Internews

Digital security for journalists from marginalized communities

LGBTQI+

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 journalists who identify as or work with sources who identify as members of the LGBTQI+ community (stands for Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, plus any other non-straight or non-cisgender communities). LGBTQI+ is inclusive of a whole range of sexual orientations and gender identities.

This guide is designed to be used by digital security specialists working with journalists who belong to this community. Some of its advice might also apply to journalists whose colleagues, sources, or other collaborators belong to this community.

LGBTQI+ Community Digital Security Challenges

Threats are the direct attacks that can impact your life.

Adversaries 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	Attackers	Vulnerabilities
• Harassment, trolling, outing	• Hate groups and anti-LGBTQI+ groups	• Lack of security around private social media profiles

• Data leaks • Phishing • Malware • Doxxing • Spyware • Ransomware	• Extremist groups • Internet trolls • Community members • Former or current partners • Law enforcement or other authoritative entities	• Network effects (large support networks that can have many digital security holes) • Lack of secure management of highly sensitive documents and data (e.g., details about romantic and sexual partners, healthcare records, community support networks, financial information, etc.) • Increasing criminalization and surveillance of the LGBTQI+ community

Threat Modeling for the LGBTQI+ Community

	Considerations for the LGBTQI+ community
Assets	Social network graphs, messages, personal data such as photos, ability to continue reporting work in the face of trolling and harassment
Adversaries	Most adversaries will be non-state, though in many contexts, state actors are using digital attacks and surveillance against the LGBTQI+ community. High risk of accidental or unintentional adversaries as well (for example, a friend who tags you on social media or reveals data that you'd prefer not to be widely or publicly known)
Likelihood	Even in largely tolerant countries the likelihood of online harassment and threats to LGBTQI+ people is high. In many countries, there is increasing criminalization and digital surveillance of LGBTQI+ communities, including undercover monitoring of the community through online community spaces and dating apps. Journalists who are LGBTQI+ are often at higher risk of trolling and harassment than others
Consequences	Consequences are often dependent on context but can include horrific trolling and harassment that aims to discourage a journalist from the profession. There is also risk of being arrested in or denied entry to countries that criminalize LGBTQI+ communities.
Effort	Potentially high and requires community collaboration. LGBTQI+ communities tend to be highly interconnected (for support) and there are numerous vectors for exposure. There are basic steps individuals can take to protect themselves (2FA, mutually agreed on privacy norms, and the like). However, wider efforts and communication are needed amongst a community that can be highly at risk, but to

whom visibility is often of paramount importance. Evangelizing strategies require

Managing Digital Security for the LGBTQI+ Community

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

- For example: secure communications and disappearing messages, using dating platforms that focus on privacy and personal safety, using pseudonyms, being cautious about what is posted on social media, having a good strategy for muting and blocking on social media, having a separate profile for journalistic work and another for personal life

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

- For example: 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: other members of the LGBTQI+ community, colleagues, friends, family

How to Talk to and Persuade Others

Allies: Identify allies to build communities and systems of good digital security practices (trusted friends, family, community members, fellow journalists and others within the newsroom, healthcare providers.)
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 LGBTQI+ journalists about the challenges they have faced and talk to your newsroom about what support they offer for those facing harassment or trolling.
Educate: Explain all pros and cons of certain digital security practices and be more direct about why adjustments would be beneficial. Don't forget that journalists often have very public profiles and need to be out there in the open; think of how to talk to them and address any concerns related to them spending a lot of time in the public eye.
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 LGBTQI+ Community

---

vpnMentor | The LGBTQI+ Guide to Online Safety

Access Now | Digital Security Helpline: In 2020, LGBTQI+ groups are facing more online harassment than ever - Access Now

OutVoices | Why cybersecurity is an LGBTQ+ issue

Palante Technology Cooperative | Palante.tech

TIERS & NDWA | Facebook LGBTQI+ Online Safety Guide

PEN America | Online Harassment Field Manual