

# Digital Safety Manual

This guide contains 12 cards with information and practical tips on enhancing digital security for embassy staff working with civil society and Human Rights Defenders (HRDs).

Each card provides items to consider and protection tactics relating to an aspect of digital security. It is important to note that contexts vary across countries and change over time due to the dynamic nature of digital developments. This guide should be accompanied by a regular analysis of context and risk, on- and offline.

The website <https://digitalsafetymanual.org> which accompanies the cards offers software recommendations and external resources as well as a glossary of technical terms. This guide was developed by the Digital Defenders Partnership.

If you are not sure where to start: begin at the beginning, and work your way through the cards. *Happy reading!*



More information  
and resources here



## Contents

- 1 Assessing Digital Security Needs – step by step
- 2 Basic Device Security
- 3 Passwords and Account Protection
- 4 Connecting to the Internet Securely
- 5 Secure Calls, Chat and Email
- 6 Security and Social Media Use

# Digital Safety Manual

*Navigating online risks:*

GUIDANCE FOR DIPLOMATS AND EMBASSY STAFF WORKING WITH CIVIL SOCIETY

- 7 Secure Data Storage and Deletion
- 8 Secure File Transfer
- 9 Secure Contract Handling
- 10 Targeted Malware and Other Attacks
- 11 Phone Tracking and Surveillance
- 12 Security Concerns Related to In-Person Meetings

