La technologie au service des escroqueries par téléphone

Pauline Meyer, le 30 décembre 2024

Le 7 novembre 2024, l'OFCS a publié dans un rapport son analyse des escroqueries par téléphone signalées ces derniers mois dans le domaine cyber.

Office fédéral de la cybersécurité, Les escroqueries par téléphone dans le domaine cyber, 7 novembre 2024

Avez-vous également reçu récemment un appel avec une voix (automatique ou non) venant de prétendument de « la police fédérale de Berne » qui requiert que vous acceptiez l'appel en raison d'une poursuite pénale ? Nous sommes malheureusement de nombreuses personnes à recevoir ce genre de coups de téléphone.

L'Office fédéral de la cybersécurité (OFCS) publie le 7 novembre 2024 son rapport semestriel 2024/I pour la période de janvier à juin de cette année. Dans son rapport, il fait état de la forte augmentation de signalements au sujet des escroqueries par téléphone (ces escroqueries ont fait l'objet de 23'104 cyberincidents signalés sur les 34'789 annoncés à l'office durant le premier semestre de 2024). Compte tenu de l'importance de ce phénomène à l'heure actuelle, l'OFCS se penche plus en profondeur sur ce type de fraude et publie un rapport séparé.

Le rapport de l'OFCS débute avec une clarification terminologique. L'escroquerie (art. 146 CP) est le terme juridique qui désigne le délit selon lequel une personne poursuivant un dessein d'enrichissement illégitime induit en erreur par une tromperie astucieuse une personne et la détermine à des actes préjudiciables à ses intérêts pécuniaires (ou à ceux d'un tiers). La fraude est un terme plus général et l'arnaque est un terme similaire informel.

L'escroquerie par téléphone est répandue, l'oralité permettant la création d'une relation de confiance ainsi que la manipulation immédiate de la personne dupée. L'évolution des technologies permet aux délinquants de combiner l'oralité au domaine cyber, de peaufiner leurs techniques et d'exploiter les données obtenues pour en dégager du profit.

La combinaison entre les nouvelles technologies et les escroqueries par téléphone ne sont pas nouvelles. La technologie Voix sur IP (*Voice over IP, VoIP*) existait déjà dans les années

2000 pour créer de faux numéros de téléphone et masquer l'identité de l'appelant, afin de faire croire qu'un appel provient d'une entité légitime. Ces techniques permettent d'automatiser des centaines d'appels frauduleux et d'entraver le retraçage des numéros utilisés.

Depuis, de nombreuses possibilités sont offertes par les technologies avant, pendant ou après les tentatives d'escroquerie. L'utilisation des technologies peut servir pour différents types d'escroquerie :

- L'appel automatisé (*robocall*), par lequel les délinquants diffusent massivement des messages émanant prétendument d'organisations légitimes, permet de limiter les ressources humaines nécessaires et de se concentrer ensuite sur les personnes qui restent en ligne après avoir entendu l'appel automatisé. Depuis l'été 2023, des escrocs appellent quotidiennement et de manière automatisée (par des *bots*) des milliers de personnes en Suisse, se faisant passer pour une autorité de police qui accuse la victime d'un délit. La victime doit appuyer sur une touche pour obtenir plus d'informations, après quoi les délinquants tentent de soustraire des données ou à installer des logiciels sur leur smartphone, ce qui leur permet d'accéder par exemple aux comptes bancaires en ligne.
- L'usurpation du numéro de téléphone (*spoofing*) par laquelle les délinquants falsifient l'identifiant de l'appelant pour afficher un numéro de téléphone légitime, ce qui peut inciter la dupe à répondre. De nombreux cas impliquant l'usurpation de numéros de téléphone de banques ou d'autorités de police ont été recensés par l'OFCS. Dans les cas de *robocall* recensés par l'OFCS, les escrocs usurpent fréquemment des numéros de téléphone.
- L'incitation à l'appel, par les criminels qui envoient un message audio enregistré, par exemple à différents employés d'une entreprise. Ce message cherche à faire passer l'appelant pour une personne de confiance interne à l'organisation et contient souvent un message urgent en demandant de rappeler.

Les délinquants utilisent désormais également des logiciels malveillants (logiciels d'hameçonnage vocal) qui implantent des messages vocaux préenregistrés, redirigent les appels du téléphone infecté vers des centres d'appel d'escrocs et requiert, une fois les applications téléchargées, l'autorisation d'accéder aux contacts, à l'appareil photo, au microphone ou encore à la géolocalisation de l'appareil.

D'autres avancées technologiques sont exploitées, à l'instar de l'utilisation des eSIM (pour prendre le contrôle du numéro de téléphone de leurs victimes et intercepter les codes de

sécurité envoyés lors d'authentification multifactorielle) ou de l'intelligence artificielle (pour automatiser les appels ou générer des voix).

Le rapport de l'OFCS se poursuit avec une analyse de la situation du côté des fournisseurs de services de télécommunication. À l'heure actuelle, ceux-ci ne peuvent pas (ni juridiquement ni techniquement) reconnaître les *robocalls* recourant à l'intelligence artificielle à partir du contenu, de la langue ou de la voix utilisée. En exploitant des alertes automatisées et respectueuses de la vie privée, ils pourraient néanmoins prendre les contre-mesures appropriées.

Ils peuvent en revanche implémenter des solutions de filtrage pour identifier et bloquer les numéros suspectés d'être utilisés pour des escroqueries (art. 45a LTC), recourir à la reconnaissance vocale pour authentifier les appelants (en particulier pour les interactions sensibles), détecter par des algorithmes des schémas d'appel inhabituels ou des comportements indiquant des tentatives d'attaques, ou encore sensibiliser la population.

Plus généralement, les infractions d'escroquerie (art. 146 CP) comme d'usurpation d'identité (art. 179^{decies} CP) peuvent en parallèle être invoquées devant les autorités de poursuite pénale en fonction des cas.

Actuellement, une initiative entre l'OFCOM et les fournisseurs existe pour trouver une solution à l'échelle du secteur, permettant de lutter contre ce défi complexe que constituent les appels frauduleux.

Finalement, le rapport de l'OFCS se conclut avec la recommandation de mesures pour la population, dans la mesure où l'humain au bout du fil reste souvent le maillon faible dans ces attaques. Il rappelle à ce titre notamment de ne pas faire confiance à tous les appelants et de ne pas se laisser intimider par ceux-ci, ainsi que de ne jamais révéler d'informations professionnelles à des inconnus.

Proposition de citation : Pauline Meyer, La technologie au service des escroqueries par téléphone, 30 décembre 2024 *in* www.swissprivacy.law/330

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.