UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

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

2 Protecting information “in transit” (securing online communications)

The term “in traffic” refers to information that is communicated from one device to another via the Internet infrastructure. While in traffic, information is vulnerable to so-called man-in-the-middle attacks, meaning that it can be intercepted at certain points on its route (e.g., router, Internet service provider (ISP) servers, gateways). “In traffic” information’s security depends on multiple levels, including account security of each person communicating, physical safety of each device involved, and the spaces where communication is happening. To protect information “in traffic”:

DO

EMAIL: It is suggested to use end-to-end encrypted email[1] for communicating sensitive information (e.g., Protonmail,[2] TutaNota[3]). Please note that emails are encrypted by default only when sent between ProtonMail or TutaNota users. As soon as you send an email from ProtonMail to some other provider, the content is sent unencrypted. Regular email is not end-to-end encrypted[4] and is not secure. Please see #1 for a definition of sensitive information. End-to-end encryption is the most secure way to communicate privately and securely online. By encrypting messages at both ends of a conversation, end-to-end encryption prevents anyone in the middle from reading private communications.[5]

CHAT: It is suggested to use an encrypted chat application such as Signal, Wire or Threema, or encrypted email. Using applications that are not end-to-end encrypted allows the storing of your messages and their history on the application’s servers. These unencrypted messages in transit can be at risk of lawful interception and review by security services, as well as subject to data retention regulations in some countries enabling data extraction later. With end-to-end encryption, all data passed from the source to its destination are encrypted. No matter what chat application you use, make sure to review and tweak its privacy and security settings accordingly before using it.

INTERNET: It is suggested to use tools such as virtual private network (VPN) and/or Tor anonymity tool.[6] Internet service providers, and network telecommunications companies, may have access to your online activities since they manage the infrastructure that your traffic is going through. Using a VPN allows you to hide your data from your ISP by encrypting the data going to your VPN server. Make sure your VPN uses end-to-end encryption and has servers in a country with strong data protection laws. While Tor (the onion router) allows you to protect your information by using an encrypted tunnel and connection as it passes through the Tor network helping your Internet traffic to remain anonymous.

WEBSITE: It is suggested to always verify that the uniform resource locator (URL)[7] of a website is correct and ensure it uses hypertext transfer protocol secure (HTTPS).[8] To check if the domain address is safe, consider using a URL checker such as Norton Safe Web[9] or VirusTotal.[10] Phishing attacks and malicious websites often mimic a real website’s domain, sometimes even using characters from other alphabets that look the same as in latin. Always check if the domain address is correct, trusted, safe, and if it is using HTTPS (secure connection), to make sure that all data sent to the website is encrypted. If you are using Firefox, you can enable the Punycode display in the address bar. That way you will be able to quickly identify spoofed URLs.

CONFERENCE CALLS: It is suggested to use trusted online conference applications for interviews and communicating sensitive information. A recommended in-browser conferencing solution called Jitsi Meet is a free and open source alternative to Zoom, Microsoft Teams, and Google hangout. When using this service, make sure to use trusted servers such as Greenhost[11] and Mayfirst.[12]

DON’T

NETWORK: It is not recommended to connect via untrusted networks (e.g., public Wi-Fi) **without using a VPN.** Malicious users can set up their own wireless network luring users to connect to it.

INTERNET: It is not recommended to send any sensitive information on websites that do not have HTTPS. Non-HTTPS websites transmit data in plain text, leaving your credentials and other information easily accessible. In addition, sent/received data can also be modified while in transit so the recipient might not receive the same content as you have sent it.

COMMUNICATIONS: It is not recommended to discuss sensitive topics or send sensitive information via short message service (SMS) or regular phone calls or any untrusted messaging services like Facebook Messenger or Instagram. SMS and regular phone calls via 3G networks are inherently susceptible to surveillance and are insecure; whereas corporations such as Facebook do not always allow independent audits of their security infrastructure and hence cannot be trusted with sensitive data (unlike Signal Private Messenger).

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] Encryption is the method by which information is converted into secret code that hides the information’s true meaning.
[2] https://proton.me
[3] https://tutanota.com
[4] End-to-end encryption is intended to prevent data being read or secretly modified, other than by the true sender and recipient(s).
[5] https://proton.me/blog/what-is-end-to-end-encryption
[6] https://www.torproject.org/
[7] A URL is the address of a given unique resource on the Web.
[8] HTTPS is a protocol that secures communication and data transfer between a user’s web browser and a website.
[9] https://safeweb.norton.com/
[10] https://virustotal.com
[11] https://meet.greenhost.net
[12] https://meet.mayfirst.org/