GENDERING THE CYBER WORLD:

Women and Girls Safety online

FE-MALE
LOUD- PROUD- FEMINISTS

INTRODUCTION

"He is the Subject, he is the Absolute; she is the Other" writes Simone De Beauvoir in 1949. Today, in the invisibility of cyberspace, women are still considered to be an e-Other, on a variety of platforms! Little has changed, even though women have fought for and achieved many landmark decisions, among them a resolution adopted by the United Nations Human Rights Council (HRC) titled: "The Promotion, Protection and Enjoyment of Human Rights on the Internet", which states that "the same human rights that people have offline must be protected online" including human rights issues related to gender. Women and girls face numerous challenges including ongoing discrimination, violence, online threats, data bias, limited internet access, data security and privacy.

For these reasons, this set of six practical fact sheets is being provided to the readers as learning tools for hands-on application. They brief the content of a guide titled "Gendering the Cyber World: Women and Girls Safety Online", which will be launched soon on our website. We here at Fe-Male collaborated with Rouba El Helou, research associate at the Gender, Communications and Global Mobility (GCGM) Studies unit to develop this content within a gendered framework of the digital sphere.

The purpose of these unique targeted fact sheets is to both raise awareness and allow female users to make a change in their use of the digital realm. The fact sheets focus on specific topics and are related to action steps which were written with an intersectional approach.

1. Facts about Internet, Cyber-Security and Women: provides information about and definitions of the internet, the World Wide Web and internet governance from a feminist perspective.

2. Get to Know More about Online Gender Based Violence: provides rapid access to knowledge related to online violence and threats against women and girls.

3. Cyber Safety for Women and Girls: provides useful steps for online protection on how to secure your personal information, privacy and devices.

4. Dating and Falling in Love Online: provides safety measures for women to protect their right to romance by simple precautionary steps and awareness tips for the online dating world.

5. Girls Safety Online: Tips for Parents: provides information and safety tips and tools for both parents in particular, and for girls surfing the internet.

6. What Is the Impact of Technology on Online Gender-based Violence? Useful Terminologies: provides brief explanations concerning cybersecurity and safety for women and girls terminology, which is commonly used online.

FACTS ABOUT INTERNET, CYBER-SECURITY AND WOMEN

The 'global system of communication network' we call internet today, is the result of collaborative work of scientists, researchers, programmers and engineers. Its foundation was in university research projects, funded by the US defense ministry more than 50 years ago. The prototype model called Advanced Research Projects Agency Network (ARPAnet) was launched in 1969 and is considered to be the first step towards the Internet. In short, the Internet is in essence a huge network of computers.

WORLD WIDE WEB –WWW: in 1989 Tim Berners Lee, a British scientist at the European Organization for Nuclear Research (CERN) developed an information system based on a hypertext markup language known as HTML. A communication model which allows exchange of information, contentions and webpages, it was available for public use via the internet since 1991. In short, WWW is a collection of webpages found on the network of computers we call Internet.

INTERNET GOVERNANCE IG is the development of policies, standards and regulations to organize and develop the world of cyberspace. It is a multi-faceted concept and includes the public and the private sector, along with civil society and the technical community. Human rights, gender and youth are integral parts of IG.

FACTS AND STATISTICS

• Ada Lovelace, a British mathematician from the 19th century. She is nicknamed the "first computer programmer" because she was a pioneer in drafting coding technology.

• Elizabeth Feinler AKA Jake! Was one of the pioneers of the ARPAnet. She led the team that organized the information system. Among her achievements is the development of top level domains known as schemes: .com; .edu; .org; .net; .gov; .mil.

• Radia Perlman is called the "mother of the internet" for her tremendous contribution in the development of the network and holds more than 80 patents in her field.

• According to the International Telecommunication Union (ITU), the worldwide Internet user penetration rates are higher for men than for women in all regions of the world.

• According to Intel, 25 percent fewer women than men have access to the internet.

• The internet can generate tangible benefits for women in developing countries, such as jobs and education opportunities.

• Social norms can block women from accessing and using information communication technology (ICT).

• Female online gamers are equal in number to male gamers, but they face more sexism and sexual harassment.

• Studies show that doubling the number of women and girls online would create an estimated additional USD13 to USD 18 billion in GDP across developing countries.

• According to UNESCO, 34-57% of STEM graduates in Arab countries are women, which is much higher than in universities in the US or Europe.

• The Middle East and North Africa (MENA) region will witness a higher need for female professionals in the field of cybersecurity by 2022.

• The cybersecurity field has a massive labor shortage.

• Women represent only 20 percent of the global cybersecurity labor force.

• Most of the cybercrime braches are caused by human error.

• The most severe cybercrime concerns in the MENA includes data exposure, cyber terrorism, hacking and ransomware, with a lack of proper understanding of what InfoSec is.

GET TO KNOW MORE ABOUT ONLINE GENDER BASED VIOLENCE

Gender based violence (GBV) often goes unseen; women victims and survivors are quite often denied simple human rights, protection, support and justice. GBV is rooted in inequality, culture and a lack of rule of law in many countries. Moving online, the same gender discrimination and culture of inequality persist. Even though these are shifting grounds, many still believe that since it is an invisible world, online GBV doesn't exist, and since it is behind a screen nothing can harm us. However words and actions online also matter. Recently, COVID19 crisis and quarantine worsened the situation for women and girls from all walks of life, including journalists, human rights activists or politicians.

DEFINITIONS:

Attacks against women and girls online perpetrated by men can be acts of violence. These attacks happen due to a person's gender sensitivity and patriarchal gender norms background. They can include cyberstalking, bullying, name calling, sex-based harassment, threatening, defamation, distribution of photos and videos without consent, gendertrolling, hate speech, sextortion, doxing, image-based abuse, and exploitation. These actions are carried out with technological assistance via the internet and leave a deep negative impact on the physical and psychological health of the individual. Other terminologies employed in this context including: "ICT-facilitated violence against women", "technology facilitated violence" and sometimes "cyberviolence against women and girls".

ASSESSING THE SITUATION, TIPS AND STATISTICS

- It is always important to remember that technology-related violence against women is simply an extension of violence against women offline.
- Gender based violence and abuse occur everywhere online: in Facebook, Twitter, Instagram, LinkedIn and many others; in messaging services (e.g. Whatsapp, Facebook Messenger, Snapchat, WeChat or Skype), in dating websites and apps, in comment sections of newspapers, news sites, and in the chat rooms of online video games.
- According to Amnesty International violence and abuse flourish on the social media platforms against women with little accountability.
- There is a gender divide between men and women in many underdeveloped countries in terms of internet accessibility, control of content and technological development. This includes low technical literacy and lack of confidence when owning and using a mobile phone by women and girls. They are thus at higher risks to be attacked online.
- Security and harassment are key concerns for women and considered as one of the top five barriers to mobile phone ownership and usage.
- Between the age of 18 to 24, women are likely to experience stalking and sexual harassment in addition to physical threats online.
- Women journalists, human rights activists, public servants and politicians face increasing amounts of online gender based violence attacks, simply because they are women.
- One in five female Internet users live in countries where online harassment and abuse of women is unlikely to be punished.
- In 2016 The Guardian newspaper of London documented and analyzed 70 million comments posted on its website. The survey results showed that eight of its 10 journalists who were the most targeted by hate notes were women.
- According to Bio Research Center, women and girls are more likely to experience online harassment compared to men, where the possibility of young girls using dating applications is double that of young men.
- According to the Lebanese Internal Security Forces, more than a hundred cases of different forms of cyber-violence are being monthly reported by women and girls. Knowing that, the percentage of cyber-crimes committed against girls, age 12 to 26, was 41%, while those 26 and above reached 27%.

CYBER SAFETY FOR WOMEN AND GIRLS

Like in the real world, women are more often exposed to cybercrime than men.
Cyber-violence and exploitation in Lebanon is becoming increasingly more serious; more than 100 cases of online violence have been reported to the authorities monthly by women and girls. Harassment, bullying, sexual abuse, and stalking are all issues that are as real online as they are offline.

How to stay safe online?
Prevention is always the best medicine! Social behavior is key!

DEFINITION

What is cyber safety?
It is an online process, culture and system designed to prevent all types of online threats. These dangers might be caused by humans, by technological challenges or by malware or viruses when logging in to unsafe websites, logging in to a publicly accessible internet connection (Wi-Fi), suspicious links, phishing links, unsecured apps or documents.
Different people call it different things, such as: digital safety, e-safety, online safety or internet safety. They all mean the same thing. That is a series of safe practices which we follow while surfing the internet to protect us from various online attacks and/or criminal activities.

CYBER SAFETY TEACHES US:

How to use information and communication technologies (ICT) responsibly;
How to be secure and protect ourselves online;
How to protect our emotional well-being;
How to back up and secure our information or data such as research and personal details.

MEASURES AND TIPS TO STAY SAFE

1- Cherish your privacy, do not share personal or sensitive information on social media.
2- Protect your password and make it random, using different signs; a different password for each social media platform or online accounts. Change it every two to three months, avoiding children's, spouse, or pet names and significant dates in your password; do not share it with anyone and do not use it on other people's devices.
3- Update all operating systems on your computers, laptops, tablets and smartphone regularly.
4- Beware of phishing links which can be sent via emails, SMS, inboxes and VoIP apps (voice & video communications). In the time of Corona, numerous scams and malicious links re being sent. Always check the spelling of the link and ask the senders about it if you know them.
5- Avoid any contact with people you don't know on social media.
6- Read the terms of use and the privacy policy of the websites and applications you use.
7- Activate the Two-Factor Authentication.
8- Use encrypted apps such as signal and jitsi for communication.
9- Remember nothing is really for free online.
10- Cover your camera with tape all the time.
11- Do not connect to public, open Wi-Fi without a proper virtual private network (VPN).
12- Do not click on websites if there is no 's' in the hypertext transfer protocol (https) or link. S stands for secure and a lock symbol is added next to it.
13- Avoid infodemics by checking the credibility of the website, the source of the information and always rechecking the validity of its content.
14- Clean your digital finger print and delete unnecessary data from your device.
15- Use a parental guidance application for your smart phones and the ones of your children.

DATING AND FALLING IN LOVE ONLINE

Dating apps are increasingly becoming the meeting place of choice. This was accentuated during the Corona lockdown. Millions of users worldwide go to online dating platforms. Numerous powerful tools can match you with your potential significant other. Some search for and find long-term commitment. Others look for short-term friendships. But the number of tragic outcomes is also on the rise. Remember, these apps and sites can lead to love or match you with an ominous other, the digital harasser. Data algorithms claim to have a more accurate compatibility level when finding you the partner of your dreams than you might have in real life. But they have a dark side, which is similar to violence in the real world. Online dating scams are on the rise! Protect your right to romance by taking simple precautionary steps.

BACKGROUND

Romance scammers are people who create fake accounts. They claim an imaginary identity or have stolen the electronic data of another individual. Romance scam is a fraudulent and criminal act. Before they strike, scammers meticulously research online dating sites and study their users carefully on social media. They can easily troll their potential victims, in particular those who post details about their lives and their dating experiences publically. Scamming is about violence and exploitation, not love or sexuality. Perpetrators are entrepreneurs who often reach out to a variety of targets on multiple networking sites and apps until they are ready to strike. You will seldom be alone. Another way women can be attacked is by “Pick Up Artists”. PUA are men who attempt to persuade women into having sex with them through a mixture of flattery, psychological manipulation, insults, coercion and undermining a woman’s self-confidence. This is referred to as misogynistic digital abuse, cyber-hate or gender trolling.

TIPS, STATISTICS AND FACTS

- Online dating companies are currently working on developing new tools to help combat harassment and threats while using their platforms. These mechanisms provide features for the victims to report abusive behaviors (such as offensive name-calling, physical threats or harassment over a sustained period of time, sexual harassment, purposeful embarrassment, and stalking).
- Reports show that in the US alone people lost around 201 million USD through online romance scams in 2019. Victims quite often experience emotional distress and huge financial losses.
- Scammers might ask you to deposit money or send it as a gift or they might send you money dragging you into a money laundering scheme.
- Be sure to read safety measures provided by the dating app or website: Most women and girls underestimate the importance of online privacy measures for their safety.
- Women represent the majority of those affected by romance scams.
- Do your online research, check the messages being sent to you by conducting reverse image searches of your partner’s pictures. Don’t automatically click on pictures or links sent to you before you verify them and never share your personal credit card information.
- Young female users of online dating sites are twice as likely as men to report that someone on a dating site or app has called them an offensive name (44% vs. 23%) or threatened to physically harm them (19% vs. 9%).
- Social media platforms are the most common venue for online dating harassment. It is also common via text messages or messaging apps like WhatsApp.
- Unfortunately many men stereotype women who open online dating accounts as someone ‘just looking for sex’. Be safe and protect your right to romance from these predators!
- Online romance imposter scams occur all the time and they are rarely reported because of shame. Being taken advantage of is not shameful; not protecting yourself is.

GIRLS SAFETY ONLINE: TIPS FOR PARENTS

The Internet can have a positive and empowering digital impact on our life, it is made easier within one click and knowledge is made more accessible for all. But this dynamic environment can also be harmful for girls. Internet safety or "e-safety" for children can be an unexpected challenge, especially if your girls are native learners with well-developed skills in using their devices and navigating online in ways that we as parents never even imagined possible when we were kids.

PARENTS TEST

- Are you familiar with which online apps your girls are using; have you tested them?
- Do you know if your girls have ever been bullied or harassed online?
- Do they visit porn sites with their electronic devices?
- Do you use a parental guidance application?
- Do you allow them to be on social media platforms if they are under 13; or under 16?
- Do you know who your girls are talking to online?

If you are confused regarding the questions, beware! Your girls might not be protected online. If you are telling yourself "this can never happen to my daughter", "I would have noticed if she were harassed or annoyed". Think again. Children will not share with you such incidents because of fear and shame. Your children often know more about the internet than you but this doesn't mean they are ready or equipped to be there without your guidance. Parents rarely monitor teenagers while using online platforms. Many female users are younger than their declared age and are not protected by parental guidance, making them easy targets for online predators.

WHAT CAN YOU DO?

- As of a certain age, Respect your girls right to access internet and emphasize this right to them while advising about the importance of their cyber safety and security.
- Start by talking to your girls about concerns and risks they might face in their online lives. Remind them, they should not talk to strangers.
- Explain why privacy matters and which pictures and other material are safe to be posted online. Most of the women and girls do not know that online privacy matters for their safety.
- Review together their privacy and security settings. Advise them not respond to bullies and stalkers emails and messages. Teach them to ignore them, block and or delete them from their lists.
- Make them trust you and let them know that they can share any problem they are facing online by praising their willingness to talk. Whatever happens online, remember not to be angry with your girls.
- Explain that good friends will not force them to fulfill unpleasant tasks.
- Educate yourself digitally. You should know as much as your girls! Link your device with a parental guidance application. Such apps aim to protect and not to censor.
- Unplug! Have a day or designated period of time without computers or smartphones. This is not a punishment and you should also do it.

FACTS AND STATISTICS

- The average age for parents to allow children to use the internet is three.
- According to Ofcom and despite setting having a minimum age limit of 16, WhatsApp has grown in popularity among 12-15 year-olds since 2018 it is followed by TikTok, Facebook, Snapchat and Instagram as one of the top used social media platforms.
- YouTube is listed as favorite among children from five to 15-year-olds.
- Girl gamers between the age of five and 15 is on the increase.
- Online porn makes up 13 to 20 per cent of web and mobile searches respectively, while the average age of first exposure to online porn is 11-years-old.

WHAT IS THE IMPACT OF TECHNOLOGY ON ONLINE GENDER-BASED VIOLENCE?

Useful Terminologies

Although technology provides us with numerous resources to counter cyberattacks, information security and cybersecurity can be easily undermined by hackers, with an average of one attack every 39 seconds. Recently, and since the beginning of the corona lockdown, cybercrime has dramatically increased worldwide. In Lebanon, according to the Internal Security Forces (ISF), cybercrime reports increased by 184 percent, primarily sextortion and sexual harassment.

To understand cybersecurity and safety for women and girls we will need to define the key terms and concepts. Find brief explanations for the terminology commonly used online.

Cybersecurity: It is a mechanism to protect servers, computers, electronic devices, programs and networks against any unauthorized access or attacks. Information security (InfoSec) is the strategy of developing tools by which we manage to defend and protect our networks and devices against attacks. Whether it is referred to as cybersecurity, computer security, or information technology security, it is important to know how to identify the threats and risks we are facing in the digital world.

Online Gender-based violence (GBV): Any form of force or exploitation rooted in discrimination. This is one of the most pressing issues for women and girls online. It is a severe violation of basic human rights.

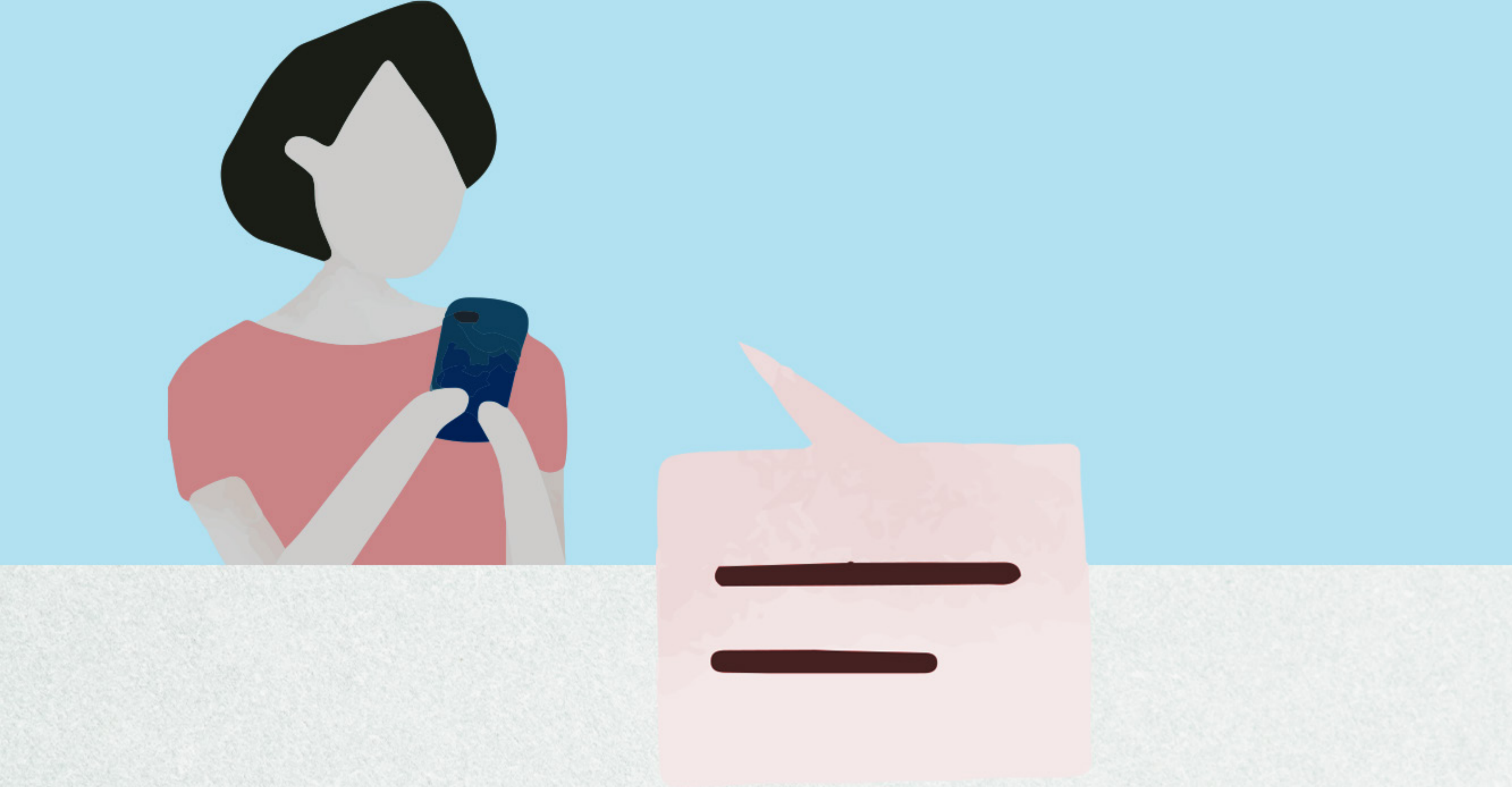
Cyberbullying: It is any form of intentional harassment, insult, assault or threats online via electronic devices in the digital sphere. It is also referred to as online bullying, online harassment and cyber-harassment.

Doxing/Doxxing: It comes from the idea of collecting “documents” or “docs”. It is the act of gathering and retrieving unauthorized information about someone and publishing it. This often occurs by hacking an individual’s personal data.

Gendertrolling: An online disruptive conversation similar to misogyny (hating women because they are women). It includes sexualized and gender based insults and intends to intimidate and upset others. It can occur on an individual level or as a group coordinated campaign against women.

Online Sextortion: A form of blackmail. It is considered to be a serious crime which occurs when someone threatens to distribute your private and sensitive material if you do not provide them with images of a sexual nature, sexual favors or money. It can happen to anyone, but it primarily targets women and girls.

Cyberstalking: It involves using electronic means to follow, secretly surveille, call, text and embarrass oth-



financial information of an individual and using it in order to make transactions or purchases and sometimes to ruin someone else's reputation.

Catfishing: Is a type of online scamming, it refers to the practice of setting up a fake online profile, most often for the purpose of seducing and luring a potential target into a fraudulent romantic relationship.

Cyber Mobs: Is an attack which occurs when a large online group gathers to try to collectively shame, harass, threaten, or discredit a target. Perpetrators usually post offensive and destructive content with the intention of shaming someone.

Phishing: a cyberattack by which a hacker can steal your data via email, messages or social media messengers by clicking on a link that will direct the hacker into your device. The link is slightly misspelled to disguise its identity. Examples: bamkofbeirut.com

Ransomware: a type of malware which intends to block the victims from using their computers or their network by locking the screen for example, unless a ransom is paid.

Malware: a software which causes damage to your server or computers; this can include computer virus-

Biometrics and Identity Theft: online biometrics can include fingerprints and face recognition, and recognition of the irises, voice or palm veins. In short, any metrics related to human features. Securing our digital identity against theft requires avoiding the use or storage of such data. Biometrics authentication of our devices is convenient because it is secured without the hassle of remembering passwords. However this data can be stolen and misused by scammers. Avoid it!

Cyber Extortion: hackers hold private information about you, which is referred to as 'information hostage', or lock your computer, breach into your online data and steal it.

DDoS Attack: happens when the request for data from a website comes from numerous channels in order to overwhelm the server making the system unavailable. In real life this could look like a highway blocked by a traffic jam. Such attacks often occur against blogs and websites run by women's organizations and feminists.

www.fe-male.org

@femalecomms