

How to spot harmful information in crises

March 2024

In times of emergency, finding reliable information online can be challenging. This guide offers practical advice to help you identify trustworthy information and avoid misinformation. By asking the right questions and using the tools provided, you can make informed decisions even during a crisis.

How can I tell if information online is reliable?

To figure out if information is likely to be accurate, follow these steps:

- 1. Check the source.** Is it from a place you trust? Review 'About' pages and history of unfamiliar sources. Be cautious of sites with strange URLs or layouts and verify social media accounts.
- 2. Look for the full story.** Headlines can be misleading. Read beyond them, check the context of quotes and images, and seek original sources of statistics. Doubt claims with altered images or videos, and compare the information with reputable sources or fact-checkers.
- 3. Watch your feelings.** Misinformation often tries to make you feel scared or angry to get more clicks. Be sceptical of information that seems too good to be true or that provokes a strong emotional reaction.

What should I do before sharing information on closed messaging channels like WhatsApp or Telegram?

- 1. Pause:** Is it necessary for me to share this content? Would sharing it cause worry or harm?
- 2. Verify:** If you're not able to verify the information or source, don't share. Receiving the same information from many people does not mean it is credible.
- 3. Assess:** Ensure the content is current, accurate and free from alarmist or stigmatising language.

How do I check the authenticity of images and videos?

- **Cross-check information** with trusted sources.
- **Analyse digital footprints** and check the credibility of social media accounts using tools like [Namechk](#) or [Instant Username Search](#).
- **Reverse image search** using [Google Images](#), [TinEye](#) or [Yandex](#) to find the original source.
- **Check the origins** of a photo or video, with tools like [Jeffrey's Exif Viewer](#) and [Amnesty Youtube Data Viewer](#).
- **Verify videos** with [InVID Verification Plugin](#).

How do I prepare for internet shutdowns?

- **Download mesh networking apps** like [FireChat](#), [Bridgefy](#) or [Briar](#) that use Bluetooth or Wi-Fi to relay messages without the internet.
- **Virtual walkie-talkie apps** like [Voxer](#) can turn your phone into a walkie-talkie for nearby communication without internet access.
- **Consider backup options** like HAM radio or satellite phones.

How can I find help in different languages on- and offline?

- **Use translation apps** like [Google Translate](#) and built-in translation features in social media and messaging apps.
- **Download language packs** on Google Translate in preparation if you're concerned about losing internet access.

What if I'm still not sure about the information?

- **Consult fact-checking services** like [Full Fact](#) to confirm suspicious stories or claims.
- **Carefully analyse content** using tools like [FotoForensics](#) for evidence of manipulation, such as inconsistencies in video or audio that might indicate a deepfake.
- **Check whether an account is a bot** using tools like [Botometer](#) or [BotSight](#).

More guidance and resources

- [CDAC Network's guide to working with rumours](#) offers strategies for managing misinformation.
- [Digital first aid kit](#) provides tools for navigating internet shutdowns and digital emergencies.
- [OSINT essentials](#) has free tools and practices for investigating online content and information.
- [Contact Access Now's digital security helpline](#) for real-time, direct technical assistance to stay safe online.
- [Full Fact's toolkit](#) for spotting misleading information, available in multiple languages.

This guide aims to support communities with the tools and knowledge to discern reliable information in crises. For more advice or to share your experiences, reach out to info@cdacnetwork.org.