Digital security belongs to everyone

By Auli Starck, from Kepa, Finland, CIVICUS member organisation

GDPR messages, updates on Facebook security settings, and email phishing messages; as a result of digitalisation and the protection of one's own privacy is becoming even more important for NGOs.

But how does digital security relate to the status of civil society? At its best, it supports freedom of expression and safeguards civil society's rights to act. At its worst, the lack thereof is a security risk. However, digital security is also much more.

At the beginning of June, I participated in CIVICUS and Access Now's training on digital security and its linkage to the state of civil society. This was held in Armenia and attended by representatives of umbrella organizations and grassroots actors and activists from Europe and Asia, for whom the power of action, and even security, is threatened.

Personally, I was thinking about digital security during the training largely in terms of how much our Finnish organisations would be in favor of working towards avoiding putting our partners at risk. When operating in countries where access to the Internet is restricted, phonecalls are listened to, e-mails are monitored and communication censored, it is important to recognise and prevent the risks. You can start with these tips:

1) Basic things to do: Regular updating of equipment and software and virus protection are an absolute prerequisite for digital security.

2) Being aware of and preventing: Find out about the risks and how to avoid them, strenghten digital security by building a risk management system - and do not click links when you are unsure of their origin.

3) Use strong passwords: Identified, complex and sufficiently long passwords or even blocking systems will effectively prevent access to your information. Luckily, no password and their hint have to be learned by heart. Two-step authentication when signing up is also advisable.

4) Avoid or treat with caution open networks: open wireless networks in airports, hotels and cafes are convenient, but they are dangerous. VPN (Virtual Private Network) is one way to improve security. At the same time, it is good to be aware that in some countries the use of a VPN connection may be illegal.

5) Talk to your partners about digital security: Do you make partners aware of the information you want to share about them? Can information or images from a partner be published on a website or social media? Care should be taken when dealing with sensitive matters of privacy. There are good options for email, Facebook, text messages and Skype, such as Signal and Jitsi.

6) Access is available: Access Now specializes in helping civil society actors with digital security. Help is available 24/7, in nine different languages. Good practice tips are also provided by the Electronic Frontier Foundation.

And do not be discouraged in front of the information flood, but focus on the essentials. Complete security can mean at worst that you are afraid to do anything. Caution should not mean paranoia (although it was a bit difficult to avoid it during training), but the most important thing is to find a good enough level of security.