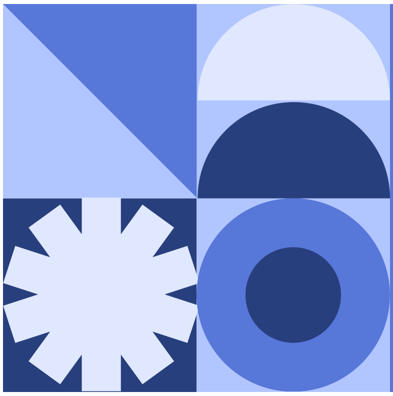
Internews



Digital security for journalists from marginalized communities

Caregivers

Developed by Internews in collaboration with Lejla Sarcevic & Madeline de Figueiredo

Who is this guide for?

This guide highlights digital security considerations, mitigation strategies, and resources for anyone who has caregiving responsibilities. Some example groups may include the following: those who care for minors (parents, guardians, etc.); those who care for people with illnesses, those who care for persons with disabilities, those that care for older adult family members, etc. This guide is designed to be used by digital security specialists working with journalists who are caregivers, though some of its advice might also apply to journalists whose colleagues, sources, or other collaborators are caregivers.

Caregiver Community Digital Security Challenges

Threats are the direct attacks that can impact your life.

Attackers are the individuals executing these threats.

Vulnerabilities are the weaknesses in societal systems, technical systems, and individual habits that make it easier for attackers to carry out the threats. Systemic inequities are often the root cause of these weaknesses.

Threats	Adversaries	Vulnerabilities
• Data leaks • Doxxing • Phishing • Malware • Spyware	• Dependents themselves can be an accidental adversary if they, for example, accidentally share	• Dependents can overhear calls with sources, see other communication. If not properly briefed, they could widely share or accidentally leak data about sensitive reporting projects.

● Ransomware	information about a caretaker journalist's work. ● Online trolls ● Extremist groups ● Financially-motivated attackers ● Law enforcement or other authoritative entities	● Lack of secure management of sensitive documents and data (e.g., medical/health information or other private details about children or other dependents) ● Can be difficult to travel to meet sources and others if it conflicts with caregiver duties ● Sharing of devices between caregivers and dependents ● Compounding responsibility: caregivers needing to protect their digital security + that of their dependents ● Depending on network (e.g., teachers, healthcare workers, etc.) to manage personal data for caregiver and dependents (increased potential for leaks)

Threat Modeling for Caregivers

	Considerations for Caregivers
Assets	All data related to journalistic work (including details of and conversations with sources), medical data, health plans, information about school location and children's whereabouts/schedule, sensitive personal information, trust between caregiver and dependent, privacy, likeness of minors, etc.
Adversaries	Mostly non-state. High risk of accidental or unintentional adversaries (a child or someone in your wider caregiving network could reveal information about you, your travels, or your reporting which you did not want to publicly share).
Likelihood	Very likely that caregivers will need to manage digital security of dependents. especially if they are taking care of a dependent's digital life (e.g., they share passwords with you). Very likely that there is highly sensitive information that will need to be protected.
Consequences	Consequences are often dependent on context but can include the following: breakdown of trust between the caregiver and the dependent, loss of control over highly sensitive data/information, issues that affect broader family/community circles.
Effort	Potentially quite high. Dependents (e.g., children, older adult parents, or persons with disabilities) may have low digital literacy which can create added risks. Digital technology is often incorporated into mechanisms of care leading to specific needs to manage digital security in the context of caretaking.

Mitigation strategies are the practices that can be leveraged to address vulnerabilities.

- For example: using password managers and putting important apps behind extra passwords to prevent accidental access or information leaks (Signal, for example, has the option to enable a separate face/ password unlock), managing notifications on phones so they aren't immediately visible, using healthcare platforms that promote and protect privacy, delaying posting photos so current location is not accessible, excluding maps/doors from photos of houses to mitigate risk of geolocation, blur faces of dependents on social media posts, etc.

Mitigation tools are the devices, applications, and workflow apparatuses that can be applied to reduce the risk of attacks.

- For example: using separate devices or device profiles whenever possible, using features like hidden folders on devices, encrypting sensitive documents, using password managers and 2FA to reduce attacks on accounts and data leaks, using social media apps with high and configurable privacy settings

Mitigation actors are the entities and individuals that can offer protection in a digital security context.

- For example: healthcare provider, school administrator, parent community, fellow caregivers, peers of the dependent, family, journalist, source, community, etc.

How to Talk to and Persuade Others

Best Practices: Implement better practices/policies through existing structures. Consider the time constraints that impact caregivers when implementing interventions.
Allies: Identify allies to build communities and systems of good digital security practices (i.e., healthcare providers, school administrators, peers, insurance coordinators, teachers, etc.). Talk regularly to other journalists who are also caregivers.
Incentives: Incentivize stakeholders to take up certain practices to promote better digital security habits. Talk to newsrooms and managers about both moral and legal responsibilities towards employees and freelancers who are caregivers. Talk to your newsroom and security teams about how the risk of accidental leaks might require that they give you additional, separate devices.
Transparency: Be transparent about challenges. Normalize that breaches do happen so that others feel comfortable speaking openly and sharing information about vulnerabilities, threats, attacks, etc. Talk to other journalists who are caregivers.

Communicate: Listen and learn from the community. Try to understand any hesitancy, address concerns, and be open-minded. Contextualize any tools or practices for the needs and profile of the community to make adoption and integration of digital security topics more accessible.
Nudge the Needle: Advocate for incremental changes and be willing to compromise for movement in a direction that promotes healthy digital security (e.g., moving primary form of communication from Facebook to a more secure platform, even if it is not the most secure platform).
Share Resources: Share tools, guidelines, and research from established and credible sources.

Digital Security Resources for Caregiver Community

Sub-community	Resources
For caregivers of children	**Digital literacy** **European Youth Portal** | Be Safe Online **Google** | Be Internet Awesome **Common Sense Education** | Everything You Need To Teach Digital Citizenship **UK Safer Internet Centre** | Homepage
For caregivers of older adults	**Digital literacy** **Age UK** | How To Stay Safe Online as an Older Person **OATS** | Older Adults Technology Services **AARP** | https://www.aarp.org/home-family/personal-technology/info-2019/privacy-for-seniors.html **Security keys** **Innovation in Aging** | Why Don't Elders Adopt Two-Factor Authentication? Because They Are Excluded by Design (academic article)
For caregivers of persons with disabilities	**Digital literacy** **European Patients Forum** | The new EU Regulation on the protection of personal data: what does it mean for patients?

Assistive technologies

European Parliament | Assistive technologies for people with disabilities: Current and emerging technologies

Oxford University Press | Privacy and Security Issues in Assistive