Gender and Cybersecurity Training Course

Professional Development Training Course Outline

Category	Gender Studies	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s hyper-connected digital world, understanding the intersection of gender and cybersecurity is critical. Cybersecurity threats disproportionately affect women and marginalized groups, highlighting the urgent need for inclusive, gender-responsive approaches to digital safety. Gender and Cybersecurity Training Course leverages cutting-edge knowledge in cybersecurity, gender equality, and digital ethics to empower participants with actionable skills, frameworks, and strategies. Participants will explore the latest cybersecurity threats, gendered cyber risks, digital inclusion, and policy frameworks, ensuring organizations and communities are both secure and equitable.

By integrating practical case studies, interactive sessions, and evidence-based methodologies, this course equips participants to design, implement, and evaluate cybersecurity initiatives with a gender lens. Emphasis is placed on building resilient digital infrastructures, promoting safe online environments, and fostering leadership in cybersecurity advocacy. The course is designed to strengthen organizational capacities, enhance policy understanding, and foster innovation at the intersection of technology, security, and gender inclusion.

Programme Curriculum

Gender and Cybersecurity Training Course

Introduction

In today’s hyper-connected digital world, understanding the intersection of gender and cybersecurity is critical. Cybersecurity threats disproportionately affect women and marginalized groups, highlighting the urgent need for inclusive, gender-responsive approaches to digital safety. Gender and Cybersecurity Training Course leverages cutting-edge knowledge in cybersecurity, gender equality, and digital ethics to empower participants with actionable skills, frameworks, and strategies. Participants will explore the latest cybersecurity threats, gendered cyber risks, digital inclusion, and policy frameworks, ensuring organizations and communities are both secure

and equitable.

By integrating practical case studies, interactive sessions, and evidence-based methodologies, this course equips participants to design, implement, and evaluate cybersecurity initiatives with a gender lens. Emphasis is placed on building resilient digital infrastructures, promoting safe online environments, and fostering leadership in cybersecurity advocacy. The course is designed to strengthen organizational capacities, enhance policy understanding, and foster innovation at the intersection of technology, security, and gender inclusion.

Course Duration

10 days

Course Objectives

1. Understand gendered dimensions of cybersecurity risks and threats
2. Analyze online harassment, cyberbullying, and digital gender-based violence
3. Apply gender-sensitive approaches to cybersecurity policies and frameworks
4. Strengthen digital literacy and secure online practices for women and marginalized groups
5. Develop gender-inclusive cybersecurity strategies for organizations
6. Examine AI, IoT, and emerging technologies through a gender lens
7. Assess cybercrime trends affecting vulnerable populations
8. Promote ethical digital behavior and responsible technology use
9. Design interventions to reduce digital gender gaps
10. Implement cybersecurity awareness campaigns targeting gender equity
11. Integrate global and regional policy perspectives on cybersecurity and gender
12. Build resilience against phishing, malware, and social engineering attacks
13. Foster leadership in gender-responsive digital security and innovation

Target Audience

1. Cybersecurity professionals and analysts
2. Gender equality and social inclusion practitioners
3. Policy makers and regulators in digital security
4. ICT educators and trainers
5. NGO and community leaders focused on women’s rights
6. Digital rights and online safety advocates
7. Human resources and organizational leaders
8. Students and researchers in technology and gender studies

Course Modules

Module 1: Introduction to Gender and Cybersecurity

- Gender and digital ecosystems
- Overview of cybersecurity threats
- Digital gender divides and inclusion challenges
- Case study: Gendered cyberattacks in developing countries
- Mapping cyber risk exposure by gender

Module 2: Cybercrime and Gender-Based Violence

- Online harassment and abuse

- Cyberstalking and doxxing
- Digital GBV reporting mechanisms
- Case study: Women activists targeted online
- Mitigation strategies for organizations

Module 3: Digital Literacy and Safe Practices

- Password hygiene and multi-factor authentication
- Securing personal devices and data
- Online privacy tools and practices
- Case study: Social media safety for female entrepreneurs
- Digital safety checklists

Module 4: Cybersecurity Policy and Gender Inclusion

- Global cybersecurity frameworks
- Gender-responsive policy design
- Regulatory compliance and ethics
- Case study: EU GDPR and women's digital rights
- Organizational policy audits

Module 5: Social Engineering and Phishing Threats

- Understanding social engineering tactics
- Gender-targeted phishing campaigns
- Detecting and responding to attacks
- Case study: Phishing attacks on female executives
- Practical threat simulation exercises

Module 6: Emerging Tech and Gender Implications

- AI bias and gendered algorithms
- IoT security and inclusivity
- Blockchain and digital identity
- Case study: Algorithmic discrimination in hiring platforms
- Tech assessment for gender equity

Module 7: Organizational Cybersecurity Strategies

- Gender-sensitive risk assessments
- Security governance frameworks
- Employee training and awareness
- Case study: Gender-inclusive cybersecurity policies in corporates
- Implementation roadmap templates

Module 8: Incident Response and Crisis Management

- Cyber incident protocols
- Gendered impact assessment
- Crisis communication strategies
- Case study: Response to online harassment of journalists
- Simulation exercises for rapid response

Module 9: Data Privacy and Protection

- Data privacy fundamentals
- Gender-sensitive data handling
- Compliance with local and international standards
- Case study: Protecting women’s health data in digital platforms
- Hands-on privacy audits

Module 10: Ethical Hacking and Gender Awareness

- Penetration testing basics
- Identifying vulnerabilities with gender lens
- Reporting findings responsibly
- Case study: Ethical hacking for NGO networks
- Practical lab exercises

Module 11: Advocacy and Digital Rights

- Online advocacy strategies
- Campaigns against digital harassment
- Leveraging tech for social impact
- Case study: #MeToo campaigns and digital safety
- Toolkit for digital rights advocacy

Module 12: Leadership in Cybersecurity

- Building inclusive cybersecurity teams
- Mentorship and capacity development
- Strategic decision-making
- Case study: Women leaders in cybersecurity
- Leadership exercises and simulations

Module 13: Risk Assessment Tools and Techniques

- Cyber risk frameworks
- Gendered threat mapping
- Tools for vulnerability assessment
- Case study: Risk assessment in educational institutions
- Hands-on assessment exercises

Module 14: Monitoring, Evaluation, and Reporting

- KPIs for cybersecurity initiatives
- Gender impact metrics
- Reporting frameworks and dashboards
- Case study: NGO cybersecurity monitoring system
- Data collection and visualization exercises

Module 15: Capstone Project and Case Study Analysis

- Integrating course learnings
- Group-based project work

- Case study presentations and peer review
- Action plan for gender-responsive cybersecurity
- Expert feedback and certification

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com