دليل الاستخدام الآمن للهواتف العاملة عبر الأقمار الصناعية

SATPHONES

مارس 2012

يقدّم هذا الدليل نظرة شاملة على الاستخدامات المحتملة للساتفون satphones في الأنظمة القمعية. أنه يحتوي على أفضل الممارسات في مجال الحفاظ على السلامة الشخصية خلال التواصل الفعال مع أقل فرصة للكشف والمراقبة.

يتألف هذا الدليل من 7أقسام وهي:

نظرة عامة

1.0 ما هو الساتفون؟

2.0 تشغيل الساتفون

2.1 التشغيل
2.2 موجة البث
2.3 استعمال الساتفون، عملية توجيه

3.0 المخاطر المعروفة لاستخدام الساتفون

3.1 مصادرة الهاتف
3.1.1 سجل المكالمات
3.1.2 ملف المرسلات
3.1.3 دليل الهاتف
3.2 اعتراض الاشارة
3.2.1 موجات الاشارات الاذاعية
3.2.2 ارسال الاحداثيات
3.3 فك التشفير

4.0 الاحتياطات الأساسية للحد من الخطر

4.1 حذف جميع السجلات
4.2 قم بتمويه هاتفك
4.3 قم بالخداع عن طريق التحدث بالرموز
4.4 تدمير الـ SIMCARD والهاتف

5.0 استخدام الساتفون بطريقة أكثر أمنا

5.1 المكالمات الصوتية
5.2 الرسائل القصيرة sms
5.3 البريد الإلكتروني

6.0 اختيار العلامة التجارية التي يجب ان تستعملها

6.1 ثريا
6.1.1 الخلفية
6.2.2 مشاكل الثريا
6.3 iSatphone \inmarsat

7.0 كيفية تحسين سلامة لـ isatphonePro

7.1 قفل الهاتف
7.2 اضافة المال لرصيد الهاتف عن بعد
7.3 مسح سجل المكالمات
7.4 حذف ملف المرسلات
7.5 حذف دليل الهاتف
7.6 استخدام سماعة بلوتوث للحد من الاشتباه
7.7 تعطيل الهاتف

نظرة عامة

أصبحت الهواتف العاملة عبر الاقمار الصناعية، والمعروفة أيضا بـ satphones، وسائل اتصال معروفة. قد يحتاج النشطاء للساتفون للوصول الى العالم الخارجي وذلك في المناطق ذات القدرة المحدودة على الدخول الى الشبكة أو حيث توجد وسائل اتصالات تقليدية أو حين يتم قطع طرق ا الأتصالات. إن استخدام الساتفون ينطوي على مخاطر معينة.

على سبيل المثال، سيكون من المستحيل أن تعرف بالضبط كيف يتم مراقبة الاتصالات الخاصة بك عندما تعتمد على هذه التكنولوجيا المعقدة. أيضا، غالبا ما تكون هذه الهواتف ممنوعة من قبل الحكومات القمعية، وقد تقوم تلك الحكومات بالبحث عن الاشخاص الذين يستخدمونها. أن هذا الدليل ساعدتك يساعدك على الابتعاد عن الاضواء وتحسين الفرص للتهرب من الكشف والرصد من جانب السلطات.

1.0 ما هو Satphone؟

هاتف متصل بالأقمار الصناعية، هاتف يعمل بالاقمار الصناعية، أو الساتفون هو نوع من الهواتف النقالة التي لها صلة بالأقمار الصناعية الدوّارة بدلا من مواقع الخلية الأرضية وهي توفر وظائف مماثلة للهواتف النقالة الأرضية مثل الصوت وخدمة الرسائل القصيرة والقدرة على الولوج الى الانترنت على الرغم من انخفاض عرض النطاق الترددي.

ان الهواتف المتصلة بالأقمار الصناعية هي أجهزة معقدة للبث الإذاعي. أجهزة الراديو والهواتف المحمولة تستخدم هوائيات على الأرض لإرسال الإشارة إما عن طريق البث الإذاعي أو المكالمات الهاتفية. أما الساتفون فتقوم بإرسال إشارة إلى قمر صناعي في مدار حول الأرض وبعد ذلك يقوم القمر الصناعي ببث الإشارة مرة أخرى إلى الأرض، إلى "محطة أرضية "، تسمى بغيس GES. يتم إرسال الإشارة من المحطة الأرضية إلى مزود خدمة للإتصالات وإلى وجهتها، اي المتلقي للمكالمة. تلعب GES دورا بمثابة بوابة بين هاتف الساتفون الخاص بك وبين شبكات الهاتف المحمول التقليدية وبين شبكات الهاتف الثابت والهواتف المتصلة بالأقمار الصناعية الأخرى.

نقل المعلومات إلى القمر الصناعي في المدار هو" الإرسال" . تلقي المعلومات من الأقمار الصناعية هو" التلقي". وقد تكون هذه المعلومات مؤلفة من بيانات أو صوت. يمكن اعتراض الاشارة في أي وقت يكون هناك اتصال نشط مع القمر الصناعي: أثناء الإرسال أو التلقي.

حقاظا على أمنك: إذا كنت تتواصل مع شخص من خارج خدمة شبكة الساتفون فان إتصالاتك قد تكون خاضعة للمراقبة على خط المستخدم الاخر (المتلقي). التواصل مع مستخدمي الساتفون الاخرين هو أمر أكثر أمنا. كما سوف نتعلم في هذا الدليل، ان هذه الطريقة ليست آمنة تماما ولكن اذا اتبعت هذه الخطوات الأساسية تستطيع أن تحد من المخاطر.

هذا الدليل يوفر التقنيات اللازمة لزيادة السلامة ولكنها ليست ضمانا لاتصالات آمنة مئة بالمئة.

2.0 تشغيل الساتفون

قد تبدو هواتف الـ Satphones هواتف نقالة كبيرة ولكنها تختلف في بعض العناصر الأساسية .عملية التشغيل مشابهة نسبيا في حين أن عملية الاتصال تحوي اختلافات ملحوظة.

2.1 التشغيل

تتطلب الأجهزة النقالة المتصلة بالأقمار الصناعية بطاقات الـ simcards لتفعيلها ويجب أن يكون لها خطة مرتبطة ببطاقة الـsimcard . قد تكون الخطة مدفوعة مسبقا أو لاحقا. إذا كانت مدفوعة مسبقا فيجب أن يكون للهاتف دقائق مرتبطة بالـ simcard ويمكن دفع ثمن الدقائق عبر الانترنت أو مباشرة من خلال تقديم رموز بطاقة الشحن عبر الرسائل القصيرة. أنظر قسم 7.2 لمزيد من التفاصيل حول إضافة المال لرصيد الساتفون.

2.2 موجة البث

ان جهاز الساتفون لا يتصل أوتوماتيكيا بشبكة الاتصال الخاصة بهواتف الساتفون بل يتصل مباشرة بقمر صناعي أو اكثر من الأقمار الصناعية الدائرة في الفضاء.
لكي تحصل على إشارة عليك ان تقف في مكانك وان توجّه لاقط الهاتف اللاسلكي نحو السماء وأن تنتظر حتى يلتقط الهاتف اشارة البث. سوف يقوم هاتفك بالتقاط إحداثية موقعك عبر نظام الـ GPS وبعدها ستقوم بالدخول الى الشبكة. ان هذه العملية قد تأخذ حوالي دقيقة من الوقت.

ملاحظة أمنية: يشكّل الوقت الذي تحتاجه للدخول الى الشبكة أول تهديد كبير لأمنك الشخصي.

فيما تنتظر أن يقوم هاتفك بدخول الشبكة تستطيع السلطات أن تراقب هذه العملية وتكتشفها. في **قسم 4.2** سوف نناقش الخطوات التي تحتاجها لتمويه هاتفك. هذا الأمر قد يؤدي الى تقليص نسبة الخطر.

ملاحظة: لكي تحصل على إشارة، يجب ان يكون هاتفك في وضعية التشغيل بما يعني أن على لاقطك اللاسلكي ان يكون في الوضعية المناسبة (ممدودا). وعلى عكس الهاتف المحمول العادي، بالرغم من أن هاتف الساتفون قد يكون في وضعية التشغيل فان ذلك لا يعني بالضرورة أنه يستطيع أن يستقبل الاتصالات. لا يستطيع الساتفون أن يقوم بالاتصالات وبتلقيّها دون أن يقوم الزبون بدخول الشبكة متعمدا. هذا قد يصّعب عملية الاتصال دون موعد محدد مع مستخدمي الساتفون الاخرين. بالتالي، لا يجب أن يتم الاعتماد على هواتف الساتفون للاتصالات الملحة والاضطرارية.

2.3 استعمال الساتفون، عملية توجيه:

إن ما يلي هو لمحة كاملة عن الخطوات اللازمة لاقامة اتصال هاتفي أو لارسال رسالة قصيرة عبر الساتفون:

1. قم بتشغيل الهاتف
2. جد مكانا تستطيع رؤية السماء منه بوضوح
3. مدّ اللاقط اللاسلكي للبحث عن إشارة بث.
4. يقوم الهاتف بتحديد الاحداثيات لنظام الـ GPS
5. يقوم الهاتف بدخول شبكة القمر الاصطناعي
6. قم بالاتصال أو ارسل رسالة قصيرة أو الكترونية
7. يقوم الهاتف بالاتصال بالقمر الصناعي
8. يقوم القمر الصناعي ببثّ الاشارة التي تلقاها الى محطة أرضية (GES)
9. تقوم المحطة الأرضية بارسال المعلومات الى المتلقي المطلوب.
10. تقوم المحطة الأرضية بتسجيل احداثيات الـ GPS فيما تقوم بارسال المعلومات
11. إنهِ الاتصال أو الرسالة القصيرة/ الاميل.
12. يقوم الهاتف بادخال احداثيات موقعه عبر الـ GPS، الرقم الذي تم الاتصال به، ومدة الاتصال.
13. أغلق اللاقط اللاسلكي.
14. أقفل الهاتف وخبئه.

3.0 الأخطار المعروفة لإستخدام الساتفون

3.1 مصادرة الهاتف

في كثير من الحالات ستكون انت وزملاؤك أسوأ الأعداء على أنفسكم. هناك العديد من المخاطر الفنية المتعلقة بالاتصالات عبر الأقمار الصناعية لكن الخطر الأكثر احتمالا يتعلق بالمستخدمين. غالبا ما يتم التغاضي عن هذه المخاطر لأنها في المقام الأول نتاج عمليات الاتصال العادية. إن خصائص الهاتف مثل سجل المكالمات، دليل الهاتف، وملف المرسلات، قد تعرض حياتك وحياة الآخرين للخطر وخاصة في الدول القمعية.

هذه الميزات تساعدك على الحفاظ على جهات الاتصال الخاصة بك في متناول اليد ولكنها توفر ايضا سجلا يسهل للسلطات الوصول اليه مما يمّكنها من التنصت على المكالمات الخاصة بك، بالرغم من عدم قدرتهم على الولوج الى البث الخاص للساتفون.

عندما يتم حذف ملف على جهاز الكمبيوتر، لا يتم تدميره بالكامل ويمكن إعادة بنائه من دون مزيد من التدابير. ومن الممكن أيضا بناء سجلات الساتفون الخاص بك عبر استعمال بيانات من مزود الخدمة أو من الساتفون نفسه. حذف المعلومات غير مأمون بالكامل ولكن سوف تجعل من الصعب على السلطات الوصول إلى المعلومات على الهاتف المصادر.

3.1.1 سجل المكالمات:

سيقوم هاتفك بالاحتفاظ بسجل جميع الذين اتصلت بهم تلقائيا لذلك تأكد من حذف هذا السجل في كل مرة تجري فيها مكالمة هاتفية. فإن أي رقم تتركه في السجل سيكون معرضا للخطر إذا تمت مصادرة الهاتف. قد يكون أمرا مشبوها أن يكون لديك سجلا فارغا ولكن ذلك سيكون له تأثير أقل على زملائك.

3.1.2 ملف المرسلات:

وبشكل مماثل لسجل المكالمات، سوف يقوم هاتفك بتخزين قائمة من الرسائل القصيرة ورسائل البريد الألكتروني المرسلة من الهاتف. تأكد من حدف هذه بعد أن ترسل اية رسالة.

3.1.3 دليل الهاتف:

يوّفر دليل الهاتف قائمة بالأسماء للسلطات وعندئذ يكون أي اسم مدرج في دليل الهاتف معرضا للخطر هذا إذا ما تم مصادرة الهاتف. قد يكون مشبوها أن يكون دليل الهاتف فارغا ولكن ذلك سيكون له تأثير أقل على زملائك.

3.2 إعتراض الإشارة

تعتبر جميع الهواتف أجهزة للبث الإذاعي. ترسل هواتف الساتفون إشارات إذاعية إلى قمر صناعي في مدار حول الأرض. من ثم يبث القمر الصناعي الإشارة نفسها مرة أخرى إلى الأرض، إلى "محطة أرضية "، أو غيس GES. تمر الإشارة من المحطة الأرضية عبر نظام آخر للاتصالات إلى وجهتها اي متلقي المكالمة. يمكن اعتراض إشارة الهاتف في أي وقت يكون هناك اتصال نشط بين الجهاز والقمر الصناعي: أثناء الإرسال أو التلقي، أي عندما يعيد القمر الصناعي ارسال صوت المتلقي اليك.

اعتمادا على نوع المعدات المتاحة للسلطات، هناك عدة مخاطر محتملة لاعتراض الاشارة مبوبة في القسم التالي.

3.2.1 موجات الاشارات الاذاعية

إتصالات القمر الصناعي تستخدم الإشارات الإذاعية لنقل المعلومات. يمكن اعتراض هذه الموجات عبر آلات رخيصة ومحلية الصنع. يقوم الاعتراض على استخدام جهازين للاستقبال أو أكثر لتحديد موقع وجود إشارة راديو الأرسال. يتم تحديد الموقع من قبل المتلقي على أساس محاور زوايا أجهزة الاستقبال. من الأرجح أن تملك الدول المتقدمة والتي تمتلك قدرات أمنية متقدمة هذه التقنية. كما يمكن للدول الأقل تطورا وحتى الجهات غير الحكومية الفاعلة أن تكون قادرة على تطوير هذه القدرات. لهذه الأسباب، يجب تقصير مدة البث قدر الامكان.

في بعض الحالات قد تملك السلطات المختصة المعدات المناسبة "للاستماع" الى ارسالك، ولكن هذا يتطلب تكنولوجيا متقدمة للغاية ومتطورة. راجع قسم **4.3 الخداع عبر التحدث بالرموز** وذلك للحصول على نصائح حول كيفية التواصل بطريقة أكثر أمنا إذا كنت تشك في المكالمات.

3.2.2 إرسال الاحداثيات

اتصالات الساتليات تتطلب احداثيات الموقع اعتمادا على نظام GPS وذلك للحصول على خدمة أفضل. نظام الـ GPS يعني نظام تحديد المواقع العالمي. موقع GPS الخاص بك يعطي الإحداثيات الدقيقة للسلطات للعثور على مكان وجودك. وهذا يوّفر امكانية تحديد موقع أي فرد يستخدم جهازا للأقمار الصناعية مع إحداثيات دقيقة. قد يتم تسجيل موقعك في مزود الخدمة الأرضية في المحطة الأرضية (GES). قد تكون بيانات GES في متناول العديد من الجماعات المختلفة بما في ذلك الحكومات المحلية أوالحكومات قريبة والمساهمين والشركاء المحليين وكل من هو قادر على اختراق أمن نظم GES.

إذا كانت السلطات تملك التكنولوجيا الصحيحة أو لديها التشفير المحدد ورموز الارسال لهاتف الساتفون الخاص بك فسيكون بامكانها استخدامها لتحديد احداثيات موقع هاتفك واعتقالك.

3.3 فتح التشفير

إن البث الفضائي مشفر، ولكن العديد من الحكومات قادرة على هزم التشفير المستخدم من قبل هذه الهواتف. ان التشفير العادي قد يكفي لردع الكشف والرصد ولكن لا يمكنه ضمان الأمان كاملا.

ملاحظة أمنية: لقد تم كسر تشفير ثريا والحكومات الأكثر تقدما قد تكون قادرة على كسر التشفير من هواتف ساتفون أخرى. لمعرفة المزيد راجع قسم 6.2.2

إن الأتصالات الساتلية هي عرضة للتنصت والمراقبة من قبل المتطفلين الذين قد يستعرضون الصوت والرسالة ونقل البيانات. بالرغم من ان المعدات والقدرة اللازمة على كسر التشفير قد لا تكون متاحة للسلطات فيمنطقتك ولكنهم يستطيعون كسر هذا مع مرور الوقت. إذا تمكنت السلطات من اعتراض الإرسال الخاص بك، فهم قادرون على تسجيل الإشارات، وبالتالي سيمكنهم هذا من كسر تشفير الاشارة بالنهاية والنظر في محتوى المكالمات والرسائل.

ملاحظة أمنية: في فبراير 2012 أثبت باحثان ألمانيان القدرة على فك معايير تشفير GMR-1 و GMR-2. لا تستخدم هذه المعايير من قبل جميع الهواتف التي تعمل بالاقمار الصناعية ولكن ثريا وإنمارسات Inmarsat iSatphoneProيستخدمان هذا المعيار على حد سواء. إن الطريقة المستخدمة هي تقنية ولكن تم توثيق الامكانية الآن ومن المرجح أنّ الحكومات ستبدأ قريبا بالحصول على التكنولوجيا اللازمة.

نظرا لإمكانية حصول السلطات على مثل هذه المعدات **يجب أن** لا تكشف معلومات شخصية التي قد تهدد حياة الأخرين أو غيرها من المعلومات الهامة عبر الأقمار الصناعية. إذا كان لا بد من ذلك من فضلك تذكر أن **تتكلم باستخدام الرموز** لردع السلطات ومنعهم من الفهم.

4.0 الاحتياطات الأساسية للحد من خطر

الساتفون هي تكنولوجيا مغلقة وليس من السهل تعديلها. وبسبب هذا فإنه من المستحيل أن يكون هناك اتصالات آمنة تماما مع الساتفون. ومع ذلك يمكن استخدام هذه الاحتياطات الأساسية مع أي ساتفون لزيادة الأمان والتقليل من خطر المراقبة أو الاحتجاز من قبل السلطات.

4.1 حذف جميع السجلات

لا تقم بحفظ المعلومات والاتصالات على الساتفون على الرغم من أن الأجهزة الأمنية قد تحصل على السجلات من خلال وسائل أخرى . لا تجعل الأمر سهلا لهم. حتى من دون أسماء يمكن لقائمة أرقام لهواتف خلوية أو هواتف الأقمار الصناعية أن تكون كارثية اذ قد تتمكن السلطات من تتبعها وتحديد موقعها. كل شركة مصنعة للهاتف لديها نظام مختلف، لذلك يجب ان أفهم كافة الخطوات المطلوبة لحذف السجلات عن هاتفك في أقرب وقت ممكن.

ملاحظة: انظر **القسم 7.0** للحصول على خطوات محددة لجعل Inmarsat iSatphonePro أكثر أمانا.

عند الاتصال مع الأفراد الذين قد يكونون مهددين أو تحت المراقبة، تأكد من الحفاظ على المعلومات الخاصة بهم في مكان آمن.

4.2 قم بتمويه هاتفك

عند استخدام الهاتف للمكالمات لا تتركه في العراء. قم باستعماله دوما مع سماعة بحيث يظهر أنّك تستخدم شبكة الاتصال المحلية الخلوية ولست تقوم بإجراء مكالمة عبر الأقمار الصناعية. ان إستخدام سماعة بلوتوث يجعل من الاسهل إخفاء الهاتف ولكن هناك مخاطر أمنية إضافية مدرجة في القسم 7.5.

حافظ على الهاتف مخبأ ومموها في جميع الأوقات إذا كان لديك الوقت. ضع الهاتف في مكان بزاوية جيدة باتجاه القمر الصناعي، ولكن قم بتمويه موقعه الفعلي بقدر الإمكان. ضع الهاتف داخل حقيبة مفتوحة، أو وراء بعض الشجيرات. قد يكون هذا صعب لأن الهاتف في حاجة إلى رؤية واضحة للسماء. جرّب اذا كان ممكنا في مكان آمن لترى كيف يمكن أن تهرب من المراقبة دون التدخل بفعالية الهاتف.

4.3 قم بالخداع عن طريق التحدث بالرموز

في الحالات التي يتم التواصل مع المتعاونين والناشطين الآخرين وما إلى ذلك قم بإخفاء نواياك الحقيقية. استخدم الرموز وناقش المواضيع الشائعة التي من يمكنك ان تشاركها ولديها المعاني المزدوجة. لا تناقش نواياك مباشرة.

مثال:
استخدم عبارات ومصطلحات لا تنسى وتحمل معان مزدوجة أو استخدم موضوعا شائعا مثل آيات دينية معينة. على سبيل المثال استخدم مصطلحا يشير إلى السلطات مثل "العم".

عند التدقيق مع جهة اتصال لتحديد أولا ما إذا كان الشخص في مأمن من السلطات، تستطيع ان تسأله ببساطة: " هل أتى عمك إلى المدينة؟" نعم قد يدل على أنه ليس وقتا مناسبا للحديث أما لا فتدل على أن الوضع آمن للكلام.

هذا قد يتيح المجال لرموز أخرى ويمكن للمتلقي أن يقول "عمي كان هنا ولكنه ذهب وانا سأكون مشغولا خلال الأيام القليلة المقبلة"، مشيرا الى انه من غير المستحسن لك أن تحاول الاتصال به في المستقبل القريب.

وإضافة إلى ذلك "عمي كان هنا وذكرني بأن لم شمل الأسرة سيحدث في وقت قريب" فيمكن أن تشير إلى أن السلطات ربما تخطط لاستجوابك أو استجواب زملاء اخرين قريبا.

قد تحتاج أيضا إلى تفحص الرموز التي لا تملك مثل هذه العلاقة المباشرة حيث أن الجمع بين المواضيع التي نوقشت يوفر معلومات. كما يمكنك تقديم معلومات خاطئة أو مضللة كموقع مكان محدد مما يصعب عملية الفهم على الذي يتنصت على المكالمة.

على سبيل المثال "هل أخبرتك عن حفل زفاف ابن عمي القادم؟ لقد تزوجت من رجل جيد جدا من حلب. " في هذه الحالة مصطلح" عرس "و" رجل جيد جدا "يمكن ان تكون عبارات حركية حيث يشير العرس الى أن السلطات تبحث عنك قريبا بينما " رجل جيد جدا " يدل على جهاز أمن معين. ويمكن استخدام عبارة أخرى مثل "تاجر ثري" للإشارة إلى جهاز مختلف.

إخفاء نوايك قد تنقذ حياتك أو حياة الآخرين.

4.4 قم بتدمير الـ simcard والهاتف

إذا تم مصادرة الهاتف الخاص بك سوف توّفر الـ SIMCARD المعلومات التي يمكن استخدامها ضدك وضد زملائك. حافظ على الـ SIMCARD بعيدة عن الهاتف بحيث يمكن تدميرها بسرعة. إذا كان بامكانك أن تدمّر هاتفك فان ذلك قد يحد من الخطر ولكن ما هو أهم هو أن تتابع الاحتياطات الثلاث السابقة وأن تحاول تجنب الاكتشاف من قبل السلطات.

5.0 طريقة استخدام الساتفون الخاص بك بطريقة آمنة

قام القسم السابق بتوضيح الاحتياطات الأساسية التي يمكنك إتخاذها مع الساتفون. يعرض هذا القسم تقنيات محددة يمكن استخدامها مع الساتفون الخاص بك فيما يتعلق بالاستخدامات الأولية بالاضافة الى إجراء المكالمات الصوتية وإرسال الرسائل القصيرة أو رسائل البريد الألكتروني.

5.1 المكالمات الصوتية

المكالمات الصوتية هي وسيلة خطرة للغاية للاتصال عبر الأقمار الصناعية. عند إجراء مكالمة تأكد أن تكون المكالمة قصيرة قدر الإمكان وذلك بسبب احتمال اعتراض **الاشارات اللاسلكية** في هاتفك أو **إحداثيات نظام الـGPS** .

يمكن للسلطات أن تستخدم إشارات هاتفك اللاسلكية لتحديد موقع تواجدك في غضون أقل من ثلاث دقائق. عندما تصبح أساليبهم أكثر تعقيدا فقد يكونوا قادرين على تحديد موقع الساتفون بسرعة أكبر. في بعض الحالات قد تكون السلطات قادرة على الاستماع الى مكالمتك عبر اعتراض الاشارات الاذاعية لهاتفك. وقد تقوم السلطات بالتنصت على الهاتف على الطرف الاخر وذلك اذا كان لديهم امكانية الوصول الى مزوّد الخدمة.

كلما أطلت البقاء على الخط كلما قدمت فرصا أكبر للسلطات للتعرف على مكانك بالضبط عبر احداثيات هاتفك.

عند إجراء مكالمة، تاكد ان الشخص المقابل لا يملك معلومات واضحة عن وضعك ولا تبقى على الخط مدة أطول مما تراه آمنا. من الأفضل الحفاظ على مدة المكالمات الى أقل من ثلاث دقائق. قم باعداد تعليقاتك من قبل وكن واضحا بأنك لن تقوم بمناقشة بنود خارج برنامج الاتصال المعد مسبقا.

عند إجراء **مكالمة صوتية** للتواصل مع زميل أو التنسيق مع ناشطين آخرين تذكر أن تتكلم **باستخدام الرموز**. وهذا مهم جدا من أجل خداع أي شخص يحاول الاستماع اليك أو يحاول أن يكسر **تشفير** هاتفك.

إن **التحدث باستخدام الرموز** واستخدام العبارات الشائعة التي لها معنى مزدوج قد تبقيك أنت وغيرك آمنين على الرغم من أنك قد لا تعرف أن أحدا ما يرصد محادثاتك الخاصة. استخدم العبارات الشائعة بدلا من كلمات خاصة قلما تستعملها.

إحذف سجل المكالمات من هاتفك. ليس هناك أسوأ من تهيئة أرشيف مفهرس من المعلومات تكون بانتظار السلطات. إذا فشلت في القيام بذلك، سوف تعّرض الآخرين للخطر ويمكن أن تزيد من الأخطار لنفسك إذا ما تم مصادرة الهاتف.

5.2 الرسائل القصيرة SMS

ان **الرسائل القصيرة** هي وسيلة مريحة للغاية لتوجيه رسالة. يتم تسليم الرسائل القصيرة عبر البريد الإلكتروني، حيث يتم إرفاق رقم الهاتف الخاص بك بعنوان الحامل الألكتروني المحدد (carrier specific server)، مثل 555555@text.phonecarrier.com.

على الرغم من إدعاءات الشركة المصنعة إن الرسائل القصيرة لا توفر تشفيرا آمنا. لا تقم بارسال المعلومات الحساسة عبر الرسائل القصيرة إلا إذا كنت على استعداد لأن يتم قراءتها من قبل السلطات. إذا تم اعتراض الـ SMS، فمن المحتمل ان تكون مسجلة ويتم كسر **التشفير** في وقت لاحق إن لم يكن على الفور.

قد تستغرق الرسالة القصيرة وقتا أقل من المكالمة الصوتية، لذلك قد يكون خطر اعتراض الإشارات الإذاعية القصيرة أو استغلال **احداثيات الهاتف** أقل من المكالمة الصوتية. ومع ذلك فمن المرجح أنّ مضمون الرسالة سيكون قابلا للاسترداد من قبل السلطات إذا تم اعتراض **الإرسال** الخاص بك.

قم **بخداع** المراقبين غير المرغوب بهم من خلال استخدام العبارات والمصطلحات مع رمز له معنى مزدوج. إحذف الرسائل من ملف المرسلات في الهاتف. ليس هناك شيء أسوأ من تهيئة أرشيف مفهرس من المعلومات التي تنتظر مراجعة السلطات في حال تم اعتقالك.

5.3 البريد الإلكتروني

ويمكن إرسال **البريد الإلكتروني** عبر أي هاتف يعمل بالاقمار الصناعية ولكن يتم تسليمها عبر بروتوكولات شبيهة بالـ SMS، وتقتصر على ما يقرب من 160حرفا.

قد تقرر إستخدام ميزة البريد الإلكتروني بدلا من الرسائل القصيرة لأنك تتوقع أن يكون البريد الإلكتروني أكثر أمنا. هذا غير صحيح. البريد الإلكتروني المرسل من الساتفون الخاص لا يّوفر نفس الحماية مثل البريد الإلكتروني المرسل عبر الكمبيوتر أو الهاتف المحمول.

يوّفر الكمبيوتر والإنترنت عبر الهاتف النقال القدرة على استخدام أدوات أمنية إضافية. فمن الأصعب اعتراض البريد الالكتروني المرسل عن طريق الكمبيوتر أو الهاتف المحمول عبر الرابط HTTPS (أنظر الى www.eff.org/https-everywhere). كما يمكن استخدام برنامج تور في بعض الهواتف المحمولة وأجهزة الكمبيوتر لحذف الاسم خلال عمل الكومبيوتر على الانترنت ولاخفاء الهوية والموقع الخاص بك. على كل حال قم باستخدام اتصال إنترنت آمن للتواصل وليس الساتفون.

فإن البريد الألكتروني مثله مثل **الرسائل القصيرة** قد يستغرق وقتا أقل من مكالمة صوتية كما أنّ الخطر من اعتراض الرسالة عبر **الإشارات اللاسلكية** أو استغلال احداثيات الهاتف قد يكون أقل من المكالمة الصوتية. ومع ذلك فمن المرجح أن بامكان السلطات استرجاع مضمون الرسالة إذا تم اعتراض **إرسالك** الخاص.

إخدع المراقبين غير المرغوب بهم من خلال استخدام العبارات والمصطلحات المرمزة ذي معنى مزدوج. **إحذف** البريد الإلكتروني من ملف مرسلات الهاتف. ليس هناك أسوأ من تهيئة أرشيف مفهرس من المعلومات التي تنتظر مراجعة السلطات في حال تم اعتقالك.

6.0 إختيار ماركة الساتفون الذي يجب ان تستعمله (العلامة التجارية)

ليس كل هواتف الساتفون متساوية. كل ماركة لها حدودها وكما سيتم الشرح فمن المستحسن عدم استخدام هواتف الثريا اذا كان بامكانك تجنبها. اذا وضعت هذا التحذير جانبا فان الأجزاء السابقة ما تزال توفر أفضل الممارسات الواجب اتباعها للتقليل من المخاطر التي قد تواجهك.

هناك مجموعة متنوعة من مقدمي خدمات الاتصالات الفضائية، بما في ذلك الثريا، انمارسات، ايريديوم، وجلوبال. هناك أيضا MSV و ICO، وتيليداسيك لكن غير متوفرين أو لا يفرّون خدمات للمستهلكين.

ووفقا لأبحاثنا، على الرغم من عدم وجود ساتفون امنا بحق وجدنا أن شركة الثريا على وجه الخصوص غير آمنة وينبغي تجنبها بأي ثمن. ونحن نوصي بـ انمارست Inmarsat's iSatphonePro لسهولتة وتوافره واكثرة استخدامه من قبل العديد من الصحفيين والناشطين في مختلف أنحاء منطقة الشرق الأوسط.

6.1 لماذا لا للثريا؟

6.1.1 الخلفية

أصبحت الثريا واحدة من أكثر شركات الاتصالات الساتلية شعبية وذلك بسبب أسعار منتجاتها المعقولة ووظائفها الواسعة لا سيما في منطقة الشرق الأوسط. طوال 2011 بدأت شعبية الثريا بالانخفاض وذلك بسبب السهولة التي تمّكن الحكومات من منع أو اعتراض الثريا. تم أول حظر للمرة الاولى لمدة تزيد عن 6 أشهر في عام 2006 حين قامت الحكومة الليبية بتشويش واسع النطاق للخدمة من داخل أراضيها. وبسبب شعبية الثريا في الشرق الأوسط استهدفت الولايات المتحدة هذا المزود وقامت باعتراضه وفك شفرتهة.

6.2.2 مشاكل الثريا

زعم نشطاء سوريون في 2011 أن الحكومة السورية قامت باختراق شبكة ثريا الأمنية ويعتقد أن رامي مخلوف يسيطر على فرع الثريا السوري. يعتقد النشطاء أنه يملك القدرة على الوصول الى رموز فك تشفير الثريا وغيرها من السجلات وقد قدّمها فعلا الى النظام السوري. وأفاد النشطاء المحتجزين في وقت لاحق سماعهم تسجيلات لمحادثات أجروها من خلال الساتفون حيث لم نكن قادرين على تحديد ما إذا كان التسجيل حصل من خلال اعتراض الارسال. من المرجح أن الناشطين كانوا يتواصلون مع شخص على مزود الخدمة المحلي والتي كان يتم التنصت عليها من قبل السلطات.

وفقا لصفحة الاستراتيجية، في عام 2003، " الثريا قد أعلنت مؤخرا أنه في حين أن الهواتف تنقل احداثيات لتحديد الموقع بشكل دوري (للتأكد من جودة إشارة القمر الصناعي) ولكنه تم ارسال المعلومات بشكل مشفر ولا يمكن لأحد أن يحصل على معلومات تحديد الموقع سوى لشخص مزود بالقدرة على الوصول إلى الرموز أو مع قدرات قوية بفك التشفير."

وقد تم توثيق بعض الحالات التي تشير الى أن الولايات المتحدة وربما السلطات الهندية قادرة على التنصت على المحادثات بين الأفراد الذين يستخدمون هواتف الثريا فقبل وقوع الهجمات الإرهابية في مومباي في عام 2008 " قول المسؤولون ان واحدا من الهواتف الذي تم ايجاده كان هاتفا يعمل بالاقمار

الصناعية من ماركة الثريا. "عندما نحصل على الرقم سنكون قادرين على التعرف على كل الذين تم الاتصال بهم والمكان الذي تم إجراء المكالمات منه" صرّح ضابط مخابرات سابق".

استنادا إلى هذه المعلومات، نحن نوصي النشطاء بتجنب استخدام هواتف الثريا في أي ظرف من الظروف.

لماذا استخدام Inmarsat's iSatphonePro ؟
لماذا نعتقد أن iSatphonePro أكثر أمانا من الثريا وآمنة نسبيا كما غيرها من العلامات التجارية؟ في حين أن الثريا مخترقة بالتأكيد، قد تكون غيرها من الخدمات مخترقة كذلك. إنّ محتويات هذا الدليل سيساعدك على الحفاظ على أكبر قدر ممكن من الأمان على الرغم من المخاطر الجدية التي تطرحها تكنولوجيا الاتصالات عبر الأقمار الصناعية.

في وقت النشر، في يناير 2012، لم يكن هناك أية حوادث اختراق معروفة للانمارسات من قبل السلطات السورية. باعتبار أن مقر الشركة في المملكة المتحدة وهناك قيود قانونية تمنع من إنمارسات توفير سجلات الهاتف للحكومة السورية. في وقت نشر هذا الدليل لم تكن هناك حسابات لمعتقلين استخدموا هاتف إنمارسات وتم اعتقالهم بسبب عملية اتصال قاموا بها عبر هاتف انمارسات.

ملاحظة أمنية: جميع الهواتف العاملة بالاقمار الصناعية تشكل خطرا كبيرا محتملا على المستخدم حيث أن هناك إمكانية حقيقية جدا لاعتراض الإرسال وتحديد احداثيات الموقع.

7.0 كيفية تحسين سلامة iSatphonePro

في كثير من الحالات، ستكون وزملاؤك أسوأ الأعداء على أنفسكم. على الرغم من أن هناك مخاطر فنية عديدة فيما يتعلق بالاتصالات عبر الأقمار الصناعية فان الخطر الأبرز يخلقه الذي المستخدمون أنفسهم غالبا ما يتم التغاضي عن هذه المخاطر لأنها ناتجة عن عملية الاستخدام العادية.

في حالة الدول القمعية، يمكن لخصائص الهاتف مثل سجل المكالمات، دليل الهاتف، وملف المرسلات أن تعرض حياتك وحياة الاخرين للخطر. هذه الميزات تحافظ على شبكة الاتصالات الخاصة بك في متناول اليدين، ولكنها أيضا توفر سجلا للسلطات يمكنها عبره التنصت على المحادثات الخاصة بك حتى لو كانوا لا يستطيعون الوصول إلى بثك الخاص.

هذه التوجيهات المرفقة سوف تجعل من iSatphonePro أكثر أمانا وتساعدك على تجنب المخاطر المذكورة في هذا الدليل.

7.1 قفّل هاتفك

لمنع العيون الحشرية من فحص هاتفك، يجب أن تدير خيار الرمز المشّفر (admin code) واضغط على وظائف الطلب (request functions). يمكن الاطلاع على هذا عن طريق الوصول الى القائمة (menu) > الضبط (settings) > الأمن (security).

عند اختيار الرموز **لا** تختر رموزا مع نفس الرقم، أو مجموعات سهلة مثل 1111أو 1122. إن الرمز المشفر يأتي جاهزا كـ 123456، ويجب أن يكون هذا الرمزمن 6أرقام .إذا أخطأت بطباعة الرمز الخاص بك يمكنك إعادة المحاولة لعدد غير محدود من المرات.

إن مفتاح الـ SIM هو تلقائيا 8888، هذا الرمز يجب أن يكون بين 4 و 8 أرقام. المفتاح الثاني للـSIM هو 9999، هذا الرمز يجب أن يكون بين 4 و 8أرقام .وإذا تم إدخال رموز الـSIM بشكل غير صحيح ثلاث مرات، فذلك سيقفل الـ SIM الخاصة بك ولا يمكنك فتحها إلا من خلال الحصول على رمز PUK.

7.2 اضافة المال لرصيد الهاتف عن بعد

للقيام باضافة المال الى رصيد الـiSatphonePro الخاص بك عليك أن تشتري أولا قيسمة الائتمان الخاصة بالهاتف. يمكنك القيام بذلك عبر عدد من المواقع الألكترونية مثل
http://satphonecity.com

للتحقق من رصيد هاتفك، قم بإجراء مكالمة مع هذا الرمز: *106#
لإضافة رصيد الى الهاتف من قسيمة، قم بإدخال الرمز التالي: *101* رقم القيسمة#
على سبيل المثال: *101* 123456789#

7.3 مسح سجل المكالمات

سوف يقوم هاتفك تلقائيا بالاحتفاظ بسجل أرقام جميع الذين قمت بالاتصال بهم. تأكد من حذف هذا السجل كل مرة تقوم باجراء مكالمة هاتفية. فان أي رقم تتركه في السجل فسيكون صاحبه معرضا للخطر إذا ما تم

مصادرة الهاتف. قد يكون مشبوها أن سجل مكالماتك الخاص فارغ ولكن ذلك سيكون له تأثير أقل على زملائك.

إحذف سجل المكالمات عن طريق الوصول الى القائمة > سجل المكالمات > الخيارات > **مسح الجميع**.

7.4 حذف ملف المرسلات

سوف يقوم هاتفك بالمحافظة على **قائمة الرسائل القصيرة ورسائل البريد الألكتروني** المرسلة من الهاتف وذلك بطريقة مشابهة **لسجل المكالمات**. تأكد من حذف هذه السجلات كلما أرسلت رسالة.

إحذف **الرسائل القصيرة والاميلات** عبر الوصول الى القائمة> الرسائل > المرسلات> خيارات > **حذف جميع الرسائل.**

7.5 حذف دليل الهاتف

دليل هاتفك سيوفر للسلطات قائمة مرجعية بأرقام هواتف زملائك. كما سيعرض أي رقم في دليل الهاتف للخطر اذا ما تم مصادرة الهاتف. قد يكون مثيرا للشبهة أن يكون دليل الهاتف فارغا، ولكن سيكون لها تأثير أقل على زملائك.

قم بحذف دليل الهاتف عن طريق الوصول الى القائمة > الأسماء> **دليل الهاتف> امسح الكل**

كما يمكنك حذف أي أسم مخزّن على الـ simcard عن طريق الوصول الى القائمة > الأسماء > أسماء الـ SIM

7.6 إستخدام سماعة بلوتوث للحد من الاشتباه

لا تترك الهاتف في العراء. إبقه مخبئا في كل الأوقات وفكّر جديا في تمويه الهاتف.

عندما تستخدم الهاتف للمكالمات، أستخدمة مع سماعة اذا كان ذلك ممكنا. سوف يظهر أنك تستخدم شبكة الاتصال المحلية الخلوية وليس أنك تجري مكالمة عبر الأقمار الصناعية. ضع الهاتف في مكان بزاوية جيدة متجهة نحو القمر الصناعي ولكن قم باخفاء موقع الهاتف. إن إستعمال سماعات بلوتوث يجعل من اخفاء الهاتف أمرا اسهل ولكن قد يؤدي الى مخاطر أخرى مذكورة أدناه.

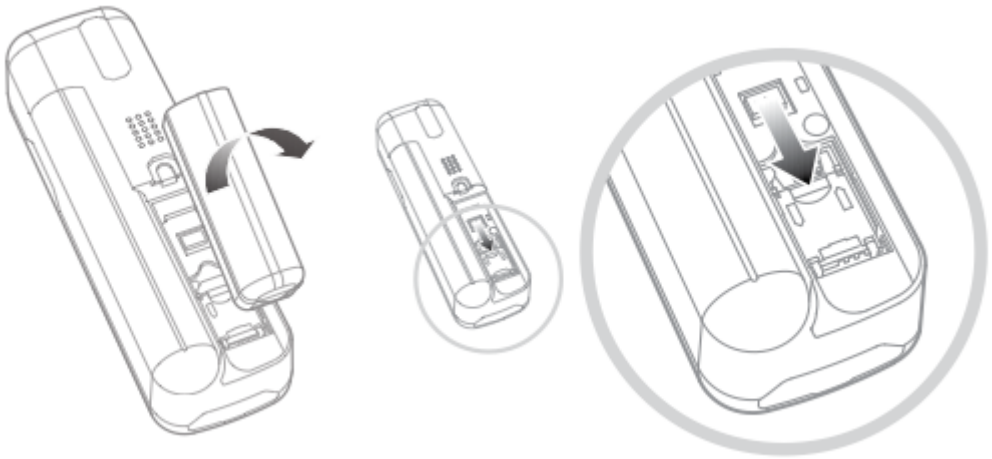
فعّل قدرة بلوتوث عن طريق الوصول الى القائمة > الضبط > بلوتوث > الأجهزة الموثوقة (paired devices) > خيارات > البحث عن أجهزة

ملاحظة: عندما تضع إشارة البلوتوث في وضعية "مكشوفة" سوف تكون واضحة لأجهزة الكشف عن بث البلوتوث على مسافة 10 أمتار. دائما ابق البلوتوث في وضعية "غير مكتشف". لا تقم بربط الساتفون الخاص بك بأي جهاز بلوتوث غير معروف. دائما استخدم سماعات الرأس مع زر " إضغط نحو التزامن" (push-to-sync). إن إشارة البلوتوث تتبدّل عشوائيا 1600 مرة في الثانية الواحدة، بين الترددات الاذاعية 79، مما يجعل من الصعب جدا إعتراض الأرسال.

ملاحظة أمنية: هناك معدات في الأسواق من شأنها تمكين أي شخص لرصد وتسجيل وفك تشفير البلوتوث في الوقت الحقيقي. إنّ احتمال حصول السلطات على هذه المعدات غير معروف ولكنه غير مستحيل. إذا لم تكن مراقبا حاليا سيكون من الصعب على السلطات مراقبتك على أساس بث بلوتوث الخاص وحده. إذا تمكنت السلطات من ايجاد موقعك، سيكون بامكانهم الحصول الى متلقي قادر على التقاط بث البلوتوث على بعد أكثر من كيلومتر.

7.7 قم بتعطيل الهاتف والحفاظ على simcard الخاصة بك آمنة

لن يقوم الساتفون بالاتصال بالشبكة ولن ينقل موقع GPS أو إشارات أخرى عندما لا يتم نشر الهوائي. قم بإزالة الـ SIMCARD وابقها معك وهذا سيجعل من السهل تدميرها في حالة تمت مصادرة الهاتف. أغلق الهوائي دوما وذلك لتعطيل الهاتف عندما لا يكون قيد الإستعمال.



في حالة iSatphonePro عملة معدنية كبيرة تعمل بشكل جيد.