



Berkman

The Berkman Center for Internet & Society
at Harvard University

Research Publication No. 2011-04
August 2011

Online Security in the Middle East and North Africa: A Survey of Perceptions, Knowledge and Practice

Rob Faris, Hal Roberts, Rebekah Heacock, Ethan Zuckerman
and Urs Gasser

This paper can be downloaded without charge at:

The Berkman Center for Internet & Society Research Publication Series:
<http://cyber.law.harvard.edu/publications>

The Social Science Research Network Electronic Paper Collection:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1942857

Online Security in the Middle East and North Africa

A Survey of Perceptions, Knowledge, and Practice

Robert Faris, Hal Roberts, Rebekah Heacock, Ethan Zuckerman, Urs Gasser

August 2011

Robert Faris is the Research Director of the Berkman Center. Hal Roberts is a fellow at the Berkman Center. Rebekah Heacock is a staff member at the Berkman Center and a volunteer author for Global Voices Online. Ethan Zuckerman is a senior researcher at the Berkman Center and the co-founder of Global Voices Online. Urs Gasser is the Executive Director of the Berkman Center.

We gratefully acknowledge support for this research from the US Department of State via a subgrant through the Institute for War & Peace Reporting.

We are grateful for the participation of Global Voices Online, for contributions from Jillian York in putting together the survey instrument, and for the translation work of Anas Qtiesh and Norbert Bousigue. We offer our special thanks to the bloggers that participated in the survey.

INTRODUCTION

Digital communication has become a more perilous activity, particularly for activists, political dissidents, and independent media. The recent surge in digital activism that has helped to shape the Arab spring has been met with stiff resistance by governments in the region intent on reducing the impact of digital organizing and independent media. No longer content with Internet filtering, many governments in the Middle East and around the world are using a variety of technological and offline strategies to go after online media and digital activists. In Tunisia, before and during the January 2011 protest movement that led to a change in government there, Internet service providers were apparently logging usernames and passwords to hack into and dismantle online organizing and information sharing among protesters. In early June 2011, Google reported a phishing attack targeted at military and human rights activists to gain access to their Gmail accounts. In Syria, a well organized effort known as the Syrian Electronic Army has been carrying out attacks to disable and compromise web sites that are critical of the Syrian regime. These stories are only a few selected from the set that have become public, and an unknown number of attacks go unnoticed and unreported. Many of these attacks are impossible to attribute to specific actors and may involve a mix of private sector and governmental actors, blurring the lines between cyber attacks and government surveillance. In such an environment, maintaining online security is a growing challenge.

In this report we describe the results of a survey of 98 bloggers in the Middle East and North Africa (MENA) carried out in May 2011 in order to study bloggers' perceptions of online risk and the actions they take to address digital communications security, including both Internet and cell phone use. The survey was implemented in the wake of the Arab spring and documents a proliferation of online security problems among the respondents. In the survey, we address the respondents' perceptions of online risk, their knowledge of digital security practices, and their reported online security practices. The survey results indicate that there is much room for improving online security practices, even among this sample of respondents who are likely to have relatively high technical knowledge and experience.

KEY FINDINGS

- The survey respondents, primarily bloggers residing in the Middle East and North Africa, experienced a remarkably high incidence of security incidents related to their online activity over the past year, including cyber attacks, personal threats, arrest, and detention.
- Survey respondents reported a wide range of methods employed to mitigate the risks of online activity, including self-censorship, obscuring their identities, and writing in ambiguous language.
- Design and ease of use, rather than security-related features, are reported to be the most important considerations in choosing online platforms.
- Even within this set of at-risk bloggers, only a small number reported that they understand or implement best practices related to online security.

METHODOLOGY

We implemented this survey on the set of bloggers that write about the MENA region and are cited by Global Voices Online (GVO), an aggregator of blogs and citizen media from around the world. Although surveying a random sample of Internet users in the MENA region would have been desirable, this would have been a very costly and time-consuming undertaking that was not possible for this study. It is difficult to draw inferences from most alternative non-random sampling strategies, such as an opt-in survey or snowball sample, as researchers are unable to understand who elected to take the survey and who did not. We chose instead to focus on a known sample that allows us to confidently draw conclusions about the behaviors and beliefs of this sample. This sample is likely to be more knowledgeable about issues of Internet security than a random sample, and the limitations of knowledge shown by this cohort suggest more serious risks for less informed users.

We collaborated with Global Voices Online (GVO) to create a list of individual blogs they cited in 2010. This list was constructed using a crawler that recorded each blog linked from at least one GVO post over the past year. We then created a MENA-focused sample of 580 blogs by including only those blogs that were referenced in posts tagged by GVO as relevant to any of the countries in the MENA region. This country tagging data represents the countries referenced in the blogs but does not indicate where the bloggers reside. Although some bloggers may specify their country of residence on their blogs, for many in the sample we were only able to determine their residence by asking them in the survey.

The bloggers linked to by GVO tend to write about politics, political freedom, Internet freedom, and international affairs, among other topics. This sample represents a more highly educated and more experienced set of Internet users than the general population of users. This group is likely to be significantly better informed about the risks of online activity and behavioral practices that will increase online security. They are also more likely to be politically active and have international connections. This is particularly true for the time period of the study given the intense international attention that was being paid to the political events in the region.

The bloggers linked to by GVO write in Arabic, English, and French, with a bias towards those that write in English. There is also a likely bias towards 'bridge bloggers', those that have an outward focus in their writing in order to describe events in their countries and communities to an international audience. In addition to providing a useful sample frame, GVO is a trusted media organization among bloggers, and collaborating with them on this survey likely increased response rates for this survey. The survey and survey invitations were offered in English, Arabic, and French. We present in this report the aggregate results of the survey; individual responses are not reported to maintain the confidentiality of the survey.¹

RESPONDENTS

Among the 580 bloggers invited to participate in the survey, 98 completed the survey for a response rate of 17%.

The respondents are about three fifths male and two fifths female. Over 90% have a university degree and more than one third a graduate degree. The respondents are overwhelmingly young: almost half are between the ages of 20 and 30, and another quarter are between 31 and 40.

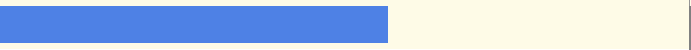
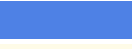


Residents of 15 MENA countries responded to the survey along with residents of 11 other countries. Egypt and Lebanon were the most represented countries with 26 and 13 respondents, respectively. Eight of the respondents live in the United States.²

¹ This research was carried out with the approval and guidance of the Harvard Committee on the Use of Human Subjects in Research. The research protocol included safeguards to minimize risks and to protect the privacy of respondents.

² The results we report here cover all of the respondents, including those living in MENA countries and those living in other countries. It is interesting that few of the results are markedly different when looking solely at residents of MENA countries, although the risks to online activity clearly depend in part on location.

Arabic is the native language for three out of five of the respondents, with English the first language for one out of five. Only 28% reported writing in Arabic over the past month, while 81% had written in English and 11% in French. (Some authors write in more than one language, so percentages total to more than 100%.) Slightly more than half of the sample writes in a non-native language. In open ended responses, the most common reason for writing a non-native language is to reach a wider audience. Many respondents described themselves as bilingual.

In what language(s) have you written on your primary blog in the past month? Please check all that apply.

Answer		%
English		81%
Arabic		28%
French		11%
Other		6%

More than 80% of the respondents include coverage of news, politics, and human rights on their blog. Almost half write about personal life and experiences, and approximately two out of five include material related to entertainment, arts, and culture. Approximately half of the sample classified their writing as critical of their government; one quarter reported balanced writing; and only 1 of the 98 respondents characterized their writing as supportive of their government.

The respondents to the survey are highly connected. Well over 90% use the Internet from their own computer, and approximately two-thirds go online with a mobile device. US-based platforms are the most popular, led by Gmail (85% of respondents) and Facebook (83% of respondents).

Many of the cyber attacks and threats transcend national boundaries. Others risks, such as the threat of arrest and detention, are location-specific.

Which devices do you use at least once a week for the following activities? Please check all that apply.

Question	A computer I own	A work or school computer	A computer at an Internet café	A mobile device
Browse the Internet	96%	35%	7%	56%
Read or send e-mails	94%	34%	8%	50%
Post content to a social media site	91%	31%	8%	46%
Post content to a blog	94%	21%	7%	22%

THE GROWING RISKS OF ONLINE ACTIVITY

Survey respondents were asked from two perspectives about their perceptions of and experiences with threats and risks associated with online activity. When asked about their perceptions of the biggest threats to bloggers in their country, the most common answers were the threat of being arrested and personal threats, accounting for half of the responses. When asked about the risks that they are most concerned about personally, the most frequently cited threats are having their online accounts and web pages hacked, personal threats, and arrest.

Which of the following do you think is the biggest threat to bloggers in your country?

Answer		%
Being arrested or detained		30%
Being personally threatened		18%
Bloggers in my country do not face threats		13%
Don't know/Not sure		9%
Having their identities exposed against their wishes		6%
Being fired, demoted or reprimanded at work		6%
Having their websites hacked or attacked		5%
Having their friends or family threatened		4%
Other		8%
Total		100%

Survey respondents, when asked about the actual incidence of problems related to online activity, reported a remarkably high level of incidents and attacks stemming from their online activities. One third of respondents reported personal threats. One fifth reported that one or more of their online accounts had been hacked. One in seven unwillingly had their online identify exposed. Nine percent of respondents had been arrested or detained. The unusual sample populated by reform-minded bloggers and the timing of the survey—following a period of intense online activism and government attempts to quell this activity—contribute to these high figures. This makes it impossible to extrapolate to other populations and regions. Nevertheless, these reported figures are astounding from our perspective and highlight the vital importance of security concerns for online activists. As we anticipated, the respondents report a mix of cyber attacks and offline responses to their online activities.

In the past year, have you experienced the following negative consequences as a result of your activities online?

Question	Yes	No	Don't know/Not sure
I was personally threatened	30%	55%	2%
My website or online account was hacked or attacked	18%	64%	2%
My computer got a computer virus	17%	58%	7%
My identity was exposed online against my wishes	11%	66%	5%
My friends or family were threatened	7%	72%	1%
I was arrested or detained	7%	70%	1%
I was fired, demoted, or reprimanded at work	5%	73%	1%

ONLINE SECURITY CHOICES AND PREFERENCES

The surveyed bloggers were asked which features were most important to them in selecting online platforms, including email, blogging, and social network providers. The responses appear, at least superficially, to be at odds with the risks and threats delineated in the prior section. In selecting email providers, design, mobile access, and data sharing with other companies were the most important considerations. The ability to encrypt communications and providers' resistance to government data requests were the least important features.

Please select the top three most important features you consider when selecting an email service.

Answer	#1: Percentage of respondents ranking this feature as the most important feature	#2: Percentage of respondents ranking this feature as the second most important feature	#3: Percentage of respondents ranking this feature as the third most important feature	Total: Percentage of respondents ranking this feature in the top three
Design and ease of use	47%	17%	8%	72%
The ability to easily access the service on your mobile phone	15%	26%	11%	53%
The company's policies about sharing data with other companies	3%	16%	26%	45%
The company's resistance to sharing data with your government	9%	10%	15%	35%
The option to encrypt your messages	8%	8%	11%	28%

In choosing social networking providers, the ability to customize privacy settings and design were listed as the most important features, followed by ability to access the platform on a mobile device.³ The company policy of sharing data with governments and other companies were the least important features. The primacy of privacy settings for social networking indicates that protecting personal information is indeed a major concern. Further research would be needed to better understand how users conceptualize the difference between privacy settings, which shield their information from the prying eyes of the general public, and data sharing policies, which represent a substantially different, though potentially no less deleterious, infringement of user privacy.

³ The most important factor that determines one's choice of a social network platform is clearly where one's friends and peers are.

Please select the top three most important features you consider when selecting a social networking site or service.

Answer	#1: Percentage of respondents ranking this feature as the most important feature	#2: Percentage of respondents ranking this feature as the second most important feature	#3: Percentage of respondents ranking this feature as the third most important feature	Total: Percentage of respondents ranking this feature in the top three
Design and ease of use	36%	22%	19%	68%
The ability to customize your privacy settings	23%	27%	19%	69%
The ability to easily access the service on your mobile phone	9%	15%	20%	45%
The company's policies about sharing data with other companies	3%	6%	17%	27%
The company's resistance to sharing data with your government	8%	6%	6%	20%

In respondents' choice of blogging provider, design and ability to customize the blog were most frequently listed as the important factors. Data sharing with governments and other companies was again cited least frequently as an important factor in deciding on a blogging provider. The importance of privacy settings was reported to be less important for blogging compared to social networking. This may be explained by the notion that blogging is more inherently a public act. It might also reveal a belief that US-based companies are largely immune from political pressure from the governments in states where activists live.

Please select the top three most important features you consider when selecting a blogging or microblogging service.

Answer	#1: Percentage of respondents ranking this feature as the most important feature	#2: Percentage of respondents ranking this feature as the second most important feature	#3: Percentage of respondents ranking this feature as the third most important feature	Total: Percentage of respondents ranking this feature in the top three
Design and ease of use	29%	29%	16%	73%
The ability to customize your blog or microblog's appearance	32%	21%	19%	63%
Cost	10%	8%	13%	32%
The ability to customize your privacy settings	4%	11%	15%	31%
The ability to easily access the service on your mobile phone	3%	5%	18%	27%
The company's resistance to sharing data with your government	9%	5%	3%	17%
The company's policies about sharing data with other companies	0%	5%	5%	10%

The survey explored several other behavioral responses to online security threats. Hiding one's true identity is a method employed by many activists engaged in risky online behavior, while others write openly under their full name.

**Thinking of your primary blog, which of the following types of information is displayed?
Please check all that apply.**

Answer		%
My full name		49%
My email address		47%
A photo that clearly shows my face		42%
My current town or city		41%
A link to another web page that contains some or all of the above information		25%
My list of friends		11%
My phone number		4%
None of the above		16%

Encrypting communications can lessen exposure to surveillance and help to maintain anonymity for those not writing in their real name. However, reported use of encryption was quite low.

Self-censorship is another possible response to avoid negative consequences associated with online expression. Half of respondents reported self-censoring themselves, and many cited the fear of repercussions from their government as the reason for limiting their online writing.

Several respondents indicated in free text answers that they are careful to avoid identifying the people included in their coverage by changing names and locations and obscuring photographs that include faces. A subset of the respondents reported writing in ambiguous or vague terms that effectively communicate their points while avoiding more overt challenges to the government.

Many of the respondents indicated that they believed that by writing in English they were less susceptible to government reactions to their online writing as their words are more likely to reach international than domestic audiences.

A significant percentage of respondents (16%) reported that they include no personally identifiable information on their blog. Blogging anonymously or under a persistent pseudonym has become common in some countries, particularly those where the perceived threats associated with online speech are high. This practice can prove confusing for international audiences, particularly when exploited as a way of creating deceptive

“sockpuppet” identities, as American researcher Tom MacMaster evidently did with his construction of putatively Syrian blogger “Amina”.

ONLINE SECURITY PERCEPTION, KNOWLEDGE, AND PRACTICE

We asked a series of questions to gauge respondents’ self-perception of their knowledge of various areas of online security, respondents’ actual knowledge of those areas of online security, and respondents’ practices in those areas of online security. Respondents’ perceptions, knowledge, and practices of online security varied widely across different topics, but in general, perceptions, knowledge, and practices of online security ranged from fair to very poor. Our questions regarding knowledge were challenging ones, but consistent with the threats activist bloggers currently face in some countries in the region.

Percent of respondents who self-reported good or very good knowledge of the given area of online security (Perception), who correctly answered a quiz question about the given area (Knowledge), and who reported adhering to best practices for the given area (Practice).

Area	Perception	Knowledge	Practice
Strong passwords	77%	40%	56%
Encryption	25%	7%	5%
Malware	53%	74% / 19% / 8%	NA
Data protection	47%	20%	57%
Mobile	NA	10%	30% / 2%

A strong password online consists of a random collection of at least eight random letters, numbers, and punctuation marks. Using a strong password for sensitive accounts is important because weaker passwords, such as those merely consisting of a random dictionary word or name, are easier for a determined attacker to guess. While a large majority (77%) of respondents perceived themselves to be knowledgeable about what constitutes a strong password, only 40% of respondents were actually able to correctly define a strong password. In practice, only a bare majority (57%) of users reported consistently using strong passwords for sensitive accounts.

Using encryption for sensitive Internet traffic is important because it makes it harder for an attacker on the network (such as an ISP controlled by a hostile government) to surveil the traffic. Only a small number (25%) of respondents claimed that they understood how to

encrypt their web and email traffic, and only 7% were able to correctly explain specifically what data web encryption protects (it protects the content but not the sender / receiver identities from snooping by a network attacker). Very few (5%) respondents claimed to always make sure that all of their sensitive web traffic was encrypted (57% of respondents claimed that they do not encrypt sensitive web traffic because they do not need to, while 35% claimed that they do not know how to).

It is critical that each user at risk understand that an attacker who has infected her computer is able to surveil not only all traffic (encrypted or not) to and from the victim's computer but also to use that computer's microphone and camera to surveil the victim offline. A small majority (53%) of respondents claimed to understand how to protect themselves from malware, and a large majority (74%) correctly understood that anti-virus software only protects a computer from some or most malware. But only a small number (19%) of respondents understood basic protection of phishing attacks (by matching the domain of the link in the email with the domain of the intended site), and only a tiny number (8%) understood how to protect themselves against targeted email attacks (by never opening an email attachment). This last finding is extremely troubling, since we have seen many reports recently of email malware attacks targeted in real time by spoofing the sender and subject of a current, ongoing conversation.

Protecting the data residing on the computer is as important as or more important than protecting data as it goes over the network. But less than half (47%) of respondents claimed good or very good knowledge of how to protect data on their computers, and only a small minority (20%) of respondents understood that physical access to a computer gives the greatest access to sensitive traffic coming from the computer. In practice, 57% of respondents reported that they never left their computers unattended in public.

We didn't ask respondents to self-report their knowledge of mobile security practices, but only 10% of respondents understood that turning off a mobile phone will not protect against government monitoring (almost all mobile phones have remote power-on capabilities designed for emergency responder use in the US but easily repurposed for government surveillance), and only a tiny number (2%) of respondents claimed to always carry out sensitive conversations out of the presence of mobile phones (even if turned off). Only a minority (30%) of respondents claimed to never make sensitive phone calls on a mobile phone.

DISCUSSION

There is an apparent divide between the relative importance accorded online security practices by bloggers in their perceptions, preferences, and practices and the growing level of risk related to online activities in the MENA region. While a large majority of respondents indicate an acute awareness of the risks of publishing sensitive material online, and most take some measures to mitigate these risks, very few appear to follow a strict set of online security practices. There are several possible factors that could explain this seeming incongruence.

A possible explanation is that the choices made prior to the past six months did not anticipate the remarkable series of events in 2011, both online and offline, and that users have not yet adapted to the expanding threats to online security.

It is true that design and ease of use are important aspects in the functionality of online tools and a necessary part of platform choices, and that trading security for ease of use is a natural but risky response. Many online media producers may prioritize getting the message out, leaving individual security as a secondary consideration despite the real security risks respondents reported facing. A related factor suggested by a few of the respondents is that they openly and willingly faced the risks associated with their actions as they felt that oppositional views should be openly voiced with real names behind those views, even taking the associated risks into account.

Online security is affected both by the choice of online platforms and providers and by the practices employed when using these tools. While user choices are constrained for both, the role of knowledge, the availability of security options, and the trade-offs between ease of use and security weigh differently on these decisions. For organizers and authors seeking a wide audience via social networking, there is not effectively any choice. This suggests that the most promising areas for improving online security are in the design choices made by platform providers and in expanding cooperative efforts between activists, online security experts, and platform providers to improve platform security options and defaults.

A gap in the knowledge and skills needed to maintain online security continues to be a relevant factor, though this is less likely to factor into platform choices than with security practices. There is clearly more work to be done in training and informing users about best practices related to online security. Even this relatively sophisticated group of bloggers seems to misunderstand some of the basic tenets of online security.

RECOMMENDATIONS

- Expand online security training efforts, with a particular focus on trouble areas identified in this survey.
- Increase efforts to monitor threats to online safety. Expand efforts to study and document online security practices and understand user behavior and perception.
- Expand outreach to online service providers to offer better security options and defaults.