Digital safety tips against cyber attacks

accessnow

What this guide is for

The cyber threats to people's human rights in Ukraine are rapidly escalating amid the ongoing Russian aggression at the Ukraine-Russia border. This short guide is to provide hands-on action plans. The goal is to help civil society respond to the situation, to protect and sustain their work, as well as to create cybersecurity resilience.

Secure your accounts

1. Do not share your login information with anyone.
2. Always keep your apps, systems, and software up to date. (Pro-tip: enable automatic updates.)
3. Activate Two-factor authentication (2FA) to safeguard your accounts.
4. Learn how to recover your compromised or hacked accounts:
   - Google
   - Twitter
   - Facebook (Report hacked / fake accounts)
   - Apple
5. Check your account security settings:
   - Google
   - Facebook
   - Twitter
   - Apple
   - Tiktok

Further reading: **https:/ digitalfirstaid.org/en/topics/account-access-issues/**

accessnow

Secure your device part 1: clean your data

The key is to **minimize your data** to reduce the burden of securing it. Especially for your personal or organizational work, start with:

1. Identifying the sensitive data that needs to be protected.
2. Identifying the critical assets that would stop you or your organization from working.

Then:

1. Reduce the data you save on your devices as much as you can.
2. Transfer critical data from physical devices to cloud-based solutions as much as possible.
3. Learn how to permanently erase data from your devices.

Further reading: **https://securityinabox.org/en/guide/secure-file-storage/**

accessnow

Secure your devices part 2: encrypt your data

To protect your data stored locally, **encrypt your devices**.

1. Make sure Full Disk Encryption is activated on your computers and smartphones.
2. Encrypt data in external hard drives with tools like Veracrypt.
3. If you lose a device that is logged-in to your accounts, disconnect that device from your accounts immediately to prevent further damage.
   a. Disconnecting your account from Google
   b. Disconnecting your account from Facebook
   c. Disconnecting your account from Apple
   d. Disconnecting your account from Twitter

Further reading: **https://digitalfirstaid.org/en/topics/lost-device/**

accessnow

Safeguard against malware

1. Keep your operating system, apps, and all software up to date.
2. Pause before you click a link or open an attachment from an instant message or email. Verify the sender and check the entirety of the link url or the attached file extension.
3. Use trusted anti-malware tools, like Microsoft Defender or Malwarebytes.
4. Beware of abnormal device behaviors, like unexpected battery drain, irregular slowdown of the operating system, frequent apps crashing, etc.
5. If you suspect your device is infected, restart your device and disconnect it by turning off bluetooth, wifi, mobile data, and other ways to connect to your device and turning on Airplane mode.
6. Use non-affected device to contact Digital Security Lab Ukraine or Access Now Digital Security Helpline for further assistance.

Further reading: **https://securityinabox.org/en/guide/malware/**

accessnow

Emergency communication

In case of **internet or telecom outage:**

1. Using Bluetooth (up to 50 metres) – Change the name of your device in settings to the message you want to convey and turn your Bluetooth on. Other people near you who have their Bluetooth turned on will be able to see your device displaying the message.
2. Using AirDrop (up to 50 metres) - People using an iOS device can use AirDrop in the same way, but also to send notes, files, screenshots of messages, etc. to iOS users alike who are nearby.

accessnow

Emergency communication

Free and easy-to-use peer-to-peer messaging apps not requiring internet**:**

1. Briar (for Android) – In case of a Telecom outage, Briar will sync via Bluetooth, enabling users to stay informed in case of a crisis situation. In order to start using Briar, an account is required, after which you can add contacts by connecting via Bluetooth and stay in touch.
2. Bridgefy (for iOS) – Bridgefy requires Bluetooth to function. There is no sign-up needed, one only has to set a nickname to use the app. This nickname will also allow people in nearby proximity to search for a particular user. Apart from private chat, it also provides a broadcast section. Messages sent to this platform will be read by any Bridgefy user nearby, which could be helpful to connect several people in an area.

In case of internet shutdown or censorship

Connectivity and internet traffic can vary between Internet Service Providers (ISPs), to ensure connectivity, **get SIM cards from as many carriers as possible,** such as Kyivstar, Lifecell, and Vodafone, in case one carrier's card does not work.

In the event that online content and communications are blocked or censored, tools like Virtual Private Networks (VPNs) may help. In the next pages, you will find detailed information about some free-to-use VPNs and Tor Browser, including the official channels to download them.

Find out more about them in the next page →

accessnow

FREE AND EASY-TO-USE VPNS

UPDATE: FEB 2022

Contact Access Now's Helpline for free codes and setup instructions.

MULLVAD

A fast and easy-to-use VPN to evade hackers and trackers

AVAILABLE ON

→ **Android 8.0 and up**
→ **iOS 12.0 and up**

→ **Windows 7 and up**
→ **macOS 10.14 and up**
→ **Linux (Ubuntu 18.04+, Debian 10+, Fedora 33+)**

TO DOWNLOAD AND USE

https://mullvad.net/en/download/

Also available as browser extensions
FIREFOX

Contact Access Now's Helpline for free codes and setup instructions.

TUNNELBEAR

A VPN that enables private browsing with no logging

AVAILABLE ON

→ **Android 5.0 and up**
→ **iOS 12 and up**

→ **Windows 7 and up**
→ **MacOS 10.10 & up**

TO DOWNLOAD AND USE

https://www.tunnelbear.com/download-devices

Also available as browser extensions
CHROME | FIREFOX | OPERA

Contact Access Now's Helpline for free codes and setup instructions.

AIRVPN

A VPN based on the OpenVPN system

AVAILABLE ON

→ **Android**
→ **iOS**

→ **Windows 7 and up**
→ **macOS 10.15 and up**
→ **Linux (Ubuntu, Debian)**
→ **Chrome OS**

TO DOWNLOAD AND USE

https://airvpn.org/download/

#KeepItOn https://www.accessnow.org/keepiton/

FREE AND EASY-TO-USE VPNS AND BROWSING TOOL

UPDATE: FEB 2022

PSIPHON

FREE

A must-have to circumvent censorship

AVAILABLE ON

- → Android 4.0 and up
- → iOS 10.2 and up
- → Windows (XP/Vista/7/8/10)
- → macOS 11.0 and up (with M1 chip)

TO DOWNLOAD AND USE

https://psiphon.ca/download.html

LANTERN

FREE

Fast, reliable, and secure access to the open internet

AVAILABLE ON

- → Android 4.4 and up
- → iOS 12.1 and up
- →Windows (XP/SP/3)
- → macOS 11.0 and up (with M1 chip)
- → Linux Ubuntu

TO DOWNLOAD AND USE

https://getlantern.org/

PROTONVPN

ProtonVPN FREE (Limited)

High-speed VPN that safeguards your privacy

AVAILABLE ON

- → Android 5.0 and up
- → iOS 11.0 and up
- → Windows
- → OSX
- → Linux

TO DOWNLOAD AND USE

https://protonvpn.com/download

TOR BROWSER

FREE

Protect yourself against surveillance & censorship.

AVAILABLE ON

- → Android
- → Windows
- → MacOS
- → Linux

TO DOWNLOAD AND USE

https://www.torproject.org/download/

Also available as browser extensions
CHROME | FIREFOX | OPERA

#KeepItOn https://www.accessnow.org/keepiton/

Important note

A VPN can help you circumvent the blocking of websites or online platforms, including specific services such as social media platforms and instant messaging apps. Download several VPNs in advance if you are at risk of a shutdown.

Not all VPNs can guarantee your privacy or offer you the same level of protection. When choosing a VPN provider, opt for open source tools with publicly accessible codes and transparency on how they protect your data. You should also ensure that the VPN is public about their peer security review process and that their security has been reviewed by independent auditors. Read **this guide** from EFF to determine which VPNs would be the best in your specific case.

Be mindful: your internet provider, or other people in your network can tell if you are using VPNs or Tor.

Find help

Access Now's Digital Security Helpline provides 24/7 technical support for journalists, civil society members, and human rights defenders in nine languages, including English and Russian.

Digital Security Lab helps Ukrainian journalists, activists, civil society organizations, and human rights defenders defend internet freedom.

accessnow