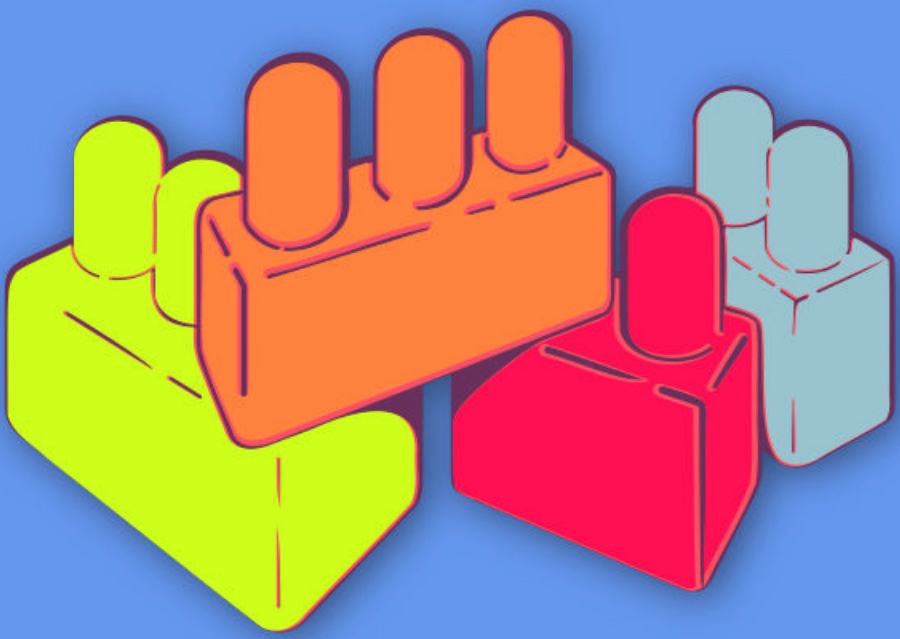
CYBERWOMEN



Digital security basics 2

Storage and encryption

https://iwpr.net/

Contents

Storage and encryption

- **Objective(s):** To reinforce the importance of regularly backing up data to participants, and discuss how they can prevent unauthorized manipulation or access to their information..
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Introduction to encryption[1]
  - How to secure your computer[2]
- **Related sessions/exercises:**
  - Privacy[3]
  - Safe online campaigning[4]
  - Introduction to encryption[5]

[1] https://cyber-women.com/en/encryption/introduction-to-encryption/
[2] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/
[3] https://cyber-women.com/en/privacy/privacy/
[4] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/
[5] https://cyber-women.com/en/encryption/introduction-to-encryption/

  - How to secure your computer[6]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Printed copies of the Backup Format Template (see below)
  - USB drives or other type of storage media (for each participant)
- **Recommendations:** This session will have participants using either veracrypt or mackeeper (depending on their operating system) to practice encryption of data backups and storage media – to save time, consider having participants download either of these ahead of time. in general, and especially for beginners, it is not advisable for participants to perform a full-disk encrypt of their computer hard drives just yet – rather, they should test out veracrypt or mackeeper on external storage media (such as a usb drive) using dummy files that they have prepared specifically for this session. you don't want to run the risk of a participant accidentally losing access to any data during the training!

Leading the session

Part 1 – Data Backups and Planning

1. Ask participants - How often do they backup their files? Share examples of best practices related to data backup, such as keeping the backup in a safe place that is separate from their computer, backing up their information on a frequent, regular basis and - depending on the information that is being backed up - to consider also encrypting the hard drive or storage media where data will be stored.
2. Share with participants the backup format template below, and have them start filling it in individually. Explain to the group that this is a useful way of creating a personal data backup policy – they can refer to

[6] https://cyber-women.com/en/digital-security-basics-1/how-to-secure-your-computer/

this after the training, as a useful resource for keeping track of where their data is stored and how often that data should be backed up.

Backup Format Template

- Type of information
- Importance/Value
- How often it is produced or changed?
- How often must it be backed up?

Part 2 – Storage and Backup Encryption

3. Now that participants have filled out the backup format template, ask them to review the types of information (and their respective importance or value) on their lists again – as they do so, have them consider what might happen if that information were to fall into the hands of an adversary, or if they were to lose that information entirely. What kind of impact would this have on them personally or on their organization?
4. Now, introduce the concept of encryption to the group – explain that they likely encounter encryption quite often in their daily routines, as it is used in different ways across different tools and platforms. You can share, for instance, that HTTPS is itself a form of encryption for data "in transit" (data enroute from point A to point

    B) whereas in this session, you will be discussing encryption for data "at rest" (data that is being stored in one location).

5. Remind participants about how they were asked to download either Veracrypt or MacKeeper onto their computers. Give participants time to install and test out these tools, using external storage media (such as USB drives) and dummy files that they have prepared specifically for this session. Especially for beginner level participants, it is not advisable to do a full-disk encrypt of a computer hard drive just yet - you don't want to run the risk of a participant accidentally losing access to any of their data during the training!

References

- https://securityinabox.org/en/guide/veracrypt/windows/
- https://securityinabox.org/en/guide/veracrypt/mac
- https://securityinabox.org/en/guide/veracrypt/linux