INTERNEWS CENTER FOR INNOVATION & LEARNING

DIGITAL SECURITY AND JOURNALISTS




A SnapShot of Awareness and Practice in Pakistan

May 2012

A research report commissioned by
the Internews Center for Innovation & Learning
and produced by Bytes for All, Pakistan

www.bytesforall.pk

Internews

ACKNOWLEDGEMENTS

About Bytes for All

Bytes for All (B4A), Pakistan is a human rights organization with a focus on information and communication technologies (ICTs). It experiments and organizes debate on the relevance of ICTs for sustainable development and strengthening human rights movements in Pakistan.

At the forefront of Internet Rights movement in the country, B4A focuses on capacity building of civil society organizations and human rights defenders on their digital security, online safety & privacy. B4A's ongoing advocacy campaigns are focused on Freedom of Expression especially Internet Freedom, Privacy Rights in Pakistan and Take Back The Tech - women's strategic use of ICTs to end Violence against women & girls.

Bytes for All wishes to acknowledge the support of Internews Pakistan in producing this report.

Internews would like to offer many sincere thanks to everyone who gave generously of their time to share insights and experiences.

Bangkok Regional Team:
Oren Murphy – Regional Director, Asia
Siriporn Tongborrisut – Regional Program Accountant
Kullada Kritsanachaiwanich – Finance Manager
Siriporn Sungkorn – Office Administrator
Dorothy Dai – Program Officer
Sam de Silva- Innovation Advisor, Asia

DC Team:
Kathleen Reen – Vice President for Asia, New Media and Environment
Shannon York – Business Manager

Internews Center for Innovation & Learning:
Mark Frohardt – Executive Director
Amanda Noonan – Director of Research
Eva Constantaras – Program Officer
Ericha Hager – Digital Media Coordinator

CREDITS

Photo credits: ***Cover***: left, Internews; middle, Shahnawaz Tarakzai; right, Mark Edwards/Still Pictures, Internews
Back cover: Mark Edwards/Still Pictures, Internews

Design: Kirsten Ankers, Citrine Sky Design

Photo courtesy of Mark Edwards/Still Pictures/Internews

CONTENTS

EXECUTIVE SUMMARY

Pakistan is among the world's most dangerous places for journalists: threats, assaults, kidnapping and murder are among the everyday dangers reporters face simply for doing their jobs. With law and order further deteriorating in Pakistan, bloggers are now as much at risk as traditional journalists. Given these challenges, in this age of online communications, Pakistani journalists and bloggers need to pay particular attention to digital security.

In December 2011, the Internews Center for Innovation & Learning commissioned the Pakistan-based ICT and human rights organization Bytes for All (B4A) to conduct research to provide a snapshot of the awareness and practice of digital security strategies by the media community in Pakistan. B4A interviewed 37 journalists and 15 bloggers from across the country. Three-quarters of those surveyed had personally experienced a security issue due to their work. However, most of the respondents were unaware of the security risks they face in their online activities, such as email interceptions and data theft. Nor were respondents aware of the widely available strategies and tools that could protect them in the digital space, including using secure email services, encrypting their data, or utilizing IP blocking services that help hide sensitive online activities. This research report aims to highlight areas where journalists and bloggers in Pakistan are particularly vulnerable in their use of digital mediums, and makes some recommendations.

Using a structured interview format, the survey led to the following key findings:

- Though only 1 in 19 Pakistanis uses the Internet (5.2%), Pakistani journalists and bloggers are quite wired: 81% of respondents used the Internet for research in writing a story or blog post.
- Most journalists and bloggers are aware of basic strategies to safeguard their online interactions, such as installing anti-virus software and using strong passwords.
- Respondents were unaware of more sophisticated digital security tools. These include IP blockers, which can be set up to block access to one's website from computers or networks that have certain internet protocol (IP) addresses, such as from particular government entities, and virtual private network (VPN) services, which encrypt and tunnel all data between the user's computer and another computer to minimize interception.
- Only 18.6% of respondents consider security to be the most important feature in an email service.
- Most respondents rate ease of use and ability to customize, rather than security, as the most important features in selecting a blogging or micro-blogging service such as Twitter.
- An overwhelming 90.4% of respondents reported that they have never received any training in how to ensure their digital security.

Additionally, through the interview conversations, the researchers found that some respondents were reluctant to use digital security tools because of perceived costs and a belief that they were complex to use. Also, it was found that journalists and bloggers need a stronger grasp of Pakistani laws on privacy and the right to information, as well as their constitutional rights to freedom of information, speech and expression.

On the basis of these findings, this report strongly points towards the need for proper training for journalists and bloggers in Pakistan, both to educate them about where they are most vulnerable, and to introduce them to the range of available online security tools. Given the dangers that Pakistani journalists risk in using a wide range of online services and digital tools, including email, blogs, micro-blogging and browsers, they urgently need to understand the importance of security relative to other features.

Given that the vast majority of Pakistani journalists and bloggers must contend with threats and concerns regarding their personal safety and job security, it is essential for them to deepen their understanding of digital security and legal rights.

1 INTRODUCTION

Pakistan has undergone drastic internal political and security changes since the start of the United States' "War on Terror." In these times, when it is difficult but essential for citizens to keep abreast of fast-moving developments, the role of Pakistan's journalists and bloggers is more important than ever.

Yet Pakistan is the world's most dangerous country for reporters, according to the Committee to Protect Journalists.[1] In fact, among 66 journalists killed worldwide in 2011, 10 were killed in Pakistan.[2] On a day-to-day-basis, journalists face hardships such as phone tapping, physical surveillance, computer hacking, threats to family and friends, the possibility of losing their jobs, and being exiled. Unfortunately, such repression is conducted not only by radical elements in society, but in some cases by the government itself. Amid Pakistan's deteriorating environment for freedom of speech and expression, not only traditional journalists but also bloggers confront threats to their personal safety and censorship of their writings.

Meanwhile, Internet usage has spread rapidly since its introduction in Pakistan in 1995. In 2000, there were only 0.1 Internet users per 100 inhabitants.[3] By 2009, there were 11.3 Internet users per 100 inhabitants. Currently, Pakistan has about 10 million Internet users out of a population of 190 million. Clearly, Pakistan's usage of digital media is surging, and with that comes an increase in digital threats. For instance, as personal information is made available on social media sites, identity theft will rise. And attempts to infiltrate and steal data from computers that are connected to the Internet will become more sophisticated and more effective. Yet journalists, like the general public, are not very sophisticated with regard to how to use the new online communication tools safely and securely.

Given the security threats to journalists and bloggers as well as their increasing use of digital communications tools, in December 2011, the Internews Center for Innovation & Learning commissioned Bytes for All to conduct a research study on the awareness of online security strategies of journalists and bloggers. Covering the whole country, including the conflict zones, the research study assessed Pakistani journalists' and bloggers' awareness of security and privacy issues related to their online activities and their use of tools and strategies for digital security, with an eye to identifying areas for improvement. Through this research and the development of capacity-building initiatives, it is hoped that the digital security of media professionals and bloggers in Pakistan can be improved.

1 Committee to Protect Journalists, "For journalists, coverage of political unrest proves deadly". http://cpj.org/reports/2011/12/journalists-killed-political-unrest-proves-deadly.php

2 AFP. (2012, January 5). 103 journalists killed in 2011, Pakistan 4th dangerous place: Report. Retrieved January 10, 2012, from The Express Tribune: http://tribune.com.pk/story/316987/103-journalists-killed-in-2011-pakistan-ranks-as-4th-dangerous-place/

3 UN Data. (2009). Country Profile - Pakistan. Retrieved January 2012, from http://data.un.org/CountryProfile.aspx?crName=PAKISTAN

2

METHODOLOGY

The primary research tool was a survey to assess online security perceptions, knowledge and practices of journalists and bloggers in Pakistan (see Appendix I). The research was inspired by a report from Harvard University's Berkman Center for Internet and Society called "Online Security in the Middle East and North Africa: A Survey of Perceptions, Knowledge, Practice."[4] As researchers were interested in comparisons between regions, some of the questions asked in the Pakistan survey were similar to those in the Berkman report.

2.1. Guiding Principles

This research was intended to be used to develop training workshops for journalists and bloggers to address the issues they face in their daily lives regarding online security. This study could also lay the groundwork for more in-depth research on this topic. Following are the guiding principles for this research.

2.1.1. SAMPLE SELECTION

Eighty journalists and bloggers around Pakistan were contacted and asked to participate in this study. Potential respondents were selected using convenience sampling, on the basis of their importance in the media world and the blogosphere. Care was taken to ensure gender, regional diversity, and national scope among participants.

Contact was made through telephone, email and various sources within the journalist community. A total of 52 people (65% of those initially contacted) completed questionnaires. Seventy percent of the respondents were working journalists and the remaining 30% identified themselves as bloggers.

2.1.2. SURVEY QUESTION DESIGN

In designing the survey questions, Internews ensured that the questions asked were relevant to both journalists and bloggers. The same questions were asked from both because the fields are interlinked: most Pakistani journalists maintain blogs, and most bloggers write posts that are at times journalistic.

2.1.3. LANGUAGE

Instead of focusing only on English-language media, journalists from Urdu- and regional language publications were included as well. Respondents had the option of selecting the language in which they could most comfortably interact. Researchers conducted the interviews in English, Urdu, and Pashto.

2.1.4. CROSS-COUNTRY SAMPLING

The researchers conducted cross-country sampling for this research, interviewing journalists and bloggers from around Pakistan to get a diversity of perspectives. Respondents' regions broke down as follows:

Area of Residence	Number of respondents
Punjab	20
Sindh	12
Khyber Pakhtunkhwa	12
Islamabad	8

2.1.5. GENDER BALANCE

The researchers ensured equal representation of male and female respondents for this research, with 26 men and 26 women participating. More detail on the demographics of survey respondents can be found in Appendix II.

2.2. Conducting the Survey Interviews

The survey was primarily administered through face-to-face interviews especially in Khyber Pukhtoonkhwa, FATA & Balochistan to ensure the safety of respondents and prevent

4 Online Security in the Middle East and North Africa: A Survey of Perceptions, Knowledge, and Practice, by Rob Faris, Hal Roberts, Rebekah Heacock, Ethan Zuckerman, and Urs Gasser, Berkman Center, August 2, 2011. http://cyber.law.harvard.edu/node/6974

any kind of possible surveillance on digital communications by authorities. In urban centers, where respondents could not meet in person due to different reasons like job restrictions or time issues, interviews were conducted via Voice over IP (VoIP) services, such as Skype, or by email. The security of respondents was given priority in the process, and the means of the interview was selected after consultation with them to ensure the safest and convenient way of communication. In order to promote dialogue instead of a flat question-and-answer session, respondents were encouraged to ask questions at any point during the interview.

Each interview took between 20 to 25 minutes, while a few ran for more than one hour as participants warmed to the subject. In such cases, they provided valuable in-depth perspectives on the survey topics. The research team for this study was trained in digital security, online tools and platforms through an intensive week-long training conducted by Bytes for All, Pakistan in collaboration with Tactical Technology Collective. The Internews Center for Innovation & Learning held several meetings with the researchers throughout the course of this study to coordinate the research effort.

Photo courtesy of Shahnawaz Tarakzai

3

USE OF DIGITAL TECHNOLOGY IN JOURNALISTS' WORK

When researchers asked participating journalists and bloggers about the use of technology in their work, it was apparent respondents are very wired. Nearly all use desktop or laptop computers and most use mobile phones and social networking websites in their day-to-day work. Over 90% use the Internet in the course of their professional duties, and most of those use it for story research.

3.1. Usage of Internet for Research

Nearly 81% of respondents use the Internet for story research, with over half reporting heavy use, as below.

Using the Internet for Story Research	%
No use	0.0
Low use	17.3
Moderate use	26.9
Heavy use	53.8

3.2. Social Media Usage

In researching, distributing or writing a story, respondents reported that Facebook, YouTube and Twitter were their three most used social media platforms. Fewer than 5% chose Google+, Flickr or Orkut. Facebook is without a doubt the most popular social networking website, with 75% of respondents using it to a moderate or heavy extent, followed by YouTube at 63.5% and then Twitter with 51.9%.

Social Media	Facebook %	YouTube %	Twitter %
No use	13.5	36.5	48.1
Low use	11.5	0.0	0.0
Moderate use	32.7	50	19.2
Heavy use	42.3	13.5	32.7

3.3. Email Provider Preference

When asked which email service they use for their work communications, 76.9% of respondents reported using Gmail. This was an encouraging result, because Gmail is relatively secure compared to other email service providers like Hotmail and Yahoo. Very few respondents use their company's private email services. According to some respondents, they prefer using Gmail even though their company provides them with an exclusive email address.

Email service	%
Gmail	76.9
Hotmail	13.5
Company email	7.7
Yahoo	5.8

Survey participants were asked what features are most important to them in selecting an email service. The results clearly explain the preference for Gmail. The largest group of respondents (49.2%) replied that 'storage space' is the most important feature for them in an email service. Gmail offers around 7.5 gigabytes (GB) of free space. The second most important feature for respondents was 'ease of use.'

Only 18.6% of those polled considered 'security' to be the most important feature for them to have in an email service. While this figure is relatively high compared to other countries, the authors of this report are concerned that journalists and bloggers, professions that face special security threats, do not take their digital security as seriously as they should.

Features you look for while selecting an email service	%
Security	18.6
Storage space	49.2
Ease of use	30.5
Any other	0.0

3.4. Awareness of Secure Email Features

The majority of respondents (60%) were unaware of the existence of secure email features, such as point-to-point encryption, where emails sent to and received from the respondent's computer to email providers' servers are encrypted using the secure sockets layer (SSL) protocol. Google's email client, Gmail, provides this feature; however the survey responses suggest that a majority of users are not fully aware of this.

3.5 Blogging and Micro-blogging Provider Preference

Most respondents rated either 'ease of use' (39.1%) or 'ability to customize' (34.8%) as the most important feature in selecting a blogging or micro-blogging service such as Twitter. 'Popularity' was another top consideration. Once again, as with email service selection, 'security/privacy' was not much of a factor: only 6.5% respondents said that they make the security features of a particular blogging or micro-blogging portal their first priority in making their decision.

Feature you look for in selecting blogging service	%
Popularity	10.9
Design/Appearance	8.7
Ability to customize	34.8
Costs	0.0
Security/Privacy	6.5
Ease of use	39.1
Any other	0.0

4

GROWING RISKS OF ONLINE ACTIVITY

To understand the risks associated with respondents' online activity, Bytes for All asked what they thought were the looming threats for journalist and blogger communities in general. They were also asked about their personal experiences with online security.

4.1. Personal Security – the Greatest Threat

The largest group of respondents (40.7%) said that 'being personally threatened' was the biggest danger faced by the journalist and blogger community in Pakistan. 15.4% respondents said that 'being sacked or demoted at work' was the most significant threat journalists face.

Threats faced by journalists/bloggers	%
Being arrested by authorities	9.9
Being personally threatened	40.7
Having their identities exposed against their wishes	5.5
Having their websites hacked or attacked	5.5
Having their emails intercepted or data stolen	7.7
Having their friends or family threatened	9.9
Being sacked, demoted or reprimanded at work	15.4
Having their publications attacked or site hacked	3.3
Don't know	2.2

Very few respondents selected security issues such as 'having their emails intercepted or data stolen', 'having their websites attacked or hacked' or 'having their identities exposed against their wishes.' While physical security is the primary concern, more work needs to be done to understand how digital security breaches and email interceptions can threaten their physical safety.

When asked whether their work as a journalist or blogger had caused them any security concern, most respondents (73.1%) said it had.

Has your work as a journalist/blogger ever caused you any security concern?	%
Yes	73.1
No	25.0
Don't know	1.9

Asked to specify what they meant by security concern, the majority of respondents (59.7%) replied 'personal safety', followed by 'security of family' and 'security of information.'

If yes, what types of issues are of concern to you?	%
Personal safety	59.7
Security of information	11.3
Security of people I work with	9.7
Security of informants	6.5
Security of family	12.9
Others	0.0
Don't know	0.0

5 KNOWLEDGE OF SECURITY

Survey participants were asked questions to understand their awareness of online security and their familiarity with digital security tools and strategies.

5.1. High Concern, Low Awareness of Tools

There are a range of online platforms and strategies to increase the security of information and individuals. When asked, the majority of survey respondents (55.8%) replied that they were aware of strategies and platforms to keep them safe online. This result was surprising because earlier questions indicated that respondents were not particularly concerned about the security aspects of their online activity.

Security strategy awareness	%
Yes	55.8
No	44.2
Don't know	0.0

To solve this enigma, respondents were given a list of the most important digital security strategies and asked which strategy they had used in the past to secure their online interactions.

If yes, which of the following have you heard of?	%
Using strong passwords	27.0
Encrypting data	8.0
Using anti-virus software	27.0
Keeping your operating system updated	17.0
Using IP disguisers/blockers	8.0
Using anti-censorship software	6.0
Using a VPN	7.0
Other	0.0

The results proved researchers' suspicions. Those respondents who said they were aware of security tools and platforms for their online interactions mainly had heard of basic strategies like 'using anti-virus software' (27%) and 'strong passwords' (27%). Another 17% replied that keeping their operating system updated was a security technique they knew of. Only 8% or fewer indicated they were familiar with encryption, IP disguisers/blockers that conceal the computer or internet connection conducting online activities, anti-censorship software or Virtual Private Networks (VPN) that give access to censored sites.

Respondents were asked which strategies they use in their day-to-day life to safeguard their online interactions. In addition to the list above, this question included three other strategies. This is how they replied:

Which of the following digital security strategies do you use?	%
Using strong passwords	29.7
Encrypting data	2.8
Using anti-virus software	31.7
Keeping your operating system updated	11.0
Using IP disguisers/blockers	2.8
Using anti-censorship software	1.4
Using a VPN	0.7
Firewall protection	6.9
Safe deletion of data	5.5
Secure backups to prevent any information loss	7.6
Other	0.0

The majority of respondents reported using 'anti-virus software' and 'strong passwords' to safeguard themselves online. Eleven percent said they update their operating system regularly. Almost no participants selected more sophisticated options such as using anti-censorship software or VPNs to safeguard their browsing.

6

ONLINE SECURITY PERCEPTION

Survey participants rated several digital security techniques to indicate how secure they thought each was.

	Strong password %	Encryption %	Anti-virus %	System updating %	IP blocker %	Anti-censorship %	VPN %
Don't know	1.9	75.0	5.8	44.2	80.8	88.5	88.5
Not secure	3.8	0.0	9.6	7.7	1.9	3.8	0.0
Moderately secure	80.8	17.3	76.9	42.3	11.5	5.8	7.7
Totally secure	13.5	7.7	7.7	5.8	5.8	1.9	3.8

The table above explains where the problem lies. Respondents believed that strong passwords and anti-virus software were moderately secure tools to safeguard against online threats, but most said they did not know about the level of security offered by the much more powerful tools of encryption, IP blocking, anti-censorship tools, or VPNs. These findings indicate that journalists' and bloggers' weak digital security practices stem from lack of awareness, and could be improved with appropriate training.

Another important conclusion one can draw from the data is that, since respondents do in fact use the security tools they are aware of, such as anti-virus software, strong passwords, and system updating, they appear willing to put security knowledge into practice once they have the information they need.

7 TRAINING EXPERIENCE

A brief set of questions was asked to gauge the level of training the respondents have had. Considering that it is literally the most lifesaving skill, the respondents were first asked if they had received any physical safety training for journalists. Nearly three-quarters had never had such training.

Training (journalist safety training)	%
Yes – in the last 12 months	25.0
Yes – over 12 months ago	1.9
No	73.1

When asked about digital security training, the response was even more one-sided. An overwhelming 90.4% of our respondents said that they never received any such training. Digital threats, and the strategies to combat them, are evolving daily, but only 7.7% respondents had any digital security training in the previous year.

Training (Digital security)	%
Yes – in the last 12 months	7.7
Yes – over 12 months ago	1.9
No	90.4

Securing data residing on computers and mobile devices is as important as protecting data as it goes over the Internet. Yet fewer than 10% of the respondents said they had adequate knowledge of how to secure data on their computers and mobile devices.

When asked about how they ensure retention of copyright and prevent plagiarism of their visual work, such as photos and videos, once again respondents were unaware of technologies that can facilitate this, such as watermarks, digital signatures, patenting and digital copyrighting. Less than 10% said that they use any tool to ensure copyright of their visual work.

8

ADDITIONAL POINTS

Several observations were made by respondents that were not covered in the questionnaire. Here are the important points from those discussions.

- Some respondents were reluctant to use advanced security tools because they thought that these tools were complex and difficult to use.
- Journalists and bloggers complained about the absence of cybercrime laws in Pakistan, citing this as a reason for many such security breaches.
- Many respondents said that they were aware of the concept of anonymous blogging, in which a writer can keep their identity hidden. However, they felt they required more information to be convinced that they could blog without revealing their identities.
- Many bloggers complained about the Pakistan Telecommunication Authority's (PTA) practice of banning any blog or website that hosts any even remotely anti-government views. They mentioned the example of a Baloch newspaper/blog that is not accessible in Pakistan due to a ban imposed by PTA.
- Journalists writing for Urdu- and regional language newspapers face more technical challenges than others. A respondent who writes for a leading Urdu newspaper, complained that even after many requests, the publication was not willing to arrange any computer training for their reporters.
- Some journalists said that they believed in the idea of 'open source' and sharing stories, and didn't think there was any need to copyright or prevent their material from being published online; instead, they encourage others to use it. Such journalists might benefit from an introduction to Creative Commons licenses, which enable stories to be distributed and shared, while protecting the rights of the journalist.
- Journalists and bloggers were not very familiar with Pakistan's Freedom of Information Act and other legal provisions that could be helpful to them.
- Many respondents requested training in online security.

Photo courtesy of Mark Edwards/Still Pictures/Internews

9 CONCLUSION AND RECOMMENDATIONS

The survey showed that Pakistani journalists and bloggers use the Internet heavily for research, email, social networking and distribution of their work. But they appear to have very little awareness of how to ensure their digital security

The majority of respondents were unfamiliar with tools such as secure email services, encrypting their communication, or IP blocking software, and they did not prioritize digital security considerations when choosing an email provider or blogging platform.

In fact, there is limited awareness of what even constitutes digital security—many respondents seemed to believe that digital security only meant keeping their computer safe from Internet viruses, and could be accomplished simply by using good anti-virus software. While it is important to use anti-virus software, there is a need to broaden the awareness of digital threats and digital security..

On the basis of this research, the following recommendations are made:

- As the majority of journalists and bloggers in the survey reported that they have experienced some security concerns, they urgently need to understand how their online activities can threaten their personal safety as well as the security of their sources.
- Digital security training for the journalist and blogger communities in Pakistan should introduce participants to various security tools and platforms available online, including encryption, IP blockers, VPNs, anti-censorship software and other security tools, with an emphasis on how they can serve journalists and bloggers.
- Such training should stress the importance of security in selecting email, blogging and micro-blogging services.
- Journalists and bloggers also need training in how and why to maximize mobile phone security, so that interviews, photos or videos recorded using these devices, or sensitive data such as sources and contact information, may remain secure if a reporter's phone is lost or stolen.
- It would also be very helpful for journalists and bloggers to learn more about Pakistan's privacy laws and constitutional rights regarding freedom of information, speech and expression.
- Special attention should be paid to training reporters for Urdu- and regional language newspapers, as they tend to be the most technologically challenged and least able to take advantage of digital technologies and security tools.

While no amount of digital security knowledge can deter all attacks, using some of the available online tools and strategies can help make Pakistan's journalists and bloggers, their families, and their sources considerably more secure. In a dangerous and fluid security environment, every extra measure of safety will help free these professionals to do their vital work safely and effectively.

APPENDIX I – RESEARCH QUESTIONNAIRE

Secure Journalist

The 'secure journalist' research aims to better understand the perceptions, awareness of digital security and the challenges and opportunities to mainstreaming digital security knowledge and practices for media and blogosphere in Pakistan.

BACKGROUND – YOUR WORK

1.1 How would you describe your current occupation?

- ☐ Freelancer (paid per story)
- ☐ Staff Journalist (paid a salary)
- ☐ Professional Blogger
- ☐ Citizen Journalist / Blogger (voluntary / not paid)
- ☐ Other _____

1.2 Please describe the type of stories you primarily cover:

- ☐ Politics and Governance
- ☐ Security and Crime
- ☐ Accidents and Disasters
- ☐ Human Rights (including women, children, minority and LGBT rights)
- ☐ Health
- ☐ Education
- ☐ Business
- ☐ Arts and Entertainment
- ☐ Technology and Innovation
- ☐ Religion and Culture
- ☐ Sports
- ☐ Others (please specify) _____

1.3 Which technologies and tools do you use in your work?

- ☐ Desktop PC
- ☐ Laptops/Tablets
- ☐ Mobile Phones
- ☐ Email and collaborative tools (eg. Google Docs)
- ☐ Internet
- ☐ Networking websites (Facebook, LinkedIn etc.)
- ☐ GPS
- ☐ Video/Audio recording devices
- ☐ Others (please specify)

1.4 Do you use the web for research when writing a story (1 = no use, 5 = heavy use)

Web usage for research: No Use 1 – 2 – 3 – 4 – 5 Heavy Use

1.5 Do you use email when writing a story? For example, do you correspond with interview subjects / informants via email? (1 = no use, 5 = heavy use)

- ☐ Researching the story: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Organizing Interviews: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Interviewing subjects: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Liaising with the media outlet: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Discussing the story with colleagues: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Distributing the story: No Use 1 – 2 – 3 – 4 – 5 Heavy Use

1.6 Which email service are you using for your work related interactions?

- ☐ Gmail
- ☐ Hotmail
- ☐ Yahoo
- ☐ Organization's private email account
- ☐ Blackberry
- ☐ Any other _____

1.7 Are you aware of secure email services?

- ☐ Yes
- ☐ No

1.8 Do you use social networking platforms such as Facebook, Twitter, etc. when researching, distributing, writing a story? (1 = no use, 5 = heavy use)

- ☐ Facebook: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ YouTube: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Twitter: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Google+: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Flickr: No Use 1 – 2 – 3 – 4 – 5 Heavy Use
- ☐ Orkut: No Use 1 – 2 – 3 – 4 – 5 Heavy Use

YOUR EXPERIENCE

2.1 Does your journalism/blogging include meeting 'sensitive' contacts/informants?

- ☐ Yes
- ☐ No
- ☐ Don't Know

2.2 Does your journalism/blogging include meeting individuals or organizations that may be wanted by authorities/gangs/criminals?

- ☐ Yes
- ☐ No
- ☐ Don't Know

2.3 Which of the following do you think is the biggest threat facing journalists and bloggers? (Check-box)

- ☐ Being arrested or detained by authorities
- ☐ Being personally threatened
- ☐ Having their identities exposed against their wishes
- ☐ Having their websites hacked or attacked.
- ☐ Having their emails intercepted or data stolen
- ☐ Having their friends or family threatened
- ☐ Being sacked, demoted or reprimanded at work
- ☐ Having their publications attacked or publication site hacked
- ☐ Others: _____
- ☐ Don't know
- ☐ No reply

2.4. Has your work as a journalist/blogger ever caused you any security concern?

- ☐ Yes
- ☐ No
- ☐ Don't know

2.4.1. If yes, what types of issues are of concern to you?

- ☐ Personal safety
- ☐ Security of information
- ☐ Security of people I work with
- ☐ Security of informants
- ☐ Security of family
- ☐ Others
- ☐ Don't know

2.5. In the past 12 months, have you experienced any negative consequences due to your journalism/blogging activities?

- ☐ Yes
- ☐ No
- ☐ Don't Know

2.5.1. If yes, please select what is relevant from below:

- ☐ I was personally threatened
- ☐ I was threatened by email
- ☐ I was threatened by SMS
- ☐ I was physically attacked
- ☐ My friends or family were threatened
- ☐ I was arrested or detained
- ☐ My computer got a computer virus and my data was affected
- ☐ My identity was exposed against my wishes
- ☐ I was sacked, demoted or reprimanded at work
- ☐ My publication, website or blog was attacked or hacked
- ☐ I had my emails intercepted or data stolen
- ☐ Any other _____

KNOWLEDGE OF SECURITY

3.1 Do you click on any web links contained in an email message:

If the sender is unknown?

- ☐ Never
- ☐ Sometimes
- ☐ Yes
- ☐ Yes, but only after checking the link location
- ☐ Don't know

If the sender is known?

- ☐ Never
- ☐ Sometimes
- ☐ Yes
- ☐ Yes, but only after checking the link location
- ☐ Don't know

3.2. There are a range of ways to increase the security of information and individuals using online platforms and tools. Do you know of any such methods?

- ☐ Yes
- ☐ No
- ☐ Don't know

3.2.1. If yes, which of the following have you heard of?

- ☐ Using strong passwords for your email or other Internet accounts
- ☐ Encrypting data
- ☐ Using anti-virus software
- ☐ Keeping your operating system updated with the latest security patches and updates
- ☐ Using IP disguisers/blockers
- ☐ Using anti-censorship software
- ☐ Using a VPN
- ☐ Other: _____

3.3. What is the most important feature you look for while selecting an email service?

- ☐ Security
- ☐ Storage space
- ☐ Ease of use
- ☐ Any other: _____

3.4. What is the most important feature you look for while selecting a blogging or micro-blogging service?

- ☐ Popularity
- ☐ Design/Appearance
- ☐ Ability to customize
- ☐ Costs
- ☐ Security/Privacy
- ☐ Ease of use
- ☐ Any other: _____

3.5. Have you heard about the concept of Anonymous Blogging?

- ☐ Yes, I use it
- ☐ Yes, but I've never used it
- ☐ No

3.6. Which of the following tools of digital security do you use?

- ☐ Using strong passwords for your email or other Internet accounts
- ☐ Encrypting data
- ☐ Using anti-virus software
- ☐ Keeping your operating system updated with the latest security patches and updates
- ☐ Using IP disguisers/blockers
- ☐ Using anti-censorship software
- ☐ Using a VPN
- ☐ Firewall protection
- ☐ Safe deletion of data
- ☐ Secure backups to prevent any information loss
- ☐ Other: _____

3.7. Please indicate the level of digital security you believe is offered by each of the following strategies.

Using strong passwords for your email or other Internet accounts
1. Don't know – 2. Not secure – 3. Somewhat insecure – 4. Somewhat secure – 5. Totally secure

Encrypting data
1. Don't know – 2. Not secure – 3. Somewhat insecure – 4. Somewhat secure – 5. Totally secure

Using anti-virus software
1. Don't know – 2. Not secure – 3. Somewhat insecure – 4. Somewhat secure – 5. Totally secure

Keeping your operating system updated with the latest security patches and updates
1. Don't know – 2. Not secure – 3. Somewhat insecure – 4. Somewhat secure – 5. Totally secure

Using IP disguisers/blockers
1. Don't know – 2. Not secure – 3. Somewhat insecure – 4. Somewhat secure – 5. Totally secure

Using anti-censorship software
1. Don't know – 2. Not secure – 3. Somewhat insecure – 4. Somewhat secure – 5. Totally secure

Using a VPN
1. Don't know – 2. Not secure – 3. Somewhat insecure – 4. Somewhat secure – 5. Totally secure

3.8. How do you ensure the retention of copyrights and prevention of plagiarism of your visual works (photography etc.)?

- ☐ Watermarks
- ☐ Digital signatures
- ☐ Patenting
- ☐ Secure publishing
- ☐ Any other _____

3.9. What security tools do you use to secure the data on your computer and mobile phone?

- ☐ Password protection
- ☐ Safe deletion of data
- ☐ Securing the data in external drives
- ☐ Encryption
- ☐ Any other _____

TRAINING

4.1 Have you participated in any safety training courses that teach journalists how to stay safe in the field, and often include first-aid training?

- ☐ Yes – in the last 12 months
- ☐ Yes – but it was over 12 months ago
- ☐ No

4.2 Have you participated in any digital security training courses which taught you how to use the Internet securely and how to protect your data?

- ☐ Yes – in the last 12 months
- ☐ Yes – but it was over 12 months ago
- ☐ No

4.2.1 If yes, which of the following did you learn, and how effective was the training? (not effective 1 – 2 – 3 – 4 – 5 very effective)

- ☐ Password security: not effective 1 – 2 – 3 – 4 – 5 very effective
- ☐ Encrypting data: not effective 1 – 2 – 3 – 4 – 5 very effective
- ☐ Using anti-virus software: not effective 1 – 2 – 3 – 4 – 5 very effective
- ☐ Keeping your operating system updated with the latest security patches and updates: not effective 1 – 2 – 3 – 4 – 5 very effective
- ☐ Using IP disguisers/blockers: not effective 1 – 2 – 3 – 4 – 5 very effective
- ☐ Using anti-censorship software: not effective 1 – 2 – 3 – 4 – 5 very effective
- ☐ Using aVPN: not effective 1 – 2 – 3 – 4 – 5 very effective

4.2.2 What was most relevant to you in terms of learning? (Choose only one)

- ☐ Using strong passwords for your email or other internet accounts
- ☐ Encrypting data
- ☐ Using anti-virus software
- ☐ Keeping your operating system updated with the latest security patches and updates
- ☐ Using IP disguisers/blockers
- ☐ Using anti-censorship software
- ☐ Using a VPN

4.3. Please indicate (narrative) the training needs in terms of digital security for your geographic area?

_____

_____

_____

_____

_____

_____

_____

_____

BACKGROUND INFORMATION OF RESPONDENT

Name _____

Age _____

Sex _____

Institution _____

Education_____

Position _____

Contact information_____

Years in current institution _____

Statement of Confidentiality: You are hereby assured that any information that you provide shall remain confidential, and usage of the same shall be for research purposes only.

ABOUT THE INTERNEWS CENTER FOR INNOVATION & LEARNING

The Internews Center for Innovation & Learning supports, captures, and shares innovative approaches to communication through a creative program of research and development worldwide. Founded in 2011, the Center seeks to strike a balance between local expertise and needs and global learning in order to develop a comprehensive approach to understanding and catalyzing information exchange.

In Internews' 30-year history of promoting independent media in more than 75 countries around the world, the last five years have arguably seen the most changes in the global media and journalism environment. Across all Internews programs, adoption of cutting-edge technology is integral to advancing the work of the journalists, bloggers, citizen reporters, schol¬ars and others who provide a vital interpretive role for their communities. The Internews Center for Innovation & Learning deepens and enhances our capacity to link existing expertise to research that helps define, understand and monitor the critical elements of changing information ecosystems and to pilot projects that apply and test the data, platforms and digital tools to meet information needs of specific communities. This is far from a solo endeavor. A network of partners, ranging from technologists to academics to activists is critical to creating and sustaining a dynamic and iterative collabora¬tive space for innovation. For more information visit http://innovation.internews.org.

Internews Washington, DC Office
1640 Rhode Island Ave. NW Suite 700
Washington, DC 20036 USA
+ 1 202 833 5740

Internews Administrative Headquarters
PO Box 4448
Arcata, CA 95518 USA
+1 707 826 2030

www.internews.org
E-mail: info@internews.org
Twitter: @internews
facebook.com/internews

Internews is an international non-profit organization whose mission is to empower local media worldwide to give people the news and information they need, the ability to connect and the means to make their voices heard.

Internews provides communities the resources to produce local news and information with integrity and independence. With global expertise and reach, Internews trains both media professionals and citizen journalists, introduces innovative media solutions, increases coverage of vital issues and helps establish policies needed for open access to information.

Internews programs create platforms for dialogue and enable informed debate, which bring about social and economic progress.

Internews' commitment to research and evaluation creates effective and sustainable programs, even in the most challenging environments.

Formed in 1982, Internews is a 501(c)(3) organization headquartered in California. Internews has worked in more than 75 countries, and currently has offices in Africa, Asia, Europe, the Middle East, Latin America and North America.

Internews
Center for Innovation
& Learning