

The background of the cover is a dark blue color. It features several abstract, stylized lines in yellow, light blue, and white. These lines form various shapes, including a profile of a person's head and neck on the left side, and several interconnected paths that resemble a circuit board or a network diagram. The lines are thick and have rounded ends, creating a modern, digital aesthetic.

# FACILITATORS' MANUAL

**CYBERSECURITY  
THREATS,  
VULNERABILITIES AND  
RESILIENCE AMONG  
WOMEN HUMAN  
RIGHTS DEFENDERS  
AND CIVIL SOCIETY  
IN SOUTH-EAST ASIA**

# ACKNOWLEDGEMENTS

This manual is informed by research undertaken as part of the UN Women Regional Office for Asia and the Pacific project, '[Women, Peace and Cybersecurity: Promoting Women's Peace and Security in the Digital World](#)'. The project has received generous support from the Government of Australia (under its Cyber and Critical Tech Cooperation Program) and from the Government of the Republic of Korea.

Exploring the connections between the Women, Peace and Security Agenda and cybersecurity is a key component of the [UN Women Regional Framework Towards Peaceful, Inclusive Societies: Advancing the Women, Peace and Security Agenda and Inclusive Governance in the Asia-Pacific Region](#).

This manual was written and compiled by Jaimee Stuart, Senior Researcher -Team Lead, United Nations University, with content authored by Mamello Thinyane, Optus Chair of Cybersecurity and Data Science and Associate Professor in the STEM unit at the University of South Australia. The team benefited from valuable technical input and support from Gaëlle Demolis and Alexandra Håkansson Schmidt from the UN Women Regional Office for Asia and the Pacific.

Attributions for reuse are required. Suggested citation for attribution:

Stuart, Jaimee, and Mamello Thinyane. 2024. *Cybersecurity Threats, Vulnerabilities and Resilience among Women Human Rights Defenders and Civil Society in South-East Asia: Facilitators' Manual*. Bangkok, Thailand and Macau (SAR), China: UN Women Regional Office of Asia and the Pacific and United Nations University Macau. <https://doi.org/10.17605/OSF.IO/H38WZ>

© 2024 UN Women. All rights reserved.

Produced by the UN Women Regional Office for Asia and the Pacific

The views expressed in this publication are those of the author(s) and do not necessarily represent the views of the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), the United Nations University Institute in Macau (UNU Macau) or the United Nations or any of its affiliated organizations.

# **FACILITATORS' MANUAL**

## **CYBERSECURITY THREATS, VULNERABILITIES AND RESILIENCE AMONG WOMEN HUMAN RIGHTS DEFENDERS AND CIVIL SOCIETY IN SOUTH-EAST ASIA**



# TABLE OF CONTENTS

---

<b>OVERVIEW OF THE MANUAL</b>	<b>5</b>
Background of the Training	5
How to use this Facilitator’s Guide	6

---

<b>GLOSSARY OF TERMS</b>	<b>13</b>
--------------------------	-----------

---

<b>MODULE 1: CYBERSECURITY AND THE WOMEN, PEACE</b>	<b>16</b>
Session 1.1. Women, Peace, Security and the Digital World	17
Session 1.2. Gender and Cybersecurity	22

---

<b>MODULE 2: FOUNDATIONS FOR CYBERSECURITY MANAGEMENT</b>	<b>30</b>
Session 2.1. The Cybersecurity Ecosystem	31
Session 2.2. Cyber Harms and Risk Management	37

---

<b>MODULE 3: SECURING YOUR DATA</b>	<b>42</b>
Session 3.1. Data Access and Control	43
Session 3.2. Encryption and Data Backup	48

---

<b>MODULE 4. BEING SECURE ONLINE</b>	<b>53</b>
Session 4.1. Online Authentication Threats	54
Session 4.2: Online Browsing and Communication Threats	62

# OVERVIEW OF THE MANUAL



This Facilitators' Manual was developed as part of the suite of resources for the UN Women Regional Office of Asia and the Pacific project '[Women, Peace and Cybersecurity: Promoting Women's Peace and Security in the Digital World](#)'. The project aims to ensure that women, including young women, lead and participate at all levels of information and communication technology policy and decision-making. As such, project resources support women across Southeast Asia to have access to information and capacity-building support to advance gender-responsive cybersecurity as underpinned by Women, Peace and Security (WPS) principles, as per United Nations Security Council Resolution 1325 and subsequent resolutions.

The materials in this manual are based on key findings from the research report 'Cybersecurity Threats, Vulnerabilities and Resilience among Women Human Rights Defenders and Civil Society in Southeast Asia', produced by the United Nations University Institute in Macau and the UN Women Regional Office for Asia and the Pacific. That report should be read in detail as background for delivering the following training. All materials associated with this training can be accessed at <https://doi.org/10.17605/OSF.IO/H38WZ>

## Background of the Training

The digital world provides numerous benefits and opportunities for individuals and organizations. Digital connectivity, particularly for women's civil society organizations (WCSOs) and women human rights defenders (WHRDs), provides critical avenues for connecting with service beneficiaries, calling for action among the broader community and supporting all elements of day-to-day activities and business. Notably, being able to communicate, access and share information quickly and easily is central to the work of activists and civil society organizations (CSOs). These benefits, however, carry significant cyber risks.

Many cyber risks are disproportionately experienced by those working with or advocating for women

and girls. For example, WCSOs and WHRDs often deal with confidential information, including the personal data of vulnerable individuals, which makes them attractive targets for cybercriminals and other adversaries. Many lack the resources and technical expertise to adequately protect themselves from cyberattacks or to prepare staff to protect and empower themselves. These risks are increasing in frequency, sophistication, severity, and impact alongside emerging technologies.

Gender shapes and influences access to and uses of digital technologies, behaviours, online interactions and cybersecurity practices. It is also a critical factor in exposure to cyber risks. Advocates are often targeted with online harassment and stalking that is specifically gendered in nature, including threats of sexual violence or attempts to discredit their work by attacking their gender identity or sexuality. This can impede their activism and limit their ability to effectively engage both on- and offline; some advocates choose to withdraw from their work out of fear for their or others' safety. Of critical importance, WCSOs and WHRDs may be more likely to be targeted by those seeking to silence or discredit feminist movements, challenge gender equality or suppress human rights. While there is increasing awareness of the risks faced by women and girls and those who advocate for them, in cyberspace, there are few evidence-based capacity-building efforts specifically aimed at empowering WCSOs and WHRDs to protect against and mitigate cyber risks.

To meet the needs of WCSOs and WHRDs, it is critical to centralize gender as it relates to experiences in accessing, using and protecting oneself in digital spaces. As such, in this training, we take a gendered lens and human-centric approach to understanding cybersecurity, acknowledging that women and girls are disproportionately affected negatively by cyber risks and that WHRDs and WCSOs are often specifically targeted by threat actors due to the nature and content of their work. This training differs from traditional cybersecurity capacity-building efforts in three ways:

- 1. Centralization of gender in cybersecurity practices:** Online gender dynamics perpetuate existing offline power relationships and inequalities such that women and girls tend to experience greater online violence. There are also gendered differences in access to and uses of digital technologies and differences in online behaviours and interactions, all of which affect cybersecurity and cyber resilience and, therefore, should be centralized in developing capacities.
- 2. A human-centric as compared to techno-centric approach to cybersecurity:** The goal of techno-centric cybersecurity is to prevent adverse events and secure technical assets (e.g. infrastructure, systems, software, and platforms) and the information contained therein. Human-centric cybersecurity positions human safety as the main aim of cybersecurity processes, practices and regulations. This training reorients towards people, their safety and their rights as central to cybersecurity.
- 3. An emphasis on human factors alongside technical cybersecurity skills:** Although digital skills are critical to achieving cybersecurity, psychological and behavioural factors have a major influence on information and systems security practices. As such, this training highlights the roles that people (including their motivations, feelings and experiences) play in perpetrating, preventing, responding and recovering from cyber risks.

### AIMS AND LEARNING OBJECTIVES

The overarching goal of the training programme presented in this manual is to ensure that all women and girls, as well as representatives of women's rights movements, women peacebuilders and WHRDs, are enabled and empowered to exercise their leadership, voice and agency in relation to digital transformation and the changing peace and security landscape. To achieve this, we seek to support and strengthen their ability to use digital strategies and tools to keep themselves, their data, devices and privacy protected, as well as to raise their awareness of cyber risks and how to mitigate against the harms these may cause.

*The aims, therefore, are to increase the overall knowledge, skills and effectiveness in preparing for and addressing gendered cybersecurity risks among*

*individuals and organizations that support women, girls and persons with diverse sexual orientation, gender identity and expression and sex characteristics.*

### Overall Learning Objectives

1. To increase knowledge and awareness of gendered cybersecurity threats and vulnerabilities, including how these may play out in conflict and crisis contexts.
2. To inform cybersecurity and cyber resilience strategies for individuals and organizations from a gendered lens and with a human-centred focus.
3. To empower women and women's advocates to reduce their cyber risks, disrupt their potential for harm and support their cyber resilience.
4. To create cybersecurity communities of practice among women and women's advocates that can support contextualized and responsive capacity-building efforts.

## How to use this Facilitator's Manual

This manual is meant to guide facilitators and organizers on how to plan, prepare for, and conduct training sessions to build cybersecurity capacity and cyber resilience among diverse audiences. Prepared with WCSOs and WHRDs in mind, it draws upon examples from across Southeast Asia. However, the training programme is flexible in that it can be adapted and modified to support the cybersecurity practices of any individual or organization that may benefit from a gender-sensitive and human rights lens on this topic. The manual is designed to speak directly to facilitators; thus, all instructions for delivery, discussion points and use of the training materials contained here are targeted at them. Materials — including all activities, PowerPoint presentations and handouts — are for reference and should be adapted to fit the facilitators' and audience's needs.

The manual has been developed to be used in association with a series of self-directed e-learning courses and related printable materials for participants. Facilitators should complete the relevant e-learning

modules before planning a training session in order to assist in selecting the appropriate modules to meet the needs of participants and to build on their knowledge and understanding of cybersecurity. All materials associated with the training can be accessed at: <https://doi.org/10.17605/OSF.IO/H38WZ>

### COURSE DESIGN

The facilitators need not possess a technical cybersecurity or data science background to successfully conduct this programme; the materials were designed for all levels of expertise. Technical skill development is not the focus of this training, rather, it was developed to support knowledge and awareness and to **assist with behaviour change**. Throughout the training, explanatory notes are provided where concepts may be new, and a glossary has been included to assist with technical terminology.

It is suggested that the size of the training should be between 15 and 25 participants due to the experiential focus and mix of small- and large-group activities.

The full course comprises four distinct, interrelated modules that are designed to be used flexibly, depending on the needs of the facilitator and audience. Each module comprises two 80-minute sessions that cover different topics. These sessions are built upon previous content but can be used as standalone training components. The total course content covers two full days of training, but could be adapted to various time-frames and configurations, depending on participant availability and the training's focus.

To assist in guiding an assessment of training needs, the overall aims of the modules and their specific sessions can be seen on the next page.

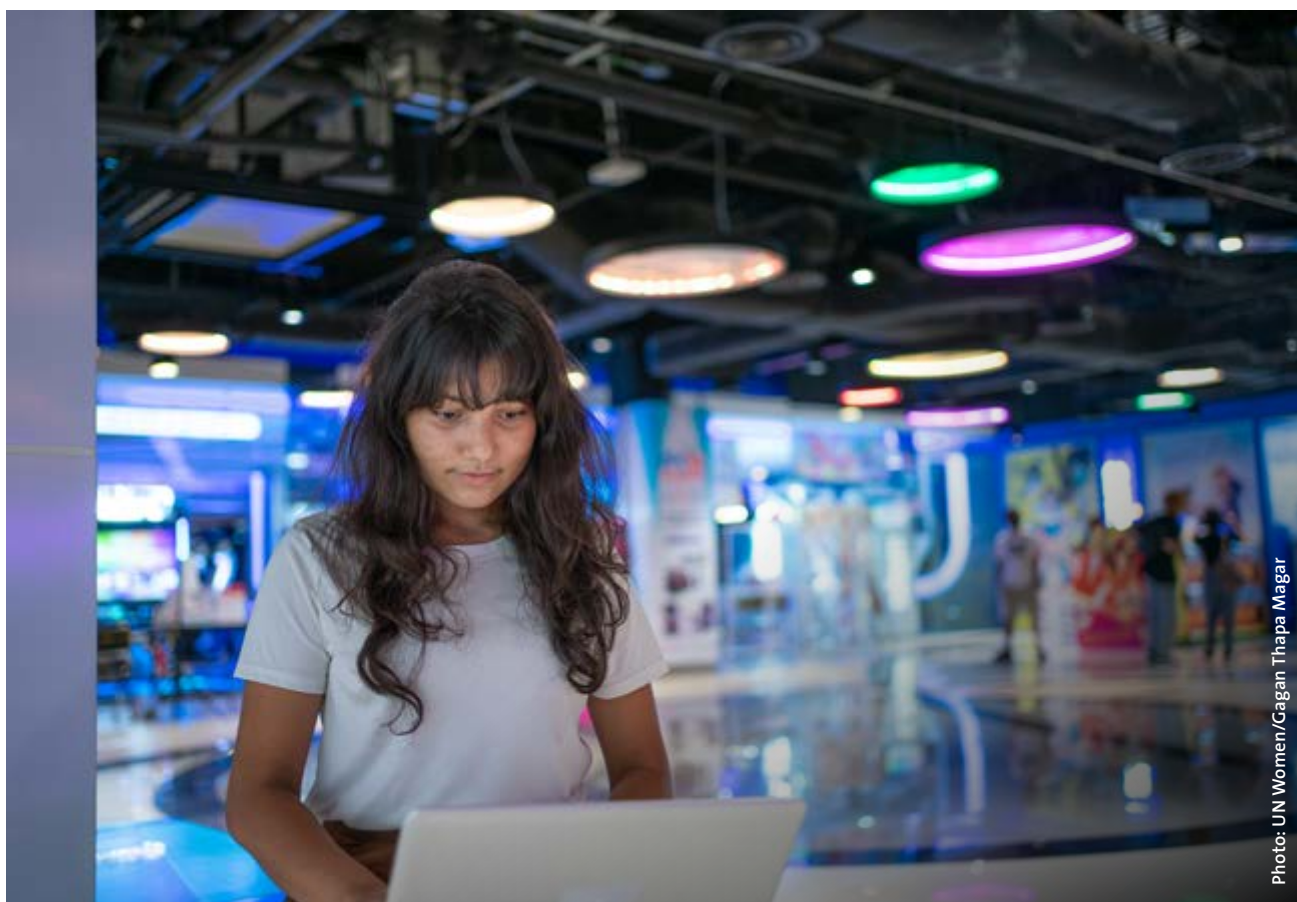


Photo: UN Women/Gagan Thapa Magar

## MODULE 1: CYBERSECURITY AND THE WOMEN, PEACE AND SECURITY AGENDA

Module 1 lays the foundation for understanding the intersections between gender, human rights, peace, security and digital technologies.

### > Session 1.1

Women, Peace and Security in the Digital World

- **Aim:** *To build knowledge on how gender is associated with peace and security in contemporary digitally connected contexts.*

### > Session 1.2

Gender and Cybersecurity

- **Aim:** *To develop an understanding of cybersecurity from a gendered lens.*

## MODULE 3: SECURING YOUR DATA

Module 3 offers practical strategies for individuals and organizations to secure their data and highlights the gendered dimensions of data-related cybersecurity threats.

### > Session 3.1: Data Access and Control

- **Aim:** *To highlight the importance of data protection and to develop skills to identify data-related threats and vulnerabilities.*

### > Session 3.2: Encryption and Data Backup

- **Aim:** *To develop an understanding of data security processes and to build data recovery skills.*

## MODULE 2: FOUNDATIONS FOR CYBERSECURITY MANAGEMENT

Module 2 introduces the basic elements of the cybersecurity ecosystem and introduces frameworks to help understand key cybersecurity concepts.

### > Session 2.1

The Cybersecurity Ecosystem

- **Aim:** *To define and contextualize the key features of cybersecurity in order to better understand their impacts and outcomes.*

### > Session 2.2

Cyber Harms and Risk Management

- **Aim:** *To build knowledge of the potential harms caused by cyber risks and to develop sufficient risk-management skills to mitigate risks and reduce harms.*

## MODULE 4: BEING SECURE ONLINE

Module 4 offers practical strategies for individuals and organizations to be secure in their online identities and online communications and highlights the gendered dimensions of cybersecurity threats that are associated with online interactions.

### > Session 4.1: Online Authentication Threats

- **Aim:** *To develop an understanding of the importance of protecting online identities and to introduce tools to support best practices.*

### > Session 4.2: Online Browsing and Communication Threats

- **Aim:** *To develop knowledge of secure networking, browsing and communications and to introduce tools to support best practices.*





**EXAMPLE COURSE SCHEDULE**

The following table presents an example of a full two-day course schedule. This schedule provides time for an introduction, review, scene-setting and closing

session. Brief guidance on how these sessions can be managed is provided below, but the facilitator should develop session contents with consideration of each session's specific needs and focus.

**TABLE 1. EXAMPLE COURSE SCHEDULE**

Session Description	Time
<b>Day 1</b>	
Introduction Session	30 minutes
<b>Session 1.1: Women, Peace, and Security in the Digital World</b>	80 minutes
<i>Morning tea break</i>	<i>15 minutes</i>
<b>Session 1.2: Gender and Cybersecurity</b>	80 minutes
<i>Lunch</i>	<i>60 minutes</i>
<b>Session 2.1: The Cybersecurity Ecosystem</b>	80 minutes
<i>Afternoon tea break</i>	<i>15 minutes</i>
<b>Session 2.2: Cyber Harms and Risk Management</b>	80 minutes
<b>Day 2</b>	
Scene-setting Session	30 minutes
<b>Session 3.1: Data Access and Control</b>	80 minutes
<i>Morning tea break</i>	<i>15 minutes</i>
<b>Session 3.2: Encryption and Data Backup</b>	80 minutes
<i>Lunch</i>	<i>60 minutes</i>
<b>Session 4.1: Online Authentication Threats</b>	80 minutes
<i>Afternoon tea break</i>	<i>15 minutes</i>
<b>Session 4.2: Online Browsing and Communication Threats</b>	80 minutes
Closing	30 minutes

### INTRODUCTION, REVIEW AND CLOSING SESSIONS

An introductory session should allow participants to get to know one another, set expectations, highlight the purpose of the training, outline learning objectives and clarify markers of programme success or achievement. Facilitators should provide an overview of the agenda and co-create or clarify norms that can contribute to an effective learning environment, encourage open discussions, foster inclusive interactions and support the sharing of ideas by all participants.

At this time, participants may agree on ground rules (e.g. active participation, listening). Co-creating these with participants, thus ensuring ownership, is encouraged. The ground rules should be displayed in the training room so that the whole group can help support them. Facilitators are encouraged to start the course with an activity of their choosing to break the ice and assist participants in building a sense of belonging, confidence and comfort.

If a course is planned to run for more than one day, a review session to highlight key takeaways, learnings and participant feedback at the end of the first day is strongly encouraged. Note that each module has a built-in review and debrief process, so this review session should attempt to gather general insights (e.g. What has been most impactful and why? What do you need more — or less — of? Do you have any major lingering questions?). The facilitator may request that participants lead this session or may take a more structured approach of summary and feedback.

A scene-setting session at the beginning of the second day should help to link the learnings (or gaps) from day one to the activities for day two. This session should reaffirm the objectives and norms, set the agenda and act as a bridge to connect the learnings of previous days to the overall objectives set by the facilitator. The closing session should act as a full review and debrief of the learnings throughout the course, focusing on overall knowledge and skills developed, gaps or questions that remain, and next steps.



Photo: UN Women/Ana Norman Bermudez

## OTHER TRAINING CONSIDERATIONS

### Timing

The following sections highlight the content for the training sessions. Although timing information is provided, these should be considered as estimates of the expected duration of modules and activities. Timing can differ significantly depending on factors such as the number of participants, their knowledge and familiarity with the topics discussed and their contributions to the discussion. Effective time management is needed to be able to progress through all the activities; the facilitator should adjust times to the needs and pace of the specific audience, especially when critical discussions emerge.

### Space

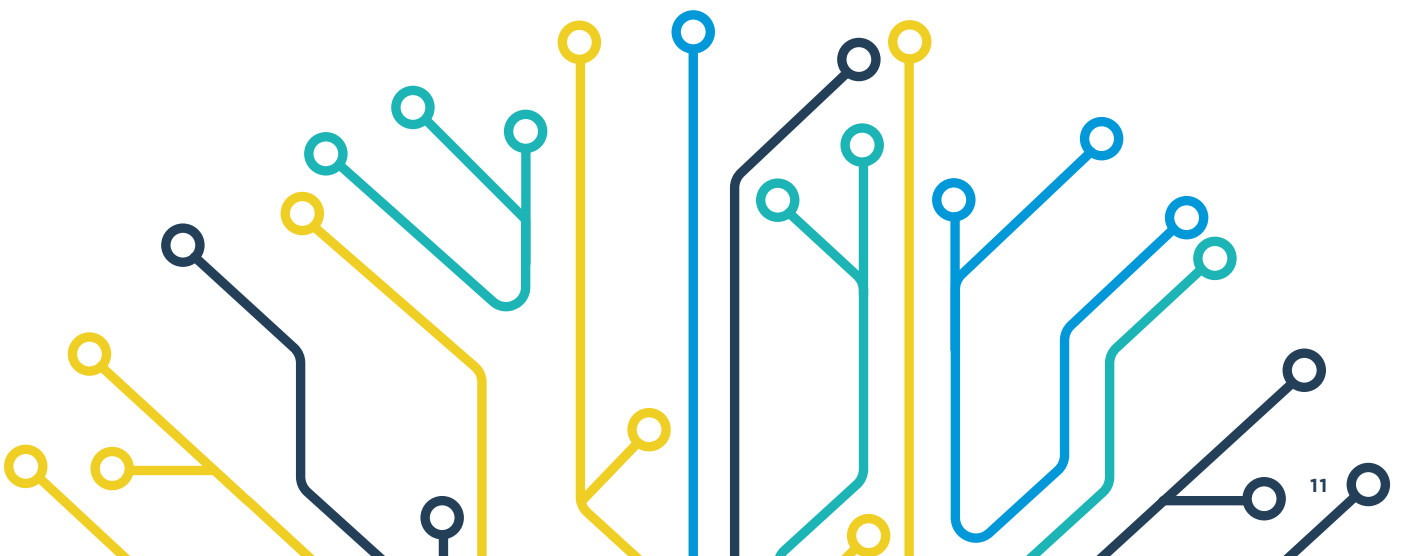
It is important to understand and plan for how the training space may impact activities and discussions. As the training is designed to be experiential, many activities require small and large group interactions. An arrangement with tables that can seat groups of four to six is likely to be best suited to the content, but the space and the organization of the chairs can be changed throughout the course to suit the activity and to create variety. For example, a circle or semi-circle arrangement (standing or sitting) can assist with large-group activities and feedback sessions.

### Debriefs

Regular debriefs and report-back sessions are integrated into the activities throughout the training. These are led by the facilitator, who should summarize and paraphrase key learnings and respond to requests

for clarification and additional information so that critical points of discussion are understood and shared by all participants. Report-backs have a very important function of consolidating learning and supporting the inclusion of multiple perspectives. While this manual includes suggested ways of conducting these report-backs, the facilitator can adapt different methods to the training. For example:

- > **Round robin reporting:** Where each individual or group presents one point at a time, going around the circle with every individual or group giving a new point until all points are thoroughly covered. In such a context, new information or thoughts are prioritized, contributions are equalized and repetition is avoided.
- > **One group/one topic:** Small group sessions in which each group brainstorms and then presents a different topic or question. This technique is useful when a lot of information needs to be covered in a short period of time; groups share new topics and information with the broader group to increase learning. The breadth of knowledge is prioritized, and repetition is avoided.
- > **Report back in paired groups:** Although this training focuses on reporting back to the larger group in all instances, this may not be the best approach for all groups. In some situations (especially with larger groups), two small groups meet and share what they have learned. The smaller numbers allow for more discussion among all participants and can assist participants in feeling safe when sharing sensitive information.



### NEEDS ASSESSMENT AND EVALUATION

Prior to organizing training and adapting content, facilitators are encouraged to conduct a learning needs assessment to measure participants' knowledge of concepts and to better tailor the training to their identified needs. It is also important to offer participants the opportunity to voice their expectations and/or motivations to undertake training on cybersecurity and how they are hoping to use the knowledge gained to support their work.

Alongside a needs assessment, organizers should consider conducting an evaluation to measure the outcomes and efficacy of the training. For example, an outcome evaluation focuses on changes that have occurred because of the training. To conduct such an evaluation, organizers may:

- › Collect participants' immediate feedback during and after the training through short polls, surveys or feedback mechanisms;

- › Assess participants' new knowledge according to the learning outcomes and aims of the materials or as per those identified by the organizers;
- › Organize a post-training group discussion (face-to-face or online) to collect participants' issues and practical examples of applying their cybersecurity knowledge; and
- › Gather information on the post-training practical integration of cybersecurity measures into participants' work or organization.

More details on conducting needs assessments and evaluations can be found in the Training for Trainers slide pack accessed at <https://doi.org/10.17605/OSF.IO/H38WZ>



Photo: UN Women/Play Phutpheng

# GLOSSARY OF TERMS



Before undertaking the training, the facilitator should familiarize themselves with the following terms, which are central to the course contents.

---

**Account hijacking** A fraudulent action that aims to take over a user’s account on an application or platform in order to take actions such as accessing their information, publishing content in their name or committing fraud. This is the primary technique through which individuals lose access to their accounts due to their credentials being compromised by attackers.

---

**Advanced persistent threat actors** Well-resourced, sophisticated and highly capable groups of threat actors who undertake targeted attacks. Some advanced persistent threat actors may be affiliated with or sponsored by state or political movements.

---

**Authentication** The process of verifying the claimed identity of a user through, for example, passwords and/or biometric information.

---

**Credential stuffing** Where credentials that have been previously compromised (e.g. through a data breach) are used to access other accounts.

---

**Cyberattack** A type of cyber threat involving a malicious act against a person, organization or nation, violating security and intentionally causing direct or indirect damage. Cyberattacks typically include deliberate acts to harm or exploit digital systems, information or processes.

---

**Cyber hygiene** The steps that computer and device users can take to improve their online security and maintain system health.

---

**Cyber resilience** The state of, or dynamic process in which, an individual, organization or entity can effectively maintain continuity or enhance operations through the prevention, disruption and mitigation of cyber threats with the result of avoiding or minimizing harm.

---

**Cyber resources** Often also referred to as ‘cyber assets’, these are physical and digital assets that belong to a person or organization that produce value, have worth and support the achievement of goals. These include tangible (e.g. computer hardware) and intangible (e.g. brand or personal reputation) assets.

---

**Cyber threats** Adverse cyber incidents that have the potential to cause harm to individuals, organizations and entities through technological systems and the way they are used (e.g. by compromising the functional capacity of assets, exploiting cyber vulnerabilities, or by leveraging social and psychological vulnerabilities).

---

---

**Cyber vulnerabilities** Technical and non-technical weaknesses that can exacerbate the harms caused by or increase the likelihood of exploitation and exposure to cyber threats.

---

**Cyber-bombing  
Zoom-bombing** A type of cyberattack in which an individual or a group of unwanted and uninvited users interrupt online meetings and events for the purpose of disruption.

---

**Cybersecurity** A state in which information and/or computer systems and networks are free from threat, as well as the set of practices undertaken by individuals and organizations to ensure such security.

---

**Data breach** Any event that exposes confidential, sensitive or protected information.

---

**Disinformation** False information that intentionally misleads, such as propaganda intended to influence elections or foster conflict (see 'misinformation' below).

---

**Distributed denial of service (DDoS):** A type of cyberattack in which threat actors disrupt or flood the services of a user's network-connected host, thereby making digital resources unavailable to or unusable by legitimate users.

---

**Doxxing** Private or identifying information distributed about a person on the Internet without their permission.

---

**Encryption** The process of encoding information to prevent anyone other than its intended recipient from viewing it.

---

**Hacking** Unauthorized access to or control over computer network security systems for an illicit purpose.

---

**Human-centric cybersecurity** Centralizing people (rather than technology) as the primary subjects of cybersecurity practices.

---

**Impersonation** Intentionally assuming an identity, name or image of someone else (or of a business or organization) to deceive, defraud or harm others.

---

**Insiders** People within an organization who have non-public knowledge of the organization's inner workings and systems, who then intentionally or unintentionally undertake actions that cause harm and damage to the organization.

---

**Malware** Any program or file that is intentionally harmful (i.e. malicious) to a computer, network or server.

---

---

**Misinformation** Incorrect or misleading information, which, in contrast to disinformation, is not spread to knowingly deceive its recipient (see 'disinformation' above).

---

**Multi-factor authentication (MFA):** A multi-step account login process that requires users to enter more information than just a password.

---

**Phishing** Malicious emails designed to trick people into falling for a scam, divulging sensitive information or taking another action against their or their organization's interests.

---

**Ransomware** A type of malware that is designed to block access to a computer system or files until a condition is met (often a sum of money to be paid).

---

**Spoofing** Pretending to be a trusted entity to extract personal information by manipulating information (e.g. email addresses, websites, domains).

---

**Spyware** A type of malware that is designed to enter a device, gather data and forward it to a third party without consent.

---

**Trolling** Deliberate attempts to offend, inflame, attack or provoke.


---

**Virtual private network (VPN)** A mechanism for creating a secure connection between a device and a network through mechanisms such as encrypting information, masking user information, and protecting online identities.

---

**Virus** A type of malware that, when executed, can self-replicate, infect/modify other programmes and spread to other computers.

---



## MODULE 1: CYBERSECURITY AND THE WOMEN, PEACE AND SECURITY AGENDA

### Overview

Gender-inclusive cybersecurity and a digital environment that protects and promotes women's digital rights is critical for global development, peace and security. This module introduces the Women, Peace and Security (WPS) agenda and discusses it in the context of cyberspace. The module lays the foundation for understanding the intersections between gender, human rights, peace, security and digital technologies. The module content outlines the links between cybersecurity and the WPS agenda in order to ensure that everyone can be better prepared and able to address current and future risks to online security in a gender-responsive manner and to build confidence in using technologies for good, including building peace.

### MODULE LEARNING OBJECTIVES

At the end of this module, participants are expected to:

1. **Be aware** of the gender digital divide and gender-specific risks in cyberspace and how gender inequities reduce opportunities to build peace and security for everyone.
2. **Be familiar** with the cybersecurity concepts and be able to both define and distinguish techno-centric and human-centric cybersecurity approaches.
3. **Understand** how gender considerations influence cybersecurity practices and outcomes.
4. **Develop an understanding** of the differences and similarities between online gendered harms and gendered cybersecurity threats.



# SESSION 1.1. WOMEN, PEACE, SECURITY AND THE DIGITAL WORLD



## AIM

To build knowledge on how gender is associated with peace and security in contemporary digitally connected contexts.



## AGENDA

- |  |            |
|--|------------|
| 1. What is the WPS Agenda?                       | 20 minutes |
| 2. The gender digital divide                     | 20 minutes |
| 3. Enabling safe online spaces                   | 30 minutes |
| 4. Innovation for technology and gender equality | 10 minutes |



## TOTAL TIME

80 mins



## RESOURCES

- > PowerPoint slides Module 1
- > Flipchart
- > Markers
- > Post-it notes

## What is the WPS agenda?



### LARGE-GROUP WORK: TIME 20 MINUTES

1. Show participants **slide 1.1**, which outlines the background and pillars of the Women, Peace and Security Agenda
  - a. Ask participants whether they are familiar with the WPS agenda, and if so, how familiar they are. Different levels of information may be needed, depending on how knowledgeable participants are.
  - b. More information on the WPS Agenda can be found at [https://www.youtube.com/watch?v=\\_bDTvGbjzjM](https://www.youtube.com/watch?v=_bDTvGbjzjM), a video from the UN Women Regional Office for Asia and the Pacific. This video can be presented as an additional resource for the training or used as background information.
  - c. Clearly highlight the four pillars of the WPS agenda: Participation, Protection, Prevention, Relief and Recovery.
2. Ask the large group, **How does the digital world impact the WPS agenda?**
  - a. The group brainstorms ways that digital technologies and how they are used might impact the WPS agenda.

- b. Capture insights on a flipchart. Insights can be grouped into main areas or topics based on discussion contents.

**3. Depending on the amount of time and participants' level of engagement and knowledge base, the facilitator may follow up by asking the following questions to guide the discussion (notes on possible responses provided):**

- a. *What is meant by the digital world?*
  - i. This refers to a variety of issues, including the omnipresence of technology in our lives due to the Internet and digital devices, the transformation of products and services to digital platforms and contexts, the shift of everyday life (social, economic, educational) to online environments, and the importance of technologies in creating and closing gaps in access.
- b. *Does technology pose mainly positive or mainly negative implications for gender equality and the safety and security of women?*
  - i. It depends on how you look at the issue, as it has the possibility of supporting peace efforts and reducing conflict. However, this does not mean that the benefits and issues are distributed evenly across groups. Those who are marginalized tend to be less likely to be recipients of positive impacts.

**> KEY FACILITATION NOTE**

While the WPS agenda sets the context for the inclusion of women in peace and security processes, now that the world is increasingly digital, we need to consider how *emerging* global issues that come about as a result of such changes influence the security of women and girls.

---

## The Gender Digital Divide



LARGE-GROUP WORK: **TIME 20 MINUTES**

**1. Show participants slide 1.2, which outlines the gender digital divide.**

- a. Highlight that there are three key issues in the gender digital divide: lower levels of access to digital technologies, less representation in tech roles and leadership, and fewer education pathways/ outcomes for women in tech.

**2. If connected to the Internet and using a slideshow, open the two links below. If not connected to a shared screen, ask participants to navigate to one of the websites on their device. Alternatively, website materials can be sourced and printed for participants beforehand.**

- a. Gender Digital Divide, UN International Telecommunication Union (ITU), available at <https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-the-gender-digital-divide>
- b. Gender Gaps, available at <https://www.digitalgendergaps.org>

### 3. Lead a guided exploration of one or both of the websites.

- a. On the ITU website, highlight the difference in proportions of women and men accessing the Internet across world regions and income levels.
- b. On the Gender Gaps website:
  - i. Draw participants' attention to the Digital Gender Gap key that shows the level of equality. The spectrum from red to blue represents lesser to more equality, respectively.
  - ii. Select and click on a country.
  - iii. Review the default selected indicator, Internet GG Online, which represents the ratio of female-to-male Internet use using the Facebook Gender Gap Index.
  - iv. Change the indicator to Mobile GG online, which represents the ratio of female-to-male mobile phone use using the Facebook Gender Gap Index.
  - v. If time allows, ask participants to select a specific country (or more than one) to investigate. Try to select countries that differ in their levels of access. You may also explore the different indicators.
- c. Depending on the amount of time and participants' level of engagement and knowledge base, the facilitator may follow up by asking the following questions to guide the discussion (notes on possible responses provided):
  - i. *Why might there be incomplete data (some countries are missing from the Gender Gaps website), meaning we cannot compare all countries?*
    - This is often because the relevant information is not routinely collected in all of the countries listed or is not made available due to data sensitivities or current geopolitical tensions. It may also be because of a lack of support or capacity to collect and disseminate the information.
  - ii. *In countries where there is gender parity in access to the Internet and mobile phones, might there be other differences between women's and men's use of technology?*
    - Even in contexts where women are able to access the Internet at the same levels as men, they may face other barriers. For example, they may have to share a device or may not have the same level of digital skills. (Much more will be discussed about this issue.)
  - iii. *When we compare the regional to the country-specific results, what does this say about variations within the region? Why do some countries fare better than others?*
    - The Asia-Pacific region is a good example of variability in regional versus national-level digital divides. The region includes countries with some of the lowest and highest levels of digital access in the world. For example, in Southeast Asia, some countries are highly digitally

connected and have few gender gaps, while others face conflict and crisis, meaning that there are likely to be greater inequities.

- d. Summarize the findings and reflect as a group; focus on addressing the following question: *What are some of the reasons why women are underrepresented in tech (access, employment, education)?*

#### > KEY FACILITATION NOTE

One of the key difficulties that remain in unlocking the benefits of the digital world for women is the gender digital divide. To assist with background information, the facilitator can read a primer on this issue from USAID at [https://www.usaid.gov/sites/default/files/2022-05/DAI-1089\\_GDD\\_Primer-web\\_rev1\\_9.6.21.pdf](https://www.usaid.gov/sites/default/files/2022-05/DAI-1089_GDD_Primer-web_rev1_9.6.21.pdf). To extend the discussion to other elements of the gender digital divide, the facilitator may introduce a report by UNICEF on digital skills and STEM education among girls and boys at <https://www.unicef.org/globalinsight/stories/mapping-gender-equality-stem-school-work>. The UNICEF website captures many critical insights, although the number of included countries is relatively small.

## Gendered Digital Access



SMALL-GROUP WORK AND PLENARY: **TIME 30 MINUTES**

1. Show participants slide 1.3 and read the quote out loud.
2. Divide participants into pairs or small groups of three to five participants. Let the groups spend five to seven minutes using their experiences to discuss what it would mean for cyberspace to be an accessible and safe place where all women and girls could freely participate.
3. Ask groups to answer this question: “How do we enable safe and secure access to online spaces for women and girls?”
  - a. Give small groups or pairs five minutes to produce as many responses as they can to this prompt, each written onto a separate Post-it note.
  - b. Each person in the group selects one Post-it that they would like to share, which they read out to the group at large.
  - c. After it is shared, the participant adds their Post-it to a larger brainstorm on a flipchart at the front of the room. Have individuals attempt to give novel answers if something that they have said has already been covered.

4. **Summarize the brainstorm and may move the initial Post-its so that they form thematic groups by asking for input from the larger group.**
    - a. Participants are then asked to come up to the flip chart and place the remainder of their ideas, assisting the facilitator with grouping similar thoughts.
    - b. Individuals can shift and move Post-its as they see fit or add more context.
  5. **Summarize the findings and asks participants to reflect on what they think are the most pressing issues identified.**
- 

## Innovation for technology and gender equality



LARGE-GROUP REFLECTION: **TIME 10 MINUTES**

1. **Ask participants to watch a short video by the Simpleshow Foundation (CC licensed) to find out more about gender as it relates to technology, available at <https://www.youtube.com/watch?v=3elqloYor5E>.**
2. **After the video, have participants use a round-robin share technique to summarize their thoughts and feelings about the impacts of digital transformation on the WPS agenda.**
  - a. Participants should each share one learning from the video, with each person sharing a new learning as they contribute.
3. **Provide a brief summary of the session and reiterate critical learning points.**

# SESSION 1.2. GENDER AND CYBERSECURITY



## AIM

To develop an understanding of cybersecurity from a gendered lens.



## AGENDA

- |                                   |            |
|-----------------------------------|------------|
| 1. What is cybersecurity?         | 10 minutes |
| 2. Personal cybersecurity         | 20 minutes |
| 3. Gender and cybersecurity       | 30 minutes |
| 4. WCSOs, WHRDs and cybersecurity | 20 minutes |
| 5. Reflection                     | 10 minutes |



## TOTAL TIME

80 mins



## RESOURCES

- > PowerPoint slides Module 1
- > Handout 1.1 – Case Studies in gendered cybersecurity
- > Note paper and pens
- > Flipchart
- > Markers

---

## What is Cybersecurity?



### LARGE-GROUP WORK: TIME 10 MINUTES

1. Ask the large group, “*What does cybersecurity mean to you?*”
2. Capture insights on a flipchart.
3. Show participants [slide 1.4](#), which outlines the many different definitions of cybersecurity.
4. Ask participants to indicate the commonalities they can see. These similarities can be drawn out using the coloured text, highlighting that cybersecurity is often conceptualised as:
  - a. Focusing on networks, devices, systems and data (technical elements);
  - b. Referring to reducing risks and protecting assets from attacks; and
  - c. Relating to the practices of organizations and individuals.

5. Ask the large group, *Do these definitions align with the understanding of cybersecurity as discussed previously? What similarities do they share, and how are they different?*
6. Show participants [slide 1.5](#), which outlines extensions to the definitions of cybersecurity. Convey the following points (guided by the slide):
  - a. Technical orientation: Traditionally, cybersecurity has been considered from the technical and organizational perspective, focusing on information security, infrastructure security, systems security, and the software and platform security of businesses.
  - b. Human orientation: Cybersecurity policies and procedures are developed and shaped by people, including the technical staff who support information and communication technology systems and those who use the organization's digital assets.
    - i. Cyber hygiene (good security practices) of individuals has a major influence on the effectiveness of cybersecurity practices.
    - ii. The harms caused by cyber threats are often felt at the individual level, even if they are targeted at the organization (e.g. impacting personal health and well-being)
7. Show participants [slide 1.6](#), which outlines human-centric cybersecurity. Convey the following points (guided by the slide):
  - a. The Association of Progressives Communication's definition of human-centric cybersecurity is: A human rights-based approach to cybersecurity means putting people at the centre and ensuring that there is trust and security in networks and devices that reinforce, rather than threaten, human security. Read more at <https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity>
  - b. This definition highlights the need to protect systems and networks so that they can support and create a foundation for the expression and exercise of human rights (e.g. access to information, freedom of thought and freedom of association).
  - c. The approach taken in this course: Positioning people (rather than technology) as the primary subjects of cybersecurity so that human safety is the main aim of cybersecurity processes, practices, and regulations.
8. Debrief with participants by asking them to reflect on and share their thoughts on the following question: *"If organizations and nations were to adopt human-centric understandings of cybersecurity, how might this change the way we approach digital safety?"*

#### > KEY FACILITATION NOTE

Human-centric cybersecurity acknowledges the importance of people's thoughts, feelings and experiences in creating cyber risks and vulnerabilities, and it positions people (rather than technology) as the primary subjects of cybersecurity. Taking a human-centred understanding reorients thinking and treats human safety as the main aim of cybersecurity processes, practices and regulations.

---

## Personal Cybersecurity Reflection

---



INDIVIDUAL ACTIVITY: TIME 15 MINUTES

---

- 1. Show participants slide 1.7, which includes a set of yes/no cybersecurity questions regarding the applications that participants use personally and professionally in everyday life:**
  - 1) Do you use the same password for more than one of your accounts?
  - 2) Did you back up your data more than six months ago?
  - 3) Do you ignore or delay software update notifications?
  - 4) Do you have antivirus software installed on your devices?
  - 5) Do you know the security settings on your devices?
  - 6) Have you checked app permissions and privacy settings recently?
- 2. These questions can be presented all at once. Participants are asked to write the numbers one through six on their paper and answer yes or no to each question on their own.**
- 3. Then show participants slide 1.8, which includes a set of reflection questions concerning the digital devices and their use. The questions should be asked one at a time. Give participants around one minute per question to quietly write their answers to each on a piece of paper.**
  - a. What sorts of information do you share?
  - b. What protections do you currently have in place?
  - c. What vulnerabilities might you have?
  - d. How likely do you think it is that your devices might be or become compromised?
  - e. How easily could you recover from a cyber threat?
- 4. After all questions have been completed, ask participants to look at their answers to the questions on slide 1.7. They should be told that if they said yes to either 1, 2 or 3 and no to 4, 5 or 6, they may be vulnerable to cyber threats. Later modules will discuss the importance of these questions as they relate to cybersecurity.**
- 5. Progress through the reflection questions on slide 1.8 one by one, asking for volunteers to give their answers, starting with the first question and moving through to the sixth question in turn. The facilitator can ask one or more of the prompt questions below to assist with a broader interactive discussion (these should be chosen based on the time allocation and the audience):**



- *Why do you share some types of information and not others?*
- *Where do you share information?*
- *What ways do you actively protect yourself and your information?*
- *In which ways do you not protect yourself enough?*
- *Why is it likely or unlikely that you will be compromised? How might you be subject to cyber threats if this were to happen?*
- *What types of threats would be more or less easy to recover from and why?*

**6. The discussion session should end with a debrief in which participants are asked to reflect on commonalities in their experience of personal cybersecurity behaviours. Use the key facilitation notes to assist with the debrief.**

#### > KEY FACILITATION NOTE

People tend to have an optimism bias when it comes to cybersecurity and believe that although cyber threats are important and potentially harmful, they are unlikely to be personally targeted. We also tend to underestimate the impacts of cyberattacks and fall victim to the privacy paradox, in which people say that they value privacy highly yet give up their personal data in exchange for very little benefits and fail to take measures to protect their privacy. People tend to prefer convenience over protecting their privacy or may believe that they are unable to protect their privacy online.

## Gendered Influences on Cybersecurity



SMALL-GROUP REFLECTION: **TIME 25 MINUTES**

1. To find out more about gender as it relates to cybersecurity, participants may watch a short video on the [gender dynamics in cybersecurity](https://www.youtube.com/watch?v=63gE25c1NSI) from the United Nations Institute of Disarmament Research, available at <https://www.youtube.com/watch?v=63gE25c1NSI>
2. After the video, divide participants into small groups of three to five people and ask them to spend five to seven minutes discussing the following questions:
  - a. *“The design of technology is gendered because it often privileges male perspectives and users and perpetuates stereotypes. What are some of the ways that cybersecurity design (e.g. the programmes, policies and tools to protect cybersecurity) is gendered?”*

- b. *“What is considered to be a gendered cyber threat that has gendered outcomes? What are some examples of gendered cyber threats and outcomes?”*
- c. *“Cybersecurity responses often involve distinct gender dynamics; in what ways might reporting of threats be gendered or minimize the experiences of women and girls?”*

**3. Each small group should briefly share their thoughts about gendered influences in cybersecurity with the larger group.**

**4. The facilitator reads the following note out loud: A critical element of gendered cybersecurity is that women and girls experience online violence at a much higher rate than men. Technology-facilitated gender-based violence (TFGBV) is a major cyber threat that has important and disproportionate implications. The risks of online harms are even greater in conflict-affected and politically volatile contexts and for women advocates and women human rights defenders.**

**5. Show participants [slide 1.9](#) concerning TFGBV; address the following talking points, guided by the slide:**

- a. By the age of 15, 10 per cent of women have already experienced some form of TFGBV.
- b. TFGBV is violence that is made possible by digital technologies.
- c. TFGBV includes any act that is committed or amplified using digital tools or technologies that causes physical, sexual, psychological, social, political or economic harm to someone because of their gender; women and girls experience TFGBV at much higher rates than men. These forms of violence are part of a larger pattern of violence against women. Women and girls are often disproportionately targeted by hate speech, sexualized online abuse and cybercrime.
  - i. TFGBV is often used systematically to discredit and silence women, particularly those in public positions such as politicians, journalists, human rights defenders and peacebuilders. This negatively impacts their ability to safely conduct their work and contribute to human/women’s rights and peacebuilding efforts. In addition, offline violence against women has strong associations with violence online, where perpetrators (individuals, organizations and other actors) use technology to directly target, surveil, stalk or harass their victims.

**6. Show participants [slide 1.10](#) and address the following talking points (listed on the slide):**

- a. TFGBV includes, but is not limited to:
  - i. Hate speech that targets women and persons with diverse sexual orientation, gender identity and expression, and sex characteristics, or gender equality advocates at large;
  - ii. Disinformation, which aims to discredit women, often those holding public positions such as politicians, journalists, peacebuilders and human rights defenders;
  - iii. Online harassment and threats of offline violence and abuse;
  - iv. Doxxing, the non-consensual spread of someone’s personal data, which can be used for slander campaigns, stalking or other forms of harassment;

- v. Image-based abuse, such as non-consensual sexual content, including those generated through new types of technologies (e.g. deep-fakes and other types of content generated by artificial intelligence);

## 7. Ask the participants to contribute their thoughts about TFGBV use the following optional prompts for the discussion:

- a. *Have you or someone you know experienced TFGBV?*
- b. *Have you seen gendered violence in online settings?*

### > KEY FACILITATION NOTE

Physical acts of violence are often considered more serious than, or separate from, TFGBV; many relevant laws, policies and practices only apply to the offline world. However, this fails to understand that violence against women is experienced as a continuum of online and offline experiences and can spill over from one context to the other. The issue of TFGBV is particularly pressing in conflict- or politically volatile contexts, given that general incidences of violence and persecution tend to be higher. For further information, the facilitator may review 'FAQs: Trolling, stalking, doxing and other forms of violence against women in the digital age' at <https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence>

## WHRDs, WCSOs, and Cybersecurity



SMALL-GROUP WORK: **TIME 20 MINUTES**

### 1. Show participants [slide 1.11](#) and read through the information (included on the slide):

- a. Digital technologies are central to the work of WHRDs and WCSOs. Women advocates are susceptible to cyber threats due to:
  - i. **The sensitive nature of their work:** Dealing with confidential information and personal data makes them attractive targets for cybercriminals and other adversaries.
  - ii. **A lack of resources and technical expertise:** Difficulties in preparing, preventing and protecting against cyberattacks.
  - iii. **The nature of issues:** Where gender is a contentious social issue, WHRDs and WCSOs are attacked in order to undermine their efforts and advocacy.

### 2. Read out loud verbatim, or adapt the following note:

- a. Those working with and for women and girls are targeted with online harassment that tends to be specifically gendered in nature, including threats of sexual violence or attempts to discredit their work by attacking their gender identity and expression or sexual orientation. This can impede their activism and limit their ability to engage effectively both online and offline; some advocates choose to withdraw from their work out of fear for their or others' safety. Of critical importance, WCSOs and WHRDs may be more likely to be targeted by those seeking to silence or discredit feminist movements, challenge gender equality or otherwise suppress human rights.
- 3. Divide participants into three small groups where they will review case studies about cybersecurity threats to WHRDs and WCSOs. Each group is provided with one of the three prepared case studies (Handout 1.1).**
- 4. For the next 10 minutes, participants in their small groups discuss the case and answer the following questions on a flip chart:**
  - a. What would you do if you had this experience? Specifically, how would you take action, and how would you feel?
  - b. What are the ways that this can be prevented? Specifically, what do you think are best practices, and what support or resources do people need to address such issues?
- 5. Discuss common themes using the answers produced by the small groups to summarize and debrief the activity.**

---

## Women, Peace and Cybersecurity Reflection



LARGE-GROUP WORK: TIME 10 MINUTES

- 1. Show participants slide 1.12 and read through the information (guided by the slide):**
  - a. As is the case in traditional peacebuilding spheres, the WPS agenda offers a framework to ensure that the different needs of women, men, girls and boys before, during and after conflict are met. The WPS agenda can be used to address cybersecurity issues, including:
    - i. **Participation:** Strengthening women's leadership and meaningful participation in the fields of cybersecurity, cyber-related legislation, cyberdiplomacy and decision-making.
    - ii. **Protection:** Safeguarding the human rights, physical safety and mental well-being of persons in online spaces, giving specific attention to the disproportionate effects that technology-facilitated harms and crimes have on women (especially in conflict and post-conflict societies).
    - iii. **Prevention:** Leveraging conflict-sensitive and gender-responsive approaches to detect and prevent the gendered impacts of digital security threats, harms and crimes that are facilitated by information and communications technologies.

- iv. **Relief and recovery:** Utilizing the positive potential of deploying context-specific, rights-based and gender-responsive technological solutions in order to enhance and expand the reach of relief and recovery efforts in post-conflict and post-crisis contexts.

**2. Asks participants to use a round-robin share technique to summarize their thoughts and feelings about the relationship between gender and cybersecurity.**


- a. Participants each share one word to represent how they feel and one learning from the session.

**3. Offers a brief summary of the session and can reiterate the module's learning objectives to address whether they were met during the session.**

- a. **Be aware** of the gender digital divide and gender-specific risks in cyberspace and how inequities in gender reduce opportunities to build peace and security for everyone.
- b. **Be familiar** with cybersecurity concepts and be able to both define and distinguish techno-centric and human-centric cybersecurity.
- c. **Understand** how gender considerations influence cybersecurity practices and outcomes.
- d. **Develop an understanding** of the differences and similarities between online gendered harms and gendered cybersecurity threats.

**> KEY FACILITATION NOTE**

Gender inequality is very prevalent offline and is replicated in our new digital worlds. Gender can no longer be seen as a marginal element of cybersecurity because even if cyberattacks themselves are not directly gendered, they often have gendered impacts. Similarly, digital spaces can no longer be seen as separate from our political, social and economic lives. Therefore, digital security is an important consideration for broader peace and security concerns.



## MODULE 2: FOUNDATIONS FOR CYBERSECURITY MANAGEMENT

### Overview

This module introduces cybersecurity and risk management from a gendered lens. It maps out the basic elements of the complex cybersecurity ecosystem and introduces frameworks to help understand key cybersecurity concepts. The module also introduces the important topic of risk management and details an approach that can be followed to systematically manage cybersecurity risks for WHRDs and WCSOs in the digital world.

#### LEARNING OBJECTIVES

At the end of this course, participants are expected to:

1. **Understand** the cybersecurity domain as comprising not only the technical elements but also the human and social elements from a gender lens.
2. **Make sense of the cybersecurity landscape for WHRDs and WCSOs** in terms of the associated resources, vulnerabilities, threats, responses and harms.
3. **Gain familiarity** with the basic terminology and concepts in cybersecurity.
4. **Understand** risk management processes and be equipped to undertake cybersecurity risk management.
5. **Have** the basic foundations on which to build further understanding and practice of cybersecurity risk management.
6. **Understand** how responses and countermeasures fit within larger cybersecurity and risk management practices.

# SESSION 2.1. THE CYBERSECURITY ECOSYSTEM



## AIM

To define and contextualize the key features of cybersecurity in order to better understand their impacts and outcomes.



## AGENDA

- |                                      |            |
|--------------------------------------|------------|
| 1. The cybersecurity ecosystem       | 15 minutes |
| 2. Cyber vulnerabilities             | 20 minutes |
| 3. Cyber threats                     | 30 minutes |
| 4. Cyber threat actors               | 15 minutes |
| 5. Human-centric cybersecurity goals | 10 minutes |



## TOTAL TIME

80 mins



## RESOURCES

- > PowerPoint slides Module 2
- > Handout 2.1 – Cyber threat terms and definitions (prepared into cards)
- > Note paper and pens
- > Flipchart

## The Cybersecurity Ecosystem



### LARGE-GROUP WORK: TIME 10 MINUTES

1. Show participants **slide 2.1**, which depicts the cybersecurity ecosystem. Read the following note out loud: *The overall cybersecurity landscape can be considered as comprising four critical features: cyber resources; two main cyber risks; cyber threats and cyber vulnerabilities; and harms. We will be talking about each of these in this module, starting with cyber resources.*
2. Show participants **slide 2.2**, which depicts the cybersecurity ecosystem and resources. Read the following (guided by the slide):
  - a. Threat actors achieve their objectives by targeting/attacking resources via cyber threats and compromising them via cyber vulnerabilities (discussed later). 'Resources' refers to all of the physical and non-physical things that belong to you and your organization that have value or worth, including:
    - i. **Tangible** resources, including digital devices and systems such as laptops, personal mobile devices, software, social media accounts and networking infrastructure; and

- ii. **Intangible** resources, including intellectual property, knowledge, online identities, information/data, relationships and reputation.
- b. How cyber risks impact resources:
- i. Cyber threats target resources directly by undertaking cyber-attacks;
  - ii. Cyber vulnerabilities compromise the security of the resources; and
  - iii. Cyber threats indirectly target resources by exploiting vulnerabilities and compromising their security.
- 3. Ask the large group: *Think about all of the Internet-connected digital devices that you have access to and the personal information that is connected or stored on these. What would be the impact if these resources were targeted or compromised? What might be gained by an actor getting access to your resources?***
- 4. Ask volunteers to share their thoughts with the group.**
- 

## Cyber Vulnerabilities



PAIR SHARE ACTIVITY: TIME 20 MINUTES

- 1. Show participants slide 2.3, which depicts the cybersecurity ecosystem and cyber vulnerabilities. Read the following note (details outlined on the slide):**
  - a. Cyber Vulnerabilities are weaknesses that can be exploited by cyber threats to gain access to cyber resources. There are three main types of vulnerabilities:
    - i. **Digital** weaknesses are associated with the software you use, the data you store, or your Internet connection;
    - ii. **Physical** weaknesses are associated with the actual devices that you own or use; and
    - iii. **Individual** weaknesses are the way that you use digital devices and the situations you are exposed to that increase the likelihood of being exploited and compromised.
- 2. Group participants into pairs that work together to develop a list of all of the vulnerabilities they may have (or can think of) for each of the three cyber vulnerability factors above.**
- 3. Participants take 10 minutes to discuss and then present their insights to the larger group.**
- 4. Capture key vulnerabilities on a flipchart and summarize the information by asking:**
  - a. *Why does this training group have these particular vulnerabilities?*



- b. *Would another group of people have similar vulnerabilities? Why or why not?*
- c. *What contextual, social or cultural factors influence these vulnerabilities? In what ways do gender identity and expression play into these dynamics?*

#### > KEY FACILITATION NOTE

Cyber vulnerabilities tend to be based on the way that we assess our use of devices, how we rate our skills and efficacy in using technology, the software and operating systems we use, the places we work, whether our devices are shared with other people, and how much weight we put on maintaining security and privacy as compared to convenience. Some of these things are outside of our control, but many of the vulnerabilities that we have can be minimized by thinking more about security and expending more effort on it, growing capacity and confidence in the use of digital devices, and being aware of behaviours that undermine security. These are being discussed now; Module 4 discusses how to manage weaknesses.

## Cyber Threats



SMALL-GROUP ACTIVITY: **TIME 30 MINUTES**

1. Show participants [slide 2.4](#), which depicts the cybersecurity ecosystem and cyber threats. Read the following note (guided by the slide):
  - a. Cyber threats are any circumstance, action or event that has the potential to adversely impact cyber resources and cause harm via unauthorised access, destruction, disclosure, information modification or other forms of disruption.
    - i. Threats often do not occur in isolation; they are typically part of a coordinated set of actions that target and attack resources to achieve specific goals. For example, a cyber threat could have the goal of accessing sensitive data or planting spyware (a piece of software designed to collect information about an individual without their consent and send it to a third party). Some of the tactics that they would employ towards these include preliminary research and investigations from publicly available data (e.g. published on social media) to gain access to the target's system to install malicious software and execute their data theft or surveillance goals.
    - ii. Cyber threats are varied but fall into two main categories:
      - Technological, through malicious targeted attacks (e.g. viruses, data breaches and ransomware) or malfunctions (e.g. of devices, systems, networks or equipment); and
      - Physical, through intentional acts (e.g. theft or confiscation of devices) or natural disasters or outages (e.g. fire, flooding, loss of resources, power outages, strike, absence of personnel or network outage).

2. Divide participants into small groups of three to five people. Give each group a set of terms and a set of definitions (prepared by printing out and cutting up [Handout 2.1](#) into distinct terms and definitions that are then mixed up).
3. Give groups five minutes to match the threats to their definitions.
4. Provide the correct answers and then debrief participants about the types of threats. The following prompts may be used:
  - a. *Which threats did you know already, and which ones were new to you?*
  - b. *What do you think are the most and least common types of threats?*
  - c. *Are there any threats that you think are more commonly faced by women or gender equality advocates?*
  - d. *Have you or anyone you know experienced any of these threats?*

**> KEY FACILITATION NOTE**

Research has found that WCSOs and WHRDs tend to be very aware and knowledgeable about many types of cyber threats and that they tend to experience these at a greater rate than CSOs that do not have a specific focus on women. The most common types of threats experienced tend to be disinformation, online harassment and phishing. Personalized and sexualized violence were more likely to be experienced by WCSOs. Cyber-bombing and organization impersonation on social media were also found to be important emerging threats.

---

## Cyber Threat Actors



LARGE-GROUP ACTIVITY: TIME 10 MINUTES

1. Show participants [slide 2.5](#), which outlines the three types of threat actors. Read the following note (guided by the slide):
  - a. Being able to characterize threat actors helps to understand their motivations, sophistication, capabilities and how they operate.
    - i. **Insiders** are people within an organization who have a detailed knowledge of the organization's workings and systems. Insiders then take actions that cause harm and damage to the organization either intentionally (malicious insiders) or unintentionally (accidental or negligent insiders);

- ii. **Hackers** are people who use technical skills to exploit cybersecurity vulnerabilities or engage in cyber attacks to target resources in pursuit of varying goals (e.g. financial rewards or access to confidential and high-value data).
- iii. **Advanced persistent threat actors** are well-resourced, sophisticated and highly capable groups of threat actors who undertake targeted attacks. Some advanced persistent threat actors may be affiliated with or sponsored by governments or political movements.

## 2. Ask the large group:

- a. Who are the most common threat actors that WHRDs and WCSOs might face?
- b. What are their motivations and goals?
- c. What are the possible ways they can be dissuaded or counteracted?

## 3. Volunteers are asked to share their thoughts with the group.

---

# Cybersecurity Goals



LARGE-GROUP ACTIVITY: TIME 10 MINUTES

1. **Ask the large group: *What are your (or your organization's) main goals in protecting against cyber risks?***
  - a. The group brainstorms all of the reasons why protection against risks is important; capture insights on a flipchart.
2. **Show participants [slide 2.6](#), which outlines two distinct models of cybersecurity goals. Read the following note (guided by the slide):**
  - a. The CIA Triad (confidentiality, integrity and availability) is a commonly used model that highlights why organizations engage in cybersecurity. It is focused on the protection of data and information.
    - i. Confidentiality: Protecting information from unauthorized access.
    - ii. Integrity: Data are trustworthy and complete and have not been accidentally altered or modified by an unauthorized user.
    - iii. Availability - Information is accessible to authorized users when it is needed.

- b. As an alternative, a focus on human-centric cybersecurity goals means that our focus changes to thinking about those who use systems and how we can uphold their rights. The goals in this context would be:
  - i. Safety: The quality of feeling protected from harmful online interactions and content;
  - ii. Security: The quality of being safe from cyber risks and in control;
  - iii. Privacy: The quality of being protected from unwanted online interactions and having control over the various dimensions of privacy; and
  - iv. Usability: The ability to satisfactorily and effectively use digital technologies in order to achieve personal and organizational goals.

**3. Ask participants to use a round-robin share technique to summarize their thoughts and feelings about the relationship between gender and cybersecurity:**

- a. Participants each share one word to represent how they feel and one learning from the session.

## SESSION 2.2. CYBER HARMS AND RISK MANAGEMENT



### AIM

To build knowledge of the potential harms caused by cyber risks and to develop sufficient risk management skills to mitigate risks and reduce harms.



### AGENDA

- |   |            |
|---|------------|
| 1. Cybersecurity harms                    | 25 minutes |
| 2. Cyber risk management                  | 45 minutes |
| 3. The cybersecurity ecosystem reflection | 10 minutes |



### TOTAL TIME

80 mins



### RESOURCES

- > PowerPoint slides Module 2
- > Handout 2.1 – Cyber threats and definitions printed as a single sheet
- > Handout 2.2 – Risk Matrix chart
- > Note paper and pens
- > Index cards
- > Flipchart

## Cybersecurity Harms



### SMALL-GROUP ACTIVITY: TIME 25 MINUTES

1. Show participants **slide 2.7**, which outlines the cybersecurity ecosystem and cyber harms. Read the following note (guided by the slide):
  - a. Cyber harms are the impacts of unmitigated cyber risks on cyber resources that increase costs, reduce worth and reduce the capabilities of individuals and organizations to function effectively. Harms are varied, but tend to fall into four categories:
    - i. **Technical:** Loss or corruption of data or loss of access to information and systems (e.g. replacement of devices, software, and systems, lack of access to information and data, lack of trust in technical systems and policies).
    - ii. **Economic:** Loss of finances or costs of recovery (e.g. loss or disrupted income, costs for paying ransoms (extortion), costs recovering systems that have been hacked or compromised, direct theft of money, disrupted work).

- iii. **Psychological:** The experience of distress, insecurity and related mental health problems (e.g. feelings of anxiety, depression, reduced agency, disempowerment, low levels of morale, self-censorship, embarrassment).
- iv. **Social:** The impact on relationships, loss of trust, withdrawal and reputational damage (e.g. withdrawal, damaged relationships, feelings of isolation, damaged personal and organizational reputation).

2. Ask participants to get into small groups of three to five people.
3. Give each group a copy of **Handout 2.1**, 'Cyber Threats and Their Definitions'.
4. Groups decide on five threats to focus on.
5. Give groups 15 minutes to brainstorm each type of threat chosen on a flipchart, addressing the following questions:
  - a. *How might this type of cyber threat cause harm, and what type of harms are likely?*
  - b. *How might this threat cause specific harms to women and girls?*
  - c. *What are some of the ways that these can harms be reduced?*
6. Each group presents to the larger group their thoughts on the type of threats and harms caused.
7. Capture critical insights on a flipchart and summarizes the findings.

**> KEY FACILITATION NOTE**

Techno-centric approaches to cybersecurity often miss the mental and social aspects of harm that are caused by cyber threats. These are particularly important for the work of WHRDs and WCSOs, as cyber threats can be traumatising and even spill into offline contexts to cause advocates and activists physical harm. Therefore, when we empower ourselves to be safe and secure regarding our digital devices and the data that is stored there, we also are protecting our health and well-being.

---

## Cybersecurity Risk Management

---



SMALL-GROUP ACTIVITY: TIME 45 MINUTES

---

1. Show participants [slide 2.8](#), which outlines cybersecurity risk management. Read the following note (guided by the slide):
  - a. Risk management is the process of strategically managing risks in order to achieve goals and objectives and to minimize harms. Representing the potential for harm, risks are considered in terms of their potential negative impacts and their likelihood of happening.
  - b. Risk management helps to prioritize and focus on those risks that are most likely to have negative impacts. Risk management is a continuous and cyclical process of four steps starting with (1) identifying the relevant risks, (2) assessing those risks to understand their impact and likelihood, (3) implementing controls to deal with those risks, and (4) monitoring and reviewing the controls to determine their suitability and effectiveness.
  - c. The first step in risk management is to identify relevant risks. One of the common approaches to do this is through an asset-based threat analysis. This approach helps focus cybersecurity efforts on addressing those threats that are most relevant based on assets owned.
2. Divide participants into groups of three to five people and ask them to select a moderator for their who will facilitate the discussions and note key points of discussion.
  - a. **Step 1. Identify and prioritize assets**
    - i. The groups list all of the digital assets (or resources as per the previous module) that are used in their organization or by themselves as individuals to conduct work or advocacy (e.g. devices, software, systems).
    - ii. The groups select the top three critical assets (note: in an actual analysis, this would be an inventory of all assets).
    - iii. Groups should create a list of associated cyber risks (threats and/or vulnerabilities) for each of the top three critical assets.
    - iv. A maximum of 10 of the identified cyber risks are written onto separate Post-it notes or index cards.
  - b. **Step 2. Assess risks**
    - i. Groups rate each of the 10 threats that were prioritized using the two metrics:
      1. Likelihood: rare, unlikely, possible, likely and certain; and
      2. Impact: insignificant, minor, major and severe.

- ii. The risk matrix (Handout 2.2) is given to groups so that they can categorize their threat cards into the relevant risk rating.
- iii. Once the risk rating is defined, it is written on the Post-it note or index card alongside the risk itself.

c. **Step 3. Control risks**

- i. Each group decides on a plan for addressing the 10 risks. Groups should consider the following:
    - 1. Which risk should be targeted first and how?
    - 2. What risks can be reduced by minimizing their impact as compared to their likelihood?
    - 3. What might be some of the technical as compared to non-technical (human-centric) controls to be put into place?
    - 4. How do gendered issues play into the risk rating and the approach to controlling risks?
- 3. Give the small groups five minutes to present their risks and approaches for addressing them to the larger group. The large group should challenge assumptions and ask questions about each approach.**
- 4. If time permits, prompt participants to consider whether the risks that were identified in this exercise are associated with the gendered focus of their work.**

---

## The Cybersecurity Ecosystem Reflection



LARGE-GROUP ACTIVITY: TIME 10 MINUTES

- 1. Bring the participants through the contents on slide 2.9, the detailed version of the cybersecurity ecosystem figure.**
- 2. Ask everyone to write down their answers to the following questions:**
  - a. *What is the most critical cyber resource for you or your organization to protect?*
  - b. *What do you think is the most pressing cyber threat you or your organization faces?*
  - c. *What is the biggest cyber vulnerability that you or your organization currently has?*
- 3. Have each participant present one of their answers to the large group.**



**4. Briefly summarize the session and reiterate the module's learning objectives in order to address whether they were met during the session.**

- a. **Understand** the cybersecurity domain as comprising not only the technical elements but also the human and social elements from a gender lens.
- b. **Make sense of the cybersecurity landscape for WHRDs and WCSOs** in terms of the associated resources, vulnerabilities, threats, responses and harms.
- c. **Gain familiarity** with the basic terminology and concepts in cybersecurity.
- d. **Understand** risk management processes and be equipped to undertake cybersecurity risk management.
- e. **Have** the basic foundations on which to build further understanding and practice of cybersecurity risk management.
- f. **Understand** how responses and countermeasures fit within larger cybersecurity and risk management practices.



## MODULE 3: SECURING YOUR DATA

### Overview

Data is often a critical resource for anyone's work. The nature of the data that each person or organization stores or accesses varies in sensitivity and requires different approaches when it comes to protecting it. WCSOs and WHRDs typically deal with particularly confidential and personal information as well as highly sensitive organizational data that is used to support everyday operations. This module offers practical strategies for how WCSOs and WHRDs can secure their personal and organizational data, highlights the gendered dimensions of data-related cybersecurity attacks and discusses the gendered considerations of relevant cybersecurity measures.

### AIM AND LEARNING OBJECTIVES

At the end of this course, participants are expected to:

1. **Gain a deeper understanding** of data-related cybersecurity threats, their gender implications and how they unfold with a specific focus on their impacts on WCSOs and WHRDs.
2. **Be familiar** with responses to deal with these common cybersecurity threats.
3. **Be able** to put into practice some of the critical cybersecurity responses.

# SESSION 3.1. DATA ACCESS AND CONTROL



## AIM

To highlight the importance of data protection and to develop skills to identify data-related threats and vulnerabilities.



## AGENDA

- |                                      |            |
|--------------------------------------|------------|
| 1. Protecting your data              | 20 minutes |
| 2. Gendered impacts of a data breach | 20 minutes |
| 3. Access control and permissions    | 20 minutes |
| 4. Managing privacy settings         | 20 minutes |



## TOTAL TIME

80 mins



## RESOURCES

- > PowerPoint slides Module 3
- > Handout 3.1 – Access and permissions walkthrough
- > Note paper and pens
- > Flipchart

## Protecting Your Data



### LARGE-GROUP WORK: TIME 20 MINUTES

1. Read out loud verbatim or adapt the following note to participants:
  - a. *For many organizations, data is the foundation of the work they undertake. Organizations collect and process different types of data that contribute to value creation for their stakeholders and beneficiaries. Data differ in terms of confidentiality and sensitivity; knowing what data you have can help you understand how to protect it and ensure individual and organizational privacy. Being able to identify and categorize different types of data is important, not only as part of the risk management process, but also because it helps organizations identify specific risks and threats.*
2. Ask the group, *What types of data do you store that a threat actor might benefit from accessing?*
3. Collate the types of data on a flipchart.
4. Show participants [slide 3.1](#), which outlines the five main types of data threats. Convey the following points (guided by the slide):

- a. **Data breaches** occur when external attackers gain unauthorized access to data. Data breaches can expose confidential and private data to those who should not have access.
  - b. **Data leakages** reveal data to unauthorized people due to the intentional or unintentional actions of people internal to an organization.
  - c. **Privacy violations** expose personal information to attackers. There are several manifestations of privacy violations, including surveillance and tracking (e.g. through spyware), doxxing, identity or data theft and impersonation.
  - d. **Denial of Service (DOS)** or distributed denial of service (DDoS) attacks deny legitimate users access to systems by overloading the servers with too many requests.
  - e. **Ransomware attacks** involve threat actors accessing data and encrypting it on the organization's systems so that it cannot be accessed, often demanding to be paid a ransom before the attackers will decrypt and make the data available.
- 5. Return to the brainstorm that was captured on the flipchart and ask participants, *Which type of data threat do you think is most likely for the types of data that you have access to and why?***
- 6. If time permits, two additional questions can be prompted for discussion:**
- a. *Have you or your organization experienced any of these threats?*
  - b. *How would you or your organization fare if you fell victim to any of these attacks?*

---

## Gendered Impacts of a Data Breach



SMALL-GROUP ACTIVITY: **TIME 20 MINUTES**

**1. The facilitator reads the case study on slide 3.3:**

a. **'Morally reprehensible': hackers publish abortion data on dark web**

The hackers behind the theft of medical data released sensitive details of customers' medical procedures, including abortions, on the dark web. The file reportedly included a spreadsheet with 303 patients' details alongside billing codes related to pregnancy terminations, including non-viable pregnancy, miscarriage and ectopic pregnancy. During question time on Thursday, minister for cyber security Clare O'Neil described the release of the data as 'morally reprehensible'. "I want to say, particularly to the women whose private health information has been compromised overnight, as the minister for cybersecurity but more importantly, as a woman, this should not have happened, and I know this is a really difficult time," she said. "I want you to know that as a parliament and as a government, we stand with you. You are entitled to keep your health information private and what

has occurred here is morally reprehensible and it is criminal.”<sup>1</sup> Participants make four small groups of three to five people ask them to select a moderator for their group who will facilitate the discussions and note key points for the larger group.

## 2. Groups are given 10 minutes to reflect on the following four questions:

- a. *What are the gendered dynamics of data breaches that were highlighted by this case?*
- b. *What are some of the ways that the online victimization of women (through the data breach) could have impacts on offline life?*
- c. *What could be the effect of having a female Minister of Cybersecurity?*
- d. *How do data breaches affect different genders (including women, men and people with SOGIE)?*

## 3. Guide each group to leads the discussion on one of the four using the key facilitation notes below.

### > KEY FACILITATION NOTES

- > **Question 1:** Data breaches can reveal sensitive information that specifically pertains to women, such as sensitive pregnancy and sexual health data. Also, because of the increased sensitivity of this information, attackers could specifically leverage this towards achieving their attack goals.
- > **Question 2:** In different contexts, there could be social and legal implications of this sensitive health information becoming public. For example, some women may experience social stigmatization associated with the early termination of pregnancy or suffer associated legal consequences. Therefore, online victimization (i.e. data breach) can cascade into offline impacts.
- > **Question 3:** As expressed in the article (“as the minister for cybersecurity but more importantly, as a woman”), the Minister was able to empathize with the women who are going through this terrible experience and whose data was breached. It affords the Minister a deeper understanding of the gendered impacts of the data breach and implies a greater impetus and commitment from officials who are addressing this challenge.

It is important to recognize that women in leadership positions may not necessarily lead to more gender-responsive policies. While women’s leadership is important, it needs to be coupled with broader efforts to advance gender equality and women’s empowerment across social, political and economic spheres.

- > **Question 4:** This case demonstrates how the impacts of online threats are linked with the offline role of different genders in specific sociocultural contexts.

<sup>1</sup> SBS News (2022). “Morally reprehensible: Medibank hackers publish abortion data on dark web”. Accessed at <https://www.sbs.com.au/news/article/we-can-make-di-scount-new-details-on-medibank-ransom-emerge-as-suspected-hackers-release-more-data/acp4ilp36>

---

## Access Control and Permissions

---



SMALL-GROUP ACTIVITY: TIME 20 MINUTES

---

**1. Show participants slide 3.3, which outlines access control and permissions. Convey the following points (guided by the slide):**

- a. Access control refers to who is allowed to access certain data, apps and resources and what measures have been implemented to ensure which users (e.g. individuals, groups or roles) have what permissions (e.g. read, write, delete, execute) to which resources (e.g. files, systems).

The first element of access control is authentication — verifying users' claimed identities. You need to have strong authentication processes in place as a basis for enforcing authorization rules (covered in a later module). The second element of access control is authorization, detailing the permissions that users and software have for different resources.

**2. Ask participants to form two groups based on whether their phone is an Android or iOS device. Each group should work together to ensure that everyone accomplishes each of the following steps on their phones:**

- a. Locate the app permissions settings on your mobile device using the illustrated walkthrough handouts for Android and Apple (see Handout 3.1).
- b. Find the permissions that are allowed (enabled) for the following apps:
  - i. Social media apps, e.g. Facebook, X (formerly Twitter);
  - ii. Email clients, e.g. Gmail, Outlook;
  - iii. Mapping app, e.g. Google Maps;
  - iv. Video app, e.g. YouTube; and
  - v. A game app.
- c. Read through the App Permissions Explained section of the handout. Do all the permissions make sense for the functionality of the app? Can you identify enabled permissions that are out of place (e.g. a game with unjustified access to your location and contacts)?
- d. Note down the types of access that seem questionable or difficult to justify.
- e. Restrict and limit permissions that are out of place.

**3. Participants present and discuss findings as a large group. The facilitator may prompt with the following questions:**

- a. *What was surprising to you about some applications' permissions?*
- b. *Do you think you will check any new application's permissions before installing? Why or why not?*

---

## Managing Privacy Settings



SMALL-GROUP ACTIVITY: **TIME 20 MINUTES**

1. Show participants [slide 3.4](#), which outlines privacy settings. Convey the following points (guided by the slide):
  - a. We are living digital lives that are more intertwined with reality than ever before; if anything is certain, it's that our privacy is at risk because our data is being collected and stored. Our operating systems (e.g. Windows), browsers (e.g. Chrome), social media platforms and applications are all collecting information. You may not realize that your data can be stored or how it could be used by different companies — some of which sell the data they track. To protect yourself, you must understand and restrict your privacy settings.
2. Open or ask participants to open the following link: <https://allaboutcookies.org/how-to-change-privacy-settings>.
3. Ask participants to get out their phones or laptops and to group up with others who are using similar operating systems (e.g. Android or iOS for mobile or Windows or macOS for laptops).
4. Each group should follow the link provided and choose the relevant example. *If unable to connect to the Internet or not sharing a screen, information should be printed and prepared by the facilitator beforehand.*
5. The groups should work together to ensure that everyone is able to check and change the privacy settings on their operating system.
  - a. Note if using a device that is managed by your organization, some settings may not be able to be changed.
6. If time permits, the same process can be duplicated with social media applications by following this link: <https://allaboutcookies.org/twitter-facebook-privacy-settings>

**Note:** Privacy settings are constantly changing and vary based on platforms and OS version; participants may need to search for updated information, particularly for social media platforms that are not listed.
7. Participants present and discuss their findings as a large group. The facilitator may prompt:
  - a. *What are some ways to keep up to date with privacy and data collection across your devices?*
  - b. *Did you already have restrictions in place, and if not, what will you continue to do in the future?*

# SESSION 3.2. ENCRYPTION AND DATA BACKUP



## AIM

To develop an understanding of data security processes and to build data recovery skills.



## AGENDA

- |                             |            |
|-----------------------------|------------|
| 1. Data encryption          | 20 minutes |
| 2. Data and system back-up  | 20 minutes |
| 3. Assessing data strategy  | 30 minutes |
| 4. Data security reflection | 10 minutes |



## TOTAL TIME

80 mins



## RESOURCES

- > PowerPoint slides Module 3
- > Note paper and pens
- > Flipchart

## Data Encryption



### LARGE-GROUP ACTIVITY: TIME 20 MINUTES

1. Show participants **slide 3.5**, which outlines encryption. Read the following note (guided by the slide):
  - a. Encryption is the process of transforming data so that it cannot be read by anyone who does not have the right authorization. Encrypting data before it is stored ensures confidentiality because only people who have access to the decryption key can access and read the data. Most operating systems provide functionality for encryption, and in some, it is turned on by default. There is also an option to use third-party encryption applications to protect data that is stored on computers or in the cloud.
  - b. Zero-knowledge encryption is when only the user has the encryption/decryption key, and the provider does not have the key and cannot access the data.
2. To assist participants' understanding, the facilitator may show the **Encryption and Public Keys** video at <https://www.youtube.com/watch?v=6-JjHa-qLPk>
3. If time permits, ask the large group: *Are you currently using encryption to protect your data, and if so, how? If not, why?*



## Data and System Backup



LARGE-GROUP ACTIVITY: TIME 20 MINUTES

**1. Show participants slide 3.6, which outlines data and systems backup processes. Convey the following points (guided by the slide):**

- a. A backup is a copy of data that can be used in case the primary, active data gets damaged or corrupted. A backup can be made for different types of data, including documents, system files and software applications.
- b. The '3-2-1' backup approach, which provides increased protection against threats to the copies of data, recommends keeping three copies of the data, with two copies on different media and one copy stored off site.
- c. Storing backed-up data on different media ensures protection in case of failure of one of those media.
- d. Storing data off site will help minimize the opportunity for malware and ransomware to corrupt backups and protect data from on-site disasters (e.g. theft, fire).

**2. Show participants slide 3.7, which outlines data and systems backup processes. Convey the following points (details outlined on the slide):**

- a. There are three strategies that you can implement for data backups:
  - i. The full backup strategy involves making copies of all files for every backup session. As per the figure on the slide, this includes a main set of data (on the device being backed up) and a backup (on another server). Each time there is a new backup, all data is copied (blue for the first backup, orange for the second backup and green for the third backup on the slide).
  - ii. A differential backup involves making a combination of full backups and backups of only the data that has changed since the last full backup. As per the figure on the slide, this includes a main set of data (on the device being backed up) and a backup (on another server). Each time there is a new backup, all data that has been added since the last full backup is copied (in the slide, blue is the full data backup at the first step. Orange is new data at the second step. Green is only new data at the third backup).
  - iii. An incremental backup involves making full backups and then backing up only data that has changed since the previous backup operation (on the slide, blue is new data at the first step, orange is new data at the second step, and green is new data at the third step).
  - iv. In choosing a backup strategy, the user needs to consider their personal needs in relation to what types of documents and files they want to secure.
- b. The following are further considerations for implementing effective backup measures:
  - i. **What to backup:** the choice of what to backup (e.g. documents, configurations and settings, applications and software) depends on the anticipated costs and effort of recovery. Data that is difficult to recover should be backed up; data that is easy to reinstall and reconfigure (e.g. some software and systems) or often a lower priority.

- ii. **When to backup:** this depends on how often data within the organization changes and, relatedly, the cost of recreating (or rebuilding or recollecting) lost data.
- iii. **Automating backups:** as far as possible, backups should be automated for improved efficiency.
- iv. **Encrypting backups:** backups should be encrypted (as discussed in the previous section), as they represent confidential organizational data.
- v. **Testing backups:** backups should be regularly tested to ensure that they work and that the data is accessible. Testing is a crucial part of the backup routine because backup operations might introduce errors or corruption due to software glitches or hardware malfunctions.

**3. Show participants slide 3.8, which outlines backups to the cloud. Read the following note (guided by the slide):**

- a. Cloud storage (storing data remotely) can be a solution for backing up data off site, but you should consider factors such as:
  - i. Whether the data is encrypted before being stored in the cloud; using cloud providers that offer zero-knowledge encryption is best;
  - ii. The cost implications of the storage;
  - iii. In some countries, data localization legislation means the data centres must be located in the country; and
  - iv. What are the company's 'privacy credentials' — does it have a privacy-respecting business model, or does it make money from the data it stores? Is it registered in a country with strong privacy laws? Has it been embroiled in privacy violations before?

**4. Show participants slides 3.9 and 3.10 as examples of how to backup data on a computer with the Windows operating system. If time permits (and a volunteer is willing), this can be done on one of the participants' laptops.**

- a. Note that these instructions may change over time; the facilitator is encouraged to test the procedure beforehand to update slide information and screenshots if necessary. Also, the outlines are a guide on how to back up, but it is suggested to not actually engage in this operation during the training session.

---

## Assessing Data Security Strategies



PAIR SHARE ACTIVITY: TIME 30 MINUTES

- 1. Group participants in pairs.
- 2. Show participants slide 3.11 and tell them that they will be presented with three cases and an associated question.

### 3. Present the first case (detailed on slide):

- a. An organization recently learned that it is important to keep multiple copies of files for backup. As a result, they now keep different copies of their data under four different folders on their computer.
- b. Ask, *What are the major weaknesses of this approach?* and give participants two to five minutes to discuss in their pairs and then share their answers with the larger group. The facilitator can use the following guidance to structure an answer:
  - i. Since the data is kept on a single device, if the hard disk fails, the data will be lost. To implement the 3-2-1 strategy, one copy should be on a different medium (e.g. DVD-ROM) and another copy at a different, off-site location.

### 4. Present the second case (detailed on slide):

- a. An organization has recently acquired a Microsoft 365 subscription that allows them to store all of their files in the cloud without having to worry about backups.
- b. Ask, *What are the potential risks and benefits of this approach?* and give participants two to five minutes to discuss in their pairs and then share their answers with the larger group. The facilitator can use the following guidance to structure an answer:
  - i. The pros of this solution are that the cloud storage provider automatically and securely handles the data backup if it's a part of the subscription. The cons of this solution are that if access to the cloud servers is lost (e.g. lack of payment, loss of Internet connectivity), access to backups would be lost. This would not be the case if the organization securely managed their own backups. Also, it must be noted that syncing data on the cloud is not the same as having a full backups. For example, if a file is accidentally deleted (locally or remotely), the file is deleted on all synced drives (therefore, not backed up).

### 5. Present the third case (detailed on slide):

- a. The director of an organization keeps a copy of sensitive organizational files on their personal computer at home and another unencrypted copy on a CD-ROM at their friend's place.
- b. Ask, *What are the potential risks and benefits of this approach?* and give participants two to five minutes to discuss in their pairs and then share their answers with the larger group. The facilitator can use the following guidance to structure an answer:
  - i. The positive of this solution is that it complies with the 3-2-1 strategy; the negative is that the data on the CD-ROM is unencrypted and not securely stored.

### 6. Ask participants to review their own current backup practices. Specifically, ask pairs the following questions:

- a. *Do you back up your data?*
- b. *What data do you back up?*
- c. *Is your backup encrypted?*

- d. *To what extent, if at all, do you or your organization use the 3-2-1 backup strategy?*
  - i. *If you do use this strategy, how do you implement it?*
  - ii. *If you do not, what are the barriers?*
- e. *What are some of the ways that you can improve data backup practices personally and within your organization?*


**7. Ask for volunteers to present poor- and good-practice backup examples to the larger group. The facilitator should then briefly summarize them.**

## Data Security Reflection



LARGE-GROUP ACTIVITY: TIME 10 MINUTES

1. This module provided an overview of data security, the importance of keeping data safe and how to engage in best practices around data protection. Putting controls in place can help reduce susceptibility to many common cyber threats and can mitigate harms caused by them.
2. Ask participants to write down their answers to the following questions:
  - a. *What types of data do you store that a threat actor might benefit from accessing? (Note that this question was asked at the beginning of Module 3, session 1; participants should reflect on how their understanding has changed throughout the module.)*
  - b. *What do you think is the most pressing data cyber threat that you or your organization faces and why?*
  - c. *What is the biggest cyber vulnerability that you or your organization currently have concerning the use, storage and protection of data?*
3. Give participants five minutes to answer these questions as individuals or in pairs or small groups to share with the larger group.
4. Present a summary of the session and reiterate the module’s learning objectives to address whether they were met during the session:
  - a. **Gain a deeper understanding** of data-related cybersecurity threats, their gender implications and how they unfold with a specific focus on their impacts on WCSOs and WHRDs.
  - b. **Be familiar** with responses to deal with these common cybersecurity threats.
  - c. **Be able** to put into practice some of the critical cybersecurity responses.



## MODULE 4: BEING SECURE ONLINE

### Overview

WCSOs and WHRDs rely on the Internet for daily operations, including accessing relevant information and services and communicating with key stakeholders. It is necessary to mitigate the increasing online risks that WCSOs and WHRDs face and to understand the associated gendered dynamics. This module, Being Secure Online, offers practical strategies for individuals and organizations to be secure in their online identities and online communications and highlights the gendered dimensions of cybersecurity threats.

### LEARNING OBJECTIVES

At the end of this course, participants are expected to:

1. **Gain a deeper understanding** of threats against WHRDs and WCSOs that are associated with online accounts, communications and web browsing, their gender implications, and how they unfold.
2. **Be familiar** with methods to deal with these threats.
3. **Be able** to put critical cybersecurity responses into practice.

# SESSION 4.1. ONLINE AUTHENTICATION THREATS



## AIM

To develop an understanding of the importance of protecting online identities and to introduce tools to support best practices.



## AGENDA

- |                                    |            |
|------------------------------------|------------|
| 1. Online authentication           | 15 minutes |
| 2. Password protection             | 20 minutes |
| 3. Password managers and MFA       | 15 minutes |
| 4. Account monitoring and recovery | 30 minutes |



## TOTAL TIME

80 mins



## RESOURCES

- > PowerPoint slides Module 4
- > Note paper and pens
- > Flipchart

## Online Authentication



### LARGE-GROUP ACTIVITY: TIME 15 MINUTES

1. Show participants **slide 4.1**, which outlines online authentication. Convey the following points (guided by the slide):
  - a. Online identities (through accounts and associated credentials) represent who we are in the digital world; for all intents and purposes, the person who can provide valid credentials for an account can assume that identity and act as the owner of that account. This is why individuals and organizations need to implement effective measures to secure their accounts and credentials.
  - b. While account security implies the protection of the accounts that individuals and organizations own and use, at a more general level, account security is about the protection of authentication — the capability to confirm the claimed identity. Confirming a claimed identity can be achieved through the following three key approaches (or a combination of them).
    - i. **‘Something you know’** credentials are a popular example of using something that you know (e.g. a password) to prove the claimed identity. This is used in most online accounts and services.
    - ii. **‘Something you have’** credentials validate identity through a physical item that an individual has. Common examples include access cards or USB keys.

- iii. **'Something you are'** credentials leverage individual physiological attributes such as fingerprints, face or voice to confirm identity. These approaches have become increasingly common for mobile device authentication and access control at physical locations.

**2. Show participants slide 4.2, which outlines different types of authentication threats. Convey the following points (guided by the slide):**

- a. **Account hijacking** is the primary technique through which individuals lose access to their accounts due to their credentials being compromised by attackers. Once an account has been compromised, attackers can launch further attacks, including phishing, posting inappropriate and malicious content and compromising other accounts. Common techniques for compromising account credentials include credential stuffing, where credentials that have been previously compromised (e.g. through a data breach) are used to access other accounts; password spraying, using lists of usernames and common passwords to get access to an account; and brute-forcing, in which all possible combinations of characters are used to try and hack into an account.
- b. **Impersonation** is intentionally assuming an identity, name or image of someone else (or of a business) to deceive, defraud or harm others. This involves deliberately portraying oneself as someone else. Impersonation is driven by many different motivations, ranging from financial gain to personal gratification to malicious intent. The two major forms of impersonation are:
  - i. Online Identity Theft: Impersonating someone online to gain access to their private information or resources or on social media (i.e., by creating fake profiles) to deceive others or cause harm.
  - ii. Spoofing: Pretending to be a trusted entity to extract personal information by manipulating information (e.g. email addresses, websites, domains).

**3. Ask the large group:**

- a. *Have you, your organization, or someone you know ever experienced account hijacking or impersonation?*
- b. *How do you think you or your organization would fare if you fell victim to these types of authentication threats?*

**4. Show participants slide 4.3, which outlines responses to authentication threats. Convey the following points (guided by the slide):**

- a. This module will cover the four key steps to mitigating online account threats:
  - i. Engage strong authentication practices for accounts and devices;
  - ii. Set up account recovery measures;
  - iii. Monitor activity on accounts to detect possible hacks; and
  - iv. Adopt secure networking, secure communications and secure browsing practices.

---

## Password Protection

---



LARGE-GROUP ACTIVITY: TIME 20 MINUTES

---

### 1. Explain that:

- a. The first line of defence for online threats is to maintain strong authentication measures to ensure that your credentials and account access are protected, enabling rightful account owners to have access while keeping attackers at bay. The main way this is achieved is by having strong passwords.

### 2. Show slide 4.4, which includes a list of six example passwords

- b. Each person individually ranks the password from one to six, with one being the best and six being the worst.
- c. As a group, rank the passwords. Start by asking for a consensus on which is the worst and moving along to which is the best.

#### a. Answer Key:

1. !2410#unWCS0@here
2. aomeN2410ChisRn
3. VwXyZ1234?
4. zpYwi
5. 734628
6. December

- ii. Note: Although 'December' seems like it could be stronger than some of the other, shorter passwords, it can easily be cracked through a dictionary attack that uses word lists.

- d. The group debriefs on the characteristics of a strong password.

### 3. Show slide 4.5, which outlines password best practices. Convey the following points (guided by the slide):

- a. Because credentials play a primary role in authentication, adopting secure password practices is the first step that individuals can take to improve their account security. Strong passwords are those that cannot be compromised either by having them guessed or by being accessed by people who shouldn't have access to them (e.g. by writing them down in an unsecured notebook). Therefore, both the complexity of passwords and how they are stored are important factors to consider.



- b. Password length is typically considered an indicator of how long it would take to guess a password by brute force (going through all possible combinations of characters until a suitable one is found). The slide illustrates how the complexity of a password increases as its length increases and as a mix of upper- and lowercase characters, numbers and special symbols are added. Best practices are listed below:
  - i. Passwords include a minimum of 12 characters;
  - ii. Passwords include uppercase, lowercase, numbers and special characters;
  - iii. Avoids common words and phrases (this is to protect against dictionary attacks);
  - iv. Users avoid reusing passwords (this is to protect against credential stuffing, where passwords that have been breached are used to gain access to other accounts);
  - v. Users avoid sharing passwords with anyone;
  - vi. Users do not send passwords over insecure or unencrypted communication channels; and
  - vii. Users change passwords if they suspect a site or password has been compromised.

#### 4. Participants are asked to reflect on the question, *How strong do you think your passwords are?* based on the best practices criteria.

---

## Password Managers and MFAs



LARGE-GROUP ACTIVITY: TIME 20 MINUTES

1. Show [slide 4.6](#), which outlines password management practices. Convey the following points (guided by the slide):
  - a. It is difficult to impossible to both adopt the recommendations for secure password practices and memorize all the passwords. As a result, people tend to write down their passwords (either digitally or on a hard copy) to help them remember passwords. This practice has major weaknesses in that people who have access to the file or paper will immediately have access to all the passwords and the associated accounts.
    - i. **Browser-based password managers.** This option is as strong as your browser and device security. If the browser is compromised, your passwords could be too. Further, if you are using a shared device, anyone with access to that device (and browser account) has access to your passwords. Browser-based password managers are also tied to a specific browser, which makes it difficult to access your passwords from a different browser. If using a browser-based password manager, it is important to use a reputable browser and confirm that it provides the needed functionality. For example, some browsers cannot synchronize saved passwords across devices.

- ii. **Dedicated password managers.** These are applications that make use of zero-knowledge encryption for storing passwords and other sensitive information. There are several password managers that individuals can choose to use, including 1Password, Bitwarden, KeePass, Keeper, LastPass and Proton Pass.

**2. Ask participants: *What are the main ways you remember your passwords? Who uses a password manager?***

**3. Show slide 4.7, which compares different password managers. Convey the following points:**

- a. A range of considerations need to be made when using a password manager, including:
  - i. **Price:** Is it free or paid? What features are associated with each?
  - ii. **Data import and export:** To avoid being locked into a specific product, it is important to be able to export your passwords and other information in a format that is readable by other tools.
  - iii. **Platform and operating system support:** The ability to use the password manager on different platforms (computers, mobile devices and browsers) makes the manager more versatile.
  - iv. **Strong password generation:** Some password managers provide the functionality to securely generate strong passwords that can be used when registering for accounts or updating credentials on existing accounts.
  - v. **Automatic password capture:** The ability to automatically store passwords that are entered on the browser can make the transition to using that manager much smoother.
  - vi. **Auto-fill forms:** A basic password manager function is to automatically fill in credentials on different websites, both on computers and on mobile devices. In addition to convenience, this adds a layer of protection against entering credentials in spoofed websites.
  - vii. **Security features:** Only use password managers that employ strong encryption algorithms. Some password managers offer further security features, such as biometric authentication, automatic lock-out and multi-factor authentication.

**4. If time permits, show the ‘Getting Started with Proton Pass’ video on how to get started with one of the password managers at <https://youtu.be/Nm4DCAjePOM>. To avoid unintentionally implying an endorsement, be clear that this is only an example.**

**5. Show slide 4.8, which outlines multi-factor authentication (MFA). Convey the following points (guided by the slide):**

- a. Another critical way to protect credentials is via MFA. MFA helps to increase security and is prevalent in many systems. For example, to use an automatic teller machine, one typically needs to have both the bank card (see ‘something that you have’ above) and also know the PIN (see ‘something that you know’ above). The most common implementation is two factors being used; hence you may see the common reference “2FA” to refer to two-factor authentication.

- b. Another common type of MFA requires the user to enter their username and password and, subsequently, a one-time password (OTP). An OTP is an authentication token that is generated and meant to be used for authentication only once. OTPs expire after a period of time (from a fraction of a minute to several hours) or after being used, depending on the specific implementation. OTPs can be generated for authentication through text messages, email, hardware and mobile applications.

## 6. Ask participants:

- a. *Do you see any difficulties or barriers in implementing MFA?*
- b. *Do you use MFA? If so, which type do you use? If not, why not?*

## Account monitoring and recovery



LARGE-GROUP ACTIVITY: TIME 30 MINUTES

### 1. Show slide 4.9, which outlines signs that an account has been compromised. Convey the following points (guided by the slide):

- a. In addition to putting in place measures to protect against account compromises, it is also important to detect when an account compromise has occurred. From a resilience perspective, it is important to implement measures to facilitate account recovery of compromised accounts. Some of the signs that an account might have been compromised include:
  - i. Unrecognized login sessions;
  - ii. Password has been changed;
  - iii. Unknown posts or messages from your account;
  - iv. Suspicious activity on your page (especially on social media);
  - v. Email notifications from the server provider; and
  - vi. Not being able to login with valid credentials.
- b. Common account recovery measures include adding security questions and a recovery email address or phone number. Different websites provide varying levels of account activity logging. Regardless, it is important for users to regularly check their account activity to confirm that their accounts have not been compromised. There are also services that individuals can use to check if their credentials have been part of any data breach (outlined subsequently). Once credentials have been in a data breach, individuals should change their passwords immediately to avoid being a victim of account hijacking or credential stuffing.

2. Show [slide 4.10](#), which outlines how to check your login history. Convey the following points (guided by the slide):
  - a. On most social media accounts, you can check the list of devices and locations where your account is being used to see if someone else has used or is using your account. Check any failed login attempts and regularly check your login and session history. If you see any suspicious login activity, change your password immediately. Also, check devices currently logged into your accounts and log out of any inactive sessions.
3. Divide participants into pairs or small groups of three to five and have each pair or group check a social media account.
4. The instructions for finding login information differ depending on the platform being checked and may change when the platform updates. However, platforms tend to follow similar patterns:
  - a. Facebook
    - i. Under “Security,” select “Security and Login.” You will find yourself on the page with a section called “Where you’re logged in.” Facebook will show you the “Active now” status in blue letters.
    - ii. If you want to see more, tap on the blue “See all” option to the right. You’ll see the last active sessions, including the approximate location, type/model of the device, and the most recent login time.
    - iii. If you see a device or location that you do not recognize, tap on the three vertical dots. Then, select “Log out.”
5. Details on other platforms can be found at <https://thenextweb.com/news/how-see-where-youre-logged-in-facebook-twitter-instagram>.
6. Say to participants, *As well as checking your logins, you can also check whether or not your credentials (email, usernames, and passwords) have been compromised in a known data breach.*
  - a. Show [slide 4.11](#), which has QR codes for the following websites:
    - i. Firefox Monitor - <https://monitor.firefox.com>
    - ii. HaveIBeenPwned - <https://haveibeenpwned.com>
7. Have participants visit the above two sites to check whether their credentials have been breached. For participants whose credentials have not been breached, ask them to check a colleague’s or friend’s email.

- 8. Tell participants whose credentials have been breached that they should change their passwords for that (and any other accounts that use the same password) to reduce the likelihood of a credential-stuffing attack.**
  
- 9. Ask participants to reflect on a series of questions and volunteer their thoughts for a group discussion:**
  - b. Did you find any suspicious logins or devices you didn't expect when checking your social media activity?*
  - c. Did you find that your credentials had been breached?*
  - d. Were the findings surprising to you?*
  - e. Overall, how did these activities make you feel?*

# SESSION 4.2. ONLINE BROWSING AND COMMUNICATION THREATS



## AIM

To develop knowledge of secure networking, browsing and communications and to introduce tools to support best practices.



## AGENDA

- |   |            |
|---|------------|
| 1. Secure networking and VPNs               | 10 minutes |
| 2. Phishing                                 | 15 minutes |
| 3. Secure online communication and browsing | 25 minutes |
| 4. Cyber hygiene review                     | 30 minutes |



## TOTAL TIME

80 mins



## RESOURCES

- > PowerPoint slides Module 4
- > Post-it notes or index cards
- > Note paper and pens
- > Flipchart

## Secure networking and VPNs



### LARGE-GROUP ACTIVITY: TIME 10 MINUTES

1. Show **slide 4.12**, which outlines secure networking and VPNs. Convey the following points (guided by the slide):
  - a. Being safe online starts with adopting secure networking practices. Connecting to a network is the first point of risk exposure. For example, connecting to the Internet via public Wi-Fi could expose individuals to privacy risks (e.g. their location could be determined, and their presence online could be detected). It could also reveal identifying information, such as the IP addresses of devices.
  - b. While not all public networks are malicious, individuals should generally avoid connecting to untrusted public Wi-Fi networks when conducting confidential or sensitive activities (including entering usernames and passwords).
  - c. If connecting to a public or unknown Wi-Fi network, there are several measures that can be taken to improve cybersecurity, such as using a **virtual private network (VPN)**.
  - d. A VPN uses encryption to create a secure point-to-point connection between two devices, typically a user device and a VPN server on another computer network. A VPN can be used to secure

communications across the Internet in a way that protects the user's communications and traffic from interception.

- e. Another service to mitigate privacy and anonymity risks is **The Onion Router (TOR)** service, which performs layered encryption of Internet communication and sends it across the Internet through multiple relay nodes such that it is impossible to identify the original sender of the information. It is worth noting, though, that Internet service providers would be able to detect when TOR is being used.
- f. Please note that some countries ban or block VPN and TOR services. Therefore, participants should determine not only the suitability service they are considering but also the legality in their specific context.
- g. The following links can help to clarify different country contexts:
  - i. <https://www.comparitech.com/vpn/where-are-vpns-legal-banned/#5>
  - ii. <https://safetydetectives.com/blog/are-vpns-legal/>
- h. The facilitator may highlight Proton VPN as a possible tool for participants if they are interested and show details for both the free and paid versions at <https://protonvpn.com>. This is not the only VPN; care should be taken to avoid an unintentional endorsement.

**2. If time permits, ask participants, *Does anyone use a VPN? If so, which VPN do you use and why?***

---

## Phishing



INDIVIDUAL AND LARGE-GROUP ACTIVITY: **TIME 15 MINUTES**

1. Direct participants to <https://phishingquiz.withgoogle.com>. This activity can be completed as a group or as individuals. If you do not have access to the Internet, this activity may be skipped and participants can move on to the discussion. Convey the following:
  - a. One of the most common forms of online communication threats is a phishing attack. Phishing is a scam that impersonates a reputable person or organization with the intent to steal credentials or sensitive information. Email is the most common vector for a phishing attack, but depending on the type of phishing scam, the attack may use a text message or even a voice message.
2. Have participants complete the quiz and discuss as a group which answers they got correct and which they got incorrect. Use [slide 4.13](#) to point to some of the known warning signs for phishing.
3. Pose the following questions to the group (notes for answers are included below):

- a. *Phishing is a type of social engineering aimed at manipulating, influencing or deceiving a victim in order to gain control over a computer system or to steal information. Why is this one of the most common cyber threats?*
  - Social engineering exploits human vulnerabilities, which are linked to the nature and complexity of human behaviour. These vulnerabilities also correspond to many positive human traits, such as being trusting, reciprocating, curiosity, etc. This makes it challenging to comprehensively mitigate social engineering attacks. These attacks are also easy to spread widely, and they draw in those who are most likely to believe them. Therefore, threat actors' initial efforts can be minimal. While many people know about and have experienced phishing, they still fall for the threat. Have participants discuss the following:
- b. *What are the challenges to implementing effective phishing mitigation measures? How can we improve our defences?*
  - Increased awareness of social engineering attacks and techniques;
  - Undertaking exercises such as phishing simulations; and
  - Empowering individuals to be responsible for recognising phishing attacks and enabling them to easily get assistance when needed.

## Secure Online Communication and Browsing



SMALL AND LARGE-GROUP ACTIVITY: TIME 25 MINUTES

1. Show **slide 4.14**, which outlines secure online communications. Convey the following points (guided by the slide):
  - a. Just like encryption of data, encrypted messaging converts information to make it unreadable to anyone who does not have an authorized tool to properly decrypt it. Many messaging and communication applications have encryption.
  - b. **End-to-end encryption** involves encrypting messages at the sender's end and only decrypting at the receiver's end. In this case, only the sender and the receiver have the encryption key, and no one — including service providers — can access the secure messages. This contrasts with situations where service providers are able to access messages by encrypting the connection between the sender and the service provider and a separate encryption process between the service provider and the receiver.
  - c. An example of different types of encryption are the two messaging applications provided by Meta: Facebook Messenger and WhatsApp. For Facebook Messenger's current default mode, a message gets encrypted on the user's device using an encryption key that Meta has access to, which allows Meta to decrypt the message to do further processing and analysis. Afterwards, the message is encrypted and forwarded to the receiver. In contrast, WhatsApp provides end-to-end encryption; the sender encrypts the message, which is then sent across the public Internet through Meta's servers to the receiver, who decrypts the message. In this case, only the sender and receiver have the keys to encrypt and decrypt the message. Applications that provide end-to-end encryption include (but are not limited to) FaceTime, iMessage, Signal, Skred, Telegram, WhatsApp and Wickr.



d. Other considerations for secure communications

- i. **Anonymous registrations:** Different communication applications require different pieces of information to register. These could include personally identifiable information such as name, date of birth, telephone number, gender and physical location. This has implications regarding the usability, functionality and security of that application.
- ii. **Vanishing mode:** Some applications provide the functionality to delete or destroy sent messages after a certain period of time. This functionality is sometimes called 'disappearing' or 'self-destructive' messages. For sensitive communication, this feature provides a layer of security that ensures that the message cannot be accessed at a later point — even if attackers gain access to the device.

**2. Divide participants into small groups of three to five people and ask them to select a moderator for their group to capture and give feedback on their discussion. Ask the small groups to spend five to seven minutes brainstorming the following questions on a flipchart:**

- a. *What are some common risks of browsing online?*
- b. *What activities increase or decrease exposure to these risks?*

**3. Each group should briefly present their thoughts to the group at large regarding online browsing risks.**

**4. After the discussion, show slide 4.15, which highlights some best practices, noting that these are not a complete list. Convey the following points (guided by the slide):**

- a. Some of the risks of online browsing include confidentiality risks associated with sensitive data (e.g. financial data or personal data), tracking and surveillance (e.g. by advertising agencies), integrity risks of web content being modified to mislead users, availability risks of denial of service and censorship, and authenticity risks associated with spoofed websites (e.g. as part of a phishing attack). The following measures can address some of these risks:
  - i. Avoid questionable websites. Some types of websites, such as file sharing, adult or freeware websites, are more prone to host malicious content and are riskier.
  - ii. Typing in the address of the website that you want to access instead of clicking links provided via email, as this could be part of a phishing attack.
  - iii. Review and limit the permissions (e.g. access to your microphone, location and camera) that are enabled for your apps and browser (including site-specific permissions).
  - iv. Always use trusted web browsers (the HTTPS protocol confirms the authenticity of websites) and keep your browser and operating system updated.
  - v. Use anonymous browsing modes coupled with secure VPNs, noting that anonymous browsing does not prevent the storage of a user's information and this can be mitigated by a VPN.
  - vi. Most online services are designed to collect personal data and to learn your online behaviour by tracking your visits to different websites; always consider how much of your data you are prepared to give up for a free online service.

5. If time permits, ask participants to reflect on the following questions: *How often do you adhere to the best practices guidance for secure browsing? What are the barriers to engaging in these practices?*

---

## Cyber Resilience Review



SMALL AND LARGE-GROUP ACTIVITY: **TIME 25 MINUTES**

1. Participants get into small groups of three to five people and ask them to select a moderator for their group to capture and provide feedback on their discussion.
2. The groups spend 10 minutes brainstorming all of the potential online risks that they can think of and write these down on separate Post-it notes.
3. Draw two columns on a whiteboard or flipchart labelled “online risks” and “mitigation strategies.”
4. Each group contributes their Post-it notes to the column of online risks, taking turns to discuss the risks they produced and grouping these together into broader categories if possible.
5. Adds broad labels to groups of Post-it notes (similar to the example table below).
6. Each group chooses around three of the online risks and considers potential mitigation strategies for the risks they have chosen.
7. Focusing on their selected risks, each group spends 10 minutes developing a second set of Post-it notes that outline strategies to decrease the likelihood and/or harms of each risk.
8. Each group contributes their Post-it notes to the column of mitigation strategies for their specific risks, discussing what these mean and how to implement the strategy.
9. Debriefs these strategies to produce a list of cyber-resilient practices.

Online Risks	Mitigation Strategies
Privacy violations	<ul style="list-style-type: none"> <li>&gt; Limit private information you share online; any information you share online can be used against you.</li> </ul>
Online abuse	<ul style="list-style-type: none"> <li>&gt; Don't engage abusers or trolls.</li> <li>&gt; Disconnect if necessary.</li> <li>&gt; Block messages and calls.</li> <li>&gt; Seek help and engage the law enforcement and police if necessary.</li> </ul>
Phishing	<ul style="list-style-type: none"> <li>&gt; Learn to detect signs of phishing (e.g. language errors, urgency, inaccuracies).</li> <li>&gt; Verify the sender's email address.</li> <li>&gt; Think before you click — type sensitive URLs directly when possible.</li> <li>&gt; Only open attachments from trusted senders.</li> </ul>
Disinformation Misinformation	<ul style="list-style-type: none"> <li>&gt; Do not trust everything you see online.</li> <li>&gt; Always triangulate news across multiple sources.</li> <li>&gt; Validate the reputation of the news sources you consume.</li> <li>&gt; Equip yourself to better understand and identify disinformation.</li> </ul>
Confidentiality risks	<ul style="list-style-type: none"> <li>&gt; Keep your devices and software up to date.</li> <li>&gt; Only install software from credible sources (e.g. official app stores).</li> <li>&gt; Always dispose of your devices securely, making sure to first delete any confidential data.</li> </ul>

## 10. Highlight the following:

- This module provided an overview of being secure online, the importance of keeping one's identity and communications safe, and how to engage in best practices for being secure online. Putting such measures in place can help to reduce the likelihood and harms caused by many common cyber threats.

## 11. Participants are asked to use a round-robin share technique to summarize their thoughts and feelings about how to protect themselves online.

- Participants each share one word to represent how they feel and one learning from the session;

## 12. Summarize the session and reiterates the module's learning objectives in order to address whether they were met during the session.

- Gain a deeper understanding of threats against WCSOs and WHRDs that are associated with online accounts, communications and web browsing, their gender implications, and how they unfold.
- Be familiar with methods to deal with these threats.
- Be able to put critical cybersecurity responses into practice.

## 13. At the completion of the training programme, the facilitator is strongly encouraged to consider ways of evaluating the overall training to assess whether this met participants' needs. See the introduction for details on how to complete such an valuation.

# HANDOUT 1.1: GENDERED CYBERSECURITY CASE STUDIES

## Case Study 1: Spyware to Monitor Human Rights Defenders

Spyware programs, highly intrusive software applications that are used to track communications, have been deployed in every country in the world. Some of these tools have been designed and marketed to prevent crime and terrorism, but are also used to hack and surveil individuals. Spyware can be used to turn someone's phone into a powerful surveillance tool, enabling an operator to extract text messages (including encrypted messages), contact lists, photos, calendar records, emails, instant messages and location, as well as to turn on microphones and cameras, enabling them to capture live footage and record conversations.

Pegasus is one of the most well-known spyware tools that has been used to target human rights defenders and journalists around the world. An investigation found that 30 individuals in one country in Southeast Asia were infected with Pegasus spyware in the 2020-2021 period following pro-democracy protests. The infections were discovered when users received an alert from their iPhones that indicated that their device might be targeted. The list of infected individuals comprised 24 activists, three academics and three NGO workers. It is thought that the main reason Pegasus was used to target these individuals was to monitor their online activities and gather information about their networks in order to learn more about the protest movements.

# HANDOUT 1.1: GENDERED CYBERSECURITY CASE STUDIES

## Case Study 2: Cyber-bombing

Cyber-bombing is a type of harassment in which an unwanted and uninvited individual or a group interrupts an online meeting or event, often to intentionally disrupt and incite hate. This type of cyberattack is also known as Zoom-bombing or Zoom-raiding, terms that came into common language due to the increasing use of (and security problems with) the Zoom videoconferencing service. These types of cyberattacks can be very difficult to prevent as almost all targeting happens in real-time and is opportunistic, so there is little or no time to prepare. Further, this type of attack is not sensitive to normal protective strategies (such as password protection).

Several events around the world held by women advocates have been subject to cyber-bombing, with reports of events for International Women's Day, LGBTQ support groups and feminist movements all being targeted in similar ways. Gatherings are often disrupted by racist, homophobic, misogynistic, pornographic, obscene and violent language, images and videos. Research by UN Women in Southeast Asia found that multiple events held by WCSOs and WHRDs were cyber-bombed due to disruption from outsiders.

# HANDOUT 1.1: GENDERED CYBERSECURITY CASE STUDIES

## Case Study 3: Impersonation and Fake Social Media Accounts

Impersonation is a distinct type of cyberattack in which fake or impostor websites and social media accounts that copy the identifying brand features of an organization are created and maintained. These types of attacks (which have also been called brand impersonation or brandjacking) are used as a way of tricking people into engaging with fraudulent websites to steal information and/or money. In the case of WCSOs, however, the reason for the imposter accounts is often to undermine and delegitimize the organization's work or message.

Research by UN Women in Southeast Asia found that two WCSOs were being impersonated online. Both discussed how their brand imagery was imitated to fool potential social media followers so that they could spread misinformation or hate content. These accounts are deliberately misleading, create confusion, compromise the legitimacy of organizations' messages, create reputational damage and even harm or threaten. It has been found that these pages become more numerous and increase the intensity of their activities when there are political or contextual issues concerning gender and human rights in the media. As such, they can be seen as organized and deliberate campaigns of misinformation and disinformation against feminist and gender rights advocacy groups.

# HANDOUT 2.1

Term	Definition
<b>Cybermob</b>	A large group of online attackers who threaten, insult and abuse a target – often in an organized or coordinated way.
<b>Cyberstalking</b>	Persistent, unwanted, and/or threatening surveillance, contact and/or pursuit by technological means.
<b>Data Breaches</b>	Any event that exposes confidential, sensitive or protected information.
<b>Deepfake</b>	A fake video or image that was created by artificial intelligence techniques to impersonate an individual.
<b>Disinformation</b>	False information that intentionally misleads, such as propaganda intended to influence elections or foster conflict (see 'misinformation' below).
<b>DOS (denial of service)</b>	An attack that disrupts a network or service by overwhelming it with excessive traffic.
<b>Doxxing</b>	Private or identifying information is distributed about a person on the Internet without their permission.
<b>Hacking</b>	Unauthorized access to or control over computer network security systems for an illicit purpose.
<b>Hate Speech</b>	Abusive or threatening speech targeting individuals or groups based on attributes such as race, religion, sexual orientation or ethnicity.
<b>Honey trapping</b>	Luring individuals into compromising situations to gather information for blackmail or exploitation.
<b>Identity theft</b>	Unauthorized use of personal information for fraudulent purposes.
<b>Malicious tagging</b>	Associating someone online with negative labels or false accusations to damage their reputation.
<b>Malware</b>	Any program or file that is intentionally harmful (i.e. malicious) to a computer, network or server.

Term	Definition
<b>Misinformation</b>	Incorrect or misleading information, which, in contrast to disinformation, is not spread to knowingly deceive its recipient (see 'disinformation' above).
<b>Non-consensual intimate image abuse</b>	The use or sharing of intimate or sexual imagery to objectify, exploit, humiliate or harass.
<b>Online harassment</b>	Repeated conduct that threatens, scares or abuses someone through degrading, offensive or insulting comments and images.
<b>Online scams</b>	Deceptive schemes on the Internet aimed at tricking individuals into providing money or personal information.
<b>Phishing</b>	Malicious emails that are designed to trick people into falling for a scam, divulging sensitive information or taking another action against their or their organization's interests.
<b>Ransomware</b>	A type of malware that is designed to block access to a computer system or files until a condition is met (often a sum of money to be paid).
<b>Sextortion</b>	A type of blackmail in which money, sex acts or explicit images are demanded in exchange for not exposing intimate images or private information.
<b>Shadow-banning</b>	Restricting a user's visibility or reach on a platform without their knowledge.
<b>Shallowfake</b>	A manipulated image made in editing software, such as attaching someone's face to someone else's body.
<b>Social engineering</b>	Manipulating individuals to disclose confidential information through psychological manipulation.
<b>Spoofing/fabrication</b>	Faking the origin of communication or data to deceive recipients.
<b>Spyware</b>	A type of malware that is designed to enter a device, gather data and forward it to a third party without consent.
<b>Trolling</b>	Deliberately provoking or harassing others online to incite emotional reactions.

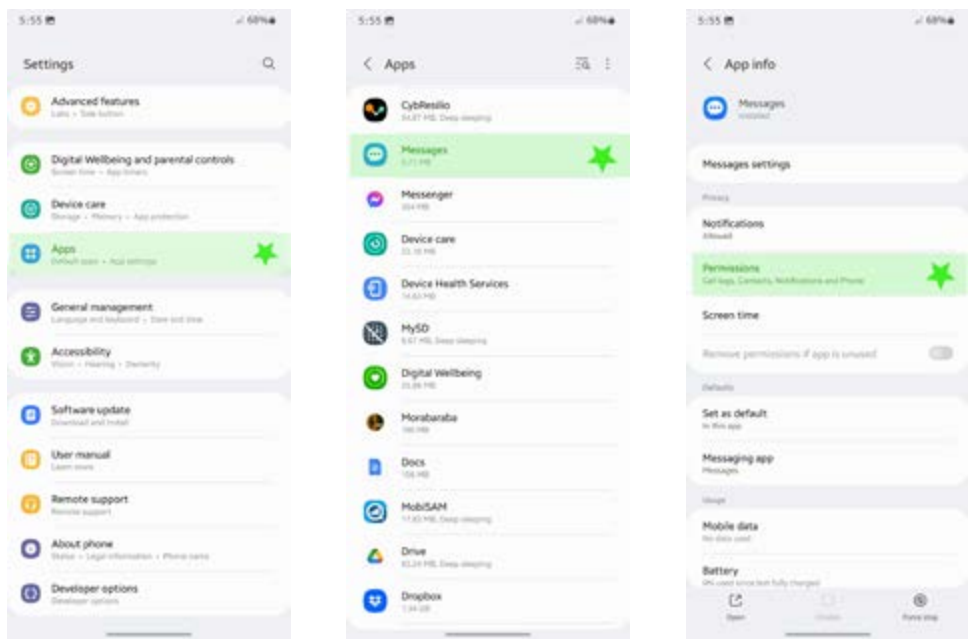


# HANDOUT 2.2: ACTIVITY 2.4 RISK RATING MATRIX

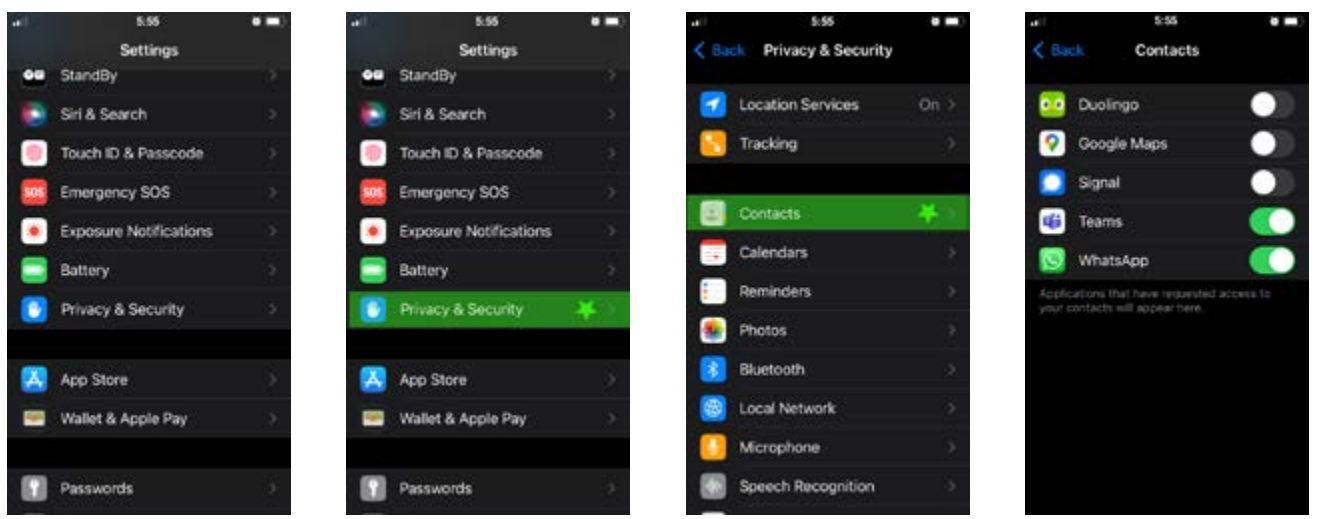
		Impact			
		Insignificant	Minor	Major	Severe
Likelihood	Certain	Medium	High	Extreme	Extreme
	Likely	Low	Medium	High	Extreme
	Unlikely	Low	Low	Medium	High
	Rare	Low	Low	Medium	High

# HANDOUT 3.1: ILLUSTRATED WALKTHROUGH: ACCESS CONTROL ON DIFFERENT PLATFORMS

## ON ANDROID



## ON APPLE



### APP PERMISSIONS EXPLAINED.

The following are common app permissions and the data that they give apps access to. While these are specific for Android, similar permission will apply for Apple and Windows devices.

- > **Body Sensors** — allows access to your health data and step count from paired heart-rate monitors, fitness trackers and other sensors.
- > **Calendar** — allows apps to read, create, edit or delete your calendar events.
- > **Call logs** — Apps with this permission can read and write phone call logs.
- > **Camera** — taking photos, recording footage and streaming video.
- > **Contacts** — read, create or edit your contact list, as well as access the list of all accounts used on your device.
- > **Files and media** — access to your files, media, photos and anything else stored in your phone's memory.
- > **Location** — access your location using GPS for high accuracy and cellular data and Wi-Fi for approximate accuracy. In more recent versions of Android, you can also choose to share your approximate location. This can come in handy for weather apps that don't need a precise location to work correctly.
- > **Microphone** — used for recording audio and video.
- > **Nearby devices** — whether an app can find, connect to and determine the position of other nearby devices.
- > **Notifications** — allows an app to send notifications to your phone's home screen.
- > **Phone** — access your phone number and network info. Required for making calls and VoIP, voicemail, call redirect and editing call logs.
- > **Physical activity** — access your physical activity logs, such as step count and exercise info.
- > **SMS** — read, receive and send MMS and SMS messages.

(Source: [androidauthority.com](http://androidauthority.com))



Ministry of Gender Equality  
and Family



Australian Government



The United Nations University Institute in Macau (UNU Macau) is a United Nations global think tank conducting research and training on digital technologies for sustainable development, encouraging data-driven and evidence-based actions and policies to achieve the Sustainable Development Goals.

#### **UN University Macau**

Casa Silva Mendes, Estrada do Engenheiro Trigo No.4  
Macau SAR, China

[www.unu.edu/macau](http://www.unu.edu/macau)

[www.twitter.com/UNUMACAU](https://www.twitter.com/UNUMACAU)

[www.facebook.com/unumacau](https://www.facebook.com/unumacau)

[weibo.com/u/2698789630](https://weibo.com/u/2698789630)



UN Women is the UN organization dedicated to gender equality and the empowerment of women. A global champion for women and girls, UN Women was established to accelerate progress on meeting their needs worldwide. UN Women supports UN Member States as they set global standards for achieving gender equality, and works with governments and civil society to design laws, policies, programmes and services needed to ensure that the standards are effectively implemented and truly benefit women and girls worldwide.

#### **UN Women Regional Office for Asia and the Pacific**

UN Building, Rajadamnern Nok Avenue  
Bangkok 10200, Thailand

[gps.asiapacific@unwomen.org](mailto:gps.asiapacific@unwomen.org)

[www.asiapacific.unwomen.org](http://www.asiapacific.unwomen.org)

[www.facebook.com/unwomenasia](https://www.facebook.com/unwomenasia)

[www.twitter.com/unwomenasia](https://www.twitter.com/unwomenasia)

[www.youtube.com/unwomenasiapacific](https://www.youtube.com/unwomenasiapacific)

[www.flickr.com/unwomenasiapacific](https://www.flickr.com/unwomenasiapacific)