USAID
FROM THE AMERICAN PEOPLE

Cybersecurity
GENDER EQUALITY

Photo Credit: Digital Empowerment Foundation (DEF)

Why Does Cybersecurity Matter for Gender Equality?

Gender impacts the ability of women and LGBTQI+ individuals to access the Internet, creating a gender digital divide—one that is more prevalent for individuals in developing countries. Gender also impacts users' experiences with the Internet and, by extension, their relationship to cybersecurity. Cyber attacks have different effects on women and members of the LGBTQI+ community because the same harmful gender norms that control and constrain their behaviorin the offline world are often replicated or even exacerbated online. What is especially alarming is that gender norms can also lead to technology-facilitated gender-based violence (TFGBV), which has the dual effect of actively harming individuals and groups while also disincentivizing them from using the Internet and other digital tools. Not only can TFGBV further widen the gender digital divide, it can also lead to physical violence offline and other serious psychological,social, and economic impacts for women and LGBTQI+ individuals.

What is cybersecurity and why does it matter for international development?

As noted in USAID's Cybersecurity Primer, USAID defines cybersecurity as "*the activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation.*" As USAID partner countries further their digital transformation and continue to adopt new digital tools and systems, cyber risks and vulnerabilities proliferate. Cybersecurity failures pose material threats to USAID partner countries and undermine partner country government legitimacy. USAID must protect its digital investments by ensuring that its digital programming addresses cyber harms and includes cybersecurity mitigation measures.

Cybersecurity Trends in Gender

The prevalence of TFGBV is disincentivizing women from using the Internet and digital tools. TFGBV is alarmingly common. A 2020 Pollicy survey found that 28 percent of female survey respondents across five African countries reported that they had experienced some form of online violence, with 27 percent of them indicating they had experienced cyberstalking. For women with intersectional identities, these statistics can be even higher. A study supported by The Collaboration on International ICT Policy for East and Southern Africa (CIPESA) revealed that three-quarters of a group of 35 women refugees

living in Uganda had faced cyber harassment, including cyberstalking and hacked social media accounts. Due to the pervasiveness of TFGBV, some women are making the choice to use digital tools less frequently, thereby further widening the gender digital divide. The 2020 Pollicy survey showed that 15 percentof surveyed women deleted or deactivated their accounts and 12 percentstopped using a digital service after experiencing online violence.

What is technology-facilitated gender-based violence (TFGBV)?

TFGBV is defined as a threat or act of violence committed, assisted, aggravated, and amplified in part or fully by using information and communication technologies or digital media that is disproportionately targeted at women, girls, and gender non-conforming individuals. It is a continuum of multiple, recurring, and interrelated forms of gender-based violence that takes place both online and offline. Examples can include online harassment and abuse; non-consensual distribution of intimate digital images; cyberstalking; sextortion; doxing; malicious deep fakes; livestreamed sexual violence of children, youth, and adults; rape and death threats; disinformation; intimate partner violence; and recruitment into trafficking and abusive labor.

Data breaches compromise women's and LGBTQI+ people's privacy in especially harmful ways. Though data breaches can be devastating for anyone or any group of people, data breaches can have especially insidious consequencesfor the privacy and dignity of women and LGBTQI+ people, even when they are not the specific target of an attack. For example, data breaches at hospitals and other healthcare facilities can reveal private health information, such as sexual and reproductive health histories about pregnancy, infertility, and HIV status, and can disclose the identities of LGBTQI+ people in places where they are particularly vulnerable to harm. There is then a likelihood that this information could be used by criminals and nation-states to extort, harass, persecute, or inflict other forms of offline violence upon LGBTQI+ individuals and groups.

Online gendered mis- and disinformation (OGDM) targets women and people of intersectional identities for online harassment and false messaging. One type of OGDM includes mis- and disinformation campaigns specifically targeted at women. For example, one well-known OGDM campaign perpetuates the false narrative that COVID-19 vaccines are dangerous for pregnant women. Other OGDM campaigns are intended to discredit individual women or members of the LGBTQI+ community. This type of OGDM sees prominent women publicly harassed online, usually on social media or through private messaging platforms like WhatsApp or Telegram. OGDM is often more severe for women with intersecting identities, as found by a 2020 Amnesty International report that exposed online abuse targeted at female Indian politicians on Twitter. Surveyed women politicians who identified or were perceived as Muslim "received 94.1 percent more ethnic or religious slurs than women from other religions," as did politicians from marginalized castes, who "received 59 percent more caste-based abuse compared to women from other castes." While these types of OGDM campaigns often target individuals, they can have a broader chilling effect on women's participation in online and offline spaces.

Cybersecurity laws can be co-opted to persecute women and LGBTQI+ communities. Some governments are adopting cybersecurity laws that effectively repress freedom of speech for women and LGBTQI+ individuals. For example,in Uganda, prominent feminist and queer activist Stella Nyanzi was charged with "cyber harassment" and "offensive communication" under sections of the country's Computer Misuse Act after posting a crass political poem on Facebook in 2018. She ultimately served 16 months in prison, then later went into exile in Germany. Similarly, survivors of non-consensual intimate image (NCII) sharing in Tanzania can be prosecuted under Section 14 of the national cybercrime law, which does not effectively distinguish between the creation of intimate digital images and their non-consensual distribution. Fear of prosecution has discouraged Tanzanian survivors from coming forward to report these crimes.

Photo Credit: Jeffrey Michael Walcott

Women are not adequately represented in technology and cybersecurity industries. In 2022, Cybersecurity Ventures estimated that women still comprised just 25 percent of the global cybersecurity workforce. The United Nations Institute for Disarmament Research (UNIDIR) cites possible reasons for this, including gender norms keeping women out of science, technology, engineering, and math (STEM) careers, a lack of cybersecurity awareness among women and girls, a lack of visibility for women within the cybersecurity field, and work cultures that are not conducive to—and sometimes actively hostile to—their participation. The underrepresentation of women in the technology and cybersecurity fields can lead to digital products and services that do not adequately incorporate controls that prevent their usage in acts of TFGBV. For many of the same reasons, the lack of participation of women also extends to the cybersecurity policymaking space. Adequately incorporating their lived experiences and diverse viewpoints will help lead to more gender-sensitive and gender-responsive cybersecurity policies.

USAID works to protect the digital safety of women activists and LGBTQI+ organizations

From 2011–2020, USAID's Information Safety & Capacity Project (ISC) supported female and LGBTQI+ activists around the world to strengthen their cybersecurity protections. In response to TFGBV against female protest leaders, journalists, and other activists during Nicaragua's 2018 protests, ISC applieda feminist approach to digital security when working with women-oriented non-government organizations (NGOs). With ISC support, these activists and NGOs led workshops with inputs from TFGBV survivors covering topics like how to secure social media accounts, safe sexting practices, and what to do in case of NCII sharing.

Key Considerations

» The following considerations present entry points for incorporating cybersecurity into gender programming:

» Understand partner country policies, strategies, and regulations around cybersecurity, data privacy, communications infrastructure, and digitalization.
  - USAID Missions and Bureaus need to understand the cybersecurity ecosystems they are operating in before designing and implementing new EEI activities. Digital Ecosystem Country Assessments (DECAs) are one mechanism for better understanding these dynamics. If your Mission does not already have a DECA, consider commissioning one.
  - You can also consider incorporating cybersecurity into your Mission's gender analyses.

» Seek input and learn from gender and cybersecurity stakeholders within each USAID partner country.

» Coordinate with other donors to identify areas of alignment in gender and cybersecurity.

» Research project-specific cyber vulnerabilities as they relate to gender, and incorporate gender-specific cybersecurity considerations, resources, responsibilities, and management tools into every project.

» Develop cybersecurity-related indicators to measure the effectiveness of cybersecurity interventions for women, LGBTQI+ people, and people of intersectional identities.

» Continue to prioritize digital literacy and cyber hygiene training that help vulnerable populations understand topics like navigating privacy settings, establishing and respecting consent in online spaces, and understanding TFGBV, including how shared images and information are used online.
  - If you have specific partners who need cyber hygiene training, consider buying into USAID's Digital APEX mechanism, which provides cybersecurity support to USAID partners. Use the email address below to contact the team for more details.

» Support STEM training specifically targeted to and designed for women and LGBTQI+ populations.

FOR FURTHER INSIGHTS into the cybersecurity and gender nexus in USAID programming, please reach out to USAID's Cybersecurity Team at cybersecurity.itr@usaid.gov.