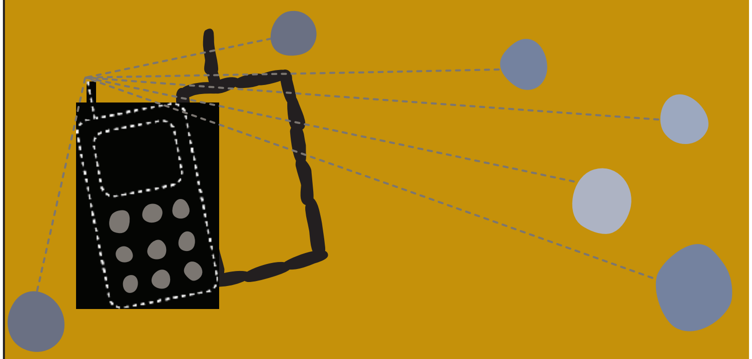
Online & mobile security & privacy



NEW TECHNOLOGIES, SUCH AS MOBILE PHONES AND THE INTERNET, ARE POWERFUL TOOLS FOR ADVOCACY BUT USING THEM TO COMMUNICATE SENSITIVE INFORMATION CAN CREATE RISKS FOR YOU, YOUR CONTACTS, FRIENDS AND COLLEAGUES. THIS CARD WILL HELP YOU ACCESS INFORMATION SECURELY AND PROTECT YOUR DATA WHEN USING MOBILES PHONES AND THE INTERNET.

WHAT IS DIGITAL SECURITY AND PRIVACY?

Signs that information rights and digital security has been comprised might include:

- Passwords that change mysteriously
- Private messages that appear to have been read by someone other than the intended recipient
- Websites that have become inaccessible from certain countries
- Officials revealing knowledge about private correspondence, including dates, names or topics discussed
- Mobile phone conversations that individuals believe have been monitored

DO I NEED TO BE CONCERNED ABOUT THIS?

If such scenarios would compromise your projects or expose you or your contacts to persecution, then you should be concerned. The knowledge and software needed to carry out such attacks on your digital privacy are often available on the internet. If the attacker has sufficient access to internet or mobile phone infrastructure in your country, the technology required is quite simple. Government agencies, Internet Service Providers (ISPs) and mobile phone companies have privileged access to this infrastructure, but office mates, neighbours and internet café operators may also have some access.

WHAT SECURITY ISSUES ARE COVERED ON THIS CARD?

Web-based tools and mobile phones are emphasised on this card. However, there are many other technologies that may also leave you vulnerable to censorship, surveillance, and persecution. Although they are not discussed here, regularly updating your computer's operating system, reliable anti-malware software, and consistent back-up procedures are the most important basic precautions. If you have reason to believe that your computers or data-storage devices, including your back-ups, are at risk of being lost, stolen or confiscated, or that your organisation may be subject to targeted internet surveillance (or if this is commonplace in the regions where you operate), then you should refer to Tactical Tech's Security in-a-Box toolkit.

Web-based advocacy tools

When using public web-based tools, such as Blogger, Facebook, and Twitter for mobilisation or coordination, remember that the information you store on such platforms becomes, to some extent, the property of the operators, and that many of these tools expose more information than you might think.

When you entrust a sensitive project to operators of any online tool, read their privacy policies or user agreements. Remember that even the most enlightened policy leaves your information under the direct control of the platform's administrators, who would be able to divulge, sell or misplace that information without your permission or knowledge. Even if you terminate your account, many of these sites do not actually delete the content you have posted or the personal information you have provided. Finally, unless it is important that you use a particular commercial service, either because of its accessibility or because doing so helps you blend in with lower-profile users, consider some of the rights-progressive alternatives: Blip.tv instead of YouTube; riseup.net rather than Gmail. If you have the technical resources, you can run your own web-based services.

If you use commercial platforms, take precautions to protect yourself from malicious individuals who know how to dig up private information on such services. This is particularly true of social network site platforms such as Facebook and MySpace. Develop a thorough understanding of the privacy features that are built into these platforms, and think about the kinds of information that you might unintentionally reveal about yourself or your organisation; for example, your real name, where you live, the places to which you travel and details about upcoming events or meetings. If monitored over a long time, such information can also provide a picture of your habits and working practices.

One helpful technique is to create multiple accounts on any web-based service that you use, allowing you to use different accounts or profiles for different projects, and to maintain test accounts that you can use to 'spy' on yourself. Your privacy is better protected if you you are able to check, in different ways, what is revealed about your account; for example, through web searches or people who hold special access privileges.

PASSWORDS

Most web-based resources depend on a single password to protect your account. If a malicious individual or organisation learns this password, it doesn't matter whether you trust the site administrators, or how carefully you have tested your privacy: you will immediately lose your confidentiality and anonymity.

Less well-known ways of cracking a password: someone could install malware on a computer that you use to log in to a secure website. Or, someone could monitor your internet connection while you log in to an insecure website.

To protect against the first kind of attack, use your own computer or a computer that is maintained by someone you trust, and ensure that its operating system and anti-malware software are up-to-date. To protect against the second kind of attack, most popular web-based email, social networking, blogging, mapping, and video platforms offer secure connections, called HTTPS. You can check whether you have a secure connection to a webpage by looking for 'https://' (rather than just 'http://') at the beginning of your browser's address bar. Many web-based tools, however, do not use HTTPS to protect any information, other than your password, that you submit to, or access from, their websites. As a result, if someone monitors your connection for long enough, they will learn what you have stored on that site. Your best defence against this is to look for web-based tools that use HTTPS for all pages.

BYPASSING CENSORSHIP

You can use secure web-based proxies, censorship circumvention tools or anonymity software such as Tor to hide your identity from the websites you visit or to bypass Internet filters. These tools are useful when you need to access websites that are blocked; for example for research, or in order to submit updates to web-based platforms such as Facebook.

BEING ANONYMOUS ONLINE

Anonymity software such as Tor is useful when you do not want to reveal what websites you have visited. Tor bounces your connection between several random volunteer computers in order to prevent even your ISP or government-level observers from knowing what you are doing on the internet. However, do not use Tor when sending or receiving sensitive information to or from insecure websites. Unless you are connected to a website that supports HTTPS, it is possible for one of the volunteer computers to monitor the content as it loads. Tor is quite secure, but for the time being it slows down your internet connection.

Mobile phones

Mobile phones are used by advocates all over the world, but they often store a great deal of information that should be kept private. In addition to contact lists, a mobile phone may contain call histories, calendars, text messages and emails.

Think about the information stored in your phone, particularly because phones are so easily confiscated. For example, you probably do not need to keep all of your contacts in your mobile if you are doing sensitive rights-focussed work, and you should delete information from your phone and SIM card whenever you can. When organising events or mobilising networks it is a good idea to use anonymous, pre-paid SIM cards and to change handsets occasionally. Because SMS can easily be searched and filtered, you should avoid sensitive keywords when sending text messages.

As long as they are turned on, mobile phones can be used to track your location. People attending a sensitive gathering should turn off their phones and remove their batteries before setting out, and wait until they have returned before reinserting their batteries and turning their phones back on. Mobile phone providers have access to details about all calls: to whom, when and where they were made. Providers may have a legal obligation to record or release these details if asked to do so by officials, and may keep such records for several years.

ACTIVITY: IDENTIFYING YOUR SECURITY RISKS

Use the questions below to assess your security risks and help you decide what tools you can use to mitigate them.

1. **I am dealing with sensitive information.** It is important to know whether you are dealing with sensitive information that may lead others to want to watch what you are doing. Are you involved in activities that might be considered sensitive or disruptive by the government, police, army or a private company? If you are, you might be putting yourself or others at risk unless you implement some security measures.
2. **I work with people whose identities and details must be kept private.** Perhaps you are collecting private information from people you support, such as information about domestic violence, forced labour or rape. If people provide you with information that could put them at risk, you must take steps to make sure it is kept private.
3. **I sometimes communicate with people online who deal with sensitive information.** Even if you feel you have no security risks, if you are communicating online with people who do run these risks you can be targeted by people who oppose what they are doing. This is because people can use you to access the private information of others.
4. **I view or post content to websites that might be considered sensitive.** Perhaps you contribute information to human rights websites, or post articles opposing groups you believe are not respecting human rights. Merely visiting sensitive sites on the internet can make you a target.

Internet security & privacy resources

To learn more and download security tools:

1. **Security in-a-box** was created by Tactical Tech and Front Line to meet the digital security and privacy needs of advocates and human rights defenders. http://security.ngoinabox.org/
2. **Digital Security and Privacy for Human Rights Defenders** by Front Line provides useful information about assessing and addressing digital threats. http://bit.ly/1aCkSs (frontlinedefenders.org)
3. **Mobiles in-a-box** by Tactical Tech features an entire section on mobile phone privacy and security. http://mobiles.tacticaltech.org/security
4. **Anonymous Blogging with Wordpress & Tor.** Global Voices created this guide to support rights advocates who want to reveal the truth and express themselves online but who may put themselves at risk by doing so. http://advocacy.globalvoicesonline.org/projects/guide/
5. **Be anonymous online and circumvent censorship.** Tor is designed to increase the anonymity of your activities on the internet and it can also be used to bypass internet filtering. You can download it on to your computer or run it from a USB stick. http://www.torproject.org/