

FICHE CYBER

Le *vishing*, technique d'ingénierie sociale

Statut : **En cours**

Secteurs affectés : **Tous**

Zones géographiques touchées : **Monde**

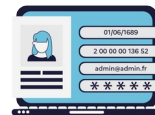
Objectif : **Accès à des données sensibles**



Contact par
téléphone



Création d'une
urgence



Accès à des
données sensibles

SYNTHÈSE

Le *vishing* est une technique d'attaque de plus en plus fréquemment utilisée par les cybercriminels. Elle repose sur la manipulation psychologique et l'urgence afin de tromper la vigilance des victimes. En utilisant l'ingénierie sociale, le *vishing* permet l'obtention de données sensibles ainsi que l'installation de maliciels à l'insu de l'utilisateur, pouvant conduire à une compromission des terminaux numériques de la victime.

I. De quoi parle-t-on ?

Le *vishing* (de l'anglais *voice phishing* ou « hameçonnage vocal ») est une technique d'ingénierie sociale, qui leurre les victimes, en les incitant à divulguer des informations sensibles ou à installer un logiciel malveillant sur leur poste informatique. Les cybercriminels créent délibérément des conditions d'urgence afin de pousser les victimes peu méfiantes à céder volontairement de précieuses informations personnelles, telles que leur nom, prénom, adresse, numéro de téléphone ou numéro de carte bancaire.

Grâce à ces informations, les cybercriminels peuvent initier des opérations frauduleuses ou usurper l'identité des victimes. Le *vishing* prospère lorsque les cybercriminels ont un minimum d'informations concernant les centres d'intérêts de l'utilisateur. Ils exploitent ces connaissances pour créer un sentiment d'urgence impliquant un problème chez la victime, puis ils interviennent en proposant une solution simple et en se montrant apaisants.

II. Exemples concrets d'escroqueries par l'utilisation du *vishing*



Arnaques à l'assistance technique : les attaquants usurpent généralement l'identité d'un employé du service informatique. L'acteur affirme que l'ordinateur de la victime est compromis et tente de convaincre cette dernière de lui accorder un accès à distance ou de le payer pour débloquer l'ordinateur.



Arnaques à l'usurpation d'identité bancaire : les fraudeurs se font passer pour des conseillers bancaires en expliquant qu'ils ont détecté une activité suspecte sur le compte bancaire de la victime. L'attaquant demande généralement des informations sensibles, telles que des mots de passe ou des PIN, au motif de sécurisation du compte, ce qui entraîne des fraudes bancaires.



Arnaques à la livraison : les attaquants usurpent l'identité d'un service de livraison en affirmant qu'il y a un problème avec une livraison de colis. Des informations personnelles ou de paiement sont demandées à la victime pour résoudre celui-ci. Les escrocs exploitent ensuite ces informations pour réaliser une fraude.

III. Mode opératoire



1. COLLECTE D'INFORMATIONS

Le cybercriminel collecte des informations sur la future victime via ses réseaux sociaux, Internet ou des bases de données fuitées.



2. CONTACT PAR TÉLÉPHONE

L'attaquant contacte la victime par un appel audio. Il usurpe l'identité d'une personne ou d'une organisation de confiance (banque, support informatique, etc).



3. CRÉATION D'UNE URGENCE

L'acteur peut prétexter un problème urgent, comme une faille de sécurité, un paiement en retard ou un problème avec le compte de la victime.



6. COMPROMISSION DU POSTE

Dans certains cas, l'acteur malveillant peut également pousser la victime à installer un logiciel tiers pour compromettre la machine de la victime et dérober des documents personnels.



5. UTILISATION DES INFORMATIONS

Une fois que la victime a fourni les informations demandées, le cybercriminel les utilise pour commettre une escroquerie financière ou usurper son identité.



4. OBTENTION DE DONNÉES SENSIBLES

L'acteur incite la victime à lui fournir des informations sensibles (identifiants, codes personnels, mots de passe, informations bancaires).

Comment s'en protéger ?

Éducation et sensibilisation : la première ligne de défense contre le *vishing* est la vigilance. Aucune organisation légitime ne sollicite ses clients pour obtenir des données sensibles par téléphone sans vérification préalable. Les escrocs tentent souvent de créer un sentiment d'urgence, affirmant qu'une action immédiate est nécessaire. Il convient de ne jamais divulguer d'informations sensibles par téléphone. Il est également important pour les entreprises de sensibiliser leurs employés aux différentes techniques existantes d'ingénierie sociale.

Vérification du numéro : si le numéro affiché semble douteux (masqué, inconnu, parfois international) ou si la qualité de l'appel est mauvaise (son médiocre, coupures ou un accent inhabituel), il est nécessaire de se méfier.

Utilisation de logiciels de sécurité : opter pour des solutions de sécurité telles que le filtrage des appels, l'installation de logiciels antivirus et de protection des données.

Authentification forte : définir des mots de passe robustes et mettre en place un double facteur d'authentification (code envoyé par SMS ou un jeton d'authentification).