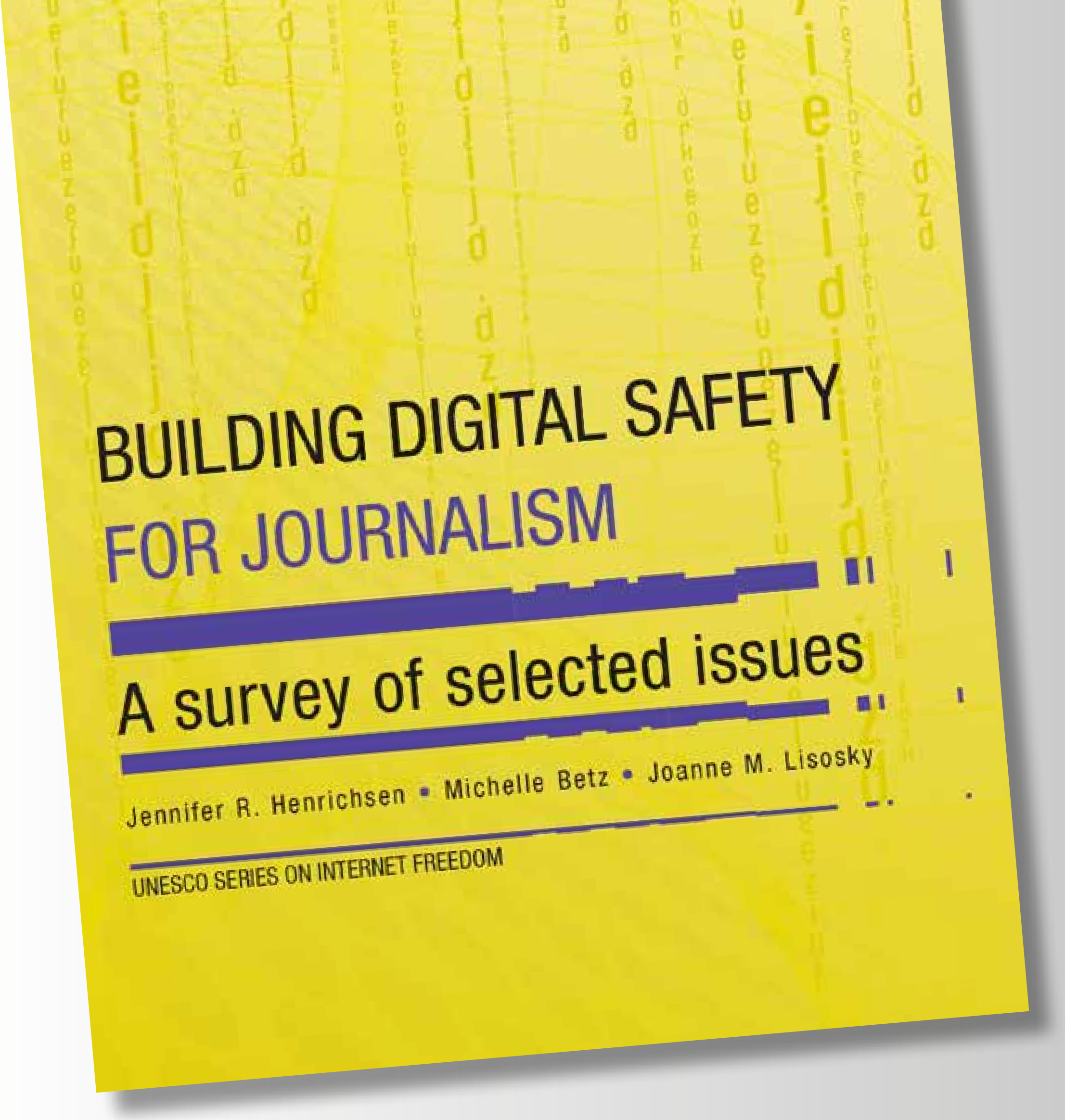
United Nations
Educational, Scientific and
Cultural Organization



BUILDING DIGITAL SAFETY FOR JOURNALISM

A survey of selected issues

Jennifer R. Henrichsen • Michelle Betz • Joanne M. Lisosky

UNESCO SERIES ON INTERNET FREEDOM

#journosafe

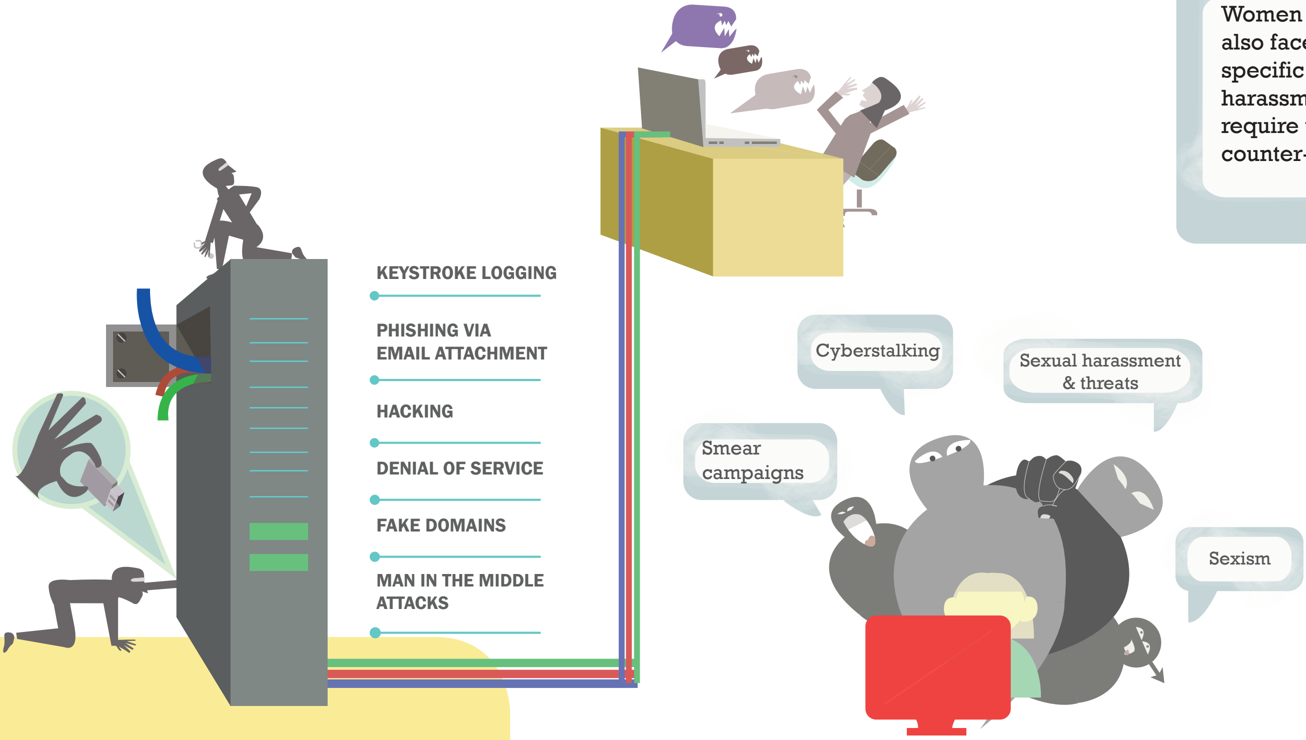
Available online

As technologies develop, so do opportunities as well as threats to journalism. Often without knowing it, those engaged in journalism expose digital information to risks that they would not accept in the physical world. But the answer is not to be paralysed by digital paranoia, nor to be overly fatalistic and neglect digital confidentiality altogether.

Understanding the dangers that come with the opportunities of digital is key to mitigating them, based on an informed threat analysis and appropriate response. This is key to building safety for producers of journalism and their sources. It is also crucial to preserve an independent and free media's function in a democratic society.

Together with many partners, UNESCO tackles digital safety for journalism – highlighting the range of technical, psychological, operational and policy issues.

Women journalists also face gender specific threats and harassment that require targeted counter-measures.



GUIDELINES FOR MEDIA ACTORS DOING JOURNALISM IN A DIGITAL CONTEXT

In general, all journalistic actors interfacing with digital technology should:

1. Develop a risk assessment plan or ‘threat model’ and develop a personal security plan with tools and techniques necessary to successfully implement it;
2. Acknowledge that security is always a trade-off of resources and prioritize security needs based on an individualized risk assessment and adaptation to different stories – avoid the extremes of paranoia on the one hand, and a sense of futility on the other;
3. Understand that digital and physical security are linked and take steps to improve both;
4. Treat digital hygiene as a habit and practice;
5. Realize that there is a need to keep up to date and to understand the strengths and weaknesses of browsers, email-providers, social media, messaging applications, software and hardware.

Building Digital Safety for Journalism – A survey of selected issues is the 4th output in UNESCO’s Internet Freedom Series. It explains some of the emerging threats to journalism safety in the digital era, and proposes a framework to help build digital safety for journalists.

“Building digital safety for journalism” is a metaphor about constructing a shelter. As with any construction, the occupants are best accommodated if many actors help design, construct and outfit the dwelling. Digital safety is no less a multistakeholder endeavour involving policy makers, public authorities, international organisations, civil society, media owners and organisations, individual journalists and sources.

This research, available for free from UNESCO’s website, analyses 12 key digital threats to journalism, ranging from hacking of journalistic communications, through to denial-of-service attacks on media websites. It surveys the evolving threats, and assesses preventive, protective and pre-emptive measures to avoid them. It shows too that digital security for journalism encompasses, but also goes beyond, the technical dimension.

The publication also gives an overview of actors and initiatives working to address digital safety through a variety of commitments, initiatives, training courses, meetings and materials. Useful resources and examples for the reader are mapped according to four categories:

- Normative work and awareness raising,
- Digital security training guides and training courses,
- Hotlines and safety assistance, and
- Reports and research.

The research is relevant to any actor who is in danger of being targeted for doing journalism, but also to human rights defenders in general and to those concerned with their safety. Specific gaps in knowledge that call for awareness-raising are identified. Recommendations are made for governments, journalism contributors and sources, news organizations, trainers, corporations and international organizations.

It is underlined that digital security training needs to go beyond technology to empower journalists with knowledge of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity, as well as key resolutions passed within the UN system. Journalists have international backing to be safe to do their work, including in the digital realm.

The holistic approach to training taken by the report also covers the importance of including pyscho-social considerations in any training courses. A chapter on gender in the study assesses how women journalists are especially targeted in the online environment.

Specific issues highlighted in the report include:

Technological, institutional and economic challenges affecting journalists and news organizations

- Surveillance, data storage capabilities and digital attack technologies are becoming less expensive and more pervasive.
- Digital security tools are not always user friendly, leading to too few journalists implementing the tools correctly or at all.
- Commercially available digital security tools may be too expensive for freelancers or bloggers to purchase, and many tools (free or otherwise) are not user friendly for non-technologists.
- Open source digital security tools often lack a sustainable business model, which means they may become obsolete after a short period of time or may not be updated against vulnerabilities.
- Denial-of-Service attacks may result in financial loss for news organizations or individual journalists.
- Many journalists and their sources are unaware of technologists willing and able to assist them if they experience a threat or attack that is digital or digitally-relayed.
- Many journalist and their sources are not adept at understanding data anonymisation or the use of secure technologies such as encryption.
- There is a lack of publicly available data documenting the types of digital attacks and threats that those doing journalism face.
- State and non-state actors can use location-tracking technology to identify media actors – and their sources – who often need confidentiality for the production of journalism.
- The digital security of both those who do journalism and their associates (sources, families, colleagues) can often easily be compromised via phishing campaigns.
- Compromised user accounts and devices can be used to identify the networks of those doing journalism, leading to increased insecurity.
- Digital security is often taught ad-hoc, if taught at all, instead of being systematic and holistic.

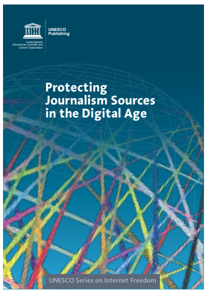
Political and/or legal challenges affecting national governments, UN bodies and intergovernmental organizations, NGOs, and corporations

- Access to journalists' data is sometimes obscured in data protection laws, while other laws are interpreted in ways that can lead to the arrest or detention of journalists for receiving, obtaining or disseminating information, by digital means.
- A lack of political will to address crimes against journalism, including digital crimes, results in a climate of impunity for the perpetrators.
- Unregulated trade in software exploits, advanced surveillance and cyber-attack technologies, can weaken journalists' digital security.
- Trade sanctions can result in reduced availability of technology or software updates needed for those doing digital journalism to stay safe, while conversely the lack of sanctions can also result in exposure to more powerful threats.

Psychosocial challenges affecting journalists, news organizations, journalism schools and other educational and training institutions, and journalist associations

- There is still a low level of appreciation and understanding of digital security principles and tools.
- Decision-fatigue among journalists and other media actors may result in weak application of digital security tools or complete avoidance.
- Digital security training is often not systematized or holistic (e.g. it may exclude operational security and psychosocial care).
- Previous traumatic experiences may result in journalists making bad decisions that lead to greater insecurity.
- Family and friends may unintentionally compromise the digital security of those doing journalism such as by inadvertent disclosures on social media.

COMPANION STUDIES AND USEFUL LINKS


UNESCO Publishing
Protecting Journalism Sources in the Digital Age
UNESCO Series on Internet Freedom

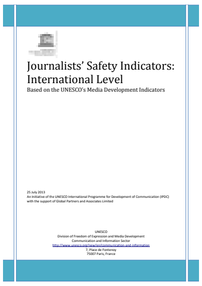
Upcoming:

Protecting Journalism Sources in the Digital Age

The legal frameworks that protect confidential sources of journalism are essential to reporting information in the public interest. However, these frameworks are under significant strain in the digital age, and there's a need to strengthen them. These are the findings of global research, undertaken for UNESCO. Read more about the study, its assessment tool, and gender dimensions of protecting journalism sources on UNESCO's website. This research also formed the foundation for a dedicated chapter in World Trends in Freedom of Expression and Media Development – Special Digital Focus 2015

Countering online hate speech

The study provides a global overview of the dynamics characterizing hate speech online and some of the measures that have been adopted to counteract and mitigate it, highlighting good practices that have emerged at the local and global levels. The publication offers a comprehensive analysis of the international, regional and national normative frameworks, with a particular emphasis on social and non-regulatory mechanisms that can help to counter the production, dissemination and impact of hateful messages online.



Journalists' Safety Indicators: International Level

Based on the UNESCO's Media Development Indicators

Journalists' Safety Indicators

UNESCO's Journalists' Safety Indicators (JSIs) pinpoint significant matters that show, or impact upon, the safety of journalists and the issue of impunity. They allow actors to map key features that can help assess the extent to which journalists are able to carry out their work under safe conditions, and to determine whether adequate follow-up is being given to crimes committed against them. The JSIs serve to identify the actions that are taken by all key stakeholders in promoting journalists' safety and fighting impunity at national and the global level. These actors include the UN, State and political actors, civil society organizations and academics, and media and intermediaries. There is also a handbook for applying the indicators.

World Trends in Freedom of Expression and Media Development:
Special Digital Focus 2015
UNESCO Publishing

World trends in freedom of expression and media development: Special digital focus 2015

The publication explores emerging opportunities and challenges for press freedom in the digital age. With a focus on online hate speech, protection of journalism sources, the role of internet intermediaries in fostering freedom online, and the safety of journalists, the report highlights the importance of new actors in promoting and protecting freedom of expression online and off-line. In a media environment transformed by digital technologies, this special volume in the World Trends series is a key reference for Governments, journalists, media workers, civil society, the private sector, academics and students.

UNESCO and Safety of Journalists

Publications in the UNESCO Series on Internet Freedom

FOR MORE INFORMATION

http://www.unesco.org/new/en/communication-and-information/

While this research was conducted for UNESCO and funded by the Kingdom of Denmark, ideas, opinions and findings are those of the authors, Jennifer R Henrichsen, Michelle Betz and Joanne M Lisosky, they do not necessarily reflect those of UNESCO or the Kingdom of Denmark and do not commit these parties.