NOVEMBRE 2012

HORS-SÉRIE

LES
MINI-GUIDES
BANCAIRES

Sécurité des opérations bancaires

www.lesclesdelabanque.com

Le site pédagogique sur la banque et l'argent

FEDERATION
BANCAIRE
FRANCAISE

FBF - 18 rue La Fayette - 75009 Paris
cles@fbf.fr

les clés
de la banque

Ce mini-guide vous est offert par :

Pour toute information complémentaire, nous contacter :
cles@fbf.fr - 01 48 00 50 05

Éditeur : FBF - 18 rue La Fayette 75009 Paris - Association Loi 1901
Directeur de publication : Ariane Obolensky
Imprimeur : Concept graphique, ZI Delaunay Belleville - 9 rue de la Poterie - 93207 Saint-Denis
Dépôt légal : novembre 2012

SOMMAIRE

INTRODUCTION

La protection des opérations bancaires nécessite un haut niveau de sécurité que ce soit en agence, par téléphone ou par internet.

Pour informer leurs clients sur les dispositifs en vigueur, les banques publient, sur leur site internet, une rubrique consacrée à la sécurité. Consultez-la régulièrement et appliquez les consignes.

En tant que client de la banque, vous avez un rôle actif dans l'utilisation de vos moyens de paiement et des services de banque à distance.

Ce guide présente les bonnes pratiques à respecter en matière de sécurité.

LES PRINCIPAUX RISQUES ET LEUR PRÉVENTION

ATTENTION

Chéquier, carte, code sont
PERSONNELS ET CONFIDENTIELS :
NE LES CONFIEZ À PERSONNE,
et NE COMMUNIQUEZ JAMAIS
LE CODE CONFIDENTIEL
de votre carte bancaire ou
vos identifiant et mot de passe
des services de banque à distance.
A défaut, vous permettriez
à quelqu'un de prendre tout l'argent
qu'il peut, sans votre accord.

Prévention des risques liés à la carte

LA PERTE, LE VOL OU LA FRAUDE

- **Retirez vous-même votre carte** à l'agence, **apprenez par cœur le code** confidentiel et détruisez le courrier qui le mentionnait,
- **notez le numéro de votre carte et sa date d'expiration** en cas de mise en opposition et **conservez ces informations et votre carte en lieu sûr**, après chaque utilisation,
- **ne communiquez votre code à personne** (même pas à votre famille) : personne n'en a besoin (ni la banque, ni l'assureur, ni la police, etc.),
- **votre carte est strictement personnelle**, ne la confiez à personne, **ne la perdez jamais de vue** lors d'un paiement chez un commerçant, il pourrait noter tous les éléments qui y figurent,
- **tapez votre code à l'abri des regards**, chez un commerçant ou au distributeur de billets, en cachant le clavier avec votre autre main,
- **si vous remarquez un élément suspect** sur un distributeur de billets ou un automate de paiement, notamment sur la partie d'insertion de la carte et/ou sur le clavier de saisie du code (par exemple surépaisseur), indiquez-le à la banque et surtout n'utilisez pas cet appareil,
- demandez à votre banque la solution la plus sécurisée pour vos achats en ligne.

conseil

Chez un commerçant ou au distributeur, cachez efficacement le clavier quand vous tapez votre code. Souvent, avant un vol de carte, le voleur observe sa victime en train de taper le code, libre de l'utiliser ensuite avec la carte volée.

ATTENTION

Au renouvellement de votre carte, pensez à détruire l'ancienne en coupant la puce et la piste magnétique en deux.

LE PAIEMENT SUR INTERNET OU PAR TÉLÉPHONE

- Avant de saisir les informations de votre carte, **vérifiez que le site est sécurisé** (https devant l'adresse du site, ou cadenas fermé, ou icône d'une clé dans le navigateur),
- **n'enregistrez pas les informations de votre carte** dans votre profil client du site commerçant, ressaisissez-les à chaque transaction,
- si votre banque vous le propose, **optez pour une e-carte bancaire**,
- en cas de doute, effectuez le paiement par un autre moyen,
- **passez par un commerçant connu et réputé** ; n'hésitez pas à vérifier ses coordonnées (nom, adresse, téléphone, service clients), ne donnez les caractéristiques de votre carte qu'à un commerçant dont vous êtes sûr,
- **n'adressez jamais le numéro de votre carte**, encore moins le code confidentiel, **par courrier électronique** ou par téléphone,
- **notez le montant** exact et la date de l'opération qui passera sur votre compte, **vérifiez le montant** qui vous sera **débité** pour réagir immédiatement auprès de votre banque en cas d'anomalie.

Sécurité des opérations à distance

PROTÉGEZ VOS CODES D'ACCÈS À LA BANQUE À DISTANCE

- **ne divulguez à personne vos identifiant et mot de passe** (ni à votre banque, ni à la police, etc.) car personne n'a besoin de les connaître, **conservez-les en sécurité** et hors de portée de quiconque,
- **ne gardez pas dans la mémoire de l'ordinateur vos codes d'accès** même s'il vous le propose,
- **utilisez le bouton de déconnexion** du site de la banque dès que vous avez terminé, si la date de votre dernière connexion est affichée, vérifiez-la,
- **n'utilisez jamais le lien figurant dans un courrier électronique pour vous connecter à votre site de banque à distance** quel qu'en soit l'objet, c'est à vous de saisir l'adresse du site internet de votre banque,
- assurez-vous que personne ne peut vous voir saisir vos codes d'accès et changez-en si vous pensez que quelqu'un a pu les découvrir,
- **si vous recevez un courrier électronique douteux et utilisant** les coordonnées ou **l'identité** (logo, visuel…) **de votre banque, prévenez-la au plus vite** en lui faisant suivre le message. En aucun cas vous ne devez y répondre ni fournir d'informations,
- faites aussi attention aux messages vous incitant à appeler votre banque : prenez le temps de vérifier le numéro de téléphone,
- **n'effectuez aucune opération de banque à distance** (connexion, virement, opposition…) **si vous pensez avoir un virus sur votre ordinateur** et contactez votre agence pour demander de nouveaux codes d'accès.

CONCERNANT PARTICULIÈREMENT VOTRE MOT DE PASSE

- Changez de mot de passe dès réception et **modifiez-le régulièrement**,
- évitez les mots de passe trop faciles à trouver (date de naissance, prénom de vos enfants…) et déjà utilisés (accès téléphone, alarme,…),
- **réservez un mot de passe à la seule banque à distance, ne l'utilisez pas pour d'autres applications ou sites internet** (messagerie, identification sur des sites internet non bancaires…)
- choisissez, si possible, un mot de passe alphanumérique (lettres et chiffres).

Prévention des risques liés au chèque

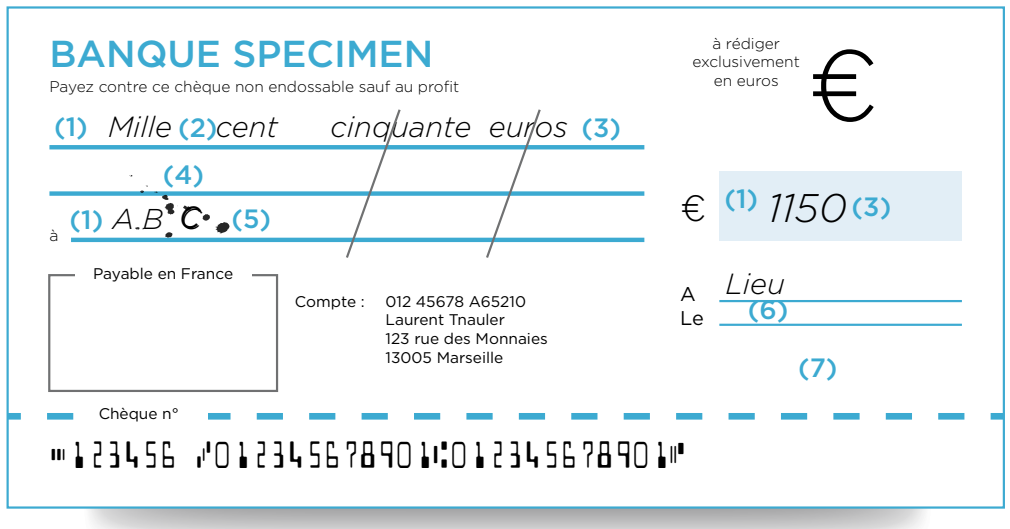
LA PERTE, LE VOL OU LA FALSIFICATION

- **Retirez vous-même votre chéquier** à l'agence. Pour le recevoir par voie postale, privilégiez un envoi sécurisé et n'hésitez pas à contacter votre agence en cas de retard,
- **notez à part les numéros** des chèques et le numéro à appeler pour faciliter une opposition rapide en cas de perte ou de vol.
- **limitez le nombre de chéquiers** en votre possession, **conservez-les en lieu sûr** et ne les laissez **jamais sans surveillance** (par exemple dans un véhicule même fermé à clé),
- **restituez à la banque les formules** de chèques inutilisées en cas de clôture du compte ou sur simple demande de sa part,
- **écrivez au stylo bille noir**, sans rature ni surcharge et **complétez-le début et la fin de chaque ligne** d'un trait horizontal, pour que rien ne puisse être ajouté avant ou après,
- **ne signez jamais** de chèque **sans** y indiquer le **montant** et le **bénéficiaire**,
- si vous ne remplissez pas vous-même le nom du bénéficiaire, vérifiez qu'il le complète devant vous,
- ne mettez pas de sigle comme nom de bénéficiaire (exemple : «A.B.C») et préférez un nom complet,
- si le chèque est rempli par une machine, vérifiez la lisibilité et l'exactitude des mentions portées (surtout le montant) par la machine avant de le signer,
- n'oubliez pas de **remplir la date et le lieu d'émission** (mentions obligatoires) **et** de **signer votre chèque**,
- **si vous recevez un chèque, vérifiez** que **toutes les mentions obligatoires** y figurent, attention aux éventuelles altérations,
- vérifiez **l'identité de la personne** vous donnant un chèque,
- en cas d'absence de bénéficiaire, **complétez-le avec votre nom et signez au dos immédiatement**.

i

- *Inutile de mettre une date postérieure à la date du jour, le chèque peut être encaissé immédiatement.*
- *Un chèque n'est pas un moyen de paiement garanti. Même si le montant du chèque a été crédité sur votre compte, il peut être ultérieurement rejeté, par exemple pour absence de provision.*

LES BONS RÉFLEXES POUR REMPLIR UN CHÈQUE



(1) Commencer en début de ligne

(2) Éviter les espaces trop grands

(3) Tirer un trait derrière

(4) Pas de rature ni surcharge

(5) Indiquer toujours un bénéficiaire nominatif (éviter les initiales)

(6) Toujours dater

(7) Toujours signer

LE FAUX CHÈQUE

- **Soyez vigilant**, ne concluez jamais de transaction dans la précipitation, **attention aux pièges.**
- **Méfiez-vous d'une offre de prix supérieur** au montant demandé et n'acceptez que des montants correspondant au montant de la transaction (voir annexes - piège 1).
- Assurez-vous que le paiement est réalisé selon les modalités convenues avec l'acheteur (voir annexes - piège 2).
- N'acceptez pas de déposer sur votre compte un chèque pour un autre bénéficiaire.

LE FAUX CHÈQUE DE BANQUE

- **Assurez-vous de la validité du chèque** en vous rendant à la banque avec l'acheteur pour vous faire remettre le chèque.
- En cas d'impossibilité, **appelez la banque** pour confirmation **au numéro que vous aurez trouvé vous-même. N'appelez pas le numéro figurant sur le chèque** car en cas de faux chèque, c'est celui d'un complice.
- **Choisissez bien le jour de la vente** (évitez les jours fériés ou le dimanche) pour pouvoir joindre l'établissement bancaire ; en cas de doute, ne vous dessaisissez pas de votre bien.
- **Soyez attentif aux altérations** (couleurs, taches, traces de grattage ou de lavage, écritures différentes) et **vérifiez la présence du filigrane** de sécurité (voir annexes - piège 3).

BIEN RÉAGIR EN CAS D'INCIDENT

ATTENTION

Pour détecter un incident, vous devez vérifier le contenu de votre relevé de compte dès sa réception ou vous connecter au moins chaque mois sur le site de banque à distance.

Examinez toutes les opérations passées sur votre compte, notamment avec les talons des chèques émis et les facturettes de carte :

- **en cas de doute sur une opération, demandez**, sans attendre, **des précisions à votre agence** bancaire,
- **si une opération ne vous concerne pas, prévenez immédiatement votre agence** par téléphone ou courrier électronique et confirmez par lettre. Selon la nature de l'opération anormale relevée, votre agence pourra faire des recherches.

En cas d'incident lié à la carte

LA PERTE OU LE VOL DE SA CARTE

- A l'étranger, appelez le numéro communiqué au préalable par votre banque ou celui figurant sur les distributeurs de billets.
- La banque conseille de porter plainte systèmatiquement auprès de la police.

à savoir

DÈS QUE VOUS VOUS APERCEVEZ QUE VOUS N'AVEZ PLUS VOTRE CARTE (PERDUE OU VOLÉE) FAITES IMMÉDIATEMENT OPPOSITION EN APPELANT LE NUMÉRO FOURNI PAR VOTRE BANQUE. A DÉFAUT AU 0.892.705.705 (0,34 € PAR MN). CONFIRMEZ AU PLUS TÔT PAR ÉCRIT À VOTRE AGENCE.

LA PERTE OU LE VOL DE SON CODE CONFIDENTIEL SANS LA CARTE

Votre code confidentiel, noté par exemple sur un papier ou dans votre téléphone, a été perdu ou volé ? Sachez qu'avec seulement le code confidentiel, personne ne peut effectuer de paiement sans le numéro de la carte. Par précaution, **demandez** néanmoins à votre agence **une nouvelle carte et un nouveau code** confidentiel.

Vous avez simplement oublié votre code ? **Contactez votre agence**, il vous parviendra sous pli confidentiel (seul le centre de gestion des cartes en a connaissance).

LA CARTE CAPTURÉE DANS UN DISTRIBUTEUR DE BILLETS

Vous avez voulu retirer de l'argent dans un distributeur et la carte n'en est pas ressortie ?

- **si** le distributeur de billets dépend d'une **agence bancaire ouverte** à ce moment-là :
  - **renseignez-vous sur place** auprès du personnel,
  - si vous avez fait une mauvaise manipulation, il est parfois possible de **récupérer la carte** immédiatement sans avoir à faire opposition,
- **dans tous les autres cas**, si le distributeur ne dépend pas d'une agence bancaire ou si celle-ci est fermée, **faites immédiatement opposition** auprès du numéro fourni par votre banque ou **au 0 892 705 705** (0,34€ par mn). Depuis l'étranger, appelez le numéro figurant sur les distributeurs de billets.

UN DÉBIT CARTE ERRONÉ

Vous venez de pointer votre relevé de compte et un montant ne correspond pas à un de vos achats ou retraits ?

Le pointage de votre relevé de compte avec vos facturettes carte permet de vérifier que les opérations par carte débitées de votre compte sont bien celles que vous avez payées et pour le bon montant.

Si vous ne retrouvez pas la facturette, pensez que vous avez peut-être effectué un paiement à distance (en donnant par téléphone ou par Internet le numéro de votre carte et son échéance).

Il arrive parfois que des proches, qui ont eu connaissance de votre code confidentiel, utilisent vos moyens de paiement à votre insu pour faire des retraits ou des achats chez des commerçants. Dans le doute, vérifiez auprès d'eux.

- **S'il s'agit vraiment d'une opération que vous n'avez pas faite**, signalez rapidement l'anomalie à votre banque. Dans ce cas, après enquête, si le débit carte bancaire est bien frauduleux, votre compte sera crédité de ce montant. **Vous pouvez contester** l'opération **dans un délai de** :
  - **13 mois pour un paiement dans l'espace économique européen - EEE** (Allemagne, Autriche, Belgique, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Liechtenstein, Luxembourg, malte, Norvège, Pays-Bas, Pologne, Portugal, République Tchèque, Royaume-Uni, Slovaquie, Slovénie, Suède),
  - **70 jours, pour un paiement hors de l'EEE**. Ce délai peut être prolongé contractuellement à 120 jours.
- **S'il s'agit d'une erreur de montant : vous devez payer le commerçant** par tout moyen pour le bon montant s'il peut justifier de la validité de sa créance.

En cas d'incident lié à la banque à distance

L'OUBLI DE VOS CODES D'ACCÈS

Vous ne pouvez plus accéder au service :

- **demandez à votre banque** de vous attribuer **un nouveau code d'accès**,
- à réception, n'oubliez pas de le personnaliser.

LA PERTE OU LE VOL DE VOS CODES D'ACCÈS À LA BANQUE À DISTANCE

Vous risquez qu'une autre personne les utilise :

- **lancez votre antivirus**. S'il détecte un virus, un cheval de Troie, etc. :
  - n'effectuez aucune opération de banque à distance,
  - procédez à la destruction du virus en suivant les consignes de l'antivirus,
  - effectuez une nouvelle vérification,
  - **changez vos codes d'accès de banque en ligne**.
- si vous pouvez accéder à Internet :
  - **connectez-vous au site de la banque** en entrant manuellement son adresse,
  - **modifiez immédiatement votre mot de passe**,
  - vérifiez que les dernières opérations enregistrées sont correctes,
  - **signalez l'incident à votre banque**, sans lui indiquer vos identifiants (elle n'a pas à les connaître).

Plus d'infos sur la sécurité informatique sur :
www.ddm.gouv.fr/surfezintelligent/

Pour signaler un site ou un courrier d'escroquerie :
www.internet-signalement.gouv.fr *et* ***www.signal-spam.fr***

En cas d'incident lié au chèque

LA PERTE OU LE VOL D'UN CHÈQUE SIGNÉ

Le bénéficiaire d'un de vos chèques ne l'a jamais reçu ?

- si le chèque a été encaissé, **la banque** :
  - **peut vous confirmer l'opération**,
  - **ne peut pas vous indiquer les coordonnées de la personne qui l'a encaissé** (cette indication au verso est couverte par le secret bancaire. Seule la police, sur réquisition judiciaire, pourra l'obtenir).
- si le chèque n'a pas été encaissé :
  - **faites immédiatement opposition en appelant** le numéro fourni par votre banque. A défaut, **appelez au 0.892.683.208** (0,34 € par mn). Confirmez au plus tôt par écrit à votre agence,
  - procédez à un nouveau paiement pour régler votre dette et demandez au bénéficiaire de vous donner une lettre de désistement (renonçant ainsi à présenter le chèque s'il était retrouvé).

LA PERTE OU LE VOL D'UN CHÉQUIER

En cas de perte ou vol d'un chéquier, **la procédure** d'opposition **est la même que pour un chèque signé**.
Tant que les chèques n'ont pas été encaissés, faites opposition en appelant le numéro fourni par votre banque. A défaut, **appelez au 0.892.683.208** (0,34 € par mn).
Le risque est cependant aggravé par le fait qu'il comprend des formules de chèques vierges pour lesquelles ni la date ni le montant des chèques ne sont connus.

Après avoir émis un chèque, il est illégal de faire opposition pour un motif autre que la perte, le vol, le redressement judiciaire ou la liquidation judiciaire du porteur, ou l'utilisation frauduleuse du chèque.

ANNEXES

La sécurité en vacances

AVANT DE PARTIR

La réservation

Lorsque le paiement de vos réservations n'est pas possible par carte, utilisez le virement. S'il s'agit d'une transaction en euro, au sein de l'Union européenne, le virement s'effectue au même prix qu'un virement avec RIB en France, dès lors que vous fournissez les codes BIC et IBAN du bénéficiaire.

Les contacts utiles

Vérifiez que vous saurez comment joindre votre banque en cas de problème, ainsi que les services d'assistance liés à l'utilisation de certains de vos moyens de paiement. Notez, dans un endroit sécurisé, en dehors de votre portefeuille :

- les numéros de téléphone et adresses,
- les numéros des chèques,
- le numéro à 16 chiffres de votre la carte et sa date d'expiration,
- les numéros d'opposition.

Vous pouvez utiliser la fiche ci-jointe.

A l'étranger, un numéro d'opposition figure sur les distributeurs de billets.

LES NUMÉROS UTILES

(A emmener et à conserver séparément des moyens de paiement)

- **Joindre mon agence bancaire : _____**
- **Joindre mon service d'assistance : _____**

Cartes

- **Faire opposition en France : 08 92 705 705**
- **Faire opposition à l'étranger : _____**
- **Numéro de ma carte bancaire : _____**
- **Date d'expiration de ma carte bancaire : _____**

Chèques

(uniquement pour la France)

- **Faire opposition : 08 92 683 208** (Centre national des chèques perdus ou volés)
- **Numéros des chèques emportés :**
  De _____ à _____

Chèques de voyage

(pour l'étranger)

- **Faire opposition : _____**
- **Numéros des chèques emportés :**
  De _____ à _____

SUR PLACE

Le paiement par chèque

- Payer par chèque à l'étranger est déconseillé, même dans la zone euro. Les chèques y sont rarement acceptés et cette opération entraîne des frais non négligeables.
- Pensez plutôt à la carte (si elle est acceptée là où vous vous rendez) ou aux chèques de voyage. Ceux-ci sont remboursés en cas de vol ou de perte.

Le paiement par carte

- Ne perdez jamais votre carte de vue lors d'un paiement chez un commerçant. Si l'appareil à carte est sur un comptoir ou en arrière-boutique, suivez le commerçant mais gardez votre carte à la main.

Les retraits au distributeur

- Soyez vigilant lorsque vous tapez votre code et assurez-vous que personne ne puisse mémoriser les chiffres que vous composez.
- Si vous remarquez un objet suspect sur un distributeur, notamment sur la partie où l'on introduit la carte et/ou sur le clavier de saisie du code, indiquez-le à la banque et n'utilisez pas cet appareil.

La consultation sur Internet

Si vous consultez vos comptes en ligne, dans un cyber café ou tout autre endroit public :

- assurez-vous que personne ne vous observe lorsque vous saisissez votre code et changez-le si vous croyez que quelqu'un a pu le noter. Ne mémorisez pas ces codes d'accès dans l'ordinateur même s'il vous le propose,
- utilisez le bouton de déconnexion du site de la banque dès que vous avez terminé,
- effacez l'historique après chaque connexion.

AU RETOUR

Suivez attentivement vos comptes et réagissez rapidement auprès de votre banque en cas d'anomalie.

Protégez votre ordinateur, votre mobile et vos connexions

LA CONFIGURATION DE VOTRE MATÉRIEL

- Choisissez un fournisseur d'accès internet reconnu et suivez ses conseils de sécurité.
- Téléchargez régulièrement les mises à jour de votre système, installez sur votre ordinateur, comme sur votre mobile, un antivirus et un pare-feu efficaces avec des mises à jour automatiques.
- Si vous utilisez un réseau Wi-Fi assurez-vous que la configuration est sécurisée.

QUAND VOUS RECEVEZ UN MESSAGE

- N'ouvrez pas un message douteux avec un objet et un contenu passe-partout, surtout si une pièce jointe est attachée, détruisez-le sans l'ouvrir.
- Si vous recevez un SMS vous demandant d'appeler un numéro, de vous connecter à un site depuis votre téléphone, n'y répondez pas et n'appelez pas.

Le WI-FI («Wireless Fidelity») est une norme de réseau sans fil utilisant des ondes radios entre l'ordinateur ou téléphone portable et un routeur Wi-Fi connecté à une prise téléphonique, chez vous ou à l'extérieur (par exemple : dans certains lieux publics, les hôtels...)

PROTÉGEZ VOS CONNEXIONS

- Vérifiez que votre connexion est sécurisée : présence de https (s pour secure) devant l'adresse du site, icône d'une clé ou d'un cadenas dans la fenêtre du navigateur Internet.
- Contrôlez qu'aucune autre fenêtre internet n'est ouverte, tapez vous-même l'adresse exacte fournie par la banque.
- N'activez la fonction bluetooth ou WI-FI que lorsque c'est nécessaire et désactivez-la dès la fin d'utilisation.
- N'utilisez pas d'équipement, ordinateur ou smartphone, de quelqu'un, dont vous ne maîtrisez pas le niveau de sécurité.
- Effacez l'historique dès que vous avez fini.
- Si vous avez supprimé des documents, n'oubliez pas d'effacer le contenu de la corbeille.

Le bluetooth est une technologie de réseau sans fil de faible portée permettant de relier des appareils entre eux (par exemple imprimante, téléphone portable, souris, clavier, etc.).

LEXIQUE

L'**antivirus** permet de détecter et de supprimer les virus sur votre ordinateur. Il doit être mis à jour pour être réellement efficace.

Le **cheval de Troie** est un virus qui peut installer des logiciels espions permettant de mémoriser et restituer l'activité de l'ordinateur (exemple : vos frappes au clavier pour les envoyer à un serveur pirate).

Le **pare-feu** (ou «firewall») permet de protéger l'ordinateur lors des connections à Internet. A chaque connexion avec un site susceptible de communiquer avec l'ordinateur, le pare-feu demande une autorisation.

Le « **pharming** » : contraction des mots anglais « farming » (« culture fermière » qui consiste pour les jeux en ligne à récolter de l'argent) et « phone phreaking » (piratage de lignes téléphoniques). Vous êtes redirigé automatiquement vers un site pirate ressemblant au vrai site. Les pirates peuvent alors récupérer toutes vos informations.

Le **« phishing »** : contraction des mots anglais « fishing », (pêche) et « phreaking » (piratage de lignes téléphoniques). Un courrier électronique vous invite, souvent pour des raisons de sécurité, à vous connecter à un site de banque, un compte de paiement en ligne ou encore un site commercial. Le lien conduit en fait vers un site pirate.

Le **virus** s'installe sur votre ordinateur via un courrier électronique reçu ou un téléchargement. Il peut altérer le fonctionnement de votre ordinateur, détruire des informations, les transmettre à distance...

Quelques pièges à éviter

Piège 1 - « UN ACQUÉREUR GÉNÉREUX »

Les circonstances : Vous vendez un bien. L'acquéreur vous propose un prix supérieur en prétextant qu'il bénéficie d'un service complémentaire (des frais de transport par exemple). Vous recevez un chèque du montant global (prix + service) que vous déposez à l'encaissement. L'acquéreur annule le service supplémentaire (transport par exemple) et vous demande de lui rembourser la différence entre le prix d'origine du bien et le montant total qu'il vous a déjà payé, soit par virement sur un compte de tiers, soit par transfert d'espèces à un tiers.

Où est le piège ? Le chèque étant un faux, il reviendra impayé.
Au mieux, vous gardez votre bien mais vous perdez le montant soi-disant « remboursé ».

Comment l'éviter ? Refusez, n'encaissez pas le chèque et ne livrez pas le bien.

Piège 2 - « ETRE PAYÉ AUTREMENT QUE PRÉVU »

Les circonstances : Vous vendez un bien. L'acquéreur vous demande vos coordonnées bancaires pour vous faire un virement. Il vous adresse finalement un chèque que vous déposez sur votre compte. Le montant prévu arrive sur votre compte et vous livrez la marchandise (un véhicule par exemple). Or le montant n'a pas été crédité par virement comme prévu mais suite au dépôt du chèque. Quelques jours plus tard, votre compte est débité de ce montant.

Où est le piège ? Le chèque déposé était un faux chèque, il a donc été rejeté. Votre compte est débité.

Comment l'éviter ? N'encaissez pas le chèque, demandez un virement. Avant de livrer le bien, vérifiez que votre compte est bien crédité par un virement.

Piège 3 - « LE FAUX CHÈQUE DE BANQUE »

Les circonstances : Vous vendez un bien. L'acquéreur vous propose de payer par chèque de banque. Vous appelez le numéro de téléphone inscrit sur le chèque pour vérifier que la banque a bien émis ce chèque. Elle vous le confirme par téléphone. Pourtant, le chèque revient impayé.

Où est le piège ? Le chèque était un faux et le numéro de téléphone celui d'un complice.

Comment l'éviter ? Pour vérifier la validité du chèque de banque, vous devez contacter la banque en cherchant le numéro dans l'annuaire ou encore mieux, vous rendre à l'agence bancaire si c'est possible.

Piège 4 - « ETRE RECRUTÉ COMME MULE »

Les circonstances : Vous recevez un courrier électronique vous proposant de collaborer à une soi-disant société financière (parfois un contrat de travail est joint à l'offre pour la rendre plus crédible). On vous offre une rémunération si vous rendez le service suivant : recevoir sur votre compte une somme d'argent d'un certain montant puis la transférer ensuite sur un autre compte qu'on vous indiquera.

Où est le piège ? Par ce transit d'argent, l'escroc « blanchit » de l'argent provenant probablement d'un trafic et tente de le remettre dans un circuit normal. La fraude est difficile à détecter et la récupération des fonds plus compliquée. En tant que « mule », vous risquez d'être reconnu complice d'une fraude passible de poursuites judiciaires.

Comment l'éviter ? Ne vous laissez pas tenter par l'appât du gain. Refusez l'opération. Détruisez ce type de message dès réception.

Piège 5 - LA FRAUDE À LA LOTERIE

Les circonstances : Vous recevez un courrier électronique sur votre ordinateur ou un SMS sur votre téléphone portable. Il prétend que vous avez gagné un prix et vous invite à répondre en joignant vos coordonnées bancaires afin que le prix puisse être viré sur votre compte.

Où est le piège ? Vous communiquez vos coordonnées bancaires à des escrocs qui sont susceptibles de les utiliser ou de les transférer. Si vous appelez au numéro indiqué, l'appel est surfacturé et n'aboutit à rien.

Comment l'éviter ? Une offre trop alléchante est sans doute une arnaque. Elle peut provenir d'un faux commerçant et/ou vous rendre complice d'une fraude.