

Les escroqueries téléphoniques

Les arnaques téléphoniques sont de plus en plus courantes.

Les arnaqueurs ont plus d'une combine dans leur sac. Vous connaissez, le **spam** téléphonique le **smishing**, le **phishing** ou **vishing**, le **spoofing**... Et le dernier tour d'escroquerie passe se nomme **wangiri**. Encore une arnaque au téléphone.

Cela ne vous parle pas ? Il faut pourtant s'en méfier, car cela peut vous coûter cher.

Ce genre de fraude téléphonique repose sur des techniques d'ingénierie sociale (manipulation psychologique à des fins d'escroquerie) pour convaincre les victimes qu'elles agissent pour leur propre bien ou pour éviter des problèmes plus graves, comme une poursuite judiciaire ou la suspension de leur compte bancaire. Des techniques qui s'avèrent souvent efficaces dans un contexte inflationniste et de perte de pouvoir d'achat.

Les arnaques sont nombreuses et les malfaiteurs ne manquent pas d'imagination pour tenter de gagner quelques euros. Alors comment les escrocs utilisent-ils le téléphone pour arnaquer les gens ?

- [Le Smishing](#)

- [Le Vishing](#)

- [Le Wangiri](#)

- [Le Spoofing](#)

Le smishing

Le spam téléphonique désigne un appel téléphonique ou SMS non voulu à des fins publicitaires, commerciales ou malveillantes.

C'est une forme de cyberattaque très inquiétante qui prend de plus en plus d'ampleur au niveau mondial.

Concrètement, c'est une forme de phishing réalisée par SMS. Les cibles peuvent tout aussi bien être des particuliers comme des entreprises ou administrations.

L'identité d'une organisation publique ou privée est souvent usurpée, et il vous est demandé de renseigner vos coordonnées sur une plateforme qui imite souvent très bien l'originale. Si vous tombez dans le panneau, vos informations peuvent être revendues sur le dark web, et le problème est encore plus grave si vous avez procédé à un paiement aux escrocs.

Cette escroquerie est massive. On estime en effet que 300 000 à 400 000 attaques par SMS ont lieu chaque jour dans le monde. Autre chiffre effarant relayé par nos confrères : d'après la Federal trade commission (FTC), 330 millions de dollars ont été dérobés aux consommateurs américains par ce biais en 2022, soit plus du double des pertes signalées l'année précédente.

Le problème est d'autant plus délicat à résoudre, que les internautes ont tendance à beaucoup plus cliquer sur des liens frauduleux lorsqu'ils les reçoivent par SMS que par e-mail (un ratio de fois 8 a même été observé).

Face à ce défi d'ampleur, les autorités ont mis en place des plateformes de signalement pour mieux bloquer ces messages. Les opérateurs ne sont pas en reste et ont eux-mêmes déployé des systèmes de filtrage pour éviter que leurs clients ne soient bombardés de ce type de SMS.

Malheureusement, cela ne suffit pas et il convient donc d'adopter certains réflexes. Vous pouvez par exemple surveiller l'orthographe et le style du message reçu. Ces derniers sont souvent approximatifs, même s'ils tendent à s'améliorer, car les hackers recourent désormais à des IA telles que ChatGPT et ses rivaux.

Pensez également à vous connecter directement sur les comptes des services mentionnés, et ce sans cliquer sur les liens présents dans ces SMS qui s'avèrent bien souvent frauduleux. Dans tous les cas, ne vous précipitez jamais et prenez le temps de la réflexion. Les hackers ont en effet pris l'habitude d'instaurer un sentiment d'urgence chez leurs cibles pour les pousser à la faute.

Le vishing ou phishing

Le hameçonnage vocal est un cybercrime qui consiste à passer des appels téléphoniques dans le but d'obtenir les renseignements personnels confidentiels des victimes. Les cybercriminels utilisent des tactiques d'ingénierie sociale pour convaincre leurs victimes de partager des informations privées comme les données d'accès à un compte bancaire.

Tout comme l'hameçonnage (**phishing**) ou l'hameçonnage par message texte (**smishing**), l'objectif de l'hameçonnage vocal est de convaincre les victimes qu'elles agissent dans l'intérêt général ou dans leur propre intérêt. Souvent, l'auteur de l'appel prétend téléphoner au nom du gouvernement, du service fiscal, de la police ou de la banque de la victime.

Les cybercriminels utilisent des menaces et un ton persuasif pour amener leurs victimes à croire que la seule option possible est de fournir l'information demandée. Certains sont très convaincants et réussissent à leur faire croire qu'ils les aident à éviter une poursuite criminelle. Une autre tactique fréquemment utilisée est de laisser des messages vocaux menaçants qui demandent au destinataire de rappeler immédiatement, sous peine par exemple d'être arrêté ou de voir son compte bancaire suspendu.

Il arrive fréquemment que les cybercriminels ajustent leurs appels et leurs messages d'hameçonnage en fonction du moment de l'année, ou d'une nouvelle populaire dans l'actualité. Par exemple, pendant la période des impôts, les criminels peuvent laisser des messages en prétendant être l'ARC. Et pendant la pandémie de COVID-19, des cybercriminels ont contacté des gens en leur promettant des vaccins et des trousseaux de test en échange de leurs informations bancaires et de leur adresse postale.

Un cybercriminel peut effectuer une recherche sur une organisation, trouver les coordonnées d'un employé en ligne, puis l'appeler en se faisant passer pour le président. Il ne lui reste qu'à demander à la victime de transférer des fonds pour payer une facture en souffrance ou de transmettre un courriel contenant des fichiers personnels.

L'ingénierie sociale est une technique utilisée par les cybercriminels et qui mise sur la tendance naturelle des êtres humains à faire confiance pour les convaincre de partager des informations confidentielles. Celles-ci peuvent ensuite être utilisées pour commettre d'autres cybercrimes.

Une attaque d'hameçonnage vocal réussie implique beaucoup plus de travail que de passer quelques coups de fil aléatoires. Les cybercriminels utilisent une approche stratégique pour voler leurs victimes :

1. Ils commencent par effectuer des recherches sur leurs victimes. Cette étape peut comprendre l'envoi d'un courriel d'hameçonnage, en espérant qu'une personne réponde et fournisse son numéro de téléphone.
2. Si la victime répond favorablement à la demande contenue dans le courriel, il est peu probable qu'elle se méfie d'un appel futur. En effet, selon le niveau de sophistication de l'attaque, la victime peut s'attendre à recevoir un appel téléphonique. Et comme les cybercriminels savent que les victimes sont plus susceptibles de répondre à un numéro provenant d'un indicatif régional local, ils peuvent utiliser un logiciel spécialisé leur permettant de simuler un appel effectué localement.
3. Dès que les cybercriminels ont établi un contact, et selon le type d'arnaque, la victime mise en confiance sera amenée à communiquer des informations bancaires, à transférer des fonds, à fournir des renseignements le concernant ou concernant son employeur ou encore à transmettre des documents confidentiels par courriel.
4. Une fois en possession de ces informations, les cybercriminels peuvent s'en servir pour commettre d'autres crimes tels que : vol d'identité, utilisation des fonds de la victime, achat en ligne avec les informations de carte de crédit, envoi de courriels aux collègues de la victime pour les inviter à leur tour à partager des informations confidentielles.

Dans certains scénarios d'hameçonnage vocal, les cybercriminels fournissent un numéro de téléphone que les victimes peuvent composer en cas de questions ou pour faire un suivi. Il peut s'agir par exemple d'obtenir des informations sur le traitement de leurs impôts ou les résultats de leur test de dépistage de la COVID-19. Ce détail permet de légitimer les actions du cybercriminel et met la victime en confiance. Si la victime utilise le numéro, elle peut être dirigée vers une boîte vocale ou vers une personne qui poursuivra l'arnaque.

Quatre techniques communes d'hameçonnage vocal

1. Balayage de numéros de téléphone (wardialing)

Le cybercriminel utilise un logiciel pour appeler un indicatif régional spécifique et laisse un message semblant provenir d'une organisation locale, comme une banque, un service public ou une entreprise. Lorsqu'une personne répond, un message automatique démarre lui demandant de fournir son nom complet, les détails liés à sa carte de crédit, ses informations bancaires, son adresse postale et même son numéro d'assurance sociale. Le message enregistré peut préciser par exemple que ces informations sont nécessaires pour confirmer que le compte de la victime n'a pas été compromis.

2. Voix sur IP (VoIP)

Grâce à la voix sur IP, il est très facile pour les cybercriminels de créer un faux numéro de téléphone. Ces types de numéros sont difficiles à retracer et peuvent être utilisés pour créer des numéros de téléphone qui paraissent locaux ou qui présentent un préfixe 1-800. Certains cybercriminels créent des numéros VoIP qui semblent provenir d'un ministère, d'un hôpital local ou du service de police.

3. Mystification de l'identité de l'appelant

Tout comme dans le cas de l'hameçonnage vocal, le cybercriminel se cache derrière un faux numéro de téléphone pour se faire passer pour quelqu'un d'autre. Une des stratégies consiste à masquer l'identité de l'appelant et qu'apparaisse la mention « Inconnu » sur l'afficheur. Il est également possible de modifier le nom pour que l'appel semble provenir du gouvernement, d'un service public ou d'une banque. Le cybercriminel peut ainsi se faire passer pour une organisation légitime.

4. Le dumpster diving ou la fouille des poubelles

Une méthode simple et populaire pour recueillir des numéros de téléphone valides est de fouiller les poubelles situées derrière les édifices à bureaux et les entreprises.

Souvent, les criminels trouvent suffisamment d'information pour lancer une attaque de harponnage contre la victime.

L'ingénierie sociale est essentielle à la réussite de tous les types d'attaques de phishing. Il faut donc se méfier de tous appels au ton urgent, ferme ou convaincant. Il est important de se rappeler que le service de soutien technique de Microsoft, Amazon, ou d'un service public ne vous demanderont jamais vos informations personnelles ou bancaires.

Si votre téléphone sonne et qu'un numéro débutant par + 229 ou 00229 s'affiche, redoublez de vigilance. Cet indicatif est celui du Bénin, un pays d'où proviennent de nombreuses arnaques téléphoniques. "Le pays est connu pour sa cybercriminalité importante".

Celles qui reviendraient le plus souvent seraient les arnaques dites sentimentales. Un homme, surnommé "brouteur" se fait passer pour un amoureux potentiel, installe une relation de confiance avec sa victime afin de lui soutirer de l'argent en inventant des mensonges justifiant ce besoin d'argent.

Le wangiri

Habitués aux anglicismes, les arnaqueurs innoveront un peu avec celle-ci. C'est un terme japonais qui signifie « sonner et raccrocher ». On l'utilise ici pour désigner une méthode utilisée par les fraudeurs qui consiste à éveiller la curiosité des victimes pour leur soutirer de l'argent en les faisant **rappeler un numéro surtaxé**.

Selon la longueur de l'appel, la surtaxe est croissante. Pour être sûrs de réussir leur coup, les escrocs appellent généralement sur des plages horaires lors desquelles nous sommes peu susceptibles de répondre (la nuit, ou lorsque nous sommes au travail). La personne découvre alors l'appel manqué, sans message pour lui indiquer la nature de cet appel, et peut être tentée de rappeler.

Voilà une filière qui ne manque malheureusement pas d'idées. T

outes les semaines, de nombreuses escroqueries émergent avec l'objectif de toucher un maximum de victimes. Lorsque certaines se déroulent sur des parkings en simulant des accrosages au rétroviseur, d'autres se passent à distance, bien souvent par téléphone. C'est le cas de la technique dite du "wangiri", qui semble inquiéter les autorités européennes.

Le concept de l'arnaque wangiri est terriblement simple, et repose sur une seule action: un escroc appelle un numéro de téléphone et raccroche rapidement avant que la victime ne puisse décrocher. Le but étant pour les faussaires d'être rappelés sur un numéro en réalité surtaxé, où chaque seconde apporte du profit.

L'agence de sécurité européenne **Europol** rappelle quelques conseils pour repérer et filtrer ce genre d'appels. Si le téléphone ne sonne qu'une fois, que le numéro vous contacte à des heures tardives, en pleine journée à des moments peu propices pour répondre, ou encore qu'il s'agit d'un indicatif étranger, c'est probablement une arnaque.

Élaborée pour attiser la curiosité des victimes, cette entourloupe se décline facilement pour les fraudeurs. Selon Presse Citron, des systèmes informatiques permettent de lancer des dizaines d'appels simultanés et multiplient ainsi les chances de piéger des victimes. D'autant que l'utilisation de numéros utilisés, bien souvent étranger, complique les poursuites judiciaires.

Pour éviter de tomber facilement dans le piège, il est nécessaire d'appliquer quelques bonnes pratiques. **Si le correspondant inconnu vous contacte, ne le rappelez pas.** "Une personne qui cherche véritablement à vous joindre laissera un message ou vous appellera".

Si vous pensez qu'un numéro frauduleux vous a contacté, il est possible de le signaler au **3.37.00**. Une fois signalé, le numéro est ensuite envoyé aux principaux opérateurs téléphoniques. À noter que ce service marche aussi avec les SMS en envoyant une capture d'écran du message au même numéro. Enfin, si vous pensez avoir été victime d'une arnaque au wangiri, il est conseillé de se rapprocher de son opérateur téléphonique et des forces de l'ordre pour porter plainte si nécessaire.

Le Spoofing téléphonique est une pratique trompeuse par laquelle des escrocs manipulent l'information de l'appelant pour faire apparaître un numéro de téléphone différent sur le dispositif du destinataire de l'appel.

Quelqu'un utilise mon numéro de téléphone à mon insu, que faire ?

Il arrive que des numéros de téléphone de particuliers soient utilisés sans même que son propriétaire soit au courant, dans le cadre de démarchage. Une pratique appelée le « spoofing », et qui peut vite être désagréable voire dangereuse pour l'utilisateur.

Plusieurs formes de spoofing téléphonique existent, chacune avec ses propres caractéristiques et méthodologies :

Spoofing d'identité : faire croire que l'appel vient d'un individu ou d'une organisation spécifique.

Spoofing de numéro : affichage d'un numéro de téléphone autre que celui de l'appelant.

Spoofing de ligne directe : imitation d'une ligne téléphonique d'entreprise pour paraître légitime.

Intention malicieuse : utilisation dans le cadre d'activités frauduleuses ou de collecte d'informations personnelles.

Protections possibles : utilisation d'applications anti-spoofing pour filtrer les appels douteux.

Ces dernières années, des cas de spoofing téléphonique ont eu des conséquences désastreuses pour certains particuliers, dans des cas d'arnaques au faux banquier. À Toulon, un sexagénaire a été dépouillé de 5 700 euros. Il pensait échanger avec sa banque, dont le numéro avait été usurpé, et, suivant les consignes du faux conseiller, a divulgué des données et même confié sa carte bancaire à un soi-disant agent venu à son domicile. À Bagnol, une femme a littéralement vidé ses comptes - 20 000 euros - guidée par un escroc par téléphone, pensant, justement, placer ses économies sur un compte sécurisé. Les « pirates » jouent sur la confiance : un numéro en 06, un autre connu ou carrément enregistré dans votre répertoire... Difficile pour les usagers de percevoir l'arnaque qui s'annonce.

Un rapport de 2022 a révélé que plus de 50 % de toutes les attaques impliquent l'interception d'informations sensibles telles que les identifiants de connexion et les informations bancaires, conduisant à des pertes estimées à environ 2 milliards de dollars annuellement à l'échelle mondiale.

* **Les particuliers** victimes de spoofing peuvent subir diverses conséquences préjudiciables.

- Le phishing, via des appels de numéros usurpés, peut amener des personnes à divulguer involontairement des informations personnelles sensibles, menant à des fraudes financières ou à l'usurpation d'identité. De plus, la récurrence de ces appels frauduleux peut créer un climat d'insécurité et de méfiance chez le consommateur, qui peut se sentir vulnérable face à cette menace peu tangible mais persistante.

- Perte financière due à des virements initiés sous la contrainte ou l'escroquerie

- Atteinte à la confidentialité et usurpation d'identité si des données personnelles sont acquises

- Sentiment de violation et méfiance vis-à-vis des appels entrants.

* **Pour les entreprises**, le spoofing peut entraîner des risques significatifs, allant de la perte de réputation à des pertes économiques conséquentes. Un numéro d'entreprise usurpé peut aboutir à des campagnes d'arnaque ciblant ses clients, ébranlant ainsi la confiance qu'ils avaient envers la marque. Par ailleurs, les escrocs peuvent utiliser le spoofing pour obtenir des informations confidentielles d'employés dupés, déséquilibrant ainsi l'infrastructure informationnelle de l'entreprise.

- Fraude financière suite à des instructions de virement frauduleuses communiquées à un employé

- Détérioration de la relation client à la suite d'escroqueries perpétrées sous l'identité de l'entreprise

- Perturbations opérationnelles dû à une défiance généralisée envers les communications téléphoniques

Que dit la loi ? Quels recours ? Que faire ?

Bloctel : liste d'opposition au démarchage téléphonique, est une liste d'opposition au démarchage téléphonique généralisée qui a été introduite par l'article 9 de la loi du 17 mars 2014 relative à la consommation. Cette liste baptisée Bloctel a été mise en place le 1er juin 2016 par la société Opposetel, conformément à l'arrêté du 25 février 2016.

Les consommateurs qui s'inscrivent sur cette liste ne doivent plus recevoir d'appels commerciaux des entreprises avec lesquelles ils ne sont pas liés par contrat.

Aussi, si une entreprise ne respecte pas la liste d'opposition au démarchage téléphonique, le consommateur inscrit sur la liste peut faire un signalement via son compte Bloctel.

Le dispositif "33 700" : contre les SMS indésirables

Suite à la réception de SMS indésirables, les consommateurs peuvent les signaler grâce au dispositif "33 700".

Pour procéder au signalement, le consommateur pourra transférer le message indésirable par SMS au 33 700 ou via le site 33700.fr.

Les signalements sont ensuite transmis à l'opérateur de l'émetteur des SMS, ainsi qu'à celui du consommateur. Ces opérateurs traiteront les SMS signalés afin de mettre en œuvre des actions à l'encontre de l'émetteur des SMS.

La CNIL explique que les entreprises doivent obtenir le consentement du consommateur avant de lui envoyer des prospections commerciales par SMS-MMS.

Suite au décret n° 2021-1528 du 26 novembre 2021, les particuliers peuvent bénéficier depuis le 1er janvier 2022 de la reconduction tacite, par période de trois ans, inscription à la liste Bloctel, encadrée par les articles L. 223-1 et suivants du code de la consommation.

À partir du 11 août 2026 : Un professionnel ne pourra plus vous contacter à des fins commerciales sans avoir recueilli au préalable votre consentement explicite, libre, spécifique, éclairé et révoquant. En pratique, cela signifie que vous ne pourrez être démarché par téléphone qu'à la condition de l'avoir expressément accepté au préalable. Plus aucune inscription ne sera requise.

L'**Arcep** "L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep)", vous invite à contacter votre opérateur téléphonique pour signaler le problème. " Il lui sera possible d'agir selon les cas. " Elle suggère également de signaler son cas sur la plateforme « [J'alerte l'Arcep](#) ». " Cela résoudra pas son problème, c'est un geste citoyen qui permettra d'améliorer notre connaissance de cette pratique " précise l'organisme.

Si le problème persiste, il est conseillé de porter plainte pour usurpation d'identité. L'Arcep donne des conseils en ce sens.

Que dit la loi ?

Concrètement, c'est la loi dite Naegelen adoptée le **24 juillet 2020**, " et en cours d'application ", qui vise à encadrer le démarchage téléphonique. Dans cette loi, plusieurs dispositions doivent contribuer à la lutte contre les appels frauduleux, notamment grâce au mécanisme d'**authentification du numéro (MAN)**. Un mécanisme déjà en place aux États-Unis et au Canada. " La France est le troisième pays à mettre en place un tel mécanisme et le seul à avoir l'ambition de proposer de couper automatiquement les appels mal authentifiés ou non authentifiés " résume la direction de la communication de l'Arcep. Si plusieurs dispositifs de la nouvelle loi sont déjà mis en place par certains opérateurs - comme la possibilité de bloquer des appels malveillants et les démarchages automatiquement grâce à leur dispositif d'identification - d'autres mesures ont pris du retard. Et notamment l'interruption de l'acheminement d'un appel ou d'un message si le dispositif d'authentification en vigueur n'est pas utilisé, ou s'il ne permet pas de confirmer l'authenticité de l'appel ou du message.

Un retard dû à " la complexité des changements demandés pour les infrastructures de téléphonie " justifie l'Arcep. " La loi contribue et contribuera à renforcer la protection des utilisateurs et pourrait, dans le cas de votre lecteur, répondre à son problème d'ici la fin 2024. "

Cependant, le « gendarme des télécoms » prévient que " toutes les escroqueries ne pourront malheureusement être évitées par le MAN, mais c'est une étape importante dans l'encadrement du démarchage. "

Spoofing une pratique légale

De manière surprenante, cette pratique est autorisée en France. Si le centre d'appel ne procède pas à aucune fraude ou arnaque, il est libre de se « cacher » derrière un numéro qui ne lui appartient pas. Ce spoofing est considéré comme « non nocif » par loi.

Comment se protéger du spoofing téléphonique ?

Malheureusement le spoofing téléphonique souffre d'un vide juridique. Bien qu'il soit autorisé dans certaines conditions (par exemple, lorsqu'un opérateur sous-traite agit pour le compte d'une entreprise qui veut être recontactée directement), des abus sont constatés.

Voici quelques mesures que vous pouvez prendre :

- Ne faites pas confiance aveuglément aux afficheurs de numéros : Même si un numéro semble familier ou local, ne présumez pas automatiquement qu'il est légitime. Les fraudeurs peuvent facilement falsifier ces informations.
- Ne rappelez pas les numéros inconnus : Si vous recevez un appel d'un numéro que vous ne connaissez pas, évitez de rappeler directement. Si c'est important, ils laisseront probablement un message.
- Utilisez des applications de filtrage d'appels : Des applications tierces peuvent identifier et bloquer les appels suspects. Recherchez des applications fiables sur votre plateforme d'appareil mobile (iOS ou Android).
- Soyez prudent avec vos informations personnelles : Ne partagez pas d'informations sensibles (comme vos coordonnées bancaires) au téléphone, même si l'appelant prétend être une institution légitime.
- Signalez les appels suspects : Si vous recevez un appel suspect, signalez-le à votre opérateur téléphonique et aux autorités compétentes.
- Vérifiez les numéros en ligne : Utilisez des sites web de vérification de numéros pour rechercher des informations sur les numéros inconnus avant de répondre.
- Méfiez-vous des appels urgents et menaçants : Les fraudeurs utilisent souvent des tactiques de peur pour inciter les gens à agir rapidement. Restez calme et prenez le temps d'évaluer la situation.

Face à la multiplication des fraudes téléphoniques et à la perte de confiance des consommateurs, la mise en place du **Mécanisme d'Authentification des Numéros (MAN)** représente un premier outil essentiel dans la lutte contre le « spoofing », plus communément appelé « usurpation d'identité ».

1er octobre 2024 pourrait marquer un tournant dans la lutte contre le démarchage abusif et les arnaques téléphoniques. On vous explique ce qu'il change, et pourquoi il va falloir encore se méfier.

Le Mécanisme d'Authentification des Numéros (MAN) ou STIR/SHAKEN pour ses équivalents internationaux, est un protocole conçu pour authentifier les appels émis, en vérifiant que le numéro affiché est bien celui de l'appelant légitime. Cela répond à un besoin croissant de sécuriser les interactions téléphoniques, surtout avec la montée en puissance des fraudes et du « spoofing », une technique où des numéros sont falsifiés pour tromper les destinataires.

Le MAN fonctionne grâce à une architecture basée sur des certificats numériques. Lorsqu'un appel est initié, le fournisseur de téléphonie de l'appelant signe l'appel avec une clé liée à un certificat attestant l'authenticité du numéro (et son niveau de confiance A,B ou C). Ce certificat est utilisé pour vérifier le numéro de l'appelant à chaque étape de l'acheminement de l'appel, jusqu'à ce qu'il atteigne le destinataire. Ce dernier peut ainsi savoir avec certitude si l'appel provient bien du numéro affiché.

Le MAN offre une solution proactive en assurant une identification précise de l'appelant. Les entreprises qui adoptent ce protocole montrent ainsi un engagement fort envers la sécurité de leurs clients, tout en renforçant leur propre crédibilité.

Le MAN repose principalement sur deux technologies :

STIR (Secure Telephone Identity Revisited) : qui permet d'attacher une signature cryptographique à l'appel en cours pour garantir l'identité de l'appelant.

SHAKEN (Signature-based Handling of Asserted information using toKENs) : qui valide l'intégrité de cette signature tout au long du processus de l'appel.

Ces technologies créent un lien de confiance entre les opérateurs téléphoniques et les entreprises, empêchant ainsi les usurpateurs de faire passer des appels frauduleux. En pratique, chaque appel se voit attribuer un des trois niveaux d'attestation :

Niveau A : L'opérateur certifie et authentifie l'appelant et le numéro.

Niveau B : L'opérateur connaît l'appelant mais ne peut pas vérifier l'intégrité du numéro.

Niveau C : L'opérateur n'a aucune information fiable sur l'appelant.

Le planning de montée en charge du MAN, qui a été présenté à l'Arcep a été le suivant :

Au 1er juin 2024 : Tous les opérateurs ont déployé le MAN sur toutes leurs interconnexions SIP, sans coupure à ce stade des appels non authentifiés. Tous les opérateurs effectuent les remontées prévues (traces et volumétries) sur la plateforme MAN de façon à pouvoir communiquer des éléments consolidés et effectuer le suivi du dispositif.

Au 1er octobre 2024 : Coupure des appels non authentifiés.

... A suivre

La loi n° 2021-402 du 8 avril 2021 a créé un nouvel article dans le code des assurances, l'article L.112-2-2. Il fixe plusieurs obligations aux distributeurs d'assurances qui contactent par téléphone un souscripteur ou un adhérent éventuel en vue de la conclusion d'un contrat d'assurance. Les principales obligations sont :

- La demande de l'accord du consommateur au début l'appel pour poursuivre l'échange téléphonique
- L'arrêt de l'échange téléphonique si le consommateur indique, au cours de la communication, qu'il n'est pas intéressé par la proposition commerciale.
- Le délai de 24h entre un accord téléphonique et la signature d'un contrat

La loi no 2022-1587 du 19 décembre 2022 visant à lutter contre la fraude au compte personnel de formation et à interdire le démarchage de ses titulaires prohibe « toute prospection commerciale des titulaires d'un compte personnel de formation, par voie téléphonique, par message provenant d'un service de communications interpersonnelles, par courrier électronique ou sur un service de réseaux sociaux en ligne visant à collecter leurs données à caractère personnel, notamment le montant des droits [...] et conclure des contrats ». La violation de cette disposition est passible d'une amende pouvant s'élever à 75 000 € pour une personne physique et 375 000 € pour une personne morale. Le démarchage reste autorisé s'il est lié à une action de formation en cours entre le titulaire du compte et l'organisme de formation.

Autre évolution en ce 1er janvier 2023 : l'interdiction du démarchage lié aux comptes personnels de formation (CPF).

Le décret n° 2022-34 du 17 janvier 2022 relatif au démarchage téléphonique en assurance renforce l'information des assurés. Ce décret encadre les appels non sollicités à visée commerciale (dit « appels à froid »), interdit explicitement les ventes réalisées lors d'un premier appel téléphonique (ou « ventes en un temps »), et précise les modalités de recueil du consentement des consommateurs. Il prévoit également une obligation de conservation des enregistrements des appels de vente durant une période de de années.

De nouvelles règles relatives au démarchage téléphonique sont entrées en vigueur le 1er janvier 2023.

Les plateformes commerciales ne pourront plus utiliser de numéros mobiles (commençant par 06 ou 07). Elles devront obligatoirement utiliser un identifiant commençant par des numéros précis.

L'Arcep, dans une décision datée du 1er septembre, a interdit certains types de numéros de téléphone aux sociétés commerciales en général et aux plateformes de démarchage en particulier, qui ne pourront plus les utiliser pour appeler en masse ou envoyer des SMS non sollicités.

La décision de l'Arcep interdit aux sociétés d'utiliser des numéros commençant par 06 ou 07. Ces numéros sont associés dans l'esprit des particuliers à des appareils mobile et obtiennent donc de meilleurs taux de réponse que les numéros fixes, d'où leur détournement par les sociétés de démarchage. L'utilisation de numéros dits « géographiques » (commençant par 01 à 05 en fonction de la région d'où ils proviennent) est également limitée à certains numéros.

Depuis le 1er janvier 2023, les plateformes de démarchage pourront donc utiliser uniquement des numéros commençant par 09 37, 09 38 et 09 39 réservés aux plateformes techniques, et les démarcheurs devront utiliser les numéros débutant par 09 48 et 09 49, 01 62 et 01 63, 02 70 et 02 71, 03 77 et 03 78, 04 24 et 04 25, 05 68 et 05 69.

Les numéros commençant par 09 37, 09 38 et 09 39 pourront, eux, être utilisés par des entreprises dans leurs relations avec les clients : conducteurs de véhicule de tourisme avec chauffeur, livreurs de colis, employés de service après-vente, etc.

Par cette mesure, l'Arcep vise à réduire l'empreinte environnementale du numérique en réduisant le démarchage téléphonique, mais aussi à protéger les consommateurs.

L'Autorité indique en effet avoir reçu « de multiples signalements d'utilisateurs à travers sa plateforme "J'alerte l'Arcep" qui témoignaient de l'utilisation de numéros mobiles à 10 chiffres pour l'envoi en masse de messages SMS dits A2P, souvent à des fins publicitaires, voire frauduleuses dans certains cas »

L'article L223-1 du code de la consommation interdit en particulier toute prospection commerciale de consommateurs par des professionnels, par voie téléphonique, ayant pour objet la vente d'équipements ou la réalisation de travaux pour des logements en vue de la réalisation d'économies d'énergie ou de la production d'énergies renouvelables, à l'exception des sollicitations intervenant dans le cadre de l'exécution d'un contrat en cours.

Depuis le 1er mars 2023, le démarchage téléphonique des consommateurs est autorisé uniquement du lundi au vendredi, de 10 heures à 13 heures et de 14 heures à 20 heures (c'est le fuseau horaire du consommateur qui est pris en compte). Il est interdit le samedi, le dimanche et les jours fériés. Ces horaires ont été déterminés dans le décret n° 2022-1313 du 13 octobre 2022.

Mais les fraudeurs ont encore de la marge de manoeuvre :

Changer le numéro affiché lorsque vous appelez quelqu'un peut être utile ou néfaste dans diverses situations, que ce soit pour préserver votre vie privée ou pour des raisons professionnelles, ou se masquer derrière un autre numéro. Cependant, il est important de noter que masquer votre numéro peut être illégal dans certaines circonstances et pays, notamment pour les appels d'urgence.

La méthode que vous utiliserez dépendra du type de téléphone ou du service que vous utilisez.

Comment changer votre numéro lorsque vous appelez quelqu'un ?

Pour les téléphones fixes traditionnels, les options de modification du numéro d'appelant sont souvent limitées par les fonctionnalités offertes par votre opérateur téléphonique.

Blocage de l'ID d'appelant : La plupart des opérateurs permettent de bloquer votre numéro pour un appel spécifique en composant un préfixe avant le numéro de votre correspondant. Par exemple, aux États-Unis, vous pouvez utiliser *67. Il est essentiel de vérifier avec votre opérateur le code correct à utiliser dans votre pays.

Affichage permanent de l'ID d'appelant : Certains opérateurs offrent également la possibilité de bloquer votre numéro de manière permanente pour tous les appels sortants. Cela nécessite généralement de contacter le service clientèle de votre opérateur pour configurer cette option.

Téléphones portables

Les portables offrent plus de flexibilité et d'options pour masquer ou changer votre numéro d'appelant.

De nombreux smartphones incluent une option dans l'application Téléphone pour masquer votre numéro pour tous les appels ou pour des appels individuels. Cette fonctionnalité est souvent accessible via les paramètres d'appel ou d'ID de l'appelant.

Codes spécifiques à l'opérateur : Certains opérateurs mobiles fournissent des codes spéciaux que vous pouvez composer avant le numéro de téléphone pour masquer votre numéro. Par exemple, en France, vous pouvez utiliser #31# suivi du numéro de téléphone.

Applications VoIP (Skype, WhatsApp, etc.)

Les applications de téléphonie sur Internet (VoIP) offrent également des options pour masquer ou changer votre numéro d'appelant.

Certaines applications VoIP permettent de configurer des options pour masquer votre numéro d'appelant dans les paramètres de l'application. Vous pouvez généralement trouver cette option dans les paramètres d'appel ou de confidentialité.

Services spécialisés

Pour ceux qui cherchent des solutions plus avancées, des services spécialisés offrent des fonctionnalités supplémentaires pour masquer ou changer votre numéro d'appelant.

Applications de numéro virtuel : Des applications comme **Burner** permettent de créer des numéros de téléphone temporaires pour passer des appels et envoyer des SMS de manière anonyme. Ces services sont idéaux pour les situations où vous avez besoin d'un numéro de téléphone temporaire.

Services d'appel masqué : Certains services vous permettent de passer des appels anonymes via leurs plateformes. Ces services sont souvent utilisés pour des raisons de sécurité ou de confidentialité.

Il est crucial de comprendre que masquer votre numéro d'appelant peut être illégal dans certaines situations et juridictions. Par exemple, dans de nombreux pays, il est interdit de masquer son numéro pour les appels d'urgence. De plus, certaines entreprises et services peuvent exiger que votre numéro soit visible pour des raisons de sécurité et de vérification.

Même lorsque vous masquez votre numéro, il peut parfois être visible pour le destinataire via des services d'identification de l'appelant ou s'il a un historique d'appels avec vous. De plus, certaines applications et services peuvent avoir des moyens de contourner le masquage de votre numéro.

Solutions et initiatives

Blocage de l'ID de l'appelant sur votre appareil

La méthode la plus simple et la plus courante pour masquer votre numéro d'appelant est de configurer les paramètres de votre appareil ou d'utiliser des codes spécifiques à l'opérateur.

Utilisation du préfixe de blocage de l'ID de l'appelant

Pour un masquage temporaire, l'utilisation de préfixes spécifiques avant le numéro de téléphone est une solution rapide et efficace. Par exemple, aux États-Unis, composez *67 avant le numéro pour rendre votre appel anonyme.

Services de téléphonie sur Internet (VoIP)

Les services VoIP offrent des options supplémentaires pour masquer votre numéro d'appelant. Vérifiez les paramètres de votre application VoIP pour voir si cette option est disponible.

Applications de numéro virtuel : Pour des besoins plus avancés, les applications de numéro virtuel comme Burner offrent des numéros de téléphone temporaires pour une utilisation anonyme. Ces services sont souvent utilisés par les personnes qui souhaitent préserver leur vie privée tout en communiquant efficacement.

Obtenir un Numéro temporaire :

Si vous cherchez un numéro temporaire gratuit, il est possible de vous le procurer sur certains sites Internet tels que **Clickatell** .

Il s'agit de sites internationaux et le numéro provisoire que vous choisissez n'est utilisable qu'en ligne, il s'agit d'un numéro jetable qui ne dure que 24h. Le numéro doit servir à vous authentifier sur les sites Internet qui le demandent. Le code est envoyé directement sur la plateforme clickatell mais attention, il est visible par tout le monde, car

plusieurs personnes peuvent utiliser le même numéro. D'ailleurs vous trouverez un disclaimer écrit en rouge sur le site en question «Tout le monde peut voir le contenu du code de vérification SMS, veuillez ne pas l'utiliser pour enregistrer des informations importantes.»

Pour utiliser un numéro sur l'un de ces sites, cliquez simplement sur l'un des numéros proposés pour la France, et copiez-collez le numéro sur le site Internet qui vous demande une double authentification. Ensuite, il vous suffira de consulter les SMS envoyés sur le numéro en cliquant sur le numéro.

L'application Virty.com : vous avez la possibilité de vous procurer un numéro de téléphone provisoire qui vous permet de recevoir vos SMS en ligne, pour des prix démarrent à partir de 1,49€. Ces numéros sont loués par l'entreprise un peu partout dans le monde (Belgique, Espagne, France, Royaume-Uni, Pologne, Suède, USA, / et sont très utilisés pour confirmer des comptes sur Internet (attention, les numéros Virty ne peuvent pas être utilisés pour l'authentification Facebook et Google).

Vous devez vous inscrire avec votre adresse mail et un mot de passe personnel et

Pour 1,49€, vous obtenez un numéro de téléphone temporaire qui sera valable 24h.

Pour 2,79€ vous obtenez un numéro de téléphone temporaire qui sera valable 48h.

Pour 6,99€ vous obtenez un numéro de téléphone temporaire qui sera valable une semaine et la possibilité d'obtenir un nouveau numéro virtuel si celui qui vous est fourni ne vous convient pas.

Toutes les offres sont renouvelables une fois arrivées à échéance. Les offres peuvent être accompagnées d'un pack de crédits SMS qui permet de faire rediriger les SMS reçus sur votre numéro virtuel directement vers votre numéro personnel (et donc sur votre mobile).

L'application ligne Bis est un service qui vous permet d'obtenir un numéro virtuel et temporaire en seulement quelques minutes, par le biais d'un simple appel. Les numéros Ligne Bis sont valables sur une période de 15 jours, renouvelable, et vous pouvez faire le choix de renouveler cette période. Pour obtenir un numéro Ligne Bis, vous devez appeler le 36 36.

Cet appel vous sera facturé 3€, qui seront prélevés par votre opérateur mobile actuel. Au téléphone, il vous sera demandé de saisir votre numéro de département : vous obtiendrez ainsi un numéro virtuel et provisoire qui commencera par l'indicatif de votre région, et qui sera automatiquement associé à votre numéro de ligne privée. Votre numéro de téléphone vous sera ensuite envoyé par SMS et l'activation est immédiate.

À savoir 48h avant la fin des deux semaines, vous recevrez un SMS qui vous invitera si vous le souhaitez à renouveler la validité de votre numéro virtuel temporaire, en rappelant le 36 36. Les numéros Ligne Bis vous permettent d'utiliser WhatsApp, d'accéder à un service de messagerie vocale, et d'appeler vos interlocuteurs.

Onoff est une entreprise qui vous permet d'obtenir un second numéro de téléphone directement sur votre mobile, grâce à une application. Vous avez la possibilité d'obtenir un numéro personnel ou un numéro professionnel. Il s'agit d'offres sans engagement : vous avez donc la possibilité d'arrêter le service quand bon vous semble. Les offres Onoff démarrent à partir de 4,99€ par mois pour l'offre Starter avec appels et SMS illimités. Pour vous abonner à Onoff, il vous suffit de télécharger l'application sur votre mobile.

Onoff propose aussi une offre business dédiée aux entreprises et aux gestionnaires de flottes mobiles, qui permet d'attribuer des numéros professionnels à des employés en seulement quelques clics. Ici encore, le service passe par l'application Onoff, qui peut se synchroniser avec Microsoft Teams. Les numéros mobiles Onoff Business sont à partir de 15€ par mois.

L'application **Burner** pratique mais moyennant un abonnement mensuel. On peut créer et garder un nombre illimité de numéros de téléphone et les détruire en toute sécurité une fois qu'on n'en a plus besoin.

...

Autres alternatives :

1 - Le changement de numéro de téléphone fixe ou mobile est généralement disponible directement en ligne via l'espace abonné ou en contactant le service client de votre opérateur.

Tous les opérateurs du marché proposent à leurs abonnés la possibilité de changer de numéro de téléphone sur demande, avec dans la plupart du temps, des frais additionnels d'une dizaine d'euros à payer sur la facture suivante.

En exemple : **Comment changer son numéro de téléphone Free ?**

Vous avez la possibilité de modifier votre numéro de téléphone Free, sans changer de forfait. Pour cela, il vous suffit de vous connecter depuis votre Espace Abonné à l'aide de vos identifiants mobile. Free vous proposera une série de numéros parmi une liste déroulante de 10 numéros au choix. Une fois le choix de changement de numéro effectué, l'abonné sera facturé à hauteur de 5€ et devra régler cette somme par carte bancaire.

L'option changer de numéro avec l'opérateur Free est de loin l'option la moins chère par rapport à ce que proposent les concurrents.

Le nouveau numéro est mis en service immédiatement. Un redémarrage de votre téléphone peut s'avérer nécessaire.

Vous aurez la possibilité de changer de numéro de téléphone à nouveau dans un délai de 30 jours. L'ancien numéro ne pourra être récupéré et sera définitivement perdu.

2 - Si vous êtes victime de harcèlement téléphonique, vous pouvez déposer une main courante au commissariat le plus proche de chez vous. Si la situation s'aggrave, il vous sera possible de déposer plainte auprès des services compétents. Pour cela, il est nécessaire de réunir les preuves suffisantes comme le numéro de téléphone qui vous harcèle avec la liste des SMS et des appels répétitifs reçus. Vous avez un délai de 6 ans depuis le dernier appel malveillant pour effectuer cette démarche. En général, en cas de motif légitime et après avoir porté plainte au commissariat de police, l'abonné peut obtenir le changement de numéro gratuitement. Il devra contacter son opérateur et lui fournir une copie de la plainte et des preuves pour obtenir un nouveau numéro sans payer des frais additionnels.

3- Si vous souhaitez un numéro temporaire pour une durée plus longue et que cela ne vous dérange pas de changer de carte SIM, il existe une solution simple et très courante : l'achat d'une carte SIM prépayée. Ces cartes SIM se trouvent en général dans les grandes surfaces et bureaux de tabac, vous pouvez également les acheter auprès de votre opérateur. Elles sont en général très peu chères, et vous les rechargez à l'aide du crédit de communication dont vous avez besoin. En outre, les numéros de mobile obtenus par les SIM prépayées n'ont aucun risque d'être interdit par certains sites tels que Google ou Facebook, qui ont durci leurs contrôles. Ici, il s'agit en quelque sorte de l'ouverture d'une seconde ligne, puisque vous obtenez une seconde carte SIM. Les démarches sont en revanche très simplifiées par rapport à la souscription d'un forfait mobile avec ou sans engagement.

Quels sont les différents types de fraude bancaire ?

Il existe plusieurs formes d'arnaque bancaire. Comme nous le savons, les banques sont les cibles des toutes les personnes malveillantes. Les banques au sens propre et au sens figuré. Car, même les banques d'énergies, les banques de données, les banques des images et autres sont la cible des personnes malveillantes. Mais, revenons à la banque que nous connaissons tous. En effet l'argent est le nerf de la guerre. Si les fraudeurs visent tant les banques, c'est notamment parce que, l'argent y est stocké et cet argent sert à tout acheter. Raison pour laquelle les personnes malveillantes utilisent toutes les techniques possibles pour extorquer de l'argent tous les clients qui possèdent des comptes bancaires. Comment ces derniers s'y prennent :

La fraude aux coordonnées bancaires

Le chantage à la webcam

La fraude au conseiller bancaire

Le ransomware

Les arnaques via les produits commercialisés sur les réseaux sociaux (voiture, trottinette, meubles)

Le faux prêt

La fraude au sentiment (application de rencontre)

La fraude des amendes Pv ou tests techniques ou entretiens d'embauche pour récupérer vos coordonnées bancaires (Rib).

Veuillez faire vraiment attention à toutes ces formes d'arnaque, car le but consiste à récupérer vos coordonnées bancaires et ensuite à s'en servir pour vider votre compte bancaire.

Quelles infractions peuvent-être retenues contre les cybercriminels ?

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

• **Prospection sans consentement préalable** (article L121-20-5 du Code de la consommation et article L34-5 du Code des postes et communications électroniques) : « est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen. Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ».

Selon l'article L470-1 du Code du commerce, « lorsque le professionnel concerné n'a pas déféré dans le délai imparti à une injonction qui lui a été notifiée à raison d'une infraction ou d'un manquement passible d'une amende administrative, l'autorité administrative chargée de la concurrence et de la consommation peut prononcer à son encontre, dans les conditions et selon les modalités prévues à l'article L. 470-2, une amende administrative dont le montant ne peut excéder 3000 € pour une personne physique et 15000 € pour une personne morale ».

Par ailleurs, selon l'article R10-1 du Code des postes et des communications électroniques, « le fait d'utiliser, dans des opérations de prospection directe, des données à

caractère personnel relatives à des personnes ayant exprimé leur opposition, par application des dispositions du 4 de l'article R.10, quel que soit le mode d'accès à ces données, est puni, pour chaque correspondance ou chaque appel, de l'amende prévue pour les contraventions de la quatrième classe, sans préjudice de l'application du premier alinéa de l'article 226-18 du code pénal ».

En outre, l'article 226-18-1 stipule que « le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de d'emprisonnement et de 300000 euros d'amende. »

• **Pratique commerciale trompeuse** (article L121-2 du Code de la consommation): « une pratique commerciale est trompeuse lorsqu'elle crée une confusion avec un autre bien ou service, une marque, un nom commercial, ou un autre signe distinctif d'un concurrent, lorsqu'elle repose sur des allégations, indications ou présentations fausses ou de nature à induire en erreur ou bien encore lorsque la personne pour le compte de laquelle elle est mise en œuvre n'est pas clairement identifiable. »

Selon l'article L121-6 du Code de la consommation, les pratiques commerciales trompeuses sont punies d'un emprisonnement de deux ans et d'une amende de 300000 €. Le montant de l'amende peut être porté, de manière proportionnée aux avantages tirés du manquement, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits, ou à 50 % des dépenses engagées pour la réalisation de la publicité ou de la pratique constituant le délit.

Lorsque le spam téléphonique a pour fonction ou objet de tromper dans un but de captation de données ou de fonds :

• **Escroquerie** (article 313-1 du code pénal) : « l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge ». L'escroquerie est punie de cinq ans d'emprisonnement et de 375000 euros d'amende.

• **Tromperie en matière commerciale** (article L213-1 du Code de la consommation): « sera puni d'un emprisonnement de deux ans au plus et d'une amende de 300000 euros quiconque, qu'il soit ou non partie au contrat, aura trompé ou tenté de tromper le contractant, par quelque moyen ou procédé que ce soit, même par l'intermédiaire d'un tiers, soit sur la nature, l'espèce, l'origine, les qualités substantielles, la composition ou la teneur en principes utiles de toutes marchandises, soit sur la quantité des choses livrées ou sur leur identité par la livraison d'une marchandise autre que la chose déterminée qui a fait l'objet du contrat ou bien soit sur l'aptitude à l'emploi, les risques inhérents à l'utilisation du produit, les contrôles effectués, les modes d'emploi ou les précautions à prendre ». Le montant de l'amende peut être porté, de manière proportionnée aux avantages tirés du manquement, à 10 % du chiffre d'affaires moyen annuel, calculé sur les trois derniers chiffres d'affaires annuels connus à la date des faits.

Si le spam téléphonique s'apparente à un harcèlement caractérisé (répétition et volonté de nuire à la victime / ne comprend pas le démarchage publicitaire) :

• **Harcèlement téléphonique** (article 222-16 du code pénal) : « les appels téléphoniques malveillants réitérés, les envois réitérés de messages malveillants émis par la voie des communications électroniques ou les agressions sonores en vue de troubler la tranquillité d'autrui sont punis d'un an d'emprisonnement et de 15000 euros d'amende. »