CYBERSQUATTI NG

Co-funded by the European Union

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

Socios

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

Co-funded by the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.

CC BY NC

Tabla de Contenidos

Co-funded by the European Union

FACTSHEET – CYBERSQUATTING

1. Definición

El cybersquatting o “ciberocupación”, se define como el acto de apropiarse de un dominio de internet idéntico o similar a uno legítimo para generar tráfico web1.

2. Relevancia general

El cibersquatting reduce la confianza y genera confusión en los usuarios, induciéndoles a pensar que están interactuando con una entidad legítima2. Esto puede resultar en que los clientes de una empresa legítima se conviertan en víctimas de fraude, robo de datos u otras formas de daño. Asimismo, puede inducir a un empleado a hacer clic en el enlace, lo que expone los sistemas de la empresa a virus o a la intrusión de un actor malicioso.

Los agentes maliciosos pueden aprovechar estas acciones mediante técnicas de phishing, la propagación de malware o la desviación de tráfico hacia competidores o sitios fraudulentos3. Como consecuencia, se erosiona la confianza de los clientes en la identidad digital y el comercio en línea, lo que obliga a las empresas a invertir tiempo y recursos en la recuperación de dominios.

3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados

En el sector sanitario, los dominios fraudulentos que se hacen pasar por servicios de salud oficiales pueden engañar a los pacientes para que compartan datos sensibles, se descarguen archivos maliciosos o contraten servicios médicos4. En consecuencia, el cybersquatting compromete no solo la privacidad y la seguridad, sino que también afecta a la confianza en las instituciones sanitarias.

4. ¿Qué puedo hacer como profesional sanitario?

- Vigilar las webs sospechosas que se hacen pasar por la web de tu centro oficial y comunicarlo al equipo informático.
- Verificar las direcciones web antes de compartir información médica o personal de manera online.
- Seguir el protocolo de tu institución para una comunicación segura.
- Realizar formaciones sobre ciberseguridad y mantenerse al día sobre cómo se manifiestan este tipo de ataques en el trabajo diario.

5. Más información

5.1 Materiales de aprendizaje

- 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 Vídeos Relacionados

Este vídeo explica en qué consiste el cybersquatting —la práctica de registrar dominios similares a marcas o nombres de otros con intención de lucro o de perjudicar— y cómo reconocerlo o prevenirlo.

Qué es el cybersquatting? Aprende Ciberseguridad con INCIBE
https://youtu.be/UvmWit3yA68?si=cNzaTGvCQF93lDMY

5. 3 Enlaces Relevantes

El siguiente artículo es un estudio que analiza dominios relacionados con COVID-19. Encuentra muchos dominios “comunes” que podrían ser ilegítimos, algunos usados para desinformación o fines maliciosos.
https://arxiv.org/abs/2102.05290

6. Bibliografía

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

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.

CC BY NC