إستعمال شبكة الإنترنت اللاسلكية العمومية إستعمالاً محمياً ومؤمَّناً بشكلٍ جيد

إرشادات الاستخدام: حسب رأي الخبير الفني، يورغن كوري، نائب رئيس تحرير مجلة c't المتخصصة في تقنيات الكمبيوتر، هايزو أونلاين heise online، بتكليف من مكتب رئاسة ولاية شمال الراين ويستفاليا. فقد تم تقديم هذا النص من أجل نسخه و توزيعه بناءً على ترخيص مقدم من Creative-Commons تحت إسم (CC BY-ND 3.0 DE)، Namensnennung-Keine Bearbeitung 3.0 Deutschland

للمزيد من التفاصيل المرجو الرجوع إلى:

https://creativcommons.org/licenses/by-nd/3.0/de/. و عند الاستعمال وجب ذكر الكاتب، صاحب الطلبية و الرخصة ـ التسمية و الرابط ـ.

يعتبر استعمال شبكة الإنترنت اللاسلكية العمومية شيئاً عملياً ، خصوصا إذا تم بشكلٍ مستقلٍ عن مقدم الخدمة و بدون مقابل مثل خدمة Freifunk

http://freifunk.net/worum-geht-es/technik-der-community-netzwerke/

يمكنكم الإستفادة من هذه الخدمة، سواء كنتم في الطريق و أو عند الانتظار في محطة القطار أو في المطار أو حتى عند التجول في المدينة، بدون الإنقاص من رصيد هاتفكم المحمول، وهو ما يسعد المستخدمين ،إلا أن الكثير منهم ليسوا على علمٍ بالمخاطر الناجمة عن استعمال الشبكة اللاسلكية العمومية و كيفية الدخول إليها. فالأشخاص الواعون بهذه المخاطر، هم فقط من يستطيع تحديد ما هو جيد وماهو سيء و وبإمكانهم القيام بإجراءات مضادة تجعل من الإستخدام اللاسلكي شيئا عمليا و آمنا، كما لو كان الأمر يتعلق بشبكة منزلية.

مسألة الثقة:

المتعارف عليه مبدئياً هو أنه، عند إستخدام الشبكة اللاسلكية العمومية، لا يمكن الثقة بأي أحد، بل و يجب اعتبار أن البيانات المستقبَلة و المُرسَلة يمكن الاطلاع عليها من طرف مستخدمين آخرين للشبكة، لأن كل شخص يستعمل نفس الشبكة التي تستعملونها ، يمكنه من الناحية المبدئية أن يطلع على مضمون المحادثة.

إن التجسس على صاحب حاسوب محمول داخل مقهى أثناء تصفح حسابه على الفيسبوك أو إطلاعه على حسابه البنكي الإلكتروني، لا يتطلب بالضرورة أن يكون خبيراً متخصصا في الشبكات، يكفي فقط أن يكون لديك هاتف ذكي مع تطبيق خاص بذلك.

إن هاته التطبيقات تجعل تقنيات الشبكة المعقدة في متناول الجميع. فقد تجد ذلك الشاب الظريف المحبى، الجالس في المقهى في الطاولة المجاورة، يستخدم تقنية هجوم رجل في الوسط بواسطة ARP-Spoofing

حتى و إن كان لا يفقه أي شيئ في Adress Resolution Protocol (ARP)، وهنا لا يكتفي فقط بالاطلاع على المعلومات العادية بل يتعداه إلى استخراج و استخدام البيانات الشخصيةالمهمة، إذ يمكنه مثلا التصرف في الحساب الشخصي بالفيسبوك أو في الحساب البنكي الإلكتروني:

(http://www.heise.de/ct/artikel/Die-Hotspot-Falle-1394646.html)

هل صدمتم؟ لا تتركوا هاته السيناريوهات تخيفكم. من كانت له اتصالات مكشوفة في الأنترنيت كإرساله للبريد الإلكتروني بشكل غير مشفر، فإن بإمكانه القيام بنفس الشيئ عبر الشبكة اللاسلكية العمومية. فقط عليه أن يدرك أن البيانات المرسلة يمكن قراءتها من قبل أشخاص آخرين وربما يصبح ذلك أمراً معتادا. بحيث يمكن تحميل البيانات التي قد يكتبها الشخص على بطاقة بريدية. غير أن الأمر لن يكون بالخطير إذا تعلق بأشياء حياتية عادية، أما إذا تعلق بكلمات المرور أو بمعلومات ذات أهمية، فإنه يجب اتخاذ إجراءات احتياطية و إجراءات مضادة يمكن بواسطتها المستخدم استعمال الشبكة اللاسلكية العمومية بدون أية مخاطر.

و على ذكر البريد الإلكتروني فإن الكلمة المفتاح بهذا الخصوص هي ـ التشفير(الترميز) ـ. فإذا كانت البيانات المنقولة عبر الشبكة اللاسلكية مشفرة، فإن محاولة أي شخص للاطلاع عليها تبوء بالفشل، ولن يطلع إلا على نفاية البيانات، و التي لا يمكن حل شفرتها هي الأخرى إذا كانت مرمزة بشكل متين.

يمكن القيام بالتشفير في الشبكة اللاسلكية العمومية على عدة مستويات و بدرجات تعقيد مختلفة و بمجهود خاص .

الطرق إلى الهدف:

يطلق على أسهل الطرق إسم "النقل المشفر"، و هي طريقة سهلة على الأقل بالنسبة لكم كمستخدمين ، حيث يجب الانتباه في هذا الصدد إلى أنه عند تصفح إحدى صفحات الإنترنيت أو إحدى الخدمات الأخرى في الشبكة العنكبوتية يجب الدخول عبر https. فإذا دخلتم على صفحة الويب الخاصة بالبنك الذي تتعاملون معه فإنه يجب عليكم دائما الدخول ب https، ذلك أن أغلب المؤسسات البنكية لا تسمح بأية طريقة أخرى غير هاته. إن برامج التصفح الحديثة تبين تشغيلها لطريق نقل البيانات المشفر ليس فقط عبر عنوان صفحة الويب: ...https:// و لكن عبر إظهار رمز التشفير في عنوان صفحة الا نترنت المراد الدخول إليها.

إن الكثير من المقدمين لخدمات البريد الإلكتروني يعرضون كذلك طريقة النقل المشفر. لذلك استخدموا بريدا إلكترونيا على الويب في المتصفح و ادخلوا عبر https. استعملوا أحد برامج البريد الإلكتروني، لأن ضوابط الإستخدام المتفردة هاته تعتبر ضرورية من أجل النقل المشفر: عند ترتيب البرنامج يجب إرسال البريد الإلكتروني بواسطة SSL أو TLS مع طريقة التصديق التي غالبا ما تكون بواسطة إدخال كلمة السر. إن جميع المعلومات الضرورية يتم وضعها من طرف مقدمي خدمات الويب في المتناول. و وإن كان العديد منهم يدعم طريقة النقل المشفر فقط للمستخدمين الذين يدفعون ثمن هذا الاستعمال.

إن الكثير من مقدمي خدمات الإنترنيت مثل الفيسبوك يقدمون دخولا آمنا بالمتصفح عبر https، و يجب استخدام هاته الطريقة كلما أمكن ذلك. إلا أن هذا الأمر لا ينطبق عند الدخول إلى صفحات الويب عبر الشبكة اللاسلكية العمومية، بل حتى عند استخدام الشبكة اللاسلكية المنزلية أثناء إستعمال الإنترنيت، لأن النقل المشفر يؤمّن اتصالاتكم. و هنا وجب التأكيد على أنه حتى و إن كانت الشبكة اللاسلكية المنزلية مشفرة، فإن نقل المعلومات يتم بشكل غي مشفر مالم تقموا بذلك بأنفسكم.

استعمالات البرامج

إذا كنتم في الشارع العمومي بالهاتف الذكي أو حاملا للكمبيوتر اللوحي فإنه يمكنكم من الناحية المبدئية استعمال هاته الخدمات و استعمال البريد الإلكتروني، لكن الصعوبة تكمن في البرامج المحملة على هاته الأجهزة الصالحة للرسائل اللحظية و للدردشة، حيث يجب في هاته الحالة أن تقوموا بتشفير البرامج بنفسك، الشيئ

الذي لا يقوم به أكثر المتسخدمين. يجب عليكم أن تقرروا بأنفسكم ، هل سرية المحادثة مهمة بالنسبة إليكم، و إذا كان الأمر كذلك فيستحسن عدم الاتصال بواسطة الشبكة اللاسلكية العمومية.

فعلى سبيل المثال: لم تكن خدمة الواتس آب تدعم و لوقت طويل أي تشفير عند الاتصال. لكن ابتداءا من شهر سبتمبر من سنة 2015 أصبح الواتس آب يقدم دعما لتشفير الاتصالات، لكن فقط للهواتف الذكية المتوفرة على برنامج جوجل أندرويد، مثل Samsung و HTC و Sony. و في المقابل و بما أنه لا يمكن معرفة نظام التشغيل الذي يستخدمه المحادث الآخر فإنه يمكن اعتبار المحادثة المشفرة عبر الواتس آب غير آمنة بالمرة.

و يختلف الأمر تماما في البرامج المعدة للدردشة و لإرسال الرسائل حيث تكون في الأصل مشفرة. و النموذج الأشهر في هذا النوع من البرامج هو Threema، و بالنسبة للنظم المجانية المفتوحة هناك Telegram و TextSecure. و كذا iMessage الذي وإن كان يقدم تشفيرا للبيانات التي يتبادلها الطرفين المتصلين، إلا أنه خاص بنظام الآبل. أما بالنسبة للبدائل المتاحة عوض الواتس آب فإن لها سلبيات واضحة: غالباً ما يمكن الاتصال بأشخاص آخرين عن طريق الواتس آب لأنهم يستخدمونه من قبل. ولإستعمال بدائل أخرى يتوجب عليكم غالبا إقناع هؤلاء الأشخاص بتحميل هاته البرامج.

أما فيما يتعلق بالتطبيقات الأخرى واستعمالها عبر الشبكات اللاسلكية العمومية فتوجد دائما مشاكل. و لا يمكنكم كمستعملين إلا ناذراً القدرة على تقييم ما إذا كانت المعلومات الحساسة قد تم فعلا نقلها بشكلٍ مشفر كما هو الحال بالنسبة للتطبيقات الخاصة بالتحويلات المالية على الانترنت. بعض الشركات وعدت بإدخال تحسينات في هذا المجال، مثل شركة آبل عبر برنامجها iOS 9 للنقل الآمن للمعلومات، لكنها تبقى لحد الساعة مجرد وعود. وبغض النظر عن كل هذا، فإنه ليس بإمكانكم إطلاقا أن تعرفوا ما إذا كان التطبيق الذي تستعملونه خاليا من الخلل، الشيء الذي قد يمكن المجرمين من إساءة استعمال معلوماتكم.
عندما يتعلق الأمر ببرامج مهمة مرتبطة بمعلومات عن الحساب وبأنظمة الدفع، فهنا ينبغي عليكم أن تفكروا جيدا في كل حالة على حدة،وفيما إذا كان الأمر يستدعي فعلا استعمال هذا التطبيق عبر الشبكة اللاسلكية العمومية.

من الأخير إلى الأخير

تسمى طريقة تشفير المعلومات الواجب نقلها مباشرة الى البرامج ب التشفير" من الأخير إلى الأخير". وهي طريقة تمتاز عن النقل المشفر بكونها تتيح فقط لكم وكذا شريككم القدرة على الوصول الى هذه المعلومات. أما

في حالة التشفير العادي فإن الشركة المقدمة لخدمات الانترنت يمكنها أن تقرأ معكم فحوى المعلومات بما أنها هي المسؤولة عن حل الشفرة قبل إيصالها إلى المتلقي. هذا الأمر قد يبدو مريحا بالنسبة إليكم، لكنه ليس آمنا مائة في المائة.

على العكس من ذلك يعمل نظام "من الأخير إلى الأخير" على تشفير المعلومات التي يرسلها المرسل ولا يتم حل شفرتها إلا عندما تصل إلى المستلم، و هو ما يحدث في يومنا هذا عبر ما يسمى بالتشفير غير المتزامن. فكل مستعمل يتوفر على مفتاحين، مفتاح خاص وآخر عمومي. فإذا رغب أحد أن يرسل لكم خبرا مشفرا، فإنه يشفره باستعمال المفتاح العمومي الذي تتوفر عليه. هذه الرسالة لايمكن حل شفرتها إلا بمفتاحكم الخاص - والذي لا يعرفه أحد غيركم. تعتبر المفاتيح تركيبات لبرمجيات معقدة يتم تحضيرها لكم من طرف أنظمة مثل نظام PGP:
يجب أن تحتفظوا بالمفتاح الخاص عندكم وتأمينه جيداً ، أما المفتاح العمومي فيمكنكم أن تسلموه لأصدقائكم ومعارفكم، وهذا يمكن أن يمر كذلك عبر الخادوم العمومي بحيث يمكن لكل واحد رغب في أن يرسل لكم أية رسالة أن يرسلها عبر مفتاحكم العمومي الذي يمكن أن يطلع عليه.

بالنسبة لأنظمة ويندوز يعتبر نظام Gpg4Win (http://www.gpg4win.de) نظام الاختيار لتشفير رسالة إلكترونية عبر PGP. كما أن هناك مثلاً برنامج Plug-Ins الخاص ببرنامج Outlook وكذا ببرنامج Thunderbird الواسع الإنتشار بين مقدمي خدمات البريد الالكتروني [https://www.enigmail.net/download/]. أما بالنسبة لمستعملي نظام الماك [Mac] فإن هناك نظام GPG Suite [https://gpgtools.org]، يمكنكم وضع iPGMail تحت iOS [https:ipgmail.com/]. أما بالنسبة للكمبيوترات اللوحية والهواتف الذكية التي تشتغل بنظام أندرويد فبإمكانكم مثلا استعمال OpenKeychain [http://www.openkeychain.org/about] بارتباط مع نظام البريد الالكتروني K9. تهدف كل أدوات الانترنت هذه إلى تسهيل التجهيز والاستعمال، لكنها في الحقيقة ليسة سهلة. في حالة الشك ينبغي عليكم أن تطلبوا المساعدة من خبير في مجال الانترنت ليضع لكم نظاما لتشفير بريدكم الالكتروني.

أما بالنسبة للأشخاص الذين يستعملون نظام الويب ميلر [Webmailer] فليست لهم حتَى الآن أية إمكانية سهلة للتزود بنظام التشفير "من الأخير إلى الأخير". بعض مقدمي خدمات الانترنت مثل GMX ومثل Web.de يقدمون الآن أدوات ل PGP حتى في الويب ميلر [Webmailer]. أما إذا كان هذا الأمر غير متوفر عند مزودكم بالبريد الالكتروني، فينبغي إذن أن تفكروا بتغيير بريدكم الالكتروني لدى مزود كلاسيكي مثل طاندربرد [Thunderbird] أو وضع تطبيق للبريد الالكتروني على هاتفكم الذكي أو حاسوبكم اللوحي بحيث تكون معه اتصالاتكم مشفرة.

الحماية الأساسية

إن تشفير البريد الالكتروني و تطبيق نظام حماية آخر لا يمكن أن يخفيا جميع المعلومات عن المسترقين، فهناك مثلا محتويات البريد الالكتروني التي تعتبر فعلاً مشفرة، لكن المعلومات الخاصة بالنقل تبقى دون تشفير. فالشخص الذي أرسل رسالة ما و لمن و في أي وقت، يضل مكشوفاً وربما يمكن أن يقدم أثناء إتصال سري معلومات لا يجوز تركها للعموم.

لكن نظام "من الأخير إلى الأخير" لا يمكن تحقيقه فقط مع التطبيقات والبرامج. بل كذلك عبر نظام شبكي مشفر داخل الشبكة، حيث يتم تشفير أيَ تداول للمعلومات التي تصدر من هاتفكم الذكي أو حاسوبكم اللوحي أو حاسوبكم المحمول قبل أن تصل إلى الشبكة، ثم يتم حل شفرتها فقط عندما تصل إلى المستلم.

إن المصطلح العلمي: Virtual Private Network [VPN] الذي يعني باللغة العربية: الشبكة الخاصة الافتراضية يدل على نظام للحماية. فبفضله ستكونون كمسعملين وكمستعملات على يقين من أن كل الإتصالات وكل المعلومات تكون مشفرة. إلا أنه سيكلفكم مجهودا للترتيب، كما أنه يتطلب مساحة غير قليلة من القدرة الحاسوبية لجهازكم، وهو ما يجب عليكم تقبله.
(http://www.heise.de/netze/artikel/Hotspot-aber-sicher-221475.html)

بفضل نظام VPN يمكن الدخول، عند الحاجة، الى الشبكة المنزلية عن طريق الشبكة اللاسلكية العمومية والانترنت بشكلٍ مؤمَّن، شريطة أن يتم طبعا إعداد خادوم VPN بالبيت بموازاة مع عميل VPN وتزويد الجهاز المحمول بمعلومات الدخول . هناك كثير من الشركات والمكاتب الذين يمكنون عمالهم من ولوج الشبكة الداخلية عبر الانترنت . إذا بذلتم قليلاً من المجهود في مرحلة التجهيز والترتيب فسوف تتمكنون بعد ذلك من دخول شبكتكم الخاصة بشكلٍ مؤمنٍ من كل بقاع العالم و يمكنكم من هناك الولوج إلى الانترنت دون خوف من تجسس شخص غير مرغوب فيه. إن برمجة الاختيار لهذه الأغراض هي Open VPN (https://openvpn.net/) المتواجدة عند لينوكس. أما من يتوفر في منزله على فغيتس بوكس / Fritz!Box لولوج الانترنت فيمكن له بكل بساطة استعمال وظيفة VPN التابعة لهذا الجهاز.

إن الشركات المتخصصة في تقديم خدمة الولوج الى الانترنت إنتبهن بسرعة إلى أن إعداد نظام VPN شخصي في البيوت ليست مهمة سهلة. يمكنكم أن تحصلوا على نظام VPN كخدمة عبر الانترنت بحيث يمكنكم

الاتصال بواسطة حاسوبكم اللوحي، أو هاتفكم الذكي أو حاسوبكم المحمول بالشبكة اللاسلكية العمومية عبر خادوم VPN التابع للشركة التي تقدم خدمات الانترنت. فهذا الخادوم يشتغل كبوابة تتواصلون عبرها بطريقة مشفرة بالكامل و بالتالي إيصال معلوماتكم للهدف المنشود، بخلاف برنامج VPN الذي يتم وضعه بطريقة شخصية هنا يجب وضع الثقة في الشركة المقدمة للخدمات على أنها سوف تتعامل مع المعلومات بطريقة آمنة دون إهمال ، وهو ما لا يتم ضمانه دائماً بحسب الاختبارات التي أ جرتها c't.

تشكيك صحي، استعمال دون قلق

بعد تقليب الموضوع من كل جوانبه يبقى الإختيار لكل مستعمل أن يؤمن اتصاله وتواصله عبر الشبكة اللاسلكية العمومية باستعمال كثير من البرامج. لكن من يرغب في استعمال شبكة الانترنت فقط من أجل إضاعة بعض الوقت ولا يهمه أن يطلع عليه شخص ما، فيمكنه استعمال شبكات الأماكن العمومية دون اتخاذ أي احتياطات تذكر.
لكن عندما ترغبون بتواصل سري، فحينئذ ينبغي أن تلجئوا إلى نظام التشفير ـ أما إلى أي مدى يمكن استعمال هذا النظام وهل ينبغي استعمال VPN، فهذا أمر يعود إلى الاحتياجات الأمنية الخاصة بكل شخص. و بخصوص المعلومات الشخصية التي من شأنها أن تجلب الأذى، إذا منحت من دون إذنكم ، فمن الأفضل هنا التفكير ملياً في تجنب الاتصال بجهازكم المحمول، وخصوصا إذا كان الأمر يتعلق بالعمليات المصرفية عبر الانترنت، فتجنبوا الإستعمال خارج شبكتكم الخاصة إلا للضرورة القصوى. لكن وحتى في إطار الشبكة الخاصة بكم في البيت فإن تواصلكم لا يعتبر مؤمَّنا إلا بمدى تَزَوُّدكم بأدوات التأمين، مثل نظام التشفير والعمل دون انقطاع على تحديث البرمجة وتوفير الحماية اللازمة التي تعتبر وسيلة فعالة ضد البرامج المضرة.

باتخاذكم لهذه الاحتياطات، سوف لن يعترض سبيلكم أي عائق اللاستمتاع بحياة الانترنت عند تنقلكم سواء عبر الشبكات اللاسلكية العمومية أو عبر الشبكة الحر ة للاتصال.

للمزيد من المعلومات:

ـ فرايفونك: Freifunk إدارة شبكة الحاسوب المحلية المنظمة بشكل ذاتي كشبكة حرة للاتصال اللاسلكي. تكنولوجيا الشبكات المجتمعية
http://freifunk.net/worum-geht-es/technik-der-community-netzwerke/

ـ فرايفونك: الشبكات اللاسلكية المجانية من خلال الممارسة ـ كراسة متضمنة لمقدمة وخلفية وتاريخ فرايفونك مقدم من طرف المؤسسة الإعلامية برلين ـ براندنبورج
http://www.mabb.de/files/content/document/Publikationen/Freifunk-Broschuere/freifunk_publikation_webversion.pdf

ـ فخ الهوت سبوت / النقطة الساخنة: الأخطار المتواجدة في الشبكات اللاسلكية العمومية
http://www.heise.de/ct/artikel/Die-Hotspot-Falle-1394646.html

ـ الحفاظ على الهدوء عند النقطة الساخنة Hotspot: اجراءات لتأمين استعمال الشبكة اللاسلكية العمومية
http://www.heise.de/artikel-archiv/ct/2012/01/088_Cool-bleiben-am-Hotspot

ـ الحيوانات الرامزة: الهجومات على مستعملي الهوت سبوت
http://www.heise.de/artikel-archiv/ct/2012/01/082_Das-Bestiarium

ـ هوت سبوت، ولكن بطريقة آمنة: الشبكات اللاسلكية خارج البيت عن طريق استعمال VPN دون وجود خطر التنصت.
http://www.heise.de/netze/artikel/Hotspot-aber-sicher-221475.html

محادثات بصوت خافت: تطبيقات الميسنجر المشفرة في الاستعمال اليومي
-http://www.heise.de/ct/ausgabe/2015-13-Test-Verschluesselnde-Messenger-Apps-im-Alltagseinsatz-2662824.html

ـ سد الطريق على المتجسسين: الخدمات البديلة للتواصل عبر البريد الالكتروني بشكل مريح وآمن من التجسس
http://www.heise.de/ct/ausgabe/2015-13-Test-Alternative-Dienste-fuer-komfortable-und-abhoersichere-Mail-Kommunikation-2661636.html

ـ الخصوصية الافتراضية: الحماية الكاملة التي تقدمها خدمات VPN

http://www.heise.de/ct/ausgabe/2013-20-Test-So-viel-Schutz-bieten-VPN-Dienste-2314876.html

- Gpg4Win und GnuPG – PGP für Windows
البرنامج الخاص بالويندووز
http://www.gpg4win.de/

- Enigmail – PGP-Plugin für Thunderbird
البرنامج الخاص ب: Thunderbird
https://www.enigmail.net/download/

iPGMail – PGP für iOS
البرنامج الخاص بنظام iOS
https://ipgmail.com/

GPG Suite – PGP für Mac OS X
البرنامج الخاص بنظام Mac OS X
https://gpgtools.org/

OpenKeychain – PGP für Android
البرنامج الخاص بنظام اندرويد
http://www.openkeychain.org/about/

OpenVPN – Open-Source-VPN für Alle
برنامج VPN لكل الأنظمة
https://openvpn.net/