Digital safety tips if you are disconnected

Three steps to respond to a network disruption

#KeepItOn

This quick guide provides three steps to help you respond to a network disruption safely.

A network disruption, or an internet shutdown, is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.

This guide is for you if your daily life depends on the internet — whether it's to study, do business and work, or contact people. If you are comfortable with technology, you can use the information in this guide to navigate your options for online protections. If you are looking for further technical assistance to enhance your safety online, this guide lists several organizations and resources at the end for you to contact. We recommend you save or print this guide in case you lose access to the internet.

Please keep in mind, this guide offers basic and general tips in tackling network disruptions. Based on where you are and your personal experience, some tools or means provided in the guide may not work well or as expected. Feel free to use any part of this document to generate your own guide for your community. If you identify any problem in the guide, please contact sage@accessnow.org and felicia@accessnow.org.

#KeepItOn

Step 1.
Research for possible disruptions of your network and electronic communications

In this step, you will answer two questions →

#KeepItOn

- **Question 1: Do you believe that an internet disruption will occur in your area?** News and articles about past or potential shutdowns can help you understand what could trigger restrictions to internet access or electronic communications. For instance, in the lead-up to an election or school exam, the authority may shut down the internet completely or partially.

- **Question 2: What's your main goal when you use the internet?** List out the most important things you need to do online. It can be contacting your loved ones, sending and receiving your work or research documents, keeping your clients and doing business, paying and receiving money, and getting news updates and information. This list will be your priority in preparing for a potential internet disruption.

You've got answers? Let's move to step 2 →

#KeepItOn

Step 2.
Prepare yourself before a shutdown happens

In this step, you will learn three actions to complete your preparation →

#KeepItOn

Action 1: Learn about different types of network disruptions and possible mitigations in the following pages. This can help you stay connected in certain types of network disruptions.

Action 2: Set up secure communication methods with your contacts. Having multiple options in place can help you to stay connected with important contacts and get further help.

Action 3: Test for ongoing internet shutdowns. Your test results can help others in the community better understand the technical details of what's happening and to provide solutions.

Now, let's get into the details of each action! →

#KeepItOn

Action 1: Learn about different types of network disruptions and possible mitigations.

You can avoid certain types of network disruptions with out-of-box tools, such as Tor browser, Virtual Private Networks (VPNs), and proxies that utilize encryption. The following table can help you understand what kind of shutdown you might be experiencing and what methods can help you stay connected.

Let's take a closer look →

#KeepItOn

Symptoms	Possible type of network disruptions	Possible ways of mitigation
All websites are immediately unreachable. No internet connection is available.	**Full blackout:** a complete shutdown caused by critical infrastructure manipulation, such as turning off the power grid, cell towers, or broadband services.	If possible, get a **roaming SIM card** from a neighboring country. Their telecom infrastructure works and may reach you. To contact people near you, you can install **encrypted mesh network** apps like Briar (Android only) and Bridgefy or devices like goTenna.
Websites and apps have become sluggish, slow, and frustrating to use. Downloads and/or uploads seem to take a lot longer than normal.	**Throttling:** intentionally slowing down internet speeds, making it difficult or impossible for users to upload or download information.	There are many ways to implement throttling, and some are more difficult to mitigate. To start, you can try using a **VPN** to see if the network bandwidth limits are lifted.

#KeepItOn

Symptoms	Possible type of network disruptions	Possible ways of mitigation
When you visit a website, you get messages saying "the connection is unsafe" or "DNS Server Not Responding," or the webpage looks strange, different, or is not working properly.	**DNS blocking and DNS poisoning:** disrupting the domain name system (DNS) lookups so when you try to visit a website it points you to the wrong place.	Try using a **reliable VPN**. **Install and test more than one** in case some of them no longer work. You can also use a **trusted DNS server** with help from civil society help desks. You may also be able to visit the **IP address** of a website.
The website/app or a version of it is not available, or the content you see is different from people in other regions. E.g. you can only visit the HTTP address of the website, not the HTTPS address.	**Network filtering:** using "middleboxes" planted in network traffic to interfere with communication protocols like Hypertext Transfer Protocol Secure (HTTPS).	A **reliable VPN** may work. You can also try **switching to a different internet service provider (ISP)**, like using broadband instead of cellular data.

#KeepItOn

Symptoms	Possible type of network disruptions	Possible ways of mitigation
Specific parts of a particular app, service, or website don't work or are unreachable (for example, you can make a new account but you can't log in), while all other apps or services seem to be ok.	**Deep Packet Inspection (DPI):** using a checkpoint to detect detailed information about what internet traffic on a network, and using that information to block certain kinds of data from getting through.	If you have an idea of what is being targeted, you may be able to reconnect. Some possible remedies include using a **reliable VPN**, using circumvention tools like **Tor Browser**, or **switching to a different ISP.**
The website or app that you are trying to use is slow or unresponsive. Sometimes it works and other times it is unreachable with things getting slower and slower.	**Denial of Service:** overwhelming the web server or related system of the website or app with so many requests that it slows down or crashes.	Try to visit the service or website **from a different country using a VPN**. You can also try visiting the **IP address** of the website or service instead of its domain name.

#KeepItOn

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! →

FREE AND EASY-TO-USE VPNS

UPDATE: NOV 2023

PSIPHON
FREE

A must-have to circumvent the censorship

AVAILABLE ON

📱	→ Android 4.4 & up → iOS 10.2 & up
💻	→ Windows (7/8/10) → MacOS 11 & up

TO DOWNLOAD AND USE

https://psiphon.ca/

LANTERN
FREE

Fast, reliable, and secure access to the open internet

AVAILABLE ON

📱	→ Android 6 & up → iOS 12 & up
💻	→ Windows (7/8/10/11) → MacOS 10.11 & up → Linux Ubuntu

TO DOWNLOAD AND USE

https://getlantern.org/

PROTONVPN
FREE

High-speed VPN that safeguards your privacy

AVAILABLE ON

📱	→ Android 5.0 & up → iOS 11.0 & up
💻	→ Windows(7/8/10/11) → MacOS (10.12 & up) → Linux

TO DOWNLOAD AND USE

https://protonvpn.com/free-vpn

TUNNELBEAR
Free 10GB/mon in selective countries

A VPN that enables private browsing with no logging

AVAILABLE ON

📱	→ Android 8.1 & up → iOS 12 & up
💻	→ Windows 10 SP1 & up → macOS 11.0 & up

TO DOWNLOAD AND USE

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

Also available as browser extensions
CHROME | FIREFOX | EDGE

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

FREE AND EASY-TO-USE BROWSING TOOL

FREE

TOR BROWSER

Protect yourself against tracking, surveillance, and censorship.

AVAILABLE ON

→ Android → iOS (download Onion Browser from the app store)

→ Windows → MacOS → Linux

TO DOWNLOAD AND USE

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

#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. In some countries, the use of circumvention tools and VPNs are illegal or subject to restrictions. Make sure to consider any legal and personal safety risks that may arise from your use of such tools.

#KeepItOn

Action 2: Set up secure communication methods with your contacts.

Proactively **establish multiple channels** of communication with your important contacts — including people who can help you during an emergency — in case one or several channels become unavailable during an internet shutdown.

For safer communication, use applications and services that support **end-to-end encryption**. It is important to choose services and applications that are open source and undergo regular independent audits. For example, there are several open source instant messaging tools that use Signal Protocol — an end-to-end encryption protocol for messages and voice or video calls — including Signal and Wire. **Read the guide** provided by each tool carefully before you use them, as some patterns of use may put you or your contacts at risk.

Some important notes →

#KeepItOn

✏️ Important note

Make sure you install and test several options. When you lose access to the internet, you may not be able to use encrypted messaging tools. If you have to send messages without encryption (e.g. sending messages via SMS), be careful with the information and messages you are sharing. Consider who you are communicating with and any risks you may be exposing yourself and them to during your communications.

Action 3: Test for ongoing internet shutdowns.

When you lose internet connection or can't visit certain websites, services, or apps, it is very difficult to tell the technical means behind these disruptions. However, there is a global internet measurement community that provides tools and data to help you investigate the technical details.

Monitoring tools such as the OONI Explorer, Internet Outage and Detection Analysis (IODA), and Google's traffic and disruption tracker provide near-real-time data to identify internet outages on various networks. There are also country-specific shutdown trackers, such as killswitch.pk and internetshutdowns.in. You can test your internet connections using the OONI Probe app, which allows you to run tests and document evidence of various forms of network interference.

Let's look at the OONI Probe app for example →

#KeepItOn

TEST YOUR INTERNET CONNECTION WITH OONI

UPDATE: NOV 2023

OONI

A tool to test whether websites, social media apps, or VPNs are blocked

OONI PROBE IS AVAILABLE ON

| | Android & iOS | https://ooni.org/install/mobile |
| | Windows, macOS, Linux | https://ooni.org/install/desktop |

NOTES

1. OONI Probe tests require turning off VPNs.
2. Running these tests could be risky. Anyone monitoring your internet activity (e.g. ISP, government, your employer) can see that you are running OONI Probe and the websites they are trying to visit.
3. These tests use megabytes of data.

WE RECOMMEND

1. Read more about **potential risks** before installing OONI Probe.
2. Close all your browsers, other applications, and your VPN service before running the test.
3. Avoid using your home or work wifi. Beware of data usage when you use your cellular data.

Open this link in app to check social media blockings
https://accessnow.org/ooni-test-social

For more information, including risks, visit
https://ooni.org/

✎ Important note

Learning more from the measurement community can not only help you understand what is happening but also how to respond appropriately. Running these tests can also help the #KeepItOn coalition respond more effectively to shutdowns as they happen.

#KeepItOn

Step 3.
Defend yourself and your community during a shutdown

In this step, you will learn two ways to help →

#KeepItOn

Way 1: Get the information out safely. If your area is affected by a shutdown, use your available channels to get the information about the situation out. This can help people demand accountability and remedy. But always make sure what you are sharing will not affect the safety of you and people around you.

Way 2: Document the loss or harm caused by a shutdown. Documentation can take different forms, including videos, testimonies, photos, and written notes. Securing and storing this information is essential to make sure you do not lose it and to avoid taking personal safety risks. As you are able, the #KeepItOn coalition welcomes you to share your Shutdown Story directly with us.

Again, important notes! →

#KeepItOn

✎ Important note

To avoid becoming a target of stalking or harassment, minimize the personal information you are sharing on social media or other communication channels. Check the privacy and security settings of your accounts to make sure no information about you is being shared without your knowledge.

It is also important to ensure the security of your accounts and devices to avoid losing access to your accounts and important information stored on your devices. Basic account security measures include using a long, strong, and unique passphrase for each of your accounts (use a password manager like KeepassXC to store them safely!), and activating two-factor authentication. Make sure your mobile devices are encrypted and the operating system and apps are up to date. If possible, back up your important data to an encrypted hard drive. More detailed tips can be found at Surveillance Self-Defense and Security Planner.

#KeepItOn

**Okay! I learned all three steps.
But I want to know more to be fully able to conduct them.**

Sure! Here are more resources and extended reading →

✎ Useful resources

Surveillance Self-Defense (SSD):
https://ssd.eff.org/
Tips, tools, and how-tos for safer online communications

Chapter on network disruptions:
https://ssd.eff.org/en/module/understanding-and-circumventing-network-censorship

Chapter on mobile phone privacy:
https://ssd.eff.org/en/playlist/privacy-breakdown-mobile-phones#playlist

#KeepItOn

✎ Useful resources

Access Now community documentations

Anti-doxxing guide: https://guides.accessnow.org/self-doxing.html
Tips and resources for exploring open source intelligence on yourself to prevent cyber stalking

Circumvention and anonymity:
https://communitydocs.accessnow.org/175-Circumvention_Anonymity_tools_list.html
List of tools in response to network disruptions

Safe travel guide: https://guides.accessnow.org/safer_travel_guide.html
A guide to help you prepare for your travels

#KeepItOn

✏ Useful resources

Security Planner:
https://securityplanner.consumerreports.org/
Keep your data secure with a personalized plan

Digital First Aid Kit:
https://digitalfirstaid.org/
A guide designed to get you to the right civil society help desk

Down For Everyone or Just Me?
https://downforeveryoneorjustme.com/
A tool for you to check if the website is down for everyone or just for you.

#KeepItOn