Cyber-security

HORMONIC
UPF_Barcelona

Cyber security

1. Ransomware

1.1. What is it?

This is a program that can lead to the total lose of information in your computer. It can block the access to the computer or damage your files. It can also affect an USB. The only way to recover your files is though a security copy. **Make security copies periodically!** They will ask you money. **Don't pay!** This money is often used to finance other criminal activities. Moreover, you will not have the certainty that your files will be liberated after the payment.

1.2. How the infection is produced?

- Spam or phishing
- When you download and install another program
- *Web Exploit / Kits* → advertisement banners
- Predictable or vulnerable passwords

1.3. How can I prevent an infection?

- Make **security copies periodically** in CD, DVD, cloud, or hard disk. USB is not a good idea because they use a less reliable technology, they are small and can get lost, they are susceptible to infections, and can have format errors that could make impossible reading the files.
- Actualize the computer and all your application
- Activate the fair-wall of your Windows computer
- Use google *antispam*
- Use advertising program blockers *(adblock, ublock...)*
- Activate the option that leads you see the extensions of the files
- Activate the option of restore the system if you use Windows
- Suspect of messages:
    - From known people but with a style different that the usual
    - From enterprises without link with you
    - Without text, but with an attached file
    - Just asking to open an attached file
- Do not open any executable files
- Save attached files to check that they are correct (they don't have a double extension)
- Surf in secure web pages
- Do not download illegal programs
- When you install a program you have to read the screens and unselect what you don't need

1.4. What should I do if I suspect that my computer is infected?

- Close the computers
- Contact with the UPF Informatics Service (https://www.upf.edu/web/cau/biblioteca-informatica) and explain them how the infection has been produced

1.5. How can I restore the infected files?

- Security copy not physically connected to the infected computer
- Security copy from Dropbox/Drive
- Option Restore the System in Windows (you have to activate it previously to the infection)
- In any case paying the rescue is recommended

2. Phishing

2.1. What is that?

This is a fraud technique that, through the e-mail, tries to get personal information like credit cards, bank account keys, or mail passwords.

2.2. How can I prevent it?

- Install Chrome Password alert (https://chrome.google.com/webstore/detail/password-alert/noondiphcddnnabmjcihcjfbhfklnnep)
- Activate verification in two steps of the e-mail (https://www.google.es/intl/ca/landing/2step/)
- Actualize browser version and antivirus
- Don't give personal data user names or passwords by mail
- Don't open messages from unknown people
- Don't open strange or suspicious messages

2.3. What should I do in case of phishing?

- Mark the mail as SPAM
- Change immediately the password
- Contact with the UPF Informatics Service (https://www.upf.edu/web/cau/biblioteca-informatica)

3. Passwords

3.1. Safe password

- You have to use at least **8 characters**
- You have to use letters, numbers and special characters
- You have to alternate capital letters with lower case
- Password have to be easy to remember and quick to write
- **Change your password once a month!**
- Don't generate sequential rules of change, ex. qWeRt01, qWeRt02, qWeRt03…

3.2. Avoid

- Using the same password in all the systems or services
- Using personal information
- Using basic sequences of the keyword, ex. qwert, 1234, asdf, 9876…
- Repeating characters, ex. 111222…
- Using only numbers, capital letters or lower case, ex. 15880864, hagfjhb, NBFAUJB…
- Passwords with the user name or nickname
- Data related with the user that could be easy to be deduced
- Saving passwords in anywhere that is not your head, ex: computer, mobile phone, notebook…
- Words that can be found in dictionaries
- Sending the password by mail or text message

- Share your password or mention it in any conversation
- Passwords that appear in explicative examples of building safe passwords
- Writing your passwords in computers of unknown security, ex. cyber-coffee, libraries…

3.3 How can I create good passwords and, at the same time, easy to remember?

- Use words with any sense but that can be pronounced
- Choose a sentence and use the first letter of each word in that sentence

4. File names

4.1. What do I have to avoid?

- Orthographic signs and other symbols (%, &, $, “, ª, ?, ¿) because can lead to access problems
- Keeping the suggested file name by the text editor
- Deep folder structure. More than 8 levels are not recommended

4.2. What should you do?

- Write short names to folders and files (no more than 10 characters)
- Use just letters and numbers
- Use normal and low hyphens
- Make subfields structures of less than 8 levels