# cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي



**العدد ١**

غسطس/آب ٢٠١١


ADDRESS

LOGIN PASSWORD

NAME

- عن الحرية والخصوصية والأمن
- كيفية إختيار كلمة سر جيدة
- هل تعرف كل شيء عن الإنترنت حقا
- مصيدة الناشطين السياسيين
- أينما وقع الحجب، فهذا هو موقعي!

# cyberarabs

Digital Security for the Arab World

الأمن الرقمي في العالم العربي




للإتصال بنا:
magazine@cyber-arabs.com


تابعنا على:


أخرج المجلة:
MGSA
لصالح شركة:
tm

## سوزان فيشر

خلال السنوات القليلة الماضية، تحوّلت الإنترنت إلى وسيلة حيوية لحرية تداول المعلومات في أنحاء العالم العربي. وقد إعتمد آلاف المدونين والصحفيين على هذه الوسيلة. إلا أنه مع ارتفاع عدد الأشخاص الذين يستخدمون الإنترنت كوسيلة للتعبير بحرية ازداد في المقابل لدى السلطات القمعية الإدراك والقدرة على تعقّب هذه الحرية المتنامية وتضييق الخناق عليها، وتهديدها.

ويُشار في هذا الصدد إلى أن حكومات عدة في المنطقة قد بدأت بتطبيق مجموعة مواقف حيال الإعلام الاجتماعي والإنترنت، فجعلت من الشرق الأوسط وأفريقيا من بين أكثر البيئات قمعاً لحرية التعبير في الإعلام التقليدي. وفي إطار لعبة القط والفأر هذه، لا يزال العديد من المدونين والناشطين في مجال حقوق الإنسان غير مطلعين بما يكفي على التهديدات الأمنية التي يتعرضون لها خلال استخدامهم لتكنولوجيا التواصل الحديثة.

وتسعى «Cyber-Arabs»، مجلة الأمن الرقمي في العالم العربي، لتضييق هوة المعلومات هذه، وتأمين معلومات باللغة العربية شاملة وسهلة الفهم بشأن الأمن الرقمي والإرشاد نحو كيفية البقاء في مأمن خلال العمل عبر شبكة الإنترنت. وسيجد قراؤنا قصص مستمدة من الواقع مباشرةً حيث يصف الناشطون كفاحهم اليومي، والصعوبات والمخاطر التي تعترضهم، والحلول التي توصلوا إليها. ومن شأن التوصية بالوسائل التي يسهل تثبيتها أن تساعد الصحفيين والناشطين على اتخاذ تدابير الحيطة لحماية أنفسهم. وستقترح تسجيلات فيديو تعليمية بعض أهم برامج الحماية وتصوّر خطوات يمكن للجميع اتخاذها لجعل الكمبيوتر الشخصي أقل انكشافاً. وستشكل المقابلات مع خبراء في مجال التكنولوجيا جسراً بين الناشطين ومجال الأمن.

وأخيراً، يسعى الموقع الإلكتروني لأن يتخطى إطاره كمجرد موقع إلكتروني على أمل أن يشاركنا القراء بخبراتهم ومخاوفهم أيضاً. وأما في المنتدى، فبالإمكان طرح الأسئلة ومناقشتها على أن يتطور الموقع الإلكتروني ليتحوّل إلى منصة وملتقى لمن تهمه مسألة أمنه على شبكة الإنترنت. وبما أن إحدى أهم قواعد الأمن هي أنك أنت آمن بقدر أمن أضعف رابط على شبكة الإنترنت التي تستخدمها، فعلى قدر المشاركة ونشر المعرفة بشأن الأمن كلما أصبحنا بمأمن أكثر.

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

# عن الحرية والخصوصية والأمن

ميراي رعد

## في خضم عيشنا الثورة الرقمية وتطورها، لعلنا نواجه أسئلة جديدة وتحديات تلامس حميمية خصوصيتنا البشرية وحقوقنا.

لقد بات بوسعنا تخزين وتحليل كمٍّ هائل من المعلومات، كما لم نكن نستطيع من قبل. واعتمادنا اليوم على الكومبيوتر والأنظمة الرقمية، غير مسبوق ويزداد باضطراد. فنحن لا نستخدم الكومبيوتر لإدارة الأموال والأصول والثروة فحسب، بل نستخدمه أيضاً طلباً للمساعدة في ما نواجهه من تحديات صحية مثلاً، بل وفي ما نواجهه في حياتنا اليومية عموماً، كما أن لا مشروع ينطلق من دون اعتماد كبير على أنظمة المعلوماتية. لكل منا الآن حضوره على شبكة الإنترنت، مثلاً من خلال مدوَّنة (شخصية أو مهنية). نكتب على «تويتر» ما نأكل، ما نشعر به، وأماكن تواجدنا. ونتشارك مع الآخرين في صورنا حيث تظهر نشاطاتنا والأشخاص الذين رافقونا فيها.

من الطبيعي إذاً أن يُطرح السؤال الأبرز: من يسيطر على كل تلك المعلومات؟ كم تبقى لنا من الخصوصية؟ أي ضمانات نملك بألا يُساء استخدام معلوماتنا الشخصية في المستقبل؟ والسؤال الأكثر إثارة للضحك هو: كيف ستحمينا الدولة، ومن سيحمينا من الدولة في الوقت نفسه؟ فلنواجه الحقيقة: كل الحكومات مصابة بجوع مزمن للمعلومات. الاستخبارات/الأمن/الاقتصاد... الصحة/أنظمة التقييم الاجتماعي، كلها تحتاج إلى المعلومات من أجل توقُّع أنماط مستقبلية، ولتفادي الخروقات الأمنية، وإجراء الدراسات، أو حتى لمجرد إشباع المبدأ الأساسي الذي تقتات عليه الحكومات عادةً: السُّلطة.

لعلك تقول إن هذا «القلق» يبدو، في حد ذاته، مدعاةً للشك، وغير مبرّر. وذلك على اعتبار أن المجرمين وحدهم لديهم ما يخفونه، أليس كذلك؟ أو كما قال الرئيس التنفيذي لـ«غوغل» مؤخراً، مكرراً مرتين وبحزن شديد: «إن كان لديك ما لا تريد لأحد أن يعرفه، فربما ما كان عليك أن تفعله منذ البداية».

وبقدر ما قد يكون مثل هذا السجال صحيحاً، فإن نقطة الضعف الأساسية فيه هي أنه يساهم في تقبّل فكرة أن الخصوصية تعني إخفاء الأخطاء. لكن الأمر ليس كذلك. فالخصوصية حقٌّ إنساني محض، وهو ضروري لاستمرارية الظروف الإنسانية بكرامة واحترام.

لا تضخيم لمفهوم الخصوصية هنا. بل المؤكد أنها حق من حقوق الإنسان الأساسية، وهي أحد المفاتيح لحقوقنا الأساسية الأخرى، مثل الحياة، والحرية، والسعي إلى السعادة.

يخطئ كثيرون إذ يصنّفون السجال في خانة «الأمن مقابل الخصوصية»، قائلين إن علينا إجراء تسوية ما. لكن الخيار الحقيقي هو ما بين الحرية والسيطرة. الطغيان هو الطغيان، بصرف النظر عما إذا أتى بفعل تهديد بضربة فعلية من الخارج، أو أتى نتيجة لتمحيص محلي سلطوي. الحرية تتطلب الأمن،

بلا تدخل. والأمن يجب أن يترافق مع الخصوصية. فتوسيع صلاحيات المراقبة، من قبل الشرطة، هو فعلياً ما يشكّل تعريف الدولة البوليسية. لذلك، علينا الاحتفاء بالخصوصية وتقديرها، حتى عندما لا يكون لدينا ما نخفيه.

إذا أصيبت السلطة بالفساد، فإن هذا الفساد سيطال مجرى المعلومات، الصافي والمتجدد، بخصوص كل إنسان موجود في كل من التفاصيل التي ذكرناها أعلاه. عندها يجب على كل منّا أن يسأل: ما الذي يُعمل بمعلوماتي؟ هل يحق لي استعادة معلوماتي من نظامك؟

هكذا، إن كنت مواطناً إلكترونياً (e-citizen) ويساورك القلق أحياناً على «أمنك» و«خصوصيتك»، فإن لديك الكثير لتقلق بشأنه. فهناك الحكومات ووكالات الاستخبارات المتعطشة دوماً للسلطة، وهناك الشركات التي تريد «بيع» معلوماتك الشخصية، ثم الأشخاص الذين قد يتمكنون من الوصول إلى أنظمة المعلومات وإساءة استخدامها من دون إذنك (مثل «هاكرز القبعة السوداء» ورفاقهم). إضافة إلى أنه عليك الموافقة على كمٍّ من التراخيص والقوانين الملتبسة.

للأسف، تتسع الفجوة بين التكنولوجيا والقانون على الدوام. لذلك، نحن بحاجة إلى أجسام قضائية ملمّة بالتكنولوجيا، بحيث تُكوّن فهماً أعمق للمسائل المطروحة عليها، حتى في وجود قوانين جيدة. وهناك أيضاً عقيدة الطرف الثالث. فحين تتواصل مع طرف آخر، إن كان عبر الهاتف، البريد الإلكتروني، أو برسالة، فإنك تجازف دائماً بأنه قد يكشف مضمون تواصلكما هذا على الملأ أو بفعل تطبيقه للقانون. وبالتالي، فإنه لا يعود بوسعك توقُّع ما سيفعله الطرف الثاني فيؤثر على خصوصيتك.

لكن هل يعتبر موقع «ياهو» طرفاً في سياق استخدامك للبريد الإلكتروني؟ هل يكون «غوغل» طرفاً في ألبوم الصور «بيكاسا» أو خدمة «وثائق غوغل» المشتركة؟ هل شركة «آبل» طرف في الأسماء والعناوين التي قد تحفظها على «موبايل مي»؟ إن كانوا كذلك، فبوسع الحكومة الاستحصال على تلك المعلومات من دون مذكرة خاصة، ومن دون الحصول على موافقتك المسبقة. وثمة دائماً طريقة لطلب لائحة «بتعاملات الإنترنت» بشكل مباشر، وبلا تصاريح، تماماً كما يمكن للشرطة أن تطلب لائحة الاتصالات الهاتفية من دون مذكرة خاصة تسمح لها بذلك.

## فكيف، إذاً، يمكن للأشخاص حماية معلوماتهم الشخصية والخاصة، وفي الوقت نفسه التمتع بميزات الإنترنت؟

لقد تطورت طرق التشفير، بشكل كبير، لتلبية مطلب الأمن الافتراضي. وبات المستهلكون اليوميون قادرين على حيازة أدوات التشفير التي يصعب اختراقها، حتى من قبل الجهات الرسمية المولجة بتطبيق القانون.

لكن ماذا لو استطاع مطبّقو القانون هؤلاء اختراق التشفير فعلاً (وهم ينجحون في ذلك في أحيان كثيرة)؟ وماذا لو استطاعت الحكومة الحصول على المعلومات من خلال موزّع خدمة الإنترنت، والذي ربما يوجد في نظامه «باباً خلفياً»، بالرغم من التأكيدات الكثيرة بأن المعلومات محمية بـ«كلمة السر» وأنها ستبقى خاصة؟ فبحسب المحكمة، وبالمعنى الحرفي المادي، فإن وضع «قفل» على الباب ليس ضرورياً لخلق توقّعات

مقبولة ومنطقية بشأن الخصوصية. والحاصل أن التوقّعات بشأن الخصوصية على الإنترنت غالباً ما ترتكز إلى مدى سهولة أو صعوبة أن يكون الشخص موضوع «بحثٍ مُجدٍ» على الإنترنت. في حين أن المنزل، كبناء ومكان ومحتويات، يُعتبر ذا خصوصية شخصية عالية رغم سهولة دخوله من حيث المبدأ.

فإذا كانت حقائبنا، وشنط ملفاتنا، وألبومات صورنا خاصة ولها حُرمة، فلماذا إذاً لا تنطبق الحُرمة عينها على صورنا المحفوظة على موقع إنترنت أو صفحة ما؟ وعلى بريدنا الإلكتروني؟ وسائر الملفات التي «نحملها معنا أينما ذهبنا» ونتناولها افتراضياً عبر الإنترنت؟ فتلك الوثائق أو «الأغراض» لا تفقد مكوّنها الشخصي والحميم لمجرد أنها أصبحت رقمية.

لا شكّ في أننا أمام نقطة تحوّل في هذا المضمار، وأقل ما يمكن قوله هو أنه يجب علينا المطالبة بحقوقنا الإلكترونية بعد أن نكون قد أصبحنا واعين لها تماماً. فاستخدام التكنولوجيا ما عاد خياراً من الخيارات المطروحة، ولا هو «تأقلم». أضحت التكنولوجيا حاجة أساسية وعلينا المطالبة، ليس فقط بحق الوصول إلى المعلومات، إنما أيضاً بحق السيطرة التامة على معلوماتنا رغم الشبكات المترابطة، بشكل جنوني، و«الاتفاقات» المعقّدة.

ميراي رعد

# هل تعرف كل شيء عن الإنترنت حقاً؟

## ١٢ سؤالاً وجواباً للتعريف بالإنترنت

**رغم العدد الكبير والمتزايد لمستخدمي الإنترنت حول العالم، فإن قلة قليلة منهم فقط تعرف ما هي الإنترنت بالضبط، وآلية عملها، إذ يكتفون بكونهم مستخدمين تجاريهم الشبكة في سهولة استخداماتها من دون أن تتكشف أمامهم بالكامل. وهذا ما قد يضع المستخدمين، من الفئات كافة لا سيما الناشطين منهم، وسط عالم مجهول الخريطة والقوانين، فيصبحون عرضة لمخاطر محتملة كثيرة.**

**هنا عدد من الأسئلة، البسيطة إنما مهمة، وسيجد الكثيرون الإجابات عنها مفيدة لجهة المعرفة والحماية.**

### ١- ما هي الإنترنت؟

الطريقة الأبسط لمعرفة ماهية شبكة الإنترنت، وآلية عملها، هي مقارنتها بشبكة الهاتف الأرضي التي نعرفها جيداً. إذا، وببساطة فإن شبكة الإنترنت هي شبكة تشبه تلك المستخدمة للهواتف تماماً، إلا أن جهاز الكومبيوتر الموجود على كل طرف (بدلاً من الهاتف) يمكّننا من تمرير قدر أكبر بكثير من المعلومات أو مجرد صوت المتصل، إذ يمكن من خلال الشبكة تبادل كافة أنواع البيانات.

### ٢- كيف تعمل الإنترنت؟

لنعد إلى نموذج الهاتف الأرضي. فأنت حينما تتصل هاتفياً من منزلك برقم ما في الولايات المتحدة، ماذا يحصل؟ أنت أولاً تطلب هذا الرقم من مقسم الهاتف في منطقتك، وحين «يستوعب» هذا المقسم أنك تتطلب رقماً خارج المنطقة، يحولك إلى مقسم المدينة أو الدولة الذي «يستوعب» بدوره أن هذا الرقم خارجي، فيقوم بتحويلك إلى مقسم الولايات المتحدة الذي سيتعرف أيضاً إلى الولاية المطلوبة ويصلك بها، وهكذا... حتى تصل إلى الرقم المطلوب بدقة. هكذا تعمل الإنترنت بالضبط، وحين يتم الاتصال يمكنك تبادل كافة البيانات التي تسمح بها الإنترنت بالصوت والصورة والنصوص والفيديو الخ...

### ٣- ما هو عنوان الـIP؟

كما أن لك رقم هاتف يمكن لأي شخص يريدك أن يتصل بك من خلاله، كذلك في عالم الإنترنت يجب أن يكون لديك عنوان (IP Internet Portal) تجري من خلاله الاتصالات وتستقبلها عليه. يكون العنوان على هذا الشكل، ويعتمد المبدأ نفسه لرقم الهاتف: أولاً رمز البلد، ثم رمز المدينة، ثم رمز المنطقة، ثم رقمك الشخصي، مثلاً: ٢١٢,٣٠,٤٢,٢٠

### ٤- ما هو الـ DNS؟

بعد اختراع الإنترنت، تبين أنه من الصعب جداً على المستخدم أن يحفظ رقم الـ IP لكل موقع يريد زيارته، فرفدوا اختراعهم بـ«مترجم» يقوم بترجمة هذه الأرقام إلى حروف. فمثلاً أنت تكتب google.com والمترجم يعرف أنك تقصد ٢٠٩,٨٥,١٣٥,١٠٤ وهو الرقم المخصص لـ«غوغل» فيحولك إليه. جرّب كتابة هذا الرقم بدلاً من «غوغل» وستحصل على النتيجة نفسها من دون خدمات المترجم. لكن هل يمكنك حفظ كافة أرقام المواقع؟ طبعاً لا، لذلك فهذه الخدمة مفيدة جداً، علماً أن DNS هي اختصار عبارة Domain Name System.

## ٥- ما هو مزود خدمة الإنترنت أو ISP؟

كما في الهاتف الثابت، كذلك في الإنترنت، أنت بحاجة إلى من يزودك بهذه الخدمة ويكون صلة الوصل بينك وبين الشبكة العالمية. وتتدرج مزودات خدمة الإنترنت، من حيث الحجم، على الشكل التالي: تصل الإنترنت إلى بلدك من طريق المزود العالمي لهذه الخدمة بواسطة كوابل ضخمة تعبر المحيطات والقارات، ثم يقوم المزود الوطني في بلدك بتوزيعها عبر شبكة خاصة على كافة المدن حيث توجد مزودات أصغر، ثم من مدينتك إلى الحي الذي تسكن فيه، ثم إلى بيتك أو عملك.

## ٦- ما هي سرعة الإنترنت ولماذا هي ضرورية؟

تخيل أن الإنترنت عبارة عن قسطل مياه، والمياه التي تجري فيه هي المعلومات المرسلة والمستقبلة، فكلما كان هذا القسطل أعرض كلما تمكن من تمرير كمية أكبر من المياه. فقط استبدل وحدة القياس من ليتر مثلاً، إلى كيلو بايت في الثانية. كل ما ترسله وتستقبله عبر الإنترنت له حجم معين، إن كان فيديو أو صورة أو نصّاً، وما يؤثر في سرعة الإنترنت في إرسالها أو استقبالها هو عرض الحزمة، وعدد الأشخاص الموزعة عليهم. وفي بلداننا قد تأخذ مزودات الخدمة حزمة غير كبيرة وتوزعها على عدد كبير جداً من الناس فتصلنا الإنترنت قطرة قطرة!

## ٧- كيف تتم مراقبة الإنترنت؟

إذا كنت تتصل بصديق من هاتفك الأرضي، فمن البديهي أن أي هاتف آخر موصول على الخط، بينك وبينه، سيسمعكما بوضوح، إن كان الهاتف المراقِب في صالون منزلك، أو تابع لأحد سكان البناية الذي قام مثلاً بوصل هاتفه على خطك الذي يمر أمام شقته، أو في أحد المقاسم الكثيرة بينك وبين الصديق الذي تحادثه. هكذا بالضبط تتم مراقبة الإنترنت، فهناك جهاز كومبيوتر موجود على الخط بينك وبين جهة الاتصال الأخرى، ويمكنه ببساطة قراءة كافة البيانات التي ترسلها وتستقبلها.

# ١٢ سؤالاً وجواباً للتعريف بالإنترنت

## ٨- ما هو الحل لمراقبة الإنترنت؟

إن الهاتف الأرضي لا يمنحك إمكانية تشفير الاتصال، لكننا نتكلم هنا عن تكنولوجيا متطورة جداً، الكومبيوتر والإنترنت، وهي تتيح لك هذه الخدمة. إذ يمكنك اختيار خدمة بريد إلكتروني مشفر مثل Gmail، أو حتى يمكنك تشفير كافة اتصالاتك الصادرة منك والعائدة إليك عن طريق برامج عديدة.

## ٩- من هم «الهاكرز» أو «قراصنة الإنترنت»؟

إن أول قرصان معلومات في التاريخ هو شخص حفر في منطقة نائية على خط هاتف يصل بين مؤسستين عسكريتين، ثم وصله على هاتفه وتنصت على المحادثات. اليوم ومع التطور التكنولوجي، وكون الجميع موصولاً على الإنترنت، فالقراصنة ليسوا بحاجة إلى الحفر. إذ يمكنهم، وهم جالسون خلف أجهزتهم، اختراق جهازك وسرقة الملفات المخزنة عليه، أو وصل أنفسهم افتراضياً على خطك ومراقبة اتصالاتك على الشبكة.

## ١٠- ما هي الفيروسات أو البرامج الخبيثة؟

هي مجموعة من الأدوات والبرامج والحيل، يستخدمها القراصنة للحصول على معلوماتك التي لا تريد لأحد أن يطلع عليها (إلا بمعرفتك وبإذنك). وهذه الأدوات والبرامج تقدّر بالآلاف، ولكل منها وظيفة وطريقة خبيثة محددة لخرق حصانة جهازك والتجسس عليك. فمنها من يراقب كل ما تطبعه على جهازك ويرسل تقاريراً بها، ومنها ما يستطيع سرقة كلمات السر الخاصة بك، ومنها ما يسمح بمراقبة كافة اتصالاتك أو يمكّن القرصان من رؤية ملفاتك، تماماً كما تراها أنت، وبعضها قد يكون شريراً لدرجة أن هدفه لا يتعدى مجرد تخريب الجهاز أو محو الملفات!

## ١١- كيف أحمي نفسي من قراصنة الإنترنت؟

سلمهم لمن كان بهم خبيراً، أو «أعطِ الخبز لخبّازه». فالقراصنة يستخدمون برامج وأدوات وثغرات وحيل كثيرة جداً لاختراقك، ويستحيل عليك أن تحاربهم بمفردك. لكن، في المقابل، هناك شركات عملاقة لديها مئات الخبراء المتخصصين في محاربه القراصنة، وهذه الشركات تقدم لك برنامجاً جاهزاً أسمه «أنتي فيروس»، لديه قاعدة بيانات تتعرف على الآلاف من أدوات القراصنة وتبطل عملها. أختر لنفسك برنامج «أنتي فيروس» ونصّبه فوراً.

## ١٢- التحديث التحديث أو Updates! ما نفعها؟

إذاً هي حرب دائرة، على أرضك أنت، بين قراصنة المعلومات وخبراء الحماية. فلا تحارب عدو اليوم بسلاح البارحة لأنك ستهزم قطعاً. كل برامج الحماية وأنظمة التشغيل، وحتى البرامج العادية تؤمن تحديثاً دائماً لدفاعاتها، وتغلق كل يوم ثغرة جديدة في وجه القراصنة، فاحرص على أن تمتلك أحدث برامج محاربتهم ولا ترفض تحديثاً (update) خصوصاً أنها عادة مجانية ولا تتطلب وقتاً أو جهداً.

# مقهى الإنترنت في سورية:
## مصيدة الناشطين السياسيين

رامي نخلة

**كان كل شيء يجري بشكل طبيعي واعتيادي بالنسبة إليهما في تلك الليلة. جلسا بالقرب من بعضهما البعض في المقهى الإلكتروني يعملان ويتناقشان همساً. كانا يعتقدان فعلاً إن الجميع مشغولون عنهما، كل بشؤونه وعمله. فجأة، قطع الهدوء المعتاد مجموعة من الرجال حاملين أسلحة رشاشة. دخلوا المقهى وصرخوا في الحاضرين، فدبّ الرعب، ووقف الجميع مخرجين بطاقاتهم الشخصية كما أُمروا.**


«تحدث صاحب المقهى إلى قائد المجموعة الأمنية»، كما يقول عهد الهندي (٢٦ عاماً) وهو ناشط سوري يقيم حالياً في الولايات المتحدة. «ما هي سوى إشارة واحدة من عينيه باتجاهي، وصديقي، حتى أظلمت الدنيا في عيوننا طوال شهر وأربعة أيام في أقبية فرع الأمن السياسي في سورية». هكذا، يشرع عهد في رواية قصة اعتقاله وتعرضه للعنف النفسي والجسدي من قبل المخابرات السورية، إثر نشاطه على الإنترنت مع مجموعة من الشباب، عام ٢٠٠٧، لتأسيس ما أطلقوا عليه إسم «شباب سورية من أجل العدالة». لم يكن عهد وأصدقاؤه يدركون حينئذ خطورة استخدام مقاهي الإنترنت، على خصوصية عملهم، مما أدى إلى اعتقاله مع صديقه واكتشاف أمر المجموعة بالكامل، بالإضافة إلى أن قوى الأمن حصلت على لائحة بأسمائهم، ووثائقهم الخاصة كافة، لا سيما المراسلات التي تمت بينهم وبين جهات أخرى.

«حتى تلك اللحظة التي عصبوا فيها عيوننا، ووضعونا في صندوق سيارتهم الستايشن، كنا نعتقد المقاهي الإلكترونية أكثر أماناً من جهاز الكومبيوتر الشخصي لأنها لا تكشف عنوان الـIP الخاص بنا»، يقول عهد. من الواضح أنه كان مخطئاً. فخلال التحقيق معه، عرض عليه عدد كبير من صوره الشخصية، والتي بدا أنها التقطت له في أيام مختلفة عن طريق الـ«ويب كام» (كاميرا الإنترنت) المثبتة على جهاز

# مصيدة الناشطين السياسيين

الكومبيوتر في المقهى. كما وجد في ملفه صوراً لسطح المكتب (سكرين شوت) وتقريباً كل بريد تلقّاه أو قام بإرساله، بل إنه وجد صوراً لكلمات قام بالبحث عنها على محرّك غوغل.

يرى عهد اليوم إنه أخطأ بشكل أساسي حين اعتمد مقهى إنترنت واحداً، فزاره بشكل متكرر. ذلك أن صاحب المقهى يملك الصلاحية والإمكانية التقنية لمراقبة سطح المكتب على كل أجهزة الكومبيوتر في المقهى. وهذا ما سمح له بحفظ وجهه هو وصديقه، وملاحظة نوع النشاط الذي يقومان به على الإنترنت، فأبلغ أجهزة المخابرات التي تفرض عليه التعاون معها. كما أن تردد عهد وصديقه على المقهى نفسه أتاح لصاحب المكان مراقبتهما لفترة طويلة، وتوثيق تفاصيل نشاطهما، إلى أن اكتملت الصورة لدى أجهزة الأمن وتحركت لاعتقالهما. وينتبه عهد الآن إلى أنه «في تلك الفترة لم تكن تُطلب منا بطاقتنا الشخصية لدى الدخول إلى المقهى. فلو أننا لم نقصده تكراراً، لما تمكنوا من القبض علينا لأننا كنا نعمل بأسماء افتراضية».

أُخلي سبيل عهد وصديقه بعد شهر وأربعة أيام، تعرضا خلالها لمعاملة قاسية وممارسات ترهيبية، وانتهى بهما الأمر إلى التوقيع على تعهد بعدم الانخراط في أي نشاط يتعلق بالشأن العام. كما استمر الضغط على عهد، في جامعته، مما اضطره إلى مغادرة سورية ومتابعة دراسته كلاجئ سياسي في الولايات المتحدة. ولا تزال الضغوط والتهديدات على عائلته مستمرة حتى اليوم.

من جهته، تعرض محي الدين عيسو، وهو كاتب صحافي وناشط في لجان إحياء المجتمع المدني في سورية، لموقف مشابه. ولا داعي للإشارة إلى أننا نسمع ونقرأ كل يوم عن أشخاص اعتقلوا في سورية والعالم العربي وفي كل الدول المقيّدة لحرية التعبير لا سيما على الإنترنت.

«كانت التجربة الأولى لي في فرع المخابرات كمعتقل»، يقول محي الدين. «لم أكن أعلم أن بإمكانهم مراقبة مقاهي الإنترنت بهذا الشكل المبرمج والدقيق، واختراق بريدي الإلكتروني الخاص أيضاً!».

فكما عهد وصديقه، كذلك محي الدين تردد على مقهى إلكتروني، بشكل متكرر، مما سمح لصاحب هذا المقهى أيضاً بملاحظة النشاط السياسي والحقوقي للمستخدم، من خلال تصفح مواقع معينة أو إرسال بريد إلكتروني بمضامين «مريبة» في نظر الأجهزة.

مرة أخرى، فوجئ محي الدين، خلال عملية التحقيق، بأن صاحب مقهى الإنترنت كان مراقباً لنشاطاته على الشبكة الدولية وتوثيقها، بل أنه سلّم جهاز الأمن أيضاً كلمة السر الخاصة ببريده الإلكتروني. ذلك أن المحقق أخذ يتصفح بريده الإلكتروني الخاص أمامه، لا سيما الرسائل المتبادلة مع نشطاء آخرين، ليناقشه فيها واحدة واحدة.

لم يعتقل محيي الدين، وأفرج عنه خلال ساعات تلت التحقيق معه، كونه ناشطاً معروفاً في سورية وسرعان ما أصدرت المنظمات الحقوقية بيانات منددّة باعتقاله. لكنه خسر كل الخصوصية المحيطة بمراسلاته مع نشطاء آخرين وجعلهم هم أيضاً مكشوفين أمام الأمن. وإذا كان انتهاك الخصوصية، من النوع هذا، يجيز للمستخدم، في دول تحترم الخصوصية وحرية الرأي، رفع دعوى قانونية على صاحب المقهى، فإن الواقع في العديد من بلداننا العربية معاكس تماماً.

«نحن ملزمون بالتوقيع على تعهد بالتعاون مع الشرطة السرية كشرط أساسي لحصولنا على رخصة المقهى الإلكتروني»، يقول صاحب مقهى إلكتروني قريب من جامعة دمشق، وقد آثر عدم ذكر اسمه. «هم يتابعون عملنا بشكل دائم، وإذا تأخرنا في إرسال تقارير، أو شعروا بأننا لا نتعاون

# مصيدة الناشطين السياسيين

معهم بصدق، فإنهم يهددون بإغلاق المقهى، والكثير من المقاهي أغلق فعلاً». هكذا، يفرض على أصحاب مقاهي الإنترنت استخدام برامج معلوماتية لتسجيل كل ما يكتب على لوحة المفاتيح، وتتيح تلك البرامج أيضاً أخذ صور لشاشة سطح المكتب، في كل لحظة، لتوثيق كل شيء.

لكن هل يمكن تدارك سلسلة الأخطاء تلك، بغية تصفح أكثر أماناً على الانترنت؟ هنا بعض الحقائق والنصائح التي تتوجه بها أسرة المجلة إلى مستخدمي الإنترنت في العالم العربي:

تجنب، قدر الإمكان، استخدام مقاهي الإنترنت العامة. وفي حال اضطرارك إلى ذلك استخدم جهاز الكمبيوتر المحمول الخاص بك، وتأكد من تشفير اتصالك بشكل كامل. وينصح بشدة بعدم ارتياد مقهى واحد بشكل متكرر مما يتيح لصاحبه تمييز شكلك وحفظه.

**أما إذا كنت مضطراً إلى استخدام المقاهي والعمل على الأجهزة الموجودة هناك، فعليك أن تدرك أن صاحب المقهى الإلكتروني قادر، في أي وقت، ومن دون أي عناء، على فعل التالي:**

١. الحصول على كل كلمات السر الخاصة بالمواقع التي دخلتها، إن كانت حساب بريدك الإلكتروني (جي ميل أو غيرها)، أو مواقع التواصل الاجتماعي، أو مدونتك الشخصية، ولن ينفع أي من برامج التشفير والحماية والبروكسي في تجنيبك ذلك.
٢. رؤية سطح المكتب الخاص بك كما تراه أنت تماماً.
٣. التقاط صورة لكل صفحة تقوم بزيارتها.
٤. تسجيل كل كلمة قمت بكتابتها على لوحة المفاتيح.
٥. الحصول على كافة الملفات والمستندات التي قمت بتحميلها أو إرسالها.
٦. تسجيل أي اتصال صوتي أو دردشة كلامية قمت بإجرائها حتى ولو كانت عبر «سكايب».

**هذه بعض الحقائق التي بات بإمكانك وضعها في الاعتبار لتستنتج بنفسك، في المرة المقبلة، إن كنت ستقبل على مثل تلك المخاطرة أم لا.**

رامي نخلة


## HTTPS Everywhere

HTTPS Everywhere هي إضافة لمتصفح فايرفوكس تؤمن تشفير الإتصال مع عدد كبير من المواقع.

إن أغلب المواقع التي تدعم خدمة تشفير المحتوى المُرسَل والمُستقبَل تركّز عادة على حماية صفحة تسجيل الدخول فقط. أي الصفحة التي يدخل فيها المستخدِم اسمه وكلمة السرّ الخاصة به. لكن بعد ذلك يصبح المحتوى بالكامل غير مشفر. وخير مثال على ذلك موقعا التواصل الاجتماعي، فايسبوك وتويتر، على فرض أن كل ما يقوم به المستخدم ينشر على الإنترنت علناً. لكن ماذا عن رسائلنا الخاصة بين الأعضاء؟ وماذا لو كنا ناشطين بأسماء افتراضية؟ ألا يشكل ذلك خطراً على خصوصيتنا.

إضافة Https لمتصفح الإنترنت فايرفوكس تجبر هذه المواقع، والعديد غيرها، على تشفير كافة البيانات المرسلة والمستقبلة بيننا وبينها، مما يقطع الطريق على أي طرف ثالث يسعى إلى معرفة ماهية هذه البيانات التي قمنا بتبادلها.

**لتحميل وتنصيب الإضافة أنقر هنا**

# تخطي الحجب في البحرين

## مناورة بين أصحاب المواقع و تقنيي السلطة

بعد أشهر قليلة من إعتماد سياسة حجب المواقع في البحرين في يناير ٢٠٠٩، صار تجاوز الحجب باستخدام البروكسيات وبرامج مثل «tor» و«hot spot shield» مهارة بديهية عند المستخدم البحريني، بعد أن سخر عارفي تقنية المعلومات أنفسهم لعمل الشروحات المبسطة وتوزيعها على أوسع نطاق في القوائم البريدية والمواقع الإلكترونية. وفيما ندر كان الوصول إلى موقع محجوب أمراً صعباً، بل ان المشكلة كانت في بطئ التصفح التي تسببه هذه البرامج وغلق منافذ البروكسي دورياً من قبل الدولة ما يضطر المستخدمين إلى تغيير الإعدادت في المتصفح بين الفينة والأخرى.

ولطريقة أكثر أمناً عمد أحد الناشطين الإلكترونيين إلى مخاطبة منظمة pisbon وهي منظمة مغلقة تزود كل عضو بمنفذ خاص لا يمكن حجبه، يستطيع من خلاله الوصول لأي موقع في العالم. وعلى الرغم من عيب المنفذ البسيط وهو عدم قدرته على تشغيل تطبيقات الجافا، وزع الناشط السالف الذكر دعوات عضوية عبر البريد الإلكتروني لشبكة الناشطين والمدونين البحرينيين، الذين بدورهم قاموا بتوزيع العضويات المغلقة على أصدقائهم وأقربائهم، وهكذا لم يعد الوصول إلى الموقع واستخدام أغلب تطبيقاتها مشكلة.

غير أن القصة لا تنتهي هنا، من المعروف أن معظم أصحاب المواقع الإلكترونية هم من محترفي علوم الحاسوب وتقنية المعلومات، أو من الهاويين الضليعين فيها، اذ يندر أن يكلف صاحب موقع بحريني أمر بناء موقعه وصيانته وحمايته إلى شركة استضافة، معظمهم يقومون بهذه الأمور في المنزل ولذا كان هؤلاء على طريقتهم ينشأون وصلات جديدة غير محجوبة إلى مواقعهم تمكن المستخدمين من دخول الموقع وكأن الحجب لم يكن. وعلى غرار الشبكات المغلقة يتم تبادل هذه الوصلات بين التقنيين فالمقربين فالأصدقاء ويمكن أن تستمر الوصلة في العمل لشهر أو أكثر قبل أن تقع في يد أحد مخبري السلطة، فيتم العمل على حجبها. ولكن هذا لا يهم فإن كنت من زائري الموقع «الموثوقين» سوف تصلك رسالة على بريدك الإلكتروني إما من إدارة الموقع أو من متعهدي توزيع الوصلات تحتوي على الوصلة الجديدة للموقع التي ربما تم تجهيزها سلفاً.

أما المنتديات الحوارية والسياسية المهمة فشأن آخر، فتسجيل الأعضاء الجدد فيها وخصوصاً في فترات التأزيم السياسي يكون مغلق، ويتم عن طريق توصية من أحد الإداريين أو الأعضاء الموثوقين والذين يعرفون المستخدم الجديد شخصياً. وتعهد إدارة هذه المواقع في بعض الأحيان إلى منظمات سياسية بحرينية تعمل في الخارج، وهي تحرص على أن لا تستخدم النسخ المقرصنة أو تتهاون في تحديث النسخ وغلق الثغرات. إذ يحدث أن يكتب فيها أحد من السياسيين أو الإعلاميين البارزين بأسماء مستعارة، وحماية قاعدة البيانات في هذه الحالة حماية لحواسيبهم وحساباتهم البريدية. وهذه السياسة الإنتقائية في تسجيل الأعضاء تقلل من احتمالية وصول المخبرين إلى الوصلات الجديدة للمواقع.

الطرفة إذاً، أن أصحاب المواقع الإلكترونية المحجوبة في البحرين لم يتركوا ازعاج المستخدمين يمر مرور الكرام، وحرصوا على الرد بالمثل بتشغيل تقنيي السلطة في تعقب الوصلات الجديدة والعمل على حجبها من جديد.

محمد عبدالله

## IMO

هل تعاني من مشكلة تعدد حسابات برامج المحادثة لديك ؟ (skype, google talk, yahoo MSN messenger,...etc)

هل أنت مضطر لتشغيلها جميعاً كي تتواصل مع أصدقائك كافة؟

هل تقلق من حقيقة أن بعض برامج «التشات» التي تستخدمها لا تؤمن خدمة تشفير المحادثات؟

هل لديك، مثلاً، حسابين على خادم واحد، مثلاً حسابين على Gmail وعليك الاختيار أو تبديل تسجيل الدخول بينهما في كل مرة.

Imo هو موقع على شبكة الإنترنت يعالج تلك المشاكل. فهو يمنحك إمكانية تسجيل الدخول إلى كافة هذه البرامج ضمن صفحة واحدة، ويرتب قائمة الاتصالات لديك بشكل أنيق، وفي الوقت نفسه يمنحك حماية قصوى عن طريق تشفير كافة المحادثات المرسلة والمستقبلة لديك.

جرب تسجيل الدخول إلى هذا الموقع وقم بإضافة كافة حساباتك إليه وسيحفظها بشكل أوتوماتيكي، فيكون بذلك نافذتك الواحدة على كل برامج المحادثة.

**جرّبه على الرابط التالي.**

## Ultra Fast Web Proxy

قد لا تكون بحاجة إلى استخدام «بروكسي» بشكل دائم. فهناك فقط بعض المواقع المحجوبة أو التي ترغب بدخولها بأي بروكسي مختلف، واستخدام بروكسي قد يسبب لك إزعاجاً نتيجة إبطاء سرعة الإنترنت بشكل عام.

هذه إضافة رائعة لمتصفح الإنترنت «غوغل كروم»، فبعد تنصيبها ستظهر أيقونة البرنامج إلى جانب شريط العناوين لديك، ويمكنك الضغط عليها في أي وقت لتفتح نافذة تكتب فيها عنوان الموقع المطلوب أو المحجوب، وبضغط «إنتر» يمكنك تصفح الموقع المحدد بمجهولية عالية.

**لتحميل الإضافة أنقر هنا.**


# أينما وقع الحجب، فهذا هو موقعي!

هكذا أنشئ... وهكذا يستمر رغم اختراقه

عماد بزي

لطالما عملت الحكومات، في العديد من دول الشرق الأوسط وشمال افريقيا، على الحد من قدرات الإعلام والناشطين على الإنترنت. وذلك إما عبر تقييد الإعلام والتعتيم عليه، وإما عبر فرض الرقابة المسبقة بحجب المواقع الإلكترونية المعارضة أو المدوّنات الناطقة بأسماء ناشطين أو مجموعات شبابية. ففي حين تهتم جمعيات متخصصة عديدة حول العالم بتدريب الناشطين على كيفية تخطي الحجب والرقابة الحكومية كضمانة لحرية الرأي والتعبير، إجتمع عدد من الناشطين الإلكترونيين من لبنان ومصر وتونس (قبل موسم الثورات الحالي) وخرجوا بخطة حديثة لمواجهة القمع الإلكتروني، إيماناً منهم بحق الأفراد في الوصول إلى المعلومات.

وقامت الخطة على إنشاء موقع stop404.org الذي يمكن للناشطين أن ينقلوا عبره كل ما يتعلق بالقضايا التي يحاول الإعلام التقليدي طمسها أو تفادي الإعلان عنها. إذ يتكفل الموقع بإعادة نشر كل المواد المنشورة على المدوّنات المحجوبة في الشرق الأوسط وشمال إفريقيا، إضافة إلى المقالات الخاصة، وروابط البرامج التي يتعلم من خلالها المستخدمون تقنيات جديدة، مثل كسر الحجب، والأمان الإلكتروني... إلى أن قامت «ثورة الياسمين» في تونس فتغيرت المعطيات كافة!

فخلال أيام الثورة التونسية، انكبّ مبرمجو الموقع على إعادة هيكلة خطة العمل للحاق بالأحداث ومواكبتها بنقلها إلى القارىء. وذلك ليس من خلال الإعلام التقليدي إنما بالاعتماد على شبكة واسعة من الناشطين على الأرض، وفي موقع الحدث، والذين كانوا يستخدمون آلات الفاكس والرسائل النصية القصيرة إذ تحاشوا اللجوء إلى الإنترنت خوفاً من الرقابة المشددة عليها آنذاك. هكذا، تجلى مبدأ إعلام المواطن للمواطن، بحيادية تامة، إذ نُقلت الأحداث بالنص والصوت والصورة كما هي. ولما كان فريق العمل في الموقع صغيراً (ثلاثة مدوّنين) فقد تأخر قليلاً، غير أن الموقع انطلق أخيراً... وما هي إلا ساعات حتى أعلن عن هرب الرئيس التونسي السابق زين العابدين بن علي.

## ٣٣ متطوعاً من أجل مصر

ثم ما لبثت أن اندلعت الثورة المصرية. أطلق الناشطون والناشطات نداء عبر «تويتر»، طالبين المساعدة والتطوع للعمل على الموقع. وتحولت واجهة الموقع فوراً إلى تصميم وتبويب جديدين، لنقل الأخبار من مصر مباشرة، عبر شبكة واسعة جداً من المواطنين والمدوّنين، فبلغ عدد العاملين في فريق الموقع ٣٣ شخصاً حول العالم، كل يمارس الدور الذي أوكل إليه. ففيما تواجد الفريق التقني في بيروت، والفريق المساند في الأردن، تولى المتطوعون في بريطانيا وألمانيا تنسيق الإتصالات الهاتفية وتسجيلها وبثها على الموقع على هيئة رسائل إخبارية من الناشطين في مصر.

ثم قُطع الإنترنت في مصر بشكل كامل، فكان الإعتماد على الإتصال بالهواتف الأرضية والنقالة، واستمر الموقع في نقل الأحداث المصرية حال وقوعها. إلا أن بعض الناشطين تنبهوا فجأة إلى ثغرة أمنية، أتاحت لهم استخدام الإنترنت من داخل مصر، عبر إستعمال قناة إتصال بالإنترنت، خاصة بالتعامل المصرفي، وهي الوحيدة التي ظلت مفتوحة طوال فترة الثورة المصرية. علماً أن هذه المعلومة تعلن، للمرة الأولى، من خلال المقالة هذه.

والجدير بالذكر أيضاً أن موقع stop404.org كان قد أطلق خدمة «إتصل لترك رسالة تويتر» (call to tweet) قبل «غوغل» و«تويتر» بيوم كامل، وإن بطريقة يدوية وبدائية. إلا أن الخدمة هذه استجلبت إلى الموقع كمية هائلة من الرسائل التضامنية الواردة من حول العالم.

ومع إستمرار الأزمة في مصر وإعتصام المتظاهرين في ميدان التحرير، برزت الحاجة إلى مساعدات طبية. فتطوع بعض الناشطين اللبنانيين والمصريين والسوريين، المقيمين في الولايات المتحدة، لإقامة مركز تنسيق لتسلّم التبرعات العينية والمادية من أجل إرسالها الى المعتصمين في ميدان التحرير. بلغت قيمة التبرعات ١٦ ألف دولار، أعيدت في مرحلة لاحقة إلى المتبرعين نظراً لعدم تمكن الناشطين بداخل ميدان التحرير من تسلّمها

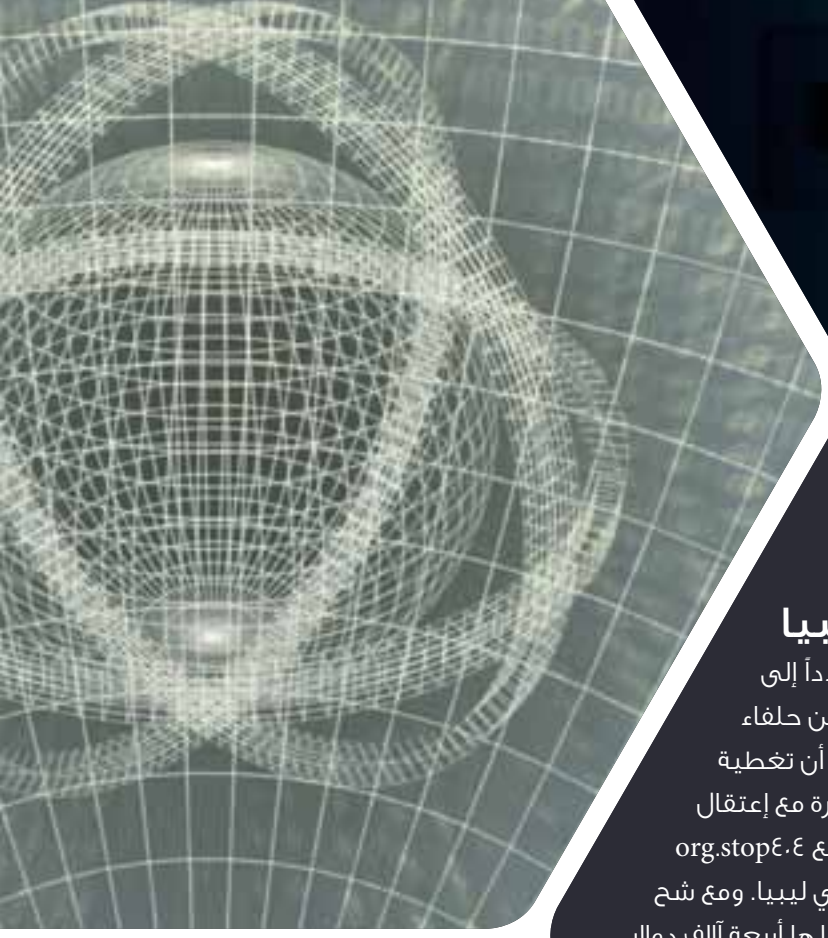
وكي لا تذهب تلك الأموال إلى غير مستحقيها. فكان القرار بالتوقف عن جمع التبرعات المادية، والإعتماد فقط على التنسيق مع مؤسسات عالمية مثل «أطباء بلا حدود» لنقل رسائل من أطباء موجودين بداخل ميدان التحرير تضمنت لوائح بالمواد الطبية التي يحتاجونها.

في هذه الأثناء، استمر العمل الناشط على الموقع بوتيرة عالية، بدعم من الناشطين على شبكات التواصل الإجتماعي، لا سيما «تويتر»، إضافة إلى الرسائل المسجلة بالصوت والصورة من داخل مصر. هكذا، تمكّن العديد من الشبكات الإجتماعية من نقل الأخبار عن الموقع، نظراً لسرعة تحديثه وتقديمه بديلاً متكاملاً عن الإعلام التقليدي، بهمة ونشاط المواطنين الذين ثابروا على تغذية الموقع بالأخبار والرسائل الصوتية، مساهمين بجدية ومناقبية في تسليط الضوء على الحقيقة الميدانية في مصر طوال تلك الفترة. وبذلك، لا يعود مستغرباً أن يبلغ عدد زوار الموقع، في الأيام العشرة الأولى لإنطلاقة الثورة المصرية، أربعة ملايين وستمئة ألف زائر، لا سيما أن بعض المترجمين المتطوعين كانوا قد انضموا إلى فريق العمل لترجمة الأخبار من العربية إلى الإنكليزية والألمانية والفرنسية، سعياً إلى نشر الحقيقة الكاملة في أقصى أصقاع الأرض.

## البحرين والعتب على الإعلام

وبعدما نجحت الثورة المصرية في إسقاط الرئيس السابق محمد حسني مبارك، لم تطل «فترة السماح»، فانطلقت من فورها الحركة الإحتجاجية في البحرين، ومجدداً تغيرت واجهة الموقع وتبيوبه لمواكبة الحدث البحريني. ذلك أن هدف الموقع يقتصر على تأمين فضاء لنقل الأخبار، بسرعة ودقة، لا تحليلها ولا التعليق السياسي عليها. فكان من الطبيعي أن تتحول أولويات الموقع نحو البحرين التي سرعان ما وُجد فيها «حلفاء». هم مواطنون وإعلاميون وناشطون على الإنترنت أبدوا إستعداداً مباشراً للتطوع لتغذية الموقع بالأخبار، خصوصاً في ظل ما اعتبروه تقصيراً إعلامياً من بعض شبكات التلفزة العربية.

ومنذ اليوم الأول، نقل الموقع صوراً حصرية ومقاطع فيديو أرسلها متطوعون ونقلتها وكالات الأنباء العالمية. وكما في مصر، واكب الموقع أحداث البحرين عن كثب، عبر أكثر من ٢٤١١ خبراً و٨٠ صورة، و٢٥ مقطع فيديو، أرسلت كلها من مواطنين وناشطين على الإنترنت إختاروا التفاعل مع الإعلام البديل أكثر من الإعلام التقليدي.



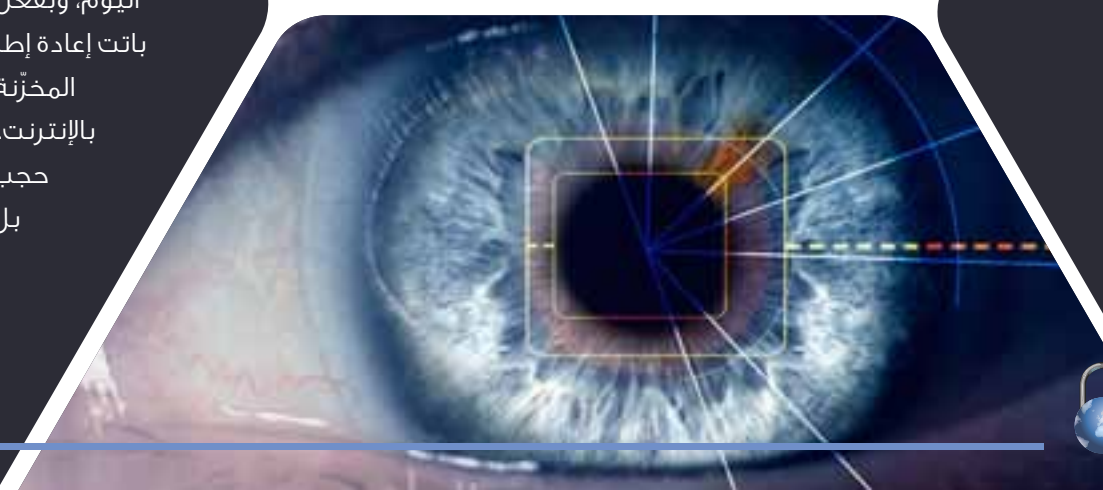

## حجب في ليبيا

وكرّت السبحة. قامت الاحتجاجات الليبية، فانتقل الموقع مجدداً إلى واجهة وتبويب جديدين، بالألوان الليبية هذه المرة، ونجح في تأمين حلفاء جدد هم مدونين وإعلاميين ومواطنين على جري العادة. غير أن تغطية الموقع لمجريات الأحداث في ليبيا بدأت تأخذ منحى أكثر خطورة مع إعتقال صحافيين محليين في بداية إحتجاجات بنغازي. هؤلاء أقروا بتغذية موقع org.stop٤،٤ بالأخبار والصور التي وجدت على كاميراتهم، فتم حجب الموقع تماماً في ليبيا. ومع شح الموارد الإخبارية من قلب ليبيا، قام الموقع بحملة للتبرعات الطبية، جمع خلالها أربعة آلاف دولار تم إرسالها الى بنغازي للمجهود الطبي بمساعدة قافلة مصرية عبرت الحدود المصرية–الليبية لإيصال المساعدات الإنسانية.

## اختراق؟ فليكن!

والحال، إن النشاط الذي لا يخبو على موقع stop٤،٤ يزعج، على ما يبدو، بعض المعارضين للأصوات الحرة حول العالم. ففي الثالث من آذار الجاري (٢٠١١)، وبالرغم من الحماية الإلكترونية القصوى التي يتمتع بها الموقع، جرى إختراقه وحذف بياناته بالكامل. وترافق ذلك مع عملية قرصنة قسرية لإسم النطاق domain take–over hacking أفقدت الشركة المستضيفة بيانات النسخة الإحتياطية back–up وبات الموقع غير متوفر.

اليوم، وبفعل الجهود المستمرة من الناشطين المتطوعين، باتت إعادة إطلاق الموقع قريبة جداً، بعد إستعادة كافة بياناته المخزّنة على أجهزة الناشطين، لا على «خوادم» متصلة بالإنترنت. وسيعود الموقع إلى ممارسة دوره في مكافحة حجب المعلومات في الشرق الأوسط وشمال إفريقيا، بل أينما حلّ خطر يتهدد الحق المكرّس بالوصول إلى المعلومات بإعتباره من اوائل الحقوق التي نصت عليها الشرعات والمواثيق الدولية وفي مقدمتها الإعلان العالمي لحقوق الإنسان.



# الشبكة الافتراضية الخاصة VPN


لأنها الطريقة الأكثر أماناً على الإطلاق للاتصال بالإنترنت في يومنا هذا، لأن تكلفة استخدامها قد تصل إلى درجة المجانية، ولأنها سهلة التطبيق إلى حد نقرة واحدة، لهذه الأسباب سنتطرق في العدد الأول من مجلتنا إلى الشبكات الافتراضية الخاصة، وسنحثكم بشدة على استخدامها.

كي نتمكن أولاً من فهم الشبكات الافتراضية الخاصة سنبدأ بخلفية بسيطة عن الشبكات الواقعية الخاصة ومشكلاتها وكيف أتت الشبكات الافتراضية كحل سحري لكل هذه المشاكل، وطبعا كما وعدنا يمكنكم تجاوز هذا المقطع والانتقال إلى الجزء الأخير من المادة لتطبيقها بنقرة واحدة، لكن من الأفضل فهم لماذا هي آمنة إلى هذا الحد وآلية عملها.

الشبكة الخاصة هي الأم الأولى لشبكة الإنترنت العالمية اليوم، وولدت هذه الشبكة من فكرة وصل جهازين كمبيوتر في غرفة واحدة مع بعضهم البعض بكابل لتسهيل نقل البيانات فيما بينهم، وبعد أن نجحت الفكرة توسعت لتصل كافة أجهزة الكمبيوتر في تلك الشركة بكابلات فيما بينهم، وهكذا كانت الولادة الأولى في بداية الستينات لشبكة واقعية خاصة في مركز أبحاث في وزارة الدفاع في الولايات المتحدة الأمريكية.

ثم ما لبثت العديد من الجهات والمراكز والشركات إلى إنشاء هذا الشبكة الخاصة في مقارها في الولايات المتحدة وغيرها من دول العالم، لكنها بقيت شبكات خاصة منفصلة معزولة تماماً، إلى أن أتت فكرة وصل كل هذه الشبكات فيما بينها في كل بلد ثم وصلها بكابلات عابرة للمحيطات بشبكات الدول الأخرى وهنا كانت ولادة الشبكة العامة أو شبكة الإنترنت العالمية.

بالقدر الذي قدمته هذه الشبكة من حلول وسهلت الاتصال إلا أنها في نفس الوقت خلقت مشكلة أخرى وهي الخصوصية فلا يمكن لأي جهة أو شركة أو وزارة أن تسمح لكل من هم على الشبكة العامة بالولوج إلى شبكتها الخاصة، لذلك كان لابد من إبقاء شبكتها خاصة ومعزولة تماماً، وفيما لو أرادت بعض الأجهزة الاتصال بالإنترنت فهناك جهاز واحد فقط نسميه اليوم «سيرفر» خادم مهمته أن يستلم هذه الطلبات من

الأجهزة ويخرج إلى الإنترنت يحضرها لهم ويعود بها ليوزعها على كل جاهز حسب طلبه.

لكن مع اتساع الشركات الخاصة وتوزع مكاتبها في أطراف مختلفة من المدينة أو الدولة أو حتى القارات كانت هناك مشكلة كبيرة تلوح في الأفق، كيف يمكننا أن نربط كل هذه الفروع المتناثرة بشبكة خاصة أي بشبكة كابلات خاصة تمدها تلك الشركة، هذا شبه مستحيل، لكن ماذا لو تمكننا من الوصل فيما بين تلك الفروع عن طريق شبكة الإنترنت الموجودة فعلياً مع الحفاظ على شرط الخصوصية وانعزال هذه الشبكة الخاصة عن العامة بالرغم من استخدامها.

رداً على هذا التحدي الكبير ولدت تكنولوجيا جديدة نسميها الشبكة الافتراضية الخاصة اختصاراً VPN فكيف تعمل هذه الشبكة؟

بقدر ما يمكن لهذه التكنولوجيا أن تكون معقدة إلا أن الجواب باختصار سهلٌ جداً فما قامت به هو الحفاظ على بنية الشبكة القديمة واستبدال الكابلات الخاصة التي تصل بين أجهزة الكمبيوتر في شركة ما بالكابلات العامة التابعة لشبكة الإنترنت وحافظت على سرية البيانات المرسلة والمستقبلة من خلال خلق نفق خاص مشفر تماماً يمر عبر شبكة الإنترنت ويصل بين جهاز المستخدم أو الفرع أينما كان في العالم بشبكة شركته الرئيسية الخاصة أينما كانت في العالم، فبهذا بات يمكننا تركيب شبكة خاصة حدودها العالم كله، دون أن نمد كابل واحد وبمجرد اتصال جميع الأطراف في الإنترنت، فكان بذلك شبكة خاصة مغلقة ضمن الشبكة العامة.

إذا ماذا يعنينا من كل هذا الكلام نحن كمستخدمي إنترنت ونشطاء ومدونين في العالم العربي؟ فليس لدينا شركات مترامية الأطراف نصل بينها، وكل ما يهمنا هو تجاوز حجب المواقع الإلكترونية التي تضعه حكوماتنا في وجهنا، بالإضافة إلى ضمان خصوصيتنا وعدم إمكانية مراقبة وتحليل وقراءة البيانات الخاصة التي نرسلها ونستقبلها.

ببساطة الشبكة الافتراضية الخاصة هي الجواب والحل الأمثل لهذه المشاكل والمخاوف التي تواجهنا، فهي تتيح لنا تشفير كافة بياناتنا على جهاز الكمبيوتر الخاص بنا ثم ترسلها من خلال مزودات خدمة الإنترنت المحلية وأجهزة الرقابة عبر نفق لا يمكنهم أبداً الإطلاع على محتوياته، وطبعا كون السيرفر أو الخادم الشبكة الافتراضية الخاصة الذي سيقوم بتلبية طلباتنا وإحضار صفحات الإنترنت لنا، موجود في دولة أخرى لا تمارس حجب المواقع فهذا يعني أننا سنتمكن من تجاوز الحجب أيضاً. ولن تتمكن الحكومات ببساطة من إيقاف أو حجب هذه الخدمة (النقل عبر أنفاق مشفرة) كما تفعل مع برامج البروكسي، لأن العديد من الشركات التجارية الكبرى التي يعتمد الاقتصاد عليها ليس لديها بديل عن استخدام الـ VPN وكذلك المؤسسات الحكومية والجيش والوزارات والسفارات وما إلى هنالك.

ويمكننا نحن أيضاً استخدام الـ VPN فكما نعلم أن هناك العديد من الجهات والمنظمات العالمية غير الربحية التي تؤمن بحق المستخدمين في الخصوصية والحرية والحق في الوصول إلى المعلومات، هذه الجهات ومن خلال عملها على هذه القضية لم توفر جهداً للاستثمار في هذه التكنولوجية الجديدة، فاليوم هناك على الشبكة الإنترنت العديد من الأدوات تتمثل في برامج بسيطة يمكن تحميلها وتشغيلها بنقرة واحدة لتضعنا في شبكة افتراضية خاصة بشكل مجاني تماماً لبعض منها أو شبه مجاني في أدوات أخرى.

ومن أشهر هذه الأدوات المجانية بالكامل «هوت سبوت شيلد» قم بتحميله وتشغيله بنقرة واحدة من هنا وكذلك «سيكيورتي كس» يسمح بالحد الأدنى بـ ٥٠ إلى ٣٠٠ ميكا يومياً مجاناً حسب الضغط على الشبكة حمله من هنا وغيرهم الكثير، لكن تثبيتها قد يتطلب أكثر من نقرة واحدة، سنتطرق في أعداد لاحقة إلى تنصيبها خطوة بخطوة.

# كيف تكون آمناً
## خلال ممارسة نشاطك السياسي على فايسبوك(*)

**أظهرت التظاهرات والأحداث في تونس ومصر، وغيرها من البلدان، هذا العام، إمكانيات موقع فايسبوك بالنسبة إلى الناشطين السياسيين. والواقع أنه لو كان الموقع الاجتماعي هذا بلداً، لاحتلّ مرتبة ثالث أكبر دولة في العالم. فإن كنتم تسعون إلى جمع حشد نقدي وفاعل حول قضية معينة، فمن المجدي كثيراً تواجدكم على فايسبوك.**

**غير أن استخدام هذا المنبر بشكل فعّال يعني أيضاً استخدامه بحذر. والأمر ينطبق أكثر ما ينطبق على البيئات القمعية، مثل بعض الدول العربية، حيث تعتقل السلطات الآن الناشطين بسبب «نشاط تخريبي يمارس عبر المواقع الاجتماعية».**

**هنا بعض النصائح المفيدة للجميع ولأي شخص يعمل على تنظيم حركة على الانترنت من أجل إحداث تغيير اجتماعي أو سياسي.**

### ١. انتبه لمعلوماتك

إن معلوماتك وأسماء «أصدقائك» على فايسبوك موجودة على خوادم الموقع، وليس على خادم الانترنت لديك أنت. فإذا ألغي حسابك عن طريق الخطأ، أو بسبب خرقك لشروط الخدمة في الموقع، فستضيع كل هذه المعلومات إن لم يكن لديك نسخة عنها. لذلك، عليك أن تذهب إلى «تفضيلات حسابك» (Account Settings) وتنقر على «تنزيل معلوماتك» (Download your information)، ثم «اعرف أكثر» (Learn more)، ثم انقر على مفتاح «التنزيل» (Download).
ويمكنك أيضاً الحصول على برنامج من Adobe Air باسم Social Safe، أو آخر من «فايرفوكس» اسمه «أرشيف فايسبوك» Archive Facebook والذي يساعدك على تنزيل معلوماتك الشخصية، خريطتك الاجتماعية والصور، على حاسوبك الخاص. غير أن هذه التطبيقات لن تنزّل أسماء وعناوين «الأصدقاء». لذا، يجب أن تحفظ هذه المعلومات بشكل يدوي في مكان آخر غير خادم موقع فايسبوك. وهذا التكتيك استخدمه الناشطون المصريون المسؤولون عن صفحة «كلنا خالد سعيد» قبل أسابيع من قطع الانترنت في مصر خلال الثورة.

### ٢. استخدم HTTPS

إن نظام HTTP القديم (ويرجح أنك تراه الآن في خانة العنوان في أعلى يسار الصفحة لدى فتح متصفّحك للانترنت) هو غير آمن كما أنه قابل للاختراق والتنصت والمراقبة. أما (Hypertext Transfer Protocol Secure) (HTTPS، فيجعل انتقال المعلومات بين متصفحك وفايسبوك أكثر أمناً بما لا يقاس. تذكّر أن HTTPS لا يعني أنك ستكون محمياً بشكل كامل، فلا ترمي الحذر جانباً لمجرد أنك ذكي كفاية لتستخدمه.

(*) للمزيد من المعلومات الرجاء زيارة الموقع التالي Movements.org حيث ستجدون تفاصيل أكثر. يتخصص هذا الموقع في تعريف الناشطين، ووصلهم ببعضهم البعض وتقديم المساعدة لهم، وذلك من طريق التكنولوجيا لتنظيم التغيير الاجتماعي.

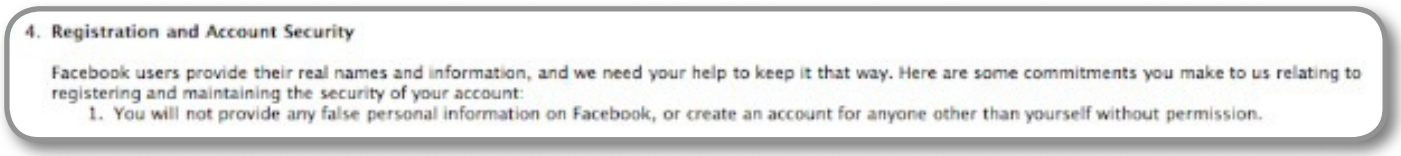
إجعل HTTPS إذاً نظامك الدائم، فاضغط على «تفضيلات الأمان» (Account Security) تحت «تفضيلات الحساب» (Account Settings). إذهب إلى «التصفح الآمن» (Secure Browsing) واختر Browse Facebook on a secure connection (https) whenever possible.

وبما أنك وصلت إلى هنا، وخصوصاً إذا كنت ممن يدخلون فايسبوك أو المواقع الاجتماعية الأخرى من مقاهي الانترنت، فانقر أيضاً على خيار يضمن إرسال بريد إلكتروني لك في حال تم اختراق حسابك وهو خيار send me an email when a new computer logs into my account.

**وطبعاً تذكّر أن تسجّل خروجك (Log out) حينما تدخل الموقع من كمبيوتر مشترك أو يعود إلى غيرك.**


## ٣. إبق مجهول الهوية من دون أن تتعرض للطرد

إن مجموعات فايسبوك، والصفحات والنشاطات المعلن عنها هي مفيدة للديكتاتوريين بقدر ما هي مفيدة للناشطين. فالموقع يعتبر الدليل المعمَّم لمنظمي الاحتجاجات، وهو كامل أيضاً، مع المواعيد والأماكن المقررة للاحتجاجات، مما يسهّل كثيراً قمع تلك الاحتجاجات واعتقال المشاركين. طبعاً، هذا النوع من القلق واجب في البيئة السياسية القمعية. إن أي مستخدم لفايسبوك يجب أن يعي ويكون حذراً إزاء مقدار انكشاف هويته، ويجب أن يحمي أكبر قدر ممكن من المعلومات الخاصة به من دون خرق شروط الخدمة في الموقع.


4. Registration and Account Security

Facebook users provide their real names and information, and we need your help to keep it that way. Here are some commitments you make to us relating to registering and maintaining the security of your account:

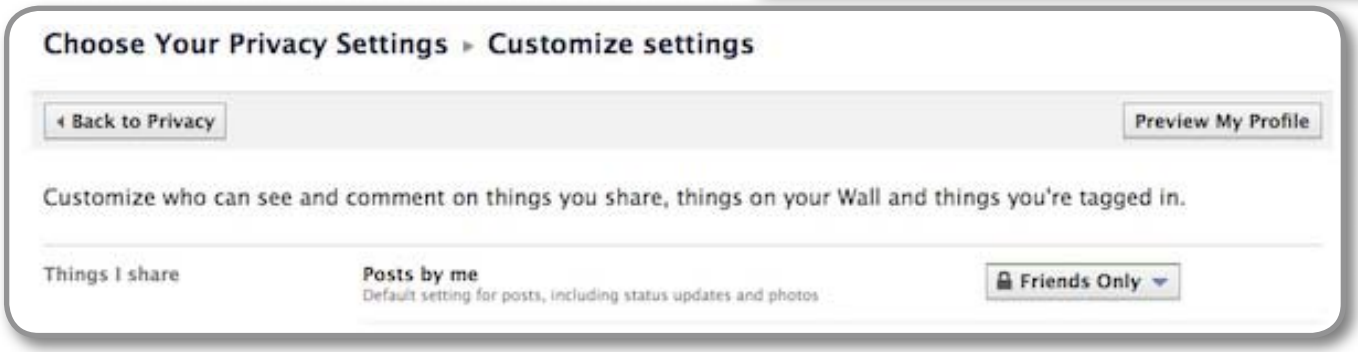
1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.

فما هو ال ( ToS Terms of Service)؟ إنه يتضمن سياسة الاسم الحقيقي ويمنع المنضمين من استخدام اسماء مستعارة. غير أن كثيرين يستخدمون أسماء مستعارة. فقد كانت قوة تطبيق الشروط، من قبل إدارة الموقع، على هؤلاء المستخدمين، عشوائية وغير منظمة. فإذا خرجت على فايسبوك باسم مستعار لتحمي هويتك الحقيقية، تحاشى أن يتم طردك من خلال إيجاد هوية بديلة مُقْنِعة. والأهم أن تكون لديك خطة بديلة في حال تم إلغاء حسابك.

جزء من هذه الخطة هو دراسة الToS كي تعرف ما إذا كنت قد خرقته، وكيف يبلغ الآخرون عن الخروقات (وهذه البلاغات يمكن أن يساء استخدامها أيضاً). إن كنت لا تملك الوقت لذلك، فاتصل بمن لديه الوقت والموارد للاتصال بفايسبوك نيابة عنك.

ملاحظة: إن موقع mashable المتخصص في متابعة أخبار وتطورات الوسائط الإعلامية الاجتماعية لا يتغاضى عن خرق شروط فايسبوك.

## ٤. التخفّي يتجاوز حجب اسمك الحقيقي:




ما هي المعلومات الأخرى التي قد تعرّف عنك؟ هل رقم هاتفك معمّم؟ هل هناك صورة لك قرب علامة فارقة في الشارع قد تدل إلى مدينتك أو الحي الذي تسكن فيه؟ (عليك في الأصل تحاشي استخدام صورة حقيقية لك). ماذا عن الأشخاص الذين صاروا «أصدقاء» على فايسبوك؟ إن ارتباطك على فايسبوك بأشخاص اعتُقلوا لممارسة النشاط السياسي، أو هم جزء من مجموعة لا تريد أن يتم ربطها بك، قد يوقعك في المشاكل، فانتبه من الذي تقبله ضمن «الأصدقاء». راقب اتصالاتك بأدوات تساعدك على تحليل شبكة معارفك. هناك مثلاً Friend Wheel أو Social Graph.

إذا حيّرتك لائحة «تفضيلات الخصوصية» Facebook Privacy Settings، تذكر أنه يمكنك دائماً رؤية كيف تبدو صفحتك للآخرين وأي معلومات تكون ظاهرة للعيان. وذلك بالتوجه إلى

Account > Privacy Settings > Customize Settings > Preview my profile.

## ٥. استخدم فايسبوك طالما أنه مفيد

أثبت منبر فايسبوك أنه مفيد للتحركات الأخيرة، ولكسب الحشد المؤيد لقضية الثورات. لكن ما إن يسمع العدد الكافي من الأشخاص بخططك فلا تخف من نقل التواصل من الانترنت إلى الشارع. فليكن التنسيق وجهاً لوجه أو بأدوات افتراضية أخرى. بعض هذه الأدوات صممها ناشطون من أجل ناشطين أمثالهم، مثل Crabgrass.

## ٦. تعلّم من أقرانك:

الأرجح أن تصبح كل النصائح أعلاه غير ذات معنى في غضون أشهر. لماذا؟ لأن الأشخاص الذين يتجسسون على الناشطين يتبنون استراتيجياتهم الخاصة على الانترنت، بالضبط كما يفعل الناشطون، وبالسرعة نفسها. لذا من المهم جداً الانتباه إلى والاطلاع على ما يقوله الآخرون حول العالم، وما يفعلونه ليحافظوا على أمنهم، وأساليبهم في تحديث إجراءاتهم الاحترازية.

## Security Kiss

هذا البرنامج يمثل حلاً مثالياً ومتكاملاً لعدد كبير من المشاكل التي تواجه الناشطين الإلكترونيين. فهو يسمح لك بإنشاء «شبكة خاصة افتراضية» ويتميز بالتالي:

– يمنحك القدرة على تجاوز حجب المواقع الإلكترونية.

– يسمح لك بتشفير الاتصال، وكافة البيانات المرسَلة والمستقبَلة، من خلال تقنية تبادل المعلومات بالأنفاق.

– حجمه صغير جداً (٢,٥ ميغابايت) يمكن تحميله حتى مع الاتصالات البطيئة جداً للانترنت (dial up)

– مجاني، ويسمح مجاناً، بتبادل معلومات بحجم ٥٠ إلى ٣٠٠ ميغابايت، وفي العادة لا نحتاج إلى أكثر من ذلك.

– سهل التنصيب (install) والتشغيل (run)، هي فقط بضع نقرات ولا حاجة إلى أي إعدادات (settings) إضافية

**لتحميل البرنامج وتنصيبه أنقر هنا**

## M86 Security

يقول المثل «درهم وقاية خير من قنطار علاج». وفي عالم الإنترنت، بعد أن تضغط على رابط معين، يكون فات وقت العلاج.

من هذا المنطلق أتت إضافة «M86 Security» والتي تقوم بعملية فحص الروابط قبل أن تقوم أنت بزيارتها، وتعطيك إشارة لسلامة رابط معين أو توقع وجود برامج خبيثة عليه.

تعمل هذه الإضافة على كل من المتصفحين فايرفوكس وإنترنت إكسبلورر إذ لم يتم بعد تطوير نسخ منها لملائمة غوغل كروم وغيره من المتصفحات.

ننصحك بشدة تحميل هذه الأداة من **هنا** وتجربتها على الأقل لفترة، وستختبر بنفسك الراحة التي تقدمها عن طريق ضمان سلامة المواقع التي تزورها.

# كيفية إختيار كلمة سر جيدة


**إن كلمات**
**المرور هي المفاتيح**
**التي تستخدم للوصول إلى معلومات**
**شخصية مخزنة على الكمبيوتر وفي حساباتك عبر**
**إنترنت.**

وإذا ما سرقت هذه المعلومات، فيمكن استخدامها لفتح حسابات أو انتحال شخصيات في المعاملات عبر شبكة إنترنت. في حالات عديدة، لن تلاحظ هذه الهجمات إلا بعد فوات الأوان.

**كيف تسرق كلمة السر؟**

هناك برامج تعمل بسرعة كبيرة على تجربة ملايين الإحتمالات بالدقيقة الواحدة لمعرفة كلمة السر. ومن الطرق التي تستعملها هذه البرامج:

Brute force attack أو الهجوم بالقوة: يستعمل القراصنة برنامج لمعرفة كلمات السر، حيث يقوم هذا البرنامج بوضع عدة تركيبات لرموز وكلمات وأرقام للوصول إلى الكلمة الصحيحة.

Dictionary Attack أو هجوم المعجم: يستعمل القراصنة من أجل ذلك برنامج يحاول معرفة كلمة السر عن طريق وضع كلمة معجمية، هذه الطريقة أسرع و أكثر فعالية لأن الناس يستعملون اجمالاً الكلمات المعجمية في كلمة السر، لكن هذه الطريقة غير فعالة مع كلمات السر المعقدة.

Cryptanalysis أو تحليل الشيفرات: وهي في الأصل علم تحليل المعلومات المشفرة أو كسر الخوارزميات ولهذا الغرض يلجأ القراصنة وفي كثير من الأحيان بعض الحكومات إلى برامج حديثة ومتطورة التي بإمكانها تخطي كلمات السر وحتى حل الوثائق المشفرة على جهاز الحاسوب إذا اقتضى الأمر. من أكثر البرامج المستعملة في هذا المجال نذكر: RainbowCrack

Phishing أو التصيد: و قد كثرت عمليات القرصنة بواسطة التصيد في الآونة الأخيرة على مواقع عدة مثل: فيسبوك: حيث يقوم المتصيدون (phishers) بإرسال رسائل إلكترونية أو ايميلات زائفة تطلب من مستخدمي الشبكة زيارة إحدى المواقع الإلكترونية بحيث يطلب من المستخدم إجراء تحديث على بياناته، مثل: اسم المستخدم، كلمة المرور، بطاقة الائتمان، الضمان الاجتماعي، رقم الحساب في البنك. هذه المواقع الإلكترونية هي مواقع زائفة، صمّمت فقط لسرقة معلومات المستخدم. ومن الأمثلة عليها موقع شبيه ب (yahoo أو hotmail و(gmail ؛ حيث يقوم الهاكر بإستحداث صفحة شبيهة تماماً بالصفحة الاصلية لتلك المواقع، حيث يقوم المستخدم بإدخال اسم البريد وكلمة السر للدخول إلى بريده الإلكتروني، دون العلم أنه تم الاطلاع على تلك البيانات المدخلة.

و من الطرق الأخرى أن يقوم المتصيدون، بشكل غير ملاحظ، بتحميل برنامج على أجهزة المستخدمين تسمح لهم بالوصول إلى تلك المعلومات الخاصة بالمستخدمين. وهناك عدة طرق أخرى. مثلاً على الفيسبوك يقوم القراصنة بتحميل صورة على الفيسبوك و يبعث بها لملاين من الناس ويضعون بجانب الصورة لينك أو وصلة خارجية وعندما يضغط المشترك على الوصلة يسرق حسابه و بريده الالكتروني. لذلك ينصح بالحذر الشديد.

**ما هي طرق الحماية؟**

أن تكون كلمة السر مكونة من اكبر عدد من الاحرف والرموز والارقام، الأفضل هو أن تكون مكونة من ١٤ رمز.

أحرص على أن كلمة السر مركبة أي أن تتضمن أرقام و رموز خاصة مثل: *#$٪^&

ان لا تتضمن رموز معروفة مثلاً: ١٢٣٤٥٦ أو تاريخ الولادة، رقم الهاتف، كلمة password، نفس الإسم الذي تستعمله للولوج أو Username، أو أية إسم يمكن إيجاده بالمعجم، يجب أن يتضمن حروف كبيرة و أخرى صغيرة مثلاً A و a.

استبدال بعض الأحرف برموز كإستعمال:

@ بدل a

$ بدل s

٪ بدل مفتاح المسافة «space bar»

o بدل الصفر ٠ و العكس

! بدل أي «ا»

و هناك ميزة للغة العربية، تمكن مستخدمي الإنترنت العرب من تعقيد كلمة السر أكثر عن طريق استعمال:

٣ بدل العين

٢ بدل الهمزة

٥ بدل الخاء

٦ بدل الطه

٧ بدل الحاء

٨ بدل الغاء

**طرق الوقاية من التصيد:**

١- يمكن حماية جهاز الحاسوب باستخدام برامج مضادة الفيروسات (anti-viruses)، تفعيل جدار النار (firewalls) وتحديثه باستمرار.

٢- التأكد من تحديث متصفح الإنترنت وإسعمال احدث الإصدارات دائماً.

٣- التأكد من استخدام موقع إلكتروني آمن في حال إدخال معلومات خاصة.

٤- تأكد من أن بداية عنوان الموقع في شريط العنوان للمتصفح هو: «https://» وليس«http://». وجود حرف اس بالانجليزية بعد اتش تي بي وهو يعني موقع مأمون الاستخدام والبيانات المنقولة مشفرة عبر هذه الصفحة.

٥- وجوب الحذر من الروابط في الرسائل الإلكترونية والتي تقود إلى صفحات إلكترونية (في حال الاشتباه بالرسالة).

٦- تجنب تعبئة النماذج (forms) المتعلقة بالمعلومات المالية أو الشخصية خاصة التي تأتي مرفقة في الرسائل الإلكترونية.

٧- إن لم تكن الرسالة الإلكترونية تحتوي على توقيع رقمي (digital sign) فليس من الممكن التأكد من أنها ليست مزيّفة.

٨- عدم إعطاء أي معلومات خاصة مثل رموز التعريف الشخصية (PIN) أو كلمات السر عند التحدّث عبر الهاتف مع البنوك أو المؤسّسات المالية لأنها لا تطلب هذه المعلومات عبر الهاتف بل تتطلّب الوجود الشّخصي.

يمكنك التحقق من مدى قوة كلمة السر الخاصة بك باستعمال هذه الخدمة: **passwordmeter**

**نصائح عامة:**

من المفضل أن تكون الكلمات المختارة سهلة الحفظ لعدم نسيانها و أن تكون هناك كلمة سر خاصة بكل موقع يزوره الشخص.

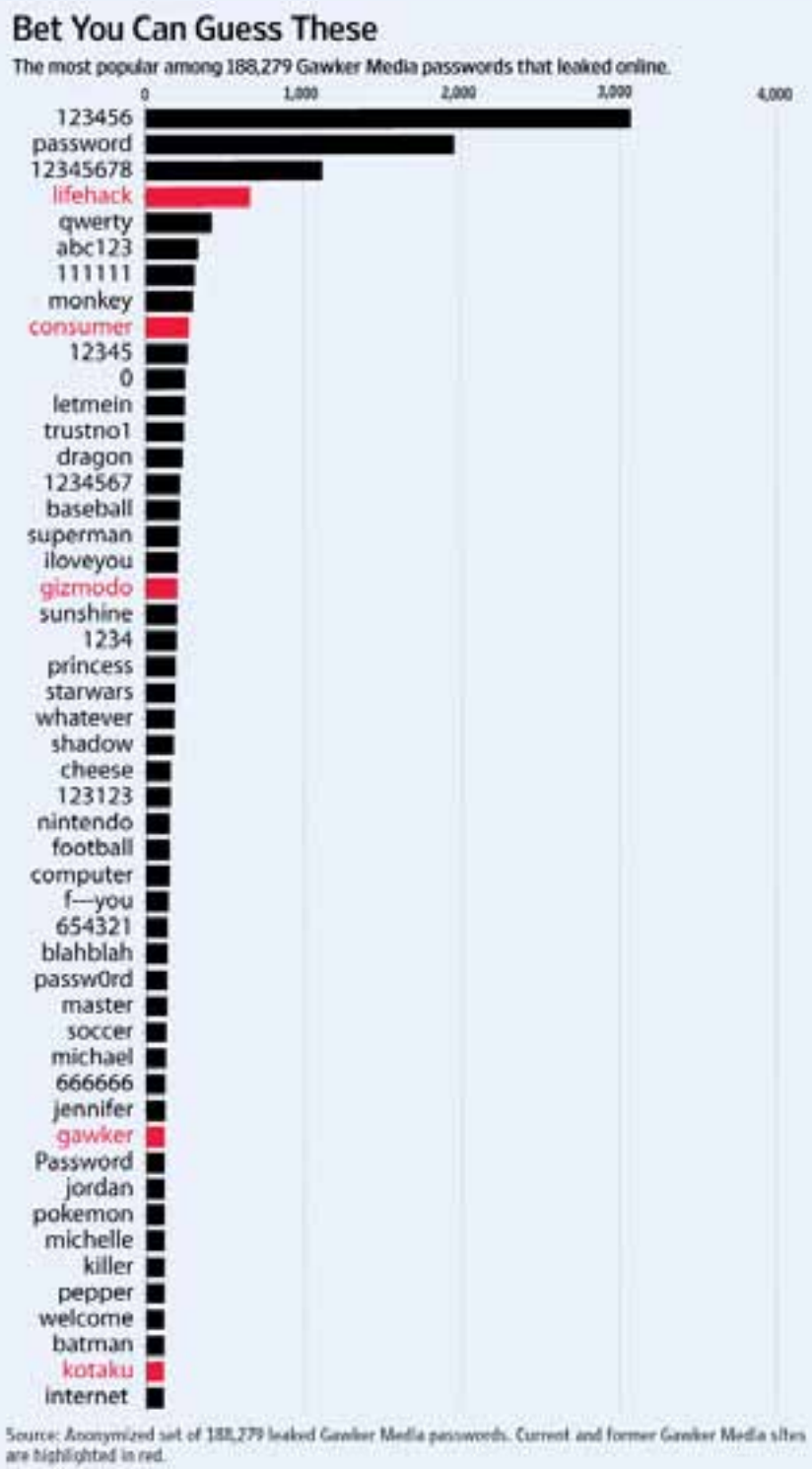
ومن المحبذ أيضاً تغيير كلمات السر بشكل منتظم، وعدم حفظها على الإنترنت، أو تدوينها على الأوراق أو الإفصاح عنها للأصدقاء.

أحرص كذلك على حماية حاسوبك وأجهزة اتصالك الإلكترونية بكلمة سر. كما ينصح بإخفاء البريد الإلكتروني من الملف الشخصي أو ما يعرف بال«profile» في موقع فيسبوك و ذلك لحماية خصوصية المستخدمين وعدم تمكين القراصنة من الحصول على عنوان بريدك عن طريق الفيسبوك.

# أغبى ٥٠ كلمة سر على الإنترنت

في دراسة نشرت على جريدة وال ستريت تبين سذاجة العديد من مستعملي الإنترنت وكسلهم في بذل بعض الجهد لحماية حساباتهم على مختلف مواقع الإنترنت. إذ تطرح الدراسة نماذج من كلمات السر المتداولة كثيرا بين المستعملين والتي من السهل للغاية اكتشافها مثل: ١٢٣٤٥٦ أو password.

نشرت مجموعة من قراصنة الإنترنت قائمة بأسماء مستعارة على الإنترنت مرفقة ايملات وكلمات سر لأكثر من مليون مستعمل انترنت. في الأول كل كلمات السر كانت مشفرة لكن القراصنة توصلوا لحل ١٨٨٢٧٩ شيفرة وتم أثر ذلك نشرهم للعموم كجزء من عملية القرصنة وباستعمال هذه القائمة تمكن وضع قائمة بأغبى كلمات السر المستعملة موضحة في الرسم البياني التالي




تراودنا هنا بعض الأسئلة. لماذا يميل العديد من مستعملي الإنترنت إلى إستخدام كلمات مستعملة كثيرا ككلمة سر لحسابهم الخاص على الإنترنت وماهو شعورهم بكون كل نشاطاتهم على الانترنت مفضوحة أمام العموم دون دراية؟

لماذا يتردد استعمال كلمات مثل: querty, f_you, blahblah, whatever ولماذا نجد كلمة monkey بين العشر الأوائل؟

على الأقل كلمتا سر اثنتان كانتا لهما علاقة بالخيال العلمي trustno1 وهي كلمة السر الخاصة بالعميل الخاص مودلر في سلسلة اكس فايلز والكلمة الثانية thx1138 من فلم لجورج لوكس الذي يطرح تصورا لمسقبل بائس.

بعض الكلمات السرية المتداولة التي تم اختراقها لم تكن تستحق الكثير من الذكاء ومنها: "dragon," "superman," "starwars" "princess," و "nintendo".

لتجنب مثل هذه الاختراقات نؤكد على أهمية تتبع نصائح إنشاء كلمة سر قوية لحماية بياناتك على الإنترنت والتي كنا غطيناها في مقال آخر هنا.

# التعامل مع التحديثات

بعضنا اختار أن يغلقها نهائياً، وبعضنا لا يملك صلاحية الحصول عليها، والبعض الآخر تركها حسب إعداداتها الافتراضية وهي تتم بغفلة تامة منه، فما هي هذه التحديثات التي لا تكف أجهزتنا بالإلحاح في طلبها، وما هي أهميتها والمخاطر الناتجة عن إهمالها، ثم ما هي أفضل طريقة للتعامل معها.

التحديثات بمفهومها العام هي تلك السلسلة من الإضافات تقوم الشركة المصنعة للبرامج بإنتاجها وإرسالها لنا عبر الإنترنت وتكون عادة لهدفين أساسيين الأول هو تطوير البرامج وإضافة ميزات جديدة عليها لمواكبة التقدم التكنولوجي والثانية تعزيز القدرات الدفاعية والحماية والخصوصية على أجهزتنا عن طريق إغلاق ثغرات تم اكتشفها مؤخراً، أو التعرف على فيروسات وبرامج خبيثة ظهرت حديثاً أو التصدي إلى أسلوب جديد في عالم قرصنة المعلومات، وهذا هو الجزء الهام بالنسبة لنا والذي سنتطرق له بالتفصيل في هذه المادة.

كما نعلم فإن هناك حرب باردة تدور بين خبراء الحماية من جهة وقراصنة المعلومات من جهة أخرى وطالما نحن متصلون بالإنترنت فهذه الحرب حتماً تدور على أرضنا وتستهدفنا نحن بدرجات تختلف حسب أهمية المعلومات التي نمتلكها، لذلك يصبح من الضروري بالنسبة لنا التحالف مع خبراء الحماية والحصول على أحدث برامجهم في مواجهة من يرغب بالحصول على معلومات من حقنا الحفاظ على خصوصيتها.

قد يتساءل أحد هنا، ما هي المعلومات التي أملكها وقد يرغب قرصان في الطرف الآخر من العالم في الحصول عليها؟ لقد انهارت مؤخراً الصورة النمطية للهاكر ذلك الشاب المدمن على الكمبيوتر ويجلس منعزلاً كل همه التلصص على خصوصيات الآخرين، وبتنا نعلم اليوم أن قرصنة المعلومات قد تكون مهمة تكلف بها جهات بحجم مؤسسات كبيرة ووزارات وأجهزة استخبارات، وفي عالمنا العربي توظف حكوماتنا ملاين الدولارات والخبراء المتمرسين لمراقبة نشاطنا على الإنترنت، ومن منا لا يمتلك بيانات يريد لها أن تبقى خاصة به أو من اختار أن يشاركهم بها فقط.

إذاً حاجتنا للخصوصية هي أمر محسوم ويبقى علينا أن نرى كيف يمكن للتحديثات أن تساعدنا في الحفاظ عليها، وما هي المشكلات التي قد تواجه بعضنا في ذلك.

كل البرمجيات بشكل عام تتطلب التحديث لكن بعضها قد نعطيه الأولوية على البعض الآخر فيما لو كنا مضطرين للاختيار وتأتي في المرتبة الأولى من حيث الأهمية البرامج المضادة للفيروسات ثم أنظمة التشغيل (الويندوز الماكنتوش وغيرها..) ثم متصفحات الإنترنت والإضافات المركبة عليها وبعدها تأتي كافة البرامج الخدماتية المثبتة على أجهزتنا.

الأنتي فايروس وهو الأهم على الإطلاق ويمكننا تشبيهه بجهاز المناعة في الجسم البشري فهو مصمم للقضاء على هذه الفيروسات ولكن عليه أن يتعرف عليها أولاً ويكون ملقحاً ضدها، فكما نعلم في كل يوم هناك فيروسات جديدة تنتشر على شبكة الإنترنت ويسارع خبراء الحماية في الشركات المصنعة للأنتي فيروس إلى التعامل معها ثم إنتاج مصل أو لقاح يحاربها ويرسلها لنا مباشرة عن طريق التحديثات، فإذا لم نحصل على ذلك اللقاح فنحن معرضون للإصابة بذلك الفيروس والتأثر به، وبغض النظر عن الأضرار المادية عادة ما تصمم الفيروسات لسرقة معلوماتنا الخاصة.

تكمن المشكلة في العادة أن البعض ليس لديهم برنامج أنتي فايروس مثبت على جهازهم لعدم تمكنهم من دفع ثمنه، أو أن البرنامج المثبت مقرصن (غير مرخص، نسخة غير شرعية) فتمنع الشركة المصنعة ذلك المستخدم من الحصول على آخر تحديثاتها، والحل هنا بسيط جداً أحصل على برنامج مجاني تماماً وقم بترخيصه لصالحك واضبط خيارات التحديث على أوتوماتيكية، وننصح باستخدام برنامج أفاست المجاني **على هذا الرابط**.

أنظمة التشغيل وتأتي ضرورة تحديثها مباشرة بعد الأنتي فايروس وهنا يأتي الويندوز في الصدارة من حيث عدد مستخدميه من جهة وحاجته المستمرة للتحديث نتيجة لاستهدافه بشكل أكبر من جهة أخرى ، ثم للانتشار الكبير للنسخ الغير مرخصة منها وبالتالي الغير قابلة للتحديث، أما الأنظمة الباقية فهي أما تأتي مدمجة في الجهاز كـ الماكنتوش أو مجانية كـ لينوكس وهنا لا توجد مشكلة في الحصول على التحديثات.

ساهم التعاون بين شركة مايكروسوفت ومصنعي أجهزة الكومبيوتر المحمول إلى حل جزء كبير من المشكلة بحيث بات أي جهاز كومبيوتر المحمول يأتي مع نسخة مرخصة من ويندوز مدفوعة الثمن سلفاً ضمن فاتورة الجهاز، ولكن المشكلة تستمر بقوة مع الأجهزة المكتبية أو أجهزة الكومبيوتر المحمول القديمة التي لازالت تستخدم نسخ مقرصنة.

وفي حال كنت تستخدم نظام تشغيل مقرصن فخصوصيتك حتماً في خطر وهناك المئات من الثغرات الغير مغلقة والتي يمكن استغلالها على الجهاز، والمشكلة الأكبر أن الحلول التي يمكننا تقديمها محدودة جداً وهي أنتقل إلى استخدام نظام تشغيل مجاني كـ لينوكس أو ببساطة أحصل لنفسك على نسخة شرعية إن نظام التشغيل يعادل في أهميته جهاز الكمبيوتر فكما نرفض أو لا يجوز لنا استخدام جهاز كمبيوتر مسروق كذلك علينا أن نرفض استخدام نظام تشغيل مسروق، من ناحية أخلاقية وكذلك نفعية (خصوصيتك بدون التحديث في خطر) وكما تمكنا جميعاً من تخصيص مبلغ للحصول على جهاز كمبيوتر علينا أن نخصص مبلغ لنظام تشغيله.

متصفحات الإنترنت: عادة هي مجانية مثل غوغل كروم وفاير فوكس أو تأتي مدمجة مع نظام التشغيل مثل إنترنت إكسبلورر أو سفاري، ويجب المحافظة دائما على تحديثها لأنها نقطة اتصالنا الأساسية مع الإنترنت وتستهدفها معظم الفيروسات كذلك يجب الانتباه بشدة إلى الإضافات التي تثبت عليها، قم الآن بزيارة هذا الرابط بواسطة كافة متصفحات الإنترنت المثبتة على جهازك للتأكد بأن كل الإضافات المنصبة لديك محدثة حتى هذا اليوم وإلا قم بتحديثها فوراً!!، كرر هذه العملية مرة واحدة في الأسبوع على الأقل. الرابط هو Vulnerable plugins

من المستحسن أن تقوم بضبط كافة البرامج على جهازك بإجراء التحديثات تلقائياً لكن في حال كانت سرعة الإنترنت لا تسمح لك بذلك أو أنك تدفع مقابل كل ميغا بايت تقوم بتحميله وهناك تحديثات بأحجام ضخمة قم بضبط الإعدادات لإبلاغك عند وجود تحديث فقط دون تحميله ثم خصص زيارة دورية إلى مقهى إنترنت لتحديث برامجك فقط.

قم بحذف البرامج المقرصنة التي لا تقبل التحديث إن وجدت على جهازك! واستبدلها ببرامج مجانية أو مفتوحة المصدر.

# تشفير الملفات وأرشفتها باستخدام تروكريبت

في هذا الفيديو يمكننا أن نتعرف، خطوة خطوة، على كيفية خلق «هارد ديسك» افتراضي، مشفّر بالكامل، ومزود بكلمة سر، بحيث يمكننا وضع كل ملفاتنا الهامة بداخله، ثم نقوم بإخفائه من الجهاز واستعادته حينما نرغب في ذلك.

**كل ذلك ممكن باستخدام برنامج شهير ومجاني ومفتوح المصدر باسم «تروكريبت».**

للبرنامج العديد من الاستخدامات المتقدمة التي سنتطرق إليها بالتفصيل في الأعداد المقبلة.

وفي الفيديو هذا ستتعلم الخطوات التالية:

١. تنصيب البرنامج
٢. خلق ملف «هارد ديسك» افتراضي وتشفيره
٣. تشغيل الملف وفتحه كهارد ديسك
٤. استخدامه ونقل الملفات إليه
٥. إعادة إخفائه من جهاز الكمبيوتر

**إضغط هنا للمشاهدة على يوتيوب**