TELECOMIX INTERNATIONAL – SYRIAN OPERATIONS
Internet Activists for Freedom - ناشطون من أجل الحرية

SAFETY GUIDELINES FOR INTERNET COMMUNICATIONS
إجراءات السلامة للتواصل عبر الإنترنت

- for immediate distribution -
- للنشر الفوري -

Dear people of Syria,

This message comes from Internet activists of Telecomix as well as from the Emergency Communication Division. We are excited and impressed by your willing to obtain democracy and freedom, but also outraged that this fight costs so many human lives. Freedom of expression is a fundamental right but is severely repressed by your government.

As we defend freedom on the Internet, we can provide means of evading from censorship and surveillance. The following guidelines can help in avoiding detection while communicating. Please read them carefully as your life may be at stake.

OPERATIONAL SECURITY GUIDELINES

1. Assume that all your traffic can be intercepted, including all Internet connections, e-mails and phone calls (either landlines or mobile phone). In particular, your nicknames, logins, passwords, the websites you visit can be seen. Switch off and remove the battery from your mobile phone to avoid being tracked.

2. On the Internet, do not disclose any information that may lead back to your real identity. Always use nicknames. Create several fake accounts on social media (Facebook, Twitter) and several fake e-mail addresses. Change your passwords often.

3. Do not log onto old accounts that have been once clearly linked to your real identity. Create distinct, anonymous accounts to perform protest activities.

4. Protect your Web browsing using SSL encryption. URLs must be prefixed by https:// instead of http:// . Connections not using SSL will be intercepted with no effort. Connections using SSL can also be spyed on, read carefully our guide at https://werebuild.telecomix.org/wiki/SSL to prevent yourself from this. Major sites such as Google, Facebook and Twitter provide SSL access. Avoid those that don't.

5. SSL alone does not prevent authorities from seeing what are the websites you are visiting. Use Tor to scramble the path between your computer and the website you visit : https://torproject.org .

6. Internet cafés are the worst places to be. Computers are full of governmental spying software. Do not go there unless you want the authorities to see your communications.

LET THE WORLD KNOW

Youtube has been reported to be censored. We can help you publish videos, sounds, texts and leaked documents while keeping your identity protected. We have knowledge for establishing alternative means of communications using radio or dialup modems.

Contact us directly on the Syria dedicated channel on the Telecomix Internet Relay Chat network by following this link : https://new.punkbob.com/chat/ .

Good luck.

TELECOMIX INTERNATIONAL – SYRIAN OPERATIONS
Internet Activists for Freedom - ناشطون من أجل الحرية

SAFETY GUIDELINES FOR INTERNET COMMUNICATIONS
إجراءات السلامة للتواصل عبر الإنترنت
- for immediate distribution -
- للنشر الفوري -

،أعزائي شعب سوريا

هذه الرسالة تأتي من ناشطي تيليكوميكس للانترنيت كما أنها تأتي من شعبة الاتصالات الطارئة. نحن متحمسون و معجبون بإرادتكم للحصول على الديمقراطية و الحرية، لكننا أيضا مستاؤون لأن هذه المعركة تكلف الكثير من الأرواح البشرية. حرية التعبير حق جوهري لكنه مقموع بشدة بوساطة حكومتكم.

بما أننا ندافع عن الحرية على الانترنيت، نستطيع توفير طرق للتهرب من الرقابة.
الدليل التالي يستطيع المساعدة لتجنب الكشف بينما تتواصلون. من فضلكم، اقرؤوه بعناية لأن حياتكم ممكن أن تكون على المحك.

الدليل الأمني الفعال:

1. افترض أن جميع تحركاتك يمكن اعتراضها، بما في ذلك جميع خطوط الانترنيت، البريد الالكتروني (الإيميل) و الإتصالات الهاتفية (سواءا الخطوط الأرضية أو الخليوية). على وجه الخصوص، أسمائكم المستعارة، عمليات تسجيل الدخول، كلمات المرور و الصفحات التي تزورها يمكن أن ترى. أطفئ جهازك الخليوي و أزل البطارية من هاتفك الخليوي لتجنب تعقبك

2. على الانترنيت، لا تكشف أي معلومة تقود إلى هويتك الحقيقية. دائما استخدم أسماءا مستعارة. أنشئ العديد من الحسابات الوهمية على وسائل الإعلام الاجتماعية (فايسبوك و تويتر) و العديد من الايميلات الوهمية. غير كلمات سرك بشكل متكرر

3. لا تدخل إلى حسابات قديمة و التي و لمرة واحدة تم ربطها بهويتك الحقيقية. أنشئ حسابات مختلفة و مجهولة لتمارس أنشطة الاحتجاجات

4. احم تصفحك للانترنيت باستخدام تشفير SSL. عناوين المواقع يجب أن تكون مسبوقة ب https:// بدلا من http://
الروابط التي لا تستخدم SSL يمكن أن تعترض من دون أي مجهود.
أيضا، إن الروايط التي تستخدم SSL يمكن أن يتم التجسس عليها، اقرأ بعناية دليلنا هنا
لتمنع نفسك من هذا. الصفحات الكبرى مثل جوجل، فايسبوك و تويتر
توفر دخول يستخدم SSL. تجنب الصفحات التي لا توفر هذه التقنية.https://werebuild.telecomix.org/wiki/SSL

5. تقنية SSL لوحدها لا تمنع السلطات من رؤية الصفحات التي تزورها. استخدم Tor لتشويش الطريق بين حاسوبك و الصفحات التي تزورها : https://torproject.org .

6. مقاهي الانترنيت هي أسوأ مكان للتواجد فيه. الحواسيب مليئة ببرامج تجسس حكومية. لا تذهب إلى هنالك إلا إذا أردت للسلطات أن ترى اتصالاتك

دع العالم يعلم
يوتوب أبلغ أنه مراقب. نستطيع مساعدتكم بنشر الفيديوهات، الأصوات، النصوص و الوثائق المسربة بينما تبقون هويتكم محمية. لدينا المعرفة لتأسيس وسائل اتصالات بديلة باستخدام الراديو أو أجهزة المودم الهاتفي

اتصل بنا مباشرة على القناة المخصصة لسوريا للدردشة المتتابعة على الانترنيت و التابعة لتيليكوميكس باتباعك لهذا الرابط
https://new.punkbob.com/chat/

حظا موفقا