



Sécurité des opérations bancaires

Juin 2006

LES MINI-GUIDES BANCAIRES

Hors série



FEDERATION
BANCAIRE
FRANCAISE

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



Sécurité des opérations bancaires

INTRODUCTION

**La technologie moderne permet
un haut degré de sécurité
dans les opérations bancaires.**

Pour permettre à chacun de profiter au mieux de cette sécurité, la FBF met à la disposition du public ce Guide Pratique reprenant les principaux points à savoir, les règles de sécurité, les bonnes pratiques, etc.

Ces quelques conseils simples ne suppriment pas les risques mais les réduisent de façon importante. Si un incident se produit, vous trouverez aussi ici la conduite à tenir pour en limiter les conséquences.

Si vous avez des questions concernant le contenu de ce guide, utilisez la fonction contact du site www.lesclesdelabanque.com ou posez-les directement par courrier électronique à l'adresse suivante : cles@fbf.fr. Vous trouverez plus d'informations sur la sécurité informatique sur le site www.protegetonordi.com.

SOMMAIRE

LES PRINCIPAUX RISQUES ET LEUR PRÉVENTION

La sécurité des moyens de paiement	5
• le chèque émis	6
• le chèque reçu	7
• la carte	8
La sécurité des opérations à distance	10
• Banque à distance	11
• Achat à distance par Internet	14
• Achat à distance par téléphone	14
<u>LA GESTION DES INCIDENTS</u>	15
La détection d'une anomalie - le relevé de compte	16
La perte ou le vol	17
• de son chéquier	17
• de sa carte ou de son code	18
• de son code d'accès à la banque à distance	19



Consultez et demandez
conseil à votre banque,
elle peut mettre à votre disposition
des informations spécifiques
sur la sécurité.



Les principaux risques et leur prévention

LA
SÉCURITÉ
DES
MOYENS
DE PAIEMENT

LE CHÈQUE ÉMIS

La perte

- Vous perdez votre chéquier,
- Votre chéquier est perdu lors de son envoi par courrier postal,
- Vous l'oubliez dans un lieu non sûr.

- Retirez votre chéquier à l'agence ou privilégiez un envoi sécurisé. A réception d'un nouveau chéquier notez à part les numéros des formules de chèques pour pouvoir faire opposition si nécessaire.
- Si vous devez le recevoir par voie

postale, n'hésitez pas à contacter votre agence en cas de retard de réception.

- Laissez votre chéquier en lieu sûr quand vous ne l'utilisez pas et évitez de le conserver avec des pièces d'identité.
- Remettez le en sécurité dès que vous l'avez utilisé.

Le vol de formules de chèques vierges

On vous dérobe une formule, ou plusieurs formules de chèques, ou tout votre chéquier alors que les formules de chèques volées ne sont pas remplies.

- Limitez le nombre de chèquiers en votre possession.
- Ne laissez jamais votre chéquier sans surveillance, par exemple, ne le laissez pas dans un véhicule même fermé à clé.
- N'inscrivez sur votre chéquier aucune information confidentielle (un code par exemple).

- Restituez à la banque vos formules de chèques inutilisées en cas de clôture du compte ou sur simple demande de sa part.
- Ne signez pas par avance de chèque ne comportant ni montant, ni indication du bénéficiaire.

La falsification

Un chèque que vous avez émis est volé avant d'être encaissé par son bénéficiaire. Le voleur tente de maquiller le chèque pour pouvoir l'encaisser.

- Écrivez au stylo bille noir, ne faites ni rature ni surcharge.
- Commencez bien au début de chaque ligne pour que rien ne puisse être ajouté avant.
- Complétez les lignes d'un trait horizontal pour que rien ne puisse être ajouté après.
- Ne signez jamais de chèque en blanc.
- Évitez de donner en paiement un chèque sans le nom du bénéficiaire ou, si vous ne remplissez pas vous-même le

- nom du bénéficiaire, vérifiez qu'il le fait 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-le et signez-le après vous être assuré de la lisibilité et de l'exactitude des mentions portées par la machine.
- N'oubliez pas de remplir la date et le lieu d'émission (mentions obligatoires) et de signer votre chèque.

■ En cas de vol ou de perte du chèque avant sa remise au bénéficiaire, faites opposition auprès de votre banque, ou en appelant le numéro d'opposition qu'elle vous a fourni, ou encore appeler le Centre

national d'Appels des Chèques Perdus ou Volés, service de la banque de France ouvert 7j/7 et 24h/24 au 0892683208 (0,34€ par min).

LE CHÈQUE REÇU

Le chèque falsifié

Vous vendez un bien et recevez un chèque en paiement qui se révèle être un chèque falsifié.

■ En tant que bénéficiaire, vous devez vérifier le chèque (le support : attention notamment aux altérations) et voir si toutes les mentions obligatoires y figurent bien.

■ Vérifiez l'identité de la personne qui vous remet le chèque en paiement.

■ En cas d'absence de bénéficiaire, complétez le de votre nom et signez au dos immédiatement.

Le faux chèque

Vous vendez un bien. L'acquéreur vous demande vos coordonnées bancaires pour vous faire un virement. Il vous règle par non par virement mais par chèque. Quelques jours plus tard, votre compte est débité de ce montant, car le chèque déposé était un faux chèque, il a donc été rejeté.

■ Soyez vigilant, ne concluez jamais de transaction dans la précipitation.

■ Assurez-vous que le paiement est réalisé pour le montant et selon les modalités convenues avec l'acheteur (chèque si vous aviez convenu d'un

chèque ou virement si vous aviez convenu d'un virement).

■ N'acceptez pas comme paiement le dépôt d'un chèque par un tiers sur votre compte.

Le montant chèque

Vous vendez un bien. L'acquéreur vous propose un meilleur prix. La majoration est justifiée par la rémunération d'un service demandé en complément (des frais de transport par exemple). Vous recevez un chèque du montant convenu (prix + service) que vous déposez à l'encaissement. Simultanément, l'acquéreur vous demande d'annuler le service spécial demandé et de lui rembourser la différence entre le prix du bien et le montant total, soit sous forme de virement sur un compte de tiers (?), soit sous forme de transfert d'espèces à un tiers. Le chèque, faux, reviendra impayé, vous garderez votre bien mais vous aurez perdu le remboursement de la différence. (pas clair)

■ Soyez vigilant, ne concluez jamais de transaction dans la précipitation.

■ Méfiez-vous d'une offre de prix supérieur au montant demandé.

■ Assurez-vous que le paiement est réalisé pour le montant et selon les modalités convenues avec l'acheteur (chèque ou virement)

■ N'acceptez que des montants correspondant au montant de la transaction.

Le faux chèque de banque

On vous propose de vous régler avec un (faux) chèque de banque en paiement.

■ Si l'acheteur propose de vous payer par chèque de banque, le plus sûr moyen de vous assurer de la validité du chèque consiste à vous rendre à la banque émettrice du chèque, avec l'acheteur pour vous faire remettre le chèque par la banque.

■ En cas d'impossibilité, n'hésitez pas à appeler la banque émettrice pour demander confirmation.

■ Avant de l'appeler vérifiez dans un annuaire que le numéro d'appel est bien celui de la banque, car si le chèque qu'on vous a remis est un faux chèque, le numéro de téléphone qui y figure est

sans doute celui d'un complice.

■ N'hésitez pas à différer le jour de la vente (évitez la vente un jour férié ou un dimanche) pour être sûr de joindre l'établissement bancaire.

■ Si vous n'avez pas pu vous assurer auprès de la banque de la validité du chèque, soyez attentifs aux altérations (couleurs, taches, traces de grattage ou de lavage, écritures différentes).

■ En cas de doute, ne vous dessaisissez pas de votre bien et préférez reporter la transaction afin d'effectuer les vérifications nécessaires.

BON À SAVOIR

Un chèque, même s'il est vrai, n'est pas un moyen de paiement garanti, un rejet de chèque est toujours possible (par exemple absence de provision)

LA CARTE

La perte

Votre carte est perdue lors de son envoi par courrier postal, vous l'oubliez dans un lieu non sûr.

■ Retirez votre carte à l'agence ou privilégiez un envoi sécurisé.

■ Conservez votre carte en lieu sûr.

■ Pensez à ranger votre carte à chaque utilisation

Le vol sans le code

Votre carte vous a été volée mais le voleur ne connaît pas votre code confidentiel.

■ Ne laissez pas votre carte à la vue de tiers, sans surveillance, même un court instant.

- Ne perdez jamais votre carte de vue lors d'un paiement chez un commerçant.
- Votre carte est personnelle, ne la confiez à personne.
- Notez sur un document qui vous est accessible (mais pas avec la carte)

le numéro de votre carte et sa date d'échéance pour faciliter la déclaration en cas d'opposition.

- En cas de renouvellement de votre carte, pensez à bien détruire l'ancienne en coupant la puce en deux.

Le vol avec le code

Votre carte vous a été volée et le voleur connaît votre code confidentiel.

- N'inscrivez pas votre code sur la carte ou sur un autre document.
- Ne communiquez votre code à personne (même pas à un membre de votre famille, à votre banquier ou à la police).
- Si le voleur de la carte ne connaît pas le code, il cherchera peut-être à l'obtenir de votre part par ruse en se faisant passer pour un banquier, un assureur, la police, etc.
- Le voleur peut également chercher à vous voler votre carte parce qu'il a précédemment pris connaissance de votre code par exemple en vous regardant payer chez un commerçant ou retirer des espèces à un distributeur. Pensez à la confidentialité quand vous tapez votre code chez un commerçant ou à un distributeur de billets.
- En cas de renouvellement de votre carte, pensez à bien détruire l'ancienne en coupant la puce en deux.

La fraude

Quelqu'un qui connaît le numéro de votre carte et sa date d'échéance cherche à utiliser ces informations pour payer à distance.

- Conservez votre carte à l'abri des regards indiscrets.
- Ne vous séparez pas de votre carte. Lors d'un paiement chez un commerçant, celui-ci ne doit pas emporter votre carte hors de votre vue.
- Ne notez le numéro de votre carte et son échéance sur aucun document susceptible de perte ou vol car cela pourrait faciliter ainsi une fraude.
- En cas de renouvellement de votre carte, pensez à bien détruire l'ancienne en coupant la puce en deux.

La fraude

Adjonction par des malfaiteurs d'un dispositif susceptible de lire les caractéristiques de votre carte et/ou présence d'un système vidéé

- Sur un distributeur de billets (DAB) ou sur un guichet automatique de banque (GAB) si vous remarquez un changement d'aspect ou un élément suspect, notamment sur la partie d'insertion de la carte et/ou sur le clavier de saisie du code (par exemple surépaisseur) n'hésitez pas à l'indiquer à la banque.

La déclaration tardive de perte ou de vol

Après la perte ou le vol de votre carte, vous n'avez pas fait immédiatement opposition.

- Notez sur un document qui vous est accessible (mais séparément de la carte) le numéro de votre carte et sa date d'échéance pour faciliter la déclaration en cas d'opposition.
- Notez les numéros à appeler pour faire opposition auprès des organismes

concernés (banque ou réseau carte ou n° d'assistance).

- Ces informations doivent être conservées à part et accessibles en cas de perte ou de vol de votre sac/portefeuille.

LA SÉCURITÉ DES OPÉRATIONS À DISTANCE

BANQUE À DISTANCE

l'usage de votre code

quelqu'un peut se servir de votre code d'accès.

- Votre code d'accès à vos comptes bancaires sur internet est strictement personnel, ne le divulguez à personne, même à une personne se présentant comme étant de votre banque, de la police, etc. et conservez-le en sécurité.
- Changez de code dès réception de celui-ci lors de votre souscription au service et modifiez le régulièrement par la suite.
- Ne choisissez pas un code facile à identifier (exemple votre date de

naissance) Choisissez de préférence un code alphanumérique contenant à la fois des lettres et des chiffres, et évitez les codes que vous utilisez pour d'autres services en ligne (e mail, messagerie instantanée...).

- Assurez-vous que personne ne vous observe lorsque vous saisissez votre code et changez-le si vous croyez que quelqu'un a pu le découvrir (par exemple lors d'une connexion dans un lieu public...)

■ Ne mémorisez pas ces codes d'accès dans votre ordinateur même s'il vous le propose.

■ Utilisez le bouton de déconnexion du site de la banque dès que vous avez terminé.

■ Si vous avez supprimé des documents,

n'oubliez pas d'effacer le contenu de la corbeille.

■ Si vous utilisez un ordinateur partagé avec d'autres personnes, effacez l'historique après chaque connexion.

■ Si la date de votre dernière connexion est affichée, vérifiez-la.

Le « phishing »

Un courrier électronique vous invite à vous connecter à votre site de banque à distance soit pour mettre à jour vos données, soit pour « une alerte sécurité » vous invitant à aller changer votre code.

ATTENTION : Le lien censé vous y conduire est relié à un site factice (copie parfaite du site de votre banque) destiné à capturer votre code d'accès. Vous risquez la fraude, l'usurpation de votre identité et l'infection de votre ordinateur.

■ Ne répondez jamais à un courrier électronique vous invitant à vous connecter à votre site de banque à distance et à y déposer vos codes d'accès, les banques n'émettent jamais de message de cette nature.

■ Assurez-vous que vos sessions internet avec votre banque sont sécurisées : dans votre espace personnel de consultation, vérifiez que le code https:// figure devant l'adresse du site ou l'icône d'une clé ou d'un cadenas dans le bas de l'écran à droite. Vos informations personnelles sont alors bien encodées, interdisant ainsi à toute personne de les lire.

■ Assurez-vous qu'aucune autre fenêtre de votre navigateur (Explorer, Netscape ...) n'est ouverte, cela vous évitera d'être connecté à d'autres sites Internet pendant votre session et vous assurera que personne d'autre que vous ne peut accéder à vos comptes par l'intermédiaire d'un autre site.

■ Ne répondez jamais à un courrier électronique vous invitant à vous

connecter à votre site de banque à distance et à y déposer vos codes d'accès, les banques n'émettent jamais de message de cette nature.

■ Si vous recevez un courrier électronique semblant douteux et utilisant les coordonnées ou l'identité (logo, visuel...) de votre banque, prévenez-la au plus vite en lui faisant suivre le message.

■ Ce type de message semble pourtant généralement provenir de votre banque elle-même et contient un lien électronique vers une copie parfaite du site de votre banque.

■ L'escroc tente par ce moyen de vous amener à lui livrer votre code d'accès.

■ Pour vous connecter sur le site de votre banque et non pas sur un site factice, tapez vous-même l'adresse exacte fournie par la banque.

■ Faites aussi attention aux messages vous incitant à appeler votre banque : prenez le temps de vérifier le numéro de téléphone.

Le virus

Il s'installe discrètement sur votre ordinateur via un e-mail reçu, un partage de répertoires ou un téléchargement. Il est susceptible d'altérer le fonctionnement de votre ordinateur, de détruire des informations, voire d'en récupérer pour les transmettre à distance.

Le cheval de Troie

Il repose sur le même principe qu'un virus, c'est un programme contenu dans un message ou un fichier reçu et qui peut s'installer sur votre ordinateur sans que vous vous en aperceviez. Si vous l'ouvrez il peut endommager l'ordinateur voire supprimer des dossiers. Il utilise lui-même votre carnet d'adresses pour se propager.

Le ver

C'est un petit programme qui utilise les réseaux (si vous avez plusieurs ordinateurs reliés entre eux) et cherche les failles de sécurité pour se répliquer de machine à machine. En se répliquant, il épuise le temps machine, l'espace du disque et la vitesse ralentissant les serveurs et rendant Internet inutilisable.

■ Assurez-vous que l'ordinateur à partir duquel vous accédez à votre service de banque à distance est équipé d'un antivirus à jour et d'un pare-feu (ou firewall).

■ Les antivirus et firewall doivent donc être très régulièrement mis à jour, car de nouveaux virus, vers et chevaux de Troie apparaissent quasiment tous les jours. Il est donc recommandé d'installer des antivirus et firewall qui se mettent à jour régulièrement et automatiquement.

■ Soyez encore plus rigoureux si votre ordinateur est connecté à Internet en permanence via un accès haut débit (ADSL ou câble).

■ Suivez les conseils de votre fournisseur d'accès et consultez régulièrement le site Internet du logiciel d'exploitation de votre ordinateur (par exemple Microsoft pour Windows) pour télécharger les patches et les mises à jour de votre système, et lutter ainsi contre les vers.

BON À SAVOIR

...l'antivirus est un outil passant au crible l'ensemble des composants de votre ordinateur : fichiers entrants (téléchargés ou reçus par messagerie) ou sortants, archives, documents exécutables, etc. En cas de contamination par un virus, il se charge de désinfecter le fichier contaminé ou procède en cas d'échec à sa mise en quarantaine dans un coin du disque dur ou encore procède à sa destruction pure et simple. Il requiert une base de données de virus à jour pour être réellement efficace.

■ Si vous recevez un message douteux, avec un objet et un contenu passe-partout, l'un comme l'autre souvent en anglais mais pas obligatoirement, soyez particulièrement méfiant en particulier si une pièce jointe est attachée. N'ouvrez pas le message, ni la pièce jointe surtout s'il s'agit d'un fichier avec l'extension .exe .com .scr .pif ou .vbs mais cette liste n'est pas exhaustive.

Si le fichier infecté est ouvert, il risque d'endommager votre disque dur, les fichiers programmes et les fichiers d'e-mail. Avant d'ouvrir un message, activez votre anti-virus pour qu'il détecte les éventuelles infections. En cas de doute, détruisez le message avec la pièce jointe sans l'ouvrir.

BON À SAVOIR

...le pare feu est un composant (logiciel ou matériel) permettant de protéger du piratage informatique un ordinateur connecté à Internet, en filtrant les échanges de données transitant à travers les différents ports de communication de l'ordinateur. Le pare feu évite les intrusions en bloquant les canaux de communication sensibles ou inutiles.

A chaque connexion avec un site susceptible de communiquer directement avec votre ordinateur, le pare feu vous demande si vous autorisez cet échange. Vérifiez donc bien à chaque fois l'origine de la requête et ne l'autorisez que si elle est fiable.

Si votre ordinateur est connecté à Internet par un réseau Wi-Fi, vous risquez :

L'interception de données : écoute par un tiers des transmissions de votre réseau sans fil ; **le détournement de connexion :** obtention par un tiers de l'accès à votre réseau local, ou à Internet par l'intermédiaire de votre réseau ; **le brouillage de transmissions :** émission par un tiers de signaux radio, destinés à produire des interférences.

Les ondes transitent de votre ordinateur équipé d'une carte Wi-Fi (émetteur récepteur) à un routeur Wi-Fi connecté au modem, lui-même branché à une prise téléphonique. Vous pouvez ainsi, sans fil, connecter votre ordinateur à Internet, chez vous ou sur des bornes Wi-Fi (par exemple : dans certains lieux publics, les hôtels...).

La sécurité d'un tel réseau passe par des mécanismes d'authentification et de chiffrement que vous devez configurer à l'installation :

■ Vous ne devez pas y conserver les valeurs par défaut : changez les mots de passe, les identifiants... et pensez à en changer régulièrement.

■ Pour protéger votre réseau, vous devez au moins activer le chiffrement à l'aide d'une clé alphanumérique qui permet d'assurer une certaine confidentialité.

BON À SAVOIR

...Le Wi-Fi (Wireless Fidelity) est une norme de réseau sans fil qui utilise des ondes radios, dont la portée peut être de 20 à 50 mètres (à travers le béton, entre plusieurs étages...).

■ En cas de doute sur la sécurité de votre réseau Wi-Fi n'hésitez pas à suivre les conseils de votre fournisseur d'accès Internet et/ou à consulter un spécialiste confidentialité.

ACHAT A DISTANCE PAR INTERNET

Le paiement par carte sur Internet

Le site du commerçant n'est pas sécurisé et vos données personnelles sont détournées par des tiers.

■ Informez-vous auprès de votre banque pour choisir avec elle la solution la plus sécurisée.

■ Assurez-vous avant de saisir les caractéristiques de votre carte bancaire (ou toute autre donnée personnelle) que le site est sécurisé (le code https:// figure devant l'adresse du site ou un cadenas apparaît (généralement en bas de l'écran à droite).

■ En cas de doute, mieux vaut passer votre commande par un autre moyen.

■ D'un seul clic, vous devez pouvoir accéder aux coordonnées du commerçant (nom, adresse, téléphone, service clients) La réputation d'un commerçant peut être un critère de choix.

■ N'adressez jamais les caractéristiques de votre carte bancaire par courrier électronique, et encore moins le code confidentiel de la carte ou celui permettant d'accéder à votre service de banque à distance.

Le « phishing », les faux sites la fraude à la loterie :

Vous recevez un e-mail qui 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.

Soyez sur vos gardes !

■ Si une offre est trop alléchante, elle peut émaner d'un faux commerçant ou vous rendre complice d'une fraude... soyez vigilant.

■ Attention : les escrocs n'hésitent pas à « relancer » leurs victimes.

ACHAT À DISTANCE PAR TÉLÉPHONE

La fraude

les informations que vous avez données par téléphone pour commander un bien ou un service ont été utilisées par une tierce personne.

■ Évitez de donner les caractéristiques de votre carte à un commerçant dont vous n'êtes pas sûr.

■ Renseignez-vous sur ce commerçant en vérifiant ses coordonnées : téléphone, adresse, service clients...

■ Faites-vous confirmer et notez le montant exact et la date de l'opération qui passera sur votre compte.

■ Suivez-en l'application pour réagir immédiatement en cas d'anomalie.

La gestion des incidents

LA DÉTECTION D'UNE ANOMALIE

LE RELEVÉ DE COMPTE

Le pointage de son relevé de compte

pour vérifier qu'aucune opération anormale n'est enregistrée. Il peut s'agir d'une simple erreur mais il peut aussi s'agir d'une tentative d'escroquerie.

- Si vous avez un doute sur une opération, mieux vaut demander sans attendre des précisions à votre agence bancaire sur les références précises de l'opération.
- Si une opération ne vous concerne pas, prévenez immédiatement votre

agence par téléphone et confirmez par lettre.

- Selon la nature de l'opération anormale relevée, votre agence pourra faire des recherches.

La recherche d'un chèque émis par vous et disparu

si vous avez envoyé un chèque à un bénéficiaire et qu'il ne l'a jamais reçu.

- Il peut s'agir d'une simple erreur qui sera alors rapidement régularisée.
- Si le chèque a été encaissé, la banque peut vous confirmer l'encaissement du chèque mais n'a pas à vous communiquer les coordonnées de la personne à qui le chèque a été payé : cette indication figurant au verso est couverte par le secret bancaire.

Seule la police, sur réquisition judiciaire, pourra obtenir le nom de la personne à qui le chèque aura été payé.

- Si le chèque n'a pas été encaissé, faites immédiatement opposition pour perte – voir ci-après – et faites un nouveau chèque pour régler votre dette au bénéficiaire et demandez-lui de vous donner une lettre de désistement.

Le pointage des factures carte

pour vérifier que les opérations par carte qui apparaissent sur votre compte sont bien celles que vous avez initiées.

- Si vous êtes débité d'un paiement par carte non réalisé par vous ou réalisé pour un montant différent, signalez très rapidement l'anomalie à votre banque (vous avez légalement 70 jours pour réagir mais mieux vaut faire le plus vite possible). Après enquête, elle vous remboursera s'il y a lieu, le paiement contesté.
- 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).

attention : certains commerçants peuvent utiliser une enseigne commerciale différente de leur raison sociale (par exemple, le nom d'un restaurant ne porte pas toujours pas le nom de la société qui l'exploite).

Le pointage des opérations effectuées à distance

pour vous assurer que le paiement à distance que vous avez effectué par téléphone ou par Internet a bien été exécuté pour le bon montant

■ En cas de contestation sur un paiement par carte à distance, la banque peut vous rembourser du montant litigieux.

■ à vous ensuite de payer le commerçant par tout moyen pour le bon montant s'il peut justifier de la validité de sa créance.

LA PERTE OU LE VOL

CHEQUIER

La perte ou le vol d'un chèque signé

■ Si le bénéficiaire d'un chèque que vous avez émis ne l'a jamais reçu, faites opposition auprès de votre banque, ou en appelant le numéro d'opposition qu'elle vous a fourni.

■ Si vous ne parvenez pas à joindre votre banque ou le numéro qu'elle vous a fourni, vous pouvez informer le Centre national d'Appels des Chèques Perdus ou Volés, service de la Banque de France ouvert 7j/7 et 24h/24 au 0.892.683.208 (0,34 e par min). Attention, cette mesure d'urgence ne vous dispense pas de faire opposition au plus tôt à votre agence par écrit.

BON À SAVOIR

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

La perte ou le vol d'un chéquier

■ Si vous avez perdu ou si on vous a volé un chéquier, la procédure pour enregistrer l'opposition est la même que pour un chèque signé, mais le

risque est aggravé par le fait qu'il s'agit de formules vierges et que donc, ni la date ni le montant des chèques ne sont connus

CARTE OU CODE

La perte ou le vol de sa carte

■ Faites immédiatement opposition en appelant le numéro fourni par votre banque.

■ Si vous ne le connaissez pas appelez le 0.892.705.705 (0,34 €par mn) accessible 24 h sur 24 qui vous orientera. Un numéro d'enregistrement vous sera alors communiqué. Confirmez ensuite sans délai cette opposition par courrier auprès de votre banque. Depuis l'étranger, vous pouvez faire opposition en appelant le numéro figurant sur les distributeurs des réseaux Visa et Eurocard Mastercard.

■ Dans certains cas, un justificatif de dépôt de plainte pourra vous être demandé.

BON À SAVOIR

Attention : il est illégal de faire opposition pour un motif autre que la perte, le vol, le redressement ou la liquidation judiciaires du bénéficiaire, l'utilisation frauduleuse de la carte ou des données liées à son utilisation.

La perte ou le vol de son code

■ Si vous avez toujours votre carte, personne ne peut accéder à votre compte avec le seul code confidentiel de la carte.

■ En cas de vol, par précaution, demandez à votre agence une nouvelle carte et un nouveau code confidentiel

■ Si vous avez simplement oublié votre code, contactez votre agence, il vous parviendra sous pli confidentiel, même la banque n'en a pas connaissance.

■ Évitez de le recopier ou de conserver le document portant le numéro,

La carte capturée dans un distributeur de billets

■ Si le distributeur de billets est attaché à une agence bancaire et que celle-ci est ouverte, renseignez-vous sur place auprès du personnel sur la cause de la capture.

■ Si la carte a été capturée suite à une mauvaise manipulation de votre part, il est parfois possible de la récupérer immédiatement sans avoir à faire opposition.

- Dans tous les autres cas, mieux vaut faire opposition par prudence.
- Si le distributeur n'est pas attaché à une agence bancaire ou si celle-ci n'est pas ouverte, faites immédiatement opposition auprès du numéro mis à votre

disposition par votre banque ou auprès du 0 892 705 705 (0,34€par mn) comme ci-dessus. Depuis l'étranger, vous pouvez faire opposition en appelant le numéro figurant sur les distributeurs des réseaux Visa et Eurocard Mastercard.

CODE D'ACCÈS À LA BANQUE EN LIGNE

L'oubli de votre code d'accès

vous ne pouvez pas accéder au service mais votre code ne peut pas être utilisé par un tiers

- 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 votre code d'accès à la banque à distance

ce code pourrait être utilisé par un tiers

- si vous êtes en mesure d'accéder à Internet, connectez-vous au site de la banque en entrant manuellement son adresse et modifiez immédiatement votre code d'accès, puis vérifiez que les dernières opérations enregistrées sont correctes
- signalez l'incident à votre banque, mais vous n'avez jamais à lui communiquer votre code qui ne doit être connu que de vous.