cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

العدد ٤

نوفمبر/تشرين التاني ٢٠١٢

كل شيئ عن أمن الفيسبوك

- وجهاً لوجه مع فيسبوك
- تخطي الرقابة
- كيفية إنشاء كلمات سرٍّ والحفاظ عليها

cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي

٢ مقدمة

٣ ملخص عن استبيان فيسبوك

٤ قصة عبد الله كابوس على فيسبوك

٥ وجهاً لوجه مع فيسبوك

١٥ فايبر غير آمن

١٧ الشبكات الإخبارية المناطقية وسبل تحسينها

١٩ نقاط التفتيش في البحرين: سباق بين مغردي تويتر وأجهزة الأمن

٢١ إضافات المتصفح

٢٣ جراء نسخ احتياطي سينك توي

٢٥ تخطي الرقابة

٢٧ بدائل عن غوغل بلاي ستور

٣١ إنشاء موقع الإنترنت الخاص بكم

٣٤ التخزين السحابي

٣٦ كيفية إنشاء كلمات سرٍّ والحفاظ عليها

للإتصال بنا:

magazine@cyber-arabs.com

تابعنا على:

أخرج المجلة:

MGSA

لصالح شركة:

tm

مقدمة

سوزان فيشر

لقد أصبح جزءاً من حياتنا؛ أداة نخوض من خلالها النضال. يساعدنا على التواصل مع أحبائنا البعيدين أو حتى أولئك الذين يسكنون بالقرب منا. نتشارك من خلاله الأخبار والصور والأفكار والمخاوف والآمال، وأحياناً أيضاً الحزن والغضب.

لقد أصبح فيس بوك منذ وقت طويل أكثر من مجرد شبكة تواصل اجتماعي.

ولكننا ننسى حين ننغمس في نشر صورنا والتعليق على أخبار أصدقائنا، أو مشاركة الروابط لمقالات على الإنترنت، أن فيس بوك، وقبل كل شيء، شركة تجارية تريد، لا بل تحتاج إلى، جني المال. ولقد أصبح هذا الأمر ملحاً أكثر منذ أن أصبح فيس بوك شركة عامة مسجلة في سوق الأسهم.

فيس بوك إذاً يحتاج إلى جني الأموال، ولكن كيف تفعل هذه الشركة ذلك؟ إن عنصر القوة الأبرز الذي يعتمد عليه موقع فيس بوك هو البيانات التي يملكها، وهي بيانات تتعلق بنا. هذه المعلومات نقوم بمشاركتها طواعية مع فيس بوك، وهي مرتبطة بما يعجبنا وما لا يعجبنا؛ أين نقضي أوقات فراغنا وكيف نصرف أموالنا. هذه المعلومات قد لا نفصح عنها إذا قام أحد مندوبي أحد شركات التسويق بطرق بابنا، ولكننا نقدم الكثير منها مجاناً عبر فيس بوك دون التفكير ولو للحظة بالمصير الذي ستؤول إليه.

لا أحد يعرف فعلياً ما الذي يحل بكل البيانات التي يجمعها فيس بوك. هل يمكنني أن أتأكد أن الصور التي أشاركها مع أصدقائي لن يتم استعمالها في إعلانات تجارية؟ والأهم من ذلك، كيف يمكنني أن أتأكد أن المعلومات حول شبكة أصدقائي لن تقع في الأيدي الخاطئة؟

لقد أصبح فيس بوك خلال السنتين الماضيتين أداة لنشطاء الديمقراطية حول العالم، وهي غاية لم يفكر بها مؤسسو فيس بوك عندما أنشؤوا منصة التواصل الإجتماعي هذه. ماذا يعني هذا الأمر بالنسبة إلى فيس بوك والقواعد التي تحكم استخدامه؟

أسئلة عدة تتراكم كانت وراء قرار فريق سايبر آرابز تخصيص العدد الرابع من المجلة لفيس بوك. في هذا العدد يحلل فريق سايبر آرابز التضارب بين كون فيس بوك شركة تجارية من جهة، واحتياجاتنا كمستخدمي الموقع من جهة أخرى. لقد سألكم فريق سايبر آرابز، بصفتكم مستخدمي فيس بوك، عن تجربتكم مع الموقع والتدابير الإحتياطية التي تتخذونها لحفظ أمنكم. أيضاً في هذا العدد من المجلة، نروي قصة ناشط دخل السجن بعد أن تم تعليق حسابه في فيس بوك. وكما جرت العادة، نقدم لكم النصائح حول أفضل الطرق لاستعمال موقع فيس بوك بشكل آمن حتى تتمكنون من مشاركة لحظاتكم المميزة وأفكاركم المهمة مع أصدقائكم دون الوقوع في المتاعب.

وبالطبع، يتطلع فريق سايبر آرابز إلى حصول صفحة الموقع على فيس بوك على إعجابكم.

سوزان فيشر – مديرة برنامج الشرق الأوسط لدى «معهد صحافة الحرب والسلام» (IWPR)

ملخص عن استبيان فيسبوك

قام فريق سايبر آرابز باستبيان حول الإجراءات التي يتبعها مستخدمو فيس بوك العرب، وقد كانت النتائج مثيرة للإهتمام. بينما صرح ١٨ بالمئة فقط ممن اشترك في الإستطلاع عن اعتقادهم أنهم قد خرقوا الشروط التي يفرضها فيس بوك، كانت إجابة أكثر من نصف المشتركين أنهم يستعملون هوية مزيفة، وهو أمر يمنعه موقع فيس بوك بشكل واضح؛ لقد شهد أناس عديدون تعطيل حساباتهم بسبب خرقهم هذه القاعدة.

أفادت إجابات نسبة كبيرة من المشتركين، ٧٧ بالمئة، أنهم قاموا بالتبليغ عن مستخدمين آخرين لخرقهم قواعد فيس بوك، كما صرح ثلث المشتركين أنهم تأثروا بقواعد فيس بوك الصارمة. ولكن الملفت كان أن نصف المشتركين أقروا أنهم لم يطلعوا على هذه القواعد. تظهر نتائج الإستبيان وجود التباس حول ما هو مسموح أو ممنوع فعله أثناء استخدام موقع فيس بوك.

أما فيما يتعلق بالإجراءات الخاصة بالأمان، فقد ظهر أن معظم المشتركين في الإستبيان هم على علم بها. فلقد صرّحوا كلهم، تقريباً، أنهم يقومون بإخفاء لوائح أصدقائهم، كما لا يسمح معظم المشتركين للآخرين بالإشارة إليهم في الصور أو المنشورات دون موافقتهم. ويقوم ثلث المشتركين بمشاركة أنواع مختلفة من المحتوى مع لوائح مختلفة من الأصدقاء. وقد صرح ٤٠ بالمئة من المشتركين أنهم قد اتخذوا إجراءات احترازية لحماية حساباتهم في حال تم اعتقالهم، مثل مشاركة تفاصيل الخاصة بإدارة صفحاتهم مع أصدقاء مقربين.

إلا أن هناك مجالاً لتحسين جوانب الأمان هذه، إذ صرح ثلث المشتركين أنهم يستخدمون الإنترنت في مقاهٍ عامة وهي، وفي بلد مثل سوريا، غالباً ما تخضع للمراقبة من قبل الحكومة، كما أنّ معظم الذين أجابوا عن الأسئلة لا يضعون قيوداً على إمكانية نشر أي محتوى على حائطهم، ومعظمهم يقبلون طلبات الصداقة المرسلة من قبل أشخاص لا يعرفونهم.

في هذا العدد من مجلة سايبر آرابز نستقصي كيف يقوم فيس بوك بالتعامل مع خصوصيتكم ونعرض عليكم بعض الطرق السهلة لجعل فيس بوك أكثر أماناً.

قصة عبد اللّه

كابوس على فيس بوك

في مظاهرة جرت في أحد أيام الجمعة في ضواحي دمشق، أجابت قوات الأمن على النداءات المطالبة بالحرية بوابل من الرصاص. تمكن عبد اللّه وأصدقاؤه من الهرب من الموت ولكن غيرهم لم يحالفه الحظ. قتل يومها خمسة أشخاص وجرح كثيرون آخرون.

قرر عبد اللّه أن يعبر عن غضبه مما حدث عبر فيس بوك، فكتب على صفحته على الموقع في تلك الليلة: «إن كان هذا ما يريده اللّه لنا، فإنه ليس أفضل من الرئيس بكثير.»

في الصباح التالي حاول عبد اللّه أن يطّلع على رسائله على فيس بوك، ولكنه فوجئ بالعبارة التالية: «لقد تم تعطيل حسابك.» حاول عبد اللّه أن يدخل إلى حسابه مجدداً، ظناً منه أنه أدخل كلمة السر بشكل خاطئ. ولكن بعد خمس محاولات، تأكد عبد اللّه أنّ حسابه قد تم تعطيله فعلاً. ما لم يعرفه عبد اللّه هو أنّ بعضاً من «أصدقائه» – الكثير منهم لم يعرفوه بشكل شخصي – قاموا بالتبليغ عن صفحته لكونه ينشر «خطاب الكراهية».

بعض الذين اطلعوا على منشوره اعتبروه مهيناً لدينهم، وقد أخذ فيس بوك بلاغهم بشكل جدي.

ولكي يتمكن من إعادة تفعيل حسابه، طُلب من عبد اللّه الإجابة عن سلسلة من الأسئلة، كما طُلب منه إرسال نسخة عن جواز سفره، وككثير من السوريين، لم يكن عبد اللّه يملك واحداً. قام عبد اللّه بإرسال نسخة عن جواز سفر أخيه من مقهى إنترنت مستعملاً جهاز «سكانر».

ولكن لسوء حظ عبد اللّه، لم تكن هذه نهاية مشاكله مع فيس بوك. في ذلك المساء، جرى توقيف عبد اللّه من قبل أجهزة الأمن تحت تهمة إضعاف سلطة الدولة، وقد تمت مواجهته بمعلومات تتعلق بصفحته على فيس بوك، من ضمنها النسخة عن جواز سفر أخيه التي أرسلها من بريده الإلكتروني في مقهى الإنترنت.
أطلق سراح عبد اللّه بعد خمسة أيام من دون توجيه أي تهم إليه. لم يتمكن عبد اللّه من استرجاع حسابه على فيس بوك، واضطر إلى إنشاء واحد جديد.

حقائق حول فيس بوك info box

إن فيس بوك ليس شفافاً فيما يتعلق بإجراءات إبطال الحسابات. يقدم بيان الحقوق والواجبات الخاص بفيس بوك بعض الإشارات إلى الأمور التي تعتبر غير قانونية، ولكن صيغة البيان تفتح المجال أمام التفسيرات. (https://www.facebook.com/legal/terms)

كشف مسح سريع أجراه فريق سايبر آرابز أن الكثير من الصفحات المرتبطة بالربيع العربي تحتوي على مواد تعتبر «غير قانونية» وقد يتمكن البعض من التبليغ عنها. لذا فقد قام الكثير من الناس باستغلال هذه النقطة لقمع بعض الآراء.

إن استعمال الإنترنت في المقاهي ليس آمناً على الإطلاق؛ في الكثير من البلدان يُطلب من أصحاب المقاهي تنصيب برمجيات للتجسس بالإضافة إلى مراقبة رواد المقهى. إذا كنتم بحاجة إلى استعمال الإنترنت لإيصال معلومات حساسة، تأكدوا أنكم تقومون بذلك من جهاز حاسوب موثوق وفي بيئة آمنة.

وجهاً لوجه مع فيس بوك

منذ بدء ما اصطلح على تسميته بـ«الربيع العربي» في كانون الأول/ ديسمبر ٢٠١٠، عمد الناشطون في أكثر من بلد إلى استعمال فيس بوك لتنظيم صفوفهم والتواصل وإثارة الوعي حول قضاياهم، كرد على محاولات حكوماتهم فرض القمع والرقابة. وبسبب التأثير الذي نتج عن فيس بوك، فقد ذهب بعض الخبراء إلى حد القول إن الإنتفاضات الشعبية في دول مثل تونس ومصر وسوريا لم تكن ممكنة الحدوث دون فيس بوك. ومهما يكن دور فيس بوك في الربيع العربي، يبقى الواقع أن ملايين الناس يضعون ثقتهم فيه كل يوم، وهم غالباً ما يفعلون ذلك من دون التفكير بالعواقب المحتملة.

وبالرغم من ثبوت نجاح فيس بوك كأداة لتشارك المعلومات والتواصل ونشر قضايا معينة، إلا أن الموقع لم يتم إنشاؤه لهذه الغايات. يملك موقع فيس بوك على قيمة صافية تبلغ خمسين مليار دولار وعائد سنوي يبلغ حوالي أربعة مليارات دولار، مما يجعل فيس بوك يظهر بوضوح أنه من أبرز الشركات المسجلة في مؤشر ناسداك للبورصة المهتمة بجني الأموال من مستخدمين مثلكم ومثلي. كما أن فيس بوك ليس مؤسسة ديمقراطية. في الواقع، فإن قوانين استعمال فيس بوك يتم سنها من قبل الإدارة حصراً وليس هناك من طرق للتأثير في سلوك الشركة إلا من خلال شراء الأسهم.

بالطبع، إن نجاح الشركة يحركه خدمة (بعض) مصالح مستخدميه. ولكن هذه المصالح، وإن كانت ترضي فئة واسعة من الناس، قد لا تتطابق مع ما يريده مستخدمون معيّنون. وبالتالي، فقد شهد العديد من المستخدمين إزالة صور أو مقاطع فيديو كانوا قد نشروها لمجرد أنها تخرق قوانين فيس بوك، وقد قام فريق سايبر آرابز بتوثيق بعض الحوادث المماثلة؛ فهناك مستخدمون خسروا القدرة على دخول حساباتهم بسبب خرقهم أحد شروط استخدام فيس بوك، وقد أتت بعض هذه الحالات بنتائج مدمرة على هؤلاء الناس. بالإضافة إلى ذلك، يقوم فيس بوك باستعمال بياناتكم في سبيل الكسب المادي دون أن يضطر إلى طلب إذن واضح منكم، وقد شكّل ذلك مضايقات للعديد من الناشطين في المنطقة.

بالرغم من مواطن الضعف هذه الذي يشكو منها فيس بوك، فإن الموقع لا يزال أداة رائعة، لا سيما في غياب البديل الأفضل. إلا أنه من الأفضل استعمال فيس بوك بحكمة وأخذ القضايا المتعلقة بالأمان بعين الإعتبار. سيشير هذا المقال إلى بعض المسائل التي ينبغي عليكم التنبه إليها أثناء استعمال فيس بوك. ستجدون في هذا المقال بعض النصائح والحِيل التي تمكنكم من جعل فيس بوك أكثر أمناً.

حددوا غايتكم من استعمال فيس بوك

يرتبط أمنكم أثناء استعمال فيس بوك، قبل كل شيء، بالهدف من وراء استعمالكم الموقع. إذا كنتم تستخدمون فيس بوك لأغراض غير سياسية، مثل التفاعل مع مجموعة من الأصدقاء المقربين، فعلى الأرجح لن تكونوا هدفاً مفضلاً لأجهزة الإستخبارات، أما إذا كنتم تستعملون فيس بوك لدعوة الجمهور إلى الإشتراك في المظاهرات، فكونوا واثقين أنكم ستجذبون الكثير من الإهتمام إلى أنفسكم.

عملياً، قلما يفرق الناس بين الأمور العامة أو السياسية والأمور الخاصة. ما قد يعد في مناطق مختلفة من العالم شأناً خاصاً يعد في العديد من الدول العربية شأناً سياسياً، وما قد يعد شأناً عاماً قد يكون شأناً خاصاً. لذا من المفيد التنبه إلى المخاطر التي تخوضونها عندما تخلطون بين هذه الشؤون في صفحتكم على موقع فيس بوك. ففي بعض بلدان الخليج العربي، تسبّب النقر على زر «الإعجاب» على صفحات معادية للدين بمتاعب لأشخاص عدة. وفي سوريا من المعروف أنه تم استجواب أشخاص بسبب التعبير عن «إعجابهم» بصفحات الثورة، بما في ذلك الثورات في دول أخرى. ولهذا السبب من الأفضل أن تجعلوا حسابكم على فيس بوك مجهول الهوية أو تقوموا بفتح حساب آخر للقيام بنشاطات أكثر خطورة.

غالباً ما تكون المخاطرة جزءاً من إعلان الرأي بشكل علني والمحاولة لتغيير الأنظمة من حولكم، إلا أنه يبقى من الحكمة أن تأخذوا حذركم عند القيام بعمليات تواصل علنية وأن تقوموا بنشاطكم على فيس بوك بطريقة منظمة تحفظ أمنكم. سنريكم لاحقاً كيف تقومون بتحديد مجموعات معينة من الناس يكون باستطاعتها الإطلاع على نشاطات محددة تقومون بها.

الأمور التي يتوجب تجنبها عند استعمال فيس بوك

كما ذكرنا سابقاً، فإن فيس بوك ليس ملاذاً آمناً تستطيعون فعل ما شئتم على صفحاته. فلقد وضع فيس بوك قواعد صارمة يؤدي خرقها إلى مسح بعض المحتوى في حسابكم أو حتى تعليق الحساب. لا تفكروا أن هذا لن يحصل معكم، فقد سبق أن حصل مع العديد من النشطاء من قبل. يمكن الإطلاع على القواعد التي

يتوجب عليكم اتباعها أثناء استعمال فيس بوك هنا:
http://www.facebook.com/legal/terms

وبشكل عام، ننصح قراءنا الإلتزام بالتالي:

• يطلب منكم فيس بوك أن تستعملوا أسماءكم كاملةً وإلا قام بإغلاق حسابكم. إذا أردتم أن تبقوا هويتكم مجهولة، لا تقوموا باستعمال اختصارات لأسمائكم الحقيقية مثل «سميرة ن.» أو «س.ن.» إستعملوا أسماءً كاملة مستعارة عوضاً عن ذلك.

• يمنع فيس بوك الخطاب الذي يدعو إلى الكراهية وتهديد الآخرين وإظهار العري، كما يمنع الصور ومقاطع الفيديو التي تظهر «عنفاً مجانياً» أي التي يكون هدفها إظهار العنف من دون أي مبرر (البند ٣,٧). وقد تم إغلاق عدة حسابات تحت حجة أنها توجه الإهانة إلى الذات الإلهية أو لتقديمها صوراً ومقاطع فيديو تظهر أعمال عنف أو آثار تلك الأعمال، أو توجيه التهديد إلى جهة ما أو حتى نشر صور لنساء يرضعن أطفالهنّ.

• يمنع فيس بوك مستخدميه من استعمال الموقع لأداء نشاط غير قانوني، أو مخادع أو خبيث أو يتصف بالتمييز (البند ٣,١٠). يأخذ فيس بوك القانون الأميركي معياراً لتحديد ما الذي يعد خرقاً للقانون.

• يمنعكم فيس بوك من إرهاب أي مستخدم أو مضايقته (البند ٣,٦). ومع أن هذه النقطة تطال القادة السياسيين، فإن فيس بوك قد أظهر تساهلاً فيما يخصها. ولكن يجب أن تعلموا أن باستطاعة أي شخص، بما في ذلك القادة السياسيين، أن يتقدم بشكوى بهذا الخصوص. وقد نتج عن هذا الأمر حجب بعض الصفحات أو إزالتها بشكل كلي.

• يمنعكم فيس بوك من نشر أي محتوى يشكل تعدياً على حقوق الآخرين أو خرقاً للقانون بأي شكل من الأشكال (البند ٥,١). وقد تم تطبيق هذه القاعدة بشكل خاص فيما يتعلق بحقوق النشر.
يطبّق القيمون على فيس بوك قوانين الموقع إما عبر فحص عشوائي، أو عبر فحص آلي منتظم للمنشورات التي تضعونها على صفحتكم. بالإضافة إلى ذلك، يمكن للمستخدمين الآخرين أن يتقدموا بشكوى بشأن أي محتوى تقومون بنشره ولا يعجبهم. ستجدون زراً في الزاوية اليسرى العليا للمنشور يتيح لكم التبليغ عنه. إذا توفر عدد كافٍ من الشكاوى حول محتوى المنشور، قد يقوم فيس بوك بإزالته أو تعليق حسابكم. ومن المعروف أن فيس بوك يأخذ المسائل المتعلقة بالدين، بشكل خاص، على محمل الجد.
إذا تم تعليق حسابكم ستتلقون رسالة من فيس بوك تبلغكم كيف تعيدون تفعيله. لسوء الحظ، يطلب فيس بوك منكم في أغلب الأحيان أن تعرّفوا عن أنفسكم عبر إرسال نسخة من بطاقة هويتكم أو جواز سفركم. إن كنتم لا تملكون وسيلة لإثبات هويتكم أو استعملتم بطاقة مزيفة، فستواجهون مشكلة.

ما هي المعلومات التي يشاركها فيس بوك؟

لقد تم تصميم فيس بوك ليكون أداة تسمح لكم بمشاركة أفكاركم وصوركم ومقاطع الفيديو الخاصة بكم، وهو أداة تؤدي هذه المهمة بشكل ممتاز. إذا كنتم لا ترغبون بمشاركة كل المعلومات التي تخصكم مع الجميع، فإن فيس بوك يسمح لمستخدميه بتغيير إعدادات حساباتهم لكي يقرروا بالضبط المحتوى الذي يريدون أن يشاركوه مع الآخرين. إلا أنكم لن تكونوا دائماً الطرف الذي يقرر طبيعة هذا المحتوى.

عندما تفتحون حساباً في فيس بوك، فإنكم تعطون الموقع ترخيصاً غير حصري ويخضع لإمكانية الترخيص الفرعي، يمكن منحه لطرف آخر ومن دون أن يكون لكم الحق في إيراد مادي من الملكية على أي شيء تقومون بنشره على فيس بوك، وذلك من دون أخذ الإذن المسبق منكم. هذا منصوص عليه في البند الثاني من قواعد فيس بوك. قد يبدو ذلك غريباً، إلا أن هذا البند في الحقيقة هو صلب النموذج الذي يتبعه فيس بوك في الأعمال، أي استعمال المعلومات عنكم لجني الأموال. من المستبعد أن يقوم فيس بوك باستعمال المعلومات المتعلقة بكم لأهداف سياسية أو تزويد حكوماتكم بها، ولكن، بالرغم من ذلك، قد تقعون في مشاكل.

لقد تم استعمال صفحات وصور من فيس بوك لأغراض تجارية في الماضي، ومؤخراً بدأ فيس بوك بإظهار صفحات «تم الإعجاب بها» في الشريط الإخباري («آخر الأخبار»). لا يشكل ذلك خطراً، ولكن بما أن هذه التحديثات تحتوي على «إعجابات» أبداها مستخدمون آخرون وقاموا بإخفائها عن الجمهور قد يكون ذلك قد تسبب بإفشاء معلومات من المفروض ألا تنكشف على الملأ.

يحق لفيس بوك أن يغيّر الطريقة التي يقدم بها المعلومات والبيانات الخاصة بكم دون الحصول على إذن مسبق منكم. وينطبق هذا الأمر بشكل خاص على المعلومات التي قمتم بوضعها على صفحتكم ولم تجعلوها مقتصرة على مجموعة محدودة من الأشخاص.

إجراءات حماية أساسية في فيس بوك

لدى استخدام فيس بوك، ينبغي اتباع التدابير نفسها التي تختص بالأمان التي تتبعونها لدى استعمال تطبيقات الإنترنت الأخرى. لقد ناقشنا في الأعداد السابقة من مجلة سايبر آرابز كما على الموقع التدابير التي ينبغي اتباعها عند ولوج الإنترنت. عند استعمال فيس بوك، يجب التنبه بالأخص لما يلي:

• لا تدعوا متصفح الإنترنت يحفظ كلمة السر الخاصة بحسابكم، لا سيما إذا كنتم في مقهى إنترنت. لدى رؤية السؤال «هل تودون أن يحفظ [إسم المتصفح] كلمة السر الخاصة بكم» أجيبوا دائماً بـ «لا».

• سجلوا خروجكم من الحساب بعد كل مرة تستعملون فيها فيس بوك. يتحاشى العديد من الناس تسجيل الخروج من حسابهم لكي لا يضطروا إلى تسجيل الدخول كل مرة. بينما يوفر ذلك بعض الوقت، إلا أنه يعد تدبيراً غير آمن. لقد تلقى فريق سايبر آرابز عدة تقارير عن حالات تم فيها النفاذ إلى معلومات على فيس بوك بسبب هذا الأمر.

• تفادوا استعمال فيس بوك في الأماكن العامة. قد تكون أجهزة الحاسوب في مقاهي الإنترنت مزودة براصد لوحة المفاتيح (Keylogger) بالإضافة إلى برمجيات تجسس أخرى تتيح لطرف ثالث الدخول إلى حسابكم في وقت لاحق، وقد يكون ذلك مفروضاً من قبل الحكومة.

• تفادوا ذكر تاريخ ميلادكم ومسقط رأسكم على فيس بوك، إذ قد يتم استعمال هذه البيانات للولوج إلى حساب البريد الإلكتروني الخاص بكم عبر خيار إنشاء كلمة سر جديدة.

هناك خطر أمني لا يفكر به معظم الناس وهو أنكم قد تعرّضون سلامة الأشخاص الآخرين للخطر من خلال النشاطات التي تقومون بها. بما أن فيس بوك هو شبكة تجمع الناس بعضهم ببعض، فإنكم تتحملون جزءاً من المسؤولية فيما يتعلق بحماية الأشخاص الذين يقعون ضمن شبكتكم. إن كنتم ناشطين في المجال السياسي، عليكم التنبه للتالي:

• تحاشوا ذكر أسماء أصدقائكم دون الحصول على إذنهم
• إحرصوا على إخفاء لائحة أصدقائكم

في البلدان التي تحكمها أنظمة سلطوية، جرت العادة أن تطّلع السلطات الأمنية على شبكة المعارف الخاصة بالأشخاص الذين يخضعون للتوقيف. لذا، تذكروا دائماً أنكم لستم مسؤولين عن أمنكم الخاص فحسب، بل أنتم مسؤولون أيضاً عن أمن الأشخاص الذين تعرفونهم.

تهيئة حساب فيس بوك

يمكنكم أن تحسنوا من مستوى الأمان والخصوصية في فيس بوك بشكل كبير عبر تغيير بعض الإعدادات في حسابكم. لسوء الحظ، قد يكون القيام بهذه العملية أمراً مزعجاً. سنشير إلى التغييرات الأكثر الإفادة لقراء سايبر آرابز.

ا. زيادة مستوى الأمان العام في حسابكم

في بادئ الأمر، من المهم أن تستعملوا فيس بوك في ظروف آمنة. هذه الظروف لا علاقة لها بإعدادات فيس بوك. تتضمن البيئة الآمنة أموراً مثل تفادي استعمال فيس بوك في مقاهي الإنترنت، بالإضافة إلى تسجيل الخروج من حسابكم لدى الإنتهاء واستعمال اتصال آمن بشبكة الإنترنت. هناك أمور ننصح بها بشكل دائم على موقع سايبر آرابز من أجل التمتع ببيئة آمنة، إلا أنّ هناك بعض الإجراءات التي يوفرها فيس بوك والتي يمكن أن تستفيدوا منها لزيادة مستوى الأمان.

ا-ا إستعمال فيس بوك من خلال اتصال مشفر

يقدم فيس بوك إمكانية استعمال الموقع من خلال اتصال مشفر عبر بروتوكول SSL (يعرف أيضاً بـ HTTPS). من الصعب اختراق بيانات الإتصال الذي تستعملونه للولوج إلى حساب فيس بوك الخاص بكم إذا كنتم تستعملون بروتوكول SSL (مثلاً إتصال واي فاي). من المثير للإستغراب أن فيس بوك قد قام بتعطيل هذا الخيار في الإعدادات القياسية (Standard) ولكن من حسن الحظ أنه من السهل إعادة تشغيل هذا الخيار.

ا. أنقروا على المثلث الموجه نزولاً في الجهة اليسرى بجانب إسمكم وزر الصفحة الرئيسية. ستظهر قائمة منسدلة. إضغطوا على «إعدادات الحساب»

٢. في العمود الأيمن، إختاروا «الأمان»

٣. أنقروا على زر «التصفح الآمن»، ثم اختاروا « تصفح فيس بوك عبر اتصال آمن (https) عندما يكون ذلك ممكناً» ثم أنقروا على «حفظ التغييرات»

٢-١ معرفة من دخل حسابكم

في القائمة نفسها (إعدادات الحساب < الأمان) ستجدون خياراً مفيداً آخر وهو «إشعارات تسجيل الدخول». يفترض فيس بوك أنكم تدخلون حسابكم دائماً من جهاز الحاسوب نفسه، إلا أنه إذا قمتم بتفعيل الخيار المذكور وغيرتم الجهاز الذي تستعملونه، أو إذا قام شخص آخر بدخول حسابكم، ستتلقون رسالة إلكترونية أو رسالة نصية قصيرة عبر الهاتف لتحذيركم. لتفعيل هذا الخيار عليكم فعل التالي:

١. النقر على زر «إشعارات تسجيل الدخول»
٢. إختيار البريد الإلكتروني أو الرسائل النصية SMS أو كليهما ومن ثم النقر على «حفظ التغييرات»

في حال اخترتم أن يتم إنذاركم عبر رسالة نصية، يجب أن تعلموا أن هذه الخدمة غير متوفرة في جميع البلدان. في سوريا مثلاً تم حجب هذه الخدمة بسبب الحظر الإقتصادي الأميركي المفروض على البلاد، كما أن التواصل عبر الرسائل النصية ليس آمناً.

٢. التحكم بما يمكن للآخرين أن يروه على التسلسل الزمني لأحداثكم

التسلسل الزمني للأحداث (Timeline) في فيس بوك هو قناة الإتصال الأساسية بينكم وبين كل من أصدقائكم وبقية العالم. لذا، فإنه من المهم أن تعرفوا كيف تتحكمون بما يظهر في التسلسل الزمني وأن تعوا ما الذي يمكن أن يطلع عليه الآخرون.

٢-١ تصميم التسلسل الزمني أو البروفايل

قوبلت ميزة التسلسل الزمني التي أدخلت إلى فيس بوك العام الماضي بالإعجاب والإنتقاد على حد سواء. لقد حسّن هذا التصميم الجديد من قدرة المستخدمين على تغيير شكل صفحتهم مما يسهل عليهم تكييفها لكي تخدم قضية معينة. إلا أن التسلسل الزمني ظهر أقل تنظيماً وشفافية، إذ تخفي هذه الميزة الكثير من التفاصيل التي كانت تظهر في التصميم القديم (البروفايل). على سبيل المثال، إذا قمتم بإزالة «الإعجاب» من التسلسل الزمني على صفحتكم قد يظهر هذا الإعجاب مجدداً إذا قمتم بالعودة إلى التصميم القديم (البروفايل). إذا كنتم تستعملون التسلسل الزمني وتودون رؤية التفاصيل التي تظهر في البروفايل القديم، يمكنكم أن تحمّلوا إضافة صغيرة تسمى «time line remove» [http://www.timelineremove.com/] تمنحكم هذه الإضافة خيار رؤية التسلسل الزمني على صفحتكم بحسب التصميم القديم وإجراء التغييرات الضرورية لتحسين إعدادات الأمان أو الخصوصية.

٢-٢ حددوا من باستطاعته رؤية منشوراتكم

في بعض الأحيان قد لا ترغبون في مشاركة صورة أو رسالة ما مع جميع أصدقائكم. يتيح لكم فيس بوك إمكانية مشاركة الأشياء مع مجموعة محددة من الأشخاص عوضاً عن مشاركتها مع الجميع.

يمكنكم أن تخلقوا لائحة جديدة كل مرة تقومون فيها بنشر شيء ما أو يمكنكم أن تخلقوا لائحة ثابتة. سنشرح في المقطع ٢,٣ كيف تقومون بخلق لائحة ثابتة. إذا قمتم بمشاركة صورة أو رسالة ما مع مجموعة من الأشخاص، تذكروا أن هؤلاء الأشخاص قد يقومون بدورهم بنشر هذا المحتوى، وقد يطلع عليه أشخاص آخرون لا تودون أن تطلعوهم على هذا المحتوى.

١. أنقروا على المثلث المتجه نحو الأسفل بجانب الحدث/المنشور الموجود في التسلسل الزمني على صفحتكم أو بجانب الزر «نشر» بجانب الفراغ الخاص بتحديث الحالة

٢. إختاروا «مخصصة» في حال كانت المجموعات المذكورة غير محددة بشكل كاف

٣. أ- إذا كنتم تريدون أن تستثنوا بعض الأشخاص من رؤية منشوركم قوموا بإدخال أسمائهم.
ب- إذا أردتم أن تختاروا بعض الأشخاص فقط للسماح لهم برؤية المنشور يمكنكم أن تختاروا «هؤلاء الأشخاص أو هذه القوائم» تحت «جعل هذا المحتوى مرئياً لـ» ومن ثم إدخال أسماء الأصدقاء الذين ستسمحون لهم برؤية هذا المحتوى.

٤. أنقروا على «حفظ التغييرات»
لاحظوا أنه عندما تقومون بحفظ التغييرات الخاصة بالنشر سيتم تطبيق الإعدادات نفسها على المنشورات التي تلي بشكل تلقائي. في حال لم ترغبوا في تطبيق هذه الإعدادت قوموا بإعادة الإعدادات إلى ما كانت عليه.

٢-٣ خلق لوائح أصدقاء لنوع مخصص من التواصل

إذا أردتم أن تشاركوا محتوى معين على فيس بوك مع مجموعة محدودة من الأشخاص فمن المفيد أن تنشئوا لوائح تحت عنوان «أشخاص موثوقون» أو «أجانب» أو «مواطنون» أو «صحافيون». بهذه الطريقة يمكنكم أن توجهوا اتصالكم نحو مجموعات محددة. مشاركة محتوى ما مع مجموعة معينة تتم عبر الإجراءات المذكورة في الفقرة ٢-٢.

١. توجهوا إلى الصفحة الرئيسية على فيس بوك، التي تعرف أيضاً بـ«آخر الأخبار».
٢. أنقروا على «أصدقاء» في العمود على الجهة اليمنى من الصفحة أو إفتحوا الصفحة التالية:
https://www.facebook.com/bookmarks/lists

٣. أنقروا على «إنشاء قائمة»
٤. أدخلوا إسماً خاصاً بالقائمة إلى جانب "List name"
٥. أدخلوا أسماء الأشخاص الذين تودون وضعهم على القائمة في الحقل بجانب كلمة «الأعضاء»
٦. أنقروا على «Create»

٢-٤ رؤية ما يراه الآخرون

من المفيد أحياناً أن تطّلعوا على ما يراه الآخرون في التسلسل الزمني الموجود على صفحتكم. على سبيل المثال، قد تودون التحقق مما إذا كان الأشخاص الذين قمتم باستثنائهم من رؤية منشور معين فعلاً لا يمكنهم أن يروا هذا المنشور أو قد تودون الإطلاع على المنشورات التي يتمكن الجميع من رؤيتها. يتمتع فيس بوك بميزة تتيح لكم رؤية صفحتكم كما يراها الآخرون.

١. توجهوا إلى التسلسل الزمني على صفحتكم
٢. أنقروا على المثلث الموجه نزولاً بجانب زر «سجل النشاطات» في أعلى يسار شاشة التسلسل الزمني للأحداث

٣. أنقروا على «عرض ك». سيظهر التسلسل الزمني الخاص بكم كما يظهر لأشخاص هم ليسوا أصدقاءكم (كما يراه الجمهور).

٤. في الزاوية اليسرى من الشاشة، أدخلوا إسم أحد أصدقائكم ثم إضغطوا على مفتاح .Enter سيظهر التسلسل الزمني الآن كما يظهر لهذا الصديق.

٢-٥ إخفاء المنشورات الظاهرة في التسلسل الزمني

قد ترغبون في بعض الأحيان في ألا يرى الناس نشاطات معينة في التسلسل الزمني الخاص بكم، أو قد ترغبون في إخفاء بعض المنشورات التي أبديتم إعجابكم بها. إن إخفاء أمر ما في التسلسل الزمني أو حذفه كلياً هو في غاية السهولة. عليكم أن تعرفوا أنكم إذا قمتم بإخفاء أمر ما سيبقى بمقدور الأشخاص الآخرين أن يروه؛ سيختفي من التسلسل الزمني الخاص بكم فقط.

١. حركوا مؤشر الفأرة فوق التسلسل الزمني للأحداث الخاص بكم إلى أن يظهر رمز قلم رصاص. أنقروا على قلم الرصاص.
٢. أنقروا على «إخفاء من التسلسل الزمني للأحداث» لإخفاء أمر ما أو «حذف» لإزالته كلياً.

إذا رغبتم أن تتأكدوا أن المنشور المخفي أو المحذوف قد أصبح غير مرئي بشكل كلي، قد يكون من الأسهل العودة إلى تصميم البروفايل القديم الذي يعطي منظوراً أكثر شفافية فيما يتعلق بالمنشورات المخفية أو المحذوفة. يتوفر شرح حول كيفية العودة إلى التصميم القديم في الفقرة ٢-١.

٣. تقييد تفاعل الأشخاص الآخرين مع صفحتكم

لا يجب أن تنتبهوا فقط لتفاعلكم مع صفحتكم، بل ينبغي أيضاً أن تنتبهوا للطريقة التي يتفاعل بها الآخرون معها. حسب إعدادات فيس بوك القياسية يمكن لأصدقائكم أن ينشروا أشياءً على صفحتكم والإشارة إليكم (Tag) في الصور من دون إذنكم. لذا ينصحكم فريق سايبر آرابز أن تراقبوا حسابكم بقدر الإمكان. لضبط الإعدادات المتعلقة بالطريقة التي يتفاعل بها الآخرون مع صفحتكم توجهوا إلى «إعدادات الخصوصية» واتبعوا الخطوات التالية:

١. أنقروا على المثلث الموجه نزولاً في الزاوية اليسرى بجانب زر «الصفحة الرئيسية» ثم أنقروا على «إعدادات الخصوصية»

تأكدوا أنكم قد اخترتم «الأصدقاء». غيروا هذا الخيار إلى «العامة» فقط إذا أردتم أن يرى كل الناس، الأصدقاء منهم وغير الأصدقاء، أن يروا محتوى صفحتكم. في الأقسام التالية سنفترض أنكم بقيتم ضمن «إعدادات الخصوصية» (الخطوة ١).

٣-١ الحد من الإشارة

في الإعدادات القياسية في فيس بوك، يمكن لأي من أصدقائكم أن يشير إليكم (Tag) في صورة أو رسالة أو منشور سياسي. سيظهر ذلك على حائطكم مع إشارة ضمنية إلى أنكم توافقون على ذلك، حتى إذا لم تكونوا قد رأيتم هذا المحتوى. لتلافي هذا الأمر، يمكنكم أن تغيّروا إعدادات فيس بوك لجعله يرسل إليكم طلباً للمراجعة

قبل أن يظهر أي منشور يتضمن إشارة إلى إسمكم على حائطكم ويتمكن أصدقائكم من رؤيته.

٢. أنقروا على «تعديل الإعدادات» إلى جانب «اليوميات والإشارة»

٣. أنقروا على «مراجعة الإشارات التي يضيفها أصدقاؤك إلى منشوراتك في فيس بوك»
٤. أنقروا على المثلث الذي يظهر في الجهة اليسرى واختاروا «ممكّنة» ثم أنقروا على «عودة»
٥. أنقروا على «مراجعة الإشارات التي يضيفها أصدقاؤك إلى منشوراتك في فيس بوك»
٦. أنقروا على المثلث الذي يظهر في الجهة اليسرى واختاروا «ممكنة» ثم أنقروا على «عودة»
٧. أنقروا على «تم»

٣-٢ منع الأشخاص من ترك رسائل على صفحتكم

في إعدادات فيس بوك القياسية، يمكن لأي كان أن ينشر رسالة أو صورة على حائطكم، وستتم مشاركة هذا المنشور مع جميع أصدقائكم. لمنع الأشخاص من التفاعل مع صفحتكم بهذه الطريقة، قوموا بتعطيل هذه الميزة التي تسمح للآخرين بالنشر على حائطكم.

٢. أنقروا على «تعديل الإعدادات» خلف «اليوميات والإشارة»
٣. خلف «من يمكنه النشر على التسلسل الزمني للأحداث الخاص بك؟» إختاروا «لا أحد»

٣-٣ منع الآخرين من إيجادكم على فيس بوك

بحسب الإعدادات القياسية يمكن لأي أحد أن يجد إسمكم أو رقم هاتفكم أو عنوان بريدكم الإلكتروني على فيس بوك. يمكن أن تكون هذه الميزة مفيدة، إلا أنكم في بعض الحالات قد لا ترغبون في أن يجدكم أحد على فيس بوك. إذا أردتم أن تكونوا خارج دليل فيس بوك إفعلوا ما يلي:

٢. أنقروا على «تعديل الإعدادات» خلف «كيفية التواصل»
٣. أضبطوا خيار «من يستطيع البحث عنك باستخدام عنوان البريد الإلكتروني أو رقم الهاتف الذي أدخلته؟» على «أصدقاء» أو «أصدقاء الأصدقاء»

٣-٤ حظر المستخدمين

إذا أردتم أن تمنعوا شخصاً ما من الإتصال بكم أو إيجادكم على فيس بوك، يمكنكم وضع هذا الشخص على «قائمة الحظر». سيقوم فيس بوك بوقف كل أشكال التفاعل بينكم وبين هذا الشخص عندما تطبقون هذا الحظر.

٢. أنقروا على «إدارة الحظر» خلف «الأشخاص المحظورون والتطبيقات المحظورة»
٣. أدخلوا عنوان البريد الإلكتروني أو إسم المستخدم الخاص بهذا الشخص في أحد الحقول تحت «حظر المستخدمين» ثم أنقروا على

«حظر»

٣-٥ تقييد بعض الأصدقاء

يمكنكم أن تضعوا بعض الأصدقاء على «قائمة المقيّدين»، مما يعني أنه سيكون بمقدورهم أن يروا فقط الرسائل والصور التي تشاركونها مع الجميع (العامة). هذا الخيار لا ينطوي على الدرجة نفسها من المنع التي ينطوي عليها خيار الحظر؛ سيبقى بمقدوركم أن تتبادلوا الإتصال مع هذا الشخص، إلا أنه سيتم منعه من التفاعل مع دائرة أصدقائكم المقربين على فيس بوك ورؤية الرسائل التي من المفترض أن يراها هؤلاء الأصدقاء فقط. بهذه الطريقة يمكنكم أن تخلقوا مستويين من التواصل مع الأصدقاء: أصدقاؤكم الحقيقيون وباقي الناس.

٢. أنقروا على «إدارة الحظر» خلف «الأشخاص المحظورون والتطبيقات المحظورة»
٣. أنقروا على عبارة «تعديل القائمة» المكتوبة باللون الأزرق تحت «إضافة أصدقاء إلى قائمة المقيّدين»
٤. أضيفوا أسماء أصدقائكم إلى القائمة من خلال البحث والنقر على «الانتهاء»

٤. استخدام المجموعات لتفاعل أكثر خصوصية

يمنح فيس بوك مستخدميه القدرة على إنشاء مجموعات. ويمكن اعتبار المجموعات جزءاً منفصلاً من فيس بوك يتمكن عدد محدود من الناس من النفاذ إليه. يمكنكم مشاركة الروابط والتعليقات والمناقشات ضمن المجموعة، مثلما تفعلون مع جميع أصدقائكم عبر خدمة التسلسل الزمني للأحداث/ آخر الأخبار الخاصة بكم .يمكن للمجموعة أن تكون «مفتوحة»، «مغلقة» أو «سرية». إذا كنتم ترغبون في أن تكون المجموعة سرية تماماً ولا يمكن الوصول إليها إلا من قبل أعضائها، يجب انتقاء الخيار «سرية».

١. إنتقلوا إلى «آخر الأخبار» على فيس بوك.

٢. في العمود الأيمن، أنقروا على «إنشاء مجموعات» أو ببساطة

إطبعوا: www.facebook.com/groups

ستظهر النافذة التالية:
٣. أكتبوا «اسم المجموعة» في الخانة المخصصة لها وأضيفوا أسماء الأعضاء (يمكنكم أيضاً إضافة الأشخاص في وقت لاحق.)

٤. إختاروا مستوى الأمان الخاص بمجموعتكم. إذا كان لا ينبغي للغرباء أن يطلعوا على محتوى التفاعل في المجموعة، نوصي باختيار «سرية». أنقروا على «إنشاء».
٥. أصبحت مجموعتكم الآن جاهزة. كما ترون، تشبه المجموعة ميزة التسلسل الزمني للأحداث/آخر الأخبار ولكن مع بعض القيود. يمكنكم إضافة تعليقات وصور وطرح الأسئلة ورفع الملفات. وكل ما تفعلونه ضمن المجموعة يبقى داخلها. إذا كنتم قد اخترتم أن تكون المجموعة سرية، لن يكون أحد قادراً على رؤية ما يحدث ضمنها، أو حتى يعرف أنها موجودة.

٥. حماية حسابكم وأصدقائكم

الأمر الذي غالباً ما ينساه الناس هو مسؤوليتهم في حماية أمن الآخرين عبر الإنترنت. يصبح هذا الأمر مهماً بشكل خاص إذا كنتم تنشرون مواداً تعتبر غير قانونية في بلدكم. غالباً ما يتلقى فريق سايبر آرابز تقارير من أشخاص تم استجوابهم عن أصدقائهم أثناء الإعتقال. حصلت أيضاً حالات أجبر خلالها الناس على تزويد أجهزة الأمن بكلمة السر الخاصة بهم. إذا كنتم لا تأخذون الإحتياطات اللازمة، يمكن لحساب فيس بوك الخاص بكم أن ينقلب ضدكم وضد أصدقائكم في حال ساءت الأمور. سوف نناقش في هذا القسم ما يمكنكم القيام به لمنع ذلك.

٥-١ إخفاء قائمة الأصدقاء

من المنطقي البدء بإخفاء قائمة أصدقائكم. مع الإعدادات القياسية، تظهر قائمة الأصدقاء لكل من يصادقكم. ولكن يمكنكم إخفاؤها عن الأنظار ببضع نقرات. تذكروا أن الناس سيبقون قادرين على رؤية ردود فعل أصدقائكم على منشوراتكم، ولكن هذا يقع ضمن مسؤولياتهم.

١. إذهبوا إلى التسلسل الزمني للأحداث وانقروا على «أصدقاء». سيتم تحويلكم إلى قائمة الأصدقاء الخاصة بكم.

٢. أنقروا على زر التعديل وغيروا خيار المتعلق بمن يستطيع رؤية لقائمة لـ «أنا فقط»

يرجى الإنتباه لكون هذا الخيار لا ينطبق على الأصدقاء الذين تشاركونهم مع الآخرين هؤلاء ستظل أسماؤهم ظاهرة.

٥-٢ عنوان البريد الإلكتروني الثاني

إذا كنتم في وضع حرج حيث لا تقدرون على النفاذ إلى حسابكم (إذا تم اعتقالكم، على سبيل المثال) فإنه من المفيد أن يكون هناك شخص تثقون به وتتشاركون معه تفاصيل هذا الحساب. عند الطوارئ، يمكن لهذا الشخص تغيير كلمة المرور الخاصة بكم، تعطيل حسابكم، حذف الرسائل الحساسة أو إخطار أصدقائكم بما حدث لكم. للقيام بذلك، من المفضل إضافة عنوان بريد إلكتروني ثانٍ إلى حسابكم، وذلك على النحو التالي:

١. أنقروا على المثلث المتجه نزولاً في بجانب اسمكم وزر الصفحة الرئيسية في القائمة التي ستظهر أنقروا على «إعدادات الحساب»
٢. انقر على «البريد الإلكتروني»
٣. انقروا على «إضافة بريد إلكتروني آخر»
٤. أدخلوا عنواناً ثانياً للبريد الإلكتروني وانقروا على «حفظ التغييرات»

يمكنكم تسجيل الدخول بواسطة كافة عناوين البريد الإلكتروني التي قدمتموها في فيس بوك. بالطبع، من الضروري أن يكون الشخص الذي لديه حق النفاذ إلى حسابكم موضع ثقة. هناك طريقة جيدة لتشارك المسؤولية وهي أن تتولوا المسؤولية نفسها تجاه هذا الشخص. لقد منعت هذه الطريقة من تدهور الأمور من سيء إلى أسوأ بالنسبة إلى عدة أشخاص اتصل بهم فريق سايبر آرابز.

٥-٣ تعطيل حسابكم في حالة الطوارئ

في بعض الحالات قد يكون من الضروري تعطيل حسابكم. في العديد من مناطق النزاع، يقوم الناس بذلك كإجراء احترازي في حال جرى اعتقالهم. عند تعطيل حسابكم، لن يتمكن أحد من رؤية أي شيء على صفحتكم، كما لو لم تكونوا أعضاء في فيس بوك. لن يتم حذف حسابكم بشكل نهائي، إذ لا يمكن تنفيذ هذه العملية بالنقر على زر واحد. إذا قمت بتسجيل الدخول بعد تعطيل حسابكم، سيتم تلقائياً تفعيله مرة أخرى. لن يتم فقدان أي شيء.

١. أنقروا على المثلث المتجه نزولاً بجانب إسمكم وزر الصفحة الرئيسية. في القائمة التي ستظهر، أنقروا على «إعدادات الحساب»
٢. في العمود الأيمن، إختاروا «الأمن»
٣. أنقروا على عبارة «تعطيل الحساب» المكتوبة باللون الأزرق واتبعوا الخطوات التي تظهر على الشاشة

في حال كنتم ترغبون في حذف الحساب بالكامل، يمكنكم الدخول إلى العنوان التالي بعد تسجيل دخول في فيسبوك:
https://www.facebook.com/help/delete_account
لا تتم هذه العملية بنقرة واحدة، إذ يطلب منكم فيس بوك الإجابة عن عدة أسئلة قبل حذف حسابكم بشكل دائم.

٦. منع فيس بوك من مشاركة موقعكم

قام فيس بوك العام الماضي، بدون سابق إنذار، بإدخال خدمة تسمح بمشاركة موقع المستخدمين. يجري الكشف عن موقعكم لدى القيام بأي تحديث، وعند استخدام هاتف محمول يتمتع بنظام تحديد المواقع GPS، تصبح هذه الخدمة دقيقة للغاية. قد تبدو هذه الميزة ممتعة، ولكن بعض قراء سايبر آرابز أشاروا إلى أنها عرضتهم لمخاطر. إذا كنتم لا تريدون للناس أن يعرفوا موقعكم، قوموا بتعطيل هذه الخدمة.

حركوا مؤشر الفأرة فوق الخانة الخاصة بتحديد المكان وانقروا على «X» بعدها لن يتم ذكر موقعكم أثناء أي نشاط مستقبلي.

إذاغيرتم رأيكم فيما بعد، فقط انقروا على علامة الموقع ودخلوا مكانكم يدوياً، ولكن تنبهوا لكون موقعكم سيظهر بعدها مع كل نشاط (إلا إذا قمتم بإيقاف الخدمة مرة أخرى). يمكنكم أيضاً حذف موقعكم في وقت لاحق.
في تطبيق فيس بوك الخاص بالهواتف المحمولة في هواتف أبل وأندرويد يمكنكم إيقاف تعطيل ميزة تحديد الموقع في فيس بوك كلياً من خلال الذهاب الى إعدادات <خدمات الموقع.

٧ . إحذروا تطبيقات فيس بوك

يسمح فيس بوك باستخدام تطبيقات طوّرها طرف ثالث. تبدو هذه التطبيقات وكأنها جزء لا يتجزأ من فيس بوك، ولكنها في الواقع أدوات منفصلة تقوم بالنفاذ إلى بياناتكم الخاصة في فيس بوك. الوظائف التي تنفذ إليها هذه التطبيقات تشمل البيانات الشخصية وقوائم الأصدقاء والقدرة على وضع رسائل على التسلسل الزمني للأحداث الخاص بكم.

عند استخدام التطبيق، يسألكم فيس بوك إذا ما كنتم تريدون منح الإذن للتطبيق بالوصول إلى البيانات الخاصة بكم. للأسف، يقوم الكثير من الناس بالموافقة على ذلك من دون قراءة هذا الشرح. قد تفقدون السيطرة على ما يحل ببياناتكم الخاصة، ومن الممكن أيضاً أن يتم إزعاج أصدقائكم برسائل ترويجية يتم وضعها بشكل تلقائي على التسلسل الزمني للأحداث الخاص بكم دون علمكم.

يوجد مصدر قلق آخر وهو أنكم باستخدام التطبيقات، يمكنكم زيادة عدد الشركات التي تتمكن من النفاذ إلى البيانات الخاصة بكم؛ هناك حالات معروفة جرى فيها تسريب بيانات خاصة بسبب استخدام التطبيقات. وعلاوة على ذلك، لا يتحكم فيس بوك بهذه التطبيقات حيث لا تنطبق شروط فيس بوك عليها، فلذلك يعود أمر التحقق من إعدادت الخصوصية إلى المستخدمين.
لهذه الأسباب، نحن لا نشجع قراءنا على استخدام تطبيقات فيس بوك إذا كانوا يخشون على خصوصيتهم.
أما أولئك الذين يصرون على استخدام هذه التطبيقات، فنوصيهم باستخدام التطبيق التالي:
https://apps.facebook.com/privacyscoreapps
يقوم هذا التطبيق بتقييم مستوى الخصوصية في تطبيقات فيس بوك عبر إعطاء كل منها علامة لمنحكم فكرة عن مدى سلامة استخدامها.

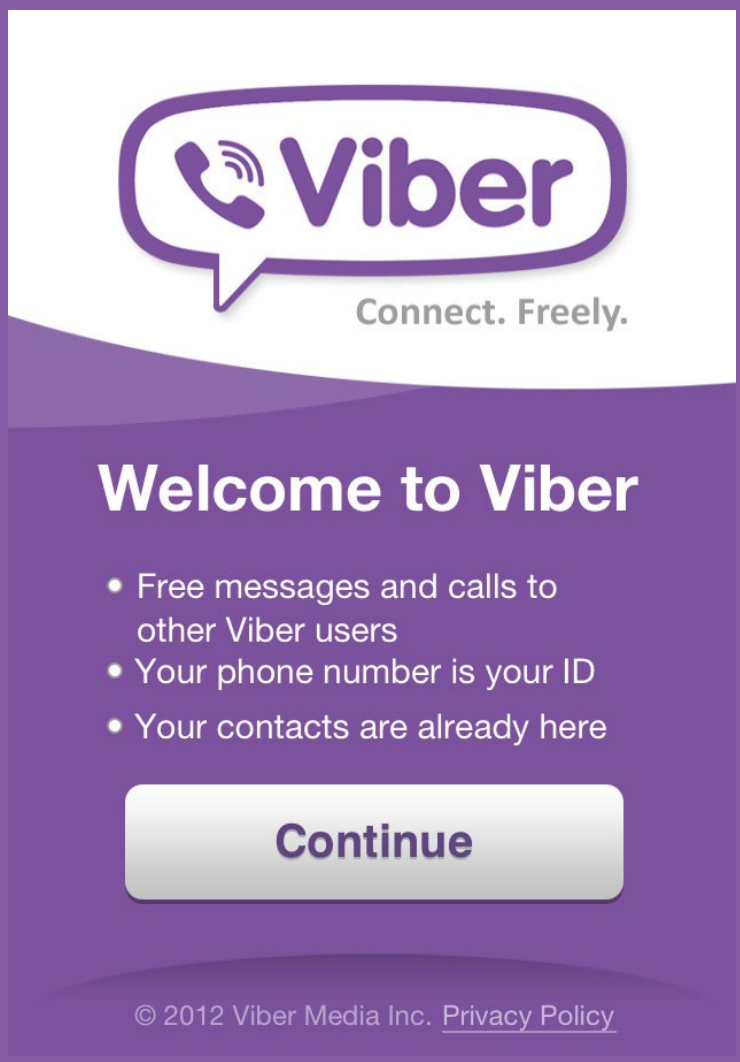
فايبر غير آمن

فايبر Viber هو أداة شعبية لإجراء الإتصالات الصوتية وتبادل الرسائل النصية بشكل مجاني وقد ظهرت في كانون الأول/ديسمبر ٢٠١٠ في بداية «الربيع العربي». بما أنها أدخلت الأسواق في وقتها المناسب، حظيت هذه الأداة بشعبية واسعة في العالم العربي لا سيما بين الناشطين. ما يقوم به فايبر هو تحويل الإتصالات الهاتفية والرسائل النصية إلى اتصال من نوع ٣G أو واي فاي، مما يوفر الكلفة المالية على المستخدم، لا سيما لدى إجراء اتصال هاتفي. لقد لاحظ فريق سايبر آرابز أن قراءه يظنون أن فايبر أداة آمنة، إلا أن ذلك غير صحيح لسوء الحظ.

مع أن فايبر يستطيع أن يتخطى شبكة جي أس أم الإعتيادية التي تحظى الحكومة بالقدرة على النفاذ إليها، إلا أن معظم البيانات التي يتم تبادلها بين المتصلين غير مشفرة. لقد أعلن القيمون على برنامج فايبر أن التفاصيل الخاصة بتسجيل الدخول والرسائل النصية مشفرة، إلا أن الإتصال الصوتي غير مشفر، مما يعني أن أي أحد يمتلك المعدات اللازمة يمكنه أن يتنصت على المكالمات التي تجري من خلال البرنامج من دون أي صعوبة. وبما أن فايبر يستعمل رقم هاتفكم المحلي من أجل أن التعرف إليكم، يصبح من غير الصعب على شركة الهاتف أن تسجل هذا الرقم، ثم تقوم باستقبال الرسالة النصية التي يرسلها برنامج فايبر من أجل تفعيل التطبيق وسرقة محتوى التواصل.

كما أن قلة من الناس يعرفون أن فايبر هي شركة إسرائيلية مسجلة في قبرص وتمتلك مكاتب تطوير في كل من تل أبيب ومينسك عاصمة روسيا البيضاء. يتم تمرير معظم اتصالاتكم من خلال الخوادم الخاصة بالشركة كما يتم الإحتفاظ بقدر كبير من البيانات المتعلقة باتصالاتكم (رقم الهاتف، المكان الجغرافي، أرقام الهواتف التي تحتفظون بها – راجعوا شروط الإستعمال). بالإضافة إلى ذلك، هناك غموض يحيط بإدارة فايبر ومصادر تمويلها. لذا فإن فريق سايبر آرابز يخشى أن تكون هذه الأداة غير آمنة، إذ إن هناك شك في أنها تبقي هويتكم مجهولة أثناء إجراء الحديث.

عوضاً عن هذه الأداة، ينصح فريق سايبر آرابز باستعمال سكايب لإجراء الإتصالات المجانية، ويفضل أن يكون ذلك بالتزامن مع استعمال برنامج آخر يتيح استعمال الإنترنت بشكل آمن مثل SSH و Tor أو VPN. مع العلم أن سكايب ليس آمناً بنسبة ١٠٠٪ إلا أن التواصل الصوتي عبره مشفر ومعظم ثغرات الأمان التي تشوبه قد تم توثيقها.



الشبكات الإخبارية المناطقية وسبل تحسينها

للنشاط المناطقي الإلكتروني حضور واسع في البحرين، ليس حالياً فحسب، بل منذ مطلع الألفية الجديدة، حين راج استخدام الإنترنت وصار الحاسوب من لوازم كل منزل.

في ذلك الوقت لم تكن شبكات التواصل الإجتماعي على ما هي عليه حالياً، حيث يمكن الوصول إلى المستخدمين وفق أماكن سكنهم أو دراستهم، وطبيعة عملهم وما شابه. كان البحرينيون يتواصلون بطريقة أكثر بدائية هي المنتديات الإلكترونية، إذ جرى العرف وقتها أن تطور كل قرية منتداها الإلكتروني الخاص، الذي يتم فيه نشر أخبار القرية من وفيات، وولادات، وأعراس، فضلاً عن النشاطات وكل ما خص القرية من قريب أوبعيد. وكانت هذه المنتديات، التي يشرف عليها عادة المعنيون بمؤسسات القرية المدنية مثل النوادي والصناديق الخيرية، تحرص على جذب الوجهاء للمشاركة فيها، وليس من المبالغة القول إنها نجحت إلى وقت متأخر في شد أطراف القرية إلى بعضها البعض بعد أن حالت انشغالات عالم اليوم دون التواصل الفعلي بين الناس.

من هنا يمكن القول إن الشبكات الاخبارية المناطقية التي انتشرت مؤخراً هي وليدة تلك المنتديات، التي دعت الحاجة إلى إعادة صياغتها بما يتناسب مع معطيات الأحداث الجارية في البحرين، في ظل غياب الصحافة غير الحكومية وتصاعد وتيرة الأحداث الميدانية في القرى. ويمكن القول أيضاً إن هذه الشبكات نقلت نشطاء الإنترنت من عتبة النقاش النظري ونشر الصور الفوتوغرافية في المناسبات إلى بدايات صحافة المواطن الحقيقية، فيقومون من خلالها بما تعجز عنه مؤسسات إعلامية ذات امتداد تاريخي على مستوى البحرين وربما الخليج.

المسيرات والمعتقلون والإصابات على رأس العناوين

تعد صور المسيرات وباقي الفعاليات «الثورية»، كما يطلق عليها الناشطون، أحد أهم اهتمامات هذه الشبكات، كما أنها تتابع حالات الإعتقال في القرية وتنشر أخبارها مع صورة المعتقل وعمره وكيفية اعتقاله وإلى أين اقتيد (إن أمكن) كعناصر أساسية للخبر. وتوثق الشبكات أيضاً صور الإصابات، لا سيما الإصابات برصاص صيد الطيور «الشوزن» المحرم دولياً، بالإضافة إلى الإختناقات أو حالات الحريق التي تنشب جراء إطلاق قنابل الغاز المسيل للدموع داخل المنازل. وتجدر الإشارة إلى أن العديد من الشبكات تولي الأهمية لتوثيق التجاوزات التي ترتكبها الأجهزة الأمنية ونشرها، بعد دعوات من حقوقيين وجماعات سياسية لتكثيف الجهود في هذا المجال.

من فيس بوك إلى يوتيوب وتويتر

تنشر معظم الشبكات موادها الإعلامية على موقع فيس بوك كونه الأسهل استخداماً في نشر وسائط الصوت والصورة والفيديو، رغم أن معظم هذه الشبكات تملك حساباً آخر في موقع تويتر الأكثر رواجاً بين البحرينيين. ومن بينها من يملك حساباً ثالثاً على موقع مقاطع الفيديو المعروف يوتيوب، إذ تنشر مقاطع توثق المسيرات وأعمال إبداعية وأناشيد ذات علاقة.

ولكن أمام هذه التجربة الوليدة طريق شاق من التجريب والتطوير. فهذه الشبكات، على الرغم من رواجها، قد تقع ضحية عثرات يقع فيها كل مشروع في بداياته. ويستحق هذا المجهود الذي يبذله نشطاء تفوقوا على هواجسهم الأمنية، وأسهموا في نشاط مدني سامٍ، أن يحظى بمقاربة نقدية مُنصفة، وتقييم صريح من وقت إلى آخر من شأنه أن يبعث بهذه الجهود نحو المزيد من النجاح.

ولبحث فعالية هذه الشبكات والتعرف على نقاط الضعف والقوة فيها، سعى فريق سايبر آرابز إلى نقل رأي من يتعامل عادةً مع موارد الاعلام بصورة مهنية وحيادية، ولذلك سبرنا أغوار هذه الشبكات بنظرة تحليلية قدمتها جناح (إسم مستعار) وهي شابة تعمل على تحرير التقارير الحقوقية لعدد من المنظمات.

الشبكات الإخبارية المناطقية وسبل تحسينها

المصداقية على حساب الأمن، أو العكس؟

في معرض إجابتنا عن سؤال حول مدى المصداقية التي تتمتع بها هذه الشبكات، إستهلت جناح حديثها بالقول إن «لها دور مجتمعي بارز، حتى أن بعض الحقوقيين يعتمدون عليها في أرشفة الصور والفيديوات والقصص.» ولكن الحقوقية الشابة ذكرت في الوقت نفسه أن المشكلة الأهم التي تعاني منها هذه الشبكات وتؤثر في مصداقيتها هي أن وجودها مرتبط نوعاً ما بعدم تعرض القائمين عليها لتهديد أمني.

«عدم ذكر الاسماء يوفر الأمن للقائمين عليها، لكنه يؤدي إلى مشكلة المصداقية،» تقول جناح.
وسعياً لحل هذه المشكلة توصي جناح بأن لا ينشر القائمون على الشبكات خبراً قبل التأكد التام من صحته، إذ إن المصادر لا تكون دائماً صحيحة والسعي إلى سبق صحفي دون التأكد القطعي من الخبر قد يؤدي إلى عواقب وخيمة. وتنصح جناح باستخدام الصور لزيادة المصداقية، فمن خبرتها في العمل الحقوقي تجد أن الناس تميل إلى تصديق الأخبار الموثقة بدليل صوري، أكثر من مجرد النقل والتبليغ.
تعترف جناح أن هذه الشبكات يميزهاالخطاب المنحاز، وتفسر سيطرة وجهة النظر الشخصية على التغطية التي تؤديها هذه الشبكات بالقول إن الأخيرة كانت رداً على الصمت الإعلامي.

رُبما يستطيع المرء أن يتفهم وجود ذلك الانحياز من جانب شبكات إعلامية أهلية انبثقت من رحم الربيع العربي، بيد أن هذا النمط من العمل يُبقيها دائماً أدنى بقليل من كونها مصدراً مستقلاً أو موثوقاً عند هؤلاء الذين يقفون على الحياد، أو يبحثون عن المعلومة من غير أن تكون معلبة سلفاً لتناسب جهة ما.

وصحيح أنه في عالمنا العربي ليس من المتوقع دائماً من النشاطات الأهلية أن تكون بالحرفية ذاتها التي تمتلكها المؤسسات المهنية، ولكن أي خبير في حملات التغيير والتأثير في النشاط الأهلي سيقول إن الفئة الأهم التي يجب على النشطاء التأثير عليها في حملاتهم هي دائماً الفئة المحايدة. ومن هنا يمكننا، بثقة، أن نخلص إلى أن إعادة صياغة هذه الشبكات بذكاء يخرجها من صيغة الخطاب المنحاز إلى صالح الخطاب الإخباري سوف تسهم وبلا شك في زيادة عدد متابعي هذه الشبكات الذي يتراوح بين ١٠٠٠ و١٢٠٠٠ تبعاً لشعبية الشبكة، والكثافة السكانية في االقرية، وتواتر النشاط القرية الميداني فيها.

شبكة المراسلين

هناك ثلاثة أنواع من المراسلين لهذه الشبكات، وفق ما أفادت جناح: سكان القرية، الذين ينقلون الأخبار عن طريق مشاهداتهم الشخصية؛ من يعتمد على شبكة أصدقائه «الموثوقين» فيكتب أخباره نقلاً عنهم؛ ومن يقوم بجمع الأخبار من على شبكة الإنترنت ويعيد نشرها.

وختمت بالقول إن «تطوير هذه الشبكات يكمن في تحولها من مجرد ناقل للأخبار، إلى شبكات تصنع الخبر وتوثقه، وتكون فعالة في كسب جمهور متعاطف مع مبادئها وأهدافها،» مضيفة «أن مشاركة المواد التحريرية والصورية في مسابقات ودورات ذات علاقة من شأنه أن يصقل مهارات هؤلاء النشطاء الإلكترونيين، بالطبع إلى جانب فتح أبواب النقاش وإفساح المجال للنقد الذاتي.»

إلى أين ؟

إذاً هي ثلاثة تحديات أمام هذه الشبكات الإجتماعية: أمان المؤسسين، المصداقية، وعدم الإنحياز. أما نقل العمل إلى المرحلة التالية، تماماً مثلما انتقل الكثير من هواة المنتديات الإلكترونية إلى تجاربهم الأولى في صحافة المواطن، أمر حتمي لكسب المزيد من المتعاطفين، وبناء نشاط مدني إلكتروني فريد من نوعه.

غير أنه إلى الآن لم يتم التطرق إلى الصورة الصحيحة التي ينبغي على هذه الشبكات اتخاذها. فهل عليها مثلاً أن تستنسخ تجربة «مرآة البحرين»، الصحيفة الإلكترونية الرائدة التي تحتضنها المعارضة الكلاسيكية «المسجلة رسمياً» عند الدولة والتي مع ذلك فرضت نفسها منافساً للصحافة المحلية التقليدية خلال عام واحد؟ أم أنّ على هذه الشبكات أن تبني صيغتها الخاصة؟ سؤال نطرحه على مائدة النقد الذاتي التي دعت إليه الناشطة الحقوقية البحرينية جناح في سبيل تطوير شبكات فرضت نفسها هي الأخرى دون تمويل أو احتضان.

نقاط التفتيش في البحرين: سباق بين مغردي تويتر وأجهزة الأمن

مضى عام ونصف على قمع «الربيع العربي» في البحرين، حينما فرضت الأحكام العرفية وحظر التجول الذي دام ثلاثة أشهر. وبعد أن رفعت الأحكام العرفية وسُمِح للناس بالتنقل ساعة يشاؤون، كان عليهم أن يعتادوا مشهد الحواجز الإسمنتية التي وضعتها وزارة الداخلية في العديد من الطرق كحواجز لنقاط تفتيش ثابتة، تستهدف النشطاء وغيرهم من الشباب الذين يشتبه بضلوعهم في أعمال سياسية. غير أن صِغر مساحة البحرين واتصال مناطقها بالكثير من الشوارع الداخلية أسهما في أن يجد الناس شوارع خلفية بعيدة عن مواقع نقاط التفتيش، تقيهم شر الإهانات واحتمال الإعتقال.

ولكن كما يقال، «دوام الحال من المحال.» فبعد أن تعاقدت الدولة مع الضابط البريطاني سيّء الصيت جون يات مستشاراً لتطوير قوى الأمن في البحرين، إختفت هذه الحواجز لتحل عوضاً عنها نقاط تفتيش متحركة، تنتشر بعشوائية يصعب التنبؤ بها. كما أن عمليات التفتيش هذه لم تعد تقتصر على القوّة الأمنية التي تبحث عن مطلوبين وحسب، بل اشتملت على شرطة المرور، ليُبعَث كل مَنْ لَمْ يثبت جرمه عند ضابط الأمن إلى ضابط السير، الذي سوف يبحث عن أي سبب يخوله تقييد مخالفة بحقه، وهو يعد أسلوباً جديداً من أساليب العقاب الجماعي.

الإنذار عبر تويتر

جرّاء هذا الوضع، صار عموم الناس، نشطاء وغير نشطاء ممن لا يرغبون في التأخير أو دفع مبالغ إضافية لإدارة المرور، بحاجة إلى وسيلة سريعة لنقل المعلومات، يستطيع من خلالها الجميع، وخاصةً من هم في الطرق، المساهمة في بث هذه المعلومات والوصول إليها على حد سواء. تطابقت هذه التوصيفات مع الوظائف التي يؤديها موقع التواصل الإجتماعي تويتر، المعروف بفضله في تصعيد وتيرة العديد من الأنشطة المدنية والإحتجاجات، من الثورة الخضراء في إيران عام ٢٠٠٩، وصولاً إلى ثورات الربيع العربي.

وبالفعل، سرعان ما أخذ العديد من مستخدمي تويتر زمام المبادرة بنشر أخبار مقتضبة عن نقاط التفتيش، تتضمن موقعها ومدى شراستها، أو أخبار تفيد بإزالة هذه النقطة أو تلك أو حتى تقترح طرقاً بديلة آمنة. ويلتزم هؤلاء بنشر تغريداتهم المتعلقة بهذا الخصوص عبر الوسم #chpo وهو اختصار للكلمة الإنجليزية checkpoint. بالمقابل، يقوم كل من يريد التأكد من أمان الطريق إلى جهة ما بالبحث في التغريدات.

بيد أن نجاح هذه المبادرة يتطلب الإلتزام بالكثير من السلوكيات المعنية بالإعلام المجتمعي وصحافة المواطن؛ فعلى سبيل المثال، يُلزم المغرد باستخدام عبارات دقيقة وصحيحة، لا تضيف على ما يحصل على الأرض ولا تنقص منه. ثم على باقي الأشخاص إعادة نشر التغريدة ذاتها لتكون واضحة في نتائج البحث عوضاً عن نسخها وإعادة تغريدها من حسابهم الخاص، مما يؤدي إلى حشو الوسم بتغريدات متكررة لا طائل منها. ويظهر البحرينيون التزاماً معقولاً بأدبيات التواصل الإجتماعي، رغم أن الوسم يشهد في أحيانٍ معدودة «سخام» تغريدات لا علاقة لها بالموضوع، لمن يبحثون عن الشهرة بأية طريقة.

تجربة واحدة تكفي

يقول الشاب ع.س. إنّ متابعة التغريدات المتعلقة بنقاط التفتيش أصبحت أمراً روتينياً بالنسبة إليه مؤخراً، بعد تجربة غير سارة مع احدى نقاط التفتيش.

«تفاجأت بنقطة تفتيش في موقع بالقرب من حي سكني هادئ، وفي وقت لم تكن فيه أي فعاليات سياسية.» يقول ع.س. «وبعد عشرين دقيقة من الإنتظار، قيدت بحقي مخالفة عدم ربط حزام الأمان وأمرت أن أعود أدراجي، فلم أتمكن من قضاء الحاجة التي خرجت من أجلها.»

وأفاد ع.س. أن هاتفه الذكي منذ تلك اللحظة صار يسدي إليه خدمات جليلة في مثل هذه المواقف.

«بعض الأحيان لا أقوم بقراءة تلك التغريدات قبل الخروج من المنزل، وإن قرأتها فإن مواقع هذه النقاط تتغير بين لحظة وأخرى. لذلك حين ألاحظ أن الحركة غير طبيعية في إحدى الطرق، أقوم بركن

نقاط التفتيش في البحرين: سباق بين مغردي تويتر وأجهزة الأمن

السيارة جانباً، وأقرأ آخر التغريدات على الوسم الخاص بنقاط التفتيش بواسطة هاتفي الذكي. فإذا تأكد لي وجود نقطة تفتيش في المنطقة أقوم بتغيير وجهتي فوراً.»

ليست آمنة تماماً...

يجدر القول إن هذه المهمة لها متاعبها وليست سهلة كما قد تبدو. أحد أهم الشواهد على خطورة استخدام الهاتف المحمول بالقرب من نقاط التفتيش هو ما حصل لمسؤول الرصد بمركز البحرين لحقوق الانسان السيد يوسف المحافظة؛ لُكِم على وجهه وجُرَ معتقلاً من رأسه امام ابنتيه، بعد أن طارده عناصر احدى نقاط التفتيش جراء التقاطه صورة للموقع من أجل نشرها في حسابه عبر تويتر، وفق ما أفاد مغردون.

لإلقاء نظرة عن كثب، أجرى فريق سايبر آرابز لقاءً مقتضباً مع أحد النشطاء الإلكترونيين في البحرين الذين يقومون بنشر مواقع نقاط التفتيش عبر تويتر بصورة مستمرة. وقد طلب عدم الإفصاح عن هويته حفاظاً على سلامته الشخصية:

١- ما الذي يدفعك إلى المساهمة في التغريد عن نقاط التفتيش؟

التغريد بشأن مواقع نقاط التفتيش ليس قراراً على المرء أن يتخذه، بقدر ما هو واجب وطني وضرورة لحماية النشطاء المطلوبين من قبل الأجهزة الأمنية، فضلاً عن تجنيب المواطنين الاستفزازات والمخالفات المرورية.

٢- برأيك، كيف من الممكن جعل شبكات التواصل الاجتماعي أكثر فعالية في حماية مستخدمي الطرق من شر نقاط التفتيش؟

من المفترض أن يكون هناك حساب خاص على شبكة التويتر مختص بالتغريد عن مواقع نقاط التفتيش، بحيث يرسل المغردون المعلومات إلى الحساب ويقوم هو بإعادة نشرها بطريقة منظمة.

٣- هل تعتقد أن شبكة تويتر هي الوسيلة الفضلى، أم ترى أنه من المفروض استخدام أداة أخرى لهذا الغرض؟

تويتر وسيلة فعالة جداً في تحديد المواقع ونشرها، ومؤخراً تمت برمجة خريطة البحرين على غوغل ماب من قبل نشطاء مبرمجين. تحدد هذه الخريطة مواقع نقاط التفتيش معتمدة على التغريدات في تويتر.

٤- هل من أخطاء يرتكبها المشاركون في التغريد عن نقاط التفتيش؟

هذه الأمور لا تعتبر أخطاء بالنسبة إلي، فلو افترضنا أن أحدهم قام بنشر تغريدة لم يتأكد من صحتها عن نقطة تفتيش في أحد الشوارع، فسيتجنب الناس المرور في هذا الشارع وحتى لو لم تكن هناك نقطة للتفتيش، سيكون ذلك من باب زيادة الحذر.

٥- ما هو الأسلوب الذي تتبعه لمعرفة مواقع نقاط التفتيش والتبليغ عنها؟

وسم #bhpo بشكل خاص، والشبكات الإخبارية للقرى وشبكة ١٤ فبراير، إضافة إلى الخريطة المبرمجة مؤخراً.

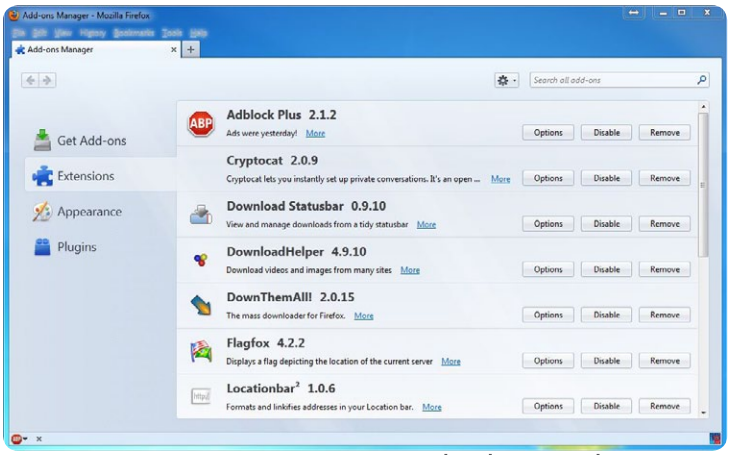
إضافات المتصفح

أصبحت متصفحات الإنترنت من البرامج الأكثر استخداماً في أجهزة الكمبيوتر. ولقد تحولت المتصفحات اليوم، وهي كانت لوحات تحكم بسيطة قبل بضع سنوات، إلى أنظمة تشغيل كاملة. واحدة من سمات متصفحات الإنترنت الحديثة هي القدرة على تنصيب الإضافات. الإضافة هي برنامج صغير يعمل جنباً إلى جنب مع متصفح الإنترنت لزيادة فاعليته. إضافات المتصفحات المشهورة تشمل مجموعة واسعة من أشرطة الأدوات(Toolbars) ، وملحقات الألعاب، وتطبيقات الأمن وبرمجيات لتشغيل تطبيقات جافا وفلاش.

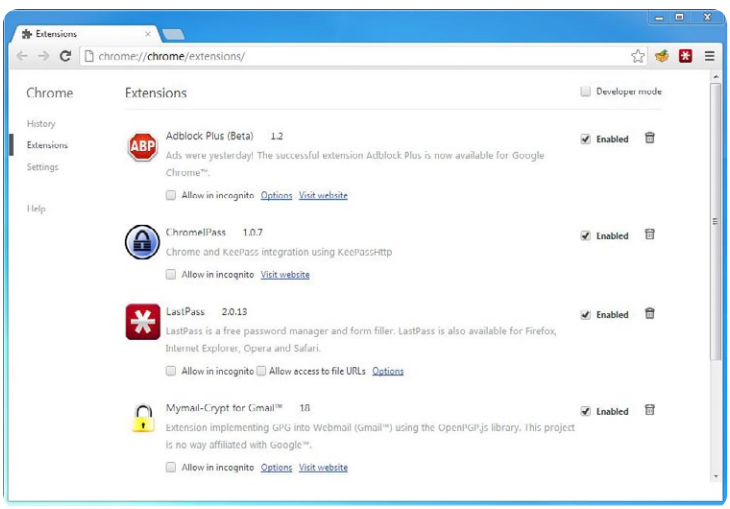
على الرغم من أن العديد من الإضافات قد تكون مفيدة، فهي في نفس الوقت لها نقاط ضعف أمنية قد توفر إمكانية التنصت على الإتصالات عبر الإنترنت. وتتمتع الإضافات بإمكانية الوصول إلى «محرك» المتصفح حتى إذا لم تدار من قِبل المتصفح. تقوم عادة الشركات المنتجة للمتصفحات، مثل جوجل ومايكروسوفت أو موزيلا، بتحديث البرامج الخاصة بها في حالة اكتشاف تهديد أمني. ومع ذلك، قد تمتنع الشركة المنتجة للإضافات أحياناً عن القيام بهذه العملية أو لا تنفذها في الوقت المناسب، كما أن المستخدم قد يتجاهل طلب التحديث. على سبيل المثال، أجريت مؤخراً دراسة تتعلق بإضافات جافا، كشفت أن خمسين بالمئة من مستخدميها لا يقومون بتحديث البرنامج المساعد.

لهذه الأسباب، يوصي فريق سايبر آرابز بتقليص استخدام الإضافات إلى أدنى حد. ولمعرفة أي إضافات تم تنصيبها على جهاز الكمبيوتر الخاص بكم، قوموا بزيارة صفحة الإشراف على إضافات المتصفح. في جوجل كروم إضغطوا على رمز الثلاثة خطوط .<الإعدادات> (Settings) الملحقات (Extensions) . أما في موزيلا فايرفوكس، إضغطوا على فايرفوكس (الزاوية العلوية اليسرى) وفي مايكروسوفت إنترنت إكسبلورر، إضغطوا على رمز <العجلة> إدارة الإضافات (Manage add-ons).

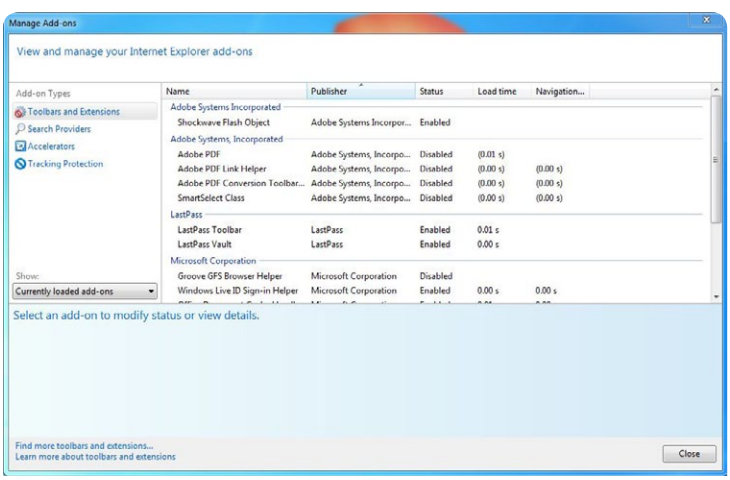
راجعوا القائمة و قوموا بإلغاء كافة الإضافات التي لم تستخدموها. قد تكون بعض الإضافات قد نُصّبت عن غير قصد. العديد من التطبيقات المجانية التي يمكن تحميلها من شبكة الإنترنت تقترن بإضافات غير ضرورية لشرائط الأدوات. هذه الإضافات للمتصفحات التي يتم تنصيبها عن غير قصد تشكل أكبر تهديد لأمن الإنترنت الخاص بكم ولذلك إحرصوا على حذفها.



إدارة الإضافات على فايرفوكس



إدارة الإضافات على جوجل كروم



إدارة الإضافات على مايكروسوفت إنترنت إكسبلورر

إضافات مفيدة

على الرغم من أن الإضافات قد تخلق ثغرات أمنية، قد يكون البعض منها في الواقع مفيداً للتعامل مع القضايا الأمنية. ومع ذلك، فمن المستحسن أيضاً استخدام إضافات الأمن مع قيود. يوصي فريق سايبر آرابز باستخدام الإضافات التالية. للأسف، هذه الإضافات متاحة فقط لجوجل كروم وفايرفوكس موزيلا (المتصفحات التي ننصح بها).

تقدم عدة مواقع على الإنترنت دعماً محدوداً للتشفير عبر بروتوكول HTTPS، ولكنها في الوقت نفسه تصعّب استعمال هذا البروتوكول. على سبيل المثال، تعمد هذه المواقع إلى استعمال بروتوكول HTTP بشكل تلقائي، أو تقوم بملء صفحات مشفرة بروابط تقود إلى موقع غير مشفر. تقوم إضافة HTTPS Everywhere بحل هذه المشكلة عبر إعادة كتابة الطلبات إلى المواقع عبر بروتوكول HTTPS.

باستطاعة HTTPS Everywhere تقديم الحماية فقط إذا كنتم تحاولون الدخول إلى مواقع تدعم بروتوكول HTTPS وإذا كانت إضافة HTTPS Everywhere تحتوي على مجموعة أوامر خاصة بها.

الموقع: https://www.eff.org/https-everywhere

نو سكربت (Noscript)/ نوت سكربت (Notscript)

النوسكريبت وشبيهتها في متصفح كروم النوت سكربت هي إضافات تتحكم في تسيير لغة البرمجة النصية)سكريبت (في المتصفح. السكريبت هو «كود» قابل للتنفيذ، مثل سكريبت جافا، الذي يمكن استخدامه على مواقع الإنترنت. ويتسبب تنفيذ السكريبت بغالبية المشاكل الأمنية أثناء تصفح الإنترنت. النوسكريبت والنوت سكربت مسؤولان عن تعطيل تنفيذ السكريبت غير المصرح به في المتصفح. ومع ذلك، يمكن وضع صفحات تثقون بها في «القائمة البيضاء» بحيث يسمح لهذه المواقع فقط بتنفيذ السكريبت.

موقع الإضافة:

لفايرفوكس: http://noscript.net

للكروم: http://goo.gl/M8UBv

إجراء النسخ الإحتياطي بواسطة سينك توي

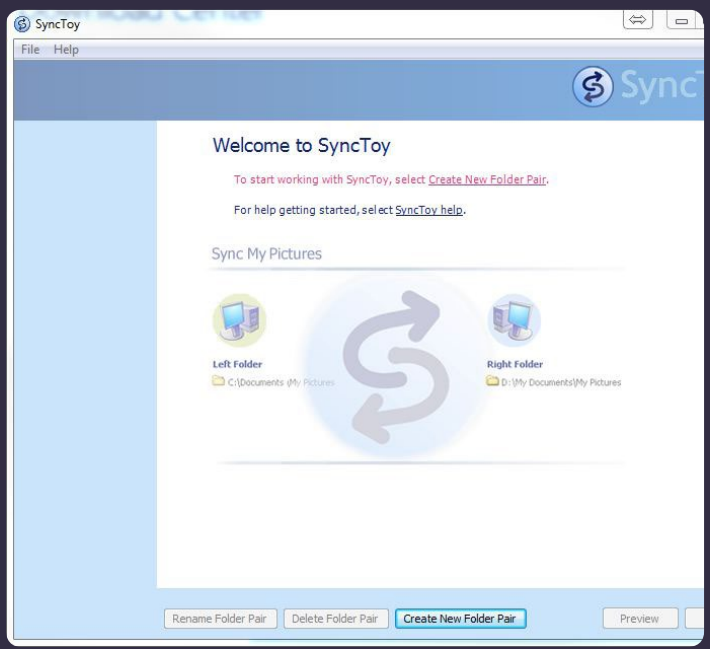
SyncToy

من المحتمل دائماً أن تتعرض أجهزة الحاسوب أو الهواتف أو الأدوات الإلكترونية الأخرى للأعطال أو السرقة أو يتم ببساطة فقدانها، مما يعرضكم لاحتمال ضياع المعلومات المخزنة في هذه الأدوات، بالإضافة إلى فقدان الأجهزة نفسها. لقد اشتكى العديد من قراء سايبر آرابز من فقدان بيانات مهمة، من ضمنها صور ومقاطع فيديو وملفات، وكانت النتائج في بعض الأحيان كارثية. لمنع فقدان البيانات، هناك دائماً نصيحة واحدة يجب اتباعها: إجراء نسخ احتياطي (Backup) بشكل منتظم.

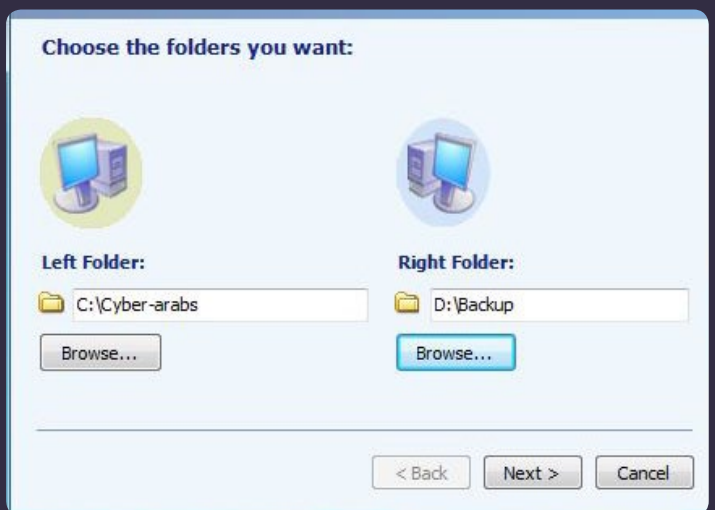
النسخ الإحتياطي هو مجرد إجراء نسخة عادية من البيانات، إلا أن هذه النسخة يجب ألا تخزن على الجهاز نفسه. ينصح فريق سايبر آرابز بإبقاء النسخة الإحتياطية بعيدة عن البيانات الأصلية قدر الإمكان. الوسائط المناسبة لتخزين النُسخ الإحتياطية هي القرص الصلب الخارجي، قرص يو إس بي (أو "الفلاشة") أو أقراص مدمجة قابلة للكتابة. تأخذ عملية النسخ الإحتياطي القليل من وقتكم وهي سهلة للغاية.

إذا كنتم من مستخدمي ويندوز، يمكنكم أن تحملوا برنامجاً سهل الإستخدام من موقع مايكروسفت يدعى سينك توي SyncToy (يمكنكم تحميله هنا: http://goo.gl/1hoCE) يأتي سينك توي في نسختين، ٣٢ و٦٤ بت. إحرصوا على تحميل النسخة الملائمة لجهاز حاسوبكم. (أنقروا على أيقونة جهاز الحاسوب My Computer بزر الفأرة الأيمن، ثم أنقروا على خصائص Properties واقرؤوا نوع النظام ٦٤ ام ٣٢ بت – ٨٦ بت هو نفسه ٣٢ بت).
ما يفعله سينك توي هو خلق رابط بين الدليل المصدر (المكان الذي تريدون نسخ البيانات منه) والمجلد حيث سيتم تخزين النسخة، مثل الفلاشة.

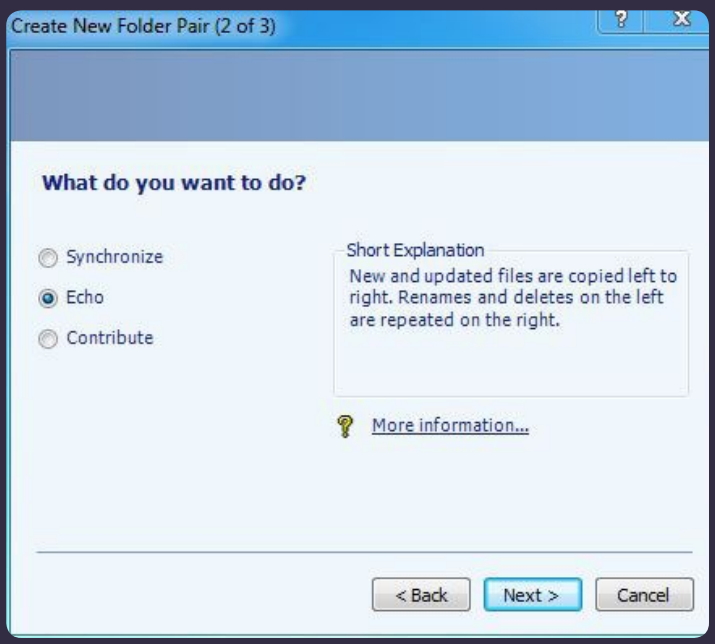
بعد تنصيب سينك توي وإطلاقه سوف ترون الشاشة التالية:



"المجلد الأيسر" (Left Folder) يشير إلى المكان حيث تتواجد الملفات التي تريدون نسخها. يتوفر سينك توي باللغة الإنجليزية فقط ويعتمد منطقاً مبنياً على اللغات الأوروبية، المكتوبة من اليسار إلى اليمين. فمن أجل ربط مجلد أيسر (أو مصدر) بمجلد النسخ الإحتياطي يجب النقر على "Create New Folder Pair". عندها سترون الشاشة التالية:



قوموا فقط باختيار المصدر ثم انسخوا المجلد الذي تريدون. بعد اختيار المجلدين الأيمن والأيسر، أنقروا على "Next". عندها سترون الشاشة التالية:



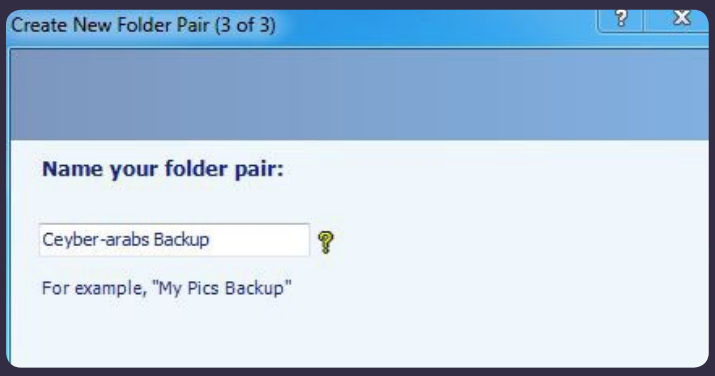
الآن عليكم أن تختاروا كيف تودون الربط بين المجلدَين. الخيارات هي التالية:

• Synchronize (مزامنة): تبعاً لهذا الخيار، يأخذ البرنامج المجلدين ويتأكد أنهما يحتويان على الملفات نفسها. . في حال تحديث ملف ما في المجلدين، تُعتمد النسخة التي تحتوي على التغييرات الأحدث وتقوم بأخذ مكان النسخ الأخرى. قد يقوم البرنامج بإزالة ملفات في أي من المجلدَين كما قد يقوم بإعادة تسمية هذه الملفات.

• (Echoصدى): يقوم هذا الخيار بالبحث عن التغييرات (التغييرات في الملفات، ملفات جديدة، تغيير الأسماء، الإزالة) وينفذها في المجلد الأيمن.

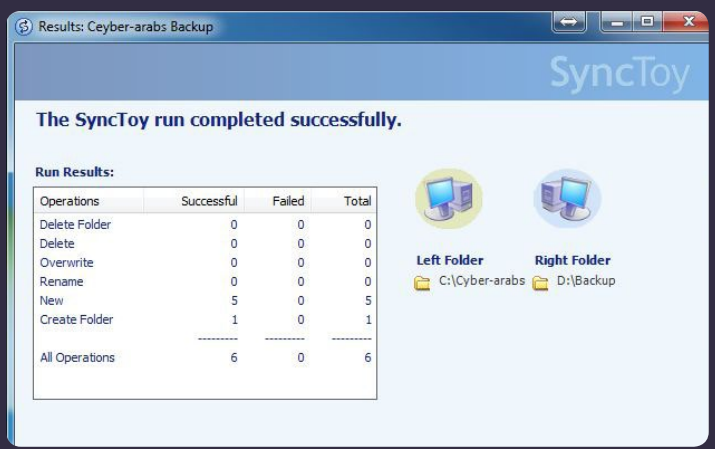
• Contribute (مساهمة): يشبه هذا الخيار Echo ولكنه لا يقوم بإزالة أي ملفات في المجلد الأيمن قد تكون تمت إزالتها في المجلد الأيسر.

ينصح فريق سايبر آرابز باعتماد إما Echo أو Contribute وذلك لأنهما يؤديان الخدمة الطبيعية التي يتوقعها المستخدم من برنامج النسخ الإحتياطي. بعد إجراء الإختيار أنقروا على OK ومن ثم سترون الشاشة التالية:



قوموا بتسمية المجلد. عندها سترون الإسم ظاهراً على الجهة اليسرى من القائمة الرئيسية.

كل ما يتبقى فعله هو استحداث النسخة الإحتياطية عبر النقر على "run"



تخطي الرقابة

يصل العديد من الأسئلة إلى فريق سايبر آرابز، وهي تتعلق بدخول الإنترنت بشكل آمن وطرق تخطي الرقابة على الإنترنت أثناء استخدام أجهزة الحاسوب الشخصية وأجهزة الهاتف. يبحث معظم الناس عن حلول سهلة ومجانية لدخول المواقع المحجوبة، ويمكن إيجاد العديد من الأدوات من خلال محرك غوغل للبحث. تَعِد هذه الأدوات بتقديم هذه الخدمة، ولكن ليس هناك من حل كامل. لكل واحدة من هذه الأدوات حسناتها وسيئاتها، وهي جميعها تبطّئ الإتصال بشبكة الإنترنت.

عليكم أن تتذكروا أنكم عندما تستعملون البرمجيات التي تتيح النفاذ الآمن إلى الإنترنت، أنتم تضعون ثقتكم بطرف ثالث، غالباً ما يكون مجهولاً. بعض البرمجيات المتوفرة هي مفتوحة المصدر، مما يمكّنكم من معرفة الوجهة التي تُرسل إليها بياناتكم، إلا أنّ العديد من هذه الأدوات هي مغلقة المصدر وتُبقي مصير بياناتكم مجهولاً عندما يتم إرسالها من جهاز الحاسوب.

وقد حذّر بعض الخبراء من أنّ الحكومات تعمل مع بعض الشركات المختصة بأمن الإنترنت من أجل النفاذ إلى معلومات حساسة، وقد اتُهمت الحكومة الصينية بهذه الممارسة بشكل خاص. كما أنّ أولوية معظم الشركات الخاصة هي جني المال وليس توفير الأمان لكم. لذا يجب أن تتذكروا هذه الأمور كلها عندما تقومون بتنصيب مثل هذه البرمجيات التي تتيح تخطي الرقابة على الإنترنت. ننصحكم باستعمال البرمجيات مفتوحة المصدر متى أمكن ذلك.

قام فريق سايبر آرابز بمسح سريع للبرمجيات التي يستعملها قراؤه. يتوفر بعض هذه الأدوات (تورTor، هوتسبوت شيلدHotspot Shield، سايفونPsiphon) في نُسخ معدة للإستعمال مع الهواتف الذكية.

ملاحظة لمستخدمي موزيلا فايرفوكس

معظم التطبيقات المذكورة تقوم بتكييف إعدادات الإتصال في جهاز الحاسوب عبر تعديل التشكيلة القياسية (Standard Configuration) في ويندوز. إلا أن فايرفوكس لا يستعمل تشكيلة ويندوز، ويتصل بالإنترنت عبر تشكيلته الخاصة. لإيجاد هذه الإعدادات توجهوا إلى:
خيارات Options > شبكة Network > إعدادات الإتصال Connection Settings

إذا لم تتمكنوا من الإتصال بالإنترنت عبر فايرفوكس يمكنكم أن تختاروا تشكيلة بروكسي اليدوية Manual Proxy Configuration ثم أدخلوا الرقم 127.0.0.1 في الحقلين الأولين المخصصين للكتابة، ثم رقم المنفذ (port 8080).

قد يتغير رقم المنفذ، ولكن سيتم إبلاغكم بذلك من قبل الموقع الذي زودكم بالبرنامج.

VPN خاص أو نفق SSH

إحدى أسرع الطرق لدخول الإنترنت وأكثرها أماناً هي استعمال شبكة خاصة إفتراضية VPN أو بروتوكول النقل عبر الأنفاق SSH. لكي تتمكنوا من استعمال هذه الأدوات يجب أن تعرفوا شخصاً تثقون به خارج البلد الذي تعيشون فيه، يكون مستعداً لمشاركة خدمة الإنترنت معكم. ليس من الصعب إعداد VPN أو نفق SSH كما أن استعمالهما يعد آمناً جداً. إلا أن الطرف المضيف يجب أن يكون على مستوى جيد من المعرفة بالتكنولوجيا ويجب أن يزودكم ببيانات الولوج. من الممكن أيضاً أن تأمنوا اتصالاً بالإنترنت من خلال هاتين الأداتين عبر هاتفكم النقال.

الموقع: ويكيبيديا العربية: بروتوكول النقل عبر الأنفاق؛ الشبكة الخاصة الإفتراضية.

شبكة تورTor (دعم الإستعمال في الهواتف النقالة)

تعد شبكة تور الأداة الأشهر والأسهل استخداماً لدخول الإنترنت. تصلكم هذه الشبكة بالإنترنت عبر شبكة من أجهزة الحاسوب بطريقة لا يمكن من خلالها تتبع الطريق التي سلكتها المعلومات عند محاولة الدخول إلى موقع معين. التكنولوجيا التي تستخدمها شبكة تور تم إثبات نجاحها، كما أن الشبكة مفتوحة المصدر وآمنة. يمكن استعمال تور لاخفاء هويتكم أثناء استعمال الإنترنت وتخطي الحجب المفروض على المواقع. الجانب السيء من شبكة تور هي أنها تبطّئ الإتصال، كما أنه يصعب استعمالها في بعض البلدان. من السهل استعمال الأدوات الخاصة بالمتصفح التي تأتي مع تور، كما أن البرنامج لا يحتاج إلى التنصيب. تتوفر أيضاً نسخة من تور للإستعمال مع نظام التشغيل أندرويد الخاص بالهواتف الذكية، تدعى أوربوت، وهي متوفرة في غوغل بلاي ستور.

الموقع: https://www.torproject.org/

سايفون Psiphon (دعم الإستعمال في الهواتف النقالة)

يعد برنامج سايفون من اللاعبين الجدد في حقل تجنب الرقابة، ولكنه كان ناجحاً منذ أن تم إطلاقه. برنامج سايفون مفتوح المصدر، تم تطويره في جامعة تورونتو بدعم من وزارة الخارجية الأميركية. يعمل سايفون من خلال تهيئة اتصال بجهاز حاسوب مجهول الهوية على الشبكة الخاصة بالبرنامج من خلال نفق SSH أو شبكة VPN. معظم أجهزة الحاسوب العاملة ضمن شبكة سايفون موجودة في الولايات المتحدة الأميركية وسرعة الإتصال عبرها في بلدان الشرق الأوسط تعتبر معقولة. سايفون سهل الإستعمال وآمن، كما أن تنصيبه ليس ضرورياً. لتحميل البرنامج يتوجب عليكم أن ترسلوا رسالة إلكترونية إلى الموقع المسؤول عنه، وسيجيب القيّمون على الموقع عليكم بإرسال رابط للتحميل. تتوفر أيضاً نسخة من البرنامج تعمل مع نظام تشغيل أندرويد (ملف APK)

الموقع: http://psiphon.ca/

دليل التنصيب باللغة العربية:
https://s3.amazonaws.com/0ubz-2q11-gi9y/ar.html

يورفريدوم YourFreedom

يورفريدوم تطبيق مجاني يقوم بتهيئة اتصال بديل (بروكسي) آمن مع جهاز حاسوب في مكان خارج البلد الذي تتواجدون فيه. التطبيق سهل الإستخدام، ولكنم ستحتاجون إلى تنصيب جافا ٦ في حال لم يكن موجوداً على جهازكم. تتواجد خوادم يورفريدوم في عدة بلدان حول العالم وسرعة الإتصال عبره جيدة نسبياً. يورفريدوم مغلق المصدر ويدعم الإستعمال باللغة العربية.

الموقع: https://www.your-freedom.net/

ألتراسورف Ultrasurf

ألتراسورف هو أداة أخرى مغلقة المصدر وسهلة الإستخدام. تقوم برمجية ألتراسورف بالإتصال بالإنترنت عبر وصل جهاز الحاسوب الخاص بكم بجهاز بديل خارج البلد الذي تتواجدون فيه. تم تصميم ألتراسورف للعمل في الصين، ولذا معظم الخوادم الخاصة به موجودة في آسيا، مما يجعل الإتصال عبر هذا البرنامج من الشرق الأوسط بطيئاً نوعاً ما.

تم توجيه الإنتقاد إلى برنامج ألتراسورف في الماضي، لا سيما من عاملين على مشروع تور، بسبب اكتشاف ثغرات أمنية فيه. وقد قام موقع سايبر آرابز بالإشارة إلى هذا الموضوع سابقاً. لذا لا ننصح باستخدام هذا التطبيق كأداة للإستخدام الآمن للإنترنت، أي الحفاظ على الهوية مجهولة أثناء الإستخدام، وإنما ننصح باستعماله كأداة لتخطي الحجب.

الموقع: http://ultrasurf.us/

جوندو JonDo

جوندو وجوندو فوكس)وهو نسخة معدلة عن متصفح فايرفوكس) هما أداتان تتيحان الإتصال الآمن بالإنترنت. الأداتان، وهما مفتوحتا المصدر، تم تطويرهما في جامعة دريسدن الألمانية. يقوم هذا التطبيق بإتاحة الإتصال بالإنترنت عبر شبكة من الحواسيب بشكل يبقي هوية المستخدم مجهولة. مع أن هذه البرمجية تعمل بشكل جيد، إلا أنها لا تزال في المرحلة بيتا (المرحلة الثالثة من مراحل تطوير البرمجيات) مما يعني أنه من الممكن أن تتخلله بعض العيوب في التصميم. يتمتع جوندو بخيار تنصيب نفسه على قرص يو إس بي («فلاشة»). ولكن للأسف، يتطلب التطبيق تنصيب نسخة حديثة من جافا، مما يجعله غير متطابق مع الكثير من أجهزة الحاسوب في مقاهي الإنترنت.

الموقع: https://anonymous-proxy-servers.net/en/jondo.html

جي تانل Gtunnel

تم تطوير برمجية جي تانل في الأساس لكي تستعمل في السوق الصينية أيضاً. تقوم هذه البرمجية بإقامة اتصال مع خادم بديل خارج البلد الذي تتواجدون فيه. يبدو أيضاً أن معظم الخوادم الخاصة بشبكة جي تانل تتواجد في آسيا، مما يجعل الإتصال بالإنترنت في الشرق الأوسط من خلالها بطيئاً بعض الشيء. تتميز برمجية جي تانل بأن تهيئتها سهلة وتترك القليل من الآثار على جهاز الحاسوب، إلا أنها مقفلةس المصدر.

الموقع: http://gardennetworks.org/download

فريغيت Freegate

يقوم فريغيت بالإتصال بالإنترنت عبر خادم بديل خارج البلد الذي تتواجدون فيه. تم تطوير فريغيت لكي تستخدم في السوق الصينية ويتواجد معظم الخوادم الخاصة به في آسيا، مما يجعل الإتصال من خلالها في الشرق الأوسط بطيئاً. فريغيت مقفل المصدر ومن الصعب الحصول على معلومات حول من يقوم بتمويل مطوّريه.

الموقع: http://www.dit-inc.us/freegate

بدائل عن غوغل بلاي ستور

تتميز الهواتف العاملة بنظام أندرويد بأنها تمكن المستخدمين من إضافة وظائف جديدة إلى الهاتف من خلال التطبيقات (Apps). يمكن تحميل مئات الآلاف من هذه التطبيقات من موقع غوغل بلاي ستور Google Play Store، الذي يمكن الولوج إليه بشكل تلقائي من معظم أجهزة أندرويد. بعض هذه التطبيقات مجاني وبعضها الآخر يمكن استخدامه لقاء مبلغ مادي صغير. ينصح موقع سايبر آرابز بشكل منتظم بتنصيب تطبيقات معينة، يتيح معظمها تحسين مستوى الأمان، مثل شبكات البروتوكول الإفتراضية VPN، برمجيات التشفير وأدوات تخطي الرقابة.

تكمن المشكلة في أن موقع غوغل بلاي ستور يخضع للحجب في عدة بلدان، ويكون ذلك في بعض الأحيان بسبب قيود يفرضها مزودو خدمة الإنترنت. ولكن في أغلب الأحيان، ينتج الحجب عن العقوبات الإقتصادية التي تفرضها الولايات المتحدة الأميركية؛ الحظر المفروض على إيران، كوبا، سوريا والسودان هو مثال واضح على هذه الأمثلة. ومع أن الحكومة الأميركية تسعى من وراء هذا التدبير إلى استهداف حكومات هذه البلدان، إلا أن الجهة التي تتعرض للأذى أكثر من غيرها هي المدنيون، الذين لا يكون بمقدورهم تحميل أي تطبيقات، بما فيها التطبيقات التي من الممكن أن توفر لهم الحماية من الإجراءات الحكومية القمعية.

لحسن الحظ، هناك طرق أخرى لتنصيب التطبيقات على هواتف أندرويد. سنناقش في هذا المقال بعض التطبيقات البديلة عن تلك التي تحصلون عليها من خلال غوغل بلاي ستور بالإضافة إلى الطريقة الخاصة بتنصيبها.

التحضيرات الضرورية

التطبيق في أندرويد هو ملف مضغوط يقوم بتنصيب نفسه بطريقة آلية. قد تكونون على معرفة بهذا النوع من الملفات في ويندوز، حيث يسمى ملف التنصيب عادة setup.exe أو setup.msi. في أندرويد، ينتهي إسم ملف التنصيب دائماً بـ «apk» على سبيل المثال، يدعى ملف التنصيب الخاص بسكايب skype.apk.

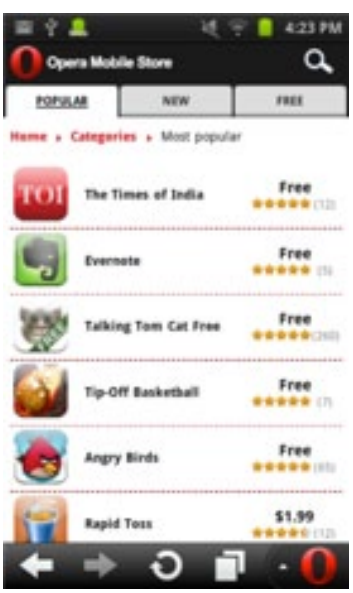
ما يفعله غوغل بلاي ستور هو أنه يجمع كل هذه الملفات ويقدمها في إطار سهل الإستخدام. لهذا السبب، فإن معظم القراء قد لا يصادفون ملفاً من نوع apk. إلا أن العديد من منتجي التطبيقات يجعلون تطبيقاتهم متاحة عبر ملف .apk. يمكن تحميله من خلال مواقعهم. وفي بلدان مثل سوريا، يمكن الحصول على هذه التطبيقات في أقراص مدمجة في المتاجر. ولكن يجب أن تعرفوا أنكم تستعملون هذه الأقراص المدمجة على مسؤوليتكم الخاصة. إن تنصيب ملف .apk على جهاز أندرويد يعد سهلاً للغاية. كل ما يتوجب عليكم فعله هو نسخ الملف على ذاكرة جهازكم أو على بطاق الذاكرة SD ومن ثم النقر عليه. إلا أنه يتوجب عليكم تعطيل آلية الحماية الخاصة بغوغل، والتي تمنع تنصيب تطبيقات غير صادرة عن غوغل بلاي ستور؛ إنها عملية بسيطة.

إضغطوا على زر الإعدادات (Settings) من أجل التنقل بين إعدادات قائمة التطبيقات (Applications) (Settings> Applications) عندها سترون الشاشة التالية:

ما يهمنا هو «المصدر المجهول» unknown source – قوموا بوضع إشارة بجانب هذه العبارة. ستحصلون عندها على تحذير شديد اللهجة؛ إضغطوا على OK وتأكدوا أن المربع بجانب العبارة جرى اختياره بشكل صحيح.

عند هذه النقطة يمكنكم أن تنفذوا إلى ملف الـ apk المحفوظ في ذاكرة جهازكم أو الموجود في الموقع البديل عن غوغل بلاي ستور؛ قوموا بتنصيبه على جهازكم. كما تشير رسالة التحذير، فإن تنصيب تطبيقات من خارج موقع غوغل بلاي ستور لا يخلو من المخاطر بشكل كامل. المواقع البديلة الوارد ذكرها في القسم التالي كلها تحظى بسمعة جيدة، ولكن يجب أن تعرفوا أنكم تستعملون هذه المواقع على مسؤوليتكم الخاصة. إذا توقفتم عن استعمال التطبيقات من المواقع البديلة، من الأفضل أن تقوموا بإعادة تشغيل خيار الحماية من المصادر المجهولة مجدداً.

البديل الأول: أوبرا أب ستور Opera App Store



إذا كنتم ممن يفضلون استعمال متصفح الإنترنت أوبرا Opera قد تتفاجؤون بأن الخدمة التي تتيح الحصول على تطبيقات أوبرا، أوبرا أب ستور، متوفرة على جهازكم. ستجدون الرابط إلى هذه الخدمة من خلال الصفحة التي تتيح الإتصال السريع على متصفح أوبرا موبايل Opera Mobile. تتوفر الخدمة أيضاً من أي متصفح آخر وليست هناك حاجة لتنصيبها، مما يجعل هذه الخدمة مثالية في بلدان تخضع فيها خدمة غوغل بلاي ستور للحجب.

في الموقع، يمكنكم أن تبحثوا عن التطبيقات عبر قائمة بحث بسيطة. متى ما وجدتم التطبيق الذي تريدون، يمكنكم أن تنقروا زر التحميل نقرة واحدة وسيبدأ عندها تحميل ملف الـ apk على جهازكم. بعد ذلك يتوجب عليكم أن تشغّلوا الملف يدوياً. وصلتنا عدة تقارير إيجابية عن أوبرا أب ستور، ويبدو حتى الآن أن ملفات apk خالية من الفيروسات وبرمجيات التجسس.

الموقع: mobilestore.opera.com

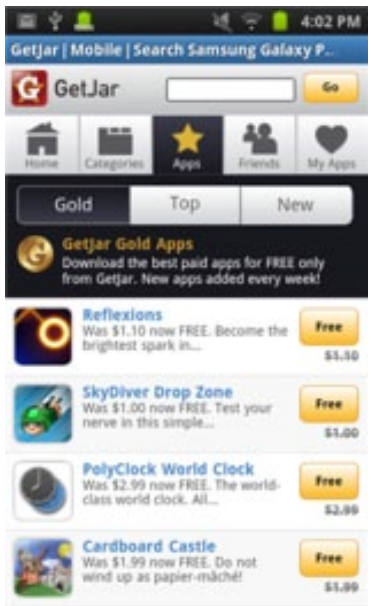
البديل الثاني: وان موبايل ماركت 1Mobile Market

يظهر موقع وان موبايل ماركت، إلى درجة كبيرة، شبيهاً بموقع غوغل بلاي ستور ويتوفر من خلاله أكثر من مئتي ألف تطبيق؛ ستتمكّنون من إيجاد التطبيقات التي تبحثون عنها. عليكم ببساطة أن تدخلوا كلمة في القائمة المخصصة للبحث، أو أن تتصفحوا التطبيقات الموضوعة في فئات مختلفة.

من أجل البدء باستعمال خدمة وان موبايل ماركت عليكم أولاً أن تنصّبوا التطبيق الخاص به على هاتف الأندرويد الخاص بكم. يمكنكم أن تحملوا ملف التنصيب هذا من الرابط المذكور أدناه. يتمتع استعمال وان موبايل ماركت بشعبية واسعة في بلدان مثل سوريا وإيران، وقد أظهرت الفحوص التي أجراها فريق سايبر آرابز أن التطبيقات الأكثر استعمالاً (بما في ذلك تطبيقات الحماية) هي آمنة وخالية من الفيروسات وبرمجيات التجسس.

الموقع: http://www.1mobile.com/app/market

البديل الثالث: جت جار GetJar



من المرجح أن يكون جت جار أكبر متجر للتطبيقات على الإنترنت. يؤمن الموقع الذي جرى تأسيسه في ليتوانيا عام ٢٠٠٤ أكثر من ٣٥٠٠٠٠ تطبيق لأندرويد، بلاكبيري، سيمبيان وأجهزة أخرى. يتمتع جت جار بشعبية واسعة بين المستخدمين والمطورين على حد سواء، بما في ذلك في العالم العربي، بفضل تعدد أوجه استعماله.

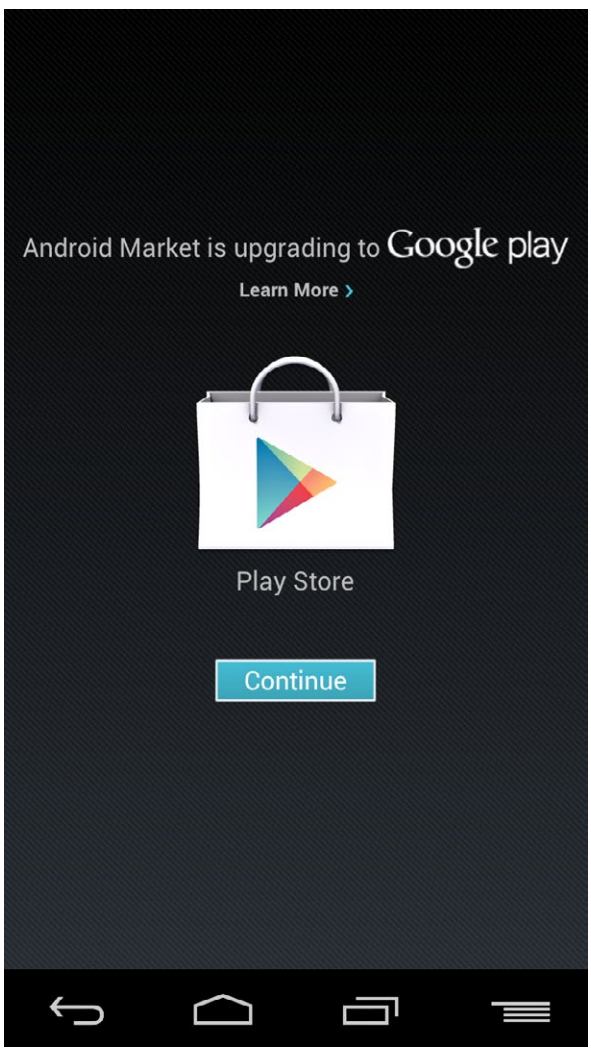
للبدء باستعمال جت جار، أدخلوا الموقع الإلكتروني وابحثوا عن التطبيقات التي ترغبون باستعمالها. عندما تجدون هذه التطبيقات قوموا بالنقر على زر التحميل. عند زيارة الموقع للمرة الأولى، سيتم تحويلكم إلى صفحة حيث سيطلب منكم أن تحملوا ملف جت جار من نوع apk . بعد تحميل الملف وتنصيبه، يمكنكم أن تنفذوا إلى المتجر عبر كل من الموقع الإلكتروني والتطبيق الخاص بالمتجر. يعد التنقل في هذا المتجر الإلكتروني سهلاً وقد أظهرت الفحوص التي أجراها فريق سايبر آرابز أن معظم التطبيقات المتوفرة – بما في ذلك التطبيقات الخاصة بالحماية – آمنة وخالية من الفيروسات وبرمجيات التجسس.

الموقع: www.getjar.com

طرق بديلة للنفاذ إلى غوغل بلاي ستور

إذا كان البلد الذي تعيشون فيه على لائحة البلدان الخاضعة للعقوبات الأميركية، يمكنكم أن تحاولوا تجنب المقاطعة التجارية المفروضة من خلال استخدام طرق مثل شبكات البروتوكول الإفتراضيةVPN ، وأنفاق SSH أو طرق بديلة أخرى. ومع ذلك يجب العلم أنه ليس من السهل خداع غوغل؛ حتى إذا قمتم بإخفاء عنوان الآي بي الخاص بكم عن طريق استخدام طريق بديل (بروكسي)، يظل غوغل قادراً على معرفة موقعكم، وذلك لأن غوغل لا يكتفي بفحص عنوان الآي بي الخاص بكم، بل يفحص علامات أخرى تبين موقعكم، مثل شبكة الهاتف التي تزودكم بالخدمة. حتى الآن، لم ينجح فريق سايبر آرابز بتجاوز الحجب المفروض سوى من خلال شبكة واي فاي بعد نزع شريحة الهاتف.

للقراء الذين يتمتعون بخبرة بالتكنولوجيا أكثر من غيرهم، هناك نسخ معدلة من غوغل بلاي ستور وجدها العديد من قرائنا مفيدة. إلا أن هذه النسخ غالباً ما تتطلب ما يسمى بـ«الروتنغ» وهو إجراء تغييرات أساسية على نظام التشغيل. يمكن إيجاد إحدى النسخ المعدلة من غوغل بلاي ستور هنا:
http://forum.xda-developers.com/showthread.php?t=1582422.



Google play

إنشاء موقع الإنترنت الخاص بكم

أظهر العديد من قراء سايبر آرابز اهتمامهم بإنشاء مواقع إنترنت خاصة بهم. توفر مواقع مثل فيس بوك، بطبيعة الحال، مكاناً لكم على الإنترنت، ولكن هذه المساحة لا تكون بالجاذبية نفسها التي تتحلى بها مواقعكم الخاصة، التي يمكنكم أن تصمموا مظهرها الخارجي كما ترغبون. الخبر السار هو أنه ليس من الصعب إنشاء موقع إنترنت خاص بكم! بينما الخبر السيء هو أن إنشاء الموقع يتطلب جهداً ومعرفة أكثر بكثير من فتح حساب على صفحة فيس بوك. في هذه المقالة سوف نقدم لكم الأمور الأساسية التي يجب معرفتها قبل إنشاء موقع الإنترنت.

موقع الانترنت يتكون من العناصر التالية:

مزود الخدمة المضيف: مزود الخدمة المضيف هو جهة توفر لكم مساحة على القرص الصلب في الخادم الخاص بهم ويمكنكم استخدامها لتخزين موقع على الانترنت وتشغيله. يمكنكم أن تعتبروه على أنه جزء من جهاز حاسوب تستأجرونه من شخص ما، لتشغيل«تطبيق» موقعكم وتخزينه.

تسجيل اسم النطاق Domain Name Registration: هذه ليست خطوة ضرورية لإنشاء موقع على شبكة الإنترنت، ولكن معظم الناس يفضلون تسجيل إسم نطاق خاص بموقعهم على الإنترنت، مثل: www.mywebsite.com. يمكنكم أيضا إعداد موقع بدون اسم نطاق مسجل. في هذه الحالة، سوف يكون الوصول إلى موقعكم أكثر صعوبة بواسطة عنوان يوفره مزود الخدمة المضيف.

نظام إدارة المحتوى CMS- Content Management System : معظم مواقع الإنترنت يتم بناؤها بما يسمى «نظام إدارة المحتوى». نظام ادارة المحتوى هو أحد التطبيقات التي تسهل تصميم موقع الإنترنت الخاص بكم وإدارته. يتم تشغيل نظام إدارة المحتوى على المساحة التي يوفرها مزود الخدمة المضيف. هذا النظام هو الأكثر إستعمالاً وهو يشمل الدروبال Drupal وجملة Joomla وورد برس Wordpress.

لوحة التحكم Control Panel : لوحة التحكم ليست ضرورية، ولكن معظم مزودي خدمة المضيفين (الذين يتقاضون مقابلاً) يوفرونها. وتتمثل مهمتها بإنشاء واجهة سهلة الإستعمال لإدارة الكثير من العوامل التي يمكن تنصبها على خادم الويب. من الممكن أيضاً استخدام لوحة التحكم لتشغيل إخطاطات التنصيب (Installation Scripts) التي تمت تهيئتها مسبقاً لنظام إدارة المحتوى. اذا لم يكن لديكم المعرفة التقنية لتهيئة نظام إدارة المحتوى من الصفر، من الضروري استخدام لوحة التحكم مع إخطاطات التنصيب الآلية. لوحتا التحكم الأكثر إستخداماً هما السي بانل Cpanel والبلسك Plesk ، بالرغم من أن العديد من مزودي الخدمة المضيفين يوفرون النسخة الخاصة بهم.

توفر عدة شركات باقات تحتوي على كافة العناصرالأربعة. وإذا كنتم مبتدئين ومعلوماتكم التقنية ضئيلة، ستكون هذه الطريقة الأنسب لكم. إذا قررتم ضبط كل شيء بنفسكم، ستكون الخطوات أصعب. إن إنشاء موقع على الإنترنت من الصفر يتطلب فهماً شاملاً للتقنيات ومهارات أساسية في البرمجة. ولكن لن نناقش هذا الموضوع في هذا المقال.

هناك خطوة مهمة جداً في انشاء أي موقع على الإنترنت وهي معرفة الهدف من ورائه. هل تريدون إنشاء مدونة؟ أو هل لديكم النية باستعمال ميزات أكثر تقدماً؟ هناك أمور أخرى يجب التفكير بها قبل البدء في إنشاء الموقع: كم عدد

الأشخاص الذين تتوقعوا أن يزوروا الموقع؟ وماذا سيفعل هؤلاء الأشخاص ؟ هذه الأمور مهمة ويجب أن تعرفوها لأن معظم المضيفين يقدمون خدماتهم في باقات مختلفة مفصلة لكل مستخدم حسب الطلب والحاجة. وإلى جانب العناصر الأربعة المذكورة أعلاه، الأمور التي من المهم البحث عنها في كل باقة هي التالية:

المساحة: ما هو مقدار المساحة الفارغة التي يمكن استخدامها لإنشاء الموقع؟ يستهلك أي موقع عادي على الإنترنت ما لايزيد عن بضع مئات ميغابايتات (بما في ذلك الـ CMS). ولكن إذا أردتم أن تضعوا مقاطع فيديو أو ملفات كبيرة على الموقع الخاص بكم، يجب أن تتأكدوا من توفر المساحة الفارغة الضرورية.

عرض الحزمة Bandwidth: الأمر الأكثر أهمية من المساحة هو عرض الحزمة الشهري المسموح بإستخدامه شهرياً، أي مقدار حركة الإستعمال التي يستهلكها الموقع الخاص بكم. إذا قام ألف شخص بزيارة الموقع كل يوم، فذلك يعني أنه جرى تحميل الموقع وجميع مكوناته ألف مرة. إذا كان الموقع متوسط المستوى ويحتوي على نص وبعض الصور، فهو لا يستهلك في العادة أكثر من بضع مئات ميغابايت لألف زائر. ولكن إذا سمح للزائرين بتحميل ملفات ومشاهدة مقاطع الفيديو، سيزيد الإستهلاك بشكل كبير. أكثر مزودي خدمة يمنعون الوصول إلى الموقع إذا تم تجاوز الكمية التي تم شراؤها.

مدة الخدمة: الخدمات المضيفة وتسجيل النطاق تستمران دائماً لفترة زمنية محدودة وهي في العادة سنة. تأكدوا من أن تعرفوا ما هي مدة العقد قبل شراء أي شيء.

الدعم: هناك الكثير من الأمورالتي يمكن التعرض إليها أثناء تهيئة الموقع على الإنترنت. لهذا السبب من المهم أن يكون لديكم شكلاً من أشكال الدعم، أو مكتباً للمساعدة، أو شخصاً يمكنكم اللجوء إليه.

ما هو مزود الخدمة الذي ينبغي أن تختاروه؟

لا يوجد إجابة عامة عن هذا السؤال. يعتمد هذا الأمر على ماذا تريدون من الخاصيات المذكورة أعلاه ويعتمد أيضاً على أشياء مثل، أين تعيشون؟ وما التكاليف التي تقدرون على تحملها؟ إذا كنتم تريدون مساعدة بلغتكم الأم، على سبيل المثال، فالمزود الأجنبي ليس خياراً جيداً. ولكن إذا كنتم تريدون أن تبقى بيانتكم بعيدة عن متناول السلطات المحلية،

يجب استبعاد خيار استضافة داخل بلدكم. يتلقى موقع سيبر آرابز الكثير من الأسئلة عن مزودي الخدمة المجانية. هناك منظمات مختلفة تقدم بعض خدمات الإستضافة مجاناً، ولكن ليس كالتي تحصلون عليها من مقدمي الخدمات المدفوعة. لا نوصي باستعمال الخدمة المجانية إذا كنتم جادين في العمل على الموقع الخاص بكم.

مواقع التدوين

إذا كنتم مهتمين فقط بإنشاء مدونة، هناك بعض الخدمات المجانية الجيدة المتاحة لإنشاء المدونة الخاصة بكم. للغة العربية، يوصي سايبرآرابز بالخدمات الثلاثة التالية:

Blogger.com يتم تشغيل هذه الخدمة بواسطة غوغل وهي تقدم لكم واجهة بسيطة لإنشاء المدونة وصيانتها. يمكنكم تغيير الشكل الخارجي من خلال اختيارتصميم من مجموعة واسعة من التصاميم. ولكن يجب أن تعرفوا أن هناك مواقع أخرى تستعمل التصامم نفسها، مما يعني أن تصاميمكم ليست فريدة. يمكن أيضاً دمج المدونة بسهولة مع وسائل الإعلام الإجتماعية. كما أن Blogger.com يتيح للمستخدمين إمكانية شراء إسم مجال خاص مثل www.mywebsite.com . ولكن هذه الخدمة غير مجانية.

Wordpress.com تقدم هذه الخدمة لكم وظائف مماثلة لتلك التي يقدمها Blogger.com، بما في ذلك مجموعة واسعة من المحاور الخاصة بالتصاميم ودمج المحتوى بوسائل الإعلام الإجتماعية وخدمة شراء اسم النطاق الخاص بكم. ولكن بسبب استخدام نظام إدارة محتوى الخاص بـ Wordpress ، يمكنكم السيطرة على بعض الوظائف أكثر مما يمكنكم أن تفعلوا ذلك في Blogger.

Maktoobblog.com هذا تم تصميمه خصيصاً من قبل ياهو لخدمة المتحدثين باللغة العربية. وعلى الرغم من أن Maktoobblog.com يفتقر خيارات التصميم الأنيق والكثير من الوظائف الموسعة التي توفرهما الخدمتان السابقتان، إلا أنه يتفوق عليهما في دعم اللغة. إذا أردتم أن تنشروا المدونة الخاصة بكم داخل العالم العربي، ننصح باستعمال هذه الخدمة.

خدمات المدونات المذكورة أعلاه لا تحتوي على القدر من التعددية في الأداء والسيطرة على التصميم والمحتوى كالمواقع المستقلة. ولكن بالنسبة إلى هؤلاء الذين ليس لديهم مشكلة في ذلك، فإن هذه الخدمات توفر بديلاً رائعاً لإنشاء موقع شخصي.

إذا قمتم بتسجيل إسم نطاق مثل www.mywebsite.com، يرجى أن تكونوا على علم أن أي شخص بإمكانه معرفة تحت أي إسم وعنوان قد جرى تسجيل الموقع الخاص بكم. من الأفضل تسجيل الموقع تحت إسم مستعار إذا كنتم لا تريدون أن يعرف أحد هويتكم على الرغم من أن ذلك غير قانوني.

التخزين السحابي

التخزين السحابي (Cloud Storage) هو التسمية التي تشير إلى تخزين البيانات على الإنترنت عوضاً عن تخزينها على قرص صلب على جهاز الحاسوب. عند استخدام التخزين السحابي، يمكنكم أن تنفذوا إلى هذه المعلومات من أي جهاز حاسوب موصول إلى الإنترنت، كما يسهّل ذلك مشاركة الملفات مع أشخاص آخرين مخوّلين بالإطلاع عليها. في العامين الأخيرين، أصبح التخزين السحابي واسع الإنتشار، لا سيما منذ أن بدأت شركات كبيرة مثل غوغل ومايكروسوفت بتقديم مساحات تخزين مجانية على الإنترنت بسعة عدة جيغابايتات.

يستعمل بعض من قراء سايبر آرابز التخزين السحابي من أجل مشاركة الملفات مع الآخرين. ويضاف إلى فوائد استعمال هذه الخدمة أنّ الملفات تكون على شبكة الإنترنت، مما يعني أنّ نسخة منها ستكون محفوظة في حال طرأ عطل على جهاز الحاسوب الخاص بكم. إلا أن هناك بعض المساوئ التي تأتي مع استخدام التخزين السحابي. باستعمال الإنترنت لتخزين الملفات، أنتم تضعون ثقتكم بشخص آخر لا تعرفونه، مما يعد نقطة ضعف من ناحية الأمان.

فعلى سبيل المثال، في حزيران/يونيو ٢٠١١ أصبح كل المحتوى المخزن في دروب بوكس Drop Box متاحاً أمام الجمهور لفترة من الزمن، وذلك بسبب خطأ برمجي. ولذلك ينصح فريق سايبر آرابز باستعمال أدوات تشفير مثل تروكريبت (يمكنكم أن تجدوا دليلاً إلى استعماله هنا (bit.ly/PCqj9F) في حال أردتم أن تخزنوا معلومات حساسة على الإنترنت.

تعد تهيئة معظم خدمات التخزين السحابي سهلة. تتطلب العملية تسجيل حساب جديد وتنصيب برنامج صغير يزود جهاز الحاسوب الخاص بكم بمجلد (Folder) جديد يبدو كأي مجلد عادي، مع فرق وحيد وهو أن ملفاتكم ستكون محفوظة على الإنترنت -- من البديهي أنّ التخزين السحابي يحتاج إلى اتصال بالإنترنت. يتيح لكم مزودو خدمة التخزين السحابي النفاذ إلى ملفاتكم من أي متصفح إنترنت طالما لديكم المعلومات الخاصة بالولولج إلى حسابكم.

وبينما تتشابه الخدمات التي يقدمها مزودو التخزين السحابي، يتميز كل منها عن الآخر ببعض الفروقات. في هذا المقال سنقوم بمناقشة

البرامج الأكثر شعبية وهي دروب بوكس Dropbox وغوغل درايف Google Drive ومايكروسوفت سكايدرايف Microsoft SkyDrive وأبل آي كلاود Apple iCloud.

دروب بوكس

دروب بوكس هو واحد من برامج التخزين السحابي الأكثر شعبية ويقدم إلى مستخدميه الجدد مساحة تخزين قدرها ٢ جيغابايت. إذا أردتم الحصول على المزيد من مساحة التخزين يمكنكم أن تحسنوا القدرة الإستيعابية لقاء مقابل مادي، كما تستطيعون الحصول على ٥٠٠ ميغابايت إضافية مقابل كل صديق تدعونه لاستخدام دروب بوكس.

ما يميز دروب بوكس عن باقي الخدمات هو أنه سهل الإستخدام. يمكنكم أن تخلقوا حساباً جديداً في دقيقة واحدة، وبعد تنصيب البرنامج يمكنكم أن تبدؤوا باستعمال مجلد التخزين فوراً. يمكنكم أن تبدؤوا بمشاركة الملفات مع الآخرين بالنقر على حافظة البرنامج وإدخال عناوين البريد الإلكتروني الخاصة بهم. ويقدم البرنامج أيضاً واجهة سهلة للإستخدام، كما أنه يتطابق مع عدة أنظمة تشغيل ويمكن استعماله في نظام اندرويد على الهواتف الذكية وتطبيقات آيفون. كل عمليات التواصل بين جهاز الحاسوب الخاص بكم وبين خوادم دروب بوكس مشفرة باستخدام بروتوكول SSL.

الموقع: http://www.dropbox.com

غوغل درايف

يقدم غوغل درايف خدمات مماثلة لما يقدمه دروب بوكس، منها ٥ جيغابايت للمستخدمين الجدد. ستحصلون على حساب غوغل درايف بشكل تلقائي إذا كان لديكم حساب غوغل. كل ما عليكم فعله هو تنصيب البرنامج على جهاز الحاسوب الخاص بكم. الميّزة الأهم في خدمة غوغل درايف هي أنها متداخلة مع غوغل دوكس Google. Docs يعني ذلك أنّ أي ملف مخزن على هذا القرص يمكن النفاذ إليه من من أي متصفح من دون الحاجة إلى تحميله على جهاز الحاسوب، مما يمنح المستخدم درجة أعلى من الأمان أثناء السفر. يدعم غوغل درايف عدة أنواع من الملفات، مثل فوتوشوب Photoshop ، وأنواع أخرى قليلة الإستعمال.

إذا كنتم تستخدمون خدمات غوغل الأخرى، قد تجدون أن غوغل درايف هو برنامج التخزين السحابي الأسهل استخداماً. يمكن استعمال غوغل درايف على هواتف اندرويد وكل عمليات التواصل مع خوادم غوغل تخضع للتشفير عبر بوتوكول SSL.

الموقع: http://drive.google.com

سكايدرايف

جاءت خدمة سكايدرايف استجابةً من شركة مايكروسوفت لتطور خدمات التخزين السحابي. مثل دروب بوكس وغوغل درايف، يقدم سكايدرايف النفاذ إلى قرص تخزين على الإنترنت من خلال مجلد موجود على جهاز الحاسوب الخاص بكم. من المفيد أن تعرفوا أنّ سكايدرايف يقدم ٧ جيغبايت وليس ٥ جيغابايت مثل بقية خدمات التخزين السحابي الأخرى التي ذكرناها. إذا كانت الأولوية بالنسبة إليكم هي مساحة التخزين، فعليكم اختيار سكايدرايف. مثل غوغل درايف، يقدم سكايدرايف خيار العمل بمجموعة برامج شبيهة بأوفيس على الإنترنت، إلا أن هذه الخدمات تأتي مع ميزات أقل من تلك التي يقدمها منافسو مايكروسوفت.

إحدى أهم ميزات سكايدرايف هي أنه في حال كنتم تستعملون جهاز حاسوب غير ذلك الذي تملكونه، بإمكانكم إحضار أي ملفات لم تقوموا برفعها(Upload) على حسابكم عبر إقامة اتصال بجهازكم الأساسي. بالطبع، يمكن لهذا الخاصية أن تشكل مشكلة أمنية. كل أشكال الإتصال بينكم وبين خادم سكايدرايف مشفرة ببروتوكول SSL.

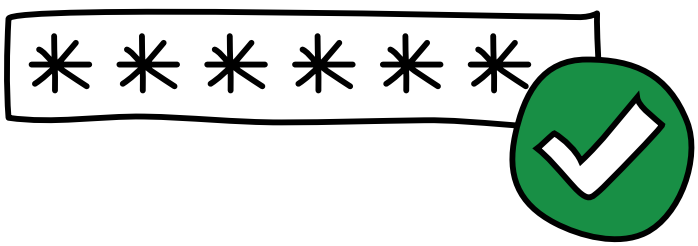
الموقع: https://skydrive.live.com

أبل آي كلاود

خدمة أبل آي كلاود متوفرة فقط لمستخدمي منتجات أبل، ولكن لا يمكن إغفالها في هذه المقارنة. آي كلاود ليست مصممة لتكون قرص تخزين على الإنترنت، بل هي أداة لتخزين الملفات في تطبيقات من أجل توفير عناء إجراء نسخ إحتياطي، مما يتيح للمستخدمين النفاذ إلى ملفاتهم على أي من أجهزتهم. تعد آي كلاود أداة ممتازة لتخزين نسخ احتياطية من ملفاتكم مع المحافظة على كل معلوماتكم الشخصية. كما أنها مناسبة جداً لرفع ملفات وورد، باوربوينت وإكسل. إلا أن آي كلاود لا تقدم لكم المرونة التي يتيحها لكم قرص التخزين، حيث لا يمكنكم أن تخزنوا أي نوع من الملفات، كما تصعب مشاركة الملفات مع الآخرين. إذا كنتم تستخدمون جهاز حاسوب أبل، فإن آي كلاود بالتأكيد ستسهل حياتكم الرقمية وتجعلها أكثر تنظيماً. أما إذا كنتم تبحثون عن أداة تسهل عليكم مشاركة الملفات مع مستخدمين آخرين لا يستعملون أجهزة أبل، عليكم أن تفكروا باستعمال آي كلاود بالتزامن مع إحدى الخدمات الأخرى التي ذكرناها.

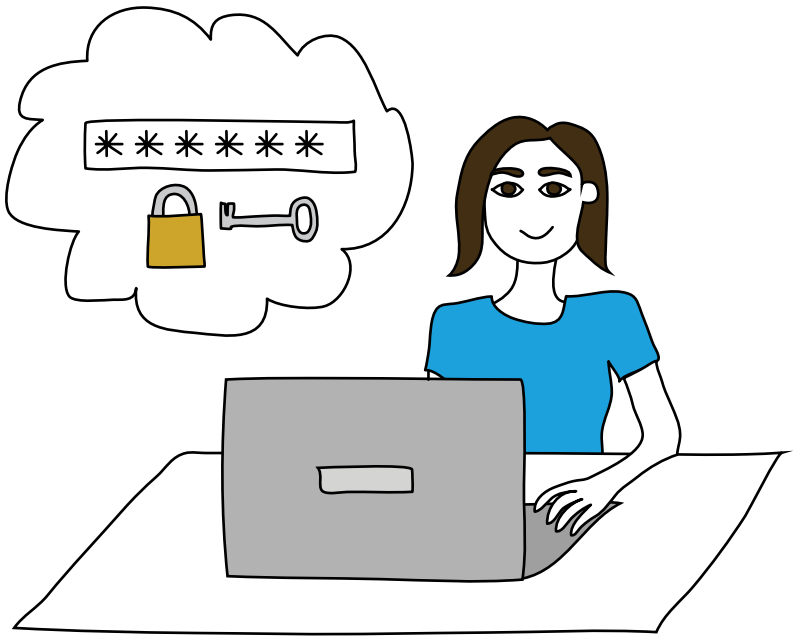
الموقع: http://www.apple.com/icloud

كيفية إنشاء كلمات سرٍّ والحفاظ عليها

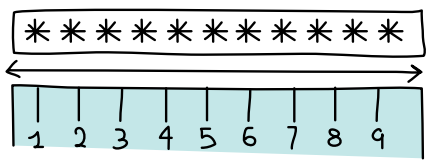


إنّ كلمات السرّ التي يصعب كشفها هي على الأرجح العنصر الأهم في أمن الحاسوب. نستخدم كلمات السرّ لحماية حواسيبنا، وحساباتنا على شبكة الإنترنت، وبياناتنا المُشفَّرة، وبإمكان خطواتٍ معتادة قليلةٍ وبسيطة أن تحمي كلمة السرّ الخاصّة بكم وتحول دون كشفها.

في ما يلي ١١ نصيحةً نقترحها عليكم لإنشاء كلمات سرٍّ آمنة والحفاظ عليها:

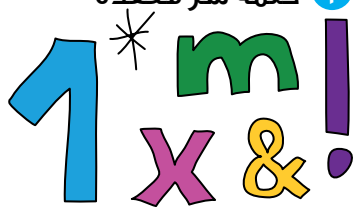


١ كلمة سر طويلة



إحرصوا قدر الإمكان على تأليف كلمة سرّ من ١٤ حرفاً على الأقلّ. غالباً ما يسهل اختراق كلمات السر القصيرة بواسطة برامج متوفرة بسهولة.

٢ كلمة سر معقدة



إحرصوا على استخدام أرقام، وأحرف (لاتينية) كبيرة وأخرى صغيرة، وعلامات وقف، ورموز خاصة. يزيد ذلك الأمر من صعوبة اختراق كلمة السر الخاصة بكم.

٣ كلمة سر عشوائية

~~1 2 3 4~~

4 8 6 5 ✓

تجنّبوا استخدام الأنماط المعتادة والكلمات الموجودة في القاموس. كلمات السرّ المكونة من كلماتٍ ذات معنى يسهل اختراقها وكذلك كلمات السر المؤلّفة من أحرف تسلسليّة مثل ١٢٣٤.

٤ كلمة سرّ غير شخصية

تجنبوا استخدام معلوماتٍ شخصية في كلمة السر. لا تستخدموا أرقام هواتف، وتواريخ ميلاد، وأماكن ولادة، إلخ... بالإمكان اختراق كلمات السرّ هذه من قبل أشخاصٍ يملكون معلوماتكم الشخصية. كما أن كلمة السر إذا تم اكتشافها وكانت شخصية قد تكشف هويتكم أيضاً.

٥ كلمة سر يمكن تذكرها

إحرصوا على إنشاء كلمة سر بإمكانكم تذكرها. إن كتابة كلمة سر على ورقة أو في ملفٍّ على الحاسوب يشكل خطراً على أمنكم.

إستخدموا وسيلة تذكّر لإنشاء كلمات سرّ طويلة ومعقدة يسهل تذكرها:

مثال:

UG3w2d@4PM.Wrur3w?

هي اختصار بالإنكليزية لعبارة:

You get 3 wishes to(2)day at 4PM. What are your 3 wishes?

[لا تقم باستخدام كلمة السر هذه لأنّنا جميعاً نعرفها الآن]

٦ كلمة سر سرية

لا يجب إعطاء كلمات السر بسهولة. بشكل عام، لا يجب تشارك كلمات السر مع الآخرين. إلا أنّه في حال الخضوع للإعتقال، من الأفضل أن تكونوا على معرفةٍ بشخصٍ (ويُستحسن أن يكون خارج البلاد) قادرٍ على تغيير كلمة السر بسرعة.

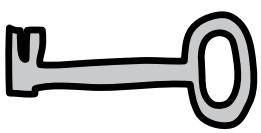
٧ كلمة سر فريدة

إحرصوا على عدم استخدام كلمة السر نفسها لحساباتٍ عديدة. قلّصوا احتمال الضرر الذي قد يتأتّى عن اكتشاف كلمة السرّ عبر استخدام كلمات سر مختلفة لحسابات عديدة. ومن خلال هذه الطريقة، في حال تم اكتشاف كلمة السر الخاصة بحسابكم على موقع «فيسبوك» (Facebook)، لن يتمكّن الفاعل رغم ذلك من النفاذ إلى بريدكم الإلكتروني، وحاسوبكم، إلخ...

٨ تغيير كلمة السر

إحرصوا على تغيير كلمات السرّ بشكل منتظم. قلّصوا المخاطر المحتملة من خلال تغيير كلمات السر الخاصة بكم بشكلٍ منتظمٍ، ولا سيّما إذا كنتم تستخدمون مقاهي الإنترنت أو حواسيب أخرى غير تلك الخاصة بكم. إلا أن كلمات السر الجديدة السهلة الإختراق تعد أكثر خطورة من كلمة السر الآمنة جداً التي تحتفظون بها لوقتٍ طويلٍ.

٩ كلمة سر مخبأة



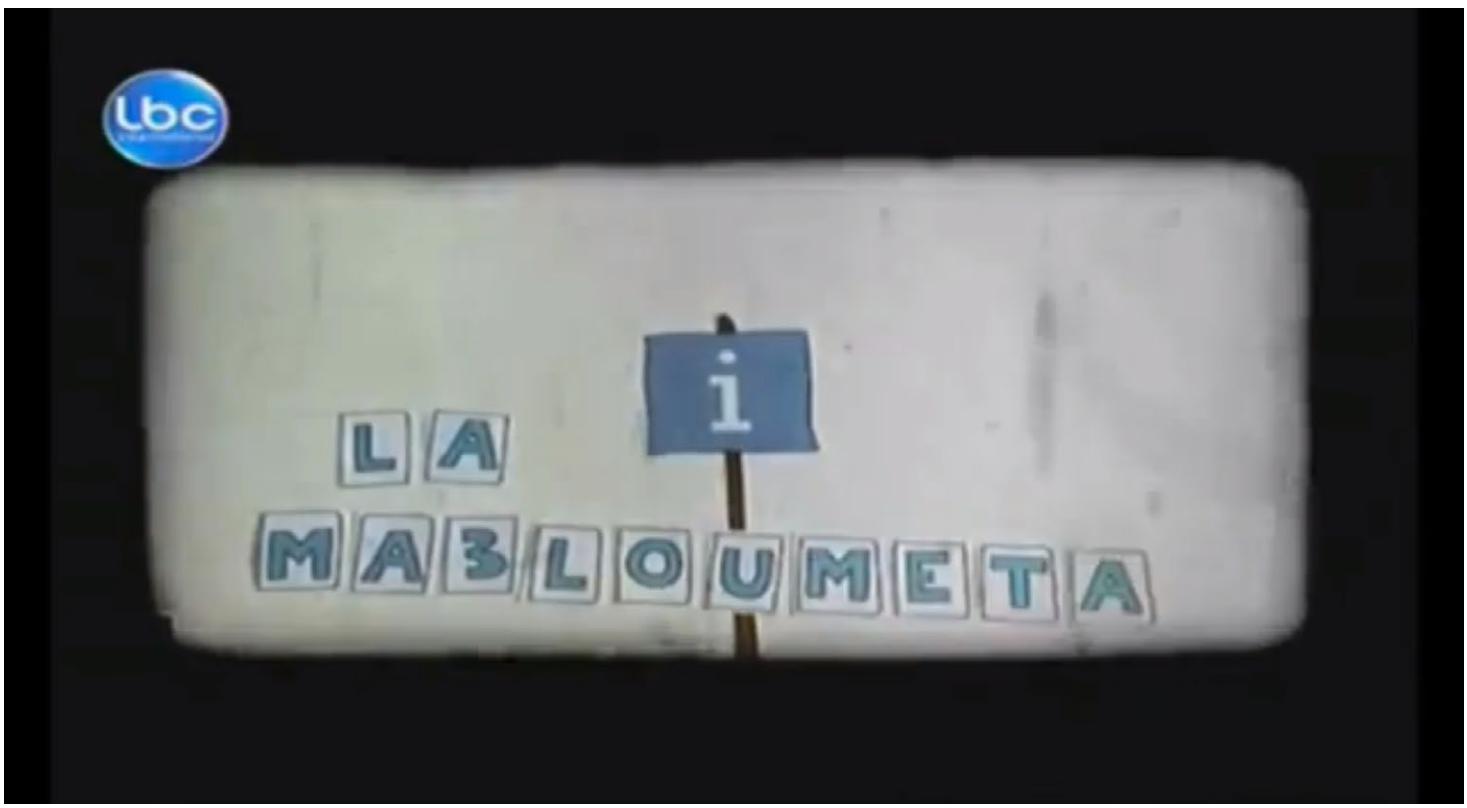
لا ترسلوا أبداً كلمة السرّ الخاصة بكم في نصّ عادي.
إستخدموا كلمة السر الخاصة بكم مع بروتوكول آمن فحسب. احرصوا على عدم إرسالها عبر الشبكة في نص عادي.
نطرح تفاصيل إضافية حول هذه النقطة في المقاطع التالية.

١٠ إطّلعوا على طريقة استعادة كلمة السر

يستخدم العديد من المواقع أدوات لاستعادة كلمات السر، فاحرصوا على أن تكون عملية استعادة كلمة السر هذه آمنة. وتجدر الإشارة إلى أنّ السؤال الذي يساعد على استعادة كلمة السر، إذا كان سهلاً، قد يكون بنفس سوء استخدام كلمة السر السهلة.

١١ إحذروا من طباعة كلمة السر مباشرةً على حاسوب عام

تقوم برامج رصد لوحة المفاتيح بتسجيل أي كلمة يتم طبعها على الحاسوب وبالإمكان سحب كلمات السر بسهولة. وتجدر الإشارة إلى أنّ هذه البرامج شائعة في مقاهي الإنترنت، إلا أنه بالإمكان أيضاً تنصيبها على حاسوبكم الخاص من خلال فيروس. وفي حال استخدمتم حاسوباً عاماً، إستخدموا برنامجاً على غرار «كي سكرامبلر» (Key Scrambler) لتلافي اكتشاف كلمة السرّ الخاصّة بكم من قبل برنامج رصد لوحة المفاتيح.



شاهدو الفيديو على يوتيوب