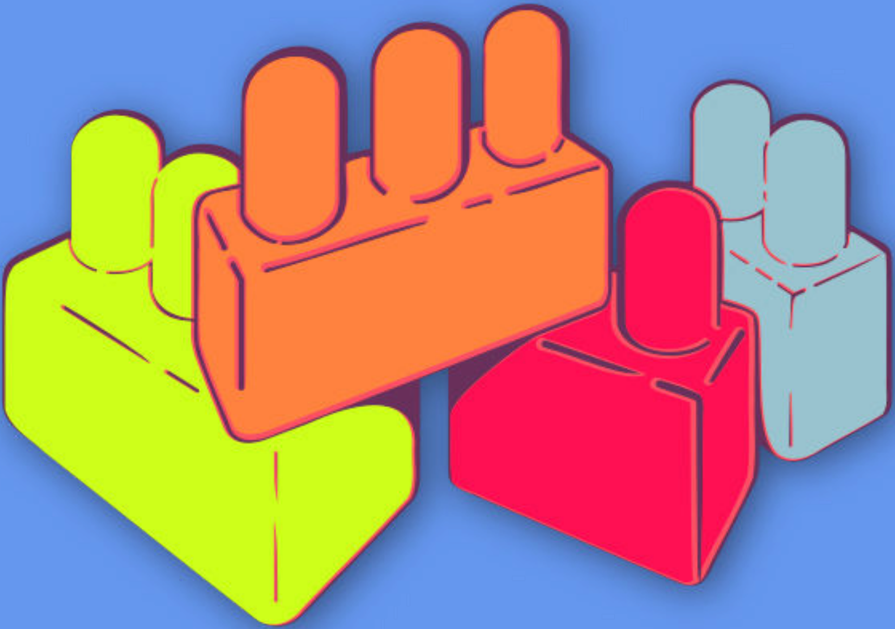
CYBERWOMEN



Digital security basics 1

How to secure your computer

Contents

How to secure your computer

- **Objective(s):** Identifying good practices to keep our computers safe.
- **Length:** 50 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - How does the internet work?[1]
  - Safe browsing[2]
  - Malware and viruses[3]
  - Storage and encryption[4]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup
  - Printed copies of the Backup Format Template (see below)
- **Recommendations:** It is strongly recommended that you do live demon-

[1] https://cyber-women.com/en/digital-security-basics-1/how-does-the-internet-work/

[2] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

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

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

stration – using a projector connected to your laptop - of any tools you choose to cover in this session, so that participants can follow along and practice on their own computers using "dummy" files created for the purposes of the session (not actually important data or files!)

Leading the Session

Part 1 - Introduction

1. Ask participants how much they value their computers - How useful or essential is it to their personal and work lives? How much information they storage in their computers?
2. Now ask them - How much time do they spend on maintenance of their equipment? The difference between the degree with which people tend to value their devices versus the amount of time they spend on maintenance and care is often quite wide. Explain to the group that this session will focus on basic practices for protecting devices.

Part 2 – Physical Environments and Maintenance

3. Mention to the group that many practices related to device safety are in fact more related to physical security than digital security (this is a good way to reinforce the holistic focus of this curriculum). A good example of this is the importance of cleaning devices – to get rid of dirt or residue that might get inside – and to conduct regular physical inspections of equipment to identify any alterations or physical intrusion attempts. In that regard, you can recommend basic digital practices – like using a password to lock a device if they won't be in its immediate vicinity while it is switched on – as well as physical protections, such as using a keyboard protector or an anti-theft cable chain to prevent unwanted access or theft. Make sure to note here how the most critical aspect of their devices' physical safety: awareness. Being aware of

where a device is at any given moment – whether on their person, in the other room, or secured in another location – is essential!

4. Ask each participant to recall the details of their workplace - Which physical risks are present? Is their computer exposed to being stolen? Are there any misplaced cables? Is it possible that their computer might be exposed to extreme heat, cold or moisture? These are other important awareness points – physical awareness isn't just about making sure an adversary doesn't get ahold of their device(s), but also about the potential damage that a device's immediate environment might present.

Part 3 – Software Safety

5. Explain to participants the risks of using pirated software (high likelihood of downloading malware, can't regularly update in the same way as with licensed software, etc.); however, licensed software is also frequently quite expensive. Here, you can share a few resources with the group that will be helpful to address this:

   Osalt[5]

   Open a browser and navigate to Osalt – this is a website that presents free and open source alternatives to many major licensed software platforms and suites (for example, using Ubuntu instead of Windows; LibreOffice instead of Microsoft Word; Inkscape instead of Adobe Illustrator).

   TechSoup[6]

   Via TechSoup, human rights activists and their organizations may be eligible to receive free, or heavily discounted, versions of commercial software: users may look for official distributors among local ICT service providers and request for a non-profit or public sector license discount. A large distribution network for donated software is run by TechSoup - the link above contains a list of partners and the countries in

[5] http://www.osalt.com

[6] http://www.techsoupglobal.org/network

which they operate.

6. Explain to participants the importance of keeping all their software updated - first and foremost, it protects against security vulnerabilities. All software and updates should only be downloaded from trusted sources; for example, when updating Adobe Acrobat Reader, one should only use updates downloaded directly from Adobe, not third-party websites.

7. Next, explain to participants the importance of having an antivirus program on their computers - provide some background that can help demystify some of the common myths related to antivirus, such as:

    - Using two or more antivirus programs offers more protection.
    - Mac and Linux don't need antivirus software because they can't get viruses.
    - It's perfectly safe to use a pirated version of antivirus software.
    - Free antivirus programs are not as safe or reliable as paid programs.

8. Share these, along with any others that participants share with you – then, discuss some basic safe practices for using antivirus software and protecting against malware (see Malware & Viruses session in this module). Some useful ones to highlight here, in case you haven't already covered them in the Malware & Viruses session in this module, are:

    - Using the uBlock browser plug-in to avoid clicking on ads that might download malicious malware files onto their computer.
    - Being aware of phishing attempts, suspicious links or attachments found within emails in particular, that appear to be sent from unknown accounts or from accounts that appear similar to those of trusted contacts.
    - This is a good opportunity to mention firewalls – these offer an automated layer of protection in their computers. Share tools like

Comodo Firewall, ZoneAlarm and Glasswire. Newer (licensed) versions of Windows and Mac OS also have robust firewalls already installed.

Part 4 – Data Protection and Backups

9. 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.
10. 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 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?

11. Explain next that, although there are backup automation tools available (such as Duplicati.com or Cobian), participants may find it easier to start doing their backups by manually dragging and dropping files to the backup storage media. This ultimately depends on the complexity or amount of data they have to manage – for the average user however, manual backups should be more than sufficient.
12. To follow-up on secure data backups, re-visit briefly the concept of encryption for storage media. Explain to the participants what it means

to do, and why encrypting their hard drives or storage media can be useful. **VeraCrypt and MacKeeper**, two relatively popular utilities for implementing file or disk encryption, could be mentioned here as options for participants to explore.

Part 5 - Deleting Files and Recovering Them

13. Read aloud the following statement:

    > From a purely technical perspective, there is no such thing as a delete function on your computer.

    Ask the group what they think about this – Does this statement make sense? How can it be that there is no such thing as a 'Delete' function? Remind the participants that they can drag a file to the Recycle Bin on their computer desktop, and then empty the bin, but all this does is clear the icon, remove the file's name from a hidden index of everything on your computer, and then tell their operating system that the space can be used for something else.

14. Ask the group - What do you think happens to the data that is 'deleted'? Until the operating system uses that newly free space, it will remain occupied by the contents of the deleted information, much like a filing cabinet that has had all its labels removed but still contains the original files.

15. Now explain that because of how a computer manages this storage space for data, if they have the right software and act quickly enough, they can restore information deleted by accident; likewise, there are also tools available that can be used to permanently delete files (not just remove them from the file index until the space is occupied). Take this opportunity to present **CCleaner, Eraser, and/or Bleachbit** as tools that can be used to delete files and Recuva as an option to recover deleted files.

References

- https://seguridaddigital.github.io/segdig/
- https://securityinabox.org/en/guide/malware
- https://level-up.cc/curriculum/malware-protection/using-antivirus-tools
- https://securityinabox.org/es/guide/avast/windows
- https://securityinabox.org/en/guide/ccleaner/windows
- https://securityinabox.org/en/guide/backup
- https://securityinabox.org/en/guide/destroy-sensitive-information
- https://chayn.gitbooks.io/Avanzado-diy-Privacidad-for-every-woman/content/Avanzado-pclaptop-security.html