SecureHospitals.eu

Raising Cybersecurity Awareness in Hospitals and Care Centers

Pain

#1 According to ENISA, the **healthcare industry** jumped to the **top** in **cybersecurity attacks** in any industry

300% increase in ransomware attacks since 2015.

+150 countries and **+230,000 systems** were **affected by cybercrime** on essential services, including **hospitals** and **ambulances**

€ The medical sector has the **highest cost** for repairing the cybersecurity safety gap (375 € per medical file)

€100b global economy cost by serious cyber attacks.

According to CheckPoint.com, **cybersecurity** is still an **unresolved issue** of the medical sector, an environment where the **consequences** for patients can be **fatal**

Research

69% of business have **no** or basic **understanding** of their exposure to cyber risk

60% of business have **never estimated** the potential **financial losses** from a major cyberattack

51% of European citizens feel not at all or **not well informed** about cyber threats

The scale of the problem makes it necessary to act at the **European level**

+100 More than **100 EU research** and innovation **programs** and initiatives aiming to improve cybersecurity. **25 national** cybersecurity European agencies.

enisa ECSO **+1 strong European cybersecurity entities.**

Ecosystem:

+28 national health systems and social security systems

>30 national cybersecurity entities

>15,000 hospitals and a vast amount of care centres

>10 million healthcare professionals

Project SecureHospitals.eu

+500 literature and publications collected and analysed

+200 projects and initiatives grouped and analysed

+100 cybersecurity programs collected and categorised

+20 cybersecurity toolkits collected and listed

According to Kaspersky.com, cybersecurity awareness raising programs delivers **proven results** as

90% Reduction in the total number of incidents

86% Participants willing to **recommend** the experience

93% Probability that knowledge will be applied in everyday work

30x Return of investment from purchase in security awareness programs

Innovation

Required innovative **awareness programs**

Develop boosting strategies and tools for raising cybersecurity awareness

Promote through multiple dissemination channels

Connect with the full potential range of trainers and researchers across Europe

Achieve impacts through effective information aggregation and dissemination materials

Lowering the number of **human errors** causing cybersecurity threats

Lowering the **risk** of data privacy breaches

Reducing cybersecurity **vulnerability** of Health and Care services, data and infrastructures

Increasing patient trust and **safety**

Cure

Awareness raising of staff working in healthcare settings on **security and data privacy**

RAISE awareness among decision makers and ICT practitioners in hospitals and care centres across Europe.

AGGREGATE all existing knowledge on cybersecurity in hospitals for the development of high quality and innovative trainings e-approaches.

Training staff working in healthcare settings

CREATE tailor-made training materials for trainers and IT practitioners to ensure the effective data protection, privacy and cybersecurity measures.

TRAIN the trainers and practitioners all over Europe using different online and on-site methods.

COMMUNICATE training needs, project training initiatives and further awareness raising on the online awareness and information hub.

Proactive managerial and technological strategies to reduce vulnerabilities !

SecureHospitals.eu

@SecureHospitals
@SecureHospitals.eu
project.securehospitals.eu
office@securehospitals.eu

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

SECUREHOSPITALS.EU

Raising Cybersecurity Awareness in Hospitals and Care Centers

office@securehospitals.eu project.securehospitals.eu @SecureHospitals @SecureHospitals.eu

Basic Cybersecurity Terms & Concepts

Share

1. Clean Desk Policy

Sensitive information on a desk such as sticky notes, papers and printouts can easily be taken by thieving hands and seen by prying eyes. All sensitive and confidential information should be removed from the desk at the end of each working day.

2. Bring-Your-Own-Device (BYOD) and Bring-Your-Own-App (BYOA) Policy

BYOD and BYOA covers the employees' personal computing possessions which might be used in a work setting, which could be utilized to steal sensitive data.

3. Data Breaches

There are numerous types of data (such as a backup copy of patient contracts or clinical data) and a lot of employees may not be aware of this fact. Employees should learn about all the types of data so that they can understand their criticality.

4. Removable Media

Your corporate personnel must be educated about the menaces of unsolicited removable media and prohibited from accessing any stray media such as an external hard drive, even if it's on a secured system.

Search

5. Phishing Attacks

- Employees must be conversant with phishing attacks and learn not to open malicious attachments or click on suspicious links.
- It's better to disable pop-up windows, as they invite risks.
- Users should refrain from installing software programs from unknown sources, especially links infected with malware. Many websites offer free Internet security programs that infect your system rather than protecting it.

6. Social Networking

Ask your employees not to provide their credentials or login information to unknown sites or sites that are similar to the original one. For example, the user must carefully see the difference between **www.google.com** and **www.gooogle.com.**

7. Email Spams

- Do not trust unsolicited emails.
- Do not send any funds to people who request them by email, especially not before checking with leadership
- Do not click on unknown links in email messages.
- Beware of email attachments. If you get one from what looks like a friend, contact them to ensure that they sent it.

Learn

8. Malware

Malware types include adware, spyware, viruses, Trojans, backdoors, rootkits, botnets, logic bombs and armored viruses. Employees should learn how to identify malware and what to do if their device or network has been infected. The immediate response should be to turn off the system or device and inform the security management team.

9. Zero-day Threats

A zero-day threat is a threat that exploits an unknown computer security vulnerability. This means that there is no known security fix because developers are oblivious to the vulnerability or threat.

10. Ransomware

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid (e.g., prevent staff from accessing patient records or scheduling appointments).

Next Steps

*Log on to **www.SecureHospitals.eu** Online Hub* !

SECUREHOSPITALS.EU

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

SecureHospitals.eu

Raising Cybersecurity Awareness in Hospitals and Care Centers

office@securehospitals.eu project.securehospitals.eu @SecureHospitals @SecureHospitals.eu

Cybersecurity Basics for Healthcare Organisations

Share

Protect Network Access

File sharing and instant messaging can expose the connected devices to security threats and vulnerabilities. Check to make sure peer-to-peer applications have not been installed without explicit approval. They must be uninstalled.

Secure Physical Access

Securing information physically should include policies limiting physical access, e.g.,securing machines in locked rooms, managing physical keys, and restricting the ability to remove devices from a secure area.

Search

Secure Health Information

Setting file access permissions may be done manually, using an access control list. This can only be done by someone with authorized rights to the system. Prior to setting these permissions, it is important to identify which files should be accessible to which staff members.

Be Prepared for Disaster

A fireproof, permanently installed home safe, which only the health care provider knows the combination for, may be the most feasible choice for many practices to store backup media. This would provide some safety against local emergencies such as fire and flood.

Learn

Change Passwords Regularly

Strong passwords are ones that are not easily guessed. Since attackers may use automated methods to try to guess a password, it is important to choose a password that does not have characteristics that could make it vulnerable.

Strong Password Characteristics:

- At least eight characters in length (the longer the better).
- A combination of uppercase and lowercase letters, one number, and at least one special charact er, such as a punctuation mark.

Next Steps

*Log on to **www.SecureHospitals.eu** Online Hub* !

SecureHospitals.eu

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

SecureHospitals.eu

Raising Cybersecurity Awareness in Hospitals and Care Centers

office@securehospitals.eu   project.securehospitals.eu   @SecureHospitals   @SecureHospitals.eu

Cyber Hygiene Basics

Share

Raise Cybersecurity Awareness

One of the most challenging aspects of raising awareness about cybersecurity among users is overcoming the perception that "it can't happen to me." People, regardless of their level of education or IT sophistication, are alike in believing that they "will never succumb to sloppy practices or place patient information at risk. That only happens to other people."

Secure Portable Devices

Because devices may be used in places where it can be visible by others, extra care must be taken by the user to prevent unwanted viewing of the electronic health information displayed on a laptop or handheld device.

Search

Install a Firewall

A firewall prevents intruders from entering in the first place. In short, the anti-virus can be thought of as infection control while the firewall has the role of disease prevention.

Update software regularly

Typical computer infections show these symptoms:

- System will not start normally.
- System crashes for no obvious reason.
- Internet browser directs you to unwanted web pages.
- Anti-virus software appears to be disabled.
- Many advertisements pop up on the screen.
- The user cannot control the mouse.

Learn

Keep Computers Healthy

The medical practitioner is familiar with the importance of healthy habits to maintain good health and reduce the risk of infection and disease. The same is true for IT systems, they must be properly maintained so that they will continue to function properly and reliably in a manner that respects the importance and the sensitive nature of the information stored within them. As with any health regimen, simple measures go a long way.

Next Steps

*Log on to **www.SecureHospitals.eu** Online Hub* !

SecureHospitals.eu

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

SecureHospitals.eu

Raising Cybersecurity Awareness in Hospitals and Care Centers

office@securehospitals.eu project.securehospitals.eu @SecureHospitals @SecureHospitals.eu

How to promote a Cybersecurity culture in your organisation

Share

1. Raise Cybersecurity Awareness

- Education and training must be frequent and ongoing.
- Those who manage and direct the work of others must set a good example.

2. Secure Portable Devices

- Health Information on mobile devices is encrypted.
- Connections between authorized mobile devices and Electronic Health Records are encrypted.

3. Install a Firewall

- All computers are protected by a properly configured firewall.
- All staff members understand and agree that they may not hinder the operation of firewalls.

Search

4. Update Software Regularly

- All staff members know how to recognize possible symptoms of viruses or malware on their computers.
- Anti-virus software is installed and operating effectively on each computer in compliance with recommendations.

5. Keep Computers Healthy

- Providers' remote maintenance connections are documented and fully secured.
- Systems and applications are updated or patched regularly as recommended by the manufacturer.

6. Protect Network Access

- Access to the network is restricted to authorized users and devices.
- Guest devices are prohibited from accessing networks that contain Health Information.

7. Secure Physical Access

- All devices containing Health Information are inventoried and can be accounted for.
- Physical access to secure areas is limited to authorized individuals.

Learn

8. Secure Health Information

- Every user account can be positively tied to a currently authorized individual.
- Users are only authorized to access the information they need to perform their duties.

9. Be Prepared for Disaster

- Backup media are physically secured. Backup media stored off-site are encrypted.
- Backup schedule is timely and regular. Every backup run is tested for its ability to restore the data accurately.

10. Change Passwords Regularly

- Each staff member has a unique username and password.
- Passwords are changed routinely. Passwords are not re-used.

Next Steps

*Log on to **www.SecureHospitals.eu** Online Hub* !

SecureHospitals.eu

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.