ESCAPE:

Preparing healthcare professionals for cyberattacks

Material for learners

Web seminars about key aspects of cibersecurity

ESCAPE: Preparing healthcare professionals for cyberattacks	
Seminarios web sobre aspectos clave de ciberseguridad	
Language	Spanish

Table of contents

1. Name of the material and description..... 3
2. Classification..... 3
3. Description..... 4
3.1. Origin..... 4
3.2. Why is it relevant/important for ESCAPE..... 4
3.3. Lessons learned..... 4
4. Direct link to the material..... 5
5. Other resources (optional)..... 5

Seminarios web sobre aspectos clave de la ciberseguridad

"Seminarios web sobre aspectos clave de ciberseguridad". Some video-format publications, designed to present cybersecurity knowledge and technical aspects in an engaging and accessible way.

1. Classification

Category	Mark if applies
Sector	☐ Healthcare
	☑ General public
	☐ Other
Topics covered	☑ Cybersecurity
	☐ Data protection
Situation type	☑ Prevention
	☐ Impact

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Seminarios web sobre aspectos clave de ciberseguridad	
Language	Spanish

	☐ Impact on all other activities not involving direct patient care.
Language of the original materials	☐ Dutch
	☐ English
	☐ German
	☐ Italian
	☑ Spanish
Type of the material	☑ Guidelines or manuals
	☐ Case or examples
	☐ Training courses
	☐ Others

2. Description

This material offers a series of tutorial videos that explain various cybersecurity aspects to consider in order to apply good cybersecurity practices.

2.1. Origin

The material was created by INCIBE, the Spanish “National Cibersecurity institution”. It is a national organisation dependent on the Ministry of digital transformation and economic issues. It is considered as the reference entity for cybersecurity development, improvement of citizen digital trust, and academic research in that matter in Spain.

2.2. Why is it relevant/important for ESCAPE

This material is highly relevant because it emphasizes the importance of cybersecurity for the protection of patient data and company information. It also shows that common measures, such as the use of antivirus software and backups, are not enough to ensure the integrity of confidential information. It highlights the importance of the Security Master Plan and provides guidelines to significantly enhance cybersecurity.

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

ESCAPE: Preparing healthcare professionals for cyberattacks	
Seminarios web sobre aspectos clave de ciberseguridad	
Language	Spanish

2.3. Lessons learned

- **Introduction:** The material aims to introduce different tools and techniques to improve cybersecurity.
- **Target group**: System administrators, network administrator, support technicians, and other IT profiles.
- **Risks summary:**
  - Problems with network traffic.
  - Unsecure Wi-Fi.
  - Software vulnerability.
  - Phishing.
  - Sharing passwords.
  - Unprotected workstation.
  - Sensitive documentation in plain sight.
  - Data leaks.
  - Non-updated software or less protected software.
  - Ransomware.
  - Packet sniffing.
  - Man in the middle.
  - Mac spoofing.
- **Solutions or contingency measures:**
  - Use Wireshark.
  - Strengthening Wi-Fi security.
  - Secure App development.
  - Phishing identification.
  - Use Owas-zap.
  - User awareness in cybersecurity.
  - Use encryption tools.
  - Use secure networks.
  - Use Snort IDS.
- **Tips and tricks:**
  - Update firmware.
  - Hide the SSID.
  - Enable the wireless guest network.
  - Reduce the IP address range.
  - Limit the access point signal power.
  - Change the default password of the access point.
  - Encrypt information.
  - Software update policy.
  - Invest in staff training.

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.

- Report phishing.
- Limit methods of data extraction, copying, and deletion.
- Block access to external webmails.
- Control of emails to third parties.
- Restrictions on the use of USB ports.
- Block access and emails of employees who are no longer part of the workforce.
- To audit the exchange between the browser and the web server in order to identify vulnerabilities.
- To review default configurations and establish a policy of minimal exposure.
- Use of secure encryption.
- Use manual connection.
- Use web sites HTTPS.
- Use VPN configuration.
- Make sure not to share resources before connecting to an unsecure network (net share).
- Disable automatic synchronization before connecting to an unsecured network.
- Detect anomalous behaviors within our network or unwanted access attempts using an Intrusion Detection System (IDS).
- Use digital password managers so you don't have to write down or remember your passwords.
- Do not share your passwords with anyone.
- Generate strong and secure passwords.
- Do not use the same password for different sites or services.
- Change your passwords periodically.
- Use password generator programs to help you (KeePass, Bitwarden).
- Avoid using "remember password" or "keep me signed in" options.
- Apply two-factor authentication.

3. Direct link to the material

https://www.incibe.es/incibe-cert/publicaciones/seminarios-web

4. Other resources (optional)

The material includes several links to get deeper into specific topics or to additional material.

Co-funded by the European Union

The project "ESCAPE: preparing healthcare professionals for cyberattacks" is co-funded by the European Union. The opinions and viewpoints expressed in this minute meeting solely commit to their author(s) (ESCAPE consortium) and do not necessarily reflect those of the European Union or the Servicio Español para la Internacionalización de la Educación (SEPIE). Neither the European Union nor the National Agency SEPIE can be held responsible for them.