Escroqueries et arnaques les plus courantes

vendredi 12 avril 2024

Menu

1)Le phishing

Qu'est-ce que c'est ?

Le phishing (« hameçonnage ») consiste pour des personnes malveillantes à envoyer des courriels frauduleux afin d'obtenir des données personnelles (le plus souvent des données bancaires) et soutirer de l'argent à leurs victimes.

L'escroc se fait passer pour une personne de confiance (un ami, un membre de la famille, etc.) ou un organisme que vous connaissez (les impôts, la Caf, votre opérateur téléphonique, etc.) et vous invite à confirmer vos coordonnées ou à les mettre à jour en

cliquant sur un lien aboutissant sur un site Internet. L'escroc se sert alors de ces données pour effectuer des prélèvements frauduleux sur votre compte bancaire.

Comment vous en prémunir ?

Quelques signes peuvent vous alerter. Nous vous conseillons de :

- vérifier l'adresse de l'expéditeur en passant votre pointeur de souris sur le nom de l'expéditeur du message pour voir son adresse e-mail complète ;
- idéalement, contacter vous-même, par un autre biais, l'organisme ou la personne censée vous avoir envoyé le courriel ;
- traquer les éventuelles fautes de grammaire et d'orthographe, voire de syntaxe ;
- vérifier que le site est sécurisé : un cadenas doit être présent dans la barre d'adresse et l'adresse du site doit commencer par HTTPS (et non HTTP) ;
- ne pas cliquer sur un lien qui ne semble pas cohérent avec l'objet du courriel ;
- ne pas vous fier aux logos officiels, faciles à reproduire ;
- ne pas valider d'opération dont vous n'êtes pas à l'origine.

Gardez en tête qu'aucun organisme officiel ne vous demandera de communiquer vos coordonnées bancaires en réponse à un courriel. Au moindre doute, ne répondez pas et ne transmettez aucune information personnelle.

Quel recours avez-vous ?

Tout d'abord, signalez sans tarder les opérations que vous n'avez pas autorisées à votre banque et, en cas de transmission des coordonnées de votre carte bancaire, faites également opposition à votre carte.

Ensuite, contestez l'opération et demandez le remboursement auprès de votre banque. En cas d'opération non autorisée, le principe est celui du droit au remboursement. En revanche, dans le cas d'agissements frauduleux ou de négligences graves de votre part, la banque n'est plus tenue de vous rembourser. Pourtant, même en pareil cas, elle doit prouver l'existence de ces manquements. En tout état de cause, elle ne peut pas se contenter d'évoquer l'hypothèse d'un phishing pour refuser le remboursement.

Cependant, si l'opération de paiement a été effectuée sans que la banque ait exigé une authentification forte (voir encadré), la banque doit vous rembourser (sauf à prouver une fraude de votre part).

Articles L.133-18, L.133-19 et L.133-44 du Code monétaire et financier, article 16 du règlement délégué (UE) n° 2018/389 du 27/11/2017

Qu’est-ce que l’authentification forte ?

L’authentification forte (ou double authentification) est un dispositif permettant de vérifier votre identité pour plus de sécurité. Il faut au moins 2 des 3 éléments suivants :

- un élément de connaissance (mot de passe, code secret ou question secrète) ;
- un élément de possession (téléphone mobile ou clé USB) ;
- un élément biométrique (empreinte digitale, forme de l’iris ou reconnaissance vocale).

Elle doit s’appliquer dès lors que le montant de l’opération dépasse 30 € et que le montant cumulé des précédentes opérations depuis la dernière authentification forte du client dépasse 100 €, ou que le nombre des précédentes opérations de paiement depuis la dernière authentification forte du client dépasse 5 opérations de paiement électronique à distance individuelles consécutives.

2)L’arnaque au faux conseiller bancaire

Qu’est-ce que c’est ?

Une personne vous contacte, le plus souvent par téléphone, en se faisant passer pour un conseiller ou un salarié de votre banque, et prétend que vous êtes actuellement victime de paiements frauduleux. L’interlocuteur vous met en confiance car il connaît de nombreuses informations (votre identité, votre numéro de compte et même le nom de votre conseiller bancaire), puis il vous indique qu’il est urgent d’agir afin de contester ces paiements.

L’escroc vous demande alors de lui communiquer vos identifiants et/ou coordonnées bancaires pour procéder au blocage de ces opérations, ainsi que le code reçu par SMS pour confirmer le blocage de ces opérations (ou de cliquer sur un lien reçu par courriel).

En réalité, ce sont ces dernières opérations qui permettent à l’escroc d’effectuer des opérations frauduleuses.

Comment vous en prémunir ?

Votre banque ne vous demandera jamais de communiquer ces informations par téléphone, ni de valider des opérations à distance.

Attention : les techniques de ces escrocs sont de plus en plus sophistiquées (par exemple : courriel imitant ceux de votre banque, lien vers une fausse interface ressemblant à votre compte en ligne, etc.). Dans certains cas, le numéro de téléphone affiché correspond même à celui de votre banque !

Dans tous les cas, nous vous invitons à raccrocher immédiatement et à ne transmettre aucune information ni cliquer sur un quelconque lien. Mieux vaut contacter votre conseiller bancaire par vos propres moyens.

Quel recours avez-vous ?

Tout d'abord, signalez sans tarder les opérations que vous n'avez pas autorisées à votre banque et, en cas de transmission des coordonnées de votre carte bancaire, faites opposition à votre carte.

Ensuite, contestez l'opération et demandez le remboursement auprès de votre banque. En cas d'opération non autorisée, le principe est celui du droit au remboursement. En revanche, dans le cas d'agissements frauduleux ou de négligences graves de votre part, la banque n'est plus tenue de vous rembourser. Toutefois, même en pareil cas, elle doit prouver l'existence de ces manquements.

Cependant, si l'opération de paiement a été effectuée sans que la banque ait exigé une authentification forte, la banque doit vous rembourser (sauf à prouver une fraude de votre part).*Articles L.133-18, L.133-19 et L.133-44 du Code monétaire et financier*

3)L'arnaque au faux support informatique ou technique

Qu'est-ce que c'est ?

L'arnaque au faux support consiste à vous faire croire que votre ordinateur a un problème grave (par exemple : la présence d'un virus, une erreur du système, un blocage de l'écran). Un message par SMS, courriel ou directement sur l'écran de l'ordinateur vous invite à contacter un numéro si vous ne souhaitez pas perdre vos données ou l'usage de votre ordinateur.

Une fois entré en communication, l'interlocuteur fait semblant de dépanner votre ordinateur en prenant la main à distance puis vous facture la soi-disant prestation et/ou vous incite à acheter des logiciels inutiles.

Il arrive même qu'en cas de refus de paiement, la personne menace de supprimer ou divulguer vos données personnelles pour vous convaincre.

Comment vous en prémunir ?

Tout d'abord, pour essayer de limiter au maximum ce type de fraude, nous vous conseillons de :

- faire les mises à jour régulières de sécurité de votre système d'exploitation (Windows, IOS, Linux…) et logiciels installés, dont votre navigateur Internet ;
- tenir à jour votre antivirus et activer le pare-feu ;
- faire des sauvegardes régulières de vos données ;
- éviter les sites Internet peu fiables ou illicites ;
- ne pas cliquer sur des liens ou pièces jointes de courriels douteux ou d'expéditeur inconnu.

Si malgré tout, vous êtes victime d'une telle tentative de fraude, nous vous conseillons de :

- ne pas appeler le numéro indiqué et ne rien payer ;
- conserver des preuves (impression écran ou photographie de l'écran) ;
- procéder au redémarrage forcé de votre ordinateur ;
- nettoyer votre navigateur Internet, supprimer les cookies et réinitialiser les paramètres par défaut ;
- réaliser une analyse complète de votre ordinateur à l'aide d'un antivirus ;
- désinstaller toute application suspecte identifiée sur votre ordinateur ;
- si besoin, vous rapprocher de votre informaticien habituel ou d'un prestataire référencé sur la plateforme d'aide aux victimes de cyberattaque.

Quel recours avez-vous ?

Tout d'abord, conservez des preuves de cette arnaque (impression écran ou photo de l'écran, documents éventuellement transmis, etc.).

Ensuite, vous pouvez faire opposition à votre carte bancaire pour éviter d'autres paiements. S'agissant d'obtenir le remboursement de la somme débitée, la banque devra vous rembourser uniquement si le montant débité est supérieur au montant que l'on vous a annoncé. Pensez à conserver des preuves si le montant vous a été communiqué par écrit (courriel, facture, photo de l'écran, etc.).

Vous pouvez tenter, en parallèle, d'obtenir le remboursement auprès du faux support informatique en précisant que vous déposez plainte.

Vérifiez par ailleurs si vous êtes couvert pour ce type de cas par l'assurance de votre carte bancaire.

Enfin, vous pouvez chercher à obtenir le remboursement, par l'intermédiaire de votre banque, auprès de la société qui a édité votre carte bancaire (Visa, Mastercard, etc.) dans le cadre de la procédure de *chargeback* (dite aussi de « rétrofacturation »).

Chargeback • Obtenir le remboursement d'un achat par carte bancaire

Article 1302 du Code civil, article L.133-25 du Code monétaire et financier

4)L'arnaque au virement

Qu'est-ce que c'est ?

Vous vous apercevez, en vous connectant à votre espace client ou en consultant vos relevés bancaires, qu'un virement a été effectué au profit d'un bénéficiaire qui vous est inconnu.

Un escroc a réussi à pirater et accéder à votre espace client afin de procéder à ce virement frauduleux.

À aucun moment vous n'avez été à l'initiative de l'ajout d'un bénéficiaire, ni d'un virement à la suite d'un faux SMS, courriel ou appel téléphonique.

Comment vous en prémunir ?

Les procédés employés dans ce type d'arnaque sont parfois mystérieux. Quoi qu'il en soit, l'escroc a réussi d'une manière ou d'une autre à obtenir vos identifiants bancaires. Pour limiter le risque de fraude, nous vous conseillons de :

- changer vos mots de passe régulièrement ;
- toujours vous connecter à votre espace en ligne directement sur le site officiel ou *via* votre application mobile, et ne jamais y accéder en cliquant sur un lien reçu par SMS ou courriel ;
- ne pas transmettre vos coordonnées, même à votre entourage, par SMS ou courriel ;
- utiliser un antivirus ;
- effectuer les mises à jour de sécurité de vos appareils (ordinateur, téléphone

portable, tablette) dès qu'elles vous sont proposées.

Quel recours avez-vous ?

Dans ce cas précis, il s'agit d'une opération frauduleuse car vous n'êtes pas à l'origine de l'opération et n'y avez pas consenti.

Contestez l'opération et demandez le remboursement auprès de votre banque. En cas d'opération non autorisée, le principe est celui du droit au remboursement. En revanche, dans le cas d'agissements frauduleux ou de négligences graves de votre part, la banque n'est plus tenue de vous rembourser.

Articles L.133-18, L.133-19 et L.133-23 du Code monétaire et financier

5)L'arnaque au faux RIB (relevé d'identité bancaire)

Qu'est-ce que c'est ?

Vous êtes en relation avec une entreprise ou une personne à qui vous devez de l'argent. Celle-ci vous adresse un RIB par courriel et une facture en pièce jointe afin de procéder au règlement.

Ce courriel est intercepté par un escroc, en piratant soit votre boîte e-mail, soit celle de votre créancier, pour remplacer le RIB de votre créancier par le sien. Vous recevez le courriel modifié dans lequel seuls ont été modifiés le RIB et l'adresse courriel de l'expéditeur et procédez ensuite au virement avec le RIB reçu.

Les fonds sont en réalité transférés directement à l'escroc et non à votre créancier.

Comment vous en prémunir ?

Avant de procéder au paiement, nous vous conseillons :

- d'essayer d'obtenir au préalable les coordonnées bancaires par remise physique par le professionnel directement ;
- de vérifier que l'adresse courriel de l'expéditeur (en passant le pointeur de votre souris sur le nom de l'expéditeur) est identique à celle utilisée lors de précédents échanges, ou d'obtenir confirmation de celle-ci par le professionnel ;
- de vérifier les coordonnées du RIB. Pour une banque française, l'IBAN commence automatiquement par FR.

Au moindre doute, n'hésitez pas à contacter directement le professionnel pour confirmer les coordonnées bancaires avec lui.

Quel recours avez-vous ?

Les chances d'obtenir un remboursement de la part de votre banque sont faibles. En effet, vous êtes à l'initiative de ce virement et dans ce cas, sauf exception (virement différé ou permanent), le virement est par principe « irrévocable ». Il ne peut pas être annulé dès lors que l'ordre de virement a été reçu par votre banque.

De plus, la réglementation prévoit que si les coordonnées fournies par l'émetteur du virement sont inexactes ou liées à une erreur, ni la banque émettrice du virement ni la banque réceptrice ne sont responsables.

Par conséquent, elles n'ont pas à vérifier l'adéquation entre le nom mentionné sur le RIB et le détenteur du compte (Cour de cassation, chambre commerciale 24/01/2018 n° 16-22336). N'hésitez pas à signaler ce(s) virement(s) frauduleux car dès lors qu'elle en est informée, votre banque doit tenter de récupérer les fonds. Pour ce faire, elle demande à la banque du bénéficiaire toutes les informations utiles en sa possession. Si elle ne parvient pas à recouvrer les sommes, la banque doit vous transmettre les informations obtenues, mais uniquement à votre demande. Ces éléments pourront vous servir si vous envisagez un recours en justice contre l'escroc.

En parallèle des démarches effectuées auprès de votre banque, vous pouvez déposer plainte auprès du commissariat de police ou de la gendarmerie proche de chez vous.

Article L.133-21 du Code monétaire et financier

6)La fraude au faux coursier

C'est en quelque sorte une variante de la fraude aux faux conseiller bancaire. En général, un **phishing** préalable aura permis à l'escroc de récupérer de nombreuses informations sur vous, votre compte… en se faisant passer par exemple pour la sécurité sociale, Colissimo, etc.

En apparence, votre **conseiller** vous appelle par téléphone. Le numéro affiché semble bien être le sien. Vous pouvez aussi recevoir un SMS en ce sens. Il vous alerte sur le fait que votre **carte** bancaire semble **compromise** par une fraude. Il vous informe donc

qu’un **coursier** viendra chez vous récupérer votre carte, bien souvent le soir. Pour gagner votre confiance, il vous communique un code que le coursier devra vous indiquer, vous assure qu’une nouvelle carte vous sera envoyée sous peu ou même vous conseille d’augmenter le plafond de paiement et de retrait de votre carte bancaire…

L’appel ou le SMS usurpe évidemment l’identité de la banque. En réalité, il s’agira donc d’un **faux coursier** qui viendra à votre domicile pour récupérer la carte bancaire soi-disant compromise. L’escroc tentera ainsi de récupérer la carte et bien sûr votre **code confidentiel**, voire les codes de sécurité ou de validation des opérations à distance. Ce coursier vous fera croire qu’il détruit la carte devant vous et il vous demandera de lui communiquer vos codes.

Ne confiez jamais à personne votre carte et votre code confidentiel ou encore les codes d’activation ou de sécurité que vous recevez. **Jamais la banque ne vous les demandera.**

7)La fraude aux livrets et placements

L’escroc se fait passer pour un établissement de crédit, une banque ou encore un courtier. Il vous propose un **livret** ou un **placement** à des conditions très attrayantes. La **fraude** repose (encore une fois) sur l’**usurpation d’identité**.

Vous pouvez ainsi être contacté par **mail** ou **téléphone**, cliquer sur une **publicité** en ligne et de plus en plus sur les **réseaux sociaux**, via le compte d’influenceurs. Le livret ou placement est proposé avec une très forte **rentabilité**, un taux d’intérêt très élevé et des **revenus garantis**.

Si vous tombez dans le piège, vous recevrez des documents et/ou serez redirigé vers un site Internet pour renseigner vos **informations personnelles et bancaires**. Très bien faits, ces sites inspirent confiance car ils utilisent des mentions légales, des noms et des logos de banques ou établissements financiers connus, etc.

Pour un faux livret, vous n’avez qu’à verser les premiers dépôts pour percevoir au plus vite les intérêts promis. La fraude fonctionne de la même façon pour les placements financiers : diamants, champagne, vin, crypto-actifs, etc.

8)La fraude au faux prêt

Dans ce type de fraude, vous recevez un message vous proposant le **rachat de vos crédits** à un **taux imbattable**. Les escrocs se font passer pour une banque ou une société financière.

L'objectif pour les fraudeurs est de récupérer vos données pour **usurper votre identité** afin de se faire octroyer un crédit en ligne à votre place.

Pour ce faire, les escrocs prétextent les démarches pour constituer votre dossier de **rachat de crédit.** La somme empruntée est bien versée sur votre compte mais vous êtes contacté ensuite pour transférer le montant vers un **compte externe**, soi-disant pour finaliser l'opération de rachat de crédit.

Avant toute démarche, contactez directement votre conseiller bancaire et/ou l'établissement de crédit concerné en trouvant vous-même les coordonnées, pour vérifier la démarche. Méfiez-vous de taux qui ne rentrent pas dans la fourchette des **taux actuellement pratiqués**.