UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

OHCHR digital security tips series for human rights defenders in South-East Asia

7 Online safety and security

In certain circumstances, information about your whereabouts (location and IP (Internet Protocol) address), the devices used, the websites visited (even those websites with HTTPS), online services purchased, the use of encrypted apps and services are tracked and recorded by Internet service providers. The routes of travel of HRDs and teams may be considered sensitive information and should be protected. Remember, Internet service providers (ISPs) and gateways can also glean some information (but NOT the content) when you use end-to-end encrypted apps such as Signal, Wire, Threema, or encrypted email (e.g., the recipient of a voice call, that a message was sent to a group, or that an attachment was sent). ISPs also know when you use an encrypted communications app. For maximum protection, connect via a VPN.

DO

It is recommended to use anonymity tools when connecting online. To protect your identity and personal information against Internet providers, hotel Wi-Fi administrators, or even state-actors, enable Tor or a VPN when connecting online.

It is recommended to always check if the website you visit is legitimate and is using HTTPs. Some beginners' tips for checking website legitimacy:

- Avoid following short links (such as bit.ly,) and use a URL expander like unshorten.it to check where the short link intends to take you. Always read the URL carefully and make sure it does not include any typos or mistakes. Error messages may indicate that someone is attempting to set up a fake website. If you are unsure, type the URL yourself to avoid being tricked using Punycode.

  Example: Let's say you receive a link to install something from Microsoft. The original URL would look like this: www.microsoft.com

  However, the domain includes an 'o' from the Russian alphabet instead of an 'o' from the latin alphabet. The URL would, therefore, look like this:

  www.microsoft.com
  [can you see the difference?]

  However, when you paste the above URL into Firefox with Punycode enabled, it will show up like this:

  http://www.xn--micrsft-djgb.com/

It is recommended to protect yourself against web-trackers and ads. Here are some suggested browser extensions to prevent tracking:

Privacy badger: blocks third-party ads and trackers to identify your location, and other demographic information.

HTTPS Everywhere: ensures that information between user and website is exchanged only using the HTTPS protocol if the website allows that facility.

uBlock Origin: is a wide spectrum content blocker that is CPD and memory efficient.

- Facebook Container: makes it harder for Facebook to track you by isolating your identity into a separate content tab.
- Cookie Autodelete: automatically deletes cookies that are not in the WhiteList.

It is recommended to protect your browser against malicious codes/plugins. Attackers may use malicious codes and embed them on vulnerable websites. Though a website may be legitimate, it can still be vulnerable to attacks through embedded malicious codes or scripts. By using a browser extention/plug-in like NoScript,[1] potentially unsafe content can be executed only by websites you trust.

It is recommended to use alternative browsers with built-in privacy features such as Brave and Epic, which contain built-in Tor, proxy and pre-installed privacy plugins to help you browse more securely. However, it is also possible to improve the security levels of popular browsers such as Mozilla Firefox and Google Chrome by tweaking their privacy and security settings.[2, 3]

It is recommended to use alternative search engines such as duckduckgo.com (instead of Google search). Search engines sometimes record and track your browsing habits. By using alternative and privacy focused search engines, this eliminates the chance of your information being sent to advertisers. You may also consider adding startpage.com and Qwant.com

It is recommended to download applications only from the developers/company websites, and not through alternative repositories.

DON'T

It is not recommended to connect to unknown/untrusted public networks and Wi-Fi as they may be managed by someone who has access to data passing through the network. They can see where you are going and what you are doing.

It is not recommended to log in through untrusted devices such as free computers at the airport as you do not know what software is installed on them. They can have physical, or software based key loggers that monitor every keystroke you make – including your passwords.

It is not recommended to click on any link from an unknown sender. Do not download any software from unknown senders besides legitimate sources such as Apple Store or Play store or the developers' website.

It is not recommended to visit any websites with errors such as "Your connection is not private." This error means that there is something wrong with the website's certificate.

It is not recommended to download pirated or cracked version of software. Cracked software is often modified and reconfigured to by-pass security checks and is considered high risk. Never use cracked software versions as it may contain other configurations that either track your activities or steal your credentials.

TIPS!

Suggested tools:

Psiphon,[4] ProtonVPN,[5] TunnelBear,[6] Mullvad,[7] NordVPN[8] and Tor.[9]

Note: References to external entities and websites are only indicative and should not be considered an OHCHR's endorsement to such entities and websites and the services provided by them. These references are provided, without warranty of any kind, either express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose and non-infringement. Under no circumstances shall OHCHR be liable for any loss, damage, liability or expense incurred or suffered that is claimed to have resulted from the use of these websites. The use of these websites is at the user's sole risk. The external websites are not under the control of OHCHR, and OHCHR is not responsible for their content or any link contained in these sites.

[1] https://noscript.net
[2] https://support.mozilla.org/en-US/products/firefox/privacy-and-security
[3] https://support.google.com/chrome/answer/10468685?hl=en&co=GENIE.Platform%3DDesktop
[4] https://psiphon.ca/
[5] https://protonvpn.com/
[6] https://www.tunnelbear.com
[7] https://mullvad.net/en/
[8] https://nordvpn.com/
[9] https://www.torproject.org/