Qu'est-ce que l'hameçonnage vocal?

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Juillet 2022 | ITSAP.00.102

L'hameçonnage vocal est un type de piratage psychologique qui met à profit les technologies de communication vocale. Dans une attaque d'hameçonnage vocal, les auteurs de menace (ou hameçonneurs) se servent de numéros de téléphone obtenus frauduleusement, de logiciels de modification vocale et d'autres techniques de piratage psychologique pour inciter les gens à divulguer, au téléphone, des renseignements personnels et privés. Les attaques sophistiquées d'hameçonnage vocal exploitent la technologie de voix sur IP pour créer de faux numéros de téléphone et masquer l'identité de l'appelant de sorte que l'appel semble provenir d'entreprises ou d'institutions légitimes. La voix sur IP facilite la tâche des hameçonneurs, car elle leur permet d'automatiser des centaines d'appels frauduleux sur Internet et complique le retraçage des numéros utilisés.

Comment fonctionne l'hameçonnage vocal?

1. Collecte de données

Les hameçonneurs ont recours à différentes techniques pour mettre la main sur des listes de numéros de téléphone qu'ils utiliseront dans leurs attaques d'hameçonnage vocal de masse lancées à l'aveugle. Parfois, ils effectuent des recherches sur leurs victimes (des personnes ou des organisations) et amassent de l'information sur elles afin de mener des attaques personnalisées.

Fouille de poubelles
Les hameçonneurs récupèrent dans les poubelles des listes de numéros de téléphone jetées par une banque ou une organisation.

Attaque par composition automatique
Les hameçonneurs appelent automatiquement tous les numéros de téléphone d'un indicatif régional donné afin de trouver les numéros actifs.

Recherche Internet
Les hameçonneurs fouillent Internet (YouTube, réseaux de médias sociaux) pour s'approprier des échantillons de voix d'une cible de grande valeur (p. ex., le PDG d'une entreprise).

Violation de données
Les hameçonneurs se procurent des listes de numéros de téléphone volés auprès d'autres escrocs qui ont profité de brèches de données.

2. Manipulation vocale

Les hameçonneurs se servent de l'apprentissage automatique, une branche de la technologie de l'intelligence artificielle, pour simuler la voix d'une personne. Cette technique, appelée **clonage vocal**, ajoute du réalisme à une attaque d'hameçonnage vocal, car elle permet aux hameçonneurs de dissimuler leur voix et de se faire passer pour une personne que la victime connait ou en qui elle a confiance (p. ex., un collègue ou son patron).

3. Appel frauduleux

Les hameçonneurs masquent leur numéro de téléphone, appellent le plus grand nombre de numéros possible et laissent un message vocal préparé dans lequel ils demandent à la victime de rappeler. Dans le cadre d'une attaque sophistiquée, les hameçonneurs se servent d'un logiciel de **synthèse vocale** pour dissimuler leur identité (accent, sexe ou âge) ou pour contrôler la voix clonée d'une cible de grande valeur durant l'appel.

Exemples d'arnaques par hameçonnage vocal

L'objectif de l'hameçonnage vocal est de convaincre la victime de dévoiler des données confidentielles, comme un numéro d'identification personnel, son numéro d'assurance sociale, ses numéros de cartes de crédit ou les mots de passe de ses comptes. Les données servent à réaliser de la fraude d'identité, à effectuer des opérations financières non autorisées ou à obtenir accès à des comptes professionnels ou personnels. La liste ci-dessous donne quelques exemples communs d'hameçonnage vocal :

Hameçonnage vocal aux fins de vol de justificatifs d'identité. Les hameçonneurs se servent de cette méthode pour mettre la main sur de l'information bancaire ou relative aux cartes de crédit. Ils vont employer les justificatifs compromis pour accéder aux comptes, prendre de l'argent ou faire des achats non autorisés.

Personnification d'un fonctionnaire. Les hameçonneurs se font faussement passer pour des fonctionnaires qui sont, le plus souvent, à l'emploi de ministères responsables des impôts et des finances personnelles. Ils sèment la peur chez les personnes visées et les convainquent qu'elles doivent payer divers frais, comme des impôts impayés, sinon elles risquent de subir des conséquences juridiques.
Ils se font aussi passer pour des membres des forces de l'ordre et demandent aux victimes de leur fournir des renseignements personnels qu'ils utiliseront à des fins de fraude d'identité.

Extorsion commerciale. Se faisant passer pour un patron ou le PDG d'une entreprise, les hameçonneurs convainquent la victime d'obtempérer à la demande du patron (débloquer des fonds, approuver les autorisations d'accès aux systèmes sensibles, etc.).

Escroquerie par télémarketing. Les hameçonneurs personnifient des spécialistes du télémarketing ou des représentants d'une entreprise et annoncent à la personne visée qu'elle a gagné un concours, mais qu'elle doit payer des frais de rachat ou fournir les informations de sa carte de crédit pour réserver son prix.

Escroquerie du soutien technique. Les hameçonneurs se présentent comme des employés de soutien technique de différentes organisations puis demandent à la victime de dévoiler des renseignements personnels ou liés au travail pour vérifier son identité.
Ils peuvent même aller jusqu'à demander la permission d'accéder à un dispositif à distance pour aider à installer un logiciel. Ce faisant, ils peuvent télécharger sur le dispositif des maliciels qui font apparaître des messages d'erreur dans le but d'inciter la victime à appeler un numéro pour faire régler des problèmes techniques ou de sécurité.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Qu'est-ce que l'hameçonnage vocal?

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Juillet 2022 | ITSAP.00.102

Conseils pour repérer l'hameçonnage vocal et éviter de tomber dans le piège

- **Méfiez-vous des appelants qui sollicitent de l'information sensible.** Ne révélez jamais au téléphone des renseignements personnels comme des noms d'utilisateur, des mots de passe ou de l'information bancaire, sauf si vous êtes absolument sûr qu'il s'agit d'une institution légitime. Demandez à l'appelant de vous donner le nom d'une personne-ressource et communiquez vous-même avec l'organisation en question par les canaux officiels (numéro de téléphone public ou site Web).
- **Faites attention aux appels provenant de numéros inconnus ou aux appels automatisés.** Si vous ne reconnaissez pas le numéro, ne répondez pas à l'appel et laissez-le passer à la messagerie vocale. N'utilisez pas la fonction de rappel du téléphone et ne rappelez pas au numéro fourni par l'appelant. Communiquez plutôt avec le site ou le service par une méthode éprouvée.
- **Méfiez-vous des tactiques pour semer la peur**. Les hameçonneurs tentent de vous coincer et de vous faire croire que vous n'avez d'autre choix que de fournir l'information voulue. Ils peuvent même adopter un ton menaçant pour vous presser d'agir. Par exemple, ils peuvent prétendre qu'à défaut de fournir l'information demandée, le compte sera désactivé.
- **Méfiez-vous des appels qui ont une mauvaise qualité audio** ou des appelants qui ont un ton robotisé ou un rythme de la parole saccadé. Raccrochez. Si la personne rappelle, ne répondez pas et attendez qu'elle vous laisse un message vocal.
- **Allez au-devant des coups et sensibilisez les membres du personnel aux attaques d'hameçonnage** vocal pour qu'ils sachent comment y réagir adéquatement. Mettez en place un processus de signalement d'incidents facile et rapide. Songez à instaurer un processus officiel au moyen duquel les employés doivent s'authentifier avant de discuter entre eux d'information sensible au téléphone.
- **Sachez que la plupart des téléphones intelligents offrent des fonctions intégrées de protection** pour filtrer, bloquer ou signaler des appels indésirables. Consultez le manuel de votre téléphone intelligent pour savoir comment activer ces fonctions.

Les Fraudeurs Tentent D'Obtenir :

Votre Identité, vos Mots de Passe ou Votre Argent

L'hameçonnage vocal peut faire partie d'une attaque par hameçonnage à grande échelle, une autre technique de piratage psychologique qui vise à soutirer de l'argent ou de l'information à des personnes ou à des organisations.

Pour en apprendre davantage sur l'hameçonnage, consultez sur notre site Web le document Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101).

NORMES STIR/ SHAKEN

STIR signifie **Secure Telephony Identity Revisited** (nouvelle approche relative à la sécurité de l'identité de l'appelant). SHAKEN signifie **Signature-based Handling of Asserted information using tokens** (traitement de l'information fournie en fonction de la signature au moyen de jetons). Le 30 novembre 2021, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) a ordonné à tous les fournisseurs de services de télécommunications au Canada de mettre en œuvre cette nouvelle technologie pour authentifier et vérifier les appels vocaux sur protocole IP.

Qu'est-ce que cela signifie?

Grâce aux normes STIR/SHAKEN, les compagnies de téléphone peuvent déterminer si un appel provient d'une source légitime et sont ainsi mieux outillées pour avertir les clients en cas d'appels indésirables. Les clients peuvent ainsi décider, en toute connaissance de cause, de répondre ou non à un appelant inconnu.

Plus le nombre de compagnies de téléphone appliquant les normes STIR/SHAKEN est élevé, plus le volume d'appels indésirables sur protocole IP devrait réduire.

Que faire après avoir été victime d'hameçonnage vocal

Si vous avez été victime d'hameçonnage vocal, prenez les mesures suivantes.

Informez les institutions financières responsables des comptes compromis. Demandez-leur d'annuler les opérations frauduleuses et de bloquer toute future transaction.

Changez immédiatement les mots de passe de tous vos comptes touchés et de ceux qui sont protégés par ces mêmes mots de passe.

Surveillez vos comptes financiers. Songez à vous inscrire à un service de surveillance du crédit qui vous informera de toute éventuelle activité frauduleuse. Cette mesure est particulièrement importante si vous croyez avoir été victime de vol d'identité.

Signalez l'escroquerie au Centre antifraude du Canada. Prenez en note le numéro de téléphone du fraudeur ainsi que les sites Web qu'il vous a demandé de visiter et fournissez cette information au Centre antifraude du Canada (antifraudcentre-centreantifraude.ca).

Signalez l'incident à l'administrateur des TI de votre organisation si vous croyez avoir compromis de l'information sensible appartenant à l'organisation. Pour ce faire, suivez le protocole mis en place par l'organisation pour le signalement des incidents de cybersécurité.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada