CYBERSQUATTING

Co-funded by the European Union

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

Partners

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAMMER

eolas

BBS Weser

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

Co-funded by
the European Union

This project has been co-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.

Table of Contents

Co-funded by the European Union

FACTSHEET – CYBERSQUATTING

1. Definition

Cybersquatting is defined as the act of appropriating an internet domain name that is identical or similar to a legitimate one in order to generate traffic1.

2. General importance

Cybersquatting undermines trust and confuses users into believing that they are actually interacting with a legitimate company2. This can result in customers of a legitimate company becoming victims of fraud, data theft, or other forms of harm. Additionally, it can cause an employee to click on the link, which exposes the company's systems to viruses or intrusion by a malicious actor.

Malicious actors can abuse these actions by phishing, spreading malware, or diverting traffic to competitors or fraudulent sites3. In consequence, it erodes customers' trust in digital identity and online commerce and makes companies invest time and resources to reclaim domains.

3. Importance in health and care, and impact in quality of care

In healthcare, fraudulent domains that impersonate official health services may trick patients into sharing sensitive data, downloading harmful files, or paying for medical services4. Consequently, cybersquatting compromises not only patient privacy and safety but also their trust in health institutions by delaying access to accurate health information.

4. What can I do as a healthcare professional?

- Keep an eye on suspicious websites that impersonate your institution's official online presence and report them to your IT.
- Always verify web addresses before sharing personal or medical information online.
- Follow your institution's protocol for safe communication.
- Take part in cybersecurity training and keep up with how to respond to incidents and the impact of patient data protection.

5. More information

5.1 Learning Materials

- Educational project on safe and responsible digital use. (IST-41)
- Research paper on Cybersecurity and critical care staff: A mixed methods study (PRAMMER-29)
- 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)

5.2 Relevant Videos

According to the video, cybersquatting occurs when someone in bad faith registers a domain name that looks like a trademarked brand in order to profit from misleading traffic or infringe on someone else's identity.

What is Cybersquatting? Types of Cybersquatting and Example
https://youtu.be/Y6tmoJDhcFk?si=gCsJUs569M2XXQx7

5. 3 Relevant Links

New Vision Pharmaceuticals is suing BioDose Pharma for registering the domain name glutadose.com, which is a trademarked name they bought in 2021, in bad faith and refusing to give it back.

https://lawstreetmedia.com/news/health/suit-filed-over-domain-name-cybersquatting/

A study of domain oversight found that almost one in three healthcare-related domains in the Netherlands were registered to people or agencies that had nothing to do with them. Some were even typosquatting on legitimate healthcare names.

https://www.sidn.nl/en/news-and-blogs/study-finds-half-of-care-sector-domain-names-have-administrative-issues

Phishing emails used a fake domain called intermountainshealthcare.org, which only had an extra "s" to make it look like the real healthcare provider. This is an example of typosquatting used for bad purposes.

https://www.adrforum.com/DomainDecisions/1966445.htm

6. Bibliography

What Is Cybersquatting? Business Impact and Prevention | Fortinet. (s. f.). Fortinet.

What is Cyber Hygiene? Definition & Best Practices. (2025b, marzo 21). SecurityScorecard.

https://securityscorecard.com/blog/what-is-cyber-hygiene-definition-benefits-best-practices/

WIPO Arbitration and Mediation Center. (2017). En HCA (N.o D2017-1201).

https://www.wipo.int/amc/en/domains/decisions/text/2017/d2017-1201.html

Theocharidou, M., & Lella, I. (2023). ENISA Threat Landscape Report: Health Sector (January 2021 to March 2023).

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

Co-funded by the European Union

This project has been co-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.