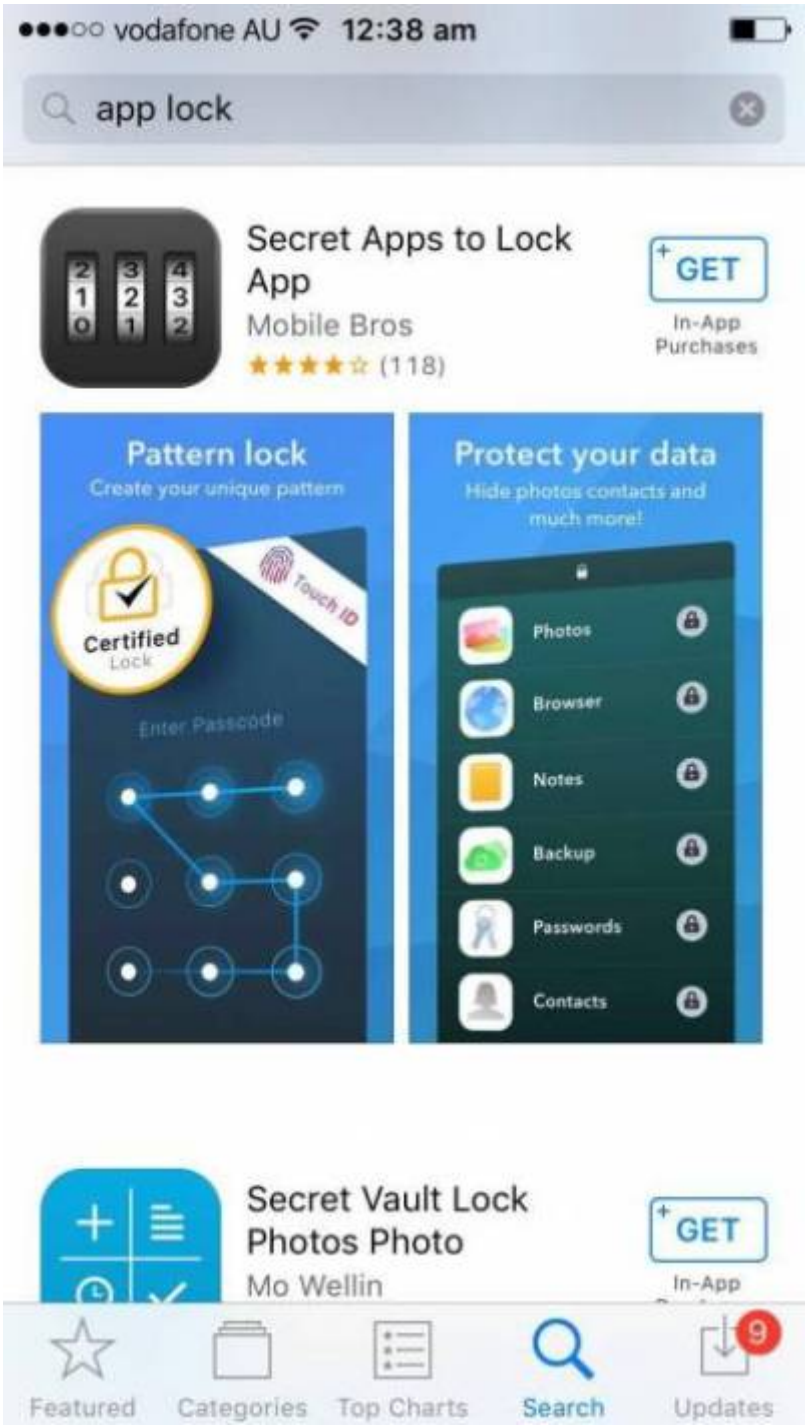
قم بتنزيل التطبيقات المعروفة من مصادر موثوقة، على سبيل المثال. Google Play.

قم بتثبيت برنامج أمان معروف مزود بقدرات مكافحة الفيروسات ومكافحة الخسارة.

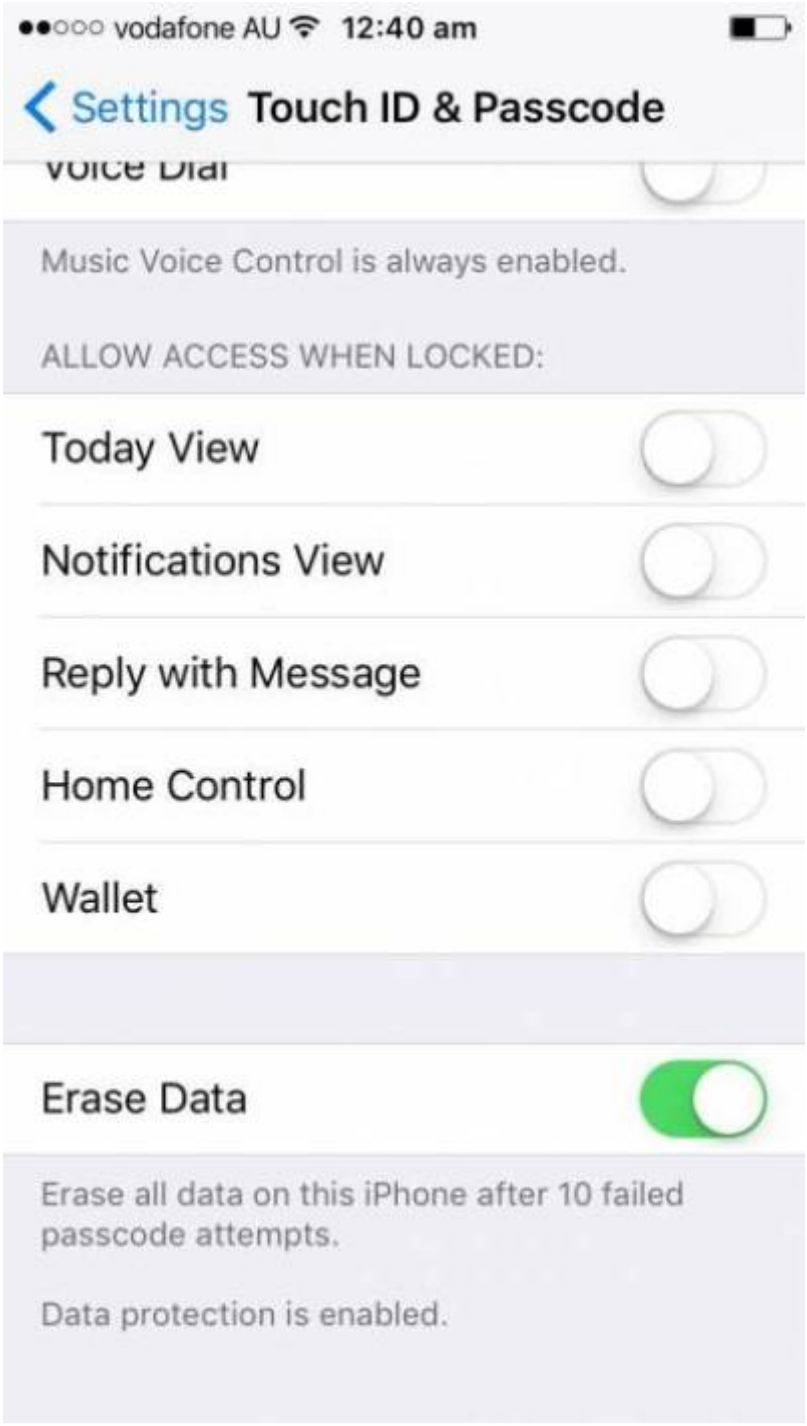
اجعل البلوتوث مغلقًا أو مخفيًا إذا لم يكن قيد الاستخدام.



فكر في تطبيقات قفل التطبيقات لحماية الدخول غير المؤمَّن للتطبيقات التي تحتوي على معلومات حساسة.



فكر في تشغيل خاصية القفل والمسح عن بُعد حتى تتمكن من قفل/مسح هاتفك من بعيد. يمكن للمسح التلقائي إزالة البيانات بعد عدد من محاولات تسجيل الدخول غير الصحيحة.



فكر في إضافة معلومات الطوارئ إلى شاشة القفل. هذا يمكن أن يساعد في إعادتها إذا فقدت.

قم بتأمين الربط

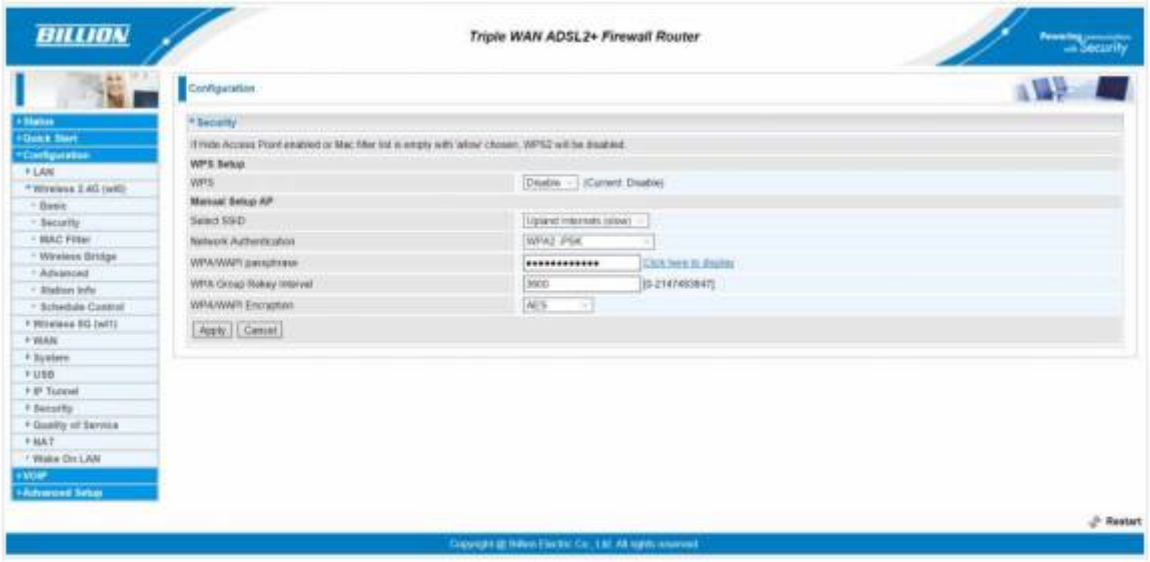
واي فاي المنزل

تسمح الروابط غير الآمنة بالوصول إلى أجهزتك / روابطك دون إذن.

قم بتغيير كلمة المرور الادارية الافتراضية (default administrator password) على جهاز التوجيه الخاص بك router.

– يمكن أحيانًا العثور على كلمات المرور الافتراضية عبر الإنترنت. اختر كلمة مرور حصينة.

- **قم بتعطيل إدارة جهاز التوجيه عن بُعد** لأن هذا يسهل على الآخرين الوصول إليه.
- **استخدم تشفيرًا قويًا.** يعد WPA2 حاليًا أقوى بروتوكول تشفير.
- **امنح SSID (معرف مجموعة الخدمات) اسمًا فريدًا غير معرف.** على سبيل المثال، ليس "Billion7800N" (افتراضي) أو "John Doe's Internet" (معلومات شخصية)
- **قم بتعيين مفتاح شبكة قوي** (كلمة مرور wifi الخاصة بك). لتعطيل المستخدمين الحاليين، قم بتغيير SSID أو مفتاح الشبكة.



- **قم بإيقاف تشغيل شبكات الضيف المفتوحة** ـ امنح حق الوصول للأشخاص الموثوق بهم فقط
- **قم بتنشيط جدار الحماية لجهاز التوجيه الخاص بك.**
- **حافظ على تحديث البرامج الثابتة لجهاز التوجيه الخاص بك.**
- **قم بتعطيل WPS (Wifi Protected Setup)** وإزالة الوصول إلى جهاز التوجيه حيث يمكن إقران الأجهزة ببعض أجهزة التوجيه عن طريق الضغط على زر جهاز التوجيه.

شبكة واي فاي عامة

يمكن أن يكون لشبكة wifi المجانية مخاطر أمنية.

- **استخدم فقط** wifi على الشبكات التي تثق بها. على سبيل المثال ، SLQ wifi. تجنب الشبكات غير المعروفة. تحقق من الشبكة مع الموظفين أولاً، إذا لم تكن متأكدًا.

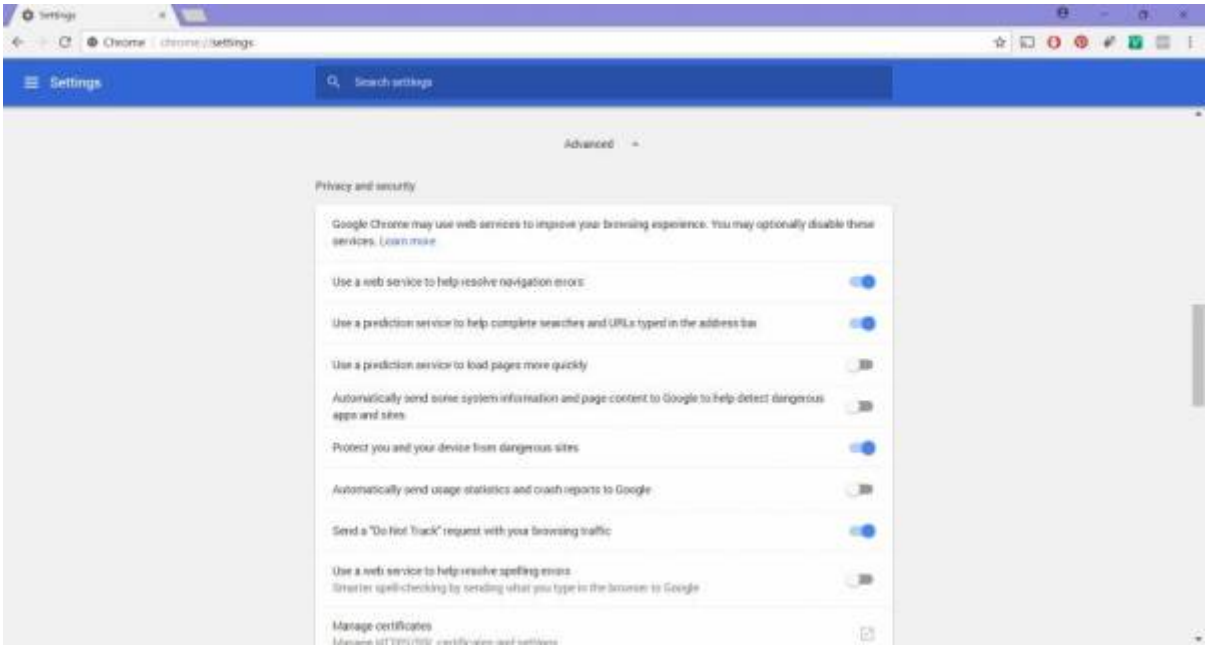
* **استخدم شبكة** wifi العامة المحمية بكلمة مرور عبر الشبكات المفتوحة بالكامل.

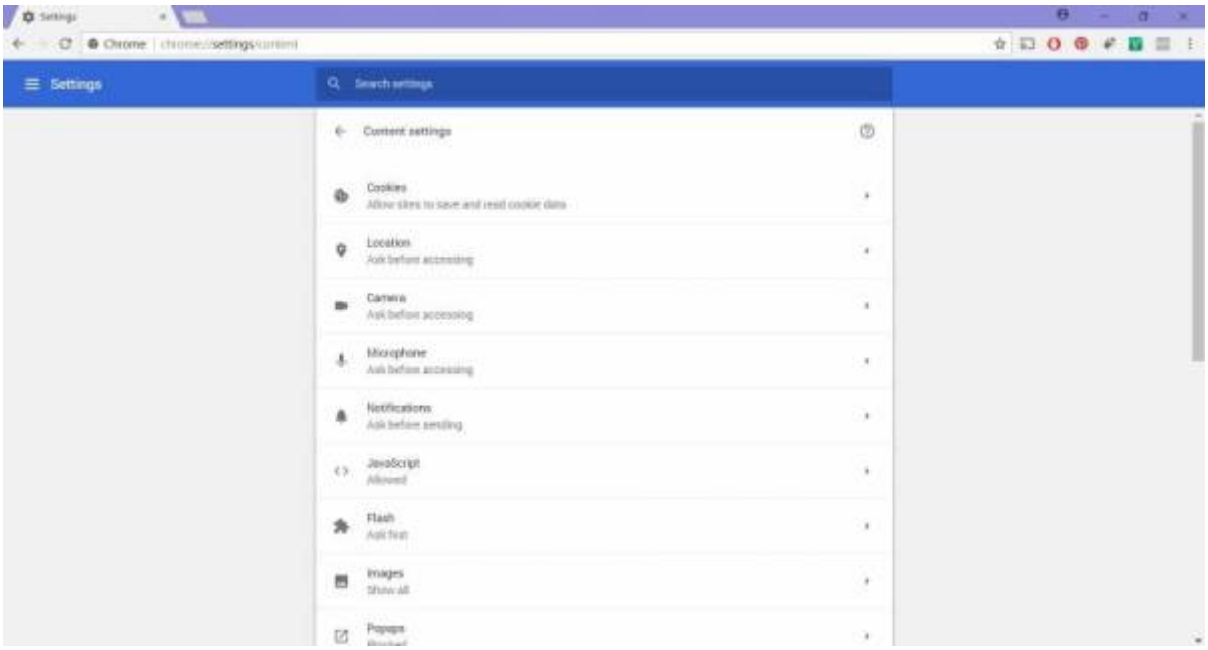
- **إذا كان استخدام** wifi له شروط خدمة ، فاقرأها. لاحظ كيف يستخدمون بياناتك وقيود المحتوى وما إلى ذلك.
- **تجنب البيانات الحساسة على شبكات** wifi العامة، على سبيل المثال. تسجيل الدخول إلى الخدمات المصرفية عبر الإنترنت ، إلخ.
- **حدد الشبكة على أنها** "عامة" 'public' على جهازك. قم بإيقاف تشغيل مشاركة الملفات / خدمات الموقع.
- **قم بإيقاف تشغيل** wifi عندما لا تكون قيد الاستخدام.
    - **ضع في اعتبارك تجنب شبكات الواي فاي العامة**. يمكنك إعداد "نقطة اتصال" لاستخدام بيانات الجوال على أجهزة أخرى. يختلف إعداد نقطة اتصال الجوال باختلاف الجهاز.

قم بتأمين التصفح الخاص بك

يعد Internet Explorer أحد المخاطر الأمنية المحددة. ضع في اعتبارك متصفحًا آخر حيثما أمكن ذلك.

تقدم برامج التصفح عددًا من إعدادات الأمان لإعدادها. في بعض الأحيان تكون هذه ضمن الخيارات "المتقدمة".





قد تقدم بعض الميزات نقاط ضعف. يمكنك إيقاف تشغيلها أو تشغيلها في بعض الأحيان فقط. على سبيل المثال:

- تخزن **ملفات تعريف الارتباط** Cookies لبيانات المواقع الإلكترونية ـ على سبيل المثال، المواقع التي تزورها أو بيانات اعتماد تسجيل الدخول. في حالة اعتراضها، يمكن للمهاجمين الوصول إلى المعلومات التي يتم إرسالها.
- يتم استخدام Java للمحتوى النشط على المواقع الإلكترونية. عادةً ما يكون لتطبيقات Java الصغيرة وصول محدود إلى نظامك. يمكن أن تسمح له الثغرات بتجاهل هذه القيود. يمكن أن تتجاهل تطبيقات Java الصغيرة الموقعة القيود، ولكن يحتاج المستخدمون غالبًا إلى ترخيصها مسبقًا.
- تساعد JavaScript في جعل المواقع الإلكترونية تفاعلية. عادةً ما تقيد معايير JavaScript ميزات مثل الوصول إلى الملفات المحلية.

قم بتثبيت الإضافات / ملحقات المتصفح ذات السمعة الطيبة فقط. هل تبحث أولاً.

احرص دائما على تحديث المتصفح الخاص بك. تصحيحات الأمان تقلل من الثغرات الأمنية.

لا تدخل معلومات حساسة في موقع إلكتروني بدون HTTPS : "**HTTPS**" يعني أنه يحتوي على شهادة SSL (اتصال مأخذ توصيل آمن) مثبتة لتشفير حركة المرور، لذا فهي أكثر أمانًا.

فكّر في استخدام VPN (الشبكة الافتراضية الخاصة) لتشفير حركة المرور الخاصة بك على الإنترنت.

انتبه دائمًا إلى ما تسمح به أو تمنعه، بما في ذلك الوصول إلى الكاميرا والميكروفون والموقع وما إلى ذلك.

تأمين حساباتك

كلمات المرور القوية هي خط دفاعك الأول. فكّر في برنامج إدارة كلمات مرور معروف أو أنشئ كلمات مرور قوية خاصة بك.

يمكن لمجرمي الإنترنت اختراق كلمات المرور الضعيفة بسهولة:

- تختبر هجمات الدخول عنوة إلى النظام مجموعات كلمات المرور بسرعة
- تختبر الهجمات المستندة إلى القاموس الكلمات الشائعة
- يمكنهم التخمين من المعلومات الشخصية

اختر أيضًا اسم مستخدم فريدًا. على سبيل المثال "admin" هو اسم مستخدم شائع جدًا (من السهل تخمينه).

اختيار كلمات المرور

استخدم:

- الأرقام والأحرف (الأحرف الكبيرة والصغيرة) والرموز
- شيء لا يُنسى، أو استخدم مدير كلمات المرور
- كلمات مرور طويلة ـ 8 أحرف على الأقل

استخدم:

- الأرقام والأحرف (الأحرف الكبيرة والصغيرة) والرموز
- شيء لا يُنسى، أو استخدم مدير كلمات المرور
- كلمات مرور طويلة ـ 8 أحرف على الأقل

إنشاء كلمة مرور سهلة

1. فكر في جملة
2. استخدام جزء من كل كلمة
3. استبدال الأرقام والرموز والأحرف الكبيرة.

علي سبيل المثال:

1. الجملة: 'ilove interiordesign'.
2. تجزء الجملة: ilointrdsgn
3. الاستبدال: !lo1nTRdsgN

جربها بلغة مختلفة أيضًا!

تأمين كلمة المرور

اجعل كلمات مرورك مختلفة إذا كنت تستخدم نفس كلمة المرور في كل مكان، فستكون معلوماتك أكثر عرضة للخطر.

هذا يمكن أن يكون سهلا! استخدم أحرفًا إضافية لجعلها مختلفة. علي سبيل المثال:

- Gmail كلمة مرور: 18GIL6SunD@e5
- Facebook كلمة مرور: FOK186SunD@e5
- كلمة مرور تويتر: 186SunD@e5TW

ما الذي تفعله:

- فكر في استخدام مدير كلمات المرور ـ غالبًا ما تحتوي البرامج المدفوعة على خيارات أكثر.
- قم دائمًا بتسجيل الخروج بعد استخدام الحسابات على أجهزة الكمبيوتر المشتركة.
- استخدم مصادقة تقوم على عاملين.

ما الذي لا تفعله: ● مشاركة كلمات المرور مع الآخرين. ● الاحتفاظ بكلمات المرور في رسائل البريد الإلكتروني أو الملفات التي يسهل العثور عليها. ● استخدام كلمات المرور على الشبكات/أجهزة الكمبيوتر العامة. ● "حفظ" كلمات المرور إلا إذا كنت المستخدم الوحيد للجهاز. ● إدخال كلمات المرور الخاصة بك من خلال رسائل البريد الإلكتروني/ الاتصالات التطفلية. ● إدخال كلمات المرور على المواقع غير الآمنة.

إذا تم استخدام حسابك من قبل شخص آخر، فقم بتغيير كلمة المرور الخاصة بك على الفور و/أو قم باستعادة كلمة المرور. ,

استعادة كلمة المرور

عند تعيين كلمة مرور، قد تحتاج إلى تقديم سؤال وإجابة سريين لاستعادة كلمة المرور. على سبيل المثال:

- اسم والدتك قبل الزواج؟

استخدم المعلومات التي تعرفها فقط. إذا كان استرداد كلمة المرور ضعيفًا، فأنت لا تزال عرضة للخطر ـ خاصةً إذا تم اختراق بريدك الإلكتروني.

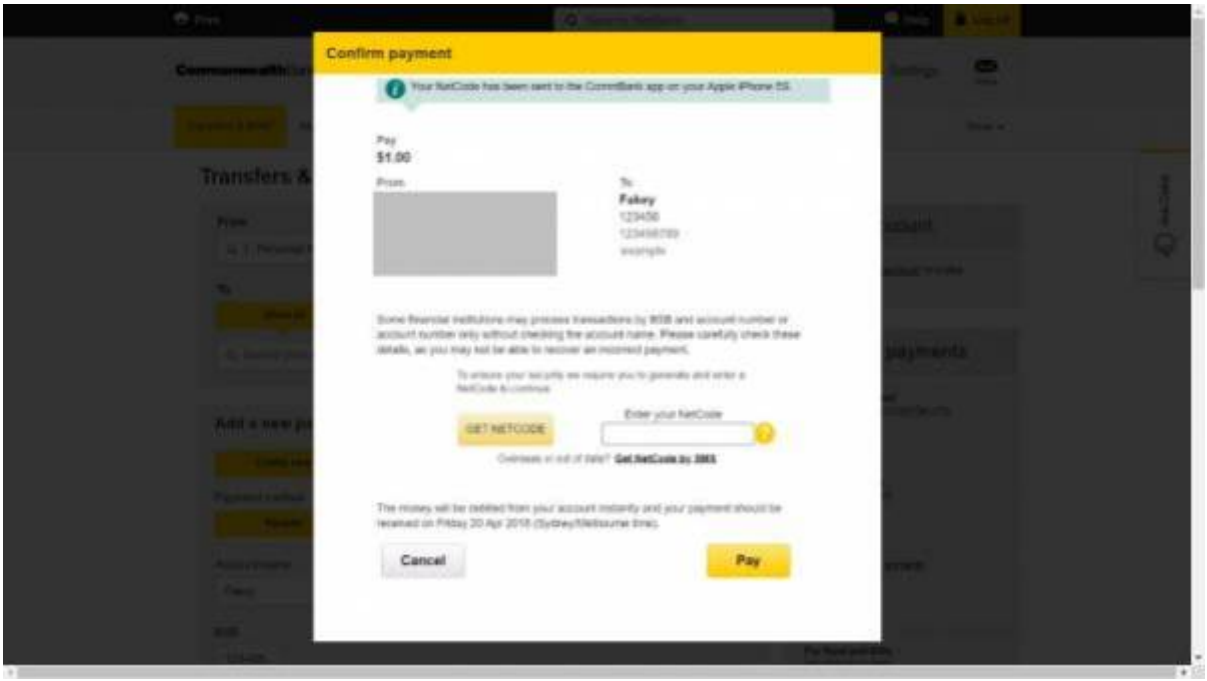
باستخدام 2FA

2FA هي المصادقة التي تقوم على عاملين. بدلاً من طريقة تحقق واحدة (على سبيل المثال، اسم المستخدم / كلمة المرور)، تضيف المصادقة الثنائية (2FA) التأمين مع طرف ثاني. على سبيل المثال:

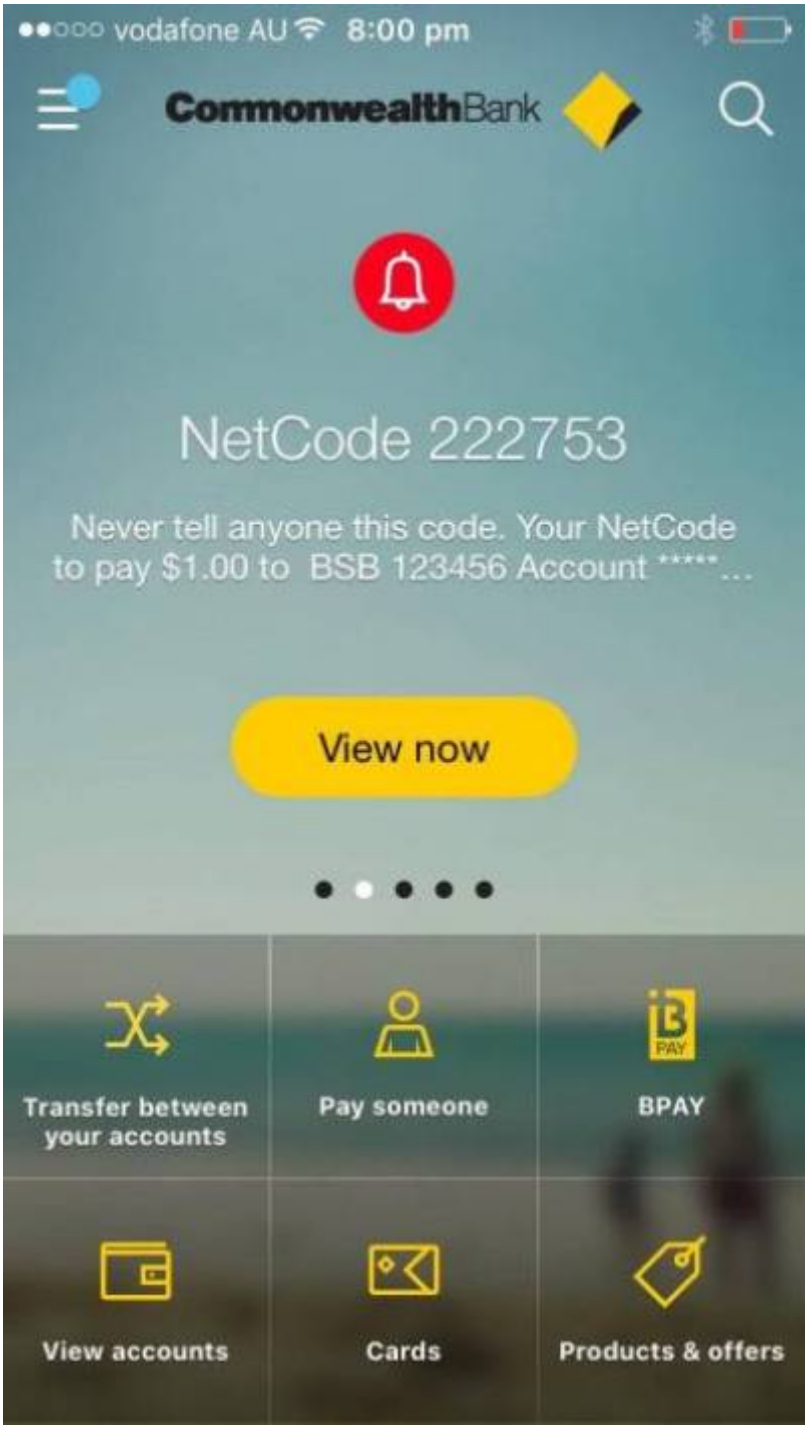
- شيء **تعرفه** (مثل رقم التعريف الشخصي أو كلمة المرور)
- شيء **تملكه** (مثل بطاقة مصرفية أو هاتف محمول)
- شيء **يرتبط بك** (مثل بصمة الإصبع)

حساباتك ومعاملاتك أكثر أمانًا مع المصادقة الثنائية (2FA).

على سبيل المثال يرسل هذا الموقع الإلكتروني رمزًا مميزًا عبر الإشعارات التنبيهية:



يجب عليك إدخال الرمز لمتابعة المعاملة:



تقلل المصادقة الثنائية من المخاطر، ولكن ليس بالكامل.

- الرموز التي يتم إرسالها عن طريق **إشعارات تنبيهية** (من التطبيق) أكثر أمانًا من **الرسائل** القصيرة.
- إذا لم تتمكن من الدخول إلى هاتفك/اتصالك، فلا **يمكنك الوصول إلى حساباتك** التي تستخدم الهاتف 2FA.
- **قد يُفقد هاتفك أو يُسرق.** يمكن لأي شخص لديه هاتفك غير المؤمّن استخدام حسابات تسجيل الدخول وطرق 2FA للهاتف.

تحديد المخاطر/الاحتيال

عمليات الاحتيال تخدع الأشخاص من أجل الحصول على معلومات (بغرض الاحتيال في الهوية) أو الأموال أو أشياء أخرى.
تعرف على عمليات الاحتيال الشائعة عبرhttps://www.scamwatch.gov.au.

مثال على الفيديو: https://www.youtube.com/watch?v=BL7WJM342Uc

الأكثر أهمية:

- ابحث عن رسائل مزيفة (رسائل بريد إلكتروني، مكالمات، مواقع إلكترونية... إلخ)
- لا تنقر على روابط غير جديرة بالثقة (مواقع إلكترونية ومرفقات البريد الإلكتروني وعناوين URL المختصرة وما إلى ذلك)
- كن حذرًا إذا طُلب منك المال أو معلومات الهوية أو تفاصيل الحساب

خدع دفعات الأقساط

- يرسل المحتالون رسائل نصية أو يتصلون من أرقام غير معروفة ويتقاضون سعرًا إضافيًا إذا قمت بإرسال رسالة نصية/معاودة الاتصال.
- لا يزال بإمكان مولدات الأرقام العشوائية الاتصال برقمك (حتى لو كان خاصًا)

حظر الأرقام التي بها مشاكل. إذا تم اختراقك، فاتصل بمزود خدمة الجوال ـ فقد يقوم بإزالة الرسوم.

خدع الدخول عن بعد

يتصل المحتالون ويدعون أنهم من شركة / خدمة تقنية تحتاج إلى الدخول إلى جهاز الكمبيوتر الخاص بك (غالبًا "لإصلاح" مشكلة غير موجودة أو عملية اعادة مال).

- لا تمنح المتصل المتطفل إمكانية الدخول عن بعد إلى جهاز الكمبيوتر الخاص بك. لن تطلب الشركات الحقيقية هذا.
- لا تقم أبدًا بإعطاء تفاصيلك الشخصية أو تفاصيل حسابك إلا إذا أجريت المكالمة (أو كانت مكالمة حقيقية تم التحقق منها).

في حالة الاختراق، اطلب المساعدة من فني كمبيوتر مؤهل، وغيّر تفاصيل الحساب واتصل بطريقة الدفع لعكس الرسوم إن أمكن.

التصيد

تحاول عمليات التصيد الاحتيالي الحصول على معلومات شخصية (على سبيل المثال، تفاصيل تسجيل الدخول/بطاقة الائتمان/ إلخ) غالبًا عن طريق التظاهر بأنه مصدرًا موثوقًا به.

على سبيل المثال، **المكالمات أو رسائل البريد الإلكتروني** التي تدعي أنها من بنك أو مؤسسة أخرى تطلب تفاصيل لتأمين

حسابك.

غالبًا ما تكون مصممة للتخويف (على سبيل المثال، تطلب "Centrelink" تأكيد التفاصيل أو سيتوقفون عن الدفع). قد يتظاهر الآخرون بتقديم جائزة أو ما شابه ذلك.

- تحقق لمعرفة ما إذا كانت المكالمات واردة من أرقام يمكن التحقق منها ورسائل البريد الإلكتروني واردة من عناوين رسمية (يجب إدراجها على الموقع الإلكتروني)
- تحقق من رسائل البريد الإلكتروني مقابل الرسائل الحقيقية. هل توجد أخطاء تنسيقية أو نحوية أو إملائية؟ لا تنقر فوق الروابط المشبوهة أو تفتح المرفقات غير المعروفة.
- تحقق من عناوين المواقع الإلكترونية. هل هي مختلفة عن المعتاد؟ (على سبيل المثال، commmbank.com بدلاً عن commbank.com.au)
- لا تقدم أبدًا تفاصيل شخصية لجهة اتصال متطفلة تدعي أنها من البنوك أو ATO وما إلى ذلك.
- **لن تهددك الشركات والمؤسسات الحقيقية أو تسيء إليك لفظيًا.**

في حالة الاختراق، قم بتغيير معلومات حسابك على الفور، واتصل بالشركة/المؤسسة الحقيقية لتأمين بياناتك.

الشراء/البيع

عند الشراء من البائعين الفرديين:

- إذا كان هناك شيء يبدو جيدًا لدرجة يصعب تصديقه، **فعادة ما يكون مخادع.** على سبيل المثال، السيارات أو الممتلكات منخفضة التكلفة التي لا يمكنك فحصها قبل الشراء.
- شاهد العناصر شخصيًا، وتحقق من مراجعات البائع، واستخدم طرق الدفع مع الحماية من الاحتيال (مثل سلع وخدمات Paypal).

عند الشراء من المتاجر:

- متاجر وهمية على الإنترنت يسهل على المحتالين إنشاؤها ، كما هو موضح هنا:https://www.youtube.com/watch?v=3IIuT4Jo4f8/watch?v=3IIuT4Jo4f8
- تحقق من أن تسجيل الأعمال وتفاصيل الاتصال بهم حقيقية قبل إجراء المعاملات.
- تحقق من أن سياسات الخصوصية/الاسترداد/الإرجاع تتوافق مع القوانين المحلية.
- إذا كانت الأسعار جيدة جدًا، فقد تتلقى منتجات مقلدة (أو لا تتلقى أي شيء على الإطلاق).
- إذا تم استخدام بوابة بطاقة الائتمان، فهل هي موثوقة/آمنة؟ استخدم فقط طرق الدفع بما في ذلك الحماية من الاحتيال.

عند البيع:

- قم بتوثيق العناصر بدقة وإرسالها **مع** التتبع (في حالة نشوء نزاعات للحصول على المبالغ المستردة من خلال Paypal وما إلى ذلك).
- لا ترسل حتى يتم إنهاء الدفع.
- لا تحذف الإعلان الأصلي إلّا بعد مرور فترة طويلة على تاريخ المعاملة.

- لا تقبل الدفع الزائد للعنصر و "استرداد" الفرق (إنها عملية احتيال شائعة).

إذا تعرضت للاختراق أثناء استخدام طريقة الدفع مع الحماية من الاحتيال (على سبيل المثال، بطاقة الائتمان أو Paypal)، فقد تتمكن من ترتيب عملية الاسترداد. اتصل أيضًا بوكالة حماية المستهلك (على سبيل المثال، مكتب التجارة العادلة: https://www.qld.gov.au/law/fair-trading

التواصل الاجتماعي عبر الانترنت

تطرح بعض ميمات وسائل التواصل الاجتماعي **أسئلة تعريف شخصية** يمكن استخدامها في **الاحتيال على الهوية**ـ على سبيل المثال، "منشئو الأسماء" الذين يستخدمون تاريخ ميلادك/الشارع الذي نشأت فيه لتكوين اسم).

كن حذرًا من **"المنتحل"** (الملفات الشخصية المزيفة للاستفادة منك، غالبًا على مواقع المواعدة). مثال على فيديو ACCChttps://youtu.be/YDt0F7ETmRU

يبدو أنهم يطورون مشاعر قوية بسرعة ويريدون منك أن تثق بهم. كثيرًا ما تطلب الهدايا أو المال أو التفاصيل الشخصية (أحيانًا مع قصة حزينة). قم بإجراء "بحث عكسي عن الصور" ـ غالبًا ما يستخدمون صورًا عشوائية لإنشاء ملفات شخصية ذات مظهر "حقيقي".

قد يتظاهرون أيضًا بأنهم عائلة أو أصدقاء بملفات تعريف مزيفة أو حسابات تم اختراقها. على سبيل المثال:

- قد يدعون أنهم بحاجة إلى المال أثناء وجودهم في الخارج (والذي يبدو حقيقيًا لأنه من "أشخاص موثوق بهم")
- تأكيد الحقائق باستخدام طريقة مختلفة ـ على سبيل المثال الاتصال بهم.
- **إذا راودك الشك، قل لا.**

ماذا لو خُدعت؟

- اتصل بمؤسستك المالية، ومقدمي الحسابات المتأثرين و/أو وكالة حماية المستهلك المحلية
- قم بتغيير كلمات المرور الخاصة بك
- استرجع هويتك المسروقة
- أبلغ عن عمليات الاحتيال إلى السلطات
- احصل على المساعدة من الوكالات الأسترالية

المزيد من المعلومات: https://www.scamwatch.gov.au/get-help/where-to-get-help

ضوابط الخصوصية

تتحكم الخصوصية في مكان عرض معلوماتك ومن يراها.

بعض المعلومات التي تقدمها عمدا. على سبيل المثال، التفاصيل الخاصة بك لفتح حساب. هذه **معلومات تعريف شخصية.**

معلومات أخرى قد لا تدرك أنك تشاركها ـ على سبيل المثال، عادات التسوق أو سجل البحث. هذه **المعلومات غير المحددة للهوية** الشخصية مرتبطة بـ "شخص ما"، ولكن ليس أنت على وجه التحديد.

من يملك بياناتك؟

شرح بالفيديو: https://www.youtube.com/watch?v=y1txYjoSQQc

قد تكون المعلومات *عنك*، لكنها *ليست* ملكك.

1. تحقق **من الشروط والأحكام وسياسات الخصوصية** قبل استخدام الخدمة.
2. تحقق من كيفية استخدام البيانات الخاصة بك.
3. غالبًا ما **نعطي بياناتنا للحصول على خدمة.** على سبيل المثال يتلقى Facebook إذنًا لاستخدام البيانات للإعلان عند الانضمام.

تأمين البيانات الخاصة بك

- **الحد من المعلومات التي تشاركها عبر الإنترنت.**
- **غالبًا ما تستخدم تواريخ الميلاد في المصادقة الثنائية، لذا** لا تخبر **الجميع بذلك**
- **قم بتأمين الاتصال والتصفح ـ** راجع الخطوات أعلاه.
- **مراجعة وتعديل إعدادات الخصوصية الخاصة بك حسب الحاجة .**
- **فكر قبل قبول ملفات تعريف الارتباط.** يمكن لملفات تعريف الارتباط تتبع معلومات مثل تفاصيل تسجيل الدخول أو محفوظات الاستعراض.
- ضع في اعتبارك **حذف البيانات** والحسابات التي لم تعد بحاجة إليها.

- **Limit information you share online**.
- **Birthdates are often used in 2FA** so **don't tell everyone**
- **Secure your connection and browsing** – see steps above.
- **Review and amend your privacy settings as needed**.
- **Think before accepting cookies.** Cookies can track information like login details or browsing history.
- Consider **deleting data** and accounts you no longer need.

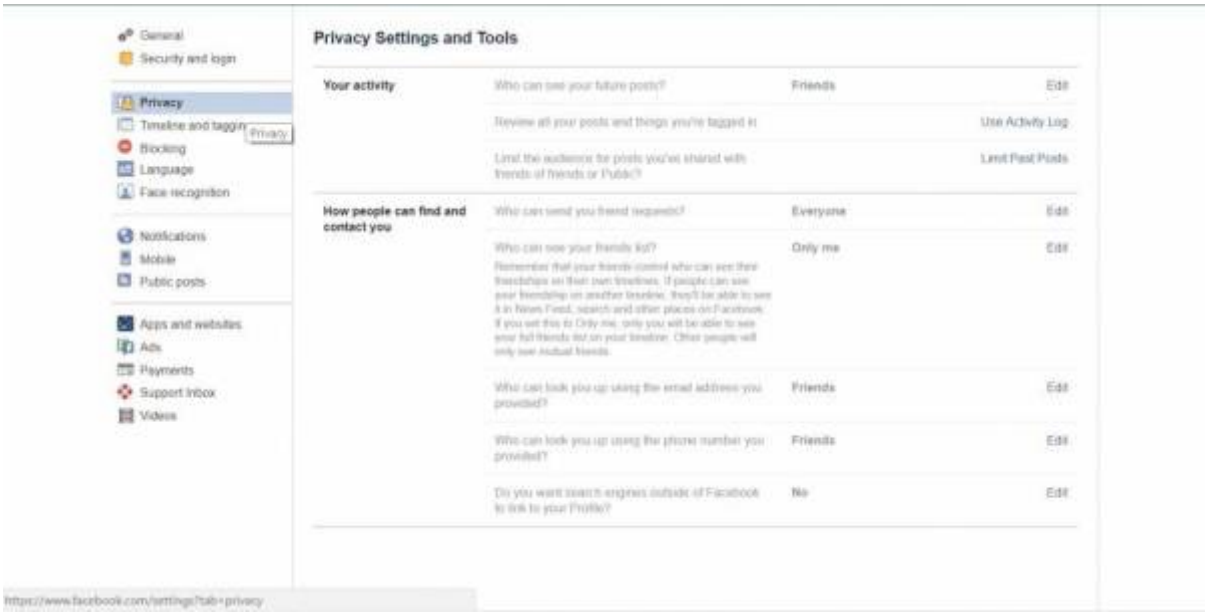
خصوصية وسائل التواصل الاجتماعي

كل منصة وسائط اجتماعية لها شروط الخدمة وخيارات الخصوصية الخاصة بها. راجع هذه قبل **وأثناء** استخدام هذه المنصات.

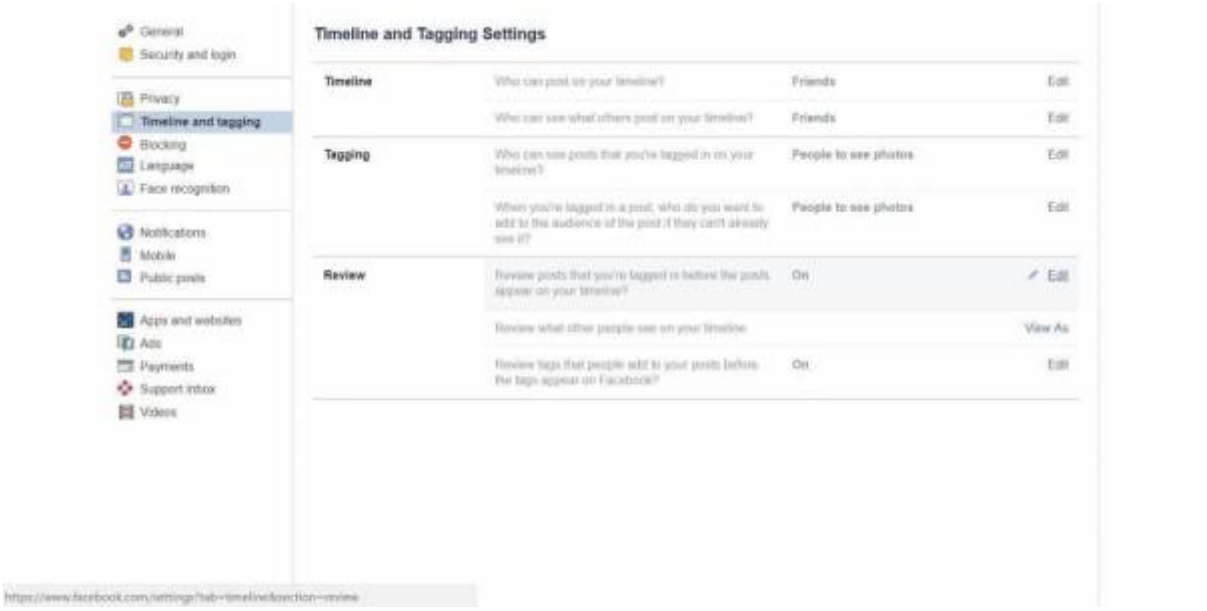
يمكنك غالبًا توجيه إرشادات من Google حول كيفية التنقل في الخصوصية على كل نظام أساسي. سنلقي نظرة على إعدادات Facebook اليوم.

فيسبوك

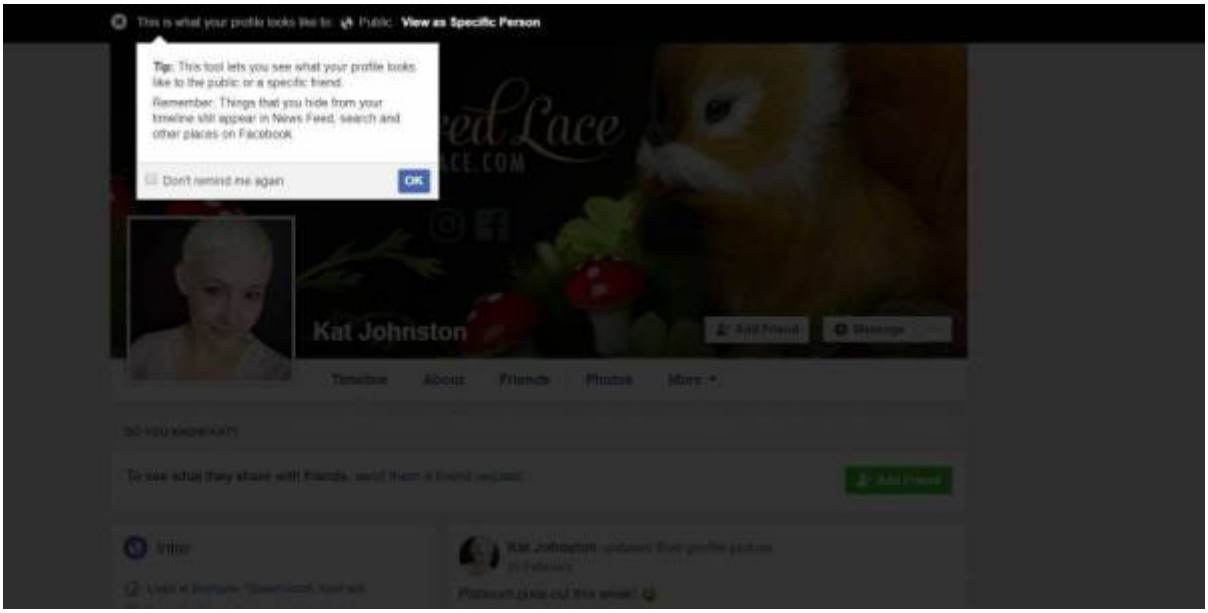
يمكن تعديل خيارات خصوصية حساب Facebook في "الإعدادات":



يقيد المخطط الزمني والعلامات من يرى المحتوى الخاص بك أو يمكنه "وضع علامة" 'tag' عليك. تسمح لك القوائم بقصرها على أشخاص محددين.



راجع ما يراه الآخرون في مخططك الزمني: اعرضه كمستخدم عام أو شخص محدد.



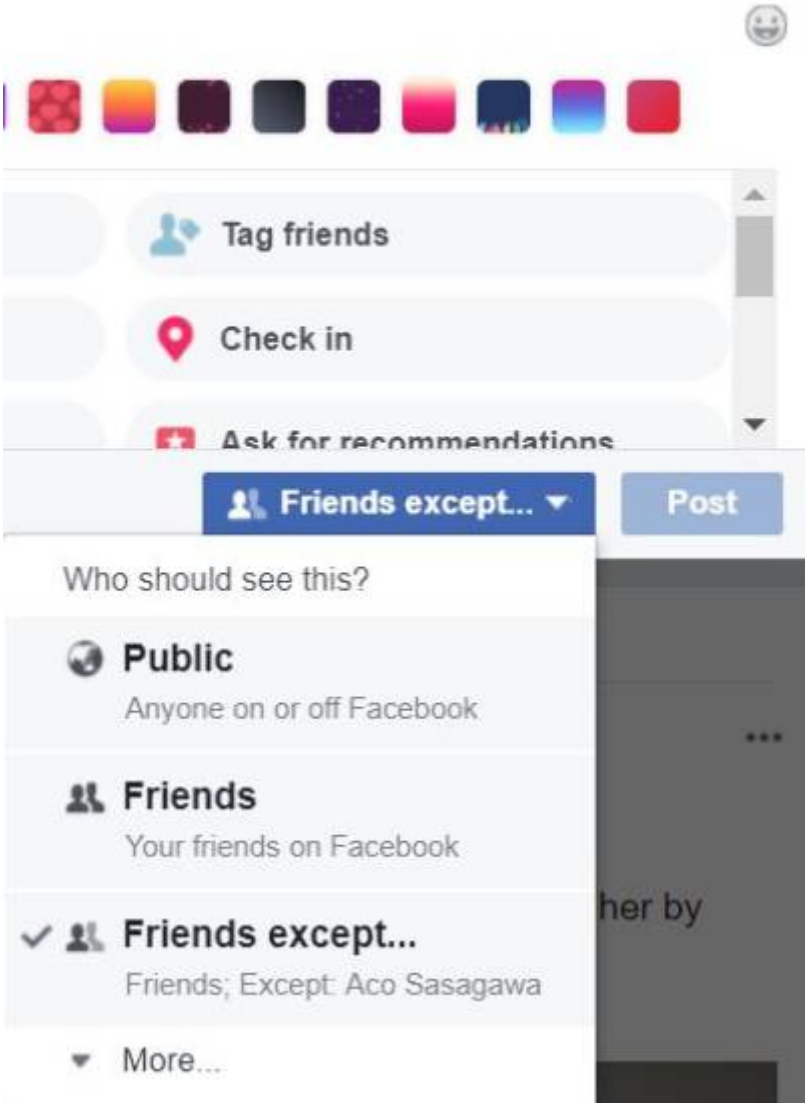
قوائم الأصدقاء

أنشئ قوائم لمشاركتها بسهولة مع أشخاص محددين فقط.

1. في موجز الأخبار، انقر فوق "قوائم الأصدقاء" على اليسار. قد تحتاج إلى النقر فوق "مشاهدة المزيد" أولاً.
2. انقر على "+ إنشاء قائمة" '+ Create List'.
3. انشئ اسمًا للقائمة واضف أصدقاءًا إلى القائمة. يمكنك إضافة / إزالة أشخاص في أي وقت.
4. انقر على إنشاء.

تعيين الخصوصية في المشاركات

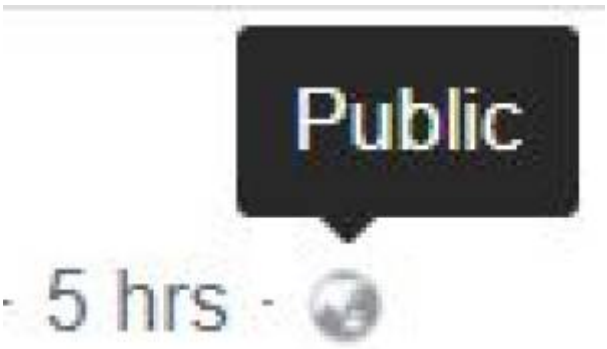
اختر من القائمة المنسدلة ـ يمكنك تحديد قائمة الأصدقاء هنا أيضًا. **تحقق من هذا الإعداد في كل مرة تنشر فيها.**



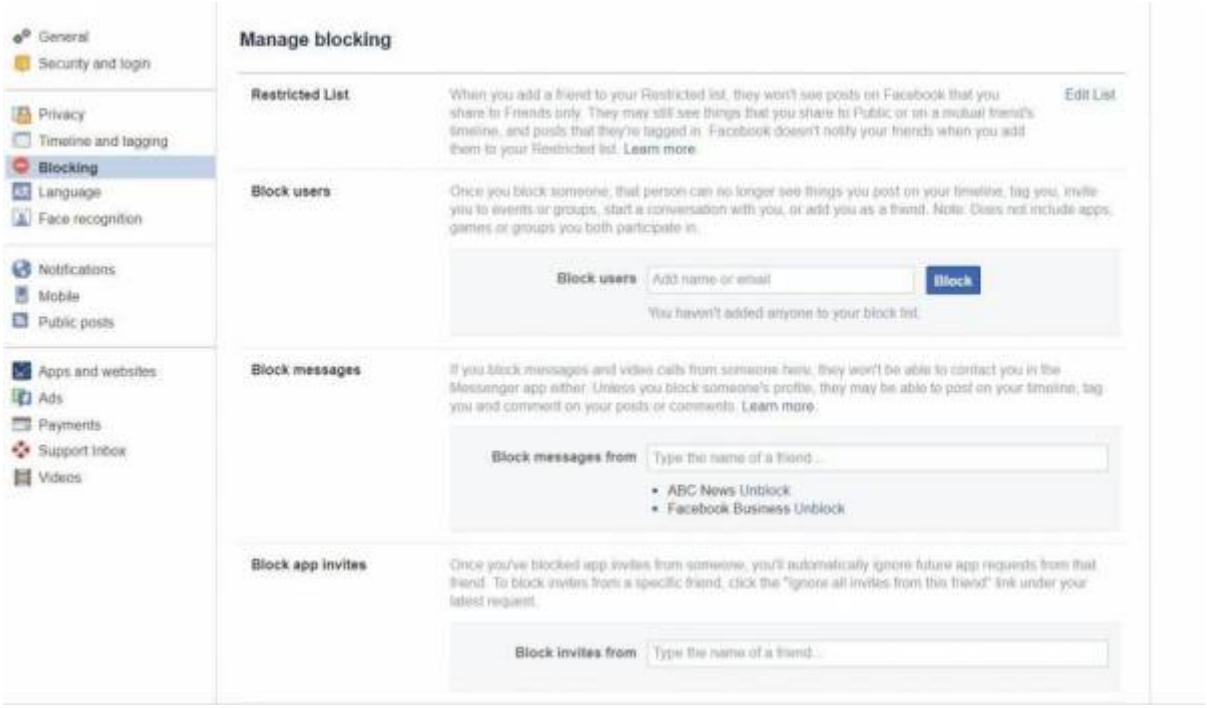
يمكنك (والآخرين) **تغيير خصوصية** المنشور لاحقًا.

التعليقات تأخذ نفس خواص إعدادات الخصوصية للمشاركات الأصلية. على سبيل المثال، **إذا كانت إحدى المشاركات عامة، فإن تعليقاتك كذلك.**

تحتوي **صفحات Facebook** ومعظم **مجموعات Facebook** على منشورات عامة. لا تغطي "خصوصية الحساب" المحتوى الموجود على شيء تم تمييزه على أنه عام.

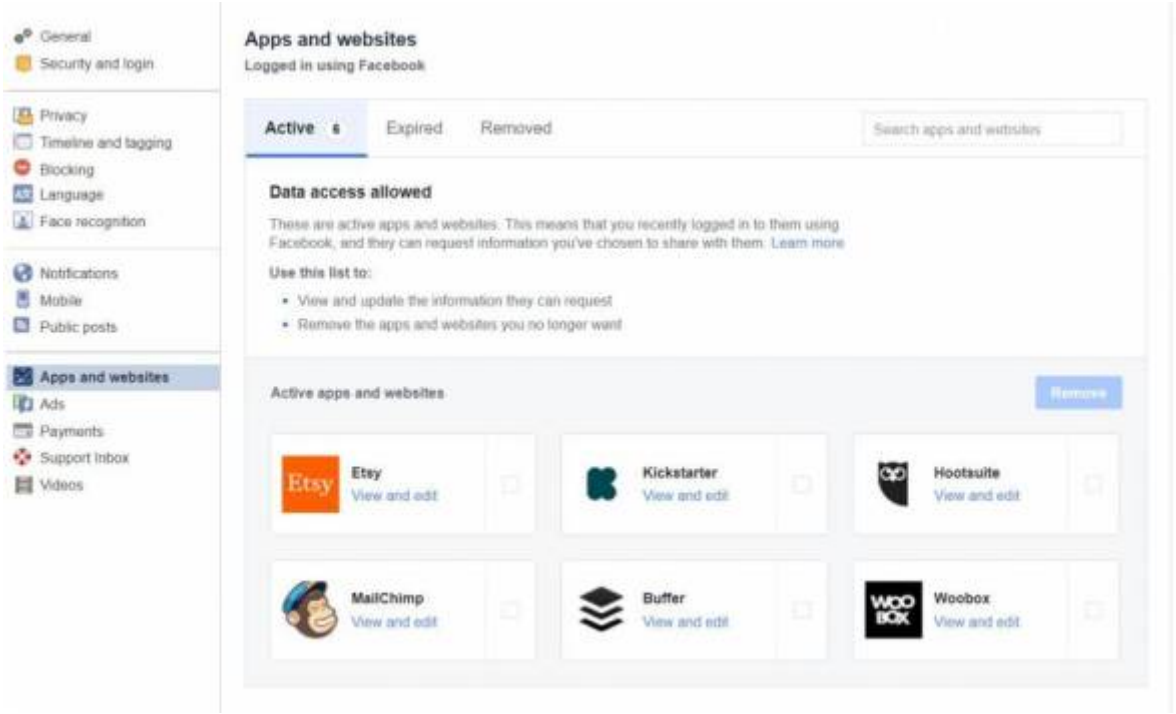


يمكنك **حظر** الأشخاص إذا كان شخص ما يضايقك أو يتنمر عليك (يقع ضمن "الإعدادات"). يمكنك أيضًا الإبلاغ عن سلوك في مشاركات فردية.

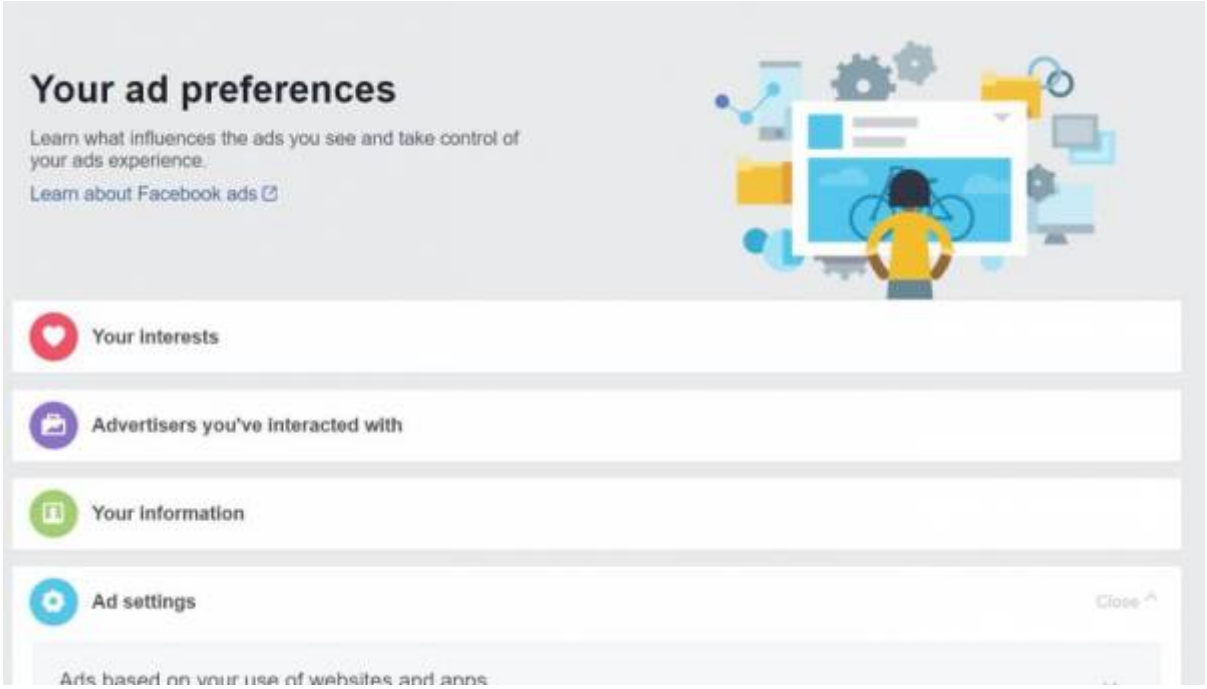


ضع في اعتبارك تعطيل **التعرف على** الوجه للحفاظ على الخصوصية.

عرض وتعديل الحسابات التي قمت بتسجيل الدخول إليها باستخدام Facebook. تسجيل الدخول باستخدام Facebook يسمح للمواقع بالوصول إلى معلومات معينة. تحقق بانتظام من المعلومات التي يتم مشاركتها وضبطها.

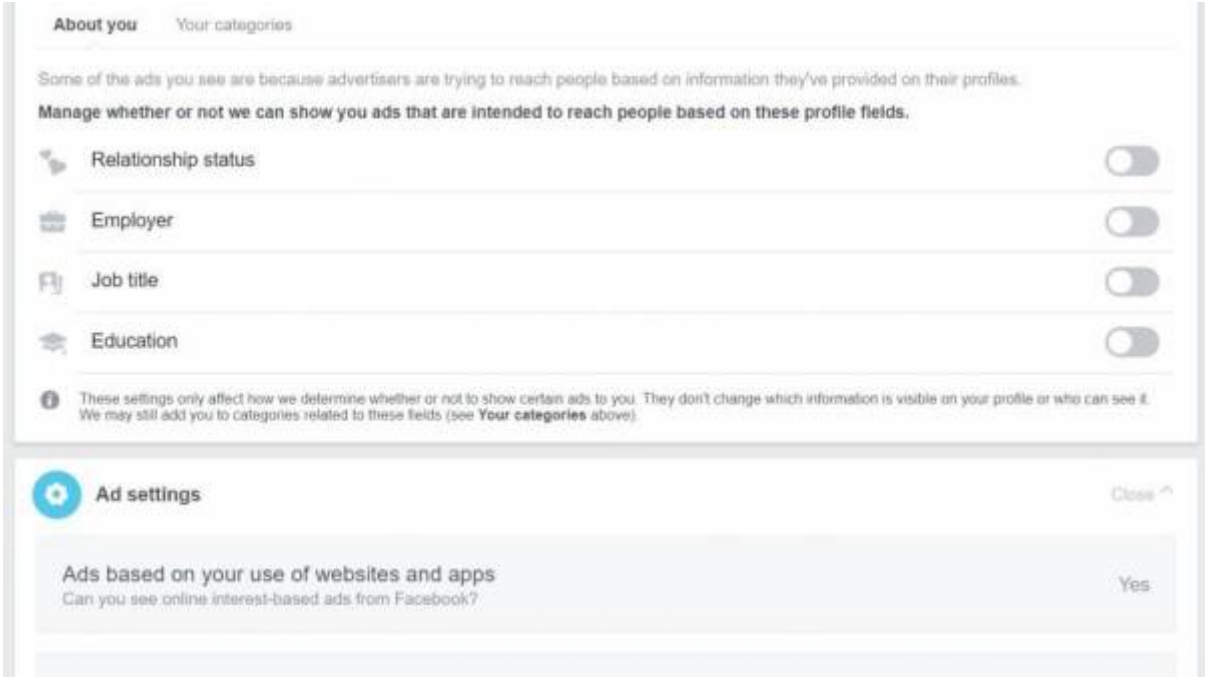


يستخدم المعلنون على Facebook بياناتك لعرض المحتوى المستهدف.



يتم تخزين الكثير من البيانات هنا. يمكنك إزالة المعلومات (مثل اهتماماتك)، لكن Facebook سيستمر في جمع البيانات لإعادة بناء القوائم.

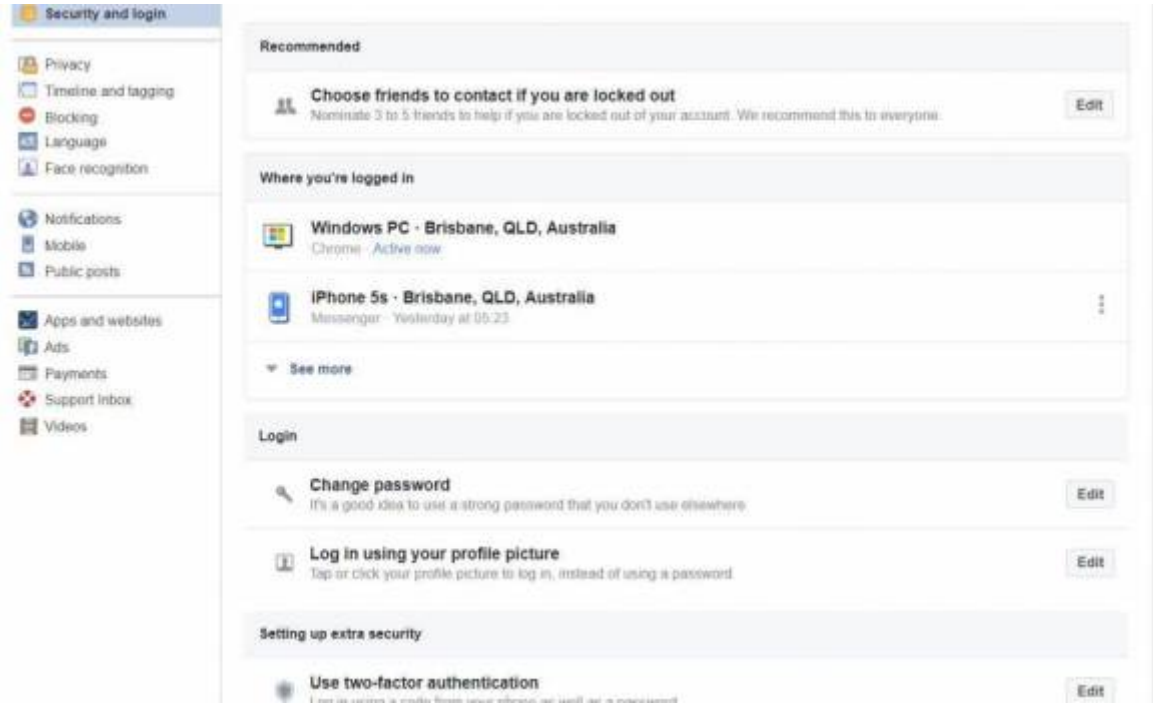
تسمح الأذونات / تمنع وصول المعلنين إلى معلومات معينة.



تحقق بانتظام من سجل نشاطك وراجع بياناتك. **هل مازلت بحاجة لمشاركتها؟** قم بإزالة ما لا تحتاجه.

استخدم شاشة الأمان وتسجيل الدخول لمراجعة عمليات تسجيل الدخول الخاصة بك وتسجيل الخروج عن بُعد. **إذا تركت Facebook مسجلاً الدخول في مكان ما عن طريق الخطأ ، فقم بتسجيل الخروج هنا.**

قم بتشغيل **المصادقة الثنائية** Two Factor Authentication، وفكر في ترشيح أشخاص لتأكيد هويتك إذا كنت محجوبًا.



تذكّر!

الخصوصية غير مضمونة حتى مع الإعدادات القوية:

1. يمكن عرض**لقطات الشاشة** للأشخاص الذين ليس لديهم عادةً إمكانية الدخول.
2. يمكن مشاركة المعلومات التي تم **نسخها** / تنزيلها.
3. يمكنك **منح حق الدخول** إلى الشخص الخطأ عن غير قصد.
4. يمكن أن تجعل **الثغرات الأمنية** المعلومات الخاصة علنية.

للحفاظ على خصوصية المعلومات بنسبة 100٪، لا تضعها على الإنترنت.

المزيد من الموارد

/https://www.staysmartonline.gov.au

/https://www.scamwatch.gov.au

https://aifs.gov.au/cfca/publications/online-safety

/https://www.esafety.gov.au

/https://www.opencolleges.edu.au/informed/cyber-safety

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

https://help.instagram.com/196883487377501

https://help.twitter.com/en/safety-and-security