Cybersecurity reporting: Human-centric messaging & your guide to cyber hygiene

Workshop

DATE: Thursday 28 October 2021
TIME: 08:00 EST / 14:00 CEST / 16:30 IST / 20:00 SGT (duration 2 hours)
LOCATION: Virtual Event - MS Teams (invitation will be sent via separate email confirmation)

Workshop Objectives:

Reporting on cyberattacks has consequences for all levels of society. Decision-makers, members of the public and industry experts are counting on civil society - such as, independent journalists, watchdogs, and newsrooms - to help explain complex cyber issues and the relevance for people's lives and livelihoods. To contribute to this endeavour, the CyberPeace Institute is facilitating a series of workshops - the first on ransomware - to share knowledge and expertise and identify insights to strengthen human-centric reporting.

This first part of the workshop is a deep-dive opportunity to engage with peers and industry experts highlighting the human-centric approach when reporting on ransomware, insights on current reporting following cyberattacks, providing practical knowledge and skills in relation to ransomware cases and participate in cyber hygiene training.

The second part of the workshop will provide free and effective training and tools to protect data, sources and reputation by industry experts from within the CyberPeace Institute and our partner community. This is an opportunity to increase the cybersecurity posture of journalists and direct them to resources to continue to strengthen their cybersecurity.

In European Cybersecurity Month, the CyberPeace Institute and the Global Cyber Alliance are joining forces to promote cybersecurity and to ensure that we include a human-centric perspective when reporting on cyberattacks.

To RSVP and for further information, please contact Lucy JAY-KENNEDY
Cyber Peace Institute’s Digital Communication Officer ljaykennedy@cyberpeaceinstitute.org

Format and focus of workshops

The workshop has three main objectives:

1. Enabling the diversification of ransomware reporting to include human-centric perspectives.
2. Equipping journalists with practical knowledge and skills to follow ransomware cases in a comprehensive and technically accurate manner.
3. Provide cyber hygiene tools and training to increase the resilience of the participants against cyberattacks.

The workshop is divided into two main parts as described below.

Part I - Reporting Cyberattacks

Part I of the workshop focuses on reporting cyberattacks, and it is divided into two sections. The first one will focus on how to cover and report on cyberattacks more effectively by maintaining the human element as an important equity of reporting. This includes but it is not limited to the language and wording used and the description of how international laws and norms apply.

The second section will focus on reporting trends, and techniques such as ransomware *modus operandi*. This includes the type of methodology used such as simple, double, triple extortion; specific threat actor group; methods of infection; the impact on services and people; crisis management; collection of evidence; recovery of strategies; ransomware negotiations; and the role of cyber-insurance in the to-pay/not-to-pay dilemma of ransomware.

Part II - Resilience Against Cyber Threats

Part II of the workshop will focus on practical training to strengthen journalists' resilience against cyber threats. We will provide a personal cybersecurity training to empower journalists both to better defend themselves from cyber threats, and better report on them. It will focus on journalists' risk profiles; provide an overview of threats against journalists; and produce an infosec/opsec for journalists on how to detect threats (such as phishing email, smishing with ransomware, etc...) and how to react to those threats.

Part II builds on the GCA Cybersecurity Toolkit for Journalists and on the Blueprint for Free Speech. The first one provides free tools, training, and resources for independent journalists, watchdogs, and small newsrooms to bolster their cyber hygiene and protect themselves from online attacks and abuse. During the session, presenters will walk through the features of the toolkit and discuss how these can be best used to best protect yourself, your work, and sources through multi-factor authentication (MFA), password management, and encryption, to cite a few elements.

The second part builds on the Blueprint for Free Speech and delves into the more specific cybersecurity challenges for journalists such as defending a source's identity via technologically-guaranteed anonymity; client-side-encrypted cloud storage of data; circumventing cybercensorship; and help developing-world contacts solve their pirate-software cybersecurity main challenge.

AGENDA

	Speaker	**Focus**
Opening Remarks	**Marietje Schaake**, President, *The CyberPeace Institute*	Policymakers perspective on cybersecurity reporting
Part I Reporting cyberattacks	**Klara Jordan**, Chief Public Policy Officer, *The CyberPeace Institute*	Covering and reporting on cyberattacks while maintaining the human element
	Roxana Radu, Research Associate in Advancement, *The CyberPeace Institute*	
	Bruno Halopeau, Chief Technology Officer, T*he CyberPeace Institute*	Reporting on trends, techniques, and modus operandi
	Bernhard Schneider Cyber Data Analyst, *The CyberPeace Institute*	
Part II Resilience against cyber threats	**Renée McLaughlin**, Toolkit Product Owner, *Global Cyber Alliance*	Personal cybersecurity training
	Anthony Cave, Craig Newmark Journalist Scholar, *Global Cyber Alliance*	
	Eric Johnson, Global cybersecurity-for-journos guru	Cybersecurity challenges for journalists and how to go about it
	Suelette Dreyfus, Founder & Director, *Blueprint for Free Speech*	