VISHING

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

PRAMMER

eolas

BBS Weser

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

Co-funded by
the European Union

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission kofinanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Informationen.

Inhaltsverzeichnis

Co-funded by the European Union

FACTSHEET – VISHING

1. Definition

Vishing sind betrügerische Telefonanrufe oder Sprachnachrichten, die darauf abzielen, Opfer zur Herausgabe vertraulicher Informationen wie Anmeldedaten, Kreditkartennummern oder Bankdaten zu verleiten. Oft geben sich die Opfer als seriöse Organisationen aus (z. B. die Bank des Opfers, das Finanzamt oder ein Paketdienst) und tätigen unerwartete Anrufe.1.

2. Allgemeine Bedeutung

Die Effektivität von Vishing beruht darauf, dass es digitale Schutzmechanismen wie Spamfilter umgeht und auf direkter verbaler Interaktion beruht, was es schwieriger macht, es zu erkennen1Da zudem die menschliche Psyche ausgenutzt wird, können sich die Opfer während eines Telefongesprächs unter Druck gesetzt fühlen, zu kooperieren.

Zu den großen Fortschritten in der KI gehört heute die Verfeinerung des Voice-Clonings. Dies, zusammen mit dem Einsatz von Techniken wie Caller-ID-Spoofing, macht Vishing raffinierter und gefährlicher und erhöht die Risiken für Unternehmen und Einzelpersonen weltweit.2.

3. Bedeutung für Gesundheit und Pflege und Auswirkungen auf die Pflegequalität

Im Gesundheitswesen können Vishing-Angriffe unter anderem den Zugriff auf elektronische Gesundheitsakten, Patientendaten oder interne Systeme zur Folge haben, was zu Identitätsdiebstahl, betrügerischer Abrechnung und Störungen der medizinischen Versorgung führen kann.3.

Wie andere Cyberangriffe können auch Vishing-Angriffe zu Datenschutzverletzungen, Behandlungsverzögerungen, finanziellen Verlusten und einem Vertrauensverlust in medizinische Einrichtungen führen. Erfolgreiche Vishing-Angriffe schwächen die Widerstandsfähigkeit von Gesundheitseinrichtungen erheblich, was die Sicherheit sensibler medizinischer Daten schwächt.

4. Was kann ich als medizinisches Fachpersonal tun?

- Überprüfen Sie die Identität des Anrufers, bevor Sie vertrauliche Patientendaten weitergeben.
- Befolgen Sie das Protokoll Ihrer Institution für eine sichere Kommunikation.
- Angreifer erzeugen Dringlichkeit, um Druck auszuüben. Halten Sie inne und bestätigen Sie dies mit offiziellen Kontakten, bevor Sie handeln.
- Nehmen Sie an Schulungen zur Cybersicherheit teil und bleiben Sie auf dem Laufenden, wie Sie auf Vorfälle reagieren und welche Auswirkungen der Schutz von Patientendaten hat.

5. Weitere Informationen

5.1 Lernmaterialien

- Cybersicherheit für Ihre Branche (JGT-1)
- Aufeinanderfolgende Videos zu allgemeinen Themen der Cybersicherheit (JGT-2)
- Sensibilisierungspaket zur Cybersicherheit in Unternehmen (JGT-4)
- Leitfaden zur Cybersicherheit im Gesundheitswesen (EU-Geltungsbereich) (JGT-7)
- Interaktive Lernumgebung zur Entwicklung von Cybersicherheitskompetenzen. Erfordert einen nationalen Ausweis (JGT-9).
- Allgemeine Schulung (71 Infopakete) zu Cybersicherheitsbeschreibungen. Angeboten vom Nationalen Kryptographiezentrum. (JGT-10)
- Bildungsprojekt zur sicheren und verantwortungsvollen digitalen Nutzung. (IST-41)
- Forschungsarbeit zum Thema Cybersicherheit und Intensivpflegepersonal: Eine Mixed-Methods-Studie (PRAMMER-29)
- Gamifizierung und Serious Games zur Sensibilisierung für Cybersicherheit und zur Ausbildung von Ersthelfern: Ein Überblick (PRAMMER-33)
- Ein Serious Game für die Gesundheitsbranche: Informationssicherheits-Sensibilisierungstraining für das Krankenhaus Universiti Kebangsaan Malaysia (PRAMMER-34)
- Videotraining für Fachleute und Studierende (FIRDA-13)

5.2 Relevante Videos

Das Video zeigt, wie Hacker „Vishing“ nutzen, um Menschen dazu zu bringen, ihnen private Informationen preiszugeben. Dies ist eine technikfreie, aber sehr effektive Methode zum Hacken.

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

In diesem Video erfahren wir mehr über die Gefahren von AI Voice Deepfakes im Gesundheitswesen und welche Maßnahmen wir ergreifen können, um „Vishing“ zu verhindern.

Die Bedrohung durch AI Voice Deepfakes im Gesundheitswesen
https://youtu.be/oeQWGgfaqqc?si=0f2Z6Bt6L4dYNCOm

5. 3 Relevante Links

Hacker gaben sich als Mitarbeiter von Spectrum Health oder Priority Health aus und nutzten gefälschte Anrufer-IDs, um Patienten dazu zu bringen, ihnen geschützte Gesundheitsinformationen (PHI) wie etwa Mitgliedsnummern preiszugeben.
https://compliancy-group.com/vishing-attack-targets-spectrum-health-patients/

Laut VUMC wurden Mitarbeiter Opfer von Deepfake-Vishing-Angriffen. Dabei wurden KI-generierte Stimmen verwendet, um die Stimme von Kollegen oder Vorgesetzten zu simulieren. Dies machte die Betrügereien glaubwürdiger und gefährlicher.
https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/vumc-sounds-alarm-on-vishing-attacks/

Die American Hospital Association (AHA) warnte vor Anrufen, bei denen sich Personen als Medicare-Vertreter ausgaben, um von der Krankenhausleitung die Herausgabe ihrer Sozialversicherungsnummer zu erzwingen.
https://www.aha.org/news/headline/2015-02-03-aha-advises-hospitals-be-alert-potential-vishing-attacks

6. Literaturverzeichnis

Demo zur sicheren E-Mail-Bedrohungsabwehr. (10. April 2025). 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, Bedrohungsbewertung der organisierten Kriminalität im Internet 2023. (2023).Europol.
https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf

Alder, S. (23. August 2022). HC3 warnt vor zunehmenden Vishing-Angriffen und den Gefahren von Social Engineering.Das 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

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission kofinanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung [Mitteilung] trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Informationen.