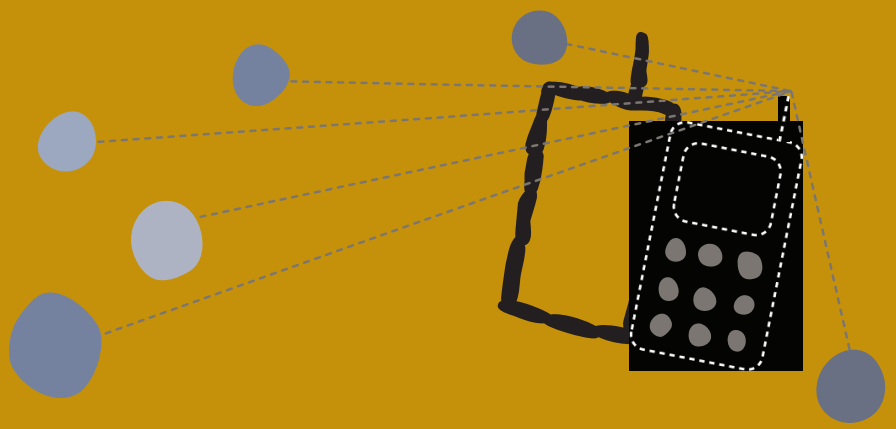
الأمن والخصوصية على الإنترنت والجوّال



لتّكنولوجيات الجديدة، كالجوّال والإنترنت، أدوات قوية للمناصرة، إلا أنّ استخدامها لنقل معلومات حساسة محفوف بالمخاطر للمرسل والمتلقّي وشبكاتهما الإجتماعية أيضاً. تساعدك هذه البطاقة للحصول على معلوماتك بشكل آمن وحماية بياناتك عند استخدام الجوال والإنترنت.

ما هو الأمن الرقمي والخصوصية؟

المؤشرات التي تدل على أن المعلومات والسرية الرقمية انتهكتا قد تشمل ما يلي:

- كلمات السّر التي تتغير بشكل غامض
- الرسائل الخاصة التي يبدو أنهًا مقروءة من قبل شخص غير المرسل إليه
- المواقع التي يصبح من غير الممكن الدخول إليها في بعض البلدان
- كشف المسؤولون عن علمهم بمحتوى مراسلات خاصة، بما في ذلك تواريخ، أو أسماء، أو مواضيع تمت مناقشتها
- المكالمات الهاتفية التي يشك الأفراد في إمكانية أن تكون مراقبة

هل من ضرورة للقلق حول هذا الموضوع؟

إذا كانت إمكانية اختراق أمنك وخصوصيتك تؤثر على مشاريعك أو تعرضك، أنت شخصياً أو من تتصّل بهم، للمضايقة، اذاً ينبغي أن تقلق. المعلومات والبرامج اللازمة لإختراق الخصوصية الرقمية غالباً ما تكون متوفّرة على شبكة الإنترنت. إذا كان للمعتدي القدرة على الوصول التّام للبنى التّحتية الخاصة بالإنترنت أو الإتصالات في بلدك، فالتّكنولوجيا المطلوبة بسيطة جداً. الأجهزة الحكومية، ومزودي خدمة الإنترنت، وشركات الهاتف الجوال لديها الوصول اللّازم إلى هذه البنى التحتية، كما وأن الزّملاء في المكتب، والجيران، وأصحاب مقاهي الإنترنت قد يكونتاحاً لديهم أيضاً الوصول.

ما المسائل الأمنية الموضّحة في هذه البطاقة؟

تشدّد هذه البطاقة على الوسائل المعتمدة للإنترنت والهواتف الجوّالة. تم أيضاً التطرّق لتكنولوجيات يمكنها أن تجعلك عرضة للرقابة والمراقبة والمضايقة. وإن لم تتم مناقشتها في هذه البطاقة، تبقى بعض الإجراءات الأساسية كتحديث نظام تشغيل الكمبيوتر الخاص بك بشكل منتظم، والبرامج الموثوقة لمكافحة البرمجيات الخبيثة، وخلق نسخ احتياطية، من أهم الاحتياطات الأساسية. إذا كان لديك سبب للاعتقاد بأن أجهزة الكمبيوتر أو أجهزة تخزين البيانات، بما في ذلك النّسخ الإحتياطية، معرّضة لخطر الفقدان، أوالسّرقة أو المصادرة، أو أن مؤسستك خاضعة لمراقبة رقمية هادفة (أو إذا كانت المراقبة شائعة في المنطقة التي تعمل فيها)، اذاً يجدر بك مراجعة دليل الأمن من مبادرة التّكنولوجيا التكتيكية (HYPERLINK “http://www.tacticaltech.org” Tactical Technology Collective) بعنوان.

أدوات المناصرة المستندة إلى الانترنت

عند استخدام الأدوات العامة على شبكة الإنترنت، مثل المذكرات، الفيسبوك، التويتر للتعبئة أو للتنسيق، لا تنسى أن المعلومات المنشورة على هكذا منصات تصبح، إلى حد ما، ملكاً للمشغّل، وأن العديد من هذه المنصات تكشف معلوماتك أكثر مما قد تعتقد.

عند إسناد مشروع حساس لمشغلي أية منصة رقمية، يجدر بك قراءة سياسات الخصوصية الخاصة بها أو اتفاقية المستخدم. لا تنس ان أكثر السياسات إنفتاحاً تترك معلوماتك تحت سيطرة مشغّلي المنصات المباشرة، سيكونون قادرين على الكشف عن، أو بيع، أو إساءة وضع معلوماتك من دون موافقتك أو علمك. وإن قمت بإغلاق حسابك، فإن الكثير من هذه المواقع لا تحذف فعلياً المحتوى الذي قمت بنشره أو المعلومات الشخصية التي شاركتها. وأخيرا، ما لم يكن من المهم أن تستخدم خدمات شعبية معينة، إما بسبب سهولة الوصول إليها، أو لتسهيل التواصل مع قاعدة المشاركين، من الأفضل أن تدرس بدائل أكثر تقدّماً: بليب بدلا من يوتيوب؛ رايز آب بدلاً من غوغل. إن توفّرت الموارد الفنية والتقنية، يمكنك تشغيل خدمات خاصة بك على شبكة الإنترنت.

إذا كنت تستخدم منصات تجارية، عليك اتخاذ الإحتياطات اللازمة لحماية نفسك من الأفراد الذين يعرفون كيفية التنقيب للوصول الى معلومات خاصة مرتبطة بهذه الخدمات. هذا ينطبق بشكل خاص على مواقع الشبكات الإجتماعية كفيسبوك وماي سبايس. عليك تطوير فهم شامل للمواصفات الأساسية لهذه المنصات، والتفكير في أنواع المعلومات التي تخصّك أنت أو مؤسّستك والتي قد تُكشف من دون قصدك، على سبيل المثال، اسمك الحقيقي، مكان السكن، الأماكن التي تسافر اليها، وتفاصيل الأحداث أو الاجتماعات القادمة. إذا تمت مراقبتك لفترة زمنية كافية، قد توفر هذه المعلومات صورة من عاداتك وممارساتك المهنية.

يمكنك إنشاء حسابات متعددة على أي منصة تستخدمها، مما يتيح لك استخدام حسابات مختلفة أو ملفات تعريف مختلفة لمشاريع مختلفة. كما يمكنك بهذه الطريقة استخدام حساب تجريبي لمراقبة نفسك. تعتبر خصوصيتك محمية بشكل أفضل إذا كنت قادراً على مراقبة حسابك بمختلف الطرق ومعرفة ما يكشف عنك هذا الحساب، من خلال البحث على الإنترنت أو بعض الأشخاص ذوي الإمتيازات الخاصة.

كلمات السر

معظم الموارد على الإنترنت تعتمد على كلمة سر واحدة لحماية حسابك. إذا ما قام أي معتدي، فرداً كان أم منظمة، من اختراق كلمة

السر هذه، عندها لا يهم ما إذا كنت تثق بمدراء الموقع أم لا، أو فعالية معايير الخصوصية؛ ستفقد على الفور السرية والخصوصية كما ستنكشف هويتك.

من الطرق غير المعروفة لخرق كلمة السر: يمكن لأحد ما وضع برامج خبيثة على جهاز الكمبيوتر الذي تستخدمه لولوج موقع آمن. كما يمكن لأحد ما رصد اتصالك بالإنترنت عند ولوجك موقع غير آمن.

لحماية نفسك ضد النوع الأول من الإعتداءات، عليك استخدام كمبيوترك الخاص أو كمبيوتر آخر تمت معالجته من قبل شخص تثق به. عليك التأكد من أن نظام التشغيل وبرنامج مكافحة البرمجيات الخبيثة يتم تحديثهم على الدوام. للحماية ضد النوع الثاني من الاعتداءات؛ معظم المنصات الإلكترونية الأكثر شعبية كالبريد الإلكتروني، الشبكات الاجتماعية، المدونات، الخرائط، ومنصات الفيديو توفر للمستهلك خيار الإتصال الآمن بالشبكة، يدعى هذا الإتصال HTTPS. يمكنك اكتشاف ذلك بكتابة عن: https:// بدلا عن كتابة http://. وذلك في بداية عنوان صفحة الويب. ومع ذلك، فالعديد من المنصات الإلكترونية لا تستخدم HTTPS لحماية أية معلومات سوى كلمة السر الخاصة بك . إذا كان هناك من يراقب اتصالاتك لفترة طويلة، سيعلم ما قمت بتخزينه على هذا الموقع. أفضل وسيلة لحماية نفسك من هكذا مراقبة تكون باستخدام مواقع تستخدم الـHTTPS لكافة صفحاتها.

تجاوز الرقابة

يمكنك استخدام برامج بروكسي على الإنترنت، وأدوات تحايل على الرقابة أو برامج مثل تور للمجهولية، لولوج المواقع دون كشف هويتك أو لتجاوز الرقابة. هذه الأدوات مفيدة عند حاجتك للوصول إلى مواقع محظورة، على سبيل المثال لاجراء بحث، أو تحديث مواقع كفيسبوك.

المجهولية الرقمية

برنامج تور للمجهولية مفيد إن لم تشأ كشف المواقع التي زُرتها. تور ينقل طلباتك الرقمية عبر عدد من الكمبيوترات العشوائية، والتي تطوّع أصحابها بها لهذا الهدف، قبل تسليم الطلب إلى الصفحة المطلوبة. بهذه الطريقة يعجز مزوّدو الإنترنت كما الحكومات عن مراقبة تحرّكاتك على الإنترنت. ومع ذلك، لا تستخدم تور عند تبادل معلومات حساسة أو من مواقع غير آمنة. ما لم تكن تقصد موقع HTTPS، فمن الممكن لأحد أجهزة الكمبيوتر المتطوعة مراقبة المحتوى بينما يتم التحميل. يعتبر تور آمناً جداً، ولكنه في الوقت الحاضر يبطئ تحرّكاتك على الإنترنت.

الهواتف الجوّالة

يستخدم الناشطون الهواتف الجوّالة حول العالم، لكن هذه الأدوات تخزّن الكثير من المعلومات التي ينبغي أن تكون خاصة. بالإضافة إلى قوائم الاتصالات، قد يحفظ الجوال تواريخ الاتصالات، دليل المواعيد، رسائل نصيّة ورسائل إلكترونية.

يجب أن تفكر في المعلومات المخزنة على هاتفك، خاصةً أن الاستيلاء على الجوال سهل. فأنت مثلاً لست مضطراً لإبقاء كل معارفك على الجوال، خاصةً إذا كان عملك حقوقي حسّاس. كما يجدر بك حذف المعلومات من الهاتف والبطاقة كلما أمكن ذلك. عند قيامك بتنظيم أحداث أو المناصرة، من المفيد أن تستخدم البطاقات المدفوعة مسبقاً وتغيير السماعات قدر المستطاع، إذ يمكن بسهولة التفتيش والتحّكم بالرسائل القصيرة، كما يجب تجنب الكلمات الرئيسية الحساسة

عند إرسال رسائل نصية. طالما أن جوالك يعمل، يمكن استخدامه لتعقب موقعك. يجدر بالمشاركين في إجتماع حساس إطفاء هواتفهم الجوالة وإزالة البطاريات قبل البدء بالاجتماع، ثم الانتظار حتى انتهاء

الاجتماع لإعادة تشغيلها. للشركات المشغّلة للجوال القدرة على الحصول على تفاصيل حول جميع المكالمات: المتلقي، تاريخ الإتصال ومحتواها. ويمكن ان يكون على مقدمي خدمات الهاتف فرض قانوني لتسجيل أو إعلان هذه التفاصيل متى طلب منهم ذلك من قبل مسؤولين رسميين، ويمكنهم الاحتفاظ بهذه السجلات لعدة سنوات.

النشاط ١ : تحديد المخاطر في أنظمة الحماية

استعن بالأسئلة التالية لتقييم المخاطر الأمنية المحيطة بك ومساعدتك على تحديد الأدوات المتوفّرة لردء المخاطر.

١. **أنا أتعامل مع معلومات حساسة.** من المهم أن تعرف ما إذا كنت تتعامل مع معلومات حساسة تجذب اهتمام جهات معيّنة. أتشارك في أنشطة تعتبر حساسة وخطيرة بالنسبة للحكومة، الجيش أو شركة خاصة ما؟ إذا كنت كذلك، قد تعرض نفسك أو الآخرين للخطر ما لم تتخذ تدابير أمنية مناسبة.

٢. **أنا أعمل مع أفراد ذوي هويات وتفاصيل يجب أن تبقى سرية.** ربما تقوم بجمع معلومات خاصة من مناصريك، كمعلومات حول العنف المنزلي، العمل القسري أو الاغتصاب. مثل هذه المعلومات تعرّض مزوّديها للخطر. إذا قام الناس بتزويدك بمعلومات من الممكن لها أن تعرضهم للخطر، عليك اتخاذ خطوات كفيلة بحماية سريتها.

٣. **أتواصل عبر الإنترنت أحياناً مع أشخاص يتعاملون بمعلومات حساسة.** حتى إذا كنت لا تشعر بوجود خطر أمني، إذا كنت على تواصل مع أشخاص معرضين لها سيتم استهدافك. وذلك لأنه من الممكن استغلالك للوصول إلى المعلومات الخاصة بالآخرين.

٤. **أقوم بعرض أو نشر معلومات على مواقع من الممكن اعتبارها تتم بالحساسية.** لعلك تضيف معلومات إلى مواقع مختصة بحقوق الإنسان، أو تقوم بنشر مقالات تهاجم من برأيك لا يحترم حقوق الإنسان. مجرد زيارة المواقع الحساسة على شبكة الإنترنت يمكن أن تجعلك هدفاً.

معلومات عن الأمن الرقمي والخصوصية

للمزيد من المعلومات ولتحميل برمجيات حماية:

١. **عدة الأمان**، مشروع بالتعاون ما بين HYPERLINK "http://www.tacticaltech.org" Tactical Technology Collective و HYPERLINK "http://www.frontlinedefenders.org/" Front Line، وقد أنجز بغرض تلبية احتياجات السرية والخصوصية للمدافعين عن حقوق الإنسان والناشطين HYPERLINK "http://security.ngoinabox.org" http://security.ngoinabox.org

٢. **الأمن والخصوصية الرقمية للمدافعين عن حقوق الإنسان**، من تحضير Frontline، تؤمن معلومات مفيدة عن تقييم ومعالجة المخاطر الرقمية. HYPERLINK "http://bit.ly/1aCkSs" http://bit.ly/1aCkSs : frontlinedefenders.org

٣. **عدة الجوال**، وهو مشروع من Tactical Technology Collective، يضم قسم كامل عن خصوصية الهواتف الجوالة وأمنها. HYPERLINK "http://mobiles.tacticaltech.org/security" http://mobiles.tacticaltech.org/security

٤. **مجهولية التدوين مع وورد برس وتور**. قامت الأصوات العالمية بتحضير هذا الدليل الإرشادي لدعم الحقوقيين الراغبين في كشف الحقيقة والتعبير عن أنفسهم على الانترنت إلا أنهم قد يعرضون أنفسهم للخطر http://advocacy.globalvoicesonline.org/projects/gu

٥. **المجهولية الرقمية وتحايل على الرقابة**. تم تصميم تور لزيادة المجهولية على الإنترنت، يمكن أيضا استخدامه لتجاوز الحجب على الانترنت. يمكنك تحميل البرنامج أو تشغيله عبر جهاز الناقل التسلسلي العام HYPERLINK "http://www.torproiect.org" http://www.torproiect.org

TACTICAL TECHNOLOGY COLLECTIVE
social media exchange
ترجمة: