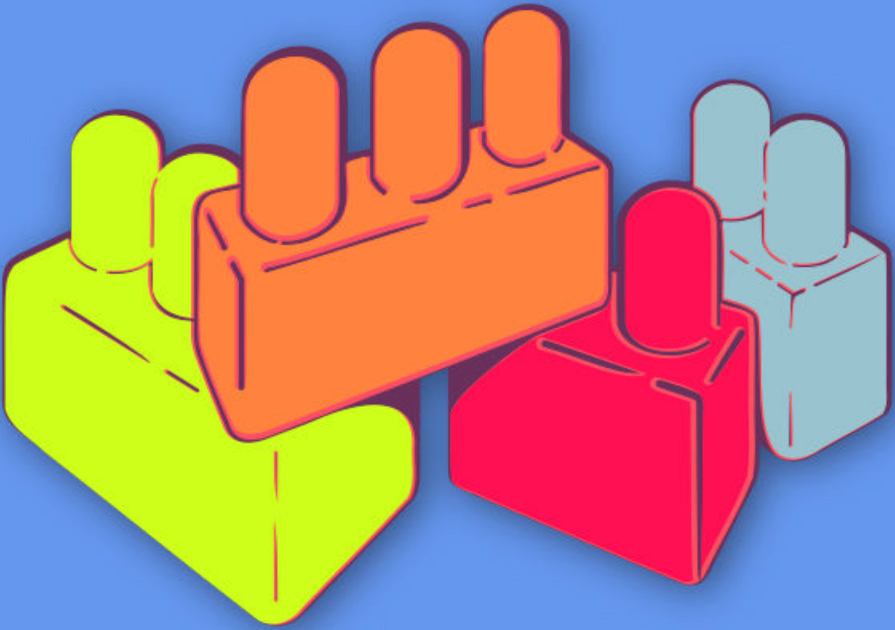
CYBERWOMEN



Digital security basics 2

Digital security basics 2

INSTITUTE FOR
WAR & PEACE REPORTING
IWPR

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

Let’s reset!

- **Objective(s):** To reinforce the idea that “tools and technology don’t have magic superpowers over us!” here, you will lead participants through an empowering process of “starting from scratch” by resetting their devices and getting a fresh start.
- **Length:** 90 minutes
- **Format:** Session
- **Skill level:** Intermediate
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Introduction to encryption[1]
  - Storage and encryption[2]
- **Related sessions/exercises:**
  - Personal perceptions of security[3]
  - Malware and viruses[4]

[1] https://cyber-women.com/en/encryption/introduction-to-encryption/

[2] https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/

[3] https://cyber-women.com/en/rethinking-our-relationship-with-technology/personal-perceptions-of-security/

[4] https://cyber-women.com/en/digital-security-basics-1/malware-and-viruses/

  - Privacy[5]
  - More online identities![6]
  - Storage and encryption[7]
- **Needed materials:**
  - Slides (with key points included below)
  - USB drives live-configured with bootable Tails and Ubuntu OS
- **Recommendations:** Consider bringing each participant a live usb for them to keep; otherwise, have a computer prepared for participants to practice on (or two, if demonstrating both tails and ubuntu) - even if the activity is just intended to run tails or ubuntu from a live usb instead of installing it, some participants not feel comfortable using their own computer to test these out. this can also be readily adapted into a session for any fearless activist women in your training who want to try changing operating systems completely, from mac os or windows to a linux distribution such as ubuntu.

Leading the session

Part 1 – Dispelling the Myth

1. Begin by explaining the goal of this session: to re-affirm the power that humans have over technology, dispelling the notion that digital devices have "superpowers" over their users. If you did the session Personal Perceptions of Security with participants, you can remind them of the following from the closing affirmations:

   > Tools and technology don't have magic superpowers over us! We are the ones who decide what we give them access to - and if something happens, we can always reset them!

[5] https://cyber-women.com/en/privacy/privacy/

[6] https://cyber-women.com/en/anonymity/more-online-identities/

[7] https://cyber-women.com/en/digital-security-basics-2/storage-and-encryption/

Part 2 – So What Do We Mean by Resetting?

2. Repeat to the group the affirmation from the previous step, highlighting the final phrase “we can always reset them” – what does this mean? Explain by presenting the following scenario:

    - Perhaps at some point along your digital security journey, you’ve felt as though you’d been doing everything wrong.
    - You look at your computer – it’s full of pirated software, torrented movies and TV shows, and cluttered with other files you don’t even remember downloading.
    - You’ve used USB sticks indiscriminately - on your laptop, on computers and printers at cybercafes, and maybe you don’t even always eject when you’re finished using them.
    - Perhaps you’ve just ended a relationship with someone who you know for sure was looking on your computer when you weren’t around – they probably guessed your password, or maybe you even told them what it was.
    - Now, you feel like you’re out of control – who knows what kind of viruses are living inside your hard drive, or who might have access to your information?
    - But guess what – it’s okay! It’s not too late to get a fresh start. Want to start over? This session is for you!

3. Now, having read through the above scenario for context, you can explain what is meant by resetting in this context: it means starting from scratch, by resetting your device or your computer to its default condition and configuration, and thus giving yourself a “blank slate” for your digital security process.

    - Be sure to remind participants that this session will explain how to perform a reset - they will not actually need to perform the reset during the session, or even during the training.

- Resetting can go seriously wrong if participants are not prepared, or haven't done a backup of their data in recent days – they also likely still need to use their laptops as they currently are to maintain access to their data until they can better prepare.
- However, during this session participants will have the opportunity to practice using alternative operating systems on their laptops, which will be an important point of preparation if they do decide that they would like to perform a reset at some point.

Part 3 – Check-In: Do You Need to Backup?

4. Ideally, you will have already covered the session Storage & Encryption with participants as it addresses important points regarding data backup. Either way, before you begin the hands-on practice portion of this session, do a quick check-in with the group about backing up their data.

   Optional: As a quick refresh from Storage & Encryption, 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.

Part 4 – Resetting & Rebooting

5. Before you begin the hands-on practice portion of this session, another important point to address is the relationship between rebooting and resetting, two terms which may have been used interchangeably during this session:

   - They refer to very similar processes in a general sense, but remind participants that "reset" is being used to illustrate the concept of “starting over” in the context of this session.

- A reboot is a technical operation that will be performed by their computers during their reset; it is also an important process to understand for the hands-on practice with alternative operating systems that will occur in the next part of the session.

6. To further clarify the above point, while also providing some valuable technical insight to participants which will be helpful for the next part of the session, introduce Tails and Ubuntu. Explain how Tails and Ubuntu are alternatives to operating systems like Mac OS and Windows – for this session, the hands-on practice portion will focus on running these operating systems from a USB drive.

Part 5 – Live Operating Systems

7. You may get a question now, which sounds like the following: How can we use a new operating system on our laptops without getting rid of the one we already have? What about our data? You should now take this opportunity to explain to participants a few vocabulary terms that will help them understand more clearly how Tails and Ubuntu operate in the context of this session:

Live System

A live system is an operating system which can be run directly from an external media storage device such as a USB stick or SD card. Tails - which stands for The Amnesic Incognito Live System - is one such example; Ubuntu, which is another “flavor” of the Linux-based operating system that Tails uses, can also be configured as a live system.

Linux

Linux is an operating system similar to Windows or Mac, the major difference being that it is distributed as free and open-source software. Because of this, there are many different adapted distributions of Linux available - Debian, one of the more popular distributions, forms the foundation for Tails.

Boot(able) Device

A Boot (or Bootable) Device is a device or drive from which a computer loads files in order to actually start. For example, on many computers the hard drive is the boot device from which an operating system (such as Windows) is loaded when you turn a computer on. Aside from hard drives, media like CDs, DVDs, SD Cards, and USB flash drives are also boot(able) devices.

BIOS

BIOS (Basic Input/Output System) is the first software many computers run when they are switched on, used to run self-tests on systems and hardware to ensure they are working properly, and to initiate the load sequence for software (like an operating system) located on available bootable devices. BIOS has an interface, but users cannot access it unless they take specific action during startup to access it directly.

Boot Sequence

The boot sequence, which can be accessed through BIOS (or UEFI) during startup on a computer, is a list of the bootable devices on a computer - it is used to determine the order in which a computer attempts to load information from these devices. Normally, a computer’s hard drive is the first device in the boot sequence, from which the operating system is loaded. However, the boot sequence can be changed to first load information from external, removeable devices like DVDs or USBs.

Part 6 – Hands-On Practice

8. To begin the hands-on practice component of the session, divide the participants into at least 2 groups. Provide each group with a computer for them to try running Ubuntu or Tails from a pre-configured live USB; alternatively, if you have enough pre-configured USBs for all participants, they can each practice on their own (in this case, you will want to have everyone practice using either Tails or Ubuntu)
9. On your own laptop or computer, using a projector, walk participants through the process of rebooting their computers and launching Tails/Ubuntu during the BIOS boot sequence. As you do this, be sure to explain the differences between Tails and Ubuntu so that the group more clearly understands how they can be used to do their own "reset".
10. Close the session by discussing how resetting using Tails or Ubuntu can be an option for starting a "blank slate" on participants' computers in the event of a malware attack or other loss of control, but also be sure to mention other types of attacks where this solution does not apply as readily, such as online violence.

References

- https://tails.boum.org/
- http://www.ubuntu.com