White paper

Cyber-security for women during the COVID-19 pandemic:

Experiences, risks, and self-care strategies in the new normal digital era

OAS More rights for more people

Table of Contents

I. Objectives 04

II. Impacts of the COVID-19 pandemic on the digital ecosystem 05

A. Risks associated with the new digital ecosystem 06
B. Different contexts, different cyber-risks 08

III. How are women faring in the new normal digital era? An analysis, from a gender perspective, of the digital ecosystem triggered by the COVID-19 pandemic 09

A. What obstacles are women facing in cyberspace? Digital gender divides 11
B. The continuity of online-offline issues: gender discrimination and the impacts of the COVID-19 pandemic on women 13
C. What do we know about the ways women are using the Internet during the COVID-19 pandemic? 16

IV. Cyber-threats and specific risks women face in the new digital ecosystem: ongoing reflections 18

A. One widespread risk factor: the lack of digital security skills 18
B. Exploring some of the risks women face in the new normal digital era 19

V. Digital security for women in the new digital ecosystem: a hard core of measures they can apply to protect themselves 24

A. Basic kit of digital security measures for the new-normal era 25
B. Digital security measures for dealing with specific risks 29
a. Protection against corona-phishing and corona-smishing 29
b. Safe teleworking 31
c. Holding safe online meetings 32
e. Banking via the Internet and online shopping 33
f. Safeguards against infodemia and fake news/misinformation 34
g. Sextortion 35
h. Cyber-security within the family 37

Glossary 39

Bibliography 42

Credits

Luis Almagro
Secretary General
Organization of American States (OAS)

Arthur Weintraub
Secretary for Multidimensional Security
Organization of American States (OAS)

Alison August Treppel
Executive Secretary
Inter-American Committee against Terrorism (CICTE)

Alejandra Mora Mora
Executive Secretary
Inter-American Commission of Women (CIM)

OAS Technical Team
Cyber-Security Program
Kerry-Ann Barrett
Mariana Cardona
Mariana Jaramillo
Gabriela Montes de Oca Fehr

Inter-American Commission of Women /
Follow-up Mechanism to the Convention of Belém do Pará
Luz Patricia Mejía Guerrero
Alejandra Negrete Morayta

Author
Katya N. Vera Morales

Design and Layout
Michelle Felguérez

01 Objectives

> *The notably expedited expansion of digitization and technical transformation triggered by the COVID-19 pandemic has fostered the development of a digital ecosystem in which new identities, experiences, and interactions are surging, being replicated, and transformed on a huge scale.*

While it is true that cyber-crime, abuse, and digital violence were already a global concern prior to the pandemic, these new conditions have provided fresh opportunities for attackers and cyber-delinquents who have now stepped up the volume and scope of their attacks, using both old techniques and novel strategies.

Since March 2020, a number of global and regional studies have striven to identify trends and salient features of online threats and the resulting challenges posed for cybersecurity in the new digital ecosystem. A perusal of those studies reveals, however, that little attention has been paid to women's digital experiences in connection with increasing vulnerabilities online and the ongoing lack of a gender-sensitive analysis of the whole range of cyber-dangers they face and the havoc cybercrime can wreak with their lives.

This lack of analysis from a gender perspective echoes the wider picture found for cybersecurity as a whole, where technology and cyber-threats are still largely perceived to be gender-neutral, without impacts that differ, depending on a person's gender identity or expression (Millar et al, 2021: 8). Within that context, a number of sources in academic, civil society, and multilateral fora have begun to underscore the need to analyze the gender dimensions of cyber security with a view to enhancing understanding of the underlying forces shaping policy and practices in that sector. In recent years, that has prompted official statements, capacity-building strategies, and investigations that are opening up new approaches in this field.

In line with those new trends, this publication seeks to contribute to dialogue about the links between cybersecurity and gender norms and roles during these critical times for cyberspace, by offering an analytical framework for identifying possible vulnerabilities and risks for women[1] in the new digital ecosystem.

To that end, the idea is to **analyze the cyber-attack scenario** prompted by the health crisis **in connection with the dynamics governing women's access to and use of the Internet** along with systemic (online and offline) **conditions of gender inequality** with a view to identifying **certain cyber-threats reportedly affecting women specifically during this phase.**

[1] The author stresses that, due to space limitations, this paper focuses solely on women's specific experiences with cybersecurity, even though she acknowledges the urgent need to draw attention also to the online experiences and cyber-threats currently experienced by other groups marginalized because of their gender and sexual identity or expression and to foster detailed analyses of the impact on cyber-security of the intersection between gender and other factors triggering discrimination and exclusion.

Hopefully, this analytical framework will prove useful for cybersecurity professionals and officials responsible for formulating public cybersecurity policies in connection with strategies devised to protect people online during the health crisis. It has also been used as a basis for outlining **a set of basic digital security measures that need to be espoused and adopted in the "new-norm" digital era.** The premise here is that it is not enough just to identify potential vulnerabilities and cyber-dangers. Digital self-protection is also a vital component of strategies for empowering women in the safe use of new technology.

The study of the gender dimensions of cybersecurity norms, policies, and strategies is a novel and constantly evolving area of research, whose findings will undoubtedly pave the way toward a more in-depth understanding of cyberspace. With that in mind, this paper hopes to contribute with ideas to the current debate, based on an appreciation of the enormous potential of a gender-based approach to the sector and to the impact of such global phenomena as COVID-19 on specific aspects of the cyber-security industry.

02 Impacts of the COVID-19 pandemic on the digital ecosystem

The COVID-19 pandemic has ushered in a turning-point in the use of cyberspace, which has become the principal shared scenario world-wide. As of March 2020, the health crisis led to confinement measures aimed at containing the spread of the virus and forcing much of the world's population to stay home, with very little ability to move around. Faced with that mandatory confinement, we found ourselves forced to reinvent our societies and modify core aspects of our daily practices, and to quickly pursue new individual and collective strategies to mitigate the impacts of the health crisis.

On an unprecedented scale, governments have resorted to technology to protect and preserve public health, keep the economy functioning, and bring public services to citizens, by rapidly digitizing their administrative and management procedures and providing digital solutions in health, education, commerce, and the workplace. Likewise, companies, universities, banks, international agencies, churches, organizations, and groups of every type, nature, and size have implemented digital tools and platforms to migrate activities hitherto based on physical presence to cyberspace[2].

As individuals, too, we have turned to cyberspace, in a bid to overcome isolation and stay in digital touch with family and friends despite physical separation, striving to preserve the sense of normality that vanished with the arrival of the pandemic. We have shifted much of our job-related, educational, commercial, entertainment, and relational activities to the Web[3], further reinforcing the *online-offline* continuity already found in human interactions even before the advent of the pandemic.

[2] According to the Economic Commission for Latin America and the Caribbean (ECLAC), between March and April 2020, the number of business websites increased by 800% in Colombia and Mexico, and by about 360% in Brazil and Chile. In Mexico and Brazil the number of new e-commerce sites increased by more than 450% in April compared to the same month in 2019 and transactional (active presence) business sites in Colombia and Mexico increased by nearly 500% in the same period. See: Economic Commission for Latin America and the Caribbean (ECLAC) (2020). Universalizing access to digital technologies to address the consequences of COVID-19.

[3] In Europe, for example, the use of the Internet for leasure activities, interaction via social networks, or pay-TV platforms increased so much that the European Union asked Netflix and HBO to reduce the number of bytes in their content so as not to saturate the network. See: José García (March 12, 2020). "Netflix reducirá la calidad del contenido para evitar saturar la red a petición de la Unión Europea". https://www.xataka.com/streaming/netflix-reducira-calidad-contenido-para-evitar-saturar-red-a-peticion-union-europea. Accessed on February 1, 2021.

A variety of technologies have enabled those affected by the pandemic to connect with authorities and agencies offering assistance, providing them with a channel through which to voice their needs, concerns, and experiences (ILO, 2020b: 17). During this emergency, it has transpired, more starkly than ever, that access to the Internet is no longer a mere luxury, but rather a lifeline to the outside and a human right vital for the exercise of other fundamental rights, such as the right to health, education, culture, and freedom of expression (Agudelo et al, 2020: 3).

For women and girls, expedited digitization during the pandemic has made it possible to break with prejudices and gender stereotypes that, for a long time, kept them from accessing digital technologies on an equal footing. For some of them, this was the first time they had a chance to explore new Internet tools and platforms, given the need to stay in contact, and to embark on the use of digital financial services, purchases via the Internet, remote learning, and on-line business activities. The confinement period has also prompted them to play an active part in digital debates, create ties to new on-line women's groups, and engage in new forms of telework enabling them to reconcile their work-related and family responsibilities.

Together, these changes in social practices during the pandemic have wrought major changes in cyberspace. Since March 2020, Internet traffic worldwide has reached record levels, with increases surpassing 50% and 70% in some countries[4]. According to the United Nations Economic Commission for Latin America and the Caribbean (ECLAC), in Latin America, during the first quarter of 2020, telework increased by 324%, online education by more than 60%, e-commerce by 157%, livestreaming 12%, and e-banking 7% (ECLAC, 2020).

At the time of writing, it is unclear how much longer the COVID-19 health crisis will last, but what is clear is that digitization is here to stay and will be a crucial part of the "new normal." During this period, the expedited (and in many cases obligatory) use of digital tools has made women and men more comfortable using them and, once the crisis is over, people are likely to use the Internet for more purposes than they did before the pandemic.

A. Risks associated with the new digital ecosystem

> *The exponential, global increase in the use of technology to mitigate the impact of measures taken to address the health crisis has also posed a huge challenge for the digital ecosystem and has laid bare structural flaws in both access to the Internet and online security.*

As women and men have resorted to cyberspace as the preferred medium for many of their activities, there has been an exponential increase in their exposure to online risks due to their lack of familiarity with large-scale use of Information and Communication Technologies (ICTs) and widespread ignorance regarding cyber-threats and digital protection and security tools.

[4] Mark Beech (March 25, 2020). "COVID-19 Pushes up internet use 70% and streaming more than 12%, first figures reveal". https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=36a6e4ab3104. Accessed on February 1, 2021.

The presence online of more people with little knowledge of cybersecurity (and exposing themselves to more online risks than they would normally do at school or in the workplace) has created a fertile environment for attackers and cyber-delinquents, who have quickly taken advantage of this "new digital norm" to exploit the fear and uncertainty generated by the pandemic and the population's thirst for information (UNODC, 2020)[5].

As several sources have reported, cyber crimes have increased in direct proportion to the digital transformation initiated in March 2020, and by the end of that month all countries had experienced at least one COVID-19-related cyber-attack[6]. The United Nations pointed to a 600% increase in the volume of malicious e-mails since the start of the pandemic and a 350% surge in false websites, with cyber-attacks averaging one every 39 seconds[7]. According to the FBI's Internet Complaint Centre (IC3), complaints filed against cyber-crimes quadrupled[8], while in Latin America a 74% increase was reported in the number of cyber-crimes committed during the pandemic[9]. More than 20.5 million cyber-attacks targeted people using the Internet at home, while 1.2 million attacks were directed at mobile devices, between January and September 2020[10].

According to analyses of the impacts of COVID-19 on cyber-crime conducted by agencies such as the United Nations Office against Drugs and Crime (UNODC), the International Criminal Police Organization (INTERPOL), and the European Union Agency for Law Enforcement Cooperation (Europol), the most frequently observed cyber-attacks since March 2020 include: social engineering methods, Internet scams, phishing, infiltrating malware into electronic devices, the creation of fake websites, ICT-facilitated sextortion, attacks via remote work tools, online disinformation, and the use of the Dark Web for criminal activities[11].

[5] Trend Micro (11 noviembre 2020). "Developing Story: COVID-19 Used in Malicious Campaigns". https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains. Accessed on February 1, 2021.

[6] News Center Microsoft Latinoamérica (16 junio 2020). "Explotar una crisis: Cómo se comportaron los cibercriminales durante el frote". https://news.microsoft.com/es-xl/explotar-una-crisis-como-se-comportaron-los-cibercriminales-durante-el-brote/. Accessed on February 1, 2021.

[7] Business Standard (7 agosto 2020). "UN reports sharp increase in cybercrime during coronavirus pandemic". https://www.business-standard.com/article/technology/un-reports-sharp-increase-in-cybercrime-during-coronavirus-pandemic-120080700289_1.html; Phil Muncaster (April 1, 2020). "Cyber-Attacks up 37% over past months as #COVID19 bites". https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/. Accessed on February 1, 2021.

[8] Maggie Miller (16 abril 2020). "FBI sees spike in cybercrime reports during coronavirus pandemic". The Hill. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

[9] Unisys. Unisys Security Index. https://www.unisys.com/unisys-security-index; Mundo Contact (1° julio 2020). "Cibercrimen aumenta 74% en AL durante la pandemia". https://mundocontact.com/cibercrimen-aumenta-74-en-al-durante-pandemia/. Accessed on February 1, 2021.

[10] September 2020sawan exponential increase in cyberattacks throughout Latin America, with Argentina, Brazil, and Mexico being the countries at greatest risk. See: Agencia EFE (September 30, 2020). "Argentina, Brasil y México, más vulnerables al cibercrimen en Latinoamérica". https://www.efe.com/efe/america/tecnologia/argentina-brasil-y-mexico-mas-vulnerables-al-cibercrimen-en-latinoamerica/20000036-4355566. Accessed on February 1, 2021.

[11] For further details on the characteristics of the mostcommon cyberattacks during the COVID-19 pandemic, see: Cyber-security Programof the Organization of American States (OAS) (2021), Twitter Alfabetismo y Seguridad Digital. Mejores prácticas en el uso de Twitter. https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-seguridad-digital-Twitter.pdf . See also: United Nations Office on Drugs and Crime (UNODC) (14 April 2020). Cibercrime and Anti-Money Laundering Section. "Cybercrime and COVID19: Risks and Responses". https://www.unodc.org/documents/Advocacy-Section/EN_-UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf; INTERPOL (August 4, 2020). "Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19". https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19; EUROPOL (October 5, 2020). "Internet Organised Crime Threat Assessment (IOCTA)". https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020; Council of Europe (March 27, 2020). "Cybercrime and COVID-19". https://www.coe.int/en/web/cybercrime/-/cybercrime-and-covid-19; INTERPOL, "COVID-1a Cyberthreat". https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats. Cibersecurity & Infraestructure Security Agency (8 abril 2020). "UK and US Security Agencies Issue COVID-19 Cyber Threat Update". https://www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update. Accessed on February 1, 2021.

This list of cybercrimes clearly exemplifies what is happening in digital spaces and the threats are likely to continue evolving in line with changing conditions associated with the COVID-19 pandemic. Nevertheless, it is important to note that the increase in cybercrime observed in recent months is no coincidence. In many cases, **COVID-19 has simply intensified pre-existing problems with cybersecurity**, by highlighting people's high level of vulnerability and exposure to online risks.

The new context has laid bare the technological paradox we have been experiencing for several years: **the vast majority of people are using technology, without being fully aware of the risks and consequences attached to using it**, in order to satisfy their connectivity needs, thereby too easily underestimating the fact that the Internet offers fertile ground to attackers and cyber-delinquents.

B. Different contexts, different cyber-risks

> *Awareness of the broad trends observed in cybercrime during the COVID-19 pandemic is vital for assessing the potential cyber-risks and dangers people are facing and will face in the "new normal" digital era and the range of digital security measures that be implemented.*

Nevertheless, when looking at this picture of the new digital ecosystem, we also need to bear in mind that people's online experiences, including their level of **exposure to threats and cybercrime**, differ and their impact varies depending on personal contexts and social factors, such as gender, geographical location, age, degree of education, or ethnic origin.

While a certain degree of idealism persists with the respect to the neutrality of the Web, the fact is, as digitization progresses, it is becoming increasingly clear that cyberspace is not the same for everyone nor is it immune to offline social issues. The technological era has revealed that people are not unidimensional; rather there is a continuity between their online and offline selves. This means that their identities and the social roles they perform offline are also transferred to cyberspace, where they shape their digital experiences and interactions and, hence, the cyber-risks they face.

A comprehensive understanding of digital security needs during the current crisis therefore requires acknowledgment that the online world reflects offline realities and that digital technologies replicate (and potentially exacerbate) the context in which people live offline.

Based on this premise, and in order to be able to identify the possible cyber-risks that women are facing at this time, we shall now examine how people's **gender**[12] **affects the impacts of the COVID-19 pandemic in cyberspace and cyber-crime,** on the understanding that mainstreaming this perspective is a prerequisite for devising digital security strategies that really work in these rapidly changing times.

[12] Gender refers to the roles, behavior, activities, and attributes that a society, at a given moment in time, considers appropriate for men and women, and to relations between women and men. Those attributes, opportunities, and relations are constucted socially and learned through the socialization process. They are specific to the context or epoch, and change over time. Gender determines what is expected, allowed, and valued in a women or a man in a given context. See: UN Women, Important Concepts Underlying Gender Mainstreaming. https://www.un.org/womenwatch/osagi/pdf/factsheet2.pdf

03 How are women faring in the new normal digital era? An analysis, from a gender perspective, of the digital ecosystem triggered by the COVID-19 pandemic

It has been shown that there are **marked differences between the type of cyber-crimes, abuse, and violence perpetrated online against women and those committed against men.** They each have specific manifestations and impacts, depending on gender (Millar, Shires, and Tropina, 2021; Brown and Pytlak, 2020).

While recognition of these differences has been gaining ground in cybersecurity circles, almost one year into the health crisis **there are still few analyses with a gender perspective of the pandemic's impacts on cyber-crime.** Thus far, studies of cyber-threats against women have focused on the various forms of online gender violence that have arisen or increased during the pandemic, disregarding the other threats and attacks women face in cyberspace. This lack of data unfortunately prevents us from ascertaining, with certainty, how women and girls are faring with the increased levels of cybercrime during this period of crisis.

To address this gap and achieve a better grasp of what is happening in cyberspace, this section underscores a series of factors to bear in mind for an analysis, with a gender perspective, of the cyber-threats facing women in the new normal digital era.

In general terms, we can say that adopting a gender approach or perspective entails analyzing the impact that people's biological and gender characteristics have on their interactions, opportunities, and social roles and revealing the dynamics of inequality and power differences between men and women[13].

Consequently, **bringing this perspective to the realm of cybersecurity shows how people's online experiences and the cyber-threats and harm they face vary, depending on their gender identity and sexual orientation.** It also reveals how **relations between men and women and gender inequality can have a bearing on matters such as the uses and risks of the Internet.** This gender approach entails asking oneself, for instance:

[13] "The gender approach is a way of looking at reality that identifies the roles and tasks performed by men and women in a society, along with the asymmetries, power relations, and inequities between them. It helps to recognize and explain the causes of those asymmetries and inequalities and to put forward measures (policies, mechanisms, affirmative actions, standards, and so on) that contribute to overcoming gender-based social gaps." Rworld. Glosario de términos relacionados al enfoque de igualdad de género. https://www.refworld.org.es/pdfid/5af1c8114.pdf

How do men and women inhabit cyberspace and what are the specific risks they run?

What are women and girls experiencing in the current context of cyber-crime?

What specifically different forms of harm are done to women by cyber-attacks?

The adoption of this perspective also reveals another aspect worth bearing in mind: digital technologies are not neutral. On the contrary, a person's gender influences and conditions access to the Internet, the use made of it, and the risks associated with it. Those differences persist through the various stages of life and interact with other social determinants, such as men and women's level of education, age, location, socio-economic status, sexual orientation, or ethnic origin.

As the World Health Organization (WHO) has acknowledged, the impacts of pandemics are never gender-neutral and, for that reason, global and national strategic plans to prepare for and address COVID-19 must be rooted in sound gender analysis and insight into the way gender interacts with other areas of inequality (WHO, 2020). That assertion naturally applies also to the impacts that the pandemic is having on cyberspace and to the cybersecurity policies and measures that need to be espoused to stem the current sharp surge in online threats and cybercrime.

Consequently, applying gender analysis to the new digital ecosystem prompted by the COVID-19 pandemic will enable us to identify the different patterns of exposure to cyberthreats that men and women are facing and the most appropriate digital security measures to protect them.

With that in mind, we will now propose a three-pronged analytical framework for showing women's differentiated experiences with the Internet and their specific needs. These three components are basic for grasping the level of vulnerability and types of risk women could be facing in the new digital ecosystem. They are:

ONE — **The conditions under which women access the Internet.**

TWO — **Gender inequality and the online-offline impacts of the COVID-19 pandemic.**

THREE — **The uses to which women put the Internet.**

A. What obstacles are women facing in cyberspace? Digital gender divides

> *The first factor to consider when analyzing the distinct impacts of cyberthreats on women is the fact that women do not have full and high-quality access to the Internet on an equal footing with men nor the knowledge needed to both protect themselves and make the most of what it can offer them.*

The COVID-19 pandemic has exposed the devastating consequences that a lack of access to the Internet, or insufficient access to it, may have for people who, deprived of the contacts or information it provides, are rendered more vulnerable to the virus, less connected to their loved ones, and cut off from government strategies to address the crisis. Unfortunately, that is the scenario in which millions of women and girls in the world now find themselves, for lack of adequate access to the web (Brown and Pytlak, 2020).

Even though reportedly women are using the Internet much more frequently than they used to, gender-based digital gaps[14] persist at numerous levels. According to the latest reports of the International Telecommunication Union (ITU), 51% of the global population (approximately four billion people) was online in 2019[15]. Of them, **only 48% of women had access to the Internet, compared to 55% of men, meaning that, in relative terms, the global gender gap is 17% (ITU, 2020).** The ITU also reported that in low and medium-income countries women are 10% less likely than men to have a mobile phone (ITU, 2020b), a factor that has major consequences, given that mobile phones are the medium most often used to access the Internet[16].

[14] The term gender gap (or divide) refers to any disparity between the status or position of men and women in society. Those gaps are differences in terms of opportunities, access, control over and use of resources constructed around biological differences and a product of historically discriminatory attitudes and practices obstructing the enjoyment and exercise of rights by men and women.

[15] In 2020, the ITU found that major connectivity gaps persist in rural areas in developing countries. Worldwide, 72% of households in urban areas have Internet, compared to 38% in rural areas. As regards connectivity in the region, ECLAC pointed out that, in 2019, 67% of urban households were connected to the Internet, compared to only 23% in rural areas. For its part, the Inter-American Development Bank (IDB) found that, in 2017-2018, access to the Internet in Latin America and the Caribbean was 63% for men and 57% for women, while mobile phone use was 80% for women and 83% for men. The World Wide Web Foundation also reported that men are 21% more likely to be online than women, a percentage that increases to 52% for least developed countries worldwide. See: World Wide Web Foundation (2020). The gender gap in internet access: using a women-centred method. https://webfoundation.org/2020/03/the-gender-gap-in-internet-access-using-a-women-centred-method/. Accessed on February 1, 2021; CEPAL (2020). Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19; IDB (2020). ¿Desigualdades en el Mundo Digital? Brechas de Género en el Uso de las TIC.

[16] It has also been documented that boys are 1.5 times more likely to have a telephone than girls. See: Jessica Posner Odede (August 2, 2019). "Yes, technology can liberate girls around the world-but it must be managed properly". World Economic Forum. https://www.weforum.org/agenda/2019/08/getting-girls-online-first-step-achieving-gender-equality/. Accessed on February 1, 2021.

It is worth recalling, too, that this gap in basic access to the Internet forms part of a much wider gender divide, encompassing all the ways in which women are less able to use and influence technology and exacerbated by the confluence of other exclusion factors, such as educational level, geographical location, age, socioeconomic status, or ethnic origin (Chair et al, 2020).

It has been documented that women and girls are not only more disconnected from the digital world. When they do access the Internet, they also have less meaningful connectivity[17] and account for a larger percentage of digital illiteracy, which implies that they are less skilled at understanding, controlling, and generating ties with technology that make them feel comfortable with it[18]. Compared with men, **women also possess fewer digital security skills**, which severely impairs the enjoyment and exercise of their human rights on line and their chances of freely and autonomously browsing the web (Chair et al, 2020).

Women also confront **time and content constraints on their access to the Internet** (Brown and Pytlak, 2020). For example, there are studies indicating that women are 25% less likely than men to know how to use digital technology to carry out basic tasks (ITU, 2020b: 13)[19], and, generally speaking, they make scant use of the Internet for financial empowerment purposes or to exercise their rights (Chair et al, 2020). Women also make little use of the Internet for e-commerce or moving funds and are estimated to make up 56% of persons who are financially excluded from the digital economy[20]. Moreover, given that women perform most unpaid domestic chores and care-giving tasks, they frequently have less time to explore cyberspace or to learn how to develop new digital skills, and when there are a limited number of electronic devices at home they often let other family members use them.

These gaps in Internet access and use and in the level of skills and digital culture tend to perpetuate gender inequalities, including inequalities related to lack of information (informational poverty), because **"they place women at a disadvantage with respect to the opportunities afforded by the new digital tools not just for employment, but also for political and social participation, and the exercise of civic rights"** (Sainz et al, 2020).

[17] According to Alliance for Affordable Internet, "meaningful connectivity" includes minimum thresholds of regular access to the Internet, an appropriate device, sufficient data and fast connection. See: Alliance for Affordable Internet. "Meaningful Connectivity- unlocking the full power of internet access". https://a4ai.org/meaningful-connectivity/. Accessed on February 1, 2021.

[18] World Wide Web Foundation (agosto 2018), Advancing Women´s Rights Online: Gaps and Opportunities in Policy and Research. http://webfoundation.org/docs/2018/08/Advancing-Womens-Rights-Online_Gaps-and-Opportunities-in-Policy-and-Research.pdf; Organization for Economic Co-operation and Development (OECD) (2018). Bridging the Digital Gender Divide: Include, Upskill, Innovate. http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf; Araba Sey y Nancy Hafkin (eds.) (2019). Taking Stock: Data and Evidence on Gender Digital Equality, United Nations University. https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf. Accessed on February 1, 2021.

[19] In the region, 35% reported that they did not know how to use a digital smart phone and 40% said they did not know how to use the Internet. See: IDB (2020). ¿Desigualdades en el Mundo Digital? Brechas de Género en el Uso de las TIC.

[20] World Bank Group (2018), "La base de datos Global Findex 2017. Medición de la inclusión financiera y la revolución de la tecnología financiera. Reseña", https://openknowledge.worldbank.org/bitstream/handle/10986/29510/211259ovSP.pdf. Accessed on February 1, 2021. [English: The Global Findex Database 2017. Measuring Financial Inclusion and the Fintech Revolution. Overview. https://globalfindex.worldbank.org/sites/globalfindex/files/2018-04/2017%20Findex%20full%20report_0.pdf]

In particular, **in connection with the COVID-19 pandemic, lack of access to ICTs and low levels of digital literacy have propitiated the exclusion of women** from actions being undertaken in the health, education[21], and labor sectors that use digital technologies to address the emergency and have limited their access to public information and news about confinement and quarantining measures and about support or subsidy programs (CIM, 2020b; ECLAC, 2020: 5). Lacking sufficient digital access or skills, women are in a weaker position to receive vital information, understand it, and consequently act on it in a timely manner (UIT, 2020a: 14), which places their health and wellbeing at risk.

Finally, it is important to bear in mind that, in today's era of increasing digitization, these digital divides not only render women more vulnerable: they also impact society as a whole. Given that women "perform a disproportionate role as front-line workers, care-givers, and educators, the gender gap has additional costs for families, communities, and economies" (Chair et al, 2020b: 5), who depend on them to be able to maintain their wellbeing, health, and, in many cases, their lives.

B. The continuity of online-offline issues: gender discrimination and the impacts of the COVID-19 pandemic on women

> *The second factor to bear in mind when analyzing the gender impacts of the pandemic in cyberspace is that the online experiences and cyber-threats women face are inseparable from the realities they live with offline (Brown and Pytlak, 2020), which are shaped by the systemic inequalities that affect all aspects of their lives and have been exacerbated by the health crisis.*

As the United Nations has acknowledged, women rank below men in all sustainable development indicators and account for the largest segment of persons living in poverty and without access to education[22]. That **inequality is also replicated with respect to ICTs**[23], an area in which women's participation barely reaches 20% (22% in Artificial Intelligence and 11% in the area of cybersecurity)[24]. According to one estimate, it will take at least 100 years to achieve gender parity in the digital technologies sectors[25].

[21] Given that they frequently lack access to on-line education methods (including the lack of electronic devices and/or connection data), girls and young people are at risk of undergoing increasing exclusion as more and more schools close during the health crisis. If we bear in mind that women and girls account for the largest percentage of poor people in the world, and that boys are 1.5 times more likely than girls to own a cellphone, it is probable that a large number of girls and female adolescents are having their education interrupted during the crisis either because at home they lack the data or devices for connection or because, if they do have them, traditionally many families attach greater value to boys' education than to that of girls, so that probably it is the boys who use whatever devices are available in the home. See: The United Nations Educational, Scientific and Cultural Organization (UNESCO), ¿Cómo estás aprendiendo durante la pandemia de COVID-19? https://es.unesco.org/covid19/educationresponse; [English: see https://en.unesco.org/covid19/educationresponse/learningneverstops] Vodafone Foundation, MITD-Lab and Girl Effect, Executive summary. Real girls, real lives, connected. A global study of girls' access and usage of mobile, told through 3000 voices, https://static1.squarespace.com/static/5b8d51837c9327d89d936a30/t/5bbe7cbe9140b7d43f282e21/1539210748592/GE_VO_Executive+Summary+Report.pdf

[22] Worldwide, only 49.6% of women form part of the economically active population, compared to 76% for men, and the salary gap remains 16%: a basis source of income inequality throughout women's lives. Women also continue to account for more than two-thirds of the world's illiterate people and, despite progress in recent years, school enrolment of girls is still below the enrolment rate for boys (above all in secondary and higher education), as women and girls face such hurdles as forced marriage and early pregnancy, gender violence, and traditional attitudes privileging education for boys over education for girls. Violence also continues to be a systemic factor in the ongoing subordination of women. One in every three women has beeen a victim of physical or sexual violence, mainly perpetrated by a partner: a reality that has been called a global pandemic that also extends to cyberspace. See: UN Women (25 September 2015). "Infografía: Igualdad de género- ¿Dónde nos encontramos hoy?"; Noticias ONU (14 February 2018). "Las mujeres están por debajo de los hombres en todos los indicadores de desarrollo sostenible", https://www.unwomen.org/es/digital-library/multimedia/2015/9/infographic-gender-equality-where-are-we-today; UN Women, "Mujeres y Pobreza". https://news.un.org/es/story/2018/02/1427081; https://beijing20.unwomen.org/es/in-focus/poverty. Accessed on February 1, 2021.

[23] PWC, "Women in Tech. time to close the gender gap". https://www.pwc.co.uk/who-we-are/women-in-technology/time-to-close-the-gender-gap.html. Accessed on February 1, 2021.

[24] World Economic Forum. "Assessing Gender Gaps in Artificial Intelligence". Global Gender Gap Index 2018, http://reports.weforum.org/global-gender-gap-report-2018/assessing-gender-gaps-in-artificial-intelligence/; The Conversation (2020). "The lack of women in cybersecurity put us all at greater risk". The Next Web. https://thenextweb.com/syndication/2020/06/28/the-lack-of-women-in-cybersecurity-puts-us-all-at-greater-risk/ Accessed on February 1, 2021.

[25] Cade Metz (June 21, 201). "The gender gap in computer science research won't close for 1000 years". The New York Times. https://www.nytimes.com/2019/06/21/technology/gender-gap-tech-computer-science.html. Accessed on February 1, 2021

These conditions of inequality and vulnerability have been magnified by the pandemic. As the Inter-American Commission of Women has stressed, "The emergency stemming from COVID-19 has specific impacts on women and is deepening existing gender inequalities" (CIM, 2020b: 4), above all for those women and girls who face multiple forms of discrimination on account of their race, ethnic origin, religion or beliefs, disability, age, sexual orientation, social class, and migration status (European Women's Lobby, 2020).

The pandemic has increased levels of poverty among women, affected their work, and widened gender divides in employment. Prior to the health emergency, women held most of the jobs in services and most of the precarious, insecure, and informal jobs[26], that is to say, the sectors hardest hit in recent months[27].

Women also make up 70% of personnel in the health, care-giving, and social assistance sector and most of the front-line medical staff responding to the crisis, at a higher physical and emotional cost to themselves and at greater risk of being infected[28]. In several countries, these women have also been victims of increasing discrimination, xenophobia, and stigmatization, derived from anxiety and fear of catching COVID-19 (UN Women, 2020d).

In addition to the above, many women have experienced an increase in the burden of domestic chores and caregiving tasks, to the detriment of their paid productive work[29]. Prior to the pandemic, women all over the world were doing almost three times more unpaid caregiving and domestic work than men, a figure that has increased during the health emergency[30]. The saturation of health systems, school closures, and confinement measures have led to a larger number of people in the home in need of food, care, and education, and many women have had to give up their jobs, reduce their working hours, or eschew full-time jobs in order to take on caregiving and domestic chores and supervise their children's learning processes: all of which has had major impacts on their physical and mental health, their independence, and the amount of time they have for themselves (CIM, 2020c; CIM 2021; UN Women 2020f).

The conditions generated by the emergency have also increased violence against women, leading some analysts to assert that under cover of the COVID-19 pandemic a gender violence pandemic is also emerging (CIM, 2020a; UN Women, 2020c). In all countries, higher rates of domestic violence have been recorded, derived from confinement measures and increased tensions and conflicts within households, as women and girls have been forced to stay home in the permanent company of their aggressors (CIM, 2020a). According to UN estimates, for every three months of ongoing confinement, there are 15 million more cases of gender violence worldwide[31]. That, too, will limit women's access to the Internet and their acquisition of digital skills.

---

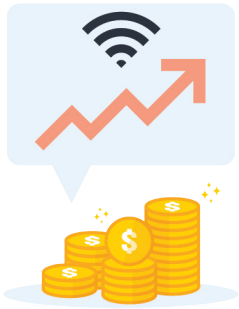
[28] Research has shown that in countries such as Germany, Italy, Spain, and the United States the number of health workers infected with COVID-19 is two to three times higher among women than among men. See: Global Health 5050. The COVID-19 Sex-Disaggregated Data Tracker. https://globalhealth5050.org/the-sex-gender-and-covid-19-project/. Accessed on February 21, 2021.

[29] The amount of time devoted to children's education is estimated to have increased by 36% and that devoted to family purchases by 24%. See: UN Women (20 October 2020). "El avance de las mujeres hacia la igualdad se estanca" https://news.un.org/es/story/2020/10/1482722; Matt Krentz et al (May 21, 2020). "Easing the COVID-10 burden on working parents". BGG; https://www.bcg.com/publications/2020/helping-working-parents-ease-the-burden-of-covid-19; Richard Blundell et al (June 11, 2020). "COVID-19: the impacts of the pandemic on inequality". Institute for Fiscal Studies. https://www.ifs.org.uk/publications/14879. Accessed on February 1, 2021.

[30] In the United States and Europe, women took on an extra 15 hours a week of unpaid domestic and caregiving workload. That change was even more marked in the case of women in charge of single-parent households, which account for 75% of the global total. There is also evidence indicating that, during the pandemic, mothers have been more likely than fathers to lose their jobs either temporarily or permanently, losing up to 60% of their income.
See: Matt Krentz et al (May 21, 2020). "Easing the COVID-10 burden on working parents". BGG. https://www.bcg.com/publications/2020/helping-working-parents-ease-the-burden-of-covid-19

[31] United Nations (28 April 2020). "Millones de mujeres sufrirán embarazos no deseados durante la pandemia de coronavirus". Noticias ONU. https://news.un.org/es/story/2020/04/1473572. Accessed on February 1, 2021. [English, see https://news.un.org/en/story/2020/04/1062742: COVID-19 could lead to millions of unintended pregnancies, new UN-backed data reveals].

Prior to the COVID-19 pandemic, women without connection to the Internet in Global South countries already pointed to high cost as one of the principal reasons hindering access to the Internet (World Wide Web Foundation, 2015)[32]: a situation that presumably will be exacerbated by their major loss of income and jobs during the pandemic.



Negative medium and long-term impacts are likewise to be expected on the development of girls' and young women's digital skills, given the overall repercussions of the pandemic for their education. In previous epidemics, school closures were found to have disproportionately affected girls, many of whom never go back to school since they find themselves forced to compensate losses in family income, or fall victim to child marriage, violence, and/or sexual exploitation. (UN Women, 2020e: 14-15). That being so, disruptions of girls' and young women's education during the COVID-19 pandemic are highly likely to impede their significant access to, and use of, the Internet, since it has been ascertained that education is one of the main drivers of the gender gap in access to ICTs. Some studies show that women with only basic education are six times less likely to be connected to the Internet than those who have completed secondary school (World Wide Web Foundation, 2015).

In addition to the above, multiple forms of cyber-abuse and online violence have surged during the COVID-19 crisis almost as much as domestic violence (APC, 2020; UN Women, 2020a; Brudvig et al, 2020). According to a series of sources, online gender abuse has increased by as much as 38% (Glitch UK, 2020), particularly in the form of non-consensual distribution of intimate images and acts of sextortion, cyber aggression and harassment, online sexual violence, as well as of "grooming" and sexual exploitation facilitated by ICTs against women and girls (UN Women, 2020a; CIM, 2020a; *Derechos Digitales*, 2020)[33].

Online violence, which is one of the most blatant manifestations of gender inequality in cyberspace, also increases the digital divide confronting women and girls, inducing them to self-censor themselves or to keep a low profile for fear that their privacy or security will be violated. It also impairs their ability to move freely and fearlessly in online spaces, denying them the opportunity to interact with the technologies they need to forge their own, autonomous, digital identities (REVM-ONU, 2018: para. 29)[34].

As indicated in Section IV, these conditions of gender-based inequality and discrimination against women are echoed in cyberspace and give rise to many of the cyber-threats to which they are exposed, since they shape Internet use patterns and possible on-line vulnerabilities.

[32] According to the Women's Rights Online investigation conducted by the World Wide Web Foundation in 10 developing countries, the cost in those countries of 1 GB of pre-paid data (equivalent to 13 minutes of Internet per day, not counting video costs) was equal to 10% of average per capita income, which is 10 times higher in relation to income per capita than the cost in OECD countries and double what a person spends on health in developing countries. See: World Wide Web Foundation (2015). Women's Rights Online. Translating Access into Empowerment. http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf Accessed on February 1, 2021.

[33] According to a study by Glitch UK and the End Violence Against Women Coalition, 46% of those surveyed said they had been victims of on-line violence. Of those abused online one year prior to the pandemic, 29% said that the abuse had become worse: a figure that increases to 38% in the case of black women or non-binary persons.

[34] According to research conducted by the United Nations Special Rapporteur on violence against women, 28% of women victims of online gender violence had deliberately reduced the amount of time they spend on line. See: Special Rapporteur on Violence against Women, its causes and consequences (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights A/HRC/38/47. United Nations..

C. What do we know about the ways women are using the Internet during the COVID-19 pandemic?

> *Finally, a third important analytical factor that needs to be borne in mind is that* ***the uses made of the Internet are, quantitatively and qualitatively, conditioned by a person's gender.*** *Major differences have been found in the ways men and women browse in cyberspace and in the objectives they pursue when they connect to it (Brown and Pytlak, 2020).*

Prior to the pandemic, studies found that the purposes for which women use the Internet have more to do with social wellbeing, keeping in touch with family members and friends (by receiving or making calls, and chatting), and with finding health-related information (Agüero, Bustelo, and Viollaz, 2020; Sainz, 2020; Brown and Pytlak, 2020). Men, on the other hand, tended to use the Internet to send e-mails, seeks news and information about the weather and transportation, access e-banking services, and entertain themselves with video games, listening to music, and watching videos. In addition, men tended to make more intensive and varied use of electronic devices and made more use of the Internet than women to conduct economic, work-related, and administrative activities (for example, to perform online procedures/formalities) (Agüero, Bustelo and Viollaz, 2020; Sainz, 2020).

It has also been documented that women depend on the Internet more than men to exercise certain rights. For instance, the Internet can facilitate their access to education if their household responsibilities prevent them from going to an educational facility; help them express their views if they live in especially oppressive communities; access information about sexual and reproductive rights if it is not available offline; or protect their personal security in cases of domestic violence (Brown and Pytlak, 2020).

While the expedited digitization that has occurred during the COVID-19 pandemic has radically modified both men and women's habits with regard to the use of electronic devices and the Internet, given the persistence of gender roles and standards in and outside cyberspace, it is highly likely that some of those usage tendencies have continued during and after the crisis. As mentioned earlier, certain studies are still needed to give us a fuller picture of how women have been using the Internet during this period. Nevertheless, some possible scenarios can be projected based on prior browsing trends and the impacts that the pandemic is having on their lives.

Thus, given that during this phase women have taken on a larger share than men of unpaid domestic and caregiving chores, it is fairly safe to say that they are mainly using the Internet as a means of staying in touch with their family members and friends, in order to ascertain their state of health, as well as to purchase food and medicines online, elicit news as to how the disease is evolving, and to facilitate their children's distance education. Likewise, given that women are a majority of the health sector personnel, it is likely that they are using technology to provide remote consultation facilities and to coordinate care and social welfare work in communities.

Other impacts of the pandemic on women's lives provide further clues regarding their uses, needs, and priorities when accessing the Internet during this period. For example, given the high percentage of women who were self-employed or worked in the informal sector, it is to be expected that some of them are trying to keep their business going **via e-commerce platforms or are for the first time tapping into sites offering jobs**, given the huge increase in female unemployment. In a similar vein and given the number of girls enrolled in primary schools, it is also likely that they (and their families) have had to rapidly overcome the gender stereotypes that traditionally hamper their access to technologies in order to take part in digital format classes.

Some other usage trends have been confirmed as the health crisis advances. For example, it is now known that, continuing a prior trend, women and young people are using the Internet during this period **to elicit information regarding their sexual and reproductive health**, for which services have been suspended in many parts of the world as budgets have been cut and preventive physical distancing measures have been introduced[35].

In addition, given the increase during this period of gender-based violence against women, in and outside the Internet, women are using digital devices as a lifeline **to request help and stay in touch with their support network**, using instant messaging with geo-tracking functions, free hotline calls to report domestic abuse, or apps providing support and information to survivors monitored by their abusers. More and more women are also resorting to the Internet **to report and publicize online acts of gender-based violence** against them and to create support networks for victims.

Undoubtedly, much more remains to be investigated about women's and girls' experiences with using the Internet in this period and more research with a gender perspective is needed into the impacts of the pandemic on the new digital ecosystem. However, as pointed out above, a combined examination of the dynamics of women's access to, and use of, the Internet and the impacts that the pandemic itself is having on their lives offline can provide us with initial insights into their digital experiences and, based on them, their needs, interests, and vulnerabilities when they access the Internet.

[35] Ximena Casas (12 Mayo 2020). "Protecting Women's Reproductive Health During the Pandemic". Human Rights Watch. https://www.hrw.org/news/2020/05/12/protecting-womens-reproductive-health-during-pandemic. Accessed on February 1, 2021.

04 Cyber-threats and specific risks women face in the new digital ecosystem: ongoing reflections

> *Given the dearth of studies and data broken down by sex on the prevalence of cybercrime during the pandemic, this section* ***contains a projection of possible threats women are reportedly facing in cyberspace during the COVID-19 pandemic.***

As the following will show, women's experiences in cyberspace reveal that the dangers and threats they face online have specific characteristics and affect them differently because of the gender roles, discrimination, and inequality they experience online and offline. (Brown and Pytlak, 2020).

It is worth stressing that the list of cyber-threats identified is indicative and by no means exhaustive, given that the constant changes observed in cyberspace and in online-offline interactions suggest that the types of cyber-threats and danger women face are likely to change as the COVID-19 pandemic evolves.

A. One widespread risk factor: the lack of digital security skills

In this risk identification scenario, special mention should be made of the level of digital security skills possessed by women. That is a factor that largely determines the type of cyber-attacks they face and the consequences of those attacks for their lives.

As pointed out above, the COVID-19 pandemic has laid bare the widespread lack of basic know-how for preventing online risks and threats and the high degree of exposure to cyber-risks. However, given the gender divide women face when it comes to acquiring digital skills in general and cybersecurity skills in particular, they find themselves especially vulnerable to cyber-attacks.

Added to that is the persistence of the gender stereotypes that preclude them boosting their digital skills. Many women think of cyberspace as an irremediably insecure place for women and girls, a reaction based on prejudices and preconceived notions regarding their supposedly natural inability to understand and master technologies. Exacerbating that are the effects of the system gender-based violence that has permeated cyberspace and made online aggression against them appear almost normal.

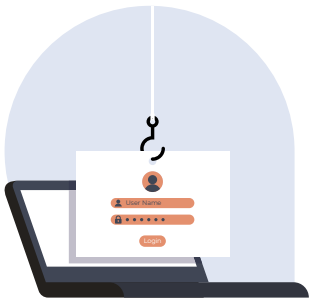
All this results in a large number of women left with few or no resources with which to confront illicit and abusive behavior online, which renders them more exposed than men to the risk of being victims of certain forms of cyber-attack, many of which are aimed at easy targets (UNODC, 2020).

Here it should also be mentioned that this lack of cybersecurity skills has additional repercussions, permeating all the digital interactions women engage in online and transcending cyberspace, given the continuity between their online and offline lives. Digital security is also a human rights issue, and the fact that women feel insecure online affects not just their access to the Internet, but also to all the opportunities it affords for exercising their online and offline rights.

This lack of skills also impacts their families and communities. It is women who, during this health crisis, have taken on the bulk of the unpaid care-giver work and supervision of their children's learning processes, during the closure of schools, so that their relative ignorance regarding potential cyber-threats against children and adolescents, or older adults, in the new-normal digital era also places the people under their care at risk[36].

B. Exploring some of the risks women face in the new normal digital era

While much is still unknown regarding the gender dimension of security incidents and the specific threats that women are facing in cyberspace during the COVID-19 pandemic, when we analyze the cyber-attacks most commonly reported worldwide during the pandemic together with women's experiences in and outside cyberspace, we can discern some kinds of online threats that particularly affect them:



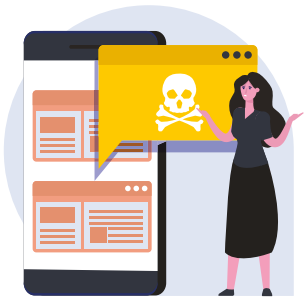
Certain kinds of fraud and scams through *phishing* campaigns or the dissemination of *malware.*

Given the preponderant role of women during the health crisis in unpaid domestic and care-giver work for families and communities, it is likely that the kind of phishing attacks that would pose the greatest risk for them are related to their purchases of food and medicine or searches for health information.

[36] In the case of children and adolescents, for instance, a lack of familiarity with virtual education processes and basic digital protection measures may put them at greater risk of "grooming," sexual violence, sextortion, or access to fake information.

Fraud and scams targeting women engaging in e-commerce, the use of mobile money services, or receipt of cash transfers under social programs.

Given that prior to the pandemic women accounted for more than half of all persons financially excluded from the digital economy, it is likely that cyber-attacks are directed specifically against new users, given their lack of familiarity with digital financial tools and their scant knowledge of cybersecurity techniques for protecting their online transactions. It is also likely that those attacks have a greater impact on women's finances than cyberattacks targeting men, given the high levels of gender inequality in employment and income.



Fraud via *phishing* targeting older women.

There have been reports of an increase in attacks on the elderly during this period, in the form of fraudulent e-mails, telephone calls, or instant messaging, in which cyber criminals attempt to pass themselves off as persons the victim trusts (such as a bank or medical personnel) with a view to eliciting personal data. In the current context of greater use of the Internet, elderly women are especially vulnerable to cyber-attacks, given their relative lack of IT skills in general, and cybersecurity skills in particular, compared to men in the same age-group[37].

Disinformation (fake news) campaigns.

Infodemic and the distribution of fake news is an online risk to which women, in particular, are exposed given that they above all use the Internet to obtain health-related news. Studies have pointed to a marked gender dimension in disinformation activities, given that gender identity and sexual orientation may become the reason why someone receives information, when assumptions are made about that person's interests and ability to be influenced (Brown and Pytlak, 2020).

[37] Women are over-represented among older adults (they make up 57% of persons over 70 years of age and 62% of those over 80) and they are three times more likely than men to live on their own. Studies in Europe show that only 48% of persons over 65 years of age possess digital skills and that older women have fewer skills than men, the difference being 10 percentage points. One finding is that only half of people aged between 65 and 74 who used the Internet in the previous 12 months possessed some kind of IT security software in their devices, and 13% said they did not know what they were. In addition, a large number of older adults do not use passwords in their devices for fear of forgetting them, or else they use weak passwords easily identifiable by hackers. The IT security firm McAfee reported that 50 percent of users of social networks aged 60 or more choose to share personal information with people they have never met in person and without any kind of security precautions. See: Abby Ellin (September 12, 2019). "Scammers Look for Vulnerability, and find it in Older People". The New York Times. https://www.nytimes.com/2019/09/12/business/retirement/scams-elderly-retirement.html; UN Women (May 2020). "Policy Brief: The Impact of COVID-19 on older persons". https://www.un.org/sites/un2.un.org/files/old_persons_spanish.pdf; Enrique Arieas Fernandez et al. (2018). "Acceso y uso de las TIC de las mujeres mayores de la Europa comunitaria". Prisma Social. Revista de Ciencias Sociales. No. 21. https://revistaprismasocial.es/article/view/2458. Accessed on February 1, 2021.

Attacks via *software*, networks and/or remote work tools.

Cyber-attacks frequently take advantage of distracted use of remote work tools to penetrate corporations' IT systems. This risk arises when an employee is tired or constantly distracted, which is frequently the case for women who, during this period, are having to combine their paid productive work with increased unpaid domestic and care-giving chores and end up doing two or three times their normal working hours (CIM, 2020c; UN Women, 2020f).

***Ransomware* attacks on hospitals through the electronic devices of female members of the medical staff.**

While research is still needed in this area, it is likely that ransomware attacks on hospitals or health centers have a gender slant, since women make up the majority of health workers and may be an easy target for cyber-attacks given that they are less familiar than their male colleagues with digital security techniques.

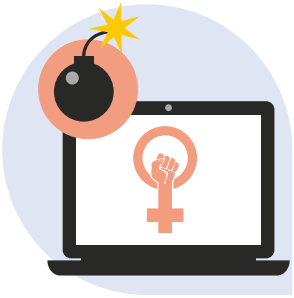
On-line gender violence.

It has been ascertained that online gender-based violence against women increases in direct proportion to their access to the Internet (REVM-ONU, 2018; EIGE, 2017; Van Der Wilk, 2018). Similarly, studies during the health crisis have confirmed that, in line with their increased participation in cyberspace, women are disproportionately falling victim to cyber-attacks and cyber-harassment, the non-consensual distribution of intimate and sexual images, doxing, sexual violence in the form of trolling, reception of unsolicited sexual images and videos, and threats of sexual violence (UN Women, 2020[a]; Glitch UK; APC, 2020).

In addition, continuing trends observed prior to the pandemic, digital gender violence is especially targeting women who are active on social networks, such as journalists reporting on the pandemic, activists, bloggers, human rights defenders, and women with a public profile who use social networks to advocate gender equality, and who have reported being victims of disinformation and smear campaigns (AI, 2018; REVM-ONU, 2018; UN Women, 2020a)[38].

[38] See: Julie Posetti et al (2020). Online violence against women journalists. A global snapshot of incidence and impacts. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000375136. Accessed on February 1, 2021; Maria Giovanna Sessa (December 4, 2020). "Misogyny and Misinformation: An analysis of Gender Disinformation Tactics during the COVID-19 Pandemic". EU Disinfo Lab. https://www.disinfo.eu/publications/misogyny-and-misinformation:-an-analysis-of-gendered-disinformation-tactics-during-the-covid-19-pandemic/. Accessed on February 1, 2021.

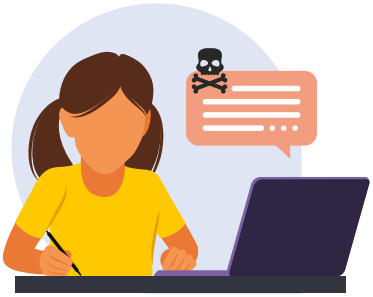
Attacks on feminist organizations or women's groups working in fields relating to gender equality and sexual and reproductive rights.



It has also been documented that online gender-based violence is specifically targeting women's organizations that are using the Internet during this period to stay connected and organize themselves, claim their rights, and provide support and care for victims of gender violence. These organizations have reported sabotaging of video calls and zoombombing[39] attacks via the sending of sexually explicit, racist, or sexist material to their communication channels, hacking of their websites, social networks, or e-mail accounts, Distributed Denial of Service (DDoS) attacks, and so on (APC, 2020).

Digital sextortion strategies.

It has been documented that this form of attack, which has increased significantly during the pandemic, has a major gender slant, focusing for the most part on women, young women, and girls , given that the public dissemination of intimate images has more serious consequences for them as a result of gender norms and stereotypes surrounding control of female sexuality[41]. The increase in this cybercrime stems from a combination of factors, including, notably, physical distancing measures and the need to use virtual tools to stay close to others, unsafe sexting practices, and sextortion scams via *phishing*.



***Grooming* and sexual harassment of girls and adolescents.**

As a result of the increased amount of time spent online, a parallel increase has been reported in surveillance, harassment, unsolicited contact, and the imposition of undesired sexual behavior on minors: cyber-attacks performed by using interaction opportunities such as online games, social networks, and chat rooms (INTERPOL, 2020).

[39] See: Lizle Loots et al. (April 14, 2020). "Online safety in a changing world- COVID-19 and cyber violence". Sexual Violence Research Initiative. http://www.svri.org/blog/online-safety-changing-world-%E2%80%93-covid-19-and-cyber-violence; Sophie Davies (March 18, 2020). "Risks of online sex trolling as coronavirus prompts home working". https://www.reuters.com/article/us-women-rights-cyberflashing-trfnidUSKBN2153HG. Accessed on February 1, 2021.

[41] Benjamin Wittes et al (May 11, 2016). "Sextortion: Cybersecurity, teenagers, and remote sexual assault". Brookings. https://www.lawfareblog.com/new-data-sextortion-124-additional-public-cases; Katherine Kelley (March 19, 2019). "New Data on Sextortion: 124 additional public cases". Lawfare. https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/. See also: Claudia Long (June 3, 2020). "Coronavirus shutdown prompts spike in reports of sextortion toe Safety Commissioner", ABC News. https://www.abc.net.au/news/2020-06-03/spike-reports-esafety-commissioner-coronavirus-shutdown/12314442. Accessed on February 1, 2021.

[41] Christina Elia (11 agosto 2020). "My sextortion birthday: Digital violence during COVID-19". Genderit.org. https://genderit.org/feminist-talk/my-sextortion-birthday-digital-violence-during-covid-19. Accessed on February 1, 2021.

Although data broken down by sex have yet to be gathered on the prevalence of these cyber-crimes, it may be surmised that grooming and sexual harassment pose a particular cyber danger for women and girls. Research conducted prior to the pandemic confirmed that they are twice as likely to be sexually harassed on the Internet[42] and that the types of violent comments they receive online are qualitatively different from those that boys and young men receive, are often based on their physical appearance, and include threats of sexual violence[43].

Sexual exploitation and trafficking of women and girls facilitated by new technologies.

Bearing in mind trends observed prior to the pandemic, it is safe to say that women and girls are at greater risk of falling victim to international trafficking in persons as a result of their increased poverty levels. Studies in this field have documented that 80% of the victims of trafficking in persons are women, who are also the victims in 95% of cases of sexual exploitation[44].

[42] Angus Reid (2016). Trolls and Tribulations: One-in-Four Canadians Say They're Being Harassed on Social Media. http://angusreid.org/wp-content/uploads/2016/10/2016.10.04-Social-Media.pdf

[43] According to a Plan Internacional study, almost 60% of girls and young women worldwide have been victims of some form of online cyber-harassment, in some cases when they are as young as 8 years old. See: Plan Internacional (2020). Inseguras Online. Experiencias de niñas, adolescentes y jóvenes en torno al acoso online. https://plan-international.es/inseguras-online. Accessed on February 1, 2021.

[44] European Parliament (2016). Briefing. The gender dimension of human trafficking 2016. http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI(2016)577950_EN.pdf; Sylvia Walby et. al. (2016). Study on the gender dimension of trafficking in human beings. Final Report. European Commission. https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._final_report.pdf

05 Digital security for women in the new digital ecosystem: a hard core of measures they can apply to protect themselves

> *The identification of possible risks that women are facing in the new-normal digital era is just the first step toward forging a gender-sensitive culture of cyber-security. Given the absence of high-quality information regarding the characteristics of these new scenarios, there is a need to gradually unravel and specify those digital risks in such a way as to generate a framework enabling women to protect themselves.*

This identification of risks must be accompanied by specific efforts by all sectors involved to highlight the tools women can use to protect themselves and safely and confidently browse the web. It is imperative to make them fully aware that in cyberspace there is a possibility of their being at risk and discriminated against just because they are women: a reflection of the same context of gender-based violence found offline.

As mentioned above, women's lack of personal digital security practices is a widespread problem, caused by the lack of high-quality information they receive. This failure to adopt digital security measures is not a problem attributable to women. On the contrary, a much greater effort is called for by all actors involved to close the gender gap in digital literacy and diminish the negative impacts of the gender stereotypes that hamper women's control over technology.

That being so, one of the principal messages worth underscoring in connection with a gender-sensitive cyber-security strategy is that, even though cyberspace is an environment that poses certain risks, women are not irremediably condemned to be victims; rather, they should receive the information they need to protect themselves and to prevent cyber-attacks and online acts of violence, by taking basic self-care precautions.

Likewise, it is important to bear in mind that the identification of these digital security practices (or their absence) must not be construed as a way of blaming women and girls for the online violence and cyber-attacks perpetrated against them. Those responsible are always the attackers and cybercriminals wreaking the damage, who must be punished for their behavior.

To address the risks women face, this section contains a hard core of basic measures for protecting women during the current health crisis. It is crucial to promote their adoption along with the development of cyber-security policies focusing on the identification of the conditions that facilitate those cyber-attacks and on prosecuting and punishing those responsible for them.

A. Basic kit of digital security measures for the new-normal era

Adopt a personal cybersecurity policy to address the pandemic

- **Realizing that one is a target. Awareness is the front-line of defense** against the new and changing cyber-treats emerging during the pandemic.
- **It is important to conduct a personal risk assessment:** What have I done to confront the risks associated with spending more time online and using new tools (such as browsing on sites that I am not used to, installing new apps, or purchasing from insecure sites)? What am I doing to protect myself from possible attacks?
- **Precaution is what matters most.** It is vital to stay alert and be more careful about how one interacts in the digital world. Now that the pandemic has forced us to espouse new technologies within a very short space of time, it is important to plan, train, and boost our digital protection as every new step we take in the digital ecosystem may create risks.
- **Human error is often needed for cyber-attacks to be successful.** When people are undergoing prolonged stress, tension, and tirednes, or when they are distracted, they are more prone to commit mistakes and lower their guard against possible cyber-risks.
- **The quest for information about COVID-19 is an especially critical area.** Many current cyber-attacks target people seeking information about the pandemic, so that only official or verified sites should be trusted, not only because of the quality of the information, but also because of the surge in malicious sites exploiting that need for information.
- **Cyber-crime is exploiting the fear and insecurity** prompted by COVID-19 and uses local news on how the pandemic is evolving. The baits used almost always replicate national news and are tailored to the victims' location.

- **Many attacks are not isolated, but deliberately combined.** For instance, unauthorized access to an electronic device may facilitate a scam or the hacking of a social networks account may serve to disseminate spam by promoting fraudulent purchases of medical products.
- **It is essential to be alert and** informed about new deceipts and cyber-threats and ways to respond to them.
- **Talk with your family,** including children and older adults, about the importance of protecting onself online. Digital corresponsibility within the family is worth fostering, because taking care in digital environments involves not just individual prctices, but also caring for the safety of others.

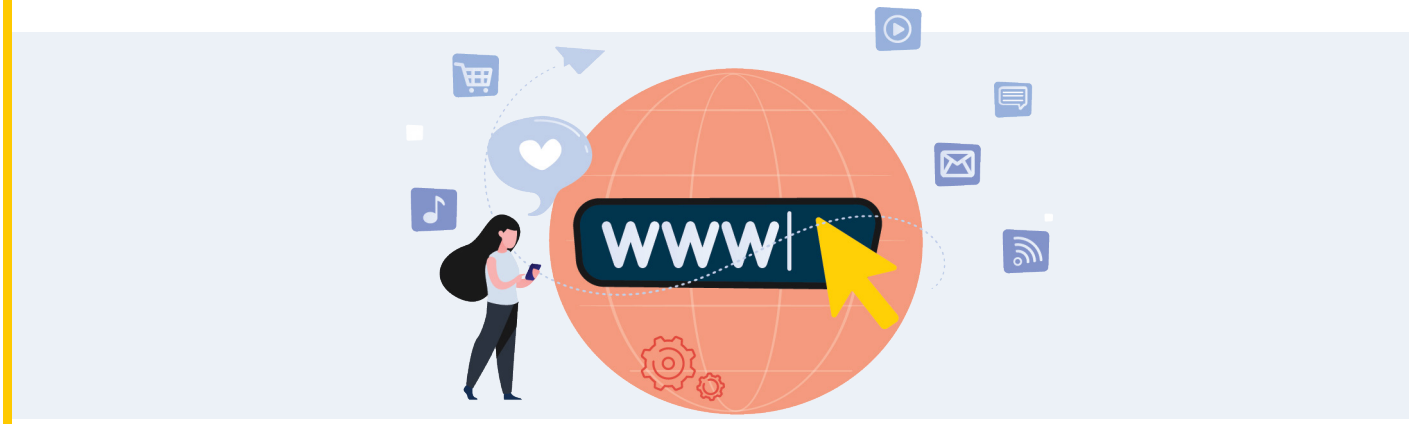
Safe passwords. Passwords as the first line of defense

Passwords are the first step for accessing accounts and devices and therefore provide a first layer of protection against threats and cyber-attacks. Therefore, a crucial part of digital secrity continues to be having sound personal habits with regard to on-line passwords.

- It is important to have **unique passwords that are long, random, and difficult to predict** (they should not contain personal information).
- To afford effective protection, passwords must include a mixture of at least 12 **upper and lower case letters, numberd, and special characters.**
- A **different password should be used for each account and should be changed frequently,** especially for more confidential accounts.
- Use automatic password generators and/or **online password administrators,** which create random passwords for each account.
- Use security questions in sites that allow that option, but the replies should not contain personal information.

- Do not store passwords in browser settings, in the cloud, or in an insecure document in the computer or telepone.
- Do not share passwords via an insecure connection, such as a text or SMS message.
- To add a second layer of protection, **activate two-stage verification** (two-factor authentication or 2FA), which is available for e-mail and social networks.

Safe browsing



- Only connect via **private and reliable WIFI networks.**
- With household networks, it is important to ensure that the Wifi router is not accessible from the outside and that it has a robust adminstrator management code that is difficult to guess. It is also necessary to regularly monitor which devices are connected to the network.
- Make sure you **always browse in safe mode.** Always check that the web site where you are browsing is recognized by the HTTPS security protocol, above all for online purchases, banking transactions, or when sensitive information and personal data are being transmitted. Those pages are also identified by a green lock icon on the browser bar, which means that the information being sent is encrypted during transmission.
- Install apps to block advertising, crawlers, and malware in the browser.

Other basic protection measures

- **Periodically back** up all important data and personal information, encrypt them, and store them on an external hard disk or in the cloud. A security copy made in good time and on a regular basis can avoid the loss of material and sensitive data in the event of hacking of devices and ransomware attacks.
- Use the latest version of **antivirus software.** Although antivirus software cannot detect all *malware*, it will add an additional layer of protection to devices.
- Always keep the operating system, browser, and apps up to date in your electronic devices. That not only makes them faster; it also provides greater security and may protect against threats and repair some of the vulnerabilities of previous versions.
- Protect personal information. Do not share it on insecure websites or publish it on social networks.
- Review and familiarize yourself with **social network privacy and security options** and take time to see what personal information is exposed on networks.
- Distrust messages about COVID-19 and links or suspicious attachments or overly attractive promotions.
- **Carefully check COVID-19-related apps** installed on electronic devices, since many of them imitate reliable sources, such as the WHO.
- **Only download apps or any other software from secure platforms** (Google Play Store or App Store), and distrust apps that ask for unnecessary permissions in the device. Also check the qualifications of other users. Reviews apps that are no longer in use and delete them because they may serve as points of entry for malware.

B. Digital security measures for dealing with specific risks

a. Protection against corona-phishing and corona-smishing

One of the most common ways currently used by attackers to install malware in computers or telephones is "phishing" or fake data fishing. This form of cyberattack consists of sending fraudulent e-mails, SMS messages or instant messaging on social networks (Whatsapp) that appear to be innocent because they falsely adopt the identity of a recognized person, company, or entity but in reality hide malicious programs or redirect to fake websites in order to gather personal information, names of users, personal codes, passwords, or bank data. Through phishing attacks, cyber-criminals can also take control of devices and of all the information they store.

During the pandemic, many of these phishing attempts have pretended to be government entitities or health care or philanthropic organizations providing information about COVID-19, updates on latest COVID-19 developments, alleged cures, vaccinations, and medical supplies, government offers of support, tax benefits, fake job offers, or offers of cost-free services. Another popular form of attack has been smishing, in which an SMS is sent from what purports to be a government body sharing a link asking for personal data.

Recommendations for protecting yourself:

- ☑ The best strategy is to **be fully aware of the frequency of phishing attempts**. As a general rule, do not trust an e-mail or strange message from an unknown user asking for private information, urging you to act rapidly or urgently, or threatening you.
- ☑ **Treat all e-mails about COVID-19 as suspect,** especially if the e-mail addres is unknown.

- **Suspect all WhatsApp chains as well.** WhatsApp is used to circulate thousands of messages with links to a wide range of websites, where alleged experts offer recommendations and solutions for dealing with the virus. Many of those messages contain malicious links or attempt to spread disinformation.

- Be suspicious if the e-mail contains **grammatical or semantic errors, is poorly designed, or of dubious quality,** and if it is not personalized (for instance, it refers to "dear colleague," "dear friend," or "esteemed customer").

- Carefully check who the e-mail is from or the web address.

- **Do not click on links** received through a message about COVID-19 (text message, WhatsApp, or mail), even though they appear to be from an official source, such as the Ministry of Health or the WHO. Many such links redirect you to fake websites seeking to deceive you into identifying yourself or providing confidential data that the scammers then use to access devices and steal money.

- **Protect personal information.** No official source elicits data via e-mail.

- **Do not open attachments in** strange e-mails, or access or download untrustworthy links or files (above all if they end in .exe). If you are in doubt and the attachment appears to be important, you can open it in Google Drive to ensure greater protectioon.

- Scan suspicious links using tools such as VirusTotal (although this tool does not recognize all forms of malware, it does reveal some common malicious programs).

- **Never answer** these mails. In doubt, directly consult the company or service it purports to represent because it is possible that they forged or hacked its e-mail address.

- **Have a firewall installed** (the most recent versions of Windows and Mac OS come with a pre-installed firewall, and tools such as Comodo Firewall, ZoneAlarm and Glasswire can also be used).

- Block advertisements embedded in sites or emerging advertiements since they can result in the downloading of malicious files (complements, such as uBlock Origin may be used to avoid having to click on those emerging advertisements.

- With job offers, check the company's website and how the offer is phrased, and do not disclose private information, review data protection policy,and use reliable job-search portals.

b. Safe teleworking

For many women, this period of confinement has entailed engaging in telework and combining their paid productive work at home with their unpaid domestic chores and care-giving work. In this new-normal digital era, it is necessary to take special precautions because home networks may not be correctly configured and/or supervised, which could let cyber-delinquents in or trigger an accidental breach of information. In addition, women's dual workload may cause tiredness and distraction rendering them more vulnerable than men working remotely but without the same level of domestic responsibilities.

- **Always connect using a secure (non-public) Wifi network** and make sure that the domestic wireless network is safely configuted (change the password when the router malfunctions and regularly update it), as this will afford greater protection agsinst unauthorized access to the organization's information by cyber-criminals. Whereever possible, connect to the corporate environment by using a virtual private network (VPN), which creates a private and encrypted connection.
- Keep work-related information in the computer used for work and avoid using your personal computer or devices for work. **Keep work and personal accounts separate,** including e-mail and social network accounts.
- **Work devices should be fully encrypted.**
- If no corporate devices are available for you to work from, install a pro-active threat detection system in your personal device, which is achieved by installing a comprehensive security solution and keeping it up to date.
- Use special care when installing programs, because unloading malicious software may jeopardize the security of the entire organization.
- Make periodical back-ups of information.
- Always check that you are using the company's legitimate website before inputting access data or confidential information. In addition, use robust passwords and two-factor authentication to access critical accounts.

- Make only safe use of collaborate tools in the cloud.
- Always take security precautions when videoconferencing.
- If you need to send confidential or sensitive information, it is advisable to use a service that encrypts the information and not use instant messaging.
- Watch out for phishing attempts, external e-mails, and unusual requests for access credentials (including unexpected telephone calls from the technology support team of the company requesting access credentials).
- Always keep your own technological support contacts ready and at hand, to denounce any security breach as soon as posible.

c. Holding safe online meetings

During the pandemic, video call apps have become essential tools for continuing to carry out day-to-day activities. Numerous attackers have seized on the popularity of videoconferencing tools ((Zoom, Webex, Hangout, Skype) to distribute malware or to access and boycott meetings (zoombombing), making it necessary to adopt extreme security precautions to prevent infiltration and guarantee the confidentiality of conversations and of the information shared.

Some basic precautions include:

- **Take steps to ensure the privacy of the meeting.** Require passwords to access it (many apps include them by default).
- Take time to review the privacy policy of the video call tool (How does it handle confidential information?).
- **Use precaution when convening the meeting, adding only known contacts.** Invitations need to be personal. Avoid using insecure communication channels to convene the meeting and require pre-registration.

- Activate the waiting-room, where the identity of each participant can be checked before they are admitted to the meeting. It is important to verify that a user wishing to join the meeting has a previously identified name and surname.
- If a videoconference is to be conducted for the first time with a new contact, **verify his or her identity** using other means.
- Once all participants have joined the video call, block access to others, to ensure that intruders cannot enter and spy on conversations.
- Download the app from the official website or official repositories (Google Play or Apple Store).
- **Activate automatic software updates** and accept whenever asked to do so, as this helps ensure that you have the most recent and safest version.
- **Apply the pre-determined encryption** and ensure that it covers the entire meeting.
- **Be careful when sharing files and screens,** as they may accidentally disclose confidential information or be used to disseminate malicious programs.
- **Disable desktop and file sharing and receipt of videos** by default.
- **Cover the camera** when the system is not in use and turn off or silence microphones.

d. Banking via the Internet and online shopping

- Use a safe password for online bank accounts and two-factor authentication.
- Install security software in all devices used for online purchases or banking transactions, and keep it up to date.
- **Do not use public computers or public Wifi networks** for banking transactions, as this increases the chances of strangers accessing bank information.

- It is best to use just one credit card for online transactions, as a way to minimize exposure of bank information.
- Review your bank account frequently to detect any suspicious activity.
- **Be wary of attempted scams via phishing mails** asking you to provide bank account details or re-directing you to sites to input those data. If you are in doubt about the veracity of the e-mail, contact the bank directly to corroborate the legitimacy of the e-mail.
- A cure for COVID-19? Don't be deceived by false offers and stay alert. If an offer is too good to be true, it's probably fake.
- Create an **e-mail to be used exclusively for online purchases.**
- Make sure providers are trustworthy before purchasing on line. Always buy from established, recognized, and reliable sellers. Check to see how long they have been in business, their on-line ratings, and sales history.
- Purchase on line from providers using secure website for transactions and payments. A secure webpage will have 'https://' in the site address and sometimes a closed lock icon in the browser address bar.
- Do not trust a web page without a legal notice containing information about, inter alia, the company, terms of sale, returns, and claims.
- Check all the details about the goods or services you are purchasing (product description, shipping charges, currency, and exchange rate, terms and conditions, guarantee, return policy).
- Report any cases of fraud.

e. Safeguards against infodemia and fake news/misinformation

The COVID-19 pandemic has been accompanied by an infodemic, causing anxiety and confusion as a result of a plethora of information circulating in tweets, Facebook messages, Whatsapp chains, videos, and news.This saturation of information makes it hard to distinguish between reliable and

useful information and that seeking to sow confusion and harder for people to take the right steps and decisions in today's critical circumstances.

The information circulating every day via the Web includes an abundance of fake news, disinformation and manipulative campaigns, conspiracy theories, rumors, myths, and pseudo-science about the effects of COVID-19, and information touting supposed cures, treatments, and vaccinations, all of which creates the perfect environment for fraud and scams. Falling victim to this infodemic or information overload can wreak havoc with a person's finances, raise anxiety levels, and even cause serious harm to the health not just of the person consulting that information but of his or her entire family.

- **Choose one or two reliable sources of information** to listen to news and avoid checking out fake or unscientific reports.
- Develop **critical capacity** to spot fake news and distruct sensationalist articles about positive outcomes of small-scale experimental treatments.
- Trust only official or verified sites, not just because of the quality of the information, but also because of the proliferation of malicious sites exploiting the current situation.
- Verify information: conduct a search of the author or organization, check whether the information comes from a reputable source, check the URL (does it begin with HTTPS?) or use fact-checking sites (Fullfact, Snopes).
- Check for spelling mistakes, errors in images, or problems with dates.
- **Help fight disinformation.** Do not share unverified information or information from dubious sources.
- **Children and young people may find it harder to distingusih** between reality and fake news, so it is important to talk to them about this matter, to help them develop critical thinking and to spot false information or dangerous myths.

f. Sextorsion

Sextortion takes the form of blackmail based on the possession (or alleged possession) by an aggressor of intimate images, which he threatens to distribute unless he receives money, more pictures, or a relationship. The aggressor may be an intimate partner, someone met on the Web, or an unknown attacker.

A frequent scam during the pandemic consists of a stranger sending a message or e-mail claiming to have hacked the device or account and threatening to publish private images unless he receives a certain sum of money. Most such e-mails seek to frighten the victim by stating that her device has been infected with malware that has monitored activity on the computer and recorded sexual practices and mentioning some password used by the victim in one of her accounts. When this happens, the following recommendations apply:

- Never open an unsolicited e-mail or e-mail from an unknown person.
- Distrust any mail that appears to come from one's own account. To render fraud more credible, cyber-criminals often forge the address of the sender using a technique known as *email spoofing.*
- Do not reply to these mails, or give in to threats, or pay the ransom. It is most likely that this is an attempted scam and the attacker does not possess intimate images and has not in fact infected the computer, even if he mentions a personal password.
- Even if the attacker does have intimate images, it is best not to reply and to immediately cease all contact, not to pay, and to report the incident as soon as possible. Making a payment will encourage requests for further payments and, in many cases, the material is published anyway, even if a payment was made.
- Take screenshots of the threats and accounts involved and keep them as evidence in case you want to report the incident to the police.
- Report the incident on social networks and block the account to prevent contact.
- Check the security configurations for all accounts and social networks.
- Talk to persons close to you and those who might be affected. Extortionists thrive on a victim's silence.
- File a complaint with the authorities.

g. Cyber-security within the family

The main types of violence experienced by children and adolescents are exposure without their consent to content of a sexual and/or violent nature, cyber-harassment, and grooming. According to a study by Save the Children, 52% of minors faced no restrictions by their parents on their access to the Internet, and among those who were subject to restrictions, these only had to do with the amount of time spent on it.

- ☑ It is impossible to be with children all the time they are online, so that it is important to talk openly with them about it and to help them develop critical thinking about the risks they may face online and the security tools available to protect them.
- ☑ Explain to minors the importance of privacy and cyber-security, including protection of their digital identity.
- ☑ Pay attention to their online experiences and get to know their surfing habits. Supervise children's access to the Internet to prevent them publishing personal and private information (address, telephone, name of the school), as well as the kind of entertainment channels they visit frequently.
- ☑ Establish some limits regarding when and where they can use electronic devices (common or shared areas are recommended)
- ☑ Install a parental oversight program to oversee children's online activity. Such programs come with almost all electronic devices, televisions, and videogame consoles. Family security controls and children's Internet search devices can also be downloaded to avoid them entering inappropriate sites.
- ☑ Check the privacy controls for videogames, apps, and smart toys, because they can disclose children's and adolescents' personal data and location.
- ☑ Remember that online games are another form of social network that needs to be taken into account when reviewing what information is shared (they also allow calls and contact with third parties).
- ☑ Stay on top of the sites, apps, social networks, video games, and chat services used by children and adolescents, and explore them together, including ways to protect information and how to report inappropriate content or conduct on those platforms.

- Sometimes mobile devices are shared in families, often containing sensitive information, such as passwords, credit card numbers, or workplace information. It is important to ensure that those accounts cannot be accessed and to use systems to protect those devices.

To prevent *grooming*:

- Make sure that social network accounts and video-game chat functions are private. Check security configurations and establish rules regarding the type of content to be shared on line. Encourage children and adolescents to delete contacts they do not know in person.
- Report and block any suspicious person.
- Let children and adolescetns know that they can always say when they receive an inappropriate contact or one that makes them feel uncomfortable.
- Urge them to drop friendships or requests from followers of persons they do not know (check whether the person making the request has friends in common).
- Be aware of the persons they socialize with online and offline.
- Watch out for any signs of anxiety.

Glossary

Gender analysis. Systematic way to observe the differential impact of developments, policies, programs, and laws on men and women. *4, 9, 10, 13*

Gender gap: Refers to any disparity between the status or position of women and men in society (differences in access to resources, rights, and opportunities). *11, 12, 13, 14, 15, 18, 24*

Encryption of information. A process for converting digital data into codes, making the information illegible except for the person possessing the key needed to decipher it. *33*

Parental control. Set of tools for blocking, restricting, or filtering access by minors to certain content or programs, in order to avoid their exposure to risks on the Internet. *37*

Firewall. Physical or digital system designed to allow or prohibit access from or to a network, in order to ensure that all communications between the network and the Internet follow the security policies established by an organization or corporation. *30*

Dark Web. A part of the Internet that is deliberately hidden from search engines containing pages that are not indexed and have hidden IP addresses accessible only to special web surfers. These pages are devoted to all kinds of criminal activities and contain illegal content. *7*

Denial of service. Cyber-attack designed to saturate a server with so many service requests that legitimate users are unable to use it. A more sophisticated method is Distributed Denial of Service (DDoS) attacks, in which several teams coordinate to send petitions. *22*

Gender-based discrimination. Any distinction, exclusion, or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field [Source: Article 1 of the Convention on the Elimination of All Form of Discrimination against Women]. *13, 15, 24*

Gender stereotypes. An opinion or widespread prejudice regarding attributes that men and women possess or should possess or the social functions they perform or should perform. [Source: OHCHR, *Gender stereotyping*]. *6, 17, 18, 22, 24*

Gender. Refers to roles, behavior, activities, and attributes that a given society in a given period considers appropriate for men and women. Gender also refers to relations among women and relations among men. Those attributes, opportunities, and relations are social constructs, acquired through socialization. [Source: UN Women, *OSAGI Gender Mainstreaming - Concepts and definitions*]. *4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24*

Grooming or child abuse by a pedophile. Deliberate acts by an adult to approach a minor (sometimes by cultivating a sentimental connection) with a view to establishing a relationship and emotional dominance enabling the adult to commit sexual abuse, engage in virtual contact, elicit child pornography, or sell the minor to others (child trafficking). *15, 19, 22, 23, 37, 38*

HTTPS. The English initials for Hypertext Transfer Protocol Secure: a network protocol for the safe transfer of encrypted data. *27, 34, 35*

Gender equality. Refers to equal rights, responsibilities, and opportunities for women and men, and girls and boys. [Source: UN Women, *OSAGI Gender Mainstreaming - Concepts and definitions*]. *21, 22*

Gender mainstreaming. A strategy for achieving inclusion of women's concerns and experiences, along with those of men, in the preparation, implementation, monitoring, and evaluation of policies and programs in all political, economic, and social spheres, in such a way that women and men can both benefit from them on an equal footing and avoid perpetuating inequality. [Source: UNICEF, UNFPA, UNDP, UN Women. *Gender Equality, UN Coherence and you*]. *8*

Social engineering. Techniques for deceiving potential victims into almost freely sharing their personal information (such as passwords, bank account details, or sensitive data). These methods typically exploit victims' good will and lack of precaution. *7*

Livestream. A live video platform that enables users to watch and disseminate video content via the Internet using a camera and computer. *6*

Malware. The term is an abbreviation for *malicious software*, meaning software intended to infiltrate and/or harm an information system without the user's consent. *7, 19, 28, 29, 30, 32, 36*

Phishing. A scam committed using a deceptive and apparently official communication (e-mail, text message, or telephone call) in which the scammer or phisher pretends to be a familiar person or company so that the receiver provides confidential information (passwords, banking data, etc.). It is called *smishing* when the scam is committed using SMS and *vishing* when it is performed by recreating an automated voice. *7, 19, 20, 22, 29, 32, 34*

Gender perspective. An analytical mechanism that consists of observing the impact of gender on people's opportunities, roles, and social interactions [Source: UN Women, *OSAGI Gender Mainstreaming - Concepts and definitions*]. *4, 8, 9, 10, 17, 24*

Gender roles. Social norms and rules of behavior that, in a given culture, are widely accepted as socially appropriate for persons of a given sex. They tend to determine the responsibilities and tasks traditionally assigned to men, women, boys, and girls. [Source: UNICEF, UNFPA, UNDP, UN Women. *Gender Equality, UN Coherence and you*]. *4, 16, 18*

Ransomware. A malicious software program used to take control of the infected device and "kidnap" the user's information (encrypting it) with a view to extorting the user by asking for a pecuniary "ransom". *21, 28*

Virtual Private Network. Also known as VPN, this is a computer network technology for establishing a safe extension from a local area network (LAN) to a public or non-controlled network, thereby allowing the computer in the network to send and receive data via public networks as if it were a private network (and ensuring that the connection is safe by encrypting the data). *31*

Sex (biological). Refers to the biological characteristics that define human beings as female (women) and male (men). *18, 23*

Sextorsion. Consists of threatening to disseminate intimate image or videos of a person with a view to eliciting more material regarding explicit sexual acts, having sex with that person, or obtaining money. *7, 15, 22, 35, 36*

Spoofing. A series of techniques for pretending to be persons or entities in the network, based on investigation or the use of *malware*, with a view to eliciting private information or managing to enter pages using false credentials. Depending on the source of the attack, *spoofing* may be classified as IP *spoofing* (theft of an IP address), mail *spoofing* (e-mail theft), web *spoofing* (using a false web page), DNS *spoofing* (theft of a domain name source), ARP *spoofing* (theft of an Address Resolution Protocol -ARP- table, which is a network protocol linking a Media Access Control -MAC- address to the computer's IP address). *36*

Unpaid caregiver work. All daily activities to safeguard human life and health, such as household chores (cooking, cleaning, the washing of clothes) and personal care. Usually these household activities are performed by women free of charge. [Sources: Orozco, Amaia. *Cadenas globales de cuidados. ¿Qué derechos para un régimen global de cuidados justo?*]. *12, 14, 16, 19, 21, 31*

URL. *Uniform Resource Locator* is the specific address allocated to each of the resources available on the network (pages, sites, documents) so that they can be located or identified. *35*

Violence against women. Any act or conduct, based on gender, which causes death or physical, sexual or psychological harm or suffering to women, whether in the public or the private sphere [Article 1 of the Inter-American Convention to Prevent, Punish, and Eradicate Violence against Women]. *9, 14, 15, 17, 18, 21, 22, 24*

Virus. A self-propagated IT program designed to alter the normal functioning of an electronic device. Viruses differ from other forms of malware in that they are automatically replicated, that is to say, are capable of copying themselves from one file or computer to another without the user's consent. *5, 11, 30*

Wi-Fi. A network of interconnected wireless devices that are generally also connected to the Internet through a wireless point of access. *27, 31, 33*

Zoombombing. Breaking, without consent, into a videoconference with obscene, pornographic, sexist, racist, homophobic, and other content, which usually puts an end to the videoconference. The term was initially coined to refer to incidents occurring during the COVID-19 pandemic on the Zoom platform, but is now used also for intrusions into other videoconferencing platforms. *32*

Bibliography

- Agudelo, Mauricio, Eduardo Chomali, Jesús Suniaga, et al (2020). Las oportunidades de la digitalización en América Latina frente al COVID-19. CEPAL, ELAC, Corporación Andina de fomento, DPL Consulting and Telecom Advisory Services.
- Agüero, Aileen, Monoserrat Bustelo y Mariana Viollaz (2020). ¿Desigualdades en el Mundo Digital? Brechas de género en el Uso de las TIC. Technical Note No. IDB-TN-01879. Inter-American Development Bank.
- Association for Progressive Communications (APC) (2020). COVID-19 and the increase of domestic violence against women: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on Violence against Women, its causes and Consequences.
- Brown, Deborah y Allison Pytlak (2020). Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom y Association for Progressive Communications (APC).
- Brudvig, Ingrid, Chenai Chair y Adriane van den Wilk (2020). COVID-19 and increasing domestic violence against women: The pandemic of online gender based violence. World Wide Web Foundation.
- Chair, Chenai, Ingrid Brudivg, Calum Cameron et al (2020a). Women's rights online. Closing the digital gender gap for a more equal world. World Wide Web Foundation.
- (2020b). Derechos de la mujer en línea. Cerrar la brecha digital de género para lograr un mundo más igualitario. Resumen ejecutivo.
- Economic Commission for Latin America and the Caribbean of the United Nations (CEPAL/ECLAC) (2020). Informe Especial COVID-19 No. 7. Universalizar el acceso a las tecnologías digitales para enfrentar los efectos del COVID-19.
- Inter-American Commission of Women (2020a). La violencia contra las mujeres frente a las medidas dirigidas a disminuir el contagio del COVID-19.
- (2020b). COVID-19 en la vida de las mujeres. Razones para reconocer los impactos diferenciados.
- (2020c). COVID-19 en la vida de las mujeres: Emergencia global de los cuidados.
- (2021). COVID-19 en la vida de las mujeres: Los cuidados como inversión
- United Nations Special Rapporteur on Violence against Women, its Causes and Consequences (REVM-ONU) (2018). Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. Human Rights Council of the United Nations. Accessed on September 9, 2020.
- Derechos Digitales América Latina (2020). COVID-19 and the increase of domestic violence against women in Latin America: A digital rights perspective.
- European Union Agency for Law Enforcement Cooperation (EUROPOL) (2020a). Internet Organised Crime Threat Assessment.
- (2020b). Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic.
- (2020c). Catching the virus. Cybercrime, disinformation and the COVID-19 pandemic.
- European Women's Lobby (2020). Policy Brief Women must not pay the price for COVID-19. Putting equality between women and men at the heart of the response to COVID-10 across Europe.
- Glitch UK y End Violence against Women Coalition (2020). The Ripple Effect: COVID-19 and the Epidemic of Online Abuse.

- European Institute of Gender Equality (EIGE) (2017). La ciberviolencia contra mujeres y niñas
- Millar, Katherine, James Shires y Tatiana Tropina (2021). Gender Approaches to Cybersecurity. United Nations Institute for Disarmament Research (UNIDIR)
- United Nations Office on Drugs and Crime (UNODC) (2020). Cybercrime and COVID-19: Risks and Responses.
- UN Women (2020a). Online and ICT facilitated violence against women and girls during COVID-19.
- (2020b). From Insights to Action. Gender Equality in the Wake of COVID-19.
- (2020c). COVID-19 and Ending Violence against Women and Girls.
- (2020d). COVID-19 en América Latina y el Caribe: Cómo incorporar a las mujeres y la igualdad de género en la gestión de la respuesta de la crisis.
- (2020e). Spotlight on Gender, COVID-19 and the SDGS. Will the Pandemic Derail Hard-Won Progress on Gender Equality?"
- (2020f). COVID-19 y la Economía de los Cuidados: Acciones inmediatas y transformación estructural para una recuperación con perspectiva de género. Documento de Políticas No. 16.
- World Health Organization (WHO) (2020). El género y la COVID-19.
- Sainz, Milagros, Lidia Arroyo y Cecilia Castaño (2020). Mujeres y digitalización. De las brechas a los algoritmos. Instituto de la Mujer para la Igualdad de Oportunidades. Ministerio de Igualdad del Gobierno de España.
- Slupska, Julia (2019). "Safe at Home: Towards a Feminist Critic of Cybersecurity". St Antony's International Review, 15, no. 1: 83-100.
- The Interantional Criminal Police Organization (INTERPOL) (2020). Cybercrime COVID-19 Impact.
- International Telecommunication Union (ITU) (2020a). Measuring digital development. Facts and Figures 2020.
- (2020b). "Las mujeres, las TIC y las telecomunicaciones de emergencia: Oportunidades y limitaciones".
- World Wide Web Foundation (2015). Women's Rights Online. Translating Access into Empowerment.

OAS Cataloging-in-Publication Data

La ciberseguridad de las mujeres durante la pandemia del COVID-19 : experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital / [Preparado por la Secretaría General de la Organización de los Estados Americanos].
v. ; cm. (OAS. Documentos oficiales ; OEA/Ser.D/XXV.16)
ISBN 978-0-8270-7184-1
1. Women's rights. 2. COVID-19 (Disease). 3. Computer security. I. Title. II. Inter-American Commission of Women. III. Inter-American Committee against Terrorism. IV. OAS/CICTE Cyber Security Program. V. Organization of American States. Secretariat for Multidimensional Security. VI. Serie Libro Blanco. VII. Series.
OEA/Ser.D/XXV.16

Secretariat for Multidimensional Security (SMS)

White paper

Cyber-security for women during the COVID-19 pandemic:

Experiences, risks, and self-care strategies in the new normal digital era

OAS More rights for more people