la médiation
des communications
électroniques

Fiche pratique

Se protéger contre les fraudes en ligne

Depuis 2020, on observe une explosion des tentatives de fraudes avec l'utilisation des techniques de phishing (ou hameçonnage) et de spoofing (usurpation d'identité) de plus en plus sophistiquées, ce qui nécessite d'être vigilant. D'autres escroqueries se développent, comme par exemple le smishing (ou hameçonnage par SMS), le SIM Swapping et la fraude au RIO.
En outre, les opérateurs peuvent être victimes d'une cyberattaque avec une fuite des données personnelles des comptes clients, comme cela a été le cas en 2024 et 2025.

Le mode opératoire du phishing ou smishing et ses conséquences

Le phishing ou smishing est une technique consistant, pour une personne mal intentionnée, à faire croire à la victime qu'elle s'adresse à un tiers de confiance en l'invitant, par exemple, à lui transmettre ses identifiants et codes confidentiels. Pour ce faire, la victime reçoit un mail ou un SMS d'une personne se faisant passer pour un tiers de confiance comme son opérateur par exemple. En cliquant sur le lien présent dans le message frauduleux, la victime abonnée de cet opérateur est automatiquement renvoyée sur une page Internet contrefaite, portant le logo du tiers de confiance. Convaincue de naviguer sur le site Internet du tiers de confiance, la victime ciblée par le phishing, fournit spontanément les diverses informations qui lui sont réclamées, et notamment l'identifiant et le mot de passe permettant d'accéder à son espace client.
A titre d'exemples, il est demandé de « mettre à jour » ou de « confirmer suite à un incident technique » ses données. Ou, il est prétendu « qu'un colis est en attente de livraison ».
Il convient de se méfier d'un mail ou SMS alarmiste ou alléguant un prétendu remboursement.

LES RÉFLEXES POUR SE PROTÉGER :

- Prendre en compte les conseils qui figurent sur le site de votre opérateur ;
- Adopter la règle d'or de ne jamais communiquer d'informations sensibles à qui que ce soit ;
- Ne jamais cliquer sur les liens suspects contenus dans les SMS ou mails (ou positionner le curseur de la souris sur le lien- sans cliquer- pour vérifier la vraisemblance) ;
- Vérifier toujours l'identité de votre interlocuteur et s'assurer que l'adresse du site (son URL) est bien l'adresse habituelle ;
- Privilégier la saisie d'informations personnelles (coordonnées bancaires, identifiants…) sur des sites internet sécurisés. Attention, le cadenas qui apparaît dans le navigateur et l'adresse du site qui commence par Https au lieu de http, ne garantissent pas que le site n'est pas un faux ;
- Changer régulièrement de mots de passe qui doivent être suffisamment solides et complexes ou utiliser un générateur de mots de passe ;
- S'assurer que l'anti-virus est mis à jour et utiliser les fonctionnalités de protection contre le phishing et les logiciels malveillants proposées par les navigateurs internet ;
- Installer un logiciel de filtre anti-spam.

la médiation
des communications
électroniques

Le mode opératoire du spoofing téléphonique

Le fraudeur va usurper l'identité d'une personne et le numéro de téléphone. Il va se faire passer par exemple pour un conseiller bancaire qui prétend que des opérations suspectes apparaissent sur le compte. Pour paraître crédible, il fournit des données personnelles (identité etc.) afin d'obtenir des mots de passe ou des codes de sécurité reçus par SMS et pouvoir ainsi réaliser des transactions financières.

La loi Naegelen du 24 juillet 2020 a pour objectif de lutter contre les abus liés aux appels téléphoniques indésirables, qu'il s'agisse de démarchage excessif ou de fraudes fondées sur l'usurpation de numéros (spoofing). Un Mécanisme d'Authentification des Numéros ou MAN a été mis en place. Ainsi, depuis le 1er octobre 2024, les opérateurs doivent désormais authentifier chaque appel émis avant qu'il ne soit acheminé vers son destinataire. Si un numéro ne peut être vérifié ou si l'émetteur ne peut prouver qu'il est bien propriétaire du numéro qu'il utilise, l'appel est automatiquement bloqué.

LES RÉFLEXES POUR SE PROTÉGER :

- Raccrocher immédiatement en cas de doute sur un appel et contacter votre banque par les moyens habituels ;
- Vérifier votre compte bancaire et, si nécessaire, prévenir votre banque, faire opposition et changer vos mots de passe ;
- Ne jamais communiquer de données sensibles par téléphone ni valider de transactions à la demande de l'interlocuteur ;
- Porter plainte si des sommes non autorisées ont été débitées sur le compte.

Le mode opératoire du SIM Swapping (échange frauduleux de carte SIM)

Le fraudeur utilise des données personnelles déjà compromises (nom, date de naissance etc.) afin de contacter l'opérateur pour obtenir un renouvellement de carte SIM en prétextant une perte ou un vol de carte SIM. Il peut aussi, grâce aux données compromises, se connecter sur l'espace client, modifier l'adresse mail de contact, le mot de passe et l'adresse postale et demander un renouvellement de carte SIM qui sera livrée à sa propre adresse. Si la demande aboutit, l'opérateur désactive la carte SIM légitime. Le fraudeur récupère alors le numéro de téléphone sur une nouvelle carte SIM. Il va pouvoir ainsi recevoir les SMS contenant les codes de sécurité à usage unique permettant d'accéder aux espaces clients de la victime, les codes permettant de valider les paiements en ligne ou ceux permettant de valider des opérations sensibles auprès de la banque.
Il peut aussi émettre des appels et SMS à l'insu de la victime entraînant une surfacturation par l'opérateur.

LES RÉFLEXES POUR SE PROTÉGER :

- Contacter le plus tôt possible votre opérateur en cas de perte de réseau et si le message « carte SIM désactivée ou absente » apparaît ;
- Vérifier que l'adresse mail de contact, le mot de passe de l'espace client et l'adresse postale n'ont pas été modifiés, et si tel est le cas, modifier immédiatement ces informations
- Changer de mot de passe et porter plainte, le cas échéant.

la médiation
des communications
électroniques

Le mode opératoire de la fraude au RIO (identifiant unique)

Pour arriver à ses fins, le fraudeur peut se faire passer pour le service technique ou un conseiller de l'opérateur afin d'inciter le consommateur à envoyer son Relevé d'Identité Opérateur (RIO) via un lien frauduleux, souvent sous prétexte de mise à jour de sécurité. Grâce à un phishing ou à des données personnelles compromises, celui-ci peut également accéder à l'espace client de la victime pour récupérer le RIO. Il peut en outre contacter le Service Client en se faisant passer pour le client et répondre aux questions de sécurité, grâce aux données personnelles compromises. Une fois le RIO obtenu, le fraudeur va demander la portabilité du numéro vers un autre opérateur et ainsi récupérer l'usage du numéro.
Cette fraude a pour conséquence la perte de la ligne. De plus, le fraudeur qui a récupéré le numéro recevra les SMS destinés à la victime et notamment les SMS de sécurité ou de double authentification permettant de valider des transactions bancaires ou d'accéder aux espaces clients des sites internet de la victime. Il peut ainsi usurper l'identité de la victime et réaliser des opérations frauduleuses (achats, virements…).

Les réflexes pour se protéger :

- Ne jamais communiquer son RIO ;
- Prêter attention aux SMS annonçant qu'une portabilité du numéro va être réalisée ;
- Contacter immédiatement l'opérateur pour annuler la portabilité ;
- Changer immédiatement les identifiants et mot de passe de l'espace client de l'opérateur ;
- Porter plainte.

Cyberattaque des sites des opérateurs

Les opérateurs peuvent aussi être victimes de cyberattaques, comme La Poste Mobile en 2022, SFR et Free en 2024 ou encore Bouygues Telecom en 2025. Ces cyberattaques ont pour conséquences la fuite de données personnelles des clients concernés (coordonnées, informations sur les contrats, IBAN…). Les données personnelles volées peuvent ensuite être utilisées par les fraudeurs pour effectuer des phishing, des escroqueries, des usurpations d'identité, des SIM Swapping ou encore des prélèvements ou paiements bancaires non autorisés.

Les réflexes pour se protéger :

- Prendre connaissance du mail d'information envoyé par l'opérateur ciblé pour vérifier quelles données ont été concernées par l'attaque (données d'état civil, numéro de téléphone…) et mettre à jour les mots de passe ;
- Ne pas cliquer sur les liens reçus par SMS ou mails, prétendument envoyés par votre banque qui alertent d'une opération suspecte sur votre compte (smishing et phishing) ;
- Être particulièrement méfiant face à tout appel téléphonique ou message de personnes qui prétendraient vous connaître ;
- Alerter immédiatement l'opérateur en cas de perte prolongée de la connexion ;
- Surveiller le compte bancaire si l'IBAN a été dérobé ;
- Déposer plainte en cas d'utilisation frauduleuse de vos données.

la médiation
des communications
électroniques

En cas de prélèvements frauduleux : que devez-vous faire ?

Il vous appartient de vous rapprocher de votre banque pour contester les prélèvements et obtenir un remboursement. Conformément aux dispositions du Code Monétaire et Financier, les banques ont normalement l'obligation de rembourser les transactions qui sont contestées dans un délai de treize mois à compter de la date de débit, sauf à démontrer que le client concerné a commis une «négligence grave» dans la préservation de la sécurité de ses données.
S'agissant plus particulièrement du cas où les informations ayant permis au fraudeur d'effectuer les transactions ont été obtenues suite à un phishing, il résulte de la position de la Cour de Cassation notamment dans un arrêt de la chambre commerciale du 25 octobre 2017 (Cass.Com 25 octobre 2017 - 16-11.644) que la «négligence grave» ne peut pas être retenue si, compte tenu des circonstances, l'intéressé ne pouvait pas avoir conscience du caractère frauduleux du courriel de phishing réceptionné.
Dans l'hypothèse où votre réclamation reste infructueuse, il est possible de saisir le Médiateur de la banque.

Utiliser les plateformes de signalement :

Les tentatives d'escroquerie par phishing peuvent être signalées sur la plateforme Pharos (www.internet-signalement.gouv.fr), portail officiel de signalement des contenus illicites de l'Internet.
Il est possible aussi de s'inscrire gratuitement sur le site www.signal-spam.fr et de télécharger une extension pour le logiciel de messagerie ou le navigateur.
En cas de réception de SMS ou MMS non sollicités, vous pouvez les signaler en envoyant un SMS au 33700 (au prix d'un SMS normal) ou sur le site www.33700.fr

Pour en savoir plus :

- Site d'information sur la cybermalveillance
- https://www.cybermalveillance.gouv.fr (vidéos pédagogiques).
- https://www.signal-spam.fr/
- PHAROS https://internet-signalement.gouv.fr/
- Site https://17cyber.gouv.fr/ , un service proposé par la Police Nationale, la Gendarmerie Nationale et Cybermalveillance.gouv.fr.
- Site de la CNIL (Commission Nationale de l'Informatique et des Libertés) https://www.cnil.fr/fr/spam-phishing-arnaques-signaler-pour-agir
- Site de la DGCCRF : Fiche pratique : Comment assurer votre sécurité numérique ? https://www.economie.gouv.fr/particuliers/numerique-et-cybersecurite/comment-assurer-votre-securite-numerique