Fraude bancaire

Le top 5 des arnaques les plus fréquentes

Pour plus de détails, contactez votre association locale

Arnaque n°1 : LE PHISHING

Qu'est-ce que c'est ?

© ©momius - stock.adobe.com

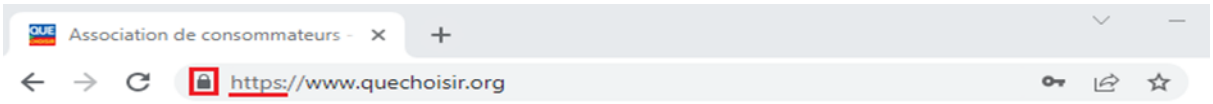
Le phishing (« hameçonnage ») consiste pour des personnes malveillantes à envoyer des courriels frauduleux afin d'obtenir des données personnelles (le plus souvent des données bancaires) et soutirer de l'argent à leurs victimes.

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 ?

©BillionPhotos.com - stock.adobe.com

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, 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

Arnaque n° 2 : L'ARNAQUE AU FAUX CONSEILLER BANCAIRE

Qu'est-ce que c'est ?

© osamuraisan - stock.adobe.com

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 ?


©BillionPhotos.com - stock.adobe.com

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).

Lire aussi

- Arnaque - Des banquiers très bien imités

Articles L.133-18, L.133-19 et L.133-44 du Code monétaire et financier

Pour plus de détails, contactez votre association locale

Arnaque n°3 : L'ARNAQUE AU FAUX SUPPORT INFORMATIQUE OU TECHNIQUE

Qu'est-ce que c'est ?

© RÉGIS FALLER

L'arnaque 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 ?

©BillionPhotos.com - stock.adobe.com

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 »). Retrouvez les conditions et modalités dans notre article « Chargeback – Obtenir le remboursement d'un achat par carte bancaire ».

Lire aussi

- Arnaque au faux support technique - Ne payez pas !

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

Arnaque n°4 : L'ARNAQUE AU VIREMENT

Qu'est-ce que c'est ?

© REA

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 ?


©BillionPhotos.com - stock.adobe.com

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

Pour plus de détails, contactez votre association locale

Arnaque n° 5 : L'ARNAQUE AU FAUX RIB

Qu'est-ce que c'est ?

© Adobe stock

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 avec lui les coordonnées bancaires.

Quel recours avez-vous ?


©BillionPhotos.com - stock.adobe.com

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.

Lire aussi

- Arnaque en ligne - Le faux RIB fait irruption dans les boîtes mail

Article L.133-21 du Code monétaire et financier

Le saviez-vous ?

Qu'est-ce que l'authentification forte ?

© tippapatt - stock.adobe.com

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.

Vous pouvez consulter notre article « Paiements en ligne – La double authentification s'impose ».

Refus de remboursement des fraudes bancaires – L'UFC-Que Choisir se mobilise

L'UFC-Que Choisir, face aux nombreux refus de remboursement injustifiés des banques, a déposé plainte contre 12 établissements pour pratiques commerciales trompeuses le 28 juin 2022. L'UFC-Que Choisir, à travers la multitude de refus injustifiés, a mis au jour une véritable stratégie des banques pour s'affranchir de leur obligation de démontrer la négligence personnelle de leurs clients afin de refuser de les rembourser (voir notre article « Refus de remboursement des fraudes bancaires – L'UFC-Que Choisir dépose plainte contre 12 banques »).

L'UFC-Que Choisir recense encore les signalements des fraudes non indemnisées par un formulaire dédié.

Vous trouverez également à votre disposition deux lettres types et outils fournissant des conseils personnalisés :

Fraude à la carte bancaire – Contestation de l'utilisation d'un code 3D Secure

Fraude à la carte bancaire – Demande de remboursement

Outil Fraude à la carte bancaire – Vos droits et les conseils de l'UFC-Que Choisir

© fizkes - stock.adobe.com

Le saviez-vous ?

Des pénalités désormais prévues en cas de retard de remboursement des opérations non autorisées


© Adobe Stock

Par principe, dès lors qu'une opération non autorisée est signalée à la banque, cette dernière est tenue de procéder immédiatement au remboursement de ladite opération et au plus tard à la fin du premier jour ouvrable suivant. Cette règle comporte une exception, si la banque a de bonnes raisons de soupçonner une fraude de l'utilisateur du service de paiement et si elle communique ces raisons, par écrit, à la Banque de France.

Depuis le 19 août 2022, des pénalités sont désormais prévues en cas de retard dans le remboursement :

« 1° Les sommes dues produisent intérêt au taux légal majoré de 5 points ;
« 2° Au-delà de 7 jours de retard, les sommes dues produisent intérêt au taux légal majoré de 10 points ;
« 3° Au-delà de 30 jours de retard, les sommes dues produisent intérêt au taux légal majoré de 15 points. »

Article L.133-18 du Code monétaire et financier modifié par l'article 22 de la loi n° 2022-1158 du 16 août 2022

Et si votre banque vous demande de déposer plainte ?

L'UFC-Que choisir constate que les banques conditionnent souvent le remboursement à un dépôt de plainte préalable. Or les services de police et de gendarmerie sont débordés par ces dépôts de plainte et refusent parfois de prendre la plainte des victimes de fraudes bancaires. En tout état de cause, la banque ne peut exiger un dépôt de plainte pour traiter votre demande de remboursement. Cette formalité n'est pas imposée par la réglementation.

Si vous souhaitez déposer plainte, vous pouvez le faire par écrit en portant plainte contre X. En revanche, faute de certitude sur les moyens employés par les fraudeurs, évitez d'évoquer des hypothèses. Restez factuel en indiquant uniquement le(s) débit(s) frauduleux constatés. En effet, la banque peut chercher des éléments dans votre déclaration pour considérer que vous avez été négligent dans la conservation de vos données bancaires et refuser de vous rembourser. Néanmoins, la négligence grave ne se présume pas. Elle devra être prouvée par la banque.

LES PLATEFORMES PERCEVAL ET THÉSÉE

Vous pouvez signaler les fraudes à la carte bancaire directement en ligne avec le téléservice Perceval (via le site Service-public.fr). Le signalement n'est pas un dépôt de plainte, mais il permet de centraliser les déclarations de fraude bancaire pour aider les services de police. De plus, un récépissé est délivré. Vous pourrez le présenter à votre banque à l'appui de votre demande de remboursement.

En parallèle existe également, depuis le 15 mars 2022, la plateforme Thésée, également accessible depuis le site Service-public.fr. Par ce biais, il est possible de déposer plainte en ligne pour les escroqueries. Attention, le phishing (« hameçonnage ») n'est pas inclus dans ce service de plainte en ligne.

Un litige ?

L'UFC-Que Choisir est à vos côtés pour vous renseigner et vous orienter dans vos démarches.

L'UFC-Que Choisir, à vos côtés !

L'UFC-Que Choisir est aux côtés des consommateurs pour les aider à résoudre leurs litiges avec les professionnels. Nos adhérents peuvent bénéficier d'un accompagnement personnalisé dans le but d'obtenir une résolution amiable de ce différend.

Si vous souhaitez obtenir une assistance ou une intervention de notre part, cela nécessite de s'acquitter au préalable d'une cotisation annuelle auprès de l'UFC-Que Choisir. En effet, en tant qu'association de défense des consommateurs, nous ne pouvons délivrer de consultations juridiques qu'à nos membres.

Devenir adhérent de l'UFC-Que Choisir, c'est rejoindre un Mouvement et bénéficier de tous les avantages liés à l'adhésion :

- Un appui et une promotion de vos actions individuelles
- Une information sur vos droits
- Une participation à la défense des consommateurs

Ce que nous ne pouvons pas faire

- Missionner un expert, un auxiliaire de justice comme un avocat ou un huissier.
- Vous assister ou vous représenter devant une juridiction ou tout organe ayant compétence pour trancher votre litige.
- Intervenir dans des matières ne relevant pas de notre objet statutaire comme le droit de la famille, le droit du travail, le droit fiscal.

Contactez-nous !

Votre Association locale

UFC-Que Choisir

Pour que notre association puisse vous accompagner dans le traitement de votre litige, il est nécessaire (loi n°71-1130 du 31 décembre 1971) que vous en deveniez adhérent. L'adhésion est distincte de l'abonnement à nos publications : elle permet aux associations UFC-Que Choisir de défendre l'intérêt individuel et collectif des consommateurs.