WHAT ARE THE DIGITAL SECURITY CONCERNS AND THREATS FACING WOMEN HUMAN RIGHTS DEFENDERS?

One of the first steps to addressing violence against women is documenting that there is a problem. This is as true online as it is offline. APC's Connect Your Rights! Campaign has conducted a survey of 40 women human rights defenders (WHRDs) from across Latin America, Eastern Europe, Africa and Asia, on their online experiences, their security concerns and their training needs. This is an important step towards developing long-term strategies, responses and policy to the ongoing threats that all women, but particularly women human rights defenders, face online.

THREATS AND RESPONSES

The most common threat faced is harassment, though the figures show that English speakers are far more likely to suffer from this than Spanish speakers. Given that this is not a technical, but a behavioural issue, this is highly significant, especially given that the English-speaking respondents came from a wide range of countries, both culturally and geographically. There were respondents from Africa, Europe and Asia.

The rest of the results are reasonably similar, with around 20-25% of respondents having faced each of the other threats (averaging over all language groups), except seizure of computer or equipment, which only around 10-15% had experienced.

From these experiences, it seems that the threats facing WHRDs are unlikely to be overt security measures taken by states, and are more likely to be either covert measures taken by states or by private groups or individuals. Examples include a distributed denial of service attack or DDOS – while there is speculation that some states or state agencies engage in these attacks, governments are unlikely to admit to complicity.

> "In Indonesia, when we experienced the problem of ISPs taking down content that was discussing LGBT rights, there is no way we could go to the police to defend our right to freedom to disseminate rights-based information. The police are more likely to harass us, than defend our rights."
> - Kamilia Manaf, Institut Pelangi

In terms of resolving these threats, campaigning around the issue is the most popular strategy over language groups. Groups are as likely to resolve it themselves as to ask for external help, but seeking redress from the police is not likely. There was a big disparity here between language groups, in the English-speakers were far more likely to just ignore the problem (nearly a third): but this could be related to the types of threat faced.

Perhaps sensibly, moving to a new medium was universally unpopular. Under one in five would report it to the site owner.

Threat / Action	Countered it technically yourself	Got external help	Moved to different medium	Campaigned or protested	Reported to site owner	Reported to police	Ignored it	Other
Email account hacked (n=5)	**3**	4		1	1			
Computer seized (n=3)	1	3	1		1			
Website hacked / DDOS (n=5)	2 **(1)**	3		1	2 **(1)**		1	
Threatened / harassed (n=12)	4	6	1	4	3		6	

These results are presented with provisos. First, there is a high degree of overlap, as in people who experienced more than one type of threat. Therefore, it is hard to say that responses were directly related to that particular threat. It also explains why in some instances respondents both ignored a threat, and took action – because they were subject to multiple threats. However, given that there is a high degree of correlation between 'threatened/ harassed' and 'ignored it' (which only appears once in any other threat), it is reasonably safe to assume that a large number of respondents chose this as a strategy in response to this particular threat.

The above table is also correlated with comments. So, for example, three of the respondents who had had their email attacked related how they handled the problem themselves. Numbers in bold can therefore be directly correlated with the threat.

WHAT DO WHRDS DO TO PROTECT THEMSELVES ONLINE?

Over half of all organisations have an online security policy, which does not seem to be linked to whether the organisation has attended a training on online security. Interestingly more English speakers have a policy than do Spanish - interesting because around 25% of Anglophones have attended a training, but around 75% of Spanish-speakers have. Obviously, the reason behind this needs investigating, but perhaps the content of some training needs to be examined to emphasise the importance of having a comprehensive online security policy, or to make the idea manageable. In both the post-survey interviews I conducted, women who had attended APC trainings on digital security said that they were in the process of implementing measures to improve online security, but that the process was an involved one.

> "The more you know about online security, the more you realise the complexity of the issues involved. We would like to be trail-blazers and just put something out there, but it would have an impact on the women we work with, how their images are used, what voice they have in the ways they are represented, so we need to work through all these things very carefully."
> - Maggie Mapondera, Just Associates

Around 90% have anti-virus software and more than half use a secure browser add-on, but less than a quarter use any other security measures - there was, however, a major discrepancy in using secure file deletion, with more than half of Spanish speakers using it, and less than 15% of

Threat / Policy and measures	Organisation has a security policy	Attended a training	Using antivirus software	Using file / disk encryption	Using password manager	Using web anonymity	Using secure browser add-on	Using email encryption	Using secure file deletion
Email account hacked (n=5)		2	5	1	2		1	1	2
Computer seized (n=3)		2	3	1	1		1		1
Website hacked / DDOS (n=5)		3	5	1	2		2	1	1
Threatened / harassed (n=12)	3	9	10	3	3	3	6	2	1

Anglophones. There appeared also to be little correlation between attending a training and increasing the level of security – but this is probably due to the nature of the sample. As I could only correlate English language results, and the majority of them had attended a training, it was difficult to spot trends. I feel that a much larger sample would be needed to give meaningful results on this issue.

Only a few respondents felt unsafe online, with the vast majority feeling either safe or neither safe nor unsafe. None felt very unsafe, only two respondents (5%) felt very safe.

One of the biggest fears online is over private information being shared without knowledge or consent, over 70%; the only area that less than half the respondents were concerned about was legal issues. This perhaps indicates both the complexity of the issues involved, and the hesitancy of WHRDs to become involved in policy arenas that are often seen as 'technical' rather than rights-based. All other areas were between 50-70%, although almost 90% of Spanish speakers were very worried about the security of social media sites.

MOVING FORWARD AND CONCLUSIONS

All the respondents said that they required some form of training, the most pressing needs being for training in secure social networking, protecting an online identity and privacy and security in online campaigning.

What training(s) you would prioritise for your networks?		
Option	Count	Percentage
Secure passwords (A)	21	52.50%
Encryption of email and files (B)	20	50.00%
Secure social networking (C)	29	72.50%
Get around internet censorship (D)	12	30.00%
Protect your online identity (E)	29	72.50%
Privacy and security in online campaigning (F)	27	67.50%
I don't need any training (G)	0	0.00%
Other	1	2.50%

The geographic spread of the 30% who asked for training on evading internet censorship was quite broad, encompassing six countries in Asia and Africa (Afghanistan, Egypt, India, Indonesia and Nigeria) from the English-speaking respondents and three countries from Spanish-speakers.

However, the comments also show a recognition of the importance of a safe online environment for feminism, in general. The contest over knowledge resources is not a level playing field and women were recognised by most respondents as being disadvantaged – the root cause of harassment online and off. It is vital, therefore, to include policy elements as part of trainings in online security and dealing with communication threats.

> "When we attended a policy meeting, there was no space on the agenda for women's issues. One of the ICT activists even asked me, what is the connection between ICTs and women!" - Kamilia Manaf, Institut Pelangi Perempuan, on the root causes of harassment.

Commissioned by the Association for Progressive Communications (APC)

Conducted with support from the Swedish International Development Cooperation Agency (Sida).

CONNECT YOUR RIGHTS!
INTERNET RIGHTS ARE HUMAN RIGHTS

RIGHTS.APC.ORG

WHAT ARE THE DIGITAL SECURITY CONCERNS AND THREATS FACING WOMEN HUMAN RIGHTS DEFENDERS?

OCTOBER 2012