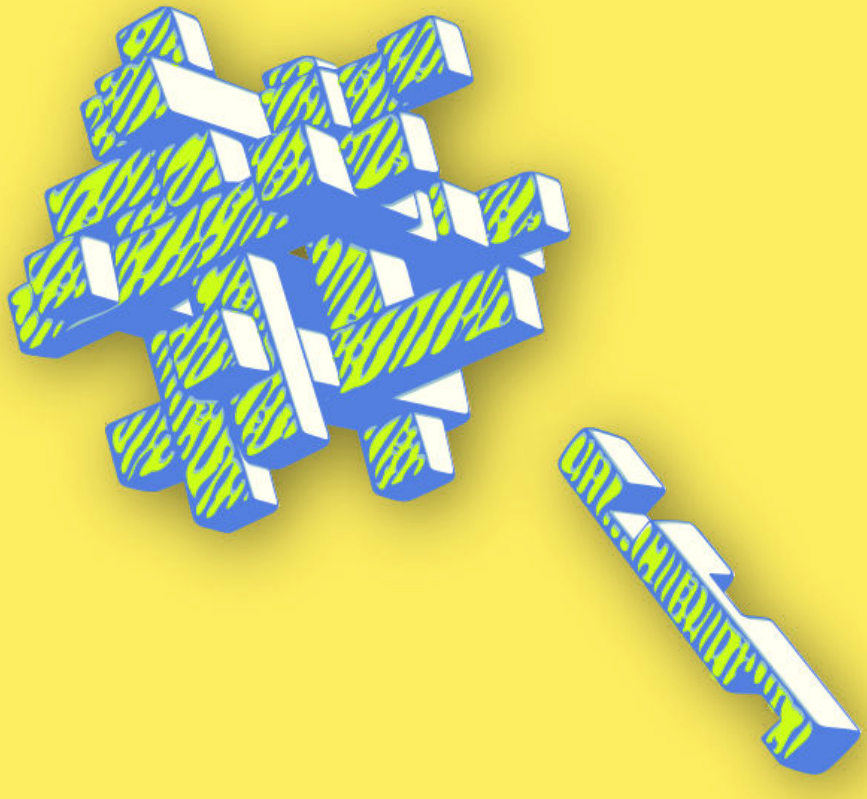
CYBERWOMEN



Encryption

Encrypted communication

https://iwpr.net/

Contents

Encrypted communication

- **Objective(s):** To convey to participants the importance and utility of encrypting communications and providing relevant tools.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Introduction to encryption[1]
- **Related sessions/exercises:**
  - Introduction to encryption[2]
  - Privacy[3]
  - Safe online campaigning[4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup

[1] https://cyber-women.com/en/encryption/introduction-to-encryption/
[2] https://cyber-women.com/en/encryption/introduction-to-encryption/
[3] https://cyber-women.com/en/privacy/privacy/
[4] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/

Leading the session

1. Start the session by sharing relevant examples of situations where encrypted communications could be useful, taking time to explain how encryption works. Demonstrate some example screenshots a GPG-encrypted email to illustrate roughly what messages and emails look like while encrypted, and highlight common implementations of encryption – in particular, HTTPS, end-to-end encryption and GPG/PGP encryption.
2. Focus the discussion now specifically on tools that permit encrypted communications: Signal for calls and messages, meet.jitsi for video calls and Tutanota or GPG & Thunderbird for emails are good examples to share.
3. Explain the security benefits of these tools to the group, primarily how they enable users to limit others' access to their communications; then discuss situations where the security of a user's data could still be compromised, even while using encrypted communication. Ask participants – How could the contents of a GPG encrypted email be compromised by keylogging or screen-capturing malware? What if a user's private GPG key was accessed by an adversary – how could they use it to gain access to their data?
4. If time allows, participants should have the opportunity for hands-on practice with at least one of the tools mentioned above in Step 2. Although there may not be enough time to set the group up with GPG/PGP for email, you may choose to demonstrate an HTTPS protected video call using meet.jitsi, or have participants install Signal on their phones to practice sending one another encrypted messages, or to exchange encrypted phone calls.

References

- https://ssd.eff.org/en/module/how-use-signal-android
- https://ssd.eff.org/en/module/how-use-signal-ios