7 novembre 2024 | Office fédéral de la cybersécurité OFCS

Les escroqueries par téléphone dans le domaine cyber

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS
Office fédéral de la cybersécurité OFCS

Table des matières

1 Introduction

Les utilisateurs de téléphonie font fréquemment face à des appels frauduleux cherchant à les escroquer. Cependant, ce phénomène criminel n'est pas nouveau. Depuis des dizaines d'années déjà, des criminels tentent de manipuler d'autres personnes à des fins pécuniaires. Se pose dès lors les questions de savoir comment se déroulent ces escroqueries, ainsi que pourquoi, grâce à l'évolution de la technologie, tout un chacun se retrouve de plus en plus souvent confronté à ce genre d'appels indésirables, de plus en plus difficiles à déceler. Finalement, il convient aussi de se poser la question de savoir quelles sont les mesures prises par les fournisseurs de télécommunications et par le régulateur.

1.1 Différence entre escroquerie, fraude et arnaque

Le grand public fait souvent référence à des « arnaques téléphoniques ». Le terme d'arnaque est le terme informel qui désigne généralement une fraude ou une tromperie visant à duper une personne ou un groupe pour obtenir de l'argent, des biens ou des services.

L'escroquerie est le terme juridique utilisé par la loi (*cf. infra*) pour désigner ce délit. Il existe un troisième terme, la fraude, qui est également souvent utilisé dans ce contexte.

Art. 146 Code Pénal Suisse (Escroquerie)

Quiconque, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, induit astucieusement en erreur une personne par des affirmations fallacieuses ou par la dissimulation de faits vrais ou la conforte astucieusement dans son erreur et détermine de la sorte la victime à des actes préjudiciables à ses intérêts pécuniaires ou à ceux d'un tiers, est puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire.

La différence entre l'escroquerie et la fraude réside dans le fait que l'escroquerie implique principalement des manœuvres trompeuses (telles que les mensonges, faux documents ou l'usurpation d'identité), alors que la fraude est un terme plus général, qui comprend toute action malhonnête, pouvant inclure tout ce qui est plus subtile, comme des omissions ou des déclarations trompeuses sans manœuvres plus complexes.

1.2 L'escroquerie par téléphone en lien avec le domaine cyber

L'escroquerie par téléphone est répandue, car l'oralité permet de créer une relation de confiance et de manipuler de manière ciblée l'interlocuteur. En effet les criminels peuvent réagir immédiatement et de manière adéquate au potentiel doute exprimé par la victime. Ils finissent par leur soutirer de l'argent ou des informations personnelles ou sensibles en se faisant passer pour une entité légitime, telle qu'une banque, un client, une autre entreprise, un service gouvernemental, voire une personne interne à une entreprise comme par exemple un collaborateur du département informatique, un supérieur, un service d'assistance etc. Dans le cadre de la vie familiale, l'« astuce du petit-enfant » est un exemple classique : les escrocs appellent des personnes âgées en prétendant être un de leurs petits-enfants qui aurait urgemment besoin d'argent.

L'évolution de la technologie pousse les criminels à combiner l'oralité au domaine cyber. Ce dernier permet aux escrocs de peaufiner leur technique et exploiter les données obtenues à leur

profit. Les nouvelles technologies peuvent être utilisées en amont, pendant et/ou en aval de la tentative d'escroquerie.

Le phénomène combinant l'escroquerie par téléphone et les nouvelles technologies a pris de l'importance au début des années 2000, lorsque les cybercriminels ont commencé à tirer parti de la technologie Voix sur IP (*Voice over IP, VoIP*), des applications de messagerie vocale et des systèmes d'appel automatisés pour mener ce type d'hameçonnage par téléphone. La technologie VoIP permet de 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 permet ainsi aux auteurs, d'automatiser des centaines d'appels frauduleux sur Internet et entrave le retraçage des numéros utilisés.

Depuis, il existe des variantes infinies de modes opératoires criminels combinant le cyber et les appels. Les criminels peuvent décider de composer un numéro au hasard ou au contraire commencer par recueillir des informations personnelles à partir de sources publiques, de réseaux sociaux ou de fuites de données antérieures pour personnaliser leurs attaques et gagner la confiance des victimes. Le phénomène de l'escroquerie téléphonique est souvent combiné à d'autres formes d'ingénierie sociale[1], ainsi qu'à l'envoi de courriels d'hameçonnage ou la création de faux sites web, pour renforcer la crédibilité de l'attaque. Par exemple certains criminels incitent leurs victimes à les appeler en leur envoyant un courriel.

Une fois les données fournies par la victime-même, les criminels peuvent se servir des informations pour s'enrichir eux-mêmes, pour commettre des délits ou pour vendre ces renseignements à d'autres groupes de cybercriminels. Le cas échéant, les auteurs servent ainsi de courtiers d'accès initial. Il s'agit là d'acteurs de la menace spécialisés dans la compromission de systèmes informatiques et de réseaux qui revendent ensuite l'accès non autorisé à d'autres acteurs de la menace.

2 Techniques utilisées

Ce phénomène revêt deux aspects : l'un relève de l'évolution des technologies dans le domaine des communications téléphoniques et l'autre de la pure manipulation psychologique.

2.1 Evolutions technologique

Les paramètres technologiques incluent par exemple :

- L'appel automatisé (en anglais *robocall*) : Des messages (très souvent en langue anglaise) sont diffusés en masse, et prétendent émaner d'organisations légitimes afin d'inspirer la confiance. Grâce à cette technique, les criminels peuvent atteindre de nombreuses victimes potentielles tout en limitant les ressources humaines nécessaires. Ainsi les criminels peuvent se concentrer sur les personnes qui ont décidé de rester en ligne après avoir entendu l'appel automatisé.
- L'usurpation du numéro de téléphone (en anglais *spoofing*) : Les cybercriminels falsifient l'identifiant de l'appelant pour afficher un numéro de téléphone légitime, ce qui peut inciter la victime à répondre. Ainsi, l'OFCS a observé des cas de spoofing usurpant non seulement des numéros de téléphone de banques, mais aussi ceux des autorités de police.

[1] Définition cf. chapitre 2.2 Tromperie et manipulations

- L'incitation au rappel : des criminels envoient un message audio enregistré à plusieurs employés d'une entreprise à la fois. L'identité de l'appelant est probablement modifiée numériquement pour ressembler à une personne interne à l'organisation. L'enregistrement contient un message urgent, souvent émis par une voix se présentant comme celle d'une source ou d'un cadre de confiance, et demandant de rappeler un numéro spécifique pour obtenir des détails (le numéro de rappel correspondant dès lors à celui que les criminels ont choisi au préalable spécialement pour l'escroquerie).

2.2 Tromperie et manipulations

En termes de schémas et méthodes, les cybercriminels sont aussi habiles en manipulation. Le recours à la psychologie et à la manipulation par les cybercriminels pour obtenir des informations confidentielles ou obtenir de l'argent s'appelle l'ingénierie sociale. Elle exploite des caractéristiques et comportements fondamentaux à l'humain pour tromper les victimes. Ainsi les cybercriminels sont renseignés sur leurs cibles à l'avance, utilisant des informations personnelles pour paraître légitimes et gagner la confiance de la victime et obtenir des informations supplémentaires. Un des élément clé à toute ingénierie sociale est l'utilisation de scénarios d'urgence, où les auteurs créent des situations de crise, comme la fermeture imminente d'un compte ou un accident, pour inciter la victime à divulguer des informations sensibles rapidement. Une personne stressée n'a pas le temps de réfléchir logiquement et rationnellement. D'autres émotions peuvent être exploitées à des fins criminelles, comme la curiosité, la culpabilité, l'empathie, la peur ou le respect de l'autorité. Ces manipulations émotionnelles incitent ainsi la victime à agir sans réfléchir.

3 Evolution technologique et criminalité

Depuis son émergence dans les années 2000, le phénomène a évolué et continue encore de le faire. L'évolution de la technologie a permis aux criminels de s'armer d'autres outils plus performants. Au début, les appels provenaient surtout d'un numéro international ou d'un numéro d'appel Internet, mais désormais il est possible de *spoofer* les numéros de téléphones locaux, c'est-à-dire que le numéro appelant du criminel est dissimulé à la personne appelée en affichant à la place un numéro local.

3.1 Exemples : SIM box, maliciels et abus de eSIM

Une des évolutions technologiques ayant amélioré les techniques d'escroquerie par téléphone, fut la *SIM box*[2]. Il s'agit d'un appareil qui achemine les connexions téléphoniques vers le réseau désiré en tant qu'appels locaux, à l'aide de plusieurs cartes SIM prépayées, qui sont souvent obtenues avec de fausses identités. Ce type d'escroquerie profite donc de la différence entre les tarifs locaux et internationaux, permettant ainsi de ne payer que les tarifs locaux. Actuellement, comme le coût de ce type de service a considérablement baissé, davantage de criminels potentiels peuvent accéder à ces méthodes.

Entre autres, les criminels utilisent désormais aussi des maliciels[3] pour perfectionner leurs escroqueries. En effet, il existe des logiciels malveillants qui manipulent les appareils, implantent des

[2] https://www.infosysbpm.com/blogs/bpm-analytics/what-is-sim-box-fraud.html

[3] Application d'hameçonnage vocal, cheval de Troie par exemple.

messages vocaux préenregistrés et redirigent les appels vers des centres d'appels d'escrocs. Une fois téléchargées et installées, ces applications demandent aux victimes la permission d'accéder aux contacts, au microphone et à l'appareil photo, à la géolocalisation et plus encore. Ces chevaux de Troie peuvent imiter les conversations avec un service clientèle lorsque les victimes appellent une banque.

Plus récemment, l'émergence de l'eSIM a permis aux criminels de développer encore une autre variante d'escroquerie par téléphone. La technologie eSIM intègre une carte SIM numérique directement dans l'appareil et offre aux utilisateurs une flexibilité et un confort d'utilisation, mais présente également de nouveaux risques de fraude. Dans le cas d'une fraude eSIM, les criminels utilisent des techniques telles que le *SIM-swapping* ou l'ingénierie sociale pour prendre le contrôle du numéro de téléphone mobile d'une victime. Ces méthodes leur permettent d'accéder à différents services tels que la banque en ligne et les réseaux sociaux, qui sont authentifiés par ce numéro. Comme de nombreux services en ligne utilisent l'authentification à deux facteurs (2FA) fondée sur les SMS, les escrocs peuvent intercepter des codes de sécurité en prenant le contrôle d'un numéro de téléphone mobile et se connecter à des comptes sans autorisation. Cela peut engendrer des pertes financières ainsi que des atteintes à la vie privée. Pour se protéger, les utilisateurs doivent utiliser des mots de passe forts et des méthodes d'authentification alternatives telles que les applications d'authentification ou des *tokens*. De plus, les opérateurs de téléphonie mobile peuvent fournir une sécurité supplémentaire en appliquant un processus de vérification plus strict lors de changements de profils eSIM.

3.2 Emergence de l'intelligence artificielle (IA)

Avec l'émergence de méthode d'intelligence artificielle (IA) et de l'apprentissage automatique (en anglais *machine learning*), cette nouvelle technologie est de plus en plus utilisée pour automatiser les appels et échapper aux systèmes de détection.

Un autre obstacle pour les escrocs est aussi la barrière de la langue. Alors que des outils de traduction fiables sont désormais utilisés pour les courriels ou les SMS, ce n'est pas encore souvent le cas pour les appels téléphoniques. Les appels sont donc principalement effectués en anglais, car il s'agit de la langue la plus parlée au monde. L'IA pourrait là aussi devenir profitable aux criminels. De nos jours, tout le monde partage des enregistrements de sa voix sur Internet. Grâce à l'émergence d'applications logicielles d'intelligence artificielle générative (*GenAI*) commercialisées qui produisent des résultats quasi instantanés et relativement crédibles, quelques clics suffisent à monter son escroquerie[4]. Cette évolution a un impact considérable sur les tactiques criminelles et la défense contre les menaces vocales. En effet, tout ce dont les criminels ont besoin pour recréer votre voix, consiste en un extrait audio, comme celui d'un appel téléphonique enregistré ou d'une vidéo publiée sur les réseaux sociaux.

Il est vrai que plus nous divulguons d'informations sur nous-mêmes sur Internet ou sur les réseaux sociaux, plus nous sommes exposés au risque d'usurpation d'identité et à d'autres activités cybercriminelles. Il est important d'être proactif en limitant les données personnelles disponibles sur Internet (ou du moins en comprenant les conséquences de leur publication).

[4] Voir le Brownbag Lunch de l'OFCS du 22 novembre 2024 : L'influence de l'intelligence artificielle sur les attaques d'ingénierie sociale. (Disponible qu'en allemand, traduction en français prévue prochainement).

En Suisse, les cas d'escroqueries qui s'appuient sur de l'IA concernent surtout les phénomènes d'escroqueries par téléphone et d'investissements frauduleux au nom de célébrités et de sextorsion, où les images sont générées par l'IA. En raison du nombre relativement faible de signalements dans ce domaine, l'OFCS estime qu'il s'agit probablement de premiers essais de la part des cybercriminels pour voir comment l'IA peut être utilisée à l'avenir de manière rentable pour des cyber-attaques. Dans de nombreux cas de fraude, il est difficile de déterminer dans quelle mesure l'intelligence artificielle a été utilisée. Par exemple, on ne peut que supposer qu'un outil de traduction a été utilisé ou non. Dans quelques cas seulement, l'utilisation de l'IA est évidente.

4 Les escroqueries par téléphone dans le domaine cyber en Suisse

Les escroqueries par téléphone sont un phénomène connu depuis longtemps en Suisse. Ainsi, depuis 2004 et la création de MELANI, devenue ensuite NCSC et désormais OFCS, de tels cas ont été signalés.

4.1 Phénomènes Fake Support et Fake Support Popup

Les premiers cas suisses d'escroqueries par téléphone enregistrés par le NCSC étaient entre autres des situations où les victimes étaient informées par un prétendu employé du service de support de Microsoft que leur ordinateur avait été piraté et qu'il fallait réagir immédiatement. Les victimes étaient amenées à installer un logiciel de contrôle à distance sur leur ordinateur (tel que *AnyDesk*). Ensuite, les criminels essayaient de se connecter au compte bancaire en ligne afin d'effectuer des virements.

Depuis quelques temps, l'OFCS observe également une variante dans laquelle les annonces sont placées sur des portails publicitaires en ligne. Ici il s'agit de jouer sur le design du site web pour convaincre un utilisateur de la véracité du contenu de la fenêtre popup qui l'informe que son ordinateur est soi-disant infecté et qu'il doit appeler un numéro de téléphone précis. A partir de là, les choses continuent selon le schéma classique précédemment décrit.

4.2 Appels frauduleux de prétendus collaborateurs bancaires

L'OFCS reçoit également régulièrement des signalements relatifs à des appels de prétendus employés de banque qui demandent si la personne appelée a effectivement effectué un paiement.[5] Dans de nombreux cas, ils prétendent par exemple qu'il y a eu un prélèvement pour un écran plat dans un magasin d'électronique. La personne recommande ensuite d'appeler immédiatement le service des fraudes de la police cantonale. Le numéro de téléphone correspondant de la police à appeler est également fourni dans la foulée. La victime est ensuite incitée à effectuer différentes actions et à vérifier ses activités bancaires en ligne. Il lui est demandé de confirmer différentes données afin d'annuler le paiement. L'OFCS suppose que dans ces cas-là la victime est amenée à se rendre sur une page web créée par les escrocs, à partir de laquelle elle pourrait annuler des paiements fictifs soi-disant frauduleux. Pour ce faire, des données d'accès et des mots de passe à usage unique sont demandés. En arrière-plan, les criminels se connectent ensuite à l'e-banking avec les données obtenues et déclenchent les paiements correspondants, tandis qu'au premier plan, la victime est amenée à croire que l'annulation a parfaitement fonctionné. Mais dans ces

[5] Cf. publication https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2023/wochenrueckblick_44.html

cas également, il existe des variantes dans lesquelles les cybercriminels tentent d'accéder à l'ordinateur au moyen d'un logiciel d'accès à distance pour ensuite effectuer des actions frauduleuses.

4.3 *Robocalls*: Les appels automatisés au nom des autorités

Depuis juillet 2023, la Suisse connaît des vagues d'appels téléphoniques frauduleux d'une ampleur sans précédent. Des escrocs appellent quotidiennement et de manière automatisée des milliers de Suisses en se faisant passer pour la police afin d'accuser la victime d'un délit. Dans ce cas, de nombreux appels téléphoniques sont passés en même temps. Lorsque la victime décroche, une voix enregistrée l'informe qu'elle est impliquée dans une enquête policière. Il faut appuyer sur la touche « 1 » pour obtenir plus d'informations. Ce n'est qu'en appuyant sur « 1 » que la victime est mise en relation avec un employé du centre d'appel. Les victimes sont alors informées qu'elles sont impliquées dans une affaire de blanchiment d'argent (ou autre délit) et que leur compte bancaire sera bloqué. Dans cette version, les criminels accèdent aussi au compte bancaire de la victime à l'aide d'*AnyDesk* ou d'un logiciel similaire.

Les escrocs sont organisés en centres d'appels et la plupart du temps, les appelants parlent anglais avec un accent étranger. Cependant, l'OFCS remarque que de plus en plus souvent certains appelants parlent bien l'allemand ou le français.

Les appelants falsifient leur *CallerID* (ce qu'on appelle en anglais *spoofing*). Souvent, ils choisissent des numéros au hasard dans le réseau de téléphonie mobile à faire afficher aux personnes appelées. Les véritables propriétaires de ces numéros de téléphone sont alors rappelés par des inconnus qui ne savent pas que l'appel ne provient pas du numéro de téléphone usurpé.

Grâce à l'astuce de la voix enregistrée, les criminels peuvent passer davantage d'appels simultanément, tout en présélectionnant leurs victimes. En effet seuls les appels des victimes qui décrochent et restent au bout du fil sont traités par les criminels (par exemple, uniquement les appels où la victime est restée en ligne ou a suivi les instructions données par la voix enregistrée).

L'OFCS a constaté que dans certains des cas, où les victimes avaient exprimé des doutes quant à l'authenticité de l'appel au cours de la conversation téléphonique, celles-ci ont été ensuite rappelées avec un numéro public d'Interpol. Les victimes sont ensuite incitées à vérifier le numéro sur Internet. Les criminels espèrent ainsi gagner en crédibilité.

Malgré quelques différences, il existe des similitudes évidentes entre les cas classiques de faux support et les appels de menace automatisés :

- Les escrocs agissent depuis des centres d'appels.
- Les escrocs utilisent des numéros de téléphone usurpés (souvent avec le même indicatif que celui des numéros visés).
- Les victimes sont amenées à installer un logiciel de contrôle à distance, puis à autoriser l'accès aux comptes bancaires en ligne.

4.3.1 Différences entre le « faux support » et les *robocalls*

Les figures 1 et 2 illustrent l'impact du phénomène des « appels de menace automatisés au nom des autorités policières » sur les signalements reçus par l'OFCS au cours des 12 derniers mois. Les phénomènes de « faux support » et d'« appels de menace au nom de la police » sont comparés ci-après.

Dans les deux cas, il s'agit en fin de compte de convaincre les victimes potentielles de télécharger un logiciel d'accès à distance et de donner ensuite accès à l'ordinateur aux escrocs. Dans le cas du faux support, cela se fait individuellement comme mentionné précédemment. Les appelants contactent chaque victime potentielle séparément. En conséquence, les signalements au OFCS sont relativement constants à un niveau bas depuis un an et demi. En moyenne, l'OFCS a reçu environ 60 annonces par mois. Le mode opératoire des escrocs semble nécessiter beaucoup de ressources et n'est pas très productif.

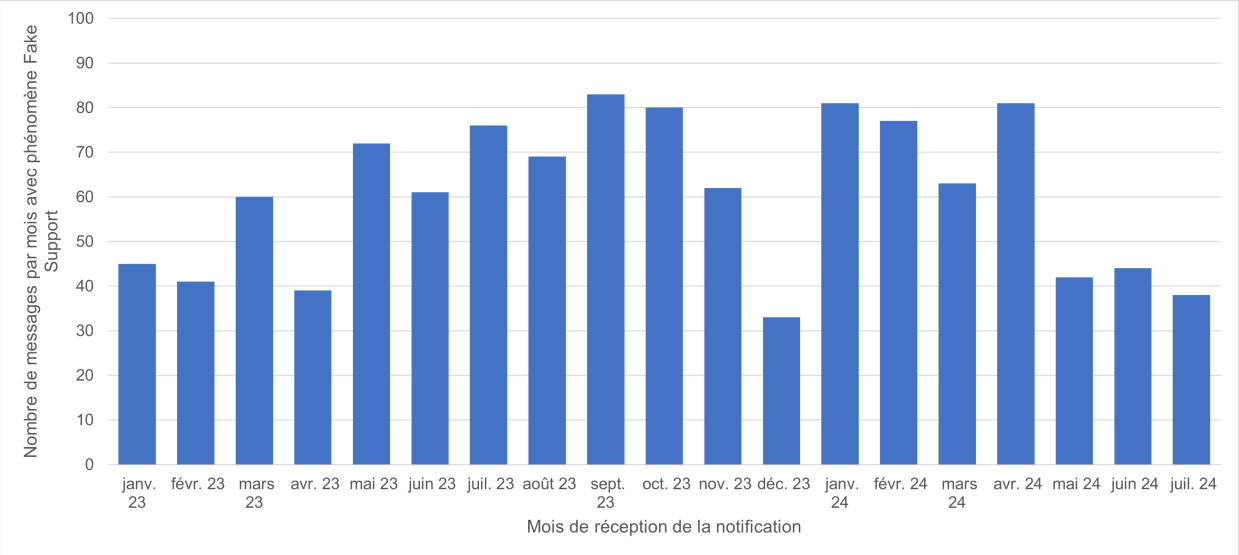

Figure 1. *Rapports d'appels de fake support par mois. Le nombre de rapports se répartit régulièrement sur l'année et se situe à un faible niveau.*

Il n'est donc pas surprenant que les escrocs aient cherché des moyens de rendre cette variante de fraude plus efficace. Dans le phénomène des « appels de menace au nom des autorités », ce ne sont plus les escrocs qui appellent personnellement, mais plutôt un bot qui teste des numéros différents au hasard en très peu de temps. Seuls les utilisateurs qui restent en ligne et appuient sur la touche mentionnée dans le message automatique sont redirigés vers un escroc. Les escrocs ne reçoivent donc que les appels téléphoniques ayant de fortes chances d'être couronnés de succès. En conséquence, la situation est très différente en ce qui concerne la réception des signalements. Jusqu'en juin 2023, le phénomène n'était que peu connu en Suisse. A partir du mois de juillet 2023, les cas n'ont cessé d'augmenter pour atteindre dès le mois d'août 2023 la barre des 1000 déclarations par mois. Il s'agissait probablement d'une première expérimentation de la part des criminels. En octobre de la même année, les chiffres ont véritablement explosé. Parfois, l'OFCS recevait près de 1000 signalements par semaine pour ce seul phénomène. Après une courte pause début 2024, le nombre de signalements a de nouveau fortement augmenté en février 2024, atteignant à nouveau des records avec plus de 1500 signalements par semaine. Au 31 juillet 2024, l'OFCS n'a plus reçu qu'une centaine de signalements par semaine concernant ce phénomène.

Le nombre d'appels frauduleux et donc de signalements auprès de l'OFCS dépend donc moins des ressources des escrocs que des capacités techniques et de l'efficacité des bots qui effectuent les appels automatiques.

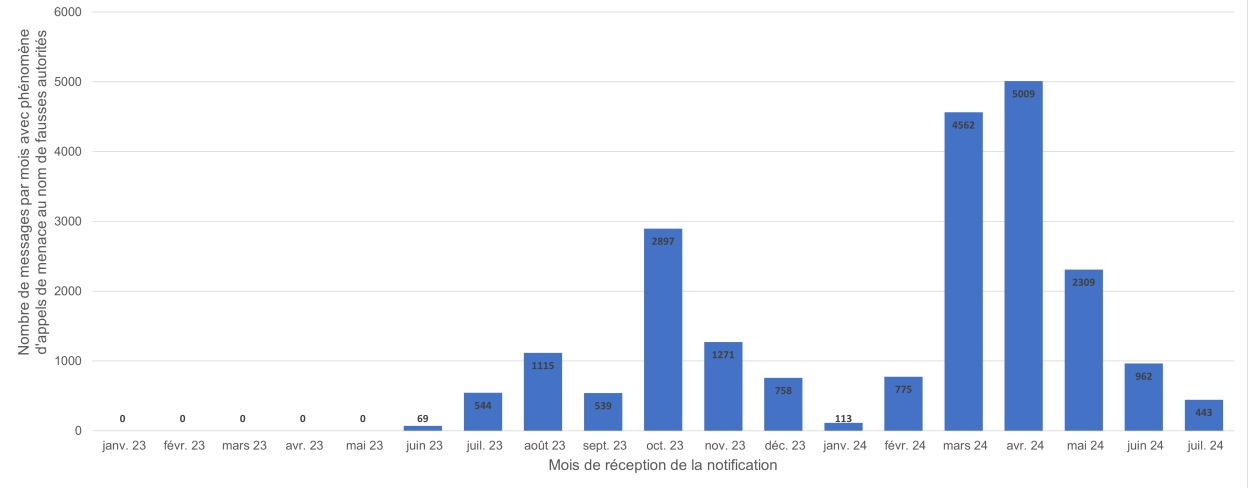

***Figure 2**. Rapports d'appels de menaces au nom de fausses autorités par mois. Il faut noter les grandes entrées de signalements en mars et avril 2024. En été 2024, les signalements ont à nouveau diminué.*

4.3.2 Les heures de travail des escrocs

La figure 3 montre la répartition moyenne des annonces reçues au cours d'une journée, sachant qu'elle ne comptabilise que les annonces relatives aux escroqueries par téléphone au nom des autorités. En ce qui concerne les appels téléphoniques frauduleux, l'OFCS part du principe que, dans la plupart des cas, ils lui sont signalés immédiatement après l'appel et que, par conséquent, la réception du message et l'heure réelle de l'appel coïncident pratiquement. Par conséquent, les heures de travail des escrocs peuvent également être estimées sur la base de la quantité d'annonces reçues.

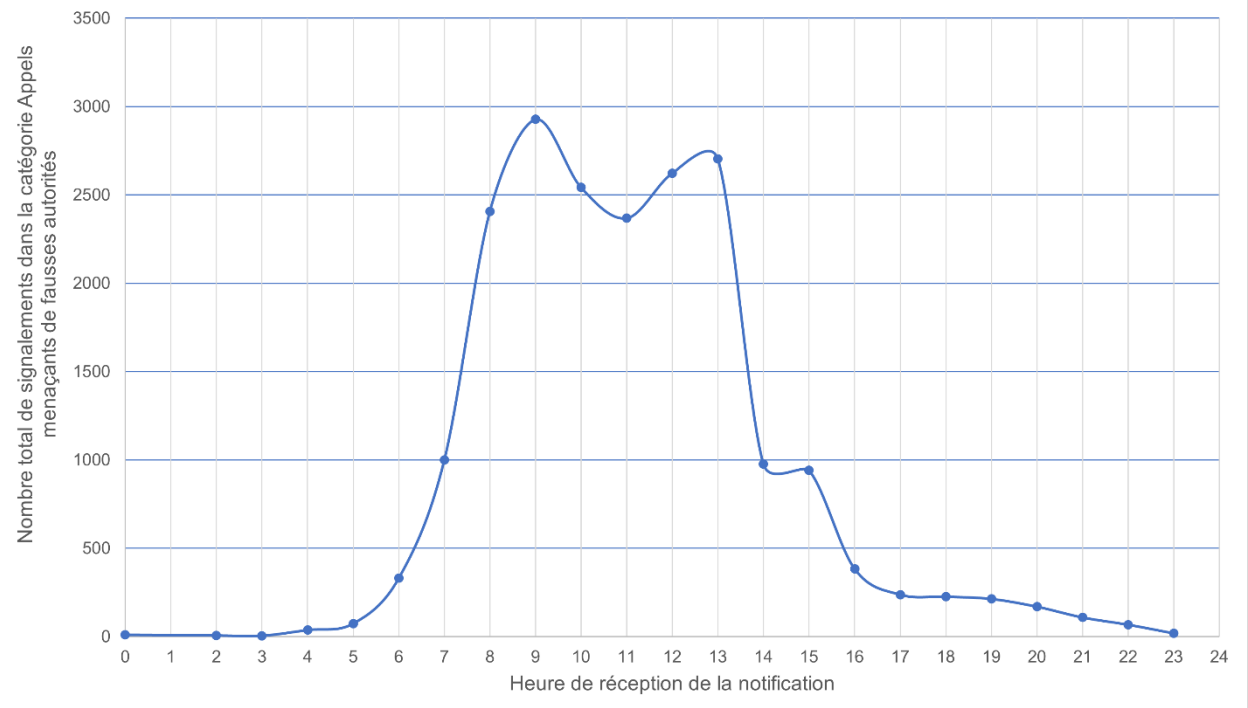

***Figure 3.** Evolution temporelle moyenne des messages concernant les faux appels des autorités. Les messages commencent à 5 heures et atteignent un premier maximum à 9 heures. Après le deuxième maximum à 13h, les messages diminuent fortement à partir de 16h.*

La distribution ressemble à une journée de travail ordinaire, qui commence à 6 heures et se termine à 16 heures. Mais les escrocs semblent également faire une pause à midi. D'après le

taux relativement faible de plaintes reçues à 11 heures, il est possible de conclure que les criminels prennent également leur pause déjeuner - alors qu'il n'est pas encore l'heure de manger en Suisse. Cela suggère que les criminels se trouvent dans un pays situé sur un fuseau horaire plus à l'est.

5 Point de vue d'un fournisseur de télécommunication

Après avoir passé en revue les annonces reçues par l'OFCS, intéressons-nous désormais au point de vue d'un fournisseur de télécommunication suisse :

5.1 Un jeu du chat et de la souris

Les auteurs développent sans cesse de nouvelles méthodes pour escroquer les usagers de la téléphonie. Ils combinent différentes techniques pour maximiser leurs chances de succès. L'une d'entre elles est l'usurpation d'identité. Cette technique consiste à dissimuler l'identité de l'appelant. Les auteurs savent que la probabilité d'une prise d'appel augmente si l'identité de l'appelant utilisée semble fiable. Cette méthode leur réussit car au cours des deux dernières années, le nombre d'appels usurpés a augmenté de 50%. Et cette tendance devrait se poursuivre.

L'utilisation de l'intelligence artificielle (IA) pour les escroqueries téléphoniques est également tendance. Bien que les méthodes mises en œuvre à ce jour pour réaliser des appels automatisés soient encore relativement simples, ce n'est qu'une question de temps avant que les criminels ne développent des techniques plus avancées pour optimiser leurs tentatives d'escroquerie. Que les appelants falsifient ou non leur identité, les fournisseurs de télécommunication (Voice Service Provider) ne sont actuellement pas autorisés, ni techniquement capables, de reconnaître les *robocalls* utilisant l'IA à partir de leur contenu, de la langue ou de la voix. C'est un inconvénient majeur, car les cybercriminels utilisent déjà l'IA à des fins malveillantes. Les fournisseurs de télécommunication pourraient utiliser les mêmes capacités techniques basées sur l'IA non seulement pour surveiller les schémas d'appels, mais aussi pour identifier les *robocalls* en fonction du contenu évalué des appels. En utilisant des alertes automatisées et respectueuses de la vie privée, ils pourraient réagir en conséquence et prendre les contre-mesures appropriées. Il convient de remédier à cette anomalie, faute de quoi les fournisseurs de télécommunication continueront à prendre du retard sur les criminels.

5.2 Mesures prises par les fournisseurs

Dans la lutte contre les escrocs, diverses mesures techniques et juridiques sont prises depuis des années. Les opérateurs de télécommunication peuvent mettre en place des mesures techniques pour bloquer de telles attaques par téléphone et limiter le nombre de tentatives :

- Le filtrage des appels permet d'analyser les appels entrants afin d'identifier et de bloquer les numéros suspects associés à des escroqueries par téléphone.
- L'utilisation de la reconnaissance vocale permet d'authentifier les appelants, en particulier pour les transactions à haut risque ou les interactions sensibles.
- Les opérateurs peuvent aussi déployer des algorithmes pour détecter des schémas d'appel inhabituels ou des comportements indiquant des tentatives d'attaques, comme un volume élevé d'appels vers des numéros spécifiques sur une courte période.

En Suisse, les fournisseurs misent sur l'analyse des modèles d'appels pour détecter les anomalies. Il existe également des initiatives visant à endiguer l'usurpation de numéros suisses depuis

l'étranger. Un autre défi réside dans le fait que les auteurs adaptent en permanence leur mode opératoire. Il est donc indispensable de sensibiliser la population à ces dangers. Certains fournisseurs par exemple informent régulièrement leurs clients sur ce sujet par le biais de différents canaux et leur recommandent de faire preuve d'un scepticisme raisonnable. Il ne faut en aucun cas communiquer des données personnelles (telles que mots de passe, codes PIN, etc.) aux personnes qui appellent. Les fournisseurs recommandent en outre à leurs clients d'activer le filtre d'appel (applicable tant au réseau fixe que mobile). Ils sont ainsi protégés contre les appels publicitaires indésirables.

5.3 Le rôle de soutien de l'Office fédéral de la communication (OFCOM) aux fournisseurs de télécommunications

Les bases juridiques existent déjà, affirment les fournisseurs. Actuellement, une initiative commune entre les fournisseurs et l'Office fédéral de la communication (OFCOM) existe pour trouver une solution à l'échelle du secteur. Dès que le secteur suisse des télécommunications aura trouvé une solution appropriée, l'OFCOM pourra apporter son soutien afin d'assurer la mise en œuvre, la réglementation et la supervision le cas échéant.

Globalement, la lutte contre les appels frauduleux reste un défi complexe. Il nécessite une étroite collaboration entre les fournisseurs, les autorités de régulation et la population afin de développer des solutions techniques conformes à la loi, efficaces et également respectueuses de la vie privée des clients. Le fait est qu'à l'avenir, il n'y aura toujours pas de protection à 100% efficace contre la fraude téléphonique. Cependant, en prenant les bonnes contre-mesures, il est possible de réduire le risque.

6 Complexité juridique à protéger les individus

Quant au cadre légal, outre l'article 146 du Code pénal suisse, quelques lois peuvent être invoquées :

- La Loi fédérale sur la concurrence déloyale (LCD) interdit les pratiques commerciales déloyales, qui peuvent inclure des pratiques trompeuses telles que l'escroquerie par téléphone.
- La Loi fédérale sur la protection des données (LPD) régit le traitement des données personnelles et peut être invoquée dans les cas où l'escroquerie par téléphone implique la collecte non autorisée ou l'utilisation abusive d'informations personnelles.
- La Loi sur les télécommunications (LTC) régit les services et les réseaux de télécommunications. Elle peut être invoquée dans les cas où l'escroquerie par téléphone implique une utilisation abusive de l'infrastructure de télécommunications.
- L'Autorité fédérale de surveillance des marchés financiers (FINMA) réglemente les institutions financières ainsi que les assurances. Elle peut donc imposer des sanctions aux entités impliquées dans l'escroquerie par téléphone ciblant le secteur financier.

6.1 Aspect juridiques (point de vue de l'OFCOM)

Quelles sont les obligations du fournisseur ? Le droit des télécommunications oblige les fournisseurs à protéger les clients contre les appels publicitaires déloyaux (art. 3, al. 1, let. u, v et w, de la loi fédérale contre la concurrence déloyale (LCD)). Les fournisseurs doivent mettre à la disposition des clients un moyen approprié pour lutter contre ces appels. Cela se traduit en pratique

par la mise en place d'une solution de filtrage[6]. Celle-ci doit combattre de tels appels dans la mesure où l'état de la technique le permet (art. 45a LTC). Cela suppose que les fournisseurs puissent également réagir aux nouvelles technologies et procédures et adapter les fonctionnalités des filtres en conséquence. Etant donné que les appels publicitaires déloyaux sont généralement accompagnés d'un spoofing du numéro affiché, les filtres qu'ils doivent mettre en place sont aussi adaptés à la lutte contre l'usurpation d'identité (article 179^{decies} du Code pénal) dans le cadre d'escroqueries par téléphone. Ces éléments peuvent contribuer à protéger les utilisateurs contre des tentatives d'escroquerie par téléphone.

Que peut faire la victime ? Du point de vue du droit des télécommunications, la victime d'une escroquerie peut invoquer l'article 146 du Code pénal suisse et exercer un droit d'information (art. 45 LTC), qui vise à ce que l'origine, c'est-à-dire le raccordement, des appels dits abusifs soit retrouvée par les fournisseurs impliqués dans la connexion. Les appels avec des numéros usurpés peuvent être considérés comme abusifs, notamment s'ils sont effectués dans le cadre d'une démarche présumée frauduleuse. Bien entendu, c'est un tribunal pénal qui devra juger si et quand les conditions sont remplies. Toutefois, le degré de la simple vraisemblance en matière de preuve suffit. En dehors de cela, le véritable problème réside dans le fait que l'origine des appels ne soit presque jamais en Suisse ou que l'origine de l'appel soit à l'étranger et que le fournisseur d'origine étranger, s'il peut être retrouvé, ne soit pas soumis au droit suisse des télécommunications.

6.2 Limites juridiques internationales

Un des problèmes du filtrage réside dans le fait qu'il ne doit pas aboutir à un blocage des appels légaux, car cela enfreindrait l'obligation d'interopérabilité (les fournisseurs doivent en principe acheminer les appels vers le destinataire). Il faut également tenir compte du fait que les fournisseurs ne peuvent pas connaître le contenu des appels en raison du secret des télécommunications. Les filtres doivent donc être réglés selon différents indicateurs et fonctionner de manière dynamique, car les criminels changent aussi toujours les numéros utilisés pour commettre leur escroquerie. Si les appelants utilisent par exemple des numéros de téléphone portable, il est encore plus difficile pour les fournisseurs de juger si l'appel est légitime car il pourrait parfaitement provenir d'un vacancier à l'étranger et non d'un escroc.

Les Etats-Unis ont détecté au mois de mai 2024 un groupe criminel qu'ils ont appelé Royal Tiger, dont le but est de faciliter les appels frauduleux à travers les réseaux internationaux. Selon un communiqué de presse[7], le groupe cherche à se faire passer pour des agences gouvernementales, des banques et des entités de services publics. Ces appels visent à duper les consommateurs internationaux en leur proposant de fausses réductions des taux d'intérêt pour leurs cartes de crédit ou visent à solliciter des autorisations d'achat pour des commandes que les victimes n'ont jamais passées. Actuellement, Royal Tiger opère en Inde, au Royaume-Uni, aux Émirats arabes unis et aux États-Unis. C'est ainsi que le législateur des Etats-Unis a décidé de créer une nouvelle classification dédiée à ces *robocalls* : *The Consumer Communications Information Services Threat (C-CIST)*[8].

En ce qui concerne l'Autriche, dès le 01 septembre 2024, un nouveau règlement[9] va entrer en vigueur, qui prévoit que les opérateurs autrichiens doivent procéder à une vérification du numéro

[6] cf. chapitre 5.2 Mesures prises par les fournisseurs

[7] https://www.documentcloud.org/documents/24661582-doc-402506a1

[8] https://www.documentcloud.org/documents/24661584-da-24-388a1

[9] https://www.rtr.at/9_novelle_kem-v

appelant lorsqu'ils traitent des appels à destination de numéros autrichiens depuis l'étranger. Si la vérification n'est pas possible, l'affichage du numéro appelant est masqué à l'écran. Cependant cela n'empêche pas que des appels frauduleux avec des numéros d'autres pays (notamment germanophones), tels que des appels spoofés allemands, puissent être effectués.

6.3 Intelligence artificielle et avenir

A cette complexité technique s'ajoute désormais la question de la manipulation de l'être humain par le biais de l'utilisation de l'IA. L'OFCS a publié un article[10] paru le 12.12.2023 concernant l'utilisation de l'IA pour les tentatives d'escroqueries. Une combinaison entre spoofing et altération de la voix au moyen de l'IA engendre de grandes opportunités pour les criminels. Plus la technologie s'améliore, plus il sera difficile de détecter les tentatives d'escroquerie.

Comment améliorer la situation actuelle alors ? Une possibilité de limiter l'usurpation serait d'introduire un processus de vérification (similaire au courriel) pour vérifier l'origine et l'authenticité du numéro. Les discussions sont en cours dans les instances internationales, telles que dans le cadre de la Conférence européenne des administrations des postes et télécommunications (CEPT), au sein du Comité des Communications Electroniques (ECC) et de l'Union internationale des télécommunications (UIT). L'OFCOM y apporte régulièrement sa contribution. Dans le droit des télécommunications, les bases légales existent aussi depuis la dernière révision pour introduire de tels processus. Cependant, pour qu'ils conduisent à une amélioration de la situation, ils devraient être introduits dans le plus grand nombre possible de pays et non uniquement en Suisse.

7 Mesures préventives recommandées par l'OFCS

Pour se protéger de l'escroquerie par téléphone, voici quelques méthodes à l'intention de la population :

1. Ne faites pas confiance à tous les appelants. Mettez immédiatement fin aux appels non plausibles ;
2. Ne vous laissez pas intimider ou mettre sous pression ;
3. Ne révélez jamais votre mot de passe ou votre code PIN au téléphone ;
4. Ne révélez pas d'informations professionnelles à des inconnus ;
5. N'autorisez jamais des inconnus à accéder à votre ordinateur, même s'ils vous semblent dignes de confiance.

[10] https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2023/wochenrueckblick_49.html

8 Conclusion

Le point faible le plus présent derrière de nombreuses tentatives d'escroquerie par téléphone réside souvent dans l'être humain à l'autre bout du fil. Lorsque ce dernier est soumis à des pressions personnelles, professionnelles et à des exigences de performance, il peut préférer la rapidité à la prudence, surtout en situation d'urgence. Dans ces cas ce sont les victimes-mêmes qui ouvrent la porte à des criminels opportunistes. Cependant la sécurité ne peut plus aujourd'hui reposer et compter principalement sur la capacité des utilisateurs à reconnaître de la fraude. Les criminels opèrent à l'international et grâce à des réseaux mondialement connectés entre eux. Les anciennes méthodes d'identification (comme la fameuse *Calling Line Identification*) sont devenues obsolètes en raison des avancées technologiques et il n'y a pas encore de nouvelles méthodes d'authentification dans le domaine de la téléphonie (contrairement au domaine du courrier électronique où grâce à l'authentification DMARC, il est possible de détecter et limiter les techniques d'usurpation de courriel). Selon l'OFCOM, les essais des protocoles STIR/SHAKEN[11] en Amérique du Nord n'ont été que peu concluantes. Beaucoup d'organisations du secteur ont abandonné ce standard[12], ce qui souligne la difficulté de mettre en place de nouvelles méthodes d'authentification à l'échelle mondiale.

[11] Ensemble de protocoles développés pour authentifier l'appelant et ses données lors d'appels effectués via le réseau VoIP.(https://www.fcc.gov/call-authentication)

[12] https://commsrisk.com/global-stir-shaken-is-dead-what-comes-next/