



VOTRE SÉCURITÉ

Votre rôle dans la sécurité
de vos données et de vos transactions

CCF

Objectif sécurité

Nous avons tous un rôle à jouer

Notre époque hyper connectée favorise l'accroissement de la fraude et de la criminalité financière. Comme l'ensemble du secteur financier, votre patrimoine est exposé à ces risques et vos besoins de protection sont plus nécessaires que jamais. Conscient que chacun recherche aujourd'hui une banque responsable, le CCF s'engage à mettre en oeuvre les mesures les plus exigeantes pour prévenir toute tentative d'intrusion criminelle dans ses systèmes et pour assurer la sécurité de vos transactions.

Rien n'est possible sans vous

La sécurité est l'affaire de tous, votre participation est donc essentielle pour prévenir les risques qui peuvent menacer vos différentes opérations bancaires. Nous vous présentons ici quelques réflexes simples à adopter pour qu'ensemble, nous puissions garantir la sérénité de votre quotidien bancaire.

Contactez-nous sans délai si vous suspectez une fraude

Besoin d'informations plus détaillées, rendez-vous sur :

<https://ccf.fr/particuliers/au-quotidien/conseils/prevention-fraude.html>



Soyez vigilants

La cybercriminalité est une menace omniprésente dans notre société numérique interconnectée. Derrière chaque clic se cache un danger potentiel : transaction en ligne, donnée personnelle partagée sur le web... Exploitant les failles de sécurité, les cybercriminels ne reculent devant rien pour atteindre leurs objectifs et multiplient les pratiques frauduleuses.

Le phishing

En vous adressant un contenu ou un lien par email dont vous pensez avoir besoin, les cybercriminels vous dirigent souvent vers un site frauduleux par lequel ils obtiennent certaines de vos informations personnelles telles que des identifiants, des mots de passe ou des codes. Cette pratique existe aussi via les SMS (Smishing) et le téléphone (Vishing).

Le malware

Par le biais d'un lien contenu dans un email ou en visitant un site Web infecté, un logiciel malveillant s'installe sur votre ordinateur à votre insu dans le but de récupérer certaines de vos données personnelles telles que vos identifiants, mots de passe ou codes.

Le pharming

En utilisant un code malveillant qui s'installe sur l'un de vos appareils, les cybercriminels vous redirigent sur leur site Web sans que vous n'ayez à cliquer sur un lien. L'objectif est de récupérer certaines de vos données personnelles.

Le ransomware

Appartenant à la catégorie des malwares, le ransomware infecte vos appareils (smartphone, tablette, ordinateur) en installant un logiciel malveillant qui chiffre et bloque l'ensemble de vos fichiers. En échange de la clé de déchiffrement le cybercriminel demande le paiement d'une rançon très souvent en crypto-monnaie.

Le spoofing

En usurpant l'identité d'une entreprise, d'une banque ou d'un organisme gouvernemental (adresse email ou numéro de téléphone qui semblent fiables), le criminel vous met en confiance et tente par téléphone, email ou SMS de vous soustraire des informations personnelles telles que vos

Nos conseils

- **Tenez-vous régulièrement informés** : des plateformes gouvernementales dédiées à la lutte contre la cybercriminalité, telles que l'ANSSI⁽¹⁾ ou cybermalveillance.gouv.fr partagent des informations essentielles.
- **Protégez votre équipement** : appliquez immédiatement les mises à jour de sécurité sur vos appareils, utilisez un antivirus, ne téléchargez vos applications que depuis les sites officiels et sauvegardez régulièrement vos données numériques.
- **Lors de chaque connexion sur votre Espace Client CCF** : vérifiez que l'URL de connexion soit en mode sécurisé « https:// », saisissez vos codes ou identifiants et informations confidentielles à l'abri des regards indiscrets, vérifiez régulièrement les opérations qui se présentent sur vos comptes et déconnectez-vous systématiquement à la fin de vos opérations.
- **Soyez vigilants à la réception d'emails ou de SMS** : ne répondez jamais à un email sollicitant la communication d'informations personnelles, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens contenus dans les emails ou SMS dont vous ne connaissez pas l'expéditeur.
- **Maîtrisez votre présence sur les réseaux sociaux** : protégez vos comptes avec des mots de passe solides, vérifiez bien vos paramètres de confidentialité et faites attention aux personnes avec qui vous communiquez.

(1) Agence nationale de la sécurité des systèmes d'information



CE QU'IL FAUT SAVOIR

Le CCF ne vous demandera jamais de communiquer vos codes ou identifiants. Refusez toujours de fournir ce type d'informations, à qui que ce soit. Vous pouvez déposer plainte en cas d'incident auprès des services de Police ou de Gendarmerie compétents et en ligne sur moncommissariat.fr. Si vous êtes victimes d'escroqueries sur internet : faux sites de vente, piratage de comptes de messagerie, extorsion d'argent pour débloquent un ordinateur... un service gratuit est mis en place pour vous accompagner : 17Cyber - Mon assistance en ligne | Site Officiel

Méfiez-vous des faux services

Méfiez-vous des offres trop alléchantes proposées sur Internet ou par téléphone, pour lesquelles on vous promet de l'argent facile et sans risques, elles s'avèrent souvent irréalistes et cachent une arnaque.

La fraude au faux conseiller bancaire ou au faux service anti-fraude

Elle consiste à vous **tromper pour vous faire valider des opérations frauduleuses sur vos comptes**. L'escroc vous appelle et **se présente comme un conseiller ou un agent du service anti-fraude de votre banque**. Il dispose souvent de nombreuses informations vous concernant pour crédibiliser son arnaque : identité, adresse...

Le fraudeur vous contacte en se faisant passer pour un employé de votre banque, souvent à partir d'un **numéro de téléphone usurpé identique à celui de votre établissement bancaire**. Placé en situation d'urgence par le fraudeur qui prétend constater plusieurs opérations frauduleuses en cours sur votre compte bancaire, vous êtes incité à procéder à diverses manipulations, pensant mettre votre trésorerie à l'abri, mais permettant en réalité au fraudeur de vider votre compte bancaire, souvent via votre application bancaire sécurisée.

La fraude au faux coursier

Dans certains cas, le faux conseiller vous indique qu'il y a **une fraude en cours sur votre carte bancaire, et envoie un coursier pour récupérer la carte à votre domicile**, au prétexte de la détruire et de vous en fournir une nouvelle. Les escrocs utiliseront alors la carte pour des retraits et/ou des achats en magasin.

La fraude au crédit immobilier

A la suite d'une simulation effectuée sur une plateforme de comparateurs de crédit, vous êtes recontactés par e-mail et/ou téléphone, par un interlocuteur se faisant passer pour un collaborateur du CCF, dans le but :

- de vous mettre en confiance en vous proposant un taux très attractif pour un nouveau crédit ou un rachat,
- de récupérer et exploiter vos informations personnelles (copie de carte d'identité nationale ou passeport, bulletins de paie, avis d'imposition, justificatif de domicile...),
- d'obtenir de votre part un virement correspondant aux frais de dossier.

Les faux placements

Ces placements, qui font de nombreuses victimes, promettent la plupart du temps des gains importants et concernent fréquemment :

- un placement sur de faux livrets d'épargne « boostés » ou dans de nouvelles cryptomonnaies,
- une souscription de parts de SCPI (Société Civile de Placement Immobilier),
- une diversification de votre patrimoine dans le vin ou autres spiritueux,
- l'acquisition d'or ou de diamants,
- un investissement pour soutenir l'agriculture locale.

Attention : en plus d'une perte financière, ce type de fraude peut vous impliquer dans un circuit frauduleux susceptible de vous exposer à d'éventuelles poursuites !

Nos conseils

- **Ne donnez pas suite aux promesses irréalistes** de gains importants ni aux comportements suspects.
- **Avant d'investir, consultez la liste noire** des sites d'investissement frauduleux et les conseils indiqués sur le site de l'AMF⁽²⁾.
- **Vérifiez la réelle existence de l'offre** proposée lorsque vous êtes contactés prétendument au nom d'un établissement financier connu, en vous rendant dans une agence ou en contactant un numéro de téléphone officiel (n'utilisez pas les coordonnées figurant sur l'offre frauduleuse).
- **Ne communiquez aucun document** ni aucune information confidentiels par email, téléphone ou courrier.

(2) <https://protectepargne.amf-france.org>



CE QU'IL FAUT SAVOIR

Les fraudeurs, prêts à tout, peuvent se faire passer pour un conseiller bancaire, un notaire, ou encore les services de police, restez toujours vigilants. Ils peuvent détenir des informations réelles sur vous, obtenues via les réseaux sociaux par exemple, ce qui aura tendance à vous mettre en confiance.

Sécurisez vos transactions

Carte bancaire, chèque, virement : ces divers moyens de paiement peuvent vous exposer à autant de tentatives d'escroquerie, aussi élaborées que discrètes. C'est donc aussi au quotidien que la vigilance s'impose.

La fraude à la carte bancaire

Bien que de nouvelles solutions technologiques vous soient régulièrement proposées pour vous apporter davantage de sécurité, les techniques de fraude évoluent en permanence et sont de plus en plus sophistiquées.

Cette fraude désigne l'utilisation frauduleuse des coordonnées de votre carte bancaire, alors même que celle-ci est toujours en votre possession. Pour obtenir les coordonnées de votre carte bancaire, le fraudeur peut utiliser de nombreuses méthodes : le phishing, le piratage d'un compte en ligne sur lequel les coordonnées de votre carte seraient enregistrées (commerce en ligne, réseaux sociaux...), les distributeurs automatiques de billets piégés.

Les demandes d'encaissement de chèques

Les fraudeurs peuvent vous contacter via les réseaux sociaux. Après avoir gagné votre confiance et prétextant l'impossibilité d'utiliser leurs comptes bancaires, ils vous demandent d'encaisser des chèques sur votre compte en échange d'une compensation financière. A la suite des remises de chèques, ils vous sollicitent pour transférer les fonds par virement à destination de différents bénéficiaires, malheureusement, les chèques vont revenir impayés et l'argent viré vers les bénéficiaires sera perdu.

L'escroquerie au virement ou faux RIB

Ce type d'escroquerie a pour objectif de vous tromper en usurpant l'identité de l'un de vos créanciers (opérateur de téléphonie mobile, fournisseur d'énergie, artisan, notaire, avocat, propriétaire/bailleur etc.). Vous livrant ses soit disant nouvelles coordonnées bancaires (RIB), il vous fait réaliser un virement vers un compte bancaire frauduleux.

Nos conseils

- **Ne donnez jamais votre code confidentiel de carte bancaire à qui que ce soit.** Il pourrait être utilisé pour des retraits ou des achats par des fraudeurs.
- En magasin, composez le code de votre carte bancaire à l'abri des regards indiscrets.
- Lors d'un retrait d'espèces, assurez-vous qu'aucun élément n'ait été ajouté au distributeur (qui pourrait conserver votre carte ou enregistrer votre code).
- Pour vos achats en ligne, n'enregistrez jamais vos données de carte bancaire, préférez les retaper pour chaque achat.
- Lors d'un achat en ligne, **vérifiez que le site est bien sécurisé : « https:// »** dans l'adresse ainsi que le cadenas à côté de la barre d'adresse.
- Rédigez vos chèques en ne laissant aucun espace avant la somme, rayez d'un trait l'espace libre après la somme ainsi qu'après le nom du bénéficiaire et enfin **ne signez jamais de chèques sans montant.**
- **Ne déposez pas de chèques pour le compte d'inconnus** et ne communiquez pas vos coordonnées bancaires ou vos identifiants de Banque à Distance pour leur permettre de le faire directement sur votre compte.



CE QU'IL FAUT SAVOIR

Ne confiez à personne le code de votre carte bancaire et mémorisez-le pour ne pas avoir à le noter. Si vous l'avez oublié, connectez-vous à votre Espace Client CCF, rubrique « Cartes » ou contactez votre conseiller CCF qui vous le fera parvenir de nouveau, par courrier sécurisé.

En savoir plus ?

Appelez ou prenez RDV avec votre conseiller CCF

Contactez le Centre de Relations Clients : **01 55 69 74 74**

Composez le **+33 1 55 69 74 74** depuis l'étranger (coût variable selon opérateurs)

Du lundi au vendredi de 8h à 20h et le samedi de 9h à 17h30.

Pour les jours fériés, les horaires d'ouverture sont de 9h à 17h30.

Sauf exception, les jours fériés qui tombent en semaine (lundi à vendredi) sont travaillés, mis à part le 1^{er} janvier, le Lundi de Pâques, le 1^{er} mai, le 8 mai et le 25 décembre.

Connectez-vous sur ccf.fr



@ccf_banque



CCF Banque



ccf.banque

CCF

S.A. au capital de 147 000 001 euros, agréée en qualité d'établissement de crédit et de prestataire de services d'investissement, immatriculée au RCS de Paris sous le numéro 315 769 257 - Siège social : 103 rue de Grenelle 75007 Paris. Intermédiaire en assurance immatriculé à l'ORIAS sous le numéro 07 030 182 (www.orias.fr).

Document non contractuel à caractère promotionnel

Publié par le CCF : 03.2026 - Réf. : 26.009

Crédit photo : VuThéara Kham

