كيف
تستخدم فيسبوك بأمان

ما انفك عدد مستخدمي الشبكة الاجتماعية فيسبوك يلتقون ويجتمعون افتراضيا ويدردشون ويتبادلون المعلومات والأفكار لينتهي بهم الأمر بالالتقاء فعليا على أرض الواقع. وقد يكون اللقاء أحيانا للاحتجاج، وأحيانا للاحتفال، وأحيانا في بلد لا يشجع على التطرق بالنقاش للحياة العامة بل وقد يعاقب عليه، وأحيانا أخرى يكون اللقاء في بلد حيث الحرية جزء لا يتجزأ من الحياة.

لا شك أن فيسبوك هو أداة فعالة، ولكن لكي تحسن استخدامه بأقصى قدر من الفعالية عليك التأكد من اتخاذ الخطوات اللازمة لكي تقلل من إمكانية الإطلاع على اتصالاتك ونشاطاتك من قبل المستخدمين.

يقدم هذا الدليل خطوات للقيام بذلك. اتبع إرشاداته لكي تنتظم بأمان، ولكن اعلم أنك، حتى لو تقيدت بكل الإرشادات، فيجب عليك توخي الحذر دائما وقطع اتصالاتك عند التشكك بقدر ما هو ممكن وآمن للقيام بذلك.

هذا الدليل متوفر للتنزيل في شكل بي دي إف pdf من الرابط التالي :
http://www.movements.org/how-to/entry/organize-on-facebook-securely

قبل أي شيء

الخطوة ١ استخدام خاصية التصفح الآمن HTTPS يعني أنك تقوم بإنشاء قناة أكثر أمانا عبر شبكة غير آمنة، تقدم حماية لك من المراقبة أو من أن يستحوذ أحدهم على حساباتك في الويب بدون إذن. ولكي لا نخوض في تقنية معقدة، اعلم فقط أن HTTP هو بروتوكول نقل النص التشعبي وهو بروتوكول يستخدم حزمة بروتوكولات الإنترنت TCP لنقل البيانات وتبادلها بين الخوادم والمتصفحات. HTTP **هو غير آمن** وقد يتعرض للتنصت والمراقبة، ومن جهة أخرى استخدام HTTPS يؤمّن الاتصالات على صفحة الويب.

خدمة التصفح الآمن HTTPS غير مشغَّلةٍ تلقائيا. لذلك يجب على المستخدم أن يغير إعداداته لتفعيلها. ولفعل ذلك، انقر على :
الحساب >> إعدادات الحساب >> الإعدادات >> انقر على تغيير أمان الحساب >> اختر خانة «التصفح الآمن (*https*)» >> اضغط على «حفظ».

ومع ذلك، تذكر دائما أن التصفح الآمن https لا يعني بالضرورة أنك تحظى بحماية كاملة، لذلك لا تتخلى عن كامل حذرك لمجرد أنك كنت ذكيا بما يكفي لتفعيل التصفح الآمن!

ضع تنبيه دخول. سوف تتوصل بتنبيه عن طريق البريد الإلكتروني كلما حاول حاسوب أو جهاز محمول جديد الدخول إلى حسابك. هكذا، إذا توصلت ببريد يخبرك أن هناك من دخل حسابك وبدا لك الأمر مشبوها، تعرف أن هناك من حاول اختراق حسابك. ربما تكون فعلت هذا لأن خانة هذا الإعداد توجد مباشرة تحت الخانة المُفعِّلة للتصفح الآمن https. وإذا لم تفعل، اذهب إلى :

الحساب >> الإعدادات >> خصوصية الحساب >> انقر على تغيير أمان الحساب >> انقر على خانة «ارسال بريد إلكتروني إلي» >> اضغط على «حفظ».

الخطوة ٢ كن مستعدا لعالم بلا فيسبوك. كل محتواك واتصالاتك مستضافة لدى خوادم فيسبوك ـ وليس على خادمك. هذا يعني أنه في حالة تعطيل حسابك نتيجة خطأ ما أو بسبب إخلالك بشروط استخدام الشركة، سوف تفقد جميع هذه المعلومات إلا إذا كنت تحتفظ بنسخة احتياطية منها.

تحت «إعدادات الحساب» اذهب إلى «تنزيل معلوماتك»، ثم «لمعرفة المزيد»، ثم اضغط على زر «تنزيل». يمكنك أيضا الحصول على تطبيق Adobe Air المسمى «سوشال سيف» SocialSafe أو امتداد فيرفُكس «أرشيف فيسبوك» ArchiveFacebook الذي يقوم بتنزيل ملفك الشخصي وبياناتك وصورك إلى قرص حاسوبك.

إعدادات الخصوصية

الخطوة ١ **افهم جيدا معاني مصطلحات فيسبوك**. ما فتئ فيسبوك ينمو. ومع هذا النمو **ظهر عدد من المصطلحات الجديدة؛ عليك أن تعرفها** لكي تفهم جيدا ما هي المعلومات التي يجمعها الموقع عنك ويشاركها. نسرد فيما يلي، **بعض المصطلحات المتداولة** الاستعمال على فيسبوك:

معلومات عمومية: يستخدم فيسبوك هذا المصطلح للدلالة على المعلومات التي تشاركها مع الجميع. **لا توجد إعدادات خصوصية لكل من أسم المستخدم، الصورة الشخصية، وأسماء الشبكات** ومتاحة للجميع رؤية هذه المعلومات.

الرؤية: ما هي المعلومات التي يمكن أن يراها الآخرون في ملفك الشخصي/صفحتك الرئيسية.

تذكر دائما أن هناك بعض المعلومات الخاصة بك التي يمكن أن يراها أي شخص حتى لو لم يكن صديقا أو مستخدِما مسجلا في فيسبوك.

الصفحات: تختلف صفحات فيسبوك عن الملفات الشخصية. فهي خاصة بغير المُستخدِمين مثل الشركات، والشخصيات العامة، والمنتجات، إلخ. وأيُّ شخص يمكنه أن يدخل الصفحات التي تتابعها (عندما تضغط على زر «أعجبني» «Like» أي عندما تصبح معجبا بهذه الصفحة) وإن لم يكن صديقا لك، مثل المُعلِنين، أو غيرهم.

الارتباطات: تنشأ بإبداء «الإعجاب» بصفحة (بالضغط على زر «أعجبني»). وهذه المعلومات تعتبر عمومية.

المكوّنات الاجتماعية الإضافية: هي أدوات بسيطة يتم «إسقاطها» على أي موقع لتمديد التجارب الاجتماعية على فيسبوك إلى مواقع أخرى. على سبيل المثال، إذا قمت بتسجيل الدخول إلى فيسبوك وكنت تتصفح موقع شبكة سي إن إن CNN.com، قد تشاهد زر «أعجبني» (Like) أو «توصية» Recommend بجوار المقال. إذا ضغطت على «توصية» مقال سي إن إن، سيُرسَل تنبيه إلى صفحة الأحداث في فيسبوك يتضمن رابطا إلى المقال. وإذا أشرت أنك تحب عنصرا بالضغط على «أعجبني»، يظهر خبر «أعجبني» في صفحة الأحداث وتُضاف كذلك إلى قسم «اهتماماتك ونشاطاتك» في ملفك الشخصي على فيسبوك.

التخصيص الفوري: يتيح لك الإطلاع على معلومات ذات صلة بأصدقائك لحظة وصولك إلى إحدى المواقع الإلكترونية الشريكة المحددة. توفر هذه المواقع الشريكة تجربة أكثر تخصصا قد تعجبك، ولكنها تسمح أيضا لهذه المواقع بالوصول إلى معلوماتك الشخصية. إذا كنت لا ترغب في استخدام التخصيص الفوري وإيقاف تشغيله، يجب عليك تعديل إعداداتك بصفحة إعدادات الخصوصية، التطبيقات والمواقع الإلكترونية ثم قم بإيقاف «تمكين التخصيص الفوري في المواقع الإلكترونية الشريكة» بالضغط على الخانة المجاورة.

الشبكات: لك الاختيار أن تلتحق بشبكة مدرسة أو مكان عمل على فيسبوك. ستكون إحدى الشبكات هي شبكتك الرئيسية ـ وهي عادةً الشبكة التي تشعر أنك أكثر ارتباطا بها. ستظهر شبكتك الرئيسية

إلى جوار اسمك وستؤثر في نتائج البحث التي تظهر أولا. يمكنك أن تتحقق من الشبكات التي انضممت إليها من خلال زيارة «الشبكات» في صفحة «إعدادات الحساب». وللالتحاق بشبكة، عليك ان تؤكد انتماءك لمدرسة أو معهد أو شبكة عمل من خلال عنوان إلكتروني موثق.

الخطوة ٢ **افهم جيدا المعلومات التي يجمعها فيسبوك عنك عندما تتفاعل مع المنصة.** اقرأ سياسة الخصوصية الخاصة بفيسبوك ودليل أدوات التحكم بالخصوصية.

وفقا لآخر سياسة خصوصية (بتاريخ ٢٢ ديسمبر/كانون الثاني ٢٠١٠)، فإن فيسبوك يجمع مجموعة متنوعة من المعلومات منها:

- معلومات عن النشاطات التي تقوم بها عندما تدخل إلى فيسبوك مثل إنشاء ألبوم صور أو إضافة صديق أو إبداء «الإعجاب» بمنشور صديق أو مشاركة فيديو.
- معلومات عن المكان الذي ترتبط منه بفيسبوك، سواء كان من حاسوب أو هاتف محمول، وبما في ذلك المتصفح الذي تستخدمه، مكان تواجدك وعنوانك IP.
- معلومات Cookie
- معلومات عن مستخدمين آخرين لفيسبوك الذين تتفاعل معهم؛ مثلا عندما يقوم صديق بالإشارة إليك في صورة لك.

الخطوة ٣ **افهم ما هي المعلومات التي يتم جمعها عنك من قبل أطراف ثالثة**، وما هي المعلومات التي يشاركها هؤلاء مع فيسبوك. الأطراف الثالثة هي مواقع أو تطبيقات تستخدمها عبر فيسبوك مثل الألعاب أو التطبيقات.

عندما تدخل إلى موقع أو تطبيق عبر منصة فيسبوك، يتلقى فيسبوك معلومات منهم بشأن أعمالك. وبإمكان فيسبوك أن يتلقى معلومات من شركاء مُعلِنين إذا تجاوبت مع الإعلانات التي تظهر على فيسبوك.

الخطوة ٤ إذا كنت تقيم في بلد يخضع فيه الأمن الخاص على الإنترنت إلى تهديد، تجنب استخدام صورتك في صورة صفحتك الرئيسية، ولا تعطي اسمك الكامل، و**سجل دائما خروجك عندما لا تستخدم الموقع**.

للتحكم في إعدادات الخصوصية لديك؟ سجل الدخول إلى فيسبوك. في الركن الأعلى من الصفحة إلى اليسار، اضغط على «الحساب» ثم على «إعدادات الخصوصية» ضمن القائمة المنسدلة.

تحت العنوان الأول، «التواصل في فيسبوك»، اضغط على رابط «عرض الإعدادات». ستظهر قائمة من الخيارات لتحديد أي معلومات ترغب في مشاركتها على فيسبوك ومع من تريد مشاركة هذه المعلومات.

إلى جوار كل عنصر، يظهر وصف وجيز، ثم **قائمة منسدلة حيث يمكنك تعيين خيارات خصوصيتك**.

لديك أربع خيارات: **الأصدقاء فقط** (فقط أصدقاؤك الذين توافق على إضافتهم يمكنهم رؤية هذه المعلومات)، **أصدقاء الأصدقاء** (أصدقاؤك على فيسبوك وأصدقاؤهم يستطيعون رؤية هذه المعلومات)، **الأصدقاء والشبكات** (أصدقاؤك على فيسبوك وأعضاء الشبكات التي التحقت بها)، **الجميع** (أي أحد على الإنترنت).

لديك أيضا خيار **تخصيص كل إعداد على حده بتعيين "تخصيص" ضمن القائمة المنسدلة**. هذه الإمكانية مفيدة إذا كنت ترغب في إخفاء محتوى بعينه عن شخص معين. في النافذة المنبثقة، يمكنك تخصيص خصوصية معلومة معينة بتعيينها لكي تظهر لعدد مختار من الأشخاص أو الشبكات التي

تريد أنت. ويمكنك أيضا أن تختار إخفاء هذه المعلومة عن مستخدمين معينين من فيسبوك سبق أن أضفتهم إلى قائمة أصدقائك فيسبوك.

وأخيرا، يمكنك كذلك أن تحدد للمعلومة خيار «أنا فقط»؛ يعني أن لا أحد ولا حتى أصدقاؤك قادر على رؤية هذه المعلومة المعينة. حدد خياراتك، ثم اضغط على «حفظ الإعداد» كي تعود إلى صفحة إعدادات الخصوصية الرئيسية.

في الصفحة الرئيسية لإعدادات الخصوصية، اضغط على "عرض الإعدادات" ثم على "معاينة صفحتي الشخصية" لكي ترى صفحتك الرئيسية كما ستبدو لأصدقائك في فيسبوك. هذه طريقة جيدة لكي تتحقق مرة ثانية من أنك حددت الإعدادات التي اخترت. وهناك موقع استعد خصوصيتك Reclaim Privacy الذي يوفر أداة مستقلة ومفتوحة المصدر تقوم بفحص إعدادات خصوصيتك على فيسبوك، ولكنها تظل ثمرة عمل تطوعي وبذلك ليست مضمونة التحديث.

إفادة !

تذكر أنه وإن لم يكن أحد سواك أنت قادر على رؤية بعض معلوماتك، فإن فيسبوك نفسه يظل قادرا على الوصول إليها ـ وهذا لا يعني أنهم يحتفظون بها لأنفسهم إذا ما طلبتها منهم حكومة. فقد تلقى تويتر مؤخرا استدعاء للمثول أمام المحكمة، ولم يكتفوا بأن تحدوا الهيئة بل أخبروا المستهدَفين أن معلوماتهم مطلوبة. طبعا هم في تويتر لم يكونوا مُجبَرين على فعل ذلك، ولا تستطيع أنت أن تفترض أن فيسبوك أو أي شركة غيرها ستفعل الشيء نفسه. ثم أنه كما حدث مؤخرا في بعض البلدان، قد تقبض عليك قوات الأمن وتجبرك على إفشاء كلمة سرك. في هذه الحالة، قد يدخلون إلى حسابك والوصول إلى أي معلومة مقترنة به مهما كانت إعدادات خصوصيتك. لذلك احرص قدر الإمكان على ألا تنشر إلا ما قل من المعلومات الحساسة على الموقع.

الخطوة 0

تحت العنوان الثاني، «المشاركة في فيسبوك»، **حدد خياراتك لمن يمكنه رؤية المعلومات التي تشاركها على فيسبوك**، بما فيها تحديثات حالتك وصورك ومنشوراتك، سيرتك والأقوال المفضلة، العائلة والعلاقات، الصور والفيديو التي تتم الإشارة إليك فيها ، الآراء الدينية والسياسية، تاريخ الميلاد، الحصول على إذن للتعليق على منشوراتك، والأماكن التي تدخلها باستعمال أماكن فيسبوك، ومعلومات الاتصال.

هنا أيضا، لديك خيار تحديد إعدادات المشاركة مع الجميع (جميع المستخدمين المسجلين في فيسبوك)، أصدقاء الأصدقاء أو الأصدقاء فقط. وثمة أيضا إعدادات يوصي بها فيسبوك، بالإضافة إلى إمكانية تخصيص إعدادات المشاركة الخاصة بك.

إنك إذ تخصص إعداداتك، تستطيع أن تحدد من يرى ويعلق على العناصر التي تشاركها والأشياء الموجودة على حائطك وتلك التي يُشار إليك فيها. هذا الخيار جميل لأنه يتيح لك أن تحدد من يرى ماذا لكل معلومة تشاركها على حده . ولديك أيضا خيار تحديد بعض أجزاء المعلومات في «أنا فقط»، يعني أن لا أحد غيرك سيرى هذه المعلومة. حاول أن تجرب وتعدل مختلف الإعدادات، ثم اضغط على «عودة إلى الخصوصية».

الخطوة 1

هل تريد التحكم في كيفية حصول التطبيقات والألعاب والمواقع على معلوماتك؟ انطلاقا من الحساب >> إعدادات الخصوصية >> انتقل إلى أسفل الصفحة >> تحت «التطبيقات والمواقع الإلكترونية» اضغط على «عدّل إعداداتك».

تصل التطبيقات تلقائيا إلى قائمة أصدقائك ولكل معلومة تختار أن تشاركها مع الجميع. انظر إلى قائمة إعدادات المعلومات التي تشارك مع التطبيقات وعدّل إعداداتك حسب خياراتك.

ولا بأس كذلك من **إزالة جميع التطبيقات التي لا تستخدمها.**

الخطوة ٧ **لا ترغب أن تكون صفحتك الشخصية على فيسبوك متاحةً لمحركات البحث عندما يبحث عنك الناس باسمك؟** اذهب إلى القائمة المنسدلة: الحساب >> إعدادات الخصوصية >> انتقل إلى أسفل الصفحة >> تحت «التطبيقات والمواقع الإلكترونية» اضغط على «عدّل إعداداتك». انتقل إلى أسفل الصفحة >> إلى جوار «البحث العام». اضغط على «تعديل الإعدادات» >> قم بإلغاء «تشغيل البحث العام» على الخانة المجاورة.

إفادة أخرى! استخدم هذه الصفحة المفيدة لكي تبحث عن معلوماتك في فيسبوك بواسطة غوغل.

الخطوة ٨ **هل ترغب بحظر شخص معين من الإطلاع على صفحتك، أو حظر استقبال دعوات التطبيقات والمناسبات من أحد الأصدقاء؟ بإمكانك ذالك عبر الذهاب إلى:**

الحساب >> إعدادات الخصوصية >> انتقل إلى أسفل الصفحة >> تحت «قوائم الحظر» اضغط على «تعديل القوائم الخاصة بك». أضف أسماء المستخدمين في خانة الخيارات التالية: «حظر المستخدمين»، «حظر دعوات التطبيقات»، و«حظر الدعوات إلى المناسبات».

الخطوة ٩ قد تكون بعض المعلومات الخاصة بك متاحة للتطبيقات والألعاب والمواقع عندما يستخدمها أصدقاؤك. لتعديل هذه الإعدادات، اذهب إلى:

الحساب >> إعدادات الخصوصية >> انتقل إلى أسفل الصفحة >> تحت «التطبيقات والمواقع الإلكترونية». اضغط على «عدّل إعداداتك» >> إلى جوار «المعلومات التي يمكن الوصول إليها عن طريق الأصدقاء» اضغط على «تعديل الإعدادات». ستظهر النافذة المنبثقة نوع المعلومات التي تود إتاحتها للتطبيقات والألعاب والمواقع الإلكترونية عند استخدام أصدقائك لها. قم بإلغاء نوع المعلومات التي لا تود أن تصل إليها تطبيقات أصدقائك على الخانة المجاورة لكل معلومة.

الخطوة ١٠ لا تنس أن تتحكم في إعدادات خصوصيتك عند نشر محتوى على الصفحة الشخصية للفيسبوك. في كل مرة تنشر فيها معلومة جديدة مثل تحديث الحالة، أو صورة، أو رابط، **لديك خيارات التحكم في من تود أن يطّلع على هذا المنشور**. وقبل نشر أي تحديث حالة أو رابطا أو أي شيء آخر، اضغط على الأيقونة التي تظهر في نهاية المربع لكي تحدد الأشخاص الذين بإمكانهم الإطلاع على هذا الموضوع.

الخطوة ١١ إذا كنت ترغب في حظر مُكوِّنات اجتماعية إضافية، قم بتنزيل قائمة خصوصية فيسبوك Adblock Plus

الخطوة ١٢ يتيح لك الأماكن خدمة تسجيل دخولك في مكان ما في العالم الواقعي ومشاركة مكان تواجدك مع الأصدقاء. كما باستطاعة أصدقائك على فيسبوك الإشارة إليك في الأماكن التي تتواجدون فيها معاً.

إذا كنت لا تود أن يُدخلك أصدقاؤك في "الأماكن"، عليك تعطيل هذه الإمكانية عبر الذهاب إلى:
الحساب >> إعدادات الخصوصية >> انتقل إلى أسفل الصفحة >> «المشاركة في فيسبوك» اضغط على «تخصيص الإعدادات» >> «تضميني في «أشخاص هنا الآن» بعد دخولي»، قم بإلغاء الخانة المجاورة «تمكين».

الخطوة ١٣ عليك أن تحمي رؤية ألبومات صورك الموجودة على فيسبوك، لكل ألبوم على حده. اذهب إلى صفحة إعدادات الخصوصية للصور ومقاطع الفيديو لكي تحدد يدويا إعدادات الخصوصية/الرؤية لكل ألبوم موجود على حده.

الخطوة ١٤ يقوم فيسبوك دائما بتغيير مكونات الخصوصية لا سيما عندما يصدر منتجا جديدا أو خدمة جديدة. تأكد دائماً من الإطلاع على هذه التغييرات وأخذ الوقت الكافي لمراجعة إعدادات خصوصيتك بشكل منتظم.

الخطوة ١٥ **شارك أصدقاءك بمعرفة كيفية حماية أنفسهم أيضا بشكل أفضل على فيسبوك.** شاركهم النصائح حول طريقة تعديل إعدادات خصوصيتهم. هل لديك إفادة خاصة للحفاظ على خصوصيتك على فيسبوك؟ شاركها في قسم التعليقات!

الخطوة ١٦ **حفظ نسخة من محتواك واتصالاتك في فيسبوك بشكل منتظم هي فكرة جيدة**. فبهذه الطريقة، إذا حدث أن قمت بخطأ تعطيل حسابك أو تم تعطيله نتيجة خرقك شروط خدمة الشركة، تكون على الأقل محتفظا بنسخة من معلوماتك (بما فيها الصور والرسائل ومنشورات الحائط وقائمة الأصدقاء).

للحصول على نسخة من معلوماتك، اذهب إلى : الحساب >> إعدادات الحساب >> تنزيل معلوماتك >> اضغط على «لمعرفة المزيد» ثم اضغط على زر «تنزيل». ستنبثق نافذة بمعلومات إضافية. اضغط على «تنزيل» مرة أخرى. ستتوصل ببريد إلكتروني عندما يصبح أرشيفك جاهزا للتنزيل في شكل مستند مضغوط. قد يتطلب جمع الصور ومنشورات الحائط والرسائل وغيرها من المعلومات بعض الوقت. الأفضل الاحتفاظ بالمعلومات الحساسة (مثلا معلومات الاتصال) بأقل ما يمكن على الموقع كله. لماذا يا ترى؟ لأن كلمة سرك قد تتعرض للسرقة أو يتعرض حسابك للاختراق، وعندئذ لا فائدة من أي إعدادات خصوصية كانت لديك.

الخطوة ١٧ هل تشعر بالقلق إزاء خصوصيتك على فيسبوك ولكنك لا تريد حذف حسابك؟

يحاول بعض المستخدمين استخدام «الخروج الخارق»، أي أن في كل مرة تنتهي من استخدام فيسبوك، **قم بتعطيل حسابك**. وإذا أردت العودة إلى فيسبوك في أي وقت بعد تعطيل حسابك، قم بإعادة تنشيط حسابك بواسطة تسجيل الدخول باستخدام بريدك الإلكتروني وكلمة السر. هذه الطريقة لا تحذف حسابك. فبتعطيل حسابك، تختفي صفحتك الشخصية وجميع المعلومات المقترنة بها من خدمة فيسبوك. بالإضافة إلى ذلك، لن يتمكن مستخدمي فيسبوك من البحث عنك أو عرض أي من معلوماتك.

لتعطيل حسابك: اذهب إلى: الحساب >> «إعدادات الحساب» ثم إلى أسفل الصفحة اضغط على «التعطيل» >> في الصفحة التالية، أدخل السبب ثم اضغط على «تأكيد». بإمكانك إعادة تنشيط حسابك كاملا بواسطة تسجيل الدخول باستخدام بريدك الإلكتروني وكلمة السر.

كلمات السر

كما يشير هذا المقال من بي بي سي «**أغلب كلمات السر التي يختارها الناس تعتمد على عناصر عامة وغالباً تكون سهلة الكشف**. وتكفي معرفة بعض المعلومات عن شخص ما، مثل أسماء أفراد عائلته وأصدقائه، وأسماء كتبه وأفلامه المفضلة، ومكان الإقامة، لتكون أدلة كافية لتخمين كلمة السر الخاصة بهذا الشخص. يعتبر اختيار كلمة السر الضعيفة من أحد أسهل الطرق لكي تصبح معلوماتك وحسابك غير محصنين على الإنترنت. وبالمقابل، فإن اختيار كلمة السر القوية والمنيعة هو أحد أبسط الخطوات لتقوية حمايتك على الإنترنيت.

إن اختراق كلمة السر، هي عملية تشغيل برامج الكمبيوتر ضد كلمة السر المُشَفَّرة لكشفها، لهو أسهل بكثير مما كنت تعتقد. والبرامج التي تشغل كل كلمة في قائمة القاموس أو قائمة مفردات ضد اسم مستخدم هي أيضا شائعة. لذلك لن تضمن تماما أن حسابك محميّ من المخادعين (راجع إفاداتنا أدناه لتفادي خداع التَّصيُّد) إلا أن هناك بعض الخطوات التي يجب ألا تغفل عنها.

الخطوة ١ أول خطوة في إنشاء كلمات السر القوية هو **معرفة كيف تبدو كلمات السر الواهية**. كلمة السر الواهية تستخدم معلومات شخصية، مثل اسمك أو تاريخ ميلادك أو أسماء أفراد عائلتك أو اسم حيوانك الأليف. كلمات السر من هذا النوع، سهلة التخمين على شخص يعرفك.

إفادة ! لا تخطر ببالك أي فكرة أصيلة؟ قلق لأن كلمة سرك ليست قوية بما فيه الكفاية؟ حاول استخدام **مولِّد كلمة السر القوية التلقائي** مثل هذا التطبيق. هناك مجموعة متنوعة من مولدات كلمات السر التلقائية ـ استعمل غوغل وحاول أن تجد ما يناسبك.

الخطوة ٢ استعمل «جُمَل السر» بدل «كلمات السر». واحرص على أن تكون «جمل السر» قوية: جمل السر شبيهة كثيرا بكلمات السر، ولكنها عادةً ما تكون أطول وأكثر تعقيدا؛ بحيث إذا كانت كلمة السر تتكون من ستة أحرف، فإن جملة سر تتكون على الأقل من عشرين إلى ثلاثين حرفا.

الخطوة ٣ تعلّم كيف تجعل كلمة سرك قوية ومنيعة. تكون كلمة السر المنيعة أكثر أمانا ويصعب تكسيرها لأنها **أصلية ومعقدة وعشوائية**. كلمة السر القوية هي كذلك كلمة طويلة، **عدد حروفها لا يقل عن ٧ إلى ١٤ حرفا وهي حروف مختلفة ومتنوعة**، مثل :

- الحروف الكبيرة A-Z
- الحروف الصغيرة a-z
- الأرقام ٠-٩
- الرموز ~!@#$%^&*()_-+={[}]\|:;"<>,.?/

الخطوة ٤ فكر في جملة سر قوية. أولا، فكر في بضع الكلمات أو أي جملة تخطر في ذهنك ـ قد تكون شيئا عشوائيا تماما. ثم **غير بعض الحروف** إلى حروف كبيرة وأضف بعض الأرقام والرموز وعلامات التنقيط بشكل عشوائي (وليس فقط في نهاية الجملة). **ولا بأس أيضا من وضع رقم أو رمز مكان حرف**، مثل استعمال الرقم ٣ عوض الحرف E.

مثلا، يصبح عنوان الأغنية «All you need is love» هو "\ALuN##d5V/.!." . ولا تنس أن تتعلم كيف تستخدم Diceware لكي تبتكر جملة سر قوية ومنيعة.

الخطوة ٥ **تحقق من مناعة كلمة سرك** عبر أداة اختبار مايكروسوفت التالية. اكتب كلمة سرك في الخانة، سيضيء الشريط الموجود تحتها مبينا قوة كلمة السر. ينبغي أن تكون القوة على الأقل Medium أي متوسطة. ثم استمر في تعديل كلمة سرك إلى أن تصبح قوية.

الخطوة ٦ اختر كلمة السر خاصة بحسابك تقتصر على فيسبوك فقط ولا تستخدمها لجميع المواقع لأنه ليس آمناً.

إفادة ! يقدم برنامج Keepass إدارة مجاني ومفتوح المصدر لكلمات السر، يسهّل عليك الوصول إلى مختلف كلمات سرك. فهو يخزّن كذلك جميع كلمات سرك في قاعدة بيانات عالية الأمان مقفلة بمفتاح واحد رئيسي أو مستند مفتاح. لن تقلق بعد الآن بشأن أي كان يريد أن يصل لكلمات سرك.

الخطوة ١٠ **إفادات أخرى:**

- **لا ترسل أبدا كلمة سرك إلى أي أحد بالبريد الإلكتروني.**
- لا تشارك كلمة سرك مع الآخرين.
- غيّر كلمة سرك كل ٣-٦ أشهر.
- **تحاشى قدر الإمكان أن تكتب كلمة سرك على حاسوب عمومي. وإذا كان لابد من ذلك، فعليك أن تغير كلمة سرك بانتظام أكبر.**
- إذا كنت تستخدم فيرفوكس، ضع كلمة سر رئيسية
- لا تقع ضحية للتَّصَيُّد

ما هو التَّصَيُّد ؟

الخطوة ١ ـ **تحقق من عنوان صفحة فيسبوك**. سجل الدخول إلى فيسبوك دائما عبر اسم النطاق الشرعي https://www.facebook.com . لا تسجل دخولك لفيسبوك إذا كان اسم النطاق مشابها ولكنه مختلف.

قد تدرج بعض المواقع المخادعة مفردة فيسبوك facebook قبل اسم نطاق .com ويسمى هذا اسم نطاق فرعي. على سبيل المثال: يبدو اسم النطاق التالي شرعيا facebook.com.profile.a340ah3.com ولكنك إذا دققت النظر، ستجد أن اسم النطاق هو في الواقع com.a٣٤٠ah٣ وليس facebook.com.

الخطوة ٣ **إذا كنت تعتقد أن هناك من يتصيد حسابك أو إذا تلقيت رابطا أو رسالة أو منشورا أو نافذة منبثقة تبعث على الريبة وتظنهم يتصيدون:**

- **أبلغ الأمر** لفيسبوك بإرسال رسالة إلكترونية إلى privacy@facebook.com . زُرْ مركز المساعدة على فيسبوك لتحصل على المزيد من المساعدة بشأن حسابك.
- **لا تضغط على أي رابط** منشور أو متضمن في رسالة.
- **لا ترسل أبدا معلومات حساسة** مثل كلمة السر أو معلومات عن بطاقتك المصرفية أو معلومات شخصية عنك عن طريق رسالة من فيسبوك.
- **بادر في الحين بتغيير كلمة سرك**. تعلم كيف تنشئ كلمات السر وجمل السر القوية والمنيعة هنا.
- إذا كان المنشور أو الرسالة من صديق لك على فيسبوك، **اتصل بهذا الشخص** في الحين وأخبره أن حسابه لم يعد آمنا. وكذلك الأمر إذا كانت الرسالة أو المنشور من شركة أو مؤسسة تتبعها على فيسبوك.
- شارك كل ما تعلمته الآن مع جميع أصدقائك.

الخطوة ٢ **اتخذ الخطوات اللازمة لحماية نفسك ضد تصيد فيسبوك مستقبلا:**

- تذكر دائما تشغيل التصفح الآمن. لقد وجد الخبراء في حالة تونس أن جافاسكريبت المدمج يظهر فقط عندما يُسجَّل الدخول إلى فيسبوك عن طريق http عوض عن https، مما يدل على أهمية التصفح الآمن بواسطة https كلما دخلت مواقع التواصل الإجتماعي.

- تأكد دائما من أنك تدخل فيسبوك من اسم نطاق شرعي.

الخطوة ٤ إذا كنت قد أعطيت معلومات شخصية للغير وظننت أنك وقعت ضحية تصيد، استشر مجموعة عمل مكافحة التصيد حول ما عليك فعله.

إخفاء الهوية

الخطوة ١ يتضمن بيان الحقوق والمسؤوليات الخاص بفيسبوك، سياسة استخدام الأسم الحقيقي ومنع المسجلين من استخدام أسماء مستعارة. ولكن الواقع أن العديد من الناس يستخدمون أسماء مستعارة.

إن ملاحقة الموقع لهؤلاء المستخدمين عشوائية وتعسفية. لذا، إذا أنشأت حسابا في فيسبوك باسم مزيف، احرص على ألا تفضح نفسك واستخدم اسما مستعارا مقنعا بدل اسم مستعار من كلمة واحدة. والأهم من ذلك، لا بد لك من خطة عمل بديلة في حال تعرض حسابك للتعطيل. ضمن خطة عملك، عليك أن تقرأ بعناية بيان الحقوق والمسؤوليات. **لكي تكون على دراية إذا ما أخللت بها أم لا**. واطلع على كيفية تبليغ الإخلال بشروط الخدمة (بواسطة المستخدمين الآخرين، والتي يمكن أن يساء استخدامها). إذا لم يكن لديك الوقت لذلك، اتصل بمن قرأ الشروط ولديه الوقت والإمكانية للاتصال مباشرة بفيسبوك نيابةً عنك جرب info@movements.org.

الخطوة ٢ إن سرية الهوية لا تقتصر على الاسم واللقب فحسب.

ما هي المعلومات الأخرى التي قد تعرّف بك؟ هل رقم هاتفك عمومي؟ هل هناك صورة قرب مكان مشار

إليه جوار مكان سكنك؟ (**قبل أي شيء عليك أن تتجنب استخدام صورك الحقيقية على صفحتك الشخصية**). وماذا عن الأشخاص الذين صادقتهم؟ الارتباط الوثيق في فيسبوك بشخص قُبِض عليه بسبب نشاطه السياسي أو متورط مع مجموعة لا تريد أن تُقرَن بها، قد يسبب لك مشاكل. لذلك كن حذرا بشأن من تصادق وألقِ نظرة على من ترتبط بهم بواسطة أدوات تتيح لك تحليل شبكاتك ـ مثلا Friend Wheel أو Social Graph. إذا حيرتك إعدادات الخصوصية على فيسبوك، تذكر أنك دائما قادر على معاينة صفحتك الرئيسية كما ستبدو للآخرين وما هي المعلومات المعروضة، وذلك بالذهاب إلى «الحساب»، ثم «إعدادات الخصوصية»، ثم «تخصيص الإعدادات» ثم معاينة صفحتي الرئيسية» (انظر الى الصورة التالية)».

الخطوة ٢ إن نصائح التصفح دون الكشف عن الهوية تنطبق على استخدام فيسبوك، راجع إذن الأدلة التالية:

١. التدوين دون الكشف عن الهوية بواسطة برنامج تور Tor
٢. استخدام جيميل بأمان
٣. استخدام الهاتف المحمول بأمان
٤. حماية هويتك أثناء تصفح الويب باستخدام هوتسبوت شيلد Hotspot Shield
٥. عزز أمانك على هاتف أندرويد بتثبيت برنامج تور Tor

تم تصميم و ترجمة
هذا الكتيب إلى العربية
من قبل منظمة
SMEXbeirut
www.smex.org
منظمة سمكس بيروت هي منظمة إجتماعية في بيروت متخصصة بالتدريب و الإستشارة على الاستعمال الاستراتيجي للإعلام الاجتماعي في لبنان و الدول العربية