VISHING

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

1. Definition 1
2. General Importance 1
3. Importance in Health and Care, and Impact on Quality of Care 1
4. What Can I Do as a Healthcare Professional? 1
5. More Information
    1. Learning Materials 2
    2. Relevant Videos 2
    3. Relevant Links 3
6. Bibliography 3

Co-funded by the European Union

FACTSHEET – VISHING

1. Definition

Vishing are fraudulent phone calls or voice messages designed to trick victims into providing sensitive information, like login credentials, credit card numbers, or bank details. They often pretend to be reputable organisations (such as the victim's bank, the IRS, or a package delivery service) and make unexpected phone calls1.

2. General importance

Vishing's effectiveness is determined by the fact that it bypasses digital safeguards like spam filters and relies on direct verbal interaction, which makes it harder to detect1. Moreover, as it exploits human psychology, victims may feel pressured to comply during a phone call.

Nowadays, great advances with AI include voice-cloning refinement. This, along with the use of techniques like caller ID spoofing, makes vishing more sophisticated and dangerous and amplifies risks for businesses and individuals worldwide2.

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

In healthcare, consequences of vishing include gaining access to electronic health records, patient data, or internal systems, which may lead to identity theft, fraudulent billing, and disruption of medical services3.

Like other cyberattacks, breaches caused by vishing can result in privacy violations, delays in care, financial losses, and reduced trust in medical institutions. Successful vishing attacks weaken the resilience of healthcare institutions on a larger scale, which makes people less sure that sensitive medical data is safe.

4. What can I do as a healthcare professional?

- Verify the caller's identity before sharing any sensitive patient data.
- Follow your institution's protocol for safe communication.
- Attackers create urgency as a pressure tactic. Pause and confirm with official contacts before acting.
- 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

- 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 Relevant Videos

The video shows how hackers use "vishing" to trick people into giving them private information. This is a tech-free but very effective way to hack.

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

In this video, we can watch the dangers of AI voice deepfakes in healthcare and what measures we can take to prevent “vishing”.

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

5. 3 Relevant Links

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. Bibliography

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%2023%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.