CYBERSQUATTING

Co-funded by the European Union

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

Partner

INSTITUTO DE EDUCACION SECUNDARIA
JAVIERGARCIATELLEZ

ISTITUTO DEI SORDI
DI TORINO

Firda

PRAXXER

eolas

BBS Weser

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

Co-funded by the European Union

FACTSHEET - CYBERSQUATTING

1. Definizione

Il cybersquatting è definito come l'atto di appropriarsi di un nome di dominio Internet identico o simile a uno legittimo al fine di creare flusso di utenti.

2. Rilevanza generale

Il cybersquatting mina la fiducia e induce gli utenti a credere di interagire con un'azienda legittima. Questo può far sì che i clienti di un'azienda legittima diventino vittime di frodi, furti di dati o altre forme di danno. Inoltre, può indurre un dipendente a cliccare sul link, esponendo i sistemi dell'azienda a virus o intrusioni da parte di malintenzionati.

Gli autori di attacchi possono abusare di queste azioni tramite phishing, diffusione di malware o dirottamento del traffico verso siti concorrenti o fraudolenti. Di conseguenza, ciò erode la fiducia dei clienti nell'identità digitale e nel commercio online e costringe le aziende a investire tempo e risorse per rivendicare i domini.

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

In ambito sanitario, domini fraudolenti che impersonano servizi sanitari ufficiali possono indurre i pazienti a condividere dati sensibili, scaricare file dannosi o pagare servizi medici. Di conseguenza, il cybersquatting compromette non solo la privacy e la sicurezza dei pazienti, ma anche la loro fiducia nelle istituzioni sanitarie, ritardando l'accesso a informazioni sanitarie accurate.

4. Cosa posso fare come professionista sanitario?

- Tieni d'occhio i siti web sospetti che impersonano la presenza online ufficiale del tuo istituto e segnalali al reparto IT.
- Verificare sempre gli indirizzi web prima di condividere online informazioni personali o mediche.
- Segui il protocollo del tuo istituto per una comunicazione sicura.
- 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

- 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 Video correlati

Secondo il video, il cybersquatting si verifica quando qualcuno in malafede registra un nome di dominio che sembra un marchio registrato, allo scopo di trarre profitto da traffico fuorviante o violare l'identità di qualcun altro.

Cos'è il cybersquatting? Tipi di cybersquatting ed esempi
https://youtu.be/Y6tmoJDhcFk?si=gCsJUs569M2XXQx7

5.3 Link rilevanti

New Vision Pharmaceuticals ha intentato causa contro BioDose Pharma per aver registrato in malafede il nome di dominio glutadose.com, un marchio registrato che hanno acquistato nel 2021, e per essersi rifiutati di restituirlo.
https://lawstreetmedia.com/news/health/suit-filed-over-domain-name-cybersquatting/

Uno studio sulla supervisione dei domini ha rilevato che quasi un dominio su tre relativo all'assistenza sanitaria nei Paesi Bassi era registrato a nome di persone o agenzie che non avevano nulla a che fare con loro. Alcuni addirittura ricorrevano al typosquatting su nomi sanitari legittimi.
https://www.sidn.nl/en/news-and-blogs/study-finds-half-of-care-sector-domain-names-have-administrative-issues

Le email di phishing utilizzavano un dominio falso chiamato intermountainshealthcare.org, con solo una "s" in più per farlo sembrare il vero fornitore di servizi sanitari. Questo è un esempio di typosquatting utilizzato per scopi illeciti.
https://www.adrforum.com/DomainDecisions/1966445.htm

6. Bibliografia

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

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.