



IGIENE INFORMATIC A



Co-funded by
the European Union

*ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536*

Partner



Firla

PRAMMER



ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536



**Co-funded by
the European Union**

Questo progetto è stato co-finanziato con il supporto della Commissione Europea. Questa pubblicazione [comunicazione] riflette solo le opinioni dell'autore, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute.



Indice

1. Definizione	1
2. Rilevanza generale	1
3. Importanza nella salute e nell'assistenza e impatto sulla qualità dell'assistenza	1
4. Cosa posso fare come professionista sanitario?	2
5. Ulteriori informazioni	
1. Materiali didattici	2
2. Video correlati	3
3. Link rilevanti	3
6. Bibliografia	4



Co-funded by
the European Union



FACTSHEET - IGIENE INFORMATICA

1. Definizione

Si riferisce alle semplici pratiche e misure che tutti possiamo adottare per proteggere le nostre informazioni personali e i nostri dispositivi dalle minacce informatiche. Alcune includono l'autenticazione a due fattori, l'utilizzo di password complesse, aggiornamenti software regolari, ecc.

2. Rilevanza generale

La maggior parte delle violazioni della sicurezza deriva direttamente da malintenzionati che sfruttano falle trascurate dalle attuali pratiche di igiene informatica dell'organizzazione. L'igiene informatica protegge computer, reti e dati da ogni tipo di rischio informatico, inclusi malware, ransomware e altri attacchi.

La manutenzione è fondamentale, poiché i sistemi correttamente gestiti sono più efficienti. La mancanza di manutenzione porta a frammentazione, programmi obsoleti e, di conseguenza, lacune nella sicurezza. L'igiene informatica previene violazioni dei dati e furti di identità e riduce i rischi finanziari, reputazionali e operativi.

3. Importanza nella salute e nell'assistenza e impatto sulla qualità dell'assistenza

L'igiene informatica riveste un'importanza fondamentale nel settore sanitario, data la delicatezza dei dati dei pazienti e la dipendenza dai sistemi digitali per diagnosi, trattamento e comunicazione. Proprio come l'igiene di base nell'assistenza clinica, l'igiene informatica previene gli incidenti informatici. Di conseguenza, le violazioni delle misure di sicurezza possono portare ad attacchi ransomware che possono paralizzare le attività ospedaliere, far trapelare informazioni private o mettere a rischio la sicurezza dei pazienti in caso di compromissione dei dispositivi medici.

L'impatto sulla qualità dell'assistenza implica anche una perdita di fiducia nelle istituzioni sanitarie, che potrebbe scoraggiare i pazienti dal condividere informazioni vitali per il loro trattamento. Per questi motivi, mantenere una buona igiene informatica non solo preserva la qualità dell'assistenza, ma garantisce anche la sicurezza dei pazienti e rafforza la fiducia del pubblico.



4. Cosa posso fare come professionista sanitario?

- Utilizzare misure preventive come password complesse e abilitare l'autenticazione a due fattori.
- Aggiornare regolarmente software, app e dispositivi medici.
- Prestare attenzione alle minacce informatiche (e-mail di phishing, link sospetti) e segnalare immediatamente eventuali irregolarità.
- Partecipa alla formazione sulla sicurezza informatica e resta aggiornato su come rispondere agli incidenti e sull'impatto della protezione dei dati dei pazienti.

5. Ulteriori informazioni

5.1 Materiali didattici

- [Cybersecurity for your sector \(JGT-1\)](#).
- [Web seminars about key aspects of cybersecurity \(JGT-3\)](#).
- [Awareness kit about cybersecurity in enterprises \(JGT-4\)](#).
- [Cybersecurity guide for healthcare sector \(EU scope\) \(JGT-7\)](#).
- [Cybersecurity training from National Cryptographic Centre of Spain. Requires National login \(JGT-8\)](#).
- [General training \(71 infopacks\) about cybersecurity descriptions. Provided by cryptographic National centre. \(JGT-10\)](#).
- [An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. \(IST-39\)](#).
- [Educational project on safe and responsible digital use. \(IST-41\)](#).
- [IT Security Requirements and Protective Measures – Tips and Practical Examples \(BBS-42\)](#).
- [An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context \(PRAMMER-31\)](#).
- [Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An overview \(PRAMMER-33\)](#).
- [A Serious Game for Healthcare Industry: Information Security Awareness Training Program for Hospital Universiti Kebangsaan Malaysia \(PRAMMER-34\)](#).
- This learning material highlights the growing role of media in the healthcare and welfare sector for both professional collaboration and client care, including attention to the consequences of media use among vulnerable groups (FIRDA-11)
- Cybersecurity for entities (HIPAA), full pack including checklists (FIRDA-12)
- Video training for professionals and students (FIRDA-14)
- Digital training in cybersecurity, fun and fast questions (FIRDA-15)
- Free e-learning courses on cybersecurity in healthcare (FIRDA-17)
- Free courses to improve digital skills for health care workers (FIRDA-18)
- Online game about cybersecurity, raises awareness. (FIRDA-19)
- Online game about phishing (FIRDA-21)





5.2 Video correlati

Questo video sottolinea l'importanza di mantenere le pratiche di sicurezza fondamentali, quali aggiornamenti software costanti, password robuste e ispezioni regolari del sistema, come misura primaria per salvaguardare le informazioni.

Cos'è la Cyber Hygiene?

https://youtu.be/J_jjI0iTI4I?si=P8wY4Fy7-mWSVWnI

Il seguente video spiega i vari tipi di attacchi informatici e illustra le strategie efficaci di prevenzione dell'igiene informatica.

Nozioni fondamentali sulla sicurezza informatica in ambito sanitario

<https://youtu.be/lqhGqZTiLsk?si=ol7UOkMn1qFvIUq7>

5.3 Link rilevanti

Uno studio su 1.454 episodi di ransomware (2016-2023) ha dimostrato che le organizzazioni con un'igiene informatica inadeguata (D o F) avevano una probabilità 35 volte maggiore di essere attaccate in modo dannoso. Ciò dimostra quanto siano importanti le eccellenti pratiche igieniche.
<https://thehackernews.com/2024/09/healthcares-diagnosis-is-critical-cure.html>

Una solida igiene informatica, come aggiornamenti regolari e controllo degli accessi, è essenziale per proteggere i dati dei pazienti e garantire servizi di assistenza continua, proprio come l'igiene clinica delle mani.
<https://www.cambridgehealth.edu/healthcare-cybersecurity-privacy/healthcare-cybersecurity-privacy-information/cyber-hygiene-the-health-of-healthcare-systems-starts-with-you/>

Secondo i sondaggi, l'utilizzo di password deboli, l'elusione delle norme di sicurezza e la mancanza di una gestione sicura dei dispositivi (come le policy BYOD) aumentano notevolmente il rischio di attacchi informatici; infatti, molti lavoratori antepongono la comodità alla sicurezza.
<https://www.techtarget.com/healthtechsecurity/news/366594401/Employee-Cyber-Hygiene-Is-Critical-to-Healthcare-Cybersecurity>

Gli esperti promuovono l'integrazione dell'igiene informatica nella formazione infermieristica e sanitaria, riconoscendo che dipendenti ben formati rappresentano la prima linea di difesa contro le violazioni che possono mettere a repentaglio l'assistenza ai pazienti.
<https://pubmed.ncbi.nlm.nih.gov/37595324/>





6. Bibliografia

Cyber Hygiene | ENISA. (2018, 18 enero).
<https://www.enisa.europa.eu/topics/cyber-hygiene>

What is Cyber Hygiene? Definition & Best Practices. (2025, 21 marzo).
SecurityScorecard.
<https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/>

World Health Organization. (2025, 26 marzo). WHO/ Europe launches guide to strengthen cybersecurity in digital health.
<https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/>





ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536



Co-funded by
the European Union



ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS
Weser

Questo progetto è stato co-finanziato con il supporto della Commissione Europea. Questa pubblicazione [comunicazione] riflette solo le opinioni dell'autore, e la Commissione non può essere ritenuta responsabile per l'uso che possa essere fatto delle informazioni ivi contenute.

