webmail providers give you information to configure your email client.

- If you do not need synchronisation between devices, prefers the POP3 protocols and delete mails form the server.
- If you have to use a webmail, always check that **https is enabled**, or your password could be intercepted.
- As for web browsing, check to what links and pictures points you in your mail client. Do not allow loading of remote pictures in email. Disable HTML formatting because it can be used to deliver a trojan in your computer.
- You should not trust attached document to mail or links, especially when coming from an unknown person.

Instantaneous Messaging and Phone Over Internet

- You should not use Skype. It can't be trusted and since it allows you to share documents and control in real time if they are received. Still, Skype's usage cannot be considered as safe, especially in text-mode. Also Microsoft (Skype's owner) have a history of collaborating with states. **Do not use Skype.**
- **Avoid using voice communication**, if there's a microphone in your office while you're speaking, no encryption will prevents your communication to be intercepted.
- You can use Jabber (**XMPP protocol**) to communicate with other people. It's a free(dom) standard, and a lot of client implemet them. Since it's mostly based on text, you can further encrypt the communication. We recommend **Pidgin** or **Adium** for XMPP communictaion, along with **OTR** for encryption. XMPP allow for easy creation of account on numrous servers.
- XMPP can manage voice and video support if your hardware and client supports it.
- For pure voice solution, we recommends the **use of SIP and ZRTP** protocols, such as **ostel.co.** They can work with free clients both on Android and iOS. Also, jit.si is a good multiplatform client for desktop computers.
- You can also use WebRTC based solutions, which works from inside your browser and provides transport encryption. For instance http://hibuddy.monkeypatch.me/ provides such a service.

Connection

- When using Wi-Fi, prefer WPA2 encryption (with a good key) to WEP (crackable in 5 minutes) or WPA (crackable in a few hours).
- When using a network, keep in mind that anyone who can acess to it can intercept all your communications.
- The network operator can logs and track all your data. They can even disable some security in SSL. The same goes for national operators. We recommand you to use another layer of encryption and anonymisation such as Tor.
- In open spaces (McDonalds, Starbucks, cafe), do as if anyone could read everything on the network. Hence, use HTTPS everytime you can and combines it with Tor. Be warry of shoulder surfing, so try to have a wall in your back, not a window or a space where people can be.

REMINDER

Computer security is never insured by a single software, but is the result of everyday behaviour. It is never total nor guaranteed.

Further more

http://www.superpeif.com
https://securityinabox.org
https://www.tacticaltech.org/digital-security-tools-and-tactics-environmental-rights-defenders-sub-saharan-africa
https://www.tacticaltech.org/digital-security-tools-and-tactics-lgbt-community-sub-saharan-africa

Acknowledgements

http://piratepad.net
http://www.pp-international.net
https://www.tacticaltech.org
https://www.eff.org
http://www.framasoft.net

This document was produced with support from the Swedish International Development Cooperation (SIDA).
The contents of this document are the sole responsibility of the FIDH, and can in no way be taken as reflecting the position SIDA.

fidh

COMPUTER SECURITY BASIS

Here are a few pieces of advice to ensure a minimal security while using computers

OCTOBER 2014

Keep in mind that security is a chain of components whose overall solidity equals the one of the weakest link.

A shielded door mounted on a wooden frame won't protect you more than a wooden door.

COMPUTER SECURITY BASIS

Use of the workstation

- Avoid uses of public computers, for instance in cybercafe. It can't be considered safe.
- If you have no choices but to use a public computer, try using a Live CD or a LIve USB Key OS, such as **Tails**, to avoid storing data on the computer.
- If you have to share a computer with several people, never accept to remember a password. Try to check what applications are running and if there's security software (antivirus, firewall and the like). Also, check for software running in the background and stop them if they're not needed. Software like Skype can give access to your Desktop to anyone connected.
- Always apply updates and upgrades of all software. In particular software like Java, Adobe Flash, PDF Readers and web browsers are prone to security flaw and exploitations. Even if it's not your computer, **install updates** if you can.
- Be suspicious of USB gadgets connected on a computer. Even an e-cigs charger can be used as a malware delivery devices. **Don't hesitate to unplug all of them.** Same goes for USB keys.
- Never store critical data on a computer. Use USB key and external hard drive which you'll have previously encrypted (using TrueCrypt or **LUKS** for instance). Do not forget to remove any temporary, downloaded and other files before logging out.
- If possible, use a different computer for critical work than for your daily life. Also, a computer can silently read and write your USB keys, so use a separate key for file transfers and for critical storage. And if you can, lock them in read-only mode. **Scan your devices** with antivirus software when you plug them back on your computers, and desactivate autorun. Separation of information is the key to security.
- If a person has physical access to your machine, he might gain access to all your passwords and data. **Never let any confidential data on a public computer.** Never leave a computer – especially laptops – unattended, an attacker might tamper with them.
- **Avoid using wireless peripherals** (bluetooth, mouse/keyboard): anyone close enough can intercept communications. Shut down bluetooth on your devices or – at least – put them in invisible mode. In the bluetooth case and if really necessary, change the password (often 0000 by default), never associate any unknown device and reject any demand you did not initiated.

Operating System

- Any operating system (Linux, Windows or MAC OS), as well as any software (MS or Open Office, Firefox, ThunderBird, Adobe Reader...), must be **updated frequently** using official tools and updates. Windows XP in not supported and won't receive any more update. It should be replaced by – ideally – Ubuntu.
- The **Linux** based operating systems are safer by default (better user privileges management) than Windows and are not vulnerable to Windows viruses (widely spread). It is recommanded to use them. And since they are free(dom) software, they allow for a much better control over your data.
- Every computer must have at least 2 user accounts on it: a standard account, with limited privileges for everyday use and an "administrator" account allowing installing and removing programs. **Each different user should have it's own accounts.** If possible activate encryption of personal folders. It narrows down the risks in case of a virus infection.

Software

- Ilegally acquired softwares ("cracked" or "pirated") are sometimes infected by viruses, trojans or cannot be updated... They must be avoid, especially when not used with an up to date and efficient antivirus !
- Free softwares such as **Firefox** (Web browser), **Libre Office** (Office Suite), **ThunderBird** (Mail client) and others have a community of users and developpers very consequent and efficient, security breaches are therefore corrected a lot faster. We recommend them.
- For Internet browsing, Internet Explorer (especially the old versions) is strongly inadvisable: you should rather choose software such as **Mozilla Firefox**, **Chromium**...
- **An antivirus must be used and kept updated** (idealy once a day). A regular antivirus scan (ex: every week) is necessary. Some good free antivirus software are distributed (Avast, Antivir, AVG). Even linux can use one (ClamAV) and, if it's not necessary for you, it will protect your contacts.
- Double check the legitimity of the website you download your antvirus from. A lot of fake sites give viruses as antivurses. One good way to do that is to check the adressbar in your browser. Legitimate antivirus website have a green/certified https certificate.
- A firewall can be installed and configured if the one provided with your system doesn't fit your requirements. As a rule of thumb, you'll probably never need incoming connections.
- **Don't install unnecessary programs.** The more there are, the harder it gets to keep them updated and to maintain security. Do not duplicate tools if not needed. If a software doesn't suit your needs, simply remove it. Yahoo and other "smart" bars are collecting a lot of data about your activity. Also avoid gadgets and third party applications on Facebook, Google+, Twitter and such...
- Do not use too many security softwares. An antivirus will consider another one as a virus and the two will block each other. Stacking firewalls (ex: add a firewall to Windows without disabling the original one) won't add any security.

Web browsing

- Everytime possible, use https instead of **http** (HTTPS Everywhere addon for instance) which allows to encrypt communication from your computer to the websites and therefore to protect data sent or received. The Firefox addon is available here: https://www.eff.org/https-everywhere
- When downloading any software, **make sure you are on a legitimate website**. Most of the website proposing paying software (such as Adobe Suite, MS Office, Windows itself) at low prices are distributing viruses.
- When in doubt, abstain. If something feels wrong, it probably is. If you need to check if a mail or a website is legitimate, ask to http://www.hoaxbuster.com for instance.
- Never click a link if you don't know where you'll arrive. Often, when hovering the link, you will get the url it is pointing to in the status bar of your browser.
- Never type a password or login data (especially banking data) if the website is not secure (padlock on the down right corner of your browser and url starting by https://).

Passwords

- You must change your passwords on a regular basis, at least once per year.
- Do not use the same password for several accounts an / or email addresses: in case it's discovered, an attacker will use it to access other accounts
- A trustworthy password must contain at least 12 characters, at least 2 of each following sets: lower case, uppercase, numbers, special characters (,;:&@ etc). **You should prefer a passphrase**, a succession of three or more words. Those longer passphrase don't need special charcaters, but it's still a plus. For instance "OnceUpponATime@" can be a good one (do not use that)
- Avoid using password based on the user (name, hometown, firstname, birthday of the children, etc.): those passwords are easier to find, especially if you use a lot of social network tools.
- A password is necessery at the boot of the computer but not enough. It will just discourage curious but impatient eyes. Removing the battery from the motherboard usually reset the BIOS hence the password.
- You can also **set up a password for the screensaver,** securing a little the computer when away. You should have a password for your user session, and disable autologin without password at boot.
- You must **lock the current session** when leaving the workstation, even for a few minutes. Anyone willing to use the computer will therefore have to log in. It can usually be done by pressing [Windows/Apple key] + L or with [Ctrl] + [Alt] + L on Ubuntu.
- Most Internet browsers allow you to save your passwords. If you do so, also **define a master password** so that you can be the only one allowed to access the stored passwords. If you're not on your computer, do not save any password.
- Never trust the "secret question" system to retrieve your password. Answers can easily be found on your different profiles on the Internet (Facebook, Twitter, LinkedIn accounts, etc.)

Emails

- Never answer to an email asking for a login, password, bank data or one which looks like an official or government one. They are scam who tries to gain access to your data.
- **Avoid the use of webmail.** All your mail will be kept on a remote server and foreign agencies can have legitimate access to all your mails, and it's hard to use encryption with them. Use a local mail client (**Thunderbird**). Most