Best practices for digital security

Whether you're a human rights activist or not, digital security matters and cyber hygiene can reduce your exposure to attacks. Here are some simple tips to be safer online.

Back up your data

This is the best way to prevent the loss of your data if a device is lost, stolen, or crashes.

Encrypt your devices

If you lose physical control of your device, your data may be safer with full disk encryption. If encryption is illegal in your country, follow these alternatives.

Set up two-factor authentication for your accounts

Two-factor authentication (2FA) ensures that even if your password is compromised, your account will still be protected. Always prefer app-based 2FA rather than SMS-based 2FA: this allows you to access your accounts even if you do not have cellular service. Access a list of recommended password managers and 2FA tools.

Use a VPN

When you connect to a VPN, all data you send (such as requests to servers when browsing the web) appears to originate from the VPN, which masks your IP address and helps protect your privacy (since the IP address indicates your general location). Learn how to choose the best VPN service for you.

Browse safely

Using a safe browser, such as Tor, can help you protect your network traffic on untrusted networks, like at airports or hotels. Avoid using public Wi-Fi whenever possible. Make sure your browser and its plugins are updated. Make sure you block pop-ups, and use an ad blocker. Use your browser in "private browsing" mode or enable "do not track" in your browser.

Keep your devices up to date

A fully patched system is more difficult to compromise and has fewer known vulnerabilities.

Engage with ILGA World on social media safely

These are ILGA World's official accounts: Facebook – X – Instagram – LinkedIn – YouTube –TikTok (inactive) – Bluesky (inactive).

Use a strong and UNIQUE password for each one of your social media profiles. Make sure you still have access to the email/phone number you registered with when signing up. If you are concerned about being outed, change your profile settings to private. Don't agree to friend requests from people you don't know on social media networks – people are not always who they say they are.

In case of a social media anti-LGBTI cyber-attack: do not engage with trolls, but screenshot and record their messages and report them instead. Do not click on suspicious links you receive in comments or DMs – especially from senders you don't know. Ensure your antivirus and firewall protections are up to date. If the trolling intensifies, change your profile setting to private or deactivate comments. **ILGA World will never ask for your passwords!**

Sources for this guide: AccessNow; GlobalPride2020; Security in a Box by Frontline Defenders and Tactical Tech; Surveillance Self-Defense by Electronic Frontier Foundation