

Erasmus Plus Programme – KA2 Strategic Partnerships for higher education



Project № 2018-1-ES01-KA203-050493



This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

Document description

Document Name	Practical Cybersecurity Guide
Revision	V4
Revision Date	23/01/2020
Author(s)	Anabel Menica, Jokin Goioaga, Kostas Papadourakis, Kostas Karampidis, Nuno Escudeiro, Joaquim dos Santos, Aris Chronopoulos



Contents

1. Overview	3
2. Practical Cybersecurity Guide	4
2.1 Computer software maintenance policy	4
2.2 PLC update policy	5
2.3 Data integrity (file transfers).....	6
2.4 Data storage - Backup	7
2.5 Passwords	8
2.6 Wifi.....	9
2.7 Internet surfing behavior	10
2.8 General rules.....	11



1. Overview

InCYS 4.0 project intends to develop a training course in cyber security awareness and responsiveness for current and future technicians/ engineers (EQF level 5+) who will work with/alongside Industrial 4.0 Control Systems. The flexible didactic modules created for InCys 4.0 consisting of a total of 30-50 hours of training will:

- Provide an overview of the most important concepts associated with the area of Industrial security.
- Understand the main differences between security policies that are carried out in IT environments and OT environments.
- Analyze the main vulnerabilities and threats that can be suffered in industrial environments.
- Know the different types of attacks that can be made to an OT network or a critical infrastructure.
- Introduce the most important aspects associated with the protection of critical infrastructures and current regulations.
- Describe the main countermeasures that can be included to strengthen industrial networks and protocols.

Additionally to the online training course the project developed a Practical Cyber Security Guide for technicians covering the fundamentals threats of cyber security for Industrial Systems.

This practical guide is developed in the form of posters that can be placed in the industrial environment and give directly to technicians the DOs and DON'Ts, in other words the correct practices in relation to keeping industrial systems safe from all forms of attacks.

This Quick Guide, summarising the main risks and steps to follow for technicians working around digital control systems in Industry 4.0, can be distributed as a stand-alone fast handbook on the most basic issues or/and as a complement to the training course.



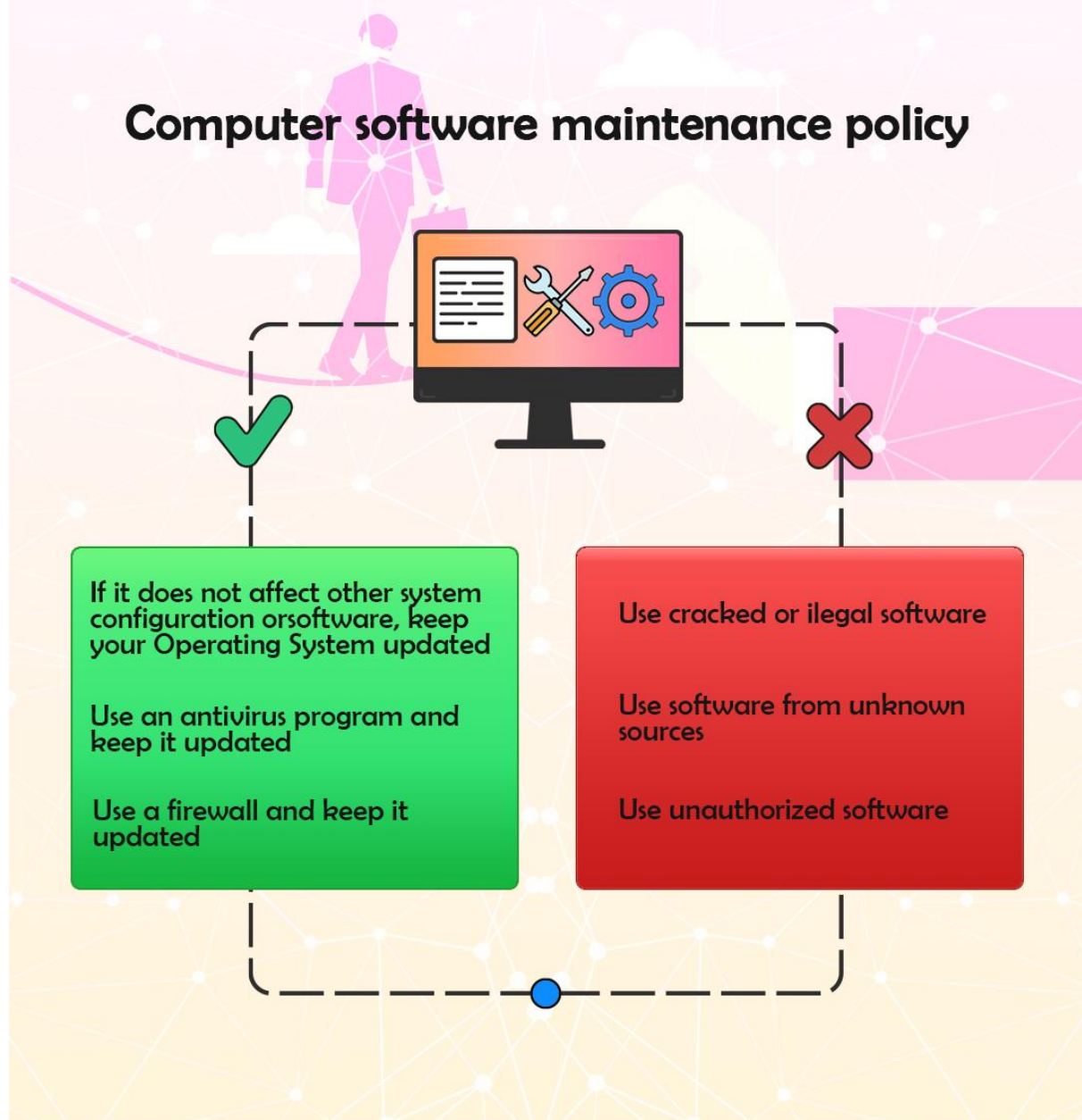
2. Practical Cybersecurity Guide

2.1 Computer software maintenance policy

“ It is important to keep updated software in company computers to avoid unnecessary risks. ”



Computer software maintenance policy





2.2 PLC update policy

“ It is important to keep updated software in company PLC’s to avoid unnecessary risks. ”



PLC update policy

When possible, keep updated your PLC firmware to latest version

Change all default passwords

Be informed about the usage of the devices and new technologies



Let unauthorized personnel to have access


Use common and simple passwords



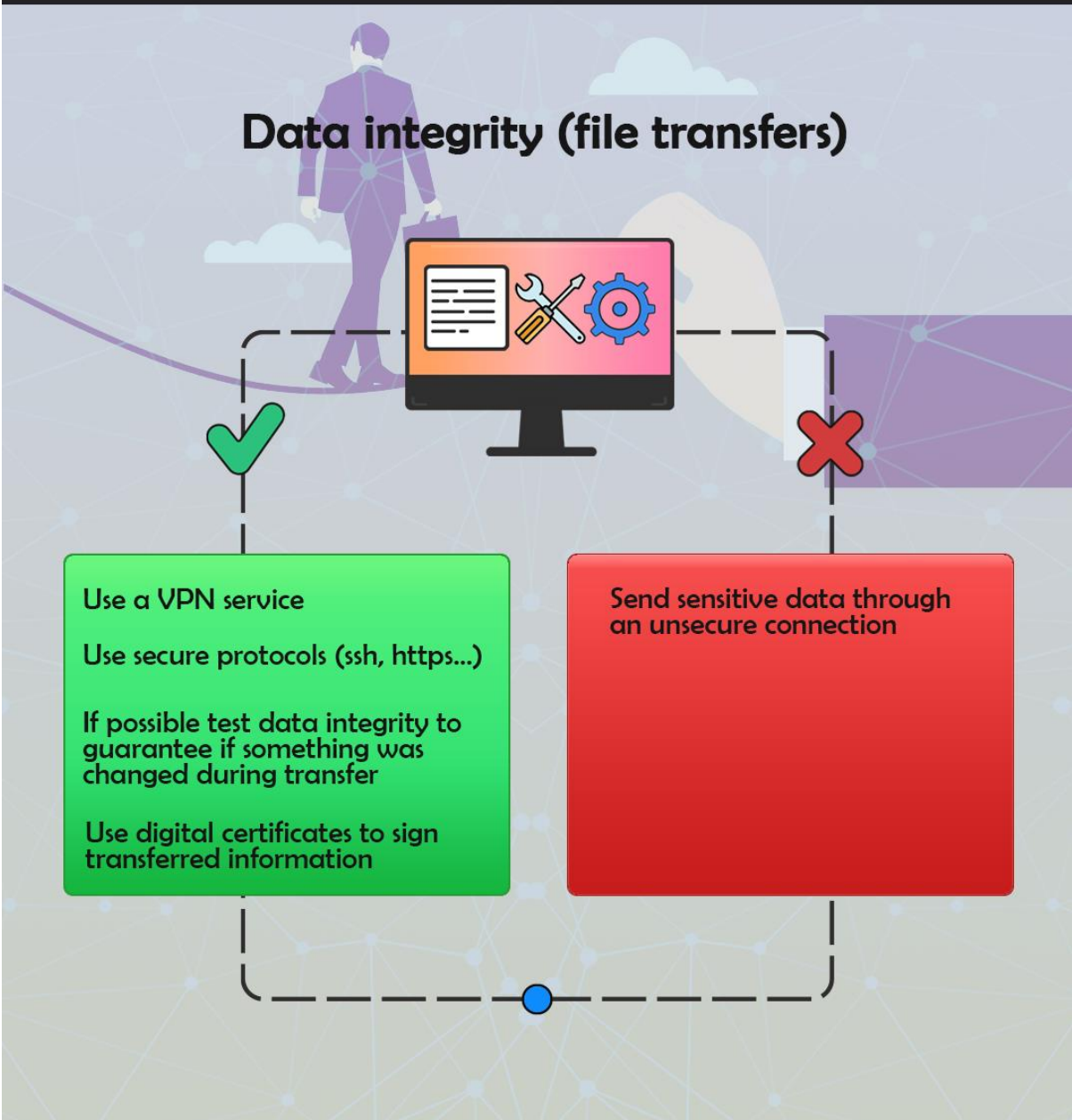


2.3 Data integrity (file transfers)

“ Keep data safe to avoid losses. ”



Data integrity (file transfers)



Checkmark (Correct Practices):


- Use a VPN service
- Use secure protocols (ssh, https...)
- If possible test data integrity to guarantee if something was changed during transfer
- Use digital certificates to sign transferred information

Red X (Incorrect Practice):

- Send sensitive data through an unsecure connection

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the
Erasmus+ Programme
of the European Union





2.4 Data storage - Backup

“ Avoid a disaster, keep your data safe. ”



Data storage / backup

Make periodical backups

Use different locations to store backups

Verify your backups when they are done

Hash your backups to guarantee their integrity

If using media for backups keep the devices in a secure, off-site location

Use good quality media storage devices

If possible maintain a completely offline version of your backups



Save all your backups in the same storage device

Delete a backup without a new one is finished and verified

Use unencrypted cloud services to store your backups





2.5 Passwords

*“ A poorly chosen password may result
in serious security problems. ”*



Passwords

Change your password
frequently

Use combination of Caps,
numbers and characters

Use long passwords, more
than 8 characters

Use an open source password
manager to store all your
passwords



Share your passwords with other
people

Write passwords down and store
them in your office

Use short passwords

Use common passwords like your
birthday etc.

Use the same password twice

Use an older password when you
change one

Be attended when you change
your passwords

Use the "Remember Password"
feature of applications



Store passwords in your computer
unencrypted

Tell your passwords to anyone even
if you are asked to do so





2.6 Wifi

“ Not all WIFI are innocent!!! ”

WIFI

Checkmarks (Green Box):

- Keep your passwords protected
- Check the name of the network before connecting to it
- Only connect to company verified WIFI

Red X (Red Box):

- Share your accounts
- Connect in unsecured wireless networks
- Connect company mobile devices to unauthorized WIFI
- Use your company's WiFi to create a hotspot

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the
Erasmus+ Programme
of the European Union

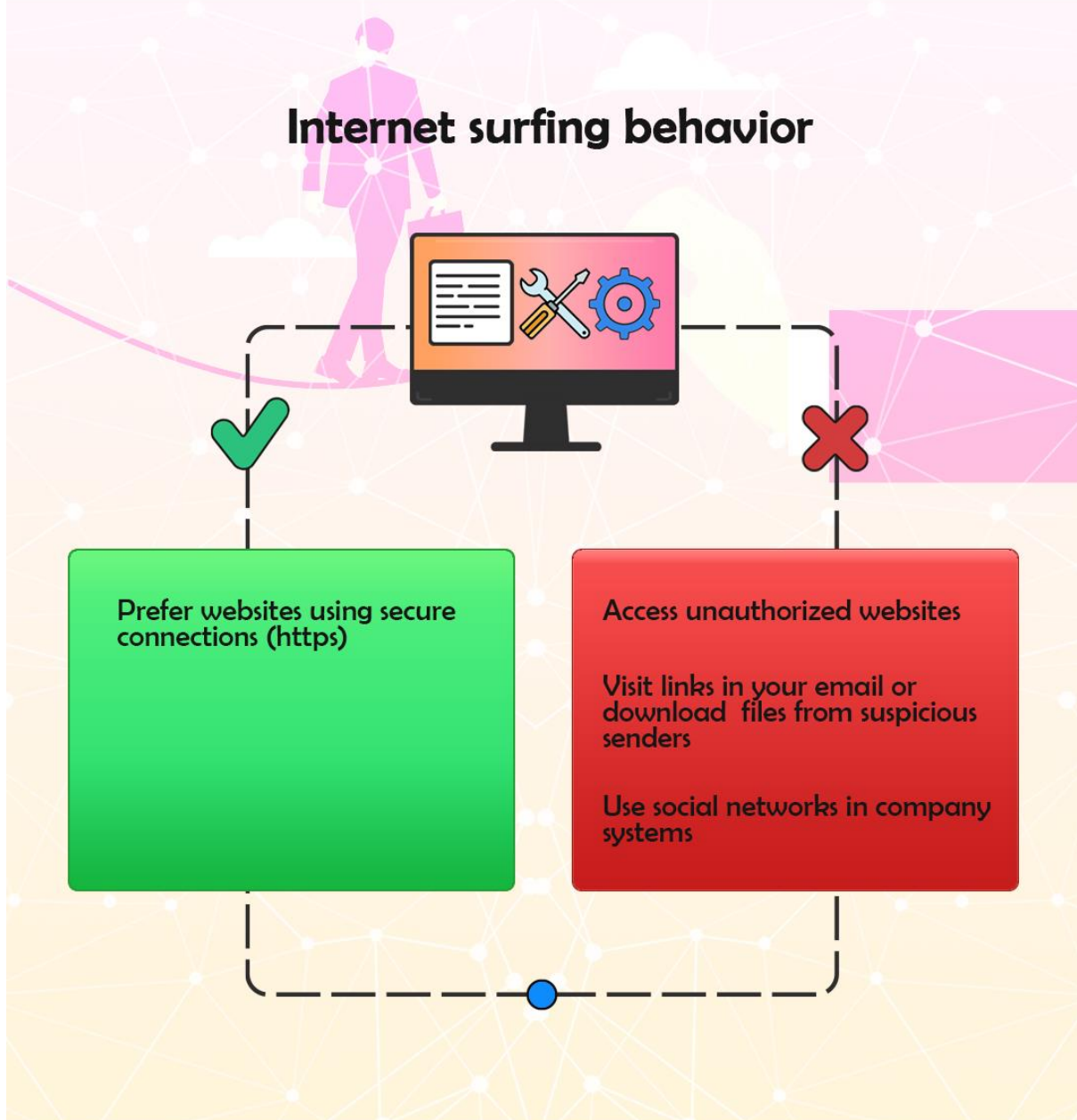


2.7 Internet surfing behavior

“ Behave yourself on the internet!!! ”



Internet surfing behavior






2.8 General rules

“ And always remember!!! ”

General rules

Be aware of strange (description needed) behaviour on your devices


If you detect a strange behaviour immediately inform your superior or the IT staff



Access network equipment you are not explicitly allowed

Publish company sensitive data on social media.

Access areas you are not allowed to



The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the
Erasmus+ Programme
of the European Union 