PEFC
PEFC/10-31-1149

Imprimé avec des encres végétales sur du papier PEFC par une imprimerie détentrice de la marque Imprim'vert, label qui garantit la gestion des déchets dangereux dans les filières agréées. La certification PEFC garantit que le bois utilisé dans la fabrication du papier provient de forêts gérées durablement.

IMPRIM'VERT
Votre imprimeur agit pour l'environnement

Sécurité des opérations bancaires

LES MINI-GUIDES BANCAIRES

www.lesclesdelabanque.com
Le site d'informations pratiques sur la banque et l'argent

FEDERATION
BANCAIRE
FRANCAISE

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

Nouvelle édition
Juin 2008 - Hors série

les clés de la banque

Ce mini-guide vous est offert par :

Éditeur : FBF - 18 rue La Fayette 75009 Paris - Association Loi 1901
Représentant légal : Ariane Obolensky • Directeur de la publication : Ariane Obolensky
Directeur délégué de la publication : Valérie Ohannessian
Rédacteur en chef : Philippe Caplet • Imprimeur : Concept graphique,
ZI Delaunay Belleville - 9 rue de la Poterie - 93207 Saint-Denis • Dépôt
légal : juin 2008 • ISSN en cours

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.

Mieux vaut prévenir que guérir et ces quelques conseils simples, s’ils ne suppriment pas les risques, les réduisent de façon importante. Si malgré tout 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, vous pouvez utiliser la fonction contact du site www.lesclesdelabanque.com ou les poser directement par courrier électronique à l’adresse suivante : cles@fbf.fr
Vous pourrez trouver plus d’informations sur la sécurité informatique sur le site http://www.protegetonordi.com et sur http://www.ddm.gouv.fr/surfezintelligent/

SOMMAIRE

> « 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.

■ 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 vos pièces d'identité.

■ Remettez-le en sécurité dès que vous l'avez utilisé.

BON À SAVOIR

A réception d'un nouveau chéquier, notez à part les numéros des formules de chèques de manière à pouvoir retrouver rapidement ces numéros en cas de perte ou de vol et pouvoir faire opposition

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 chéquiers en votre possession.

■ Votre chéquier ne doit pas rester 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 jamais 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.

■ Ecrivez au stylo bille noir, ne faites ni rature ni surcharge.

■ Commencez bien à remplir le chèque 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.

■ Evitez 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 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-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.

■ Notez sur un document, séparément du chéquier, les numéros des chèques pour faciliter la déclaration en cas d'opposition. Notez les numéros à appeler pour faire opposition. (Voir page 19).

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

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 montant du chèque

Vous vendez un bien à un certain prix. L'acquéreur vous propose un prix supérieur. 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 supplémentaire (transport par exemple) et donc de lui rembourser la différence entre le prix d'origine du bien et le montant total qu'il vous a déjà payé, 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.
D'ailleurs 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). Voir Piège 2.

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

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

Le faux chèque

Vous vendez un bien. L'acquéreur vous demande vos coordonnées bancaires pour vous faire un virement. Votre compte a bien été crédité, non par virement mais par un dépôt de chèque, et au vu du crédit vous livrez la marchandise (un véhicule par exemple).
Quelques jours plus tard, votre compte est débité de ce montant, car le chèque déposé s'avère être un faux chèque, il a donc été rejeté. Voir Piège 1.

- 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.

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 pour absence de provision)

Le faux chèque de banque

Vous recevez un (faux) chèque de banque en paiement Voir Piège 3.

- 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.
- 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. N'hésitez pas à vous y rendre si besoin.
- 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.

LA CARTE

La perte

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

- Retirez votre carte à l'agence ou privilégiez un envoi sécurisé.
- Conservez votre carte en lieu sûr.
- Pensez à ranger votre carte après 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 séparément de 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 et la piste magnétique 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.
- Détruisez dès réception le courrier envoyé par votre banque vous indiquant votre code confidentiel
- 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 et la piste magnétique en deux.

La fraude sur un paiement à distance

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 et la piste magnétique en deux.

LA SÉCURITÉ DES OPÉRATIONS À DISTANCE

BANQUE À DISTANCE

L'usage de vos codes Internet

Quelqu'un peut se servir de vos codes d'accès.

- Vos codes d'accès (identifiant, mot de passe, …) à vos comptes bancaires sur Internet sont strictement personnels, ne les divulguez à personne, ni même à votre banque, ni à une personne se présentant comme étant de votre banque ou de la police, etc. et conservez-les en sécurité.
- Changez de mot de passe dès réception de celui-ci lors de votre souscription au service et modifiez-le régulièrement par la suite.
- Ne prenez pas pour code un code facile à identifier (exemple votre date de naissance, le prénom de vos enfants…) Choisissez de préférence un code alphanumérique (contenant à la fois des lettres et des chiffres), et évitez surtout les codes que vous utilisez pour d'autres services en ligne (que ce soit pour l'e mail, une messagerie instantanée, l'accès à des sites communautaires et affinitaires qui sont souvent moins sécurisés).

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 voir page 18).
- Ces informations doivent être conservées à part et accessibles en cas de perte ou de vol de votre sac / portefeuille.

La fraude lors d'un retrait d'espèces

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

- 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
- Assurez-vous que personne ne vous observe lorsque vous saisissez vos codes et changez votre mot de passe 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.
Le lien censé vous y conduire est relié à un site factice destiné à capturer votre code d'accès.
Vous risquez la fraude, l'usurpation de votre identité et l'infection de votre ordinateur.

- Assurez-vous que vos sessions Internet avec votre banque sont sécurisées : dans votre espace personnel de consultation, vérifiez que l'indication https:// figure devant l'adresse du site. Vous pouvez aussi trouver l'icône d'une clé ou d'un cadenas. L'endroit dépend alors du navigateur Internet que vous utilisez (parfois en 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 (internet Explorer, Netscape, Mozilla Firefox, Opera, …) 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, quel qu'en soit l'objet.
- Si vous recevez un courrier électronique semblant douteux et utilisant les coordonnées ou l'identité (logo, visuel…) de votre banque, prévenez-là au plus vite en lui faisant suivre ce 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 vos codes d'accès ou d'autres données personnelles.
- 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 « pharming »

Le «pharming» est une technique qui consiste à détourner l'accès à un site Internet vers un site pirate, via l'installation, à votre insu, d'un virus de type «Cheval de Troie» sur votre ordinateur. L'adresse que vous saisissez est correcte mais vous êtes redirigé sans le voir vers un faux site. Le pirate peut alors avoir accès à vos informations confidentielles.
Différentes versions de ce type de virus circulent actuellement sur Internet et touchent essentiellement les internautes utilisant le navigateur le plus répandu (Internet Explorer). Ce virus est reconnu par les principaux éditeurs d'antivirus. Aussi, pour vous prémunir contre d'éventuelles attaques, il est fortement recommandé de mettre à jour sans tarder et très régulièrement vos antivirus et de toujours vérifier que vous êtes bien dans l'espace sécurisé de votre banque.

- Munissez-vous d'une protection antivirus efficace intégrant les dernières mises à jour.
- Vérifiez régulièrement le certificat de sécurité : votre banque s'appuie sur un protocole de communication (généralement SSL 128 bits - Secure Socket Layer- qui est le chiffrement le plus élevé) pour chiffrer l'ensemble des informations échangées sur le site et permettre ainsi de garantir leur confidentialité et leur intégrité.

Vérifiez que vous êtes sur un site sécurisé en vous assurant que la lettre «s» (pour «secure») apparaît, après «http», dans la barre d'adresse de votre navigateur Internet. Un petit cadenas fermé ou l'icône d'une clé doit figurer dans la fenêtre de votre navigateur. Ceci confirme que le protocole SSL est utilisé pour sécuriser votre connexion.

Pour accéder au certificat en détails, le chemin à suivre dépend de votre navigateur, vous devez rechercher les informations de connexion sécurité Internet : par exemple menu Fichier > Propriétés > Connexion > certificats ou Outils > informations sur la page ...

- Choisissez un fournisseur d'accès Internet reconnu. Une sécurité maximale au niveau de votre fournisseur constitue la première ligne de défense contre le «pharming».
- Ne cliquez jamais directement sur un lien dans un message électronique ou une page web. «Copier/collez» ce lien dans une nouvelle fenêtre de navigation ou utilisez vos favoris.
- Vérifiez l'adresse de l'espace sécurisé dans la barre de navigation et assurez-vous que la session s'ouvre sur la véritable page du site.

Vous pouvez vérifier si votre ordinateur est infecté. En cas d'infection relevée par votre antivirus :

- N'effectuez aucune opération de banque à distance (connexion, virement, opposition...)
- Contactez le Centre de Relations Clientèle et demandez au conseiller de réinitialiser votre code d'accès Internet.
- Procédez à l'éradication du virus selon les prescriptions de votre éditeur antivirus.
- Assurez-vous que ces fichiers virus ont bien disparu en procédant à nouveau à la vérification de votre ordinateur par votre antivirus.
- Changez vos codes d'accès et mot de passe.

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 peut également installer des logiciels espions qui permettent de mémoriser et restituer (en différé ou en temps réel) toutes formes d'activités sur un ordinateur, par exemple des key-loggers ou screen-loggers qui peuvent enregistrer vos frappes au clavier (en particulier vos identifiant et mot de passe) pour les envoyer ensuite à un serveur pirate qui crée un fichier d'identifiants / mots de passe. Le cheval de Troie 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.
- 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,

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.

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 antivirus 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.
Ainsi, à 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.

Les risques liés aux téléphones portables et assistants personnels

Si vous consultez le site de votre banque ou effectuez des achats sur Internet par le biais de votre téléphone portable ou de votre assistant personnel, celui-ci peut être infecté par un virus …

De plus en plus de téléphones permettent la consultation de sites Internet et notamment les sites des banques. La plupart des téléphones sont désormais équipés de la technologie « bluetooth » qui, par des réseaux sans fils d'une faible portée, permet de relier des appareils entre eux sans liaison filaire. (soit ordinateurs entre eux, soit téléphones entre eux, soit ordinateur avec téléphone…)

On peut ainsi transmettre des données entre des équipements, sur un rayon de l'ordre d'une dizaine de mètres à un peu moins d'une centaine de mètres. Comme dans tout système récent, il existe des failles de sécurité qui peuvent permettre à des pirates de prendre le contrôle de votre téléphone.

Par défaut, les paramètres de votre téléphone autorisent par exemple la communication avec tous les autres appareils. Pour éviter qu'un virus se propage sur votre téléphone, vous devez au moins paramétrer votre bluetooth en mode masqué. D'une manière générale, n'activez la fonction Bluetooth que lorsque c'est nécessaire.

Le nombre de virus concernant les téléphones portables et assistants personnels, encore peu nombreux, risquent de se développer. En téléchargeant des fichiers (Musique MP3, vidéos, etc.) vous risquez de télécharger également des virus. Vous devez équiper votre téléphone portable et/ou votre assistant personnel d'un antivirus adapté et le mettre à jour régulièrement.

Evitez d'utiliser un équipement (celui d'un ami par exemple) dont vous ne maîtrisez pas le niveau de sécurité.

Si vous recevez un SMS vous demandant d'appeler un numéro, de vous connecter à un site (depuis votre téléphone) ou de saisir vos codes, n'y répondez surtout pas et n'appelez pas. Informez votre conseiller clientèle au plus vite.

Les risques liés aux réseaux Wi-Fi

Si votre ordinateur est connecté à Internet par un réseau Wi-Fi, vous risquez :
- l'interception de données : Ecoute 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 : Emission par un tiers de signaux radio, destinés à produire des interférences.

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.
- 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.

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…).
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…).

ACHAT À DISTANCE PAR INTERNET

Le paiement par chèque

Vous risquez de recevoir en paiment un faux chèque ou encore un chèque falsifié.

Voir page 7 les conseils donnés quant au «chèque reçu».

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 fermé, ou l'icône d'une clé, apparaît dans la fenêtre du navigateur ; l'endroit dépend du navigateur utilisé parfois 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 sur votre ordinateur ou sur votre téléphone portable 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.
Vous recevez un SMS sur votre téléphone portable qui prétend que vous avez gagné un prix et vous invite à rappeler un numéro, où vous donnerez vos coordonnées bancaires, afin que le prix puisse être viré (parfois pour déposer un chèque) sur votre compte. Voir *« quelques pièges à éviter »* (page 22).

Soyez sur vos gardes !

- Si une offre est trop alléchante, c'est sans doute une arnaque. Elle peut émaner d'un faux commerçant et/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

- Evitez 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 votre 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 évidemment 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 procédez à un nouveau règlement pour éteindre votre dette et demandez au bénéficiaire de vous donner une lettre de désistement.

Le pointage des facturettes 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.
- A 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

CHÉQUIER

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 € par mn).

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 de chèques 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 auprès de la police pourra vous être demandé.

BON À SAVOIR

Après un règlement par carte, 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.

■ Evitez de le recopier ou de conserver le document portant le numéro, cherchez plutôt à le mémoriser.

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 vos codes d'accès (identifiant et mot de passe)

Vous ne pouvez pas accéder au service mais vos codes ne peuvent pas être utilisés 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 vos codes d'accès à la banque à distance

Vous risquez leur usage par un tiers

■ Si votre antivirus a détecté un virus, un cheval de Troie ou un ver, n'effectuez aucune opération de banque à distance. Procédez à leur éradication en respectant les prescriptions de l'éditeur de votre antivirus. Effectuez une nouvelle vérification, puis changez vos codes d'accès de banque en ligne.

■ 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 mot de passe, puis vérifiez que les dernières opérations enregistrées sont correctes.

■ Signalez l'incident à votre banque, mais vous n'avez jamais à lui communiquer votre mot de passe qui ne doit être connu que de vous.

Annexe 1

Quelques pièges à éviter

Piège 1 - « L'acquéreur … généreux »

Les circonstances

Vous vendez un bien à un certain prix. L'acquéreur vous propose un prix supérieur. 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 supplémentaire (transport par exemple) et donc de lui rembourser la différence entre le prix d'origine du bien et le montant total qu'il vous a déjà payé, soit sous forme de virement sur un compte de tiers, soit sous forme de transfert d'espèces à un tiers.

Où est le piège ?

Le chèque, faux, reviendra impayé, vous garderez votre bien mais vous aurez perdu le remboursement de la différence.

D'ailleurs un chèque personnel (par opposition au chèque de banque) 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).

Piège 2 - « Vous recevez un chèque en paiement en croyant que le crédit au compte provient d'un virement »

Les circonstances

Vous vendez un bien. L'acquéreur vous demande vos coordonnées bancaires pour vous faire un virement. Votre compte a bien été crédité, non par virement comme prévu, mais par un dépôt de chèque, et au vu du crédit vous livrez la marchandise (un véhicule par exemple).Quelques jours plus tard, votre compte est débité de ce montant.

Où est le piège ?

Le chèque déposé s'avère être un faux chèque, il a donc été rejeté. Votre compte est débité.

Piège 3 - « L'arnaque au chèque de banque »

Les circonstances

Vous vendez un bien. L'acquéreur vous propose de payer par chèque de banque, moyen de paiement garanti puisque c'est la banque qui émet ce type de chèque. 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 va revenir impayé.

Où est le piège ?

Le chèque de banque était un faux chèque. Et le numéro de téléphone inscrit sur le chèque était celui d'un complice. Pour vérifier la validité du chèque de banque, vous devez contacter la banque en cherchant le numéro dans l'annuaire ou encore mieux, en vous rendant à l'agence bancaire.

Piège 4 - Etre recruté comme « mule »

Les circonstances

Vous recevez un e-mail 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).

Où est le piège ?

Il vous sera demandé de recevoir sur votre compte une somme d'argent d'un certain montant que vous devrez transférer ensuite sur un autre compte qu'on vous indiquera, moyennant rémunération pour ce « travail ». Une fois les fonds reçus en effet, vous effectuez un virement d'un montant moindre (c'est-à-dire diminué du montant de votre « rémunération ») vers le compte dont les coordonnées vous ont été communiquées.

Par ce transit d'argent, l'escroc « blanchit » l'argent sale qui provient en général d'un trafic quelconque ou du moins le transfère dans un autre pays. Passer par une mule rend plus difficile la détection de la fraude et la récupération des fonds.

En tant que « mule », vous risquez d'être reconnu complice d'une fraude passible de poursuites judiciaires.

Annexe 2

La sécurité en vacances

Avant de partir

La réservation

Lorsque le paiement de vos réservations n'est pas possible par carte, pensez au 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 si vous fournissez les codes BIC et IBAN du destinataire.

Les contacts utiles

Vérifiez que vous saurez comment joindre votre banque en cas de problème, ainsi que les contacts des services d'assistance que vous permet l'utilisation de certains moyens de paiement. Notez les numéros de téléphone et adresses dans un endroit sécurisé, en dehors de votre portefeuille.

Pour le chèque

Notez à part les numéros de formule de chèque, ils vous seront demandés si vous faites opposition.

- Notez le numéro du Centre national d'appel des chèques perdus ou volés : **0 892 683 208** (0,337 € la minute). Si la banque est fermée, cet organisme enregistrera votre opposition pendant 48 heures, le temps que vous confirmiez auprès de votre agence.
- Notez également les numéros des chèques de voyage que vous emmenez pour faire opposition plus facilement en cas de besoin, ainsi que le numéro de téléphone à contacter.

Pour la carte

- Chaque banque a son propre centre d'opposition. A défaut, vous pouvez appeler le numéro spécial interbancaire **0 892 705 705** (0,34€ /mn), serveur vocal interactif, qui oriente chaque appel vers le centre d'opposition compétent. Il faut également noter le numéro à 16 chiffres qui figure sur la carte. Depuis l'étranger, vous pouvez faire opposition en appelant le numéro figurant sur les distributeurs des réseaux Visa et Eurocard Mastercard.

Sur place

Le paiement par chèque

Payer par chèque à l'étranger est vivement déconseillé, même dans la zone euro. Les chèques sont très rarement acceptés à l'étranger, et cette opération entraîne des frais non négligeables.

Pensez plutôt aux chèques de voyage. Ils sont remboursés en cas de vol ou de perte, et sont largement acceptés. Notez séparément les numéros de chèque pour faire opposition plus facilement en cas de besoin, ainsi que le numéro de téléphone à contacter.

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.

Les retraits au distributeur

Soyez vigilant lorsque vous tapez votre code et veillez à ce que personne ne puisse repérer 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 avant utilisation de l'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 découvrir.
- 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 en cas d'anomalie.

Mémo : les numéros utiles

A emmener et à conserver séparément des moyens de paiement

Numéro de téléphone de l'agence bancaire : ……..
Numéro de téléphone du service d'assistance : ……

Cartes
Numéro de téléphone pour faire opposition en France : ……....
Numéro de téléphone pour faire opposition à l'étranger : ……....
Numéro à 16 chiffres de la carte : ….……..
Date d'échéance de la carte : ……..……

Chèques *(uniquement pour la France)*
Numéro de téléphone pour faire opposition : ……
Fourni par la banque. A défaut, appeler le 08 92 68 32 08 (Centre national des chèques perdus ou volés)

Numéros des chèques emportés :
De …… **à** ……..……..
……..... ...……..

Chèques de voyage *(pour l'étranger)*
Numéro de téléphone pour faire opposition : .....……..……
Fourni par la banque.

Numéros des chèques emportés :
De …… **à** ……..……..
……..... ...……..

DÉJÀ PARUS DANS CETTE COLLECTION

Les hors-séries

- Le Guide de la mobilité
- Sécurité des opérations bancaires
- Glossaire des opérations bancaires courantes
- Envoyer de l'argent à l'étranger (uniquement en version électronique)
- La commercialisation des instruments financiers

Les numéros non-indiqués, périmés, ne sont pas réédités