Digital and Mobile Security for Mexican Journalists and Bloggers

Results of a survey of Mexican journalists and bloggers

Prepared by Jorge Luis Sierra
ICFJ Knight International Journalism Fellow

FREEDOM HOUSE

ICFJ International Center for Journalists
Advancing Quality Journalism Worldwide
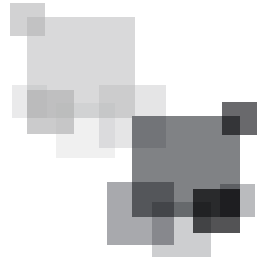
Results of a survey of Mexican journalists and bloggers

Prepared by Jorge Luis Sierra
ICFJ Knight International Journalism Fellow

SUMMARY

A new survey of 102 journalists and bloggers in 20 Mexican states shows nearly 70 percent have been threatened or have suffered attacks because of their work. In addition, 96 percent say they know of colleagues who have been attacked. Respondents to the survey also say they view cyber-espionage and email-account cracking as the most serious digital risks they face. And while nearly all have access to and rely on the Internet, social networks, mobile phones and blogging platforms for their work, they also admit that they have little or no command of digital security tools such as encryption, use of virtual private networks (VPNs), anonymous Internet navigation and secure file removal. The results of this survey show the urgent need to introduce Mexican journalists and bloggers to new technologies and protocols and help newsrooms develop a culture of digital-security awareness to counter increasingly sophisticated threats and attacks from both governmental agencies and criminal organizations.

INTRODUCTION

Advances in computer and mobile technology, the expansion of the Internet and the development of social networks and digital tools have removed many geographic, social and political barriers to the exchange of news and information. At the same time, these developments have created new areas of vulnerability for media professionals and bloggers who often are not fully aware of how these new technologies can threaten their privacy and security.

This is particularly true in countries where citizens face major security challenges such as organized crime groups and corrupt officials. In Mexico in particular, digital and mobile insecurity has become a new and uncontrolled source of danger to the physical and psychological safety of independent journalists and bloggers alike.

In September 2011, two bloggers who reported frequently about local crime – particularly violent incidents related to drug trafficking – were found hanged from a pedestrian bridge in Nuevo Laredo. This city is the turf of the Zetas, one of Mexico's most active and dangerous criminal organizations. A message left near the bodies warned that the same thing could happen to any Internet user who crossed that criminal organization. Those murders were followed by the killing of a journalist using the nickname "la Nena de Laredo" (the Baby of Laredo) who had posted entries against criminal activity on Nuevo Laredo en Vivo, a social media forum.

Professional journalists also are at risk. In June 2012, Victor Manuel Baez, an editor working for reporterospoliciacos.mx, a website covering crime in Veracruz, was kidnapped when he left his office in that city. He was found dead hours later. A reporter working in the southern state of Michoacán

says members of a criminal organization are sending threatening text messages to his phone in an effort to force him to become a public relations officer for them.

These events are among the most extreme attacks so far by criminal elements against journalists and bloggers in Mexico. There also have been incidents involving official surveillance of Twitter users who were suspected of terrorism. In September 2011, the state of Veracruz initiated a terrorism case against two Twitter users, accusing them of spreading rumors about a school attack. Two months later, the Mexican Federal Police arrested a Twitter user because he posted a comment about "flying officials" minutes before the Interior minister died in an airplane crash in Mexico City. Reporters investigating corruption and human rights abuses in Chiapas, where government forces have intermittently battled guerrillas since the 1990s, say they have been under continuous electronic surveillance over the last two years.

These events indicate that both officials and criminal organizations monitor social networks to see what journalists and bloggers post, often responding to stories and information they don't like with harassment, threats or violence.

Given the level of insecurity surrounding the use of digital and mobile technology by journalists and bloggers, protection of users' identity and privacy is now crucial, particularly when citizens and journalists use online platforms, social networks and mobile devices to post comments or reports about crime, corruption or violence.

With this in mind, a group of journalists and bloggers who cover human rights issues, crime, corruption and the impact of state activities against criminal groups were surveyed to see if they understand the risks and threats they face when using digital and mobile technology. The goal: to develop simple protocols and identify the best tools to help them better protect themselves so they can continue to serve the public interest. The survey asked questions such as:

- How do you rate your ability to use digital and mobile tools?
- How do you rate your ability to use risk-reduction tools and strategies when working on computers, using cellular phones or navigating the Web?
- How much do you mix personal information with professional activity when using social networks like Facebook or Twitter?
- How vulnerable do you think you are to physical and digital risks and threats?
- Have you been threatened or attacked because of your professional online/mobile activity?

The information generated by this survey will help improve training programs for bloggers and journalists so they can be more aware of digital and mobile risks and the need to use security tools, protocols and strategies to reduce those risks as they pursue investigative stories.

METHODOLOGY

The Knight International Journalism Fellow designed and distributed a 21-question electronic survey to a group of trusted journalists, bloggers and human rights activists in Mexico. All of the participants use computers, the Internet and an array of digital tools and mobile devices to report on crime, corruption, violence and human rights issues. More than half say they cover corruption, victims of violence, abuses by authorities and human rights issues. Ten percent report on drug trafficking. Coverage of these sensitive topics makes those journalists and bloggers even more vulnerable to electronic surveillance and other digital attacks.

Journalism organizations and networks, human rights groups and independent journalists helped to generate the list of journalists and bloggers for the survey. In October and November 2012, an electronic link to the survey was distributed to networks of journalists, particularly in the Mexican states most affected by drug violence and where journalists and bloggers have been under stress due to a wave of murders, kidnappings, physical attacks and death threats.

The results of this survey are not a statistical representation of the general state of security for journalists in Mexico. However, they offer quantitative evidence of the digital and mobile vulnerability of journalists and bloggers working in high-risk areas of Mexico.

SURVEY PARTICIPANTS PER STATE AND SEX
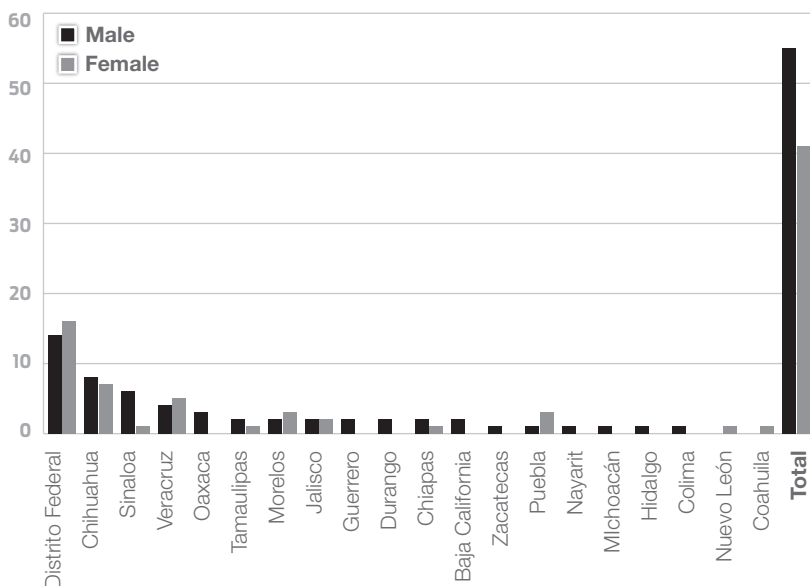
The selected group is representative of professional journalists and bloggers who regularly use digital and mobile tools and are deeply involved in adapting to one of the most dangerous reporting environments in the world. Some of them have participated in the "Cobertura Segura" course, a program organized by ICFJ and the University of Guadalajara, to train journalists to use a combination of risk-reduction strategies and auto-protection protocols.
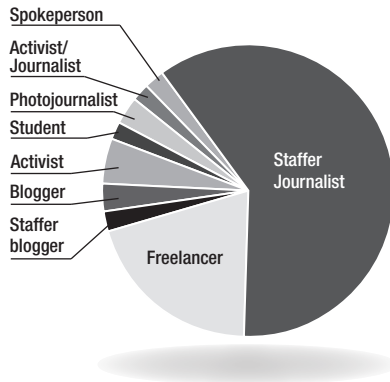
The results of this evaluation will be used to design an online course and in-person workshop to train participants to develop and use digital and mobile risk-reduction strategies and protocols.

A total of 102 journalists and bloggers from 20 Mexican states, including the Federal District of Mexico (Mexico City), responded to the survey. Forty percent of the respondents were female.

Almost 80 percent of the answers came from participants who received a direct invitation to participate in the survey via electronic mail. Twelve percent of the answers came from participants invited through a Facebook group. The rest of the answers were obtained from invitations sent by Twitter and in person.

Nearly 60 percent of the participants are staff journalists working for media organizations. Another 23 percent are freelancers. More than 5 percent of the respondents are bloggers, 7 percent are human rights activists and 5 percent are students.

POSITION

Spokeperson
Activist/Journalist
Photojournalist
Student
Activist
Blogger
Staffer blogger
Freelancer
Staffer Journalist

RESULTS

PHYSICAL RISKS

Almost 70 percent say they have been threatened or been the victim of an attack as a journalist or blogger. More than 20 percent say they have been threatened or attacked recently. Nearly 10 percent of all participants say they recently were attacked physically. Thirty percent of respondents, half of them working in Mexico City, said they have never been attacked, which signals that journalists and bloggers working in Mexico City are relatively safer than those working in other areas of Mexico. Even so, half of the 32 participants from Mexico City say they have been threatened or attacked.
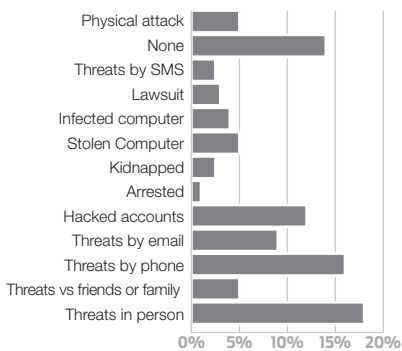
Twenty-seven percent say physical threats are the most serious risk for journalists and bloggers in their communities. Eleven percent see lawsuits and murders as the biggest risks.

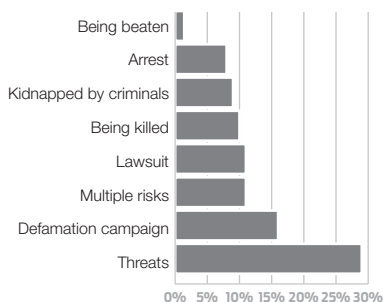Personal and family security are the two biggest concerns for those

surveyed, while 11 percent think information security and the safety of colleagues are the most important concerns.

Forty-nine percent report that they, their friends or family members have received threats.

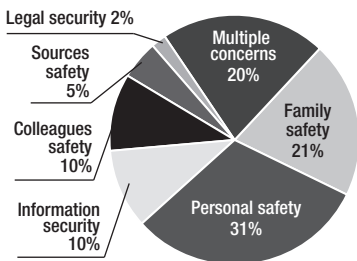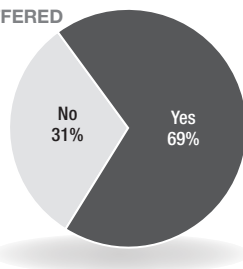**TYPES OF ATTACKS YOU HAVE SUFFERED**

Category	
Physical attack	
None	
Threats by SMS	
Lawsuit	
Infected computer	
Stolen Computer	
Kidnapped	
Arrested	
Hacked accounts	
Threats by email	
Threats by phone	
Threats vs friends or family	
Threats in person	

0%   5%   10%   15%   20%

BIGGEST PHYSICAL RISK

Category	
Being beaten	
Arrest	
Kidnapped by criminals	
Being killed	
Lawsuit	
Multiple risks	
Defamation campaign	
Threats	

0%   5%   10% 15% 20% 25% 30%

None of the respondents claimed they face a risk of extortion.

MAIN SECURITY CONCERNS

Legal security 2%
Sources safety 5%
Colleagues safety 10%
Information security 10%
Multiple concerns 20%
Family safety 21%
Personal safety 31%

HAVE YOU SUFFERED THREATS OR ATTACKS?

No 31%
Yes 69%

FRECUENCY OF THREATS OR ATTACKS

| Category	
Never	
Long time ago	
Recently	
Often	
Often and Recently	

0%   5% 10% 15% 20% 25% 30% 35% 40%
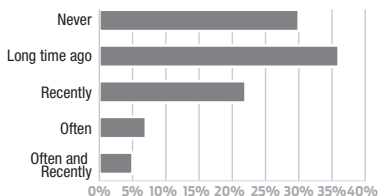
The perception of risk is high due to past experiences in their communities. More than 95 percent of respondents say that other colleagues in their communities have been attacked. Thirty percent say their colleagues were frequently and recently attacked.

HAVE YOUR COLLEAGUES BEEN THREATENED OR ATTACKED?

Yes 96%
No 4%

HAVE YOUR COLLEAGUES BEEN THREATENED OR ATTACKED?

Recently 29%
Often 25%
Never 4%
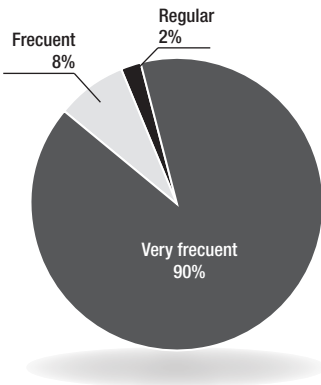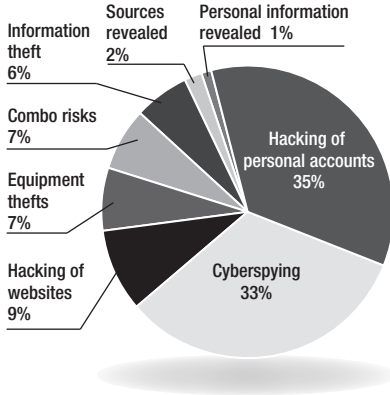Long time ago 24%
Often and recently 18%
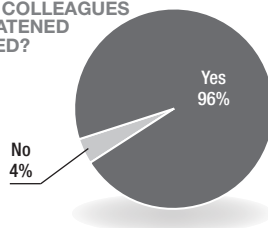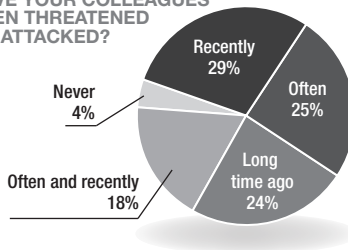
DIGITAL RISKS

Participants say cyber-espionage and email-account cracking are the most serious digital risks they face. These journalists and bloggers rely heavily on the Internet and actively use digital tools to contact sources and share information. They regularly use the Internet and various electronic and mobile devices to gather and transmit information. About 12 percent fear their social-network accounts have been compromised by a digital attack. About 8 percent worry that their websites will be attacked. Six percent identify information theft as a serious risk.

Because all the survey participants rely on the Internet, and officials and criminal organizations monitor their electronic, digital and mobile activity, it seems certain that most journalists in Mexico are affected by digital insecurity.

BIGGEST DIGITAL RISK

Information theft 6%
Sources revealed 2%
Personal information revealed 1%
Combo risks 7%
Equipment thefts 7%
Hacking of websites 9%
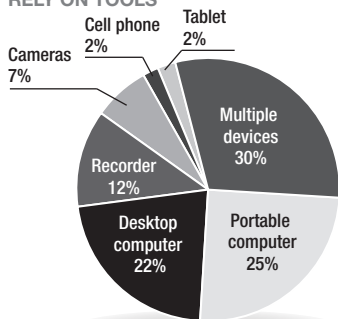Hacking of personal accounts 35%
Cyberspying 33%

As mentioned, more than half of the participants cover corruption, victims of violence, abuses by authorities and human rights issues. Ten percent of those surveyed report on drug trafficking. Coverage of these sensitive topics makes those journalists and bloggers even more vulnerable to electronic surveillance and other digital attacks.

USE OF TECHNOLOGY

Based on the survey results, Mexican journalists and bloggers seem to rely on mobile technology to gather and report news and information. Seventy percent of participants say they use portable devices for their work. One out of every three participants uses multiple technologies: computers, laptops, tablets, cell phones and cameras. At the same time, most also rate their skill level in digital technologies as low. This means journalists and bloggers need to be introduced to new applications and strategies to improve their safety

RELY ON THE INTERNET

Regular 2%
Frecuent 8%
Very frecuent 90%

as they use their devices to report on crime, violence, human rights and corruption.

RELY ON TOOLS

Cell phone 2%
Tablet 2%
Cameras 7%
Multiple devices 30%
Recorder 12%
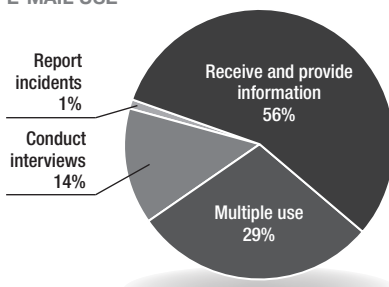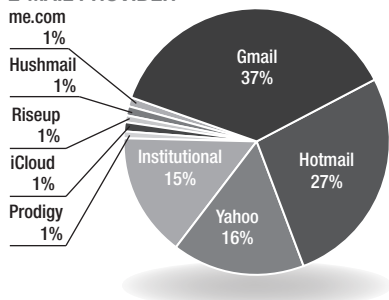Desktop computer 22%
Portable computer 25%

USE OF EMAIL

All the survey participants use email to obtain and share information. Of that group, 56 percent say they use email to deliver and receive information. Thirty percent use email services for multiple purposes, and 14 percent use email to conduct interviews. Thirty-eight percent use Gmail as their primary email service. This is positive since Gmail doesn't show senders' IP address in the headers, provides a Secure Socket Layer (SSL) with HTTPS:// navigation, and offers an alert when the email is accessed from an unknown or infrequent IP. However, 60 percent of the survey participants say they use email services that show the users' IP address in the headers, putting them at risk. Twenty-seven percent use Hotmail, which has an SSL, but shows the senders' IP address

in the headers. Only 3 percent of participants use encrypted email services such as Hushmail or Rise-up.

E-MAIL USE

Report incidents 1%
Conduct interviews 14%
Receive and provide information 56%
Multiple use 29%

E-MAIL PROVIDER

me.com 1%
Hushmail 1%
Riseup 1%
iCloud 1%
Prodigy 1%
Gmail 37%
Institutional 15%
Hotmail 27%
Yahoo 16%

COMMAND OF SECURITY TOOLS

Although participants perceive information theft as a major risk, more than 60 percent report that they have little to no understanding of encryption technologies. Only about 15 percent say they have a good command of security tools like data encryption, use of VPNs, anonymous Internet navigation and secure file removal. One positive finding from the survey: More than 50 percent of participants say they can create secure passwords. The following

tables offer a detailed view of these vulnerabilities:

■DATA ENCRYPTION

More than 60 percent of participants report little or no skill at data encryption. Tools to encrypt data would be extremely valuable for journalists and bloggers who work on such topics as organized crime, corruption and victims of violence to keep their sources, sensitive documents and investigations safe.
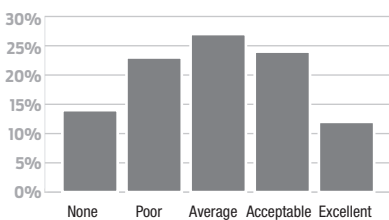
DATA ENCRYPTION
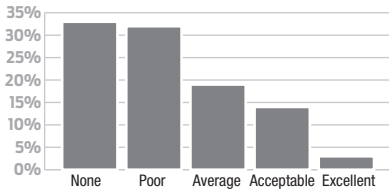
■ANTIVIRUS SOFTWARE

It is encouraging that most participants have a good command of antivirus software. It can prevent their computers and mobile devices from being infected by malware. Nonetheless, 40 percent of the survey participants have little or no command of antivirus software.

ANTIVIRUS SOFTWARE

■ANONYMOUS INTERNET NAVIGATION

More than 70 percent of respondents say they are not using tools to remain anonymous on the Internet. It is crucial for journalists and bloggers to remain anonymous to maintain their physical, psychological and digital security, since criminal organizations and intelligence offices now closely monitor the activity of citizens and journalists on the Internet. Journalists and bloggers would benefit immediately from learning how to access and use these tools, particularly the TOR platform in computers and mobile devices.

ANONYMOUS INTERNET NAVIGATION
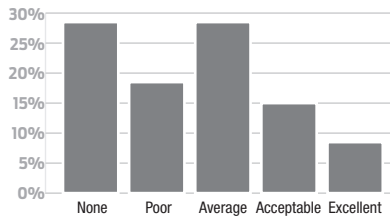

■SECURE FILE STORAGE

Two Milenio TV reporters were kidnapped by a criminal organization in March 2010 because the reporters had taken pictures of military commanders at a ceremony. Because the stored pictures were found, the reporters were accused of being associated with a rival criminal organization that included former soldiers. This was a harsh reminder for reporters working in dangerous zones of the need to protect their files.

More than 50 percent of the participants say they have little or no experience with tools to securely store and erase documents. Knowing how to store sensitive documents securely and prevent them from loss, theft or unauthorized access is an important digital-security skill.

SECURE FILE STORAGE
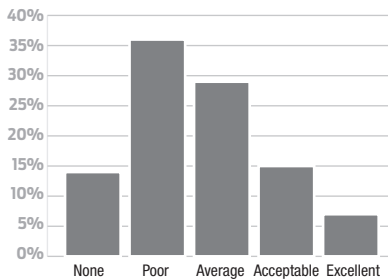
SECURE FILE REMOVAL
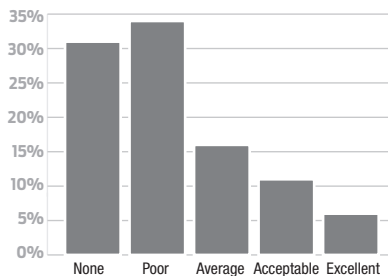
VIRTUAL PRIVATE NETWORKS

More than 80 percent of participants have little or no familiarity with or skill in using virtual private networks (VPNs). VPNs connect users to a remote location such as a corporate server, providing anonymity and encryption. Media companies use these networks to securely connect reporters, photographers and editors to remote and centralized locations. This is particularly useful for re-

porters and photographers who report from dangerous areas and need to transmit stories and other information to the media company's headquarters.
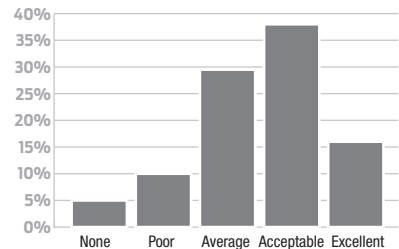
USE OF VPN
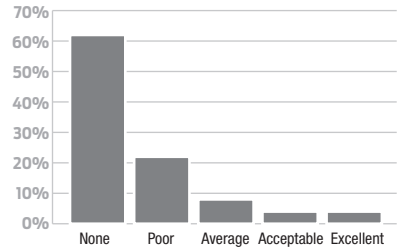
STRONG PASSWORDS

Sixty percent of participants rate their ability to create strong passwords as above average. Strong passwords are the most basic and fundamental element of digital security.
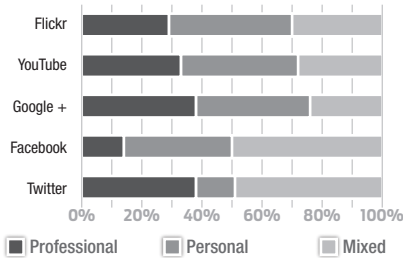
STRONG PASSWORDS

USE OF SOCIAL NETWORKS

Most participants say they rely on social networks to do their work as journalists and bloggers. However, they lack the skill to make full use of those social networks. One serious problem is that 50 percent of the survey participants say they mix personal and professional information on Twitter and Facebook. Just 13 percent say they use Facebook
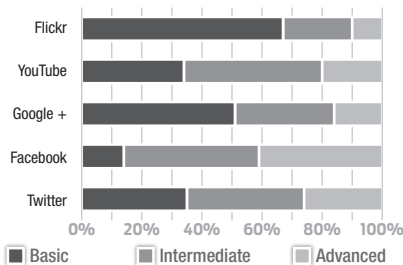
for professional reasons only. Combining personal and professional information is a dangerous practice because it can provide an opening into the journalist or blogger's personal life and activities.

Although 90 percent of the survey respondents say they use social networks (Twitter, Facebook, Google+, YouTube and Flickr), less than 30 percent report an advanced-level use of those tools. They say Twitter is the social network with which they are most familiar. More than 35 percent say they use Twitter and Google+ only for professional reasons.

PERSONAL VS PROFESSIONAL USAGE

Flickr
YouTube
Google +
Facebook
Twitter

0%   20%   40%   60%   80%   100%

■ Professional   ■ Personal   ■ Mixed

SKILLS IN SOCIAL NETWORKS

Flickr
YouTube
Google +
Facebook
Twitter

0%   20%   40%   60%   80%   100%

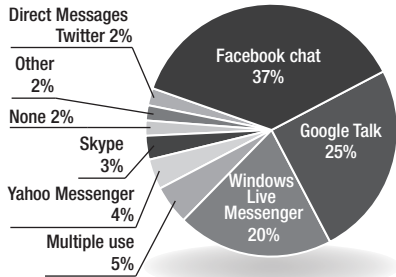■ Basic   ■ Intermediate   ■ Advanced

■ INSTANT MESSAGING
SERVICES

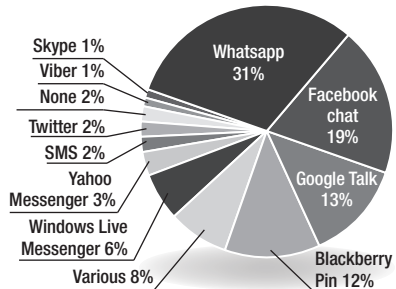Journalists and bloggers also rely heavily on instant messaging ser-

vices to provide and receive information. Almost all of the survey respondents (90 percent) access these systems from computers and mobile devices, with most using Facebook's instant messaging function. However, many also say they don't use security systems to encrypt information during instant messenger exchanges.

INSTANT MESSAGING SERVICE

Direct Messages Twitter 2%
Other 2%
None 2%
Skype 3%
Yahoo Messenger 4%
Multiple use 5%
Windows Live Messenger 20%
Google Talk 25%
Facebook chat 37%

Among Mexican journalists, Whatsapp has displaced Facebook chat as the preferred messaging tool among mobile-device users. It can facilitate communication between journalists and citizens in real time. Twelve percent of participants also say they use Blackberry PIN, which is a positive development since that service automatically encrypts all PIN messages.
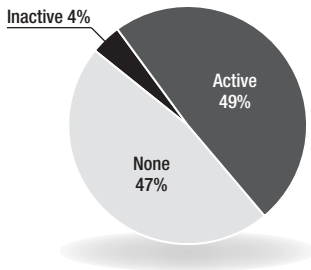
MOBILE MESSAGING SERVICE

Skype 1%
Viber 1%
None 2%
Twitter 2%
SMS 2%
Yahoo Messenger 3%
Windows Live Messenger 6%
Various 8%
Whatsapp 31%
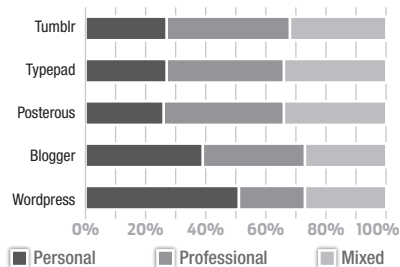Facebook chat 19%
Google Talk 13%
Blackberry Pin 12%

■ BLOGGING

Almost Fifty percent of participants say they have an active blog. The rest do not blog or have inactive blogs. Wordpress is the most commonly used platform, followed by Tumblr and Posterous. According to the survey, Wordpress and Blogger are used more often for professional blogs. Posterous and Tumblr are used more for personal blogs. About 30 percent of the respondents mix personal and professional information on their blogging platforms.

USE OF A BLOGGING PLATFORM

Inactive 4%
Active 49%
None 47%

BLOGGING PLATFORMS USAGE

Tumblr
Typepad
Posterous
Blogger
Wordpress

0% 20% 40% 60% 80% 100%

■ Personal   ■ Professional   ■ Mixed

RECOMMENDATIONS

Journalists and bloggers in Mexico urgently need to increase their digital and mobile security. Although it is impossible to eliminate all risks, it is essential to help journalists and newsrooms adopt new applications and strategies that are designed to minimize their vulnerability as they cover high-risk topics such as drug trafficking, organized crime, corruption, abuse, violence and human rights abuses. It also is essential for Mexican journalists, bloggers and newsrooms to connect with each other and with others around the world dedicated to helping journalists stay ahead of constantly evolving digital threats.

Suggested steps for organizations working with media and journalists in areas where secure communications can provide more protection from risk:

■ Work with media companies to help them better understand the online and mobile threats their employees face and improve their editorial and non-editorial security systems. Help their newsrooms adopt a culture of security awareness that includes digital vigilance and a readiness to adopt and adapt the technologies and strategies needed to maintain cyber-security.

■ Encourage media companies to increase resources devoted to helping reporters, editors, photographers and producers maintain individual digital security.

■ Build a community of media-security experts comprised of Mexican computer engineers, journalists and bloggers who participate in the Hack/Hackers Mexico chapter to customize

technology that helps to reduce the risks journalists and bloggers face when they work online or on mobile phones.

- Use social media, the Internet and existing networks to communicate the need for secure communications tools to media organizations, reporters, photographers and editors who work in dangerous zones.

- Invite journalists to form a network dedicated to online and mobile security.

- Offer more online and in-person programs that help journalists and bloggers embrace security tools such as encryption software and platforms, safe email providers, secure storage and erasing of documents. These programs also should focus on increasing their ability to protect their identity and privacy by using anonymous Internet navigation systems in computer, portable devices and smart phones.