



SECURITY AWARENESS SERVICE

FOR HEALTHCARE ORGANIZATIONS

Cyber threats in healthcare continue to escalate as human error, digital vulnerabilities, and complex supply chains put critical data at risk. Integrated cybersecurity initiatives combined with tailored security awareness training empower your team to strengthen defenses and safeguard essential services.



GROWING THREATS TO THE HEALTHCARE SECTOR

Healthcare organizations are increasingly becoming targets for sophisticated cyberattacks, with several major attacks and recent trends such as:

- » **Rising Cyber Incidents:** In 2023, cyber events in the healthcare sector nearly quadrupled, exposing over 133 million records in 725 breaches.
- » **Ransomware Disruptions:** Attacks like the Change Healthcare incident and others have shown how ransomware can delay critical medical procedures, create emergency room gridlock, and compromise patient safety.
- » **Digital Expansion Vulnerabilities:** As hospitals adopt more digital tools—electronic health records, telemedicine, AI diagnostics, and more — the number of potential entry points for cybercriminals grows.
- » **Supply Chain and Compliance Risks:** The interdependence of digital systems and the pressure to meet strict cybersecurity regulations have added further complexities to healthcare cybersecurity.

These challenges not only compromise patient care but also expose organizations to significant financial and reputational risks.

TAKE ACTION TODAY

Don't let cyber threats compromise your healthcare services. Empower your team with the proactive defense it needs.

**BOOK
A DEMO**





EU ACTION: A DIRECTIVE FOR PROACTIVE CYBERSECURITY MEASURES

In response to these escalating threats, the European Commission has unveiled a comprehensive action plan aimed at fortifying cybersecurity in healthcare. Key aspects include:

- » Prevention Guidance & Financial Aid: Offering cybersecurity vouchers and tailored guidance to help hospitals establish stronger defenses.
- » Threat Detection & Rapid Response: Proposing an EU-wide early warning system and a dedicated Cybersecurity Support Centre for healthcare.
- » International Cooperation: Utilizing tools like the Cyber Diplomacy Toolbox to deter malicious cyber activities.

THE IMPORTANCE OF SECURITY AWARENESS

95% of all cybersecurity incidents are caused by human error. Employees are the first line of defense against cyber threats. Comprehensive security awareness training can:

- » Empower Staff: Equip every team member with the knowledge to identify and mitigate threats such as phishing and ransomware.
- » Enhance Compliance: Ensure your organization meets stringent EU cybersecurity regulations.
- » Reduce Disruptions: Prevent delays in critical healthcare services by minimizing the risk of successful cyberattacks.
- » Protect Patient Data: Safeguard the sensitive information that forms the lifeblood of patient care and trust.

SECURITY AWARENESS SERVICE: HEALTHCARE'S CYBER DEFENSE PARTNER

Hornetsecurity offers a state-of-the-art Security Awareness Service designed to protect organizations across a wide range of industries, including healthcare. Here's how our solution makes a difference:

- » Tailored Training Programs: Customized modules address the unique challenges of healthcare cybersecurity, ensuring your staff is prepared to face real-world threats.
- » Comprehensive Content: From safe web browsing to secure handling of personal health information, our training covers all essential topics.
- » Ease of Implementation: Our service is designed to integrate seamlessly into your existing systems, reducing downtime and boosting overall resilience.
- » Ongoing Support: Continuous updates and follow-ups ensure that your organization stays ahead of evolving cyber threats.