



# CYBERWOMEN



INSTITUTE FOR  
WAR & PEACE REPORTING

I W P R

## Appendix

## Appendix

**INSTITUTE FOR  
WAR & PEACE REPORTING**



© 2019– Institute For War And Peace Reporting

<https://iwpr.net/>



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) license.

<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

# Contents

<b>1 IWPR's Digital Security and Capacity Tool (DISC)</b>	<b>5</b>
Internal document with Scores . . . . .	5
<b>2 Example training agendas</b>	<b>13</b>
Example Agendas for 1-Day to 1.5-Day Workshops . . . . .	14
1.5-Day Introductory Workshop on Risk Assessment . . . . .	14
1-Day Awareness Training for WHRDs Dealing with Online Harassment . . . . .	15
1-Day Risk Assessment Training for WHRDs Dealing with Online Harassment . . . . .	17
Example Agendas for 3-Day Workshops . . . . .	18
3-Day Introductory-Level Training . . . . .	18
3-Day Intermediate-Level Training . . . . .	20
3-Day Advanced-Level Training . . . . .	22
<b>3 Resources</b>	<b>25</b>
Coding rights <sup>1</sup> . . . . .	25
Cuida tu info <sup>2</sup> . . . . .	25
Derechos Digitales <sup>3</sup> . . . . .	26

---

<sup>1</sup><https://codingrights.org>

<sup>2</sup><https://cuidatuinfo.org>

<sup>3</sup><https://derechosdigitales.org>

Feminist Internet <sup>4</sup>	26
Gender Sec wiki   Tactical Tech <sup>5</sup>	26
Karisma Foundation <sup>6</sup>	26
Me and My Shadow <sup>7</sup>	27
PRISM Break <sup>8</sup>	27
Red en defensa de los derechos digitales <sup>9</sup>	27
Security in a box <sup>10</sup>	27
Surveillance self-defense <sup>11</sup>	27
Take back the tech <sup>12</sup>	28
Tem boi na linha   is There an Ox in Your Line? <sup>13</sup>	28
Protection of Human Rights Defenders <sup>14</sup>	28
Donestech <sup>15</sup>	28
No fear <sup>16</sup>	28
La violencia en línea es violencia (video) <sup>17</sup>	29
Quick tips for spaces <sup>18</sup>	29
Level Up <sup>19</sup>	29

---

<sup>4</sup><https://feministinternet.org>

<sup>5</sup><https://gendersec.tacticaltech.org>

<sup>6</sup><https://karisma.org.co>

<sup>7</sup><https://myshadow.org>

<sup>8</sup><https://prism-break.org>

<sup>9</sup><https://r3d.mx>

<sup>10</sup><https://securityinabox.org>

<sup>11</sup><https://ssd.eff.org>

<sup>12</sup><https://takebackthetech.net>

<sup>13</sup><https://temboinalinha.org>

<sup>14</sup><http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos>

<sup>15</sup><http://donestech.net>

<sup>16</sup><http://sinmiedo.com.co>

<sup>17</sup><https://vimeo.com/207361788>

<sup>18</sup><https://cyber-women.com/en/downloads/quick-tips-gender-sensitive-learning-spaces-digital-security.pdf>

<sup>19</sup><https://level-up.cc/>

# IWPR's Digital Security and Capacity Tool (DISC)

- **Objective(s):** To gauge participants' existing digital security skill level, while also providing qualitative information on strengths and areas for improvement at a more granular, practice-specific level. disc tool is also a useful way to track their learning and comprehension progress.
- **Format:** Appendix
- **Needed materials:**
  - Copies of the DISC questionnaire

## Internal document with Scores

To Be Completed at Baseline and every six months, or at end of Training Period, as appropriate.

Below you will find a series of questions that will allow your trainer to both understand the level of digital security practices within your organization, as well as to monitor any progress that it made thanks to the training you will or have received. The results are purely for monitoring and evaluation

purposes and will only be shared anonymously within IWPR and with the donors supporting this project.

Country .....

At your organization:

**1. The operating system and software I use to work have been updated: (please circle)**

- Never (0 points)
- In the last 6 months (1 point)
- Within last 30 days (4 points)
- Within last 15 days (5 points)
- More than 6 months ago (0 points)
- We have the newest system installed on this computer (5 points)
- They are being updated at this moment (3 points)
- I don't know that information (0 points)

**2. ¿Do you backup your data through an external hard-drive or a cloud service: (please circle)**

- Never (0 points)
- More than a year ago (0 points)
- In the last year (1 point)
- In the last 6 months (2 points)
- Within last 60 days (3 points)
- Within last 30 days (4 points)
- The data has been backed up within the last 14 days (5 points)
- I don't know that information (0 points)

**3. Are your hard drive or cloud service encrypted?**

- Yes, both are encrypted (5 points)
- No (0 points)
- Only one of them is encrypted (3 points)
- I don't know that information (0 points)

- 
- If you answered affirmatively, which encryption tool do you use?

.....

**4. The computer I use for work has original licensed software (for example Microsoft Windows, Microsoft Office, Adobe Photoshop, Adobe Illustrator, Corel Draw, Antivirus) or open source software programs (Open office, Scribus).**

- Every program is pirated (0 points)
- Some programs are pirated (1 point)
- Most programs are licensed originals (2 points)
- All programs are licensed and original (5 points)
- Most programs are open source (2 points)
- All programs are open source (5 points)
- I am not sure (0 points)

**5. Anti-virus programs are loaded on the computer and the mobile phone that I use to work, are up to date and run each time the equipment is turned on.**

- Yes, computer and mobile phone (5 points)
- Only on my computer (3 points)
- Only on my mobile phone (3 points)
- I don't have anti-virus programs (0 points)
- I don't know if I have an antivirus program on all my devices (0 points)
- If affirmative, which antivirus do you have on your computer?

.....

- If affirmative, which antivirus do you have on your phone?

.....

**6. I have locked my office computer screen/cellphone with a password for the screen lock.**

- Yes (5 points)



- No (0 points)
- Only one of those devices has a password (2 points)

**7. The Wi-Fi network where I work has a different password from the one that the internet service provider gave me, and it meets the standards for a strong password (Criteria: 1. includes at least 25 characters and, 2. includes both letters and numbers, and 3. Includes special characters, and 4. includes both lowercase and capital letters).**

- Yes - password changed and meets at least two of the criteria for strong passwords (5 points)
- No - service provider password was maintained (0 points)
- Partially - only one of the criteria for passwords mentioned above has been applied (3 points)
- Partially- the password was changed but none of the criteria for passwords were applied (1 point)

**8. About the use of public Wi-Fi in hotels, airports or cafés**

- I never use public Wi-Fi in hotels, airports or cafés unless I connect through a virtual private network (VPN) service. (5 points)
- I sometimes use public Wi-Fi in hotels, airports or cafés without connecting through a VPN service. (2 points)
- I always use public Wi-Fi in hotels, airports or cafés without a VPN service. (0 points)

**9. About the back up of my work documents, I use file encryption tools for saving documents in my laptop**

- Yes (5 points)
- No (0 points)
- Only for some documents (3 points)
- If you answered yes, which file encryption tool do you use?

.....

**10. Regarding the text via email or SMS between the members of your organization.**

- 
- I always use encryption for email, SMS or chats to transmit sensitive data (5 points)
  - I usually use encryption for email, SMS or chats to transmit sensitive data (3 points)
  - I rarely use encryption for email, SMS or chats to transmit sensitive data (2 points)
  - I never use encryption for email, SMS or chats to transmit sensitive data (0 points)

**11. I share my passwords with (please circle all that apply):**

- Intimate partner (0 points)
- Siblings and/or parents (0 points)
- Best friend (0 points)
- Work colleagues (0 points)
- No one (5 points)

**12. Secure passwords have at least 25 characters (letters, numbers, special characters, small and capital). Do not use words from the dictionary, birthdays or any personal information. All my passwords meet these standards identified above to ensure a strong password.**

- Yes (5 points)
- No (0 points)
- Only some of them (3 points)

**13. I have different passwords for each of my devices and accounts (computer, phone, email, social media, bank etc)**

- Yes (5 points)
- No (0 points)
- I have a few different passwords that I use, but sometimes repeat (1 point)
- Some of my passwords are set by default by my organization/office/provider of service (3 points)

**14. I have made a strategic decision about how to manage my social media identities for my private, work/activism accounts based on my level of risk.**

(For example using false/different identities and accounts for activism/work, or openly using my real name, photo and identity if I don't feel under threat ...)

- Yes - I have considered it and feel secure with my current management of online identities (5 points)
- No - I haven't thought about it (0 points)
- Partially- I consider it may make sense to create different or more anonymous online identities but haven't made the changes yet (2 points)
- Partially - I have considered my online identities and made the changes, but I am still not sure if the setup is secure (4 points)
- My situation means that it makes more sense for me to use my own name and real identity in all my social media accounts (5 points)

**15. I store my passwords in a password protected secure digital keychain**

- Yes (5 points)
- No (0 points)
- Only some accounts (3 points)
- I don't know what that is (0 points)
- Where is the key chain stored and in what format?

**16. When you are browsing do you always navigate with HTTPS?**

- Yes (5 points)
- No (0 points)
- What is that? (0 points)
- I always check it but it is not always possible to navigate with HTTPS (3 points)

**17. About your personal social media accounts.**

- All my posts on social media are public (0 points)
- I don't know who can see my posts on social media (0 points)
- I choose specific settings for each post (4 points)

- 
- I adjust the settings to control who can see which information on my social media accounts (5 points)
  - I don't know how to set admin controls on any of my social media accounts (0 points)

**18. click on links or open attachments in emails when: (please circle the dates closest to clicking)**

- They seem to contain important or urgent information (0 points)
- I know the sender, but unexpected email (ex. Emotional Partners, old friends) (1 point)
- They come from my trusted network (2 point)
- I expected them (3 points)
- I know and verified the sender (5 points)

**19. I use secure chats and secure online voice communications tools (VOIP) for my communications.**

- Yes (5 points)
- No (0 points)
- Sometimes (2 points)
- I don't know what this is (0 points)
- Which secure tools do you use?

.....

**20. I use power regulators to protect my important electronic devices from electrical surges:**

- Yes (5 points)
- No (0 points)
- Only at my office (2 points)
- Only at home (2 points)
- Only for some devices (2 points)

**Add up the points and record them on the Organizational Scorecard. .... points/ 100 points**



# Example training agendas

- **Format:** Appendix

Although we are aware that the final content of a training session will be based on the diagnosis each trainer does of the group they will work with and we invite each trainer to adjust this session to better meeting the needs of the group, we do suggest a few options for what we think could be regular scenarios of trainings.

The example agendas below are organized by length (in days), and then by participant skill level. Other planning parameters will of course inform the ultimate design of your training; however, time is almost always the most critical:

How much time you have available ultimately determines how much content you can cover in a single workshop; this is furthermore determined by the collective skill level of the participants.

You're more likely to know how many hours or days are available to work with a group before knowing other factors, such as the venue, the number of participants, or their collective skill level.

## Example Agendas for 1-Day to 1.5-Day Workshops

### 1.5-Day Introductory Workshop on Risk Assessment

#### Approximate Time Required: 10 hours

This training agenda was planned for a scenario involving a 1.5 day introductory digital security workshop, with a group of WHRDs or a women's collective, oriented primarily around general risk assessment. Ideally, the outcome of this workshop is that women participants can more easily identify their perceived risks, and can more clearly articulate their digital security needs.

This agenda includes sessions on basic digital security, self-care practices and techniques for documenting and responding to abuse or threats. For this scenario, a follow-up strategy would need to be crafted by the trainer to address the results of participants' risk assessment(s).

1. Exercise: The rules of the game<sup>1</sup> (Trust-building exercises<sup>2</sup>)
2. Exercise: Defenders bingo<sup>3</sup> (Trust-building exercises<sup>4</sup>)
3. Session: Personal perceptions of security<sup>5</sup> (Rethinking our relationship with technology<sup>6</sup>)
4. Exercise: Who do you trust?<sup>7</sup> (Trust-building exercises<sup>8</sup>)
5. Session: Your rights, your technology<sup>9</sup> (Rethinking our relationship with technology<sup>10</sup>)

---

<sup>1</sup><https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/>

<sup>2</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>3</sup><https://cyber-women.com/en/trust-building-exercises/defenders-bingo/>

<sup>4</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>5</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/>

<sup>6</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/>

<sup>7</sup><https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/>

<sup>8</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>9</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/your-rights-your-technology/>

<sup>10</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/>

- 
6. Exercise: Gender-based risk model<sup>11</sup> (Determining the best solution<sup>12</sup>)
  7. Exercise: Building feminist self-care<sup>13</sup> (Self-care<sup>14</sup>)
  8. Session: Building stronger passwords<sup>15</sup> (Digital security basics 1<sup>16</sup>)
  9. Session: How to secure your computer<sup>17</sup> (Digital security basics 1<sup>18</sup>)
  10. Session: Safe browsing<sup>19</sup> (Digital security basics 1<sup>20</sup>)
  11. Session: Privacy<sup>21</sup> (Privacy<sup>22</sup>)
  12. Session: Mobile phones 1<sup>23</sup> (Safer mobiles<sup>24</sup>)
  13. Session: Let's start a documentation journal<sup>25</sup> (Online violence against women<sup>26</sup>)
  14. Exercise: Feminist flowers<sup>27</sup> (Closing and review exercises<sup>28</sup>)

## 1-Day Awareness Training for WHRDs Dealing with Online Harassment

### Approximate Time Required: 5 hours

This training agenda was planned for a scenario involving a 1 day introductory digital security workshop with WHRDs who have just begun to deal with incidents of online harassment. Ideally, the outcome of this workshop

---

<sup>11</sup><https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/>

<sup>12</sup><https://cyber-women.com/en/determining-the-best-solution/>

<sup>13</sup><https://cyber-women.com/en/self-care/building-feminist-self-care/>

<sup>14</sup><https://cyber-women.com/en/self-care/>

<sup>15</sup><https://cyber-women.com/en/digital-security-basics-1/building-stronger-passwords/>

<sup>16</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>17</sup><https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/>

<sup>18</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>19</sup><https://cyber-women.com/en/digital-security-basics-1/safe-browsing/>

<sup>20</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>21</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>22</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>23</sup><https://cyber-women.com/en/safer-mobiles/mobile-phones-1/>

<sup>24</sup><https://cyber-women.com/en/safer-mobiles/>

<sup>25</sup><https://cyber-women.com/en/online-violence-against-women/lets-start-a-documentation-journal/>

<sup>26</sup><https://cyber-women.com/en/online-violence-against-women/>

<sup>27</sup><https://cyber-women.com/en/closing-and-review-exercises/feminist-flowers/>

<sup>28</sup><https://cyber-women.com/en/closing-and-review-exercises/>



is that women participants can more clearly articulate their digital security needs, and can more quickly identify warning signs or patterns of online gender-based violence.

This agenda includes sessions about defining safety and security on a personal level, basic digital security practices and recognizing patterns of abuse and harassment.

1. Exercise: The rules of the game<sup>29</sup> (Trust-building exercises<sup>30</sup>)
2. Exercise: Tricky candy<sup>31</sup> (Trust-building exercises<sup>32</sup>)
3. Session: Personal perceptions of security<sup>33</sup> (Rethinking our relationship with technology<sup>34</sup>)
4. Session: Building stronger passwords<sup>35</sup> (Digital security basics 1<sup>36</sup>)
5. Exercise: Symbolic violence<sup>37</sup> (Online violence against women<sup>38</sup>)
6. Exercise: Time to watch!<sup>39</sup> (Sexting<sup>40</sup>)
7. Session: Sexting<sup>41</sup> (Sexting<sup>42</sup>)
8. Exercise: Our Reflection<sup>43</sup> (Self-care<sup>44</sup>)

---

<sup>29</sup><https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/>

<sup>30</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>31</sup><https://cyber-women.com/en/trust-building-exercises/tricky-candy/>

<sup>32</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>33</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/>

<sup>34</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/>

<sup>35</sup><https://cyber-women.com/en/digital-security-basics-1/building-stronger-passwords/>

<sup>36</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>37</sup><https://cyber-women.com/en/online-violence-against-women/symbolic-violence/>

<sup>38</sup><https://cyber-women.com/en/online-violence-against-women/>

<sup>39</sup><https://cyber-women.com/en/sexting/time-to-watch/>

<sup>40</sup><https://cyber-women.com/en/sexting/sexting/>

<sup>41</sup><https://cyber-women.com/en/sexting/sexting/>

<sup>42</sup><https://cyber-women.com/en/sexting/sexting/>

<sup>43</sup><https://cyber-women.com/en/self-care/our-reflection/>

<sup>44</sup><https://cyber-women.com/en/self-care/>

---

## 1-Day Risk Assessment Training for WHRDs Dealing with Online Harassment

### Approximate Time Required: 7 hours

This training agenda was planned for a scenario involving a 1 day workshop with WHRDs who are dealing with ongoing incidents of online harassment, and who need support developing security plans and response strategies. Ideally, the outcome of this workshop is that women participants can more clearly articulate their digital security needs, feel more in control of their personal risk environment, and are able to develop a responsive, context-specific security plan and protocol for themselves.

This agenda includes sessions about defining safety and security on a personal level, basic digital security practices and gender-based risk assessment.

1. Exercise: The rules of the game<sup>45</sup> (Trust-building exercises<sup>46</sup>)
2. Session: Personal perceptions of security<sup>47</sup> (Rethinking our relationship with technology<sup>48</sup>)
3. Exercise: Who do you trust?<sup>49</sup> (Trust-building exercises<sup>50</sup>)
4. Exercise: Gender-based risk model<sup>51</sup> (Determining the best solution<sup>52</sup>)
5. Session: Privacy<sup>53</sup> (Privacy<sup>54</sup>)
6. Exercise: Doxxing the Troll<sup>55</sup> (Online violence against women<sup>56</sup>)

---

<sup>45</sup><https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/>

<sup>46</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>47</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/>

<sup>48</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/>

<sup>49</sup><https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/>

<sup>50</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>51</sup><https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/>

<sup>52</sup><https://cyber-women.com/en/determining-the-best-solution/>

<sup>53</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>54</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>55</sup><https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/>

<sup>56</sup><https://cyber-women.com/en/online-violence-against-women/>

7. Exercise: Building feminist self-care<sup>57</sup> (Self-care<sup>58</sup>)

## Example Agendas for 3-Day Workshops

### 3-Day Introductory-Level Training

#### Approximate Time Required: 15 hours

This training agenda is designed for a 3-day long workshop with beginner-level WHRDs who have not yet had a great deal of (or any) prior exposure to digital security practices. Introducing basic digital security and risk assessment practices, with an explicit parallel emphasis on self-care strategies, this training agenda would be appropriate for either an organizationally-focused workshop or a workshop for a mixed group of WHRDs from different collectives or countries within the same region.

Furthermore, this agenda will prepare the group for an intermediate level follow-up training (see 3-Day Intermediate-Level Training example below); however, it can also be used for a standalone workshop.

1. Exercise: The rules of the game<sup>59</sup> (Trust-building exercises<sup>60</sup>)
2. Exercise: Defenders bingo<sup>61</sup> (Trust-building exercises<sup>62</sup>)
3. Session: Personal perceptions of security<sup>63</sup> (Rethinking our relationship with technology<sup>64</sup>)
4. Exercise: Who do you trust?<sup>65</sup> (Trust-building exercises<sup>66</sup>)

---

<sup>57</sup><https://cyber-women.com/en/self-care/building-feminist-self-care/>

<sup>58</sup><https://cyber-women.com/en/self-care/>

<sup>59</sup><https://cyber-women.com/en/trust-building-exercises/the-rules-of-the-game/>

<sup>60</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>61</sup><https://cyber-women.com/en/trust-building-exercises/defenders-bingo/>

<sup>62</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>63</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/>

<sup>64</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/>

<sup>65</sup><https://cyber-women.com/en/trust-building-exercises/who-do-you-trust/>

<sup>66</sup><https://cyber-women.com/en/trust-building-exercises/>

- 
5. Session: Your rights, your technology<sup>67</sup> (Rethinking our relationship with technology<sup>68</sup>)
  6. Session: How does the internet work?<sup>69</sup> (Digital security basics 1<sup>70</sup>)
  7. Exercise: Feminist flowers<sup>71</sup> (Closing and review exercises<sup>72</sup>)
  8. Exercise: Gender-based risk model<sup>73</sup> (Determining the best solution<sup>74</sup>)
  9. Exercise: The act of NO<sup>75</sup> (Self-Care<sup>76</sup>)
  10. Session: Building stronger passwords<sup>77</sup> (Digital security basics 1<sup>78</sup>)
  11. Session: Safe browsing<sup>79</sup> (Digital security basics 1<sup>80</sup>)
  12. Session: Malware and viruses<sup>81</sup> (Digital security basics 1<sup>82</sup>)
  13. Exercise: Building feminist self-care<sup>83</sup> (Self-care<sup>84</sup>)
  14. Session: How to secure your computer<sup>85</sup> (Digital security basics 1<sup>86</sup>)
  15. Session: What does your metadata say about you?<sup>87</sup> (Safe online advocacy<sup>88</sup>)

---

<sup>67</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/your-rights-your-technology/>

<sup>68</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/>

<sup>69</sup><https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/>

<sup>70</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>71</sup><https://cyber-women.com/en/closing-and-review-exercises/feminist-flowers/>

<sup>72</sup><https://cyber-women.com/en/closing-and-review-exercises/>

<sup>73</sup><https://cyber-women.com/en/determining-the-best-solution/gender-based-risk-model/>

<sup>74</sup><https://cyber-women.com/en/determining-the-best-solution/>

<sup>75</sup><https://cyber-women.com/en/self-care/the-act-of-no/>

<sup>76</sup><https://cyber-women.com/en/self-care/>

<sup>77</sup><https://cyber-women.com/en/digital-security-basics-1/building-stronger-passwords/>

<sup>78</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>79</sup><https://cyber-women.com/en/digital-security-basics-1/safe-browsing/>

<sup>80</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>81</sup><https://cyber-women.com/en/digital-security-basics-1/malware-and-viruses/>

<sup>82</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>83</sup><https://cyber-women.com/en/self-care/building-feminist-self-care/>

<sup>84</sup><https://cyber-women.com/en/self-care/>

<sup>85</sup><https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/>

<sup>86</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>87</sup><https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/>

<sup>88</sup><https://cyber-women.com/en/safe-online-advocacy/>

16. Exercise: Marco Polo<sup>89</sup> (Safer Mobiles<sup>90</sup>)
17. Session: Mobile phones 1<sup>91</sup> (Safer Mobiles<sup>92</sup>)
18. Session: Networked publics<sup>93</sup> (Privacy<sup>94</sup>)
19. Session: Privacy<sup>95</sup> (Privacy<sup>96</sup>)
20. Session: Let's start a documentation journal!<sup>97</sup> (Online violence against women<sup>98</sup>)

### 3-Day Intermediate-Level Training

#### Approximate Time Required: 15 hours

This training agenda is designed for a 3-day long workshop with WHRDs who have already had a more introductory level training (see 3-Day Intermediate-Level Training example above) and is intended to be offered as a follow-up. It is considerably more technical in nature than the introductory-level agenda, focusing on practical applications of digital security concepts as well as critical thinking skills for informed decision making on tool use. It also goes more into depth on topics such as women and technology, privacy, encryption and anonymity.

If working with participants from the same organization, this training will also provide them with strategic approaches to begin sharing their knowledge with others at their organization, including designing organization security plans and protocols.

---

<sup>89</sup><https://cyber-women.com/en/safer-mobiles/marco-polo/>

<sup>90</sup><https://cyber-women.com/en/safer-mobiles/>

<sup>91</sup><https://cyber-women.com/en/safer-mobiles/mobile-phones-1/>

<sup>92</sup><https://cyber-women.com/en/safer-mobiles/>

<sup>93</sup><https://cyber-women.com/en/privacy/networked-publics/>

<sup>94</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>95</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>96</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>97</sup><https://cyber-women.com/en/online-violence-against-women/lets-start-a-documentation-journal/>

<sup>98</sup><https://cyber-women.com/en/online-violence-against-women/>

- 
1. Exercise: Tricky candy<sup>99</sup> (Trust-building exercises<sup>100</sup>)
  2. Exercise: I decide<sup>101</sup> (Determining the best solution<sup>102</sup>)
  3. Session: Her-story of technology<sup>103</sup> (Rethinking our relationship with technology<sup>104</sup>)
  4. Exercise: Ask me anything!<sup>105</sup> (Privacy<sup>106</sup>)
  5. Session: Apps and online platforms: friend or foe?<sup>107</sup> (Privacy<sup>108</sup>)
  6. Session: Safe online campaigning<sup>109</sup> (Safe online advocacy<sup>110</sup>)
  7. Session: Mobile phones 2<sup>111</sup> (Digital security basics 1<sup>112</sup>)
  8. Session: Introduction to encryption<sup>113</sup> (Encryption<sup>114</sup>)
  9. Session: Encrypted communication<sup>115</sup> (Encryption<sup>116</sup>)
  10. Exercise: The cauldron<sup>117</sup> (Closing and review exercises<sup>118</sup>)
  11. Session: Storage and encryption<sup>119</sup> (Digital security basics 2<sup>120</sup>)
  12. Exercise: Secret friend<sup>121</sup> (Anonymity<sup>122</sup>)

---

<sup>99</sup><https://cyber-women.com/en/trust-building-exercises/tricky-candy/>

<sup>100</sup><https://cyber-women.com/en/trust-building-exercises/>

<sup>101</sup><https://cyber-women.com/en/determining-the-best-solution/i-decide/>

<sup>102</sup><https://cyber-women.com/en/determining-the-best-solution/>

<sup>103</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/herstory-of-technology/>

<sup>104</sup><https://cyber-women.com/en/rethinking-our-relationship-with-technology/>

<sup>105</sup><https://cyber-women.com/en/privacy/ask-me-anything/>

<sup>106</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>107</sup><https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/>

<sup>108</sup><https://cyber-women.com/en/privacy/privacy/>

<sup>109</sup><https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/>

<sup>110</sup><https://cyber-women.com/en/safe-online-advocacy/>

<sup>111</sup><https://cyber-women.com/en/safer-mobiles/mobile-phones-2/>

<sup>112</sup><https://cyber-women.com/en/digital-security-basics-1/>

<sup>113</sup><https://cyber-women.com/en/encryption/introduction-to-encryption/>

<sup>114</sup><https://cyber-women.com/en/encryption/>

<sup>115</sup><https://cyber-women.com/en/encryption/encrypted-communication/>

<sup>116</sup><https://cyber-women.com/en/encryption/>

<sup>117</sup><https://cyber-women.com/en/closing-and-review-exercises/the-cauldron/>

<sup>118</sup><https://cyber-women.com/en/closing-and-review-exercises/>

<sup>119</sup><https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/>

<sup>120</sup><https://cyber-women.com/en/digital-security-basics-2/>

<sup>121</sup><https://cyber-women.com/en/anonymity/secret-friend/>

<sup>122</sup><https://cyber-women.com/en/anonymity/anonymity/>

13. Session: Anonymity<sup>123</sup> (Anonymity<sup>124</sup>)
14. Session: Digital security decisions<sup>125</sup> (Determining the best solution<sup>126</sup>)
15. Session: Organizational security plans and protocols<sup>127</sup> (Planning ahead<sup>128</sup>)
16. Exercise: Love Letter to Myself<sup>129</sup> (Self-care<sup>130</sup>)

### 3-Day Advanced-Level Training

#### Approximate Time Required: 12 hours

This training agenda is designed for a 3-day long workshop with WHRDs who have already progressed through introductory and intermediate-level trainings (see prior examples) and are ready for more advanced-level experience.

This workshop – more tactical in nature than the previous trainings - focuses less on leveraging conceptual knowledge into development of practices for specific tools, and more on real world scenario-based applications of critical thinking and decision making skills (which also allows you, as the trainer, to more comprehensively assess the overall progress of the group).

1. Exercise: Charades<sup>131</sup> (Closing and review exercises<sup>132</sup>)
2. Session: Safer websites<sup>133</sup> (Safe online advocacy<sup>134</sup>)

---

<sup>123</sup><https://cyber-women.com/en/anonymity/anonymity/>

<sup>124</sup><https://cyber-women.com/en/anonymity/anonymity/>

<sup>125</sup><https://cyber-women.com/en/determining-the-best-solution/digital-security-decisions/>

<sup>126</sup><https://cyber-women.com/en/determining-the-best-solution/>

<sup>127</sup><https://cyber-women.com/en/planning-ahead/organizational-security-plans-and-protocols/>

<sup>128</sup><https://cyber-women.com/en/planning-ahead/>

<sup>129</sup><https://cyber-women.com/en/self-care/love-letter-to-myself/>

<sup>130</sup><https://cyber-women.com/en/self-care/>

<sup>131</sup><https://cyber-women.com/en/closing-and-review-exercises/charades/>

<sup>132</sup><https://cyber-women.com/en/closing-and-review-exercises/>

<sup>133</sup><https://cyber-women.com/en/safe-online-advocacy/safer-websites/>

<sup>134</sup><https://cyber-women.com/en/safe-online-advocacy/>

- 
3. Exercise: More online identities!<sup>135</sup> (Anonymity<sup>136</sup>)
  4. Session: Let's reset!<sup>137</sup> (Digital security basics 2<sup>138</sup>)
  5. Exercise: Doxxing the troll<sup>139</sup> (Online violence against women<sup>140</sup>)
  6. Session: Digital security plans and protocols: post-training replication<sup>141</sup> (Planning ahead<sup>142</sup>)
  7. Exercise: The loving touch<sup>143</sup> (Self-care<sup>144</sup>)
  8. Exercise: DigiSec rally<sup>145</sup> (Closing and review exercises<sup>146</sup>)

---

<sup>135</sup><https://cyber-women.com/en/anonymity/more-online-identities/>

<sup>136</sup><https://cyber-women.com/en/anonymity/anonymity/>

<sup>137</sup><https://cyber-women.com/en/digital-security-basics-2/lets-reset/>

<sup>138</sup><https://cyber-women.com/en/digital-security-basics-2/>

<sup>139</sup><https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/>

<sup>140</sup><https://cyber-women.com/en/online-violence-against-women/>

<sup>141</sup><https://cyber-women.com/en/planning-ahead/digital-security-plans-and-protocols-post-training-replication/>

<sup>142</sup><https://cyber-women.com/en/planning-ahead/>

<sup>143</sup><https://cyber-women.com/en/self-care/the-loving-touch/>

<sup>144</sup><https://cyber-women.com/en/self-care/>

<sup>145</sup><https://cyber-women.com/en/closing-and-review-exercises/digisec-rally/>

<sup>146</sup><https://cyber-women.com/en/closing-and-review-exercises/>





# Resources

## **Coding rights<sup>1</sup>**

Brazilian-born women lead Think-and-Do tank that aims to advance in the enforcement of Human Rights in the digital world by integrating usages and understandings of technology into policy making processes.

## **Cuida tu info<sup>2</sup>**

Security of information and communication.

---

<sup>1</sup><https://codingrights.org>

<sup>2</sup><https://cuidatuinfo.org>

## **Derechos Digitales<sup>3</sup>**

Latin American independent organization and non-profit founded in 2005 and whose main objective is the development, defense and promotion of human rights in the digital environment in the region.

## **Feminist Internet<sup>4</sup>**

Works towards empowering more women and queer persons – in all our diversities – to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy.

## **Gender Sec wiki | Tactical Tech<sup>5</sup>**

This manual is a community-built resource for our growing community of women and trans\* activists, human rights defenders and technologists.

## **Karisma Foundation<sup>6</sup>**

A civil society organization dedicated to supporting and spreading the good use of technologies in digital environments.

---

<sup>3</sup><https://derechosdigitales.org>

<sup>4</sup><https://feministinternet.org>

<sup>5</sup><https://gendersec.tacticaltech.org>

<sup>6</sup><https://karisma.org.co>

---

## **Me and My Shadow<sup>7</sup>**

Tactical Tech's Me and My Shadow project helps you control your data traces, see how you're being tracked, and learn more about the data industry.

## **PRISM Break<sup>8</sup>**

Opt out of global data surveillance programs like PRISM, XKeyscore and Tempora.

## **Red en defensa de los derechos digitales<sup>9</sup>**

Mexican organization dedicated to the defense of human rights in the digital environment.

## **Security in a box<sup>10</sup>**

If you're new to digital security, the Tactics Guides cover the basic principles, including advice on how to use social networking platforms and mobile phones more safely.

## **Surveillance self-defense<sup>11</sup>**

Tips, tools and how-tos for safer online communications.

---

<sup>7</sup><https://myshadow.org>

<sup>8</sup><https://prism-break.org>

<sup>9</sup><https://r3d.mx>

<sup>10</sup><https://securityinabox.org>

<sup>11</sup><https://ssd.eff.org>

## **Take back the tech<sup>12</sup>**

Take Back The Tech! is a call to everyone, especially women and girls, to take control of technology to end violence against women.

## **Tem boi na linha | is There an Ox in Your Line?<sup>13</sup>**

Practical guide to combat online surveillance.

## **Protection of Human Rights Defenders<sup>14</sup>**

Protection, security and self-care for human rights defenders.

## **Donestech<sup>15</sup>**

An investigation that arises from the desire to elucidate certain questions to transform research into a reservoir of useful knowledge for people concerned about gender inequalities and, also, for people oriented to social and political transformation.

## **No fear<sup>16</sup>**

To the streets without fear, tools against repression.

---

<sup>12</sup><https://takebackthetech.net>

<sup>13</sup><https://temboinalinha.org>

<sup>14</sup><http://consorciooaxaca.org.mx/proteccion-a-defensoras-de-derechos-humanos>

<sup>15</sup><http://donestech.net>

<sup>16</sup><http://sinmiedo.com.co>

---

## **La violencia en línea es violencia (video)**<sup>17</sup>

Online violence is violence

## **Quick tips for spaces**<sup>18</sup>

Quick tips for facilitating gender-sensitive learning spaces on digital security. A guide created by IWPR and Social Tic, with content by Indira Cornelio, Dhaniella Falk and Alma Ugarte.

## **Level Up**<sup>19</sup>

Resources for the global digital safety training community.

---

<sup>17</sup><https://vimeo.com/207361788>

<sup>18</sup><https://cyber-women.com/en/downloads/quick-tips-gender-sensitive-learning-spaces-digital-security.pdf>

<sup>19</sup><https://level-up.cc/>