
# VISHING

Co-funded by
the European Union

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

# Socios







**ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.° 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 la opinión del autor, y la Comisión no se responsabiliza del uso que pueda hacerse de la información que contiene.*

# Tabla de contenido




Co-funded by the European Union

# FACTSHEET – VISHING

## 1. Definición

El vishing consiste en llamadas telefónicas o mensajes de voz fraudulentos diseñados para engañar a las víctimas y obtener información confidencial, como credenciales de inicio de sesión, números de tarjetas de crédito o datos bancarios. A menudo se hacen pasar por organizaciones de buena reputación (como el banco de la víctima, el IRS o un servicio de entrega de paquetes) y realizan llamadas telefónicas inesperadas.

## 2. Importancia general

La eficacia del vishing se debe a que elude las protecciones digitales, como los filtros de spam, y se basa en la interacción verbal directa, lo que dificulta su detección.[1] Además, al explotar la psicología humana, las víctimas pueden sentirse presionadas a obedecer durante una llamada telefónica.

Hoy en día, los grandes avances de la IA incluyen el refinamiento de la clonación de voz. Esto, junto con el uso de técnicas como la suplantación de identidad de llamadas, hace que el vishing sea más sofisticado y peligroso, y aumenta los riesgos para empresas y particulares en todo el mundo.

### 3. Importancia en la salud y la atención, e impacto en la calidad de la atención

En el ámbito sanitario, las consecuencias del vishing incluyen el acceso a registros médicos electrónicos, datos de pacientes o sistemas internos, lo que puede derivar en robo de identidad, facturación fraudulenta e interrupción de los servicios médicos3.

Al igual que otros ciberataques, las filtraciones causadas por vishing pueden provocar violaciones de la privacidad, retrasos en la atención médica, pérdidas financieras y una menor confianza en las instituciones médicas. Los ataques de vishing exitosos debilitan la resiliencia de las instituciones sanitarias a gran escala, lo que genera menos confianza en la seguridad de los datos médicos confidenciales.

## 4. ¿Qué puedo hacer como profesional sanitario?

Verifique la identidad de la persona que llama antes de compartir cualquier dato confidencial del paciente.

- Siga el protocolo de su institución para una comunicación segura.
- Los atacantes crean urgencia como táctica de presión. Haga una pausa y confirme con sus contactos oficiales antes de actuar.
- Participe en la capacitación sobre ciberseguridad y manténgase al día sobre cómo responder ante incidentes y el impacto de la protección de datos de los pacientes.

## 5. Más información

### 5.1 Materiales de aprendizaje

- Cybersecurity for your sector (JGT-1)
- Sequential videos for general topics about cybersecurity (JGT-2)
- Awareness kit about cibersecurity in enterprises (JGT-4)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- Interactive learning environment to develop cybersecurity skills. Requires national identification (JGT-9)
- General training (71 infopacks) about cibersecurity descriptions. Provided by cryptographic National centre. (JGT-10)
- 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 relevantes

El video muestra cómo los hackers usan el "vishing" para engañar a las personas y conseguir que les den información privada. Es una forma de hackear sin tecnología, pero muy efectiva.

| **Hack Attack - Vishing** |
| --- |
| https://youtu.be/BEHl2lAuWCk?si=Akl5CQz7ESeai6Cd |

En este vídeo, podemos ver los peligros de las falsificaciones de voz con IA en la atención médica y qué medidas podemos tomar para prevenir el "vishing".

| **The Threat of AI Voice Deepfakes in Healthcare** |
| --- |
| https://youtu.be/oeQWGgfaqqc?si=0f2Z6Bt6L4dYNCOm |

### 5. 3 Enlaces relevantes

Hackers pretending to be employees of Spectrum Health or Priority Health used fake caller IDs to get patients to give them protected health information (PHI), like member numbers.
https://compliancy-group.com/vishing-attack-targets-spectrum-health-patients/

VUMC said that staff were targeted by deepfake vishing attacks, which used AI-generated voices to sound like coworkers or bosses. This made the scams more believable and dangerous.
https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/vumc-sounds-alarm-on-vishing-attacks/

The American Hospital Association (AHA) warned of calls where people pretended to be Medicare representatives in order to get hospital executives to give them Social Security Numbers.
https://www.aha.org/news/headline/2015-02-03-aha-advises-hospitals-be-alert-potential-vishing-attacks

## 6. Bibliografía

Secure Email Threat Defense demo. (2025, 10 abril). Cisco.
https://www.cisco.com/site/us/en/learn/topics/security/what-is-vishing.html#:~:text=Vishing%2C%20short%20for%20voice%20phishing%2C%20refers%20to%20fraudulent%20phone%20calls,card%20numbers%2C%20or%20bank%20details

IOCTA, Internet Organised Crime Threat Assessment 2023. (2023). Europol.
https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf

Alder, S. (2022, 23 agosto). HC3 Warns of Increase in Vishing Attacks and the Dangers of Social Engineering. The HIPAA Journal.
https://www.hipaajournal.com/hc3-warns-of-increase-in-vishing-attacks-and-the-dangers-of-social-engineering/


**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.


**ESCAPE. Preparación de profesionales sanitarios ante ciberataques. Proyecto n.° 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 la opinión del autor, y la Comisión no se responsabiliza del uso que pueda hacerse de la información que contiene.