OFFERT PAR
AXA Banque

PETIT e-GUIDE PRATIQUE DE LA PROTECTION DES DONNÉES BANCAIRES

SOMMAIRE

EDITO

Dans le monde contemporain, chacun utilise régulièrement services en ligne et applications mobiles, y compris dans le domaine bancaire. Votre banque vous permet d'effectuer vos opérations quand vous le souhaitez, quel que soit le lieu où vous vous trouvez, aussi simplement et rapidement que possible… et en toute sécurité.

Cette dernière exigence est particulièrement critique car ces nouvelles facilités d'accès à distance sont aussi les moyens qu'utilisent les *hackers* pour commettre leurs méfaits. Savez-vous, par exemple, que la fraude sur les cartes bancaires, en constante augmentation depuis 2005, a atteint plus de 450 millions d'euros en 2012[1], dont l'essentiel sur internet ? Naturellement, votre banque met tout en œuvre afin de garantir que votre argent, ainsi que toutes les informations qui vous concernent, restent en permanence à l'abri des fraudeurs et autres « cybercriminels », dont l'actualité nous expose régulièrement les tristes exploits.

Cependant, comme dans toutes les circonstances dans lesquelles la sécurité est en cause, vous aussi avez un rôle important à jouer : il ne vous viendrait pas à l'idée de quitter votre domicile sans en fermer les portes et les fenêtres même si vous avez une bonne assurance, pourquoi laisseriez-vous les « clés » de vos comptes bancaires sur leur « entrée » virtuelle ?

Car aujourd'hui, vos moyens de paiement (chèques, cartes…), votre accès internet, votre téléphone portable… sont comme les « clés » de vos finances personnelles. Elles requièrent votre vigilance pour ne pas tomber entre de « mauvaises » mains et elles méritent donc certainement que vous lisiez les quelques pages qui suivent.

En effet, AXA Banque vous offre ce guide pour vous rappeler quelques bonnes pratiques, parfois oubliées, et vous donner quelques recommandations complémentaires, faciles à appliquer, pour encore mieux vous protéger contre les menaces qui évoluent sans cesse.

Vous y retrouverez, sous un format clair et synthétique, tous les conseils utiles – connus et moins connus – qui permettront d'assurer une sécurité optimale à votre argent : ne jamais noter vos mots de passe, masquer le code de vérification au dos de votre carte bancaire, éviter de saisir vos codes secrets dans les lieux publics…

Cet e-guide a été conçu pour vous. Les équipes d'AXA Banque et moi-même espérons sincèrement qu'il répondra à vos interrogations sur la protection de vos comptes bancaires. Si, malgré tout, vous aviez encore des questions ou des doutes sur la sécurité, n'hésitez pas : contactez votre conseiller !

Patrice BERNARD
Consultant Innovation, Technologies et Sécurité pour Conix

1. Rapport 2012 de l'Observatoire de la Sécurité des Cartes de Paiement :
http://www.banque-france.fr/observatoire/rap_act_fr_12.htm

COMME DANS TOUTES LES CIRCONSTANCES DANS LESQUELLES LA SÉCURITÉ EST EN CAUSE, VOUS AUSSI AVEZ UN RÔLE IMPORTANT À JOUER

INTRODUCTION

En matière bancaire comme dans tous les domaines, la sécurité et la vigilance sont primordiales.

Des systèmes de protection sont mis en place par votre banque mais vous êtes également responsable de vos données bancaires et des moyens de paiement qui sont mis à votre disposition.

Cette vigilance est requise au quotidien, que ce soit sur Internet, sur votre téléphone, dans la rue, chez votre commerçant ou à l'étranger.

Les informations que vous devez protéger sont toutes les données à caractère confidentiel, à savoir :

- **vos données personnelles :** nom, adresse, numéro de téléphone, date et lieu de naissance
- **vos données bancaires :** identifiants, codes d'accès, mot de passe, numéros de compte, état de vos comptes...
- **vos moyens de paiement :** numéros de carte bancaire, cryptogramme, chéquiers...

LE SAVIEZ-VOUS ?

En 2011, **650 000** ménages victimes d'au moins un débit frauduleux sur son compte bancaire*

En France, Internet représente **33 %** de la fraude et seulement **5 %** des paiements*

** Source : Enquête de l'Observatoire National de la Délinquance et des Réponses Pénales*

EN MATIÈRE BANCAIRE COMME DANS TOUS LES DOMAINES, LA SÉCURITÉ ET LA VIGILANCE SONT PRIMORDIALES

FICHE 1 **AU QUOTIDIEN**

1 LES CONSEILS ÉLÉMENTAIRES DE PRUDENCE

DONNÉES BANCAIRES

- Ne communiquez jamais vos codes d'accès à vos comptes bancaires, pensez aussi à changer régulièrement de mot de passe. Évitez les codes trop simples et pensez à vous déconnecter du site de votre banque à chaque fin d'utilisation.
- Vérifiez régulièrement et attentivement vos relevés de compte : sur votre compte, ce sont souvent des opérations autour de 10 € qui peuvent passer inaperçues.
- Déchirez en petits morceaux les courriers de votre banque avant de les jeter dans deux poubelles différentes pour éviter les usurpations d'identité.

CHÉQUIER

Préférez le stylo-bille pour rédiger vos chèques. Commencez bien à les remplir au début de chaque ligne pour que rien ne puisse être ajouté avant. Pensez à compléter les lignes d'un trait pour que rien ne puisse être ajouté après.

CARTE BANCAIRE

Ne prêtez pas votre carte bancaire, ne divulguez jamais votre code et tapez-le de façon discrète lors de vos achats.

Faites opposition rapidement lorsque la carte a été avalée par un distributeur de billets et que vous ne pouvez pas la récupérer directement au guichet de l'agence.

Si vous avez égaré ou que vous vous êtes fait voler votre carte bancaire, n'attendez pas pour le déclarer. Même si la personne ne connaît pas le code, cela ne l'empêchera pas de faire des achats sur Internet.

Et **apprenez votre cryptogramme par cœur** (3 derniers chiffres présents au dos d'une carte de paiement) puis coller une gommette sur ces chiffres pour éviter qu'un tiers (commerçant ou autre) ne puisse les capter et utiliser votre carte à votre insu pour des paiements à distance (internet ou téléphone).

LE SAVIEZ-VOUS ?

Fraude moyenne **130 €**

(Source : Observatoire de la sécurité des cartes de paiement 2011)

DES PRÉCAU-TIONS DE BASE ET DES GESTES SIMPLES CONSTITUENT UNE BONNE PROTECTION

2 L'USURPATION D'IDENTITÉ

Pour usurper une identité, les fraudeurs vont récupérer les coordonnées d'une personne dans les poubelles, les boîtes aux lettres, sur les réseaux sociaux... À partir de ces informations, le fraudeur prend alors votre identité. Il peut ainsi contracter des crédits, ouvrir un compte de dépôt...

LE SAVIEZ-VOUS ?

L'usurpation d'identité touche environ **213 000** personnes par an.
Le coût moyen d'une usurpation d'identité s'élève à **2 229 €**.
(Source : CREDOC)

3 LE PIRATAGE À LA CARTE BANCAIRE

Le piratage de carte bancaire peut avoir lieu au distributeur, sur internet ou chez un commerçant.

Contrefaçon de carte bancaire par la technique du *skimming* qui consiste à équiper un distributeur d'une fente d'insertion modifiée. Cela permet de copier les informations de la bande magnétique à l'insu de l'utilisateur. Les données récupérées permettent ensuite de fabriquer un double de la carte réelle.

Modification du montant de l'achat : c'est une fraude qui peut être évitée facilement. Il vous suffit de bien vérifier le montant inscrit sur le terminal de paiement.

Récupération du numéro de carte bancaire : bien vérifier que lors d'une transaction avec un commerçant, ce dernier vous remet la facture avec votre numéro de compte complet. Le commerçant conserve le ticket avec le numéro de compte incomplet.

LE SAVIEZ-VOUS ?

Le montant moyen d'une fraude à la carte bleue sur internet est de **297 €**.
(Source : FIA-NET)

En 2012, plus de **1 100** distributeurs ont été piratés contre 634 en 2011.
(Source : Observatoire de la sécurité des cartes de paiement - 2012)

LE PIRATAGE DE CARTE BANCAIRE PEUT AVOIR LIEU AU DISTRIBUTEUR, SUR INTERNET OU CHEZ UN COMMERÇANT

FICHE 2 SUR INTERNET

1 SUR INTERNET COMME AU QUOTIDIEN, LA VIGILANCE EST DE MISE

Sur les sites internet des banques, tout est mis en œuvre pour vous garantir une sécurité maximale.

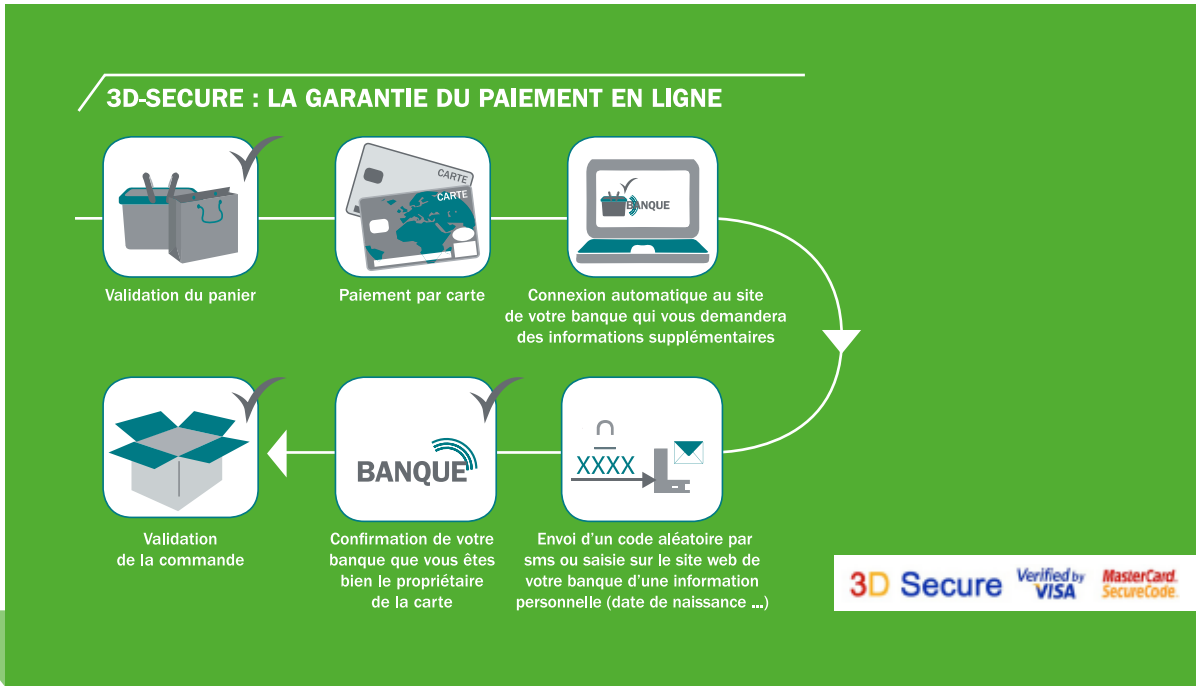
Néanmoins, les arnaques et autres moyens de récupérer les informations personnelles et confidentielles se multiplient.

2 LES PRÉCAUTIONS PRÉALABLES AVANT D'EFFECTUER UN PAIEMENT SUR INTERNET

Limitez-vous au site à forte notoriété. D'une manière générale, ne faites aucune opération sur un ordinateur non protégé par un anti virus et évitez les sites dont vous n'avez jamais entendu parler.

Prenez le temps de vérifier le sérieux du commerçant, entrez vous-même l'adresse du site au lieu de cliquer sur le lien d'un email non sollicité. **Et vérifiez que l'URL du site commence par «https» et qu'un cadenas est présent en bas de la fenêtre.**

Privilégiez les sites internet ayant la norme **3D Secure**.



PRENEZ LE TEMPS DE VÉRIFIER LE SÉRIEUX DU COMMERÇANT, ENTREZ VOUS-MÊME L'ADRESSE DU SITE AU LIEU DE CLIQUER SUR LE LIEN D'UN EMAIL NON SOLLICITÉ

3 LES CONSEILS À RESPECTER LORSQUE VOUS VOUS CONNECTEZ AU SITE INTERNET DE VOTRE BANQUE

Ne vous connectez jamais aux services en ligne de votre banque via un **réseau wi-fi ouvert ou public**. Une personne mal intentionnée peut récupérer vos données et se connecter à votre compte. Dans ce cas, il est plus difficile de prouver qu'il s'agit d'une fraude.

Ne répondez jamais à une demande d'informations bancaires **par mail, SMS ou sur un site internet**. Une banque contacte généralement ses clients par courrier. Si vous avez un doute, n'hésitez pas à contacter votre conseiller bancaire.

Si une fenêtre s'ouvre pendant que vous êtes connecté à votre banque, ne cliquez jamais sur un lien proposé. Il vous suffit de la fermer. Si vous acceptez une action, cela peut être un moyen d'accéder à vos données bancaires.

Ne renseignez jamais vos données bancaires sur des **réseaux sociaux** ou tout autre média qui est accessible à tous.

Ne mettez jamais votre date de naissance ou celles de vos enfants en **mot de passe ou code secret**, que ce soit pour vos applications ou votre code de carte bancaire. Préférez un mot de passe qui n'ait aucun lien avec votre identité.

4 ZOOM SUR LE PHISHING

QU'EST-CE QUE LE PHISHING ?

Le *phishing*, ou « hameçonnage », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations bancaires auprès d'internautes.

Cela consiste à faire croire à la victime que sa banque ou une administration de confiance lui demande par email de rentrer son mot de passe, numéro de carte de crédit, date de naissance… pour une fausse raison.

COMMENT S'EN PRÉMUNIR ?

Evitez de cliquer sur les liens contenus dans les courriers électroniques : ils peuvent en réalité diriger les internautes vers des sites frauduleux. En cas de doute, il est préférable de saisir manuellement l'adresse dans le navigateur.

Préférez saisir vos informations personnelles (coordonnées bancaires, identifiants…) sur des sites internet sécurisés : un cadenas apparaît dans le navigateur et l'adresse du site commence par https au lieu de http.

COMMENT LE SIGNALER AUX AUTORITÉS COMPÉTENTES ?

Si vous pensez avoir été victime d'une escroquerie par *phishing*, signalez le immédiatement à **www.internet-signalement.gouv.fr** et prenez contact avec votre banque.

Vous pouvez également signaler les sites de phishing afin qu'ils soient bloqués en vous rendant sur le site de Phishing Initiative : **www.phishing-initiative.com**

NE RÉPONDEZ JAMAIS À UNE DEMANDE D'INFORMATIONS BANCAIRES PAR MAIL, SMS OU SUR UN SITE INTERNET

FICHE 3 SUR SMARTPHONE

1 PROFITER DE SON MOBILE EN TOUTE SÉCURITÉ

Il est très pratique de pouvoir consulter ses comptes ou d'effectuer ses virements directement sur son téléphone. Mais il faut avoir conscience des risques pour bien sécuriser vos données personnelles et bancaires.

Heureusement, il existe des astuces simples pour protéger efficacement son contenu :

- Ne prêtez pas votre téléphone. S'il est perdu ou volé, contactez votre banque rapidement car il peut être utilisé comme élément de sécurité (3D Secure, validation d'opérations sensibles...).
- Protégez votre téléphone par un code PIN et mettez en place un verrouillage automatique, Éteignez le bluetooth s'il n'est pas utile.
- Ne stockez jamais de mot de passe (application bancaire, carte bancaire ou le code d'accès à votre site bancaire).

Attention aux fausses applications mobiles bancaires : ne télécharger l'application de votre banque que sur les stores officiels, l'application doit être gratuite.

- Ne « jailbreakez » pas votre téléphone : cela réduit la sécurité notamment en autorisant l'installation d'applications non vali- dées par les marques de téléphone.
- Supprimez les SMS en provenance de votre banque après en avoir pris connaissance.
- Supprimez toutes les informations stockées sur votre téléphone avant de le revendre/recycler.

LE SAVIEZ-VOUS ?

1 jeune sur 2 stocke des informations bancaires ou codes confidentiels sur des appareils connectés. Et seulement la moitié les protège par un code de verrouillage. *(Source : TNS Sofres - AXA Prévention - 2014)*

IL EXISTE DES ASTUCES SIMPLES POUR PROTÉGER EFFICACEMENT LE CONTENU DE VOTRE SMARTPHONE

2 PRÉFÉREZ LES APPLICATIONS MOBILES

Sur votre téléphone mobile ou sur votre tablette, vous pouvez accéder à vos services bancaires comme sur votre ordinateur, en ouvrant le navigateur web intégré sur le site AXA Banque. Pour plus de sécurité, nous vous recommandons plutôt de **télécharger l'application gratuite** que votre banque met à votre disposition sur l'App Store ou le Google Play de votre système.

3 QUELLES APPLICATIONS INSTALLER ?

Le marché d'applications de votre smartphone comporte des milliers de titres différents, parmi lesquels se cachent quelques logiciels dangereux, prenant souvent l'apparence d'outils de sécurité ou arborant un logo connu. Ne vous laissez pas tromper ! Avant d'installer une application sur votre téléphone, prenez soin de **vérifier qu'elle est bien publiée par une entreprise de confiance.**

Pour télécharger l'application de votre banque, par exemple, utilisez de préférence les liens proposés sur son site web.

4 UTILISER LES SERVICES BANCAIRES DANS LES LIEUX PUBLICS

La banque sur son téléphone, c'est pratique : on peut y accéder partout et à tout moment ! Mais il faut tout de même rester prudent. Ainsi, **évitez de saisir vos codes secrets (de banque ou autres) dans les lieux publics** : une personne indélicate est peut-être en train de vous épier à votre insu !

5 LES MENACES « MOBILES »

L'explosion des applications mobiles est un phénomène très récent mais il attire déjà les malfaiteurs en tout genre et les logiciels malveillants se répandent rapidement. Face à ces risques, méfiez-vous des messages (SMS ou e-mail) venant d'inconnus, évitez d'installer des applications d'origine incertaine aux promesses alléchantes… **En un mot, restez toujours vigilant !**

6 VEILLEZ SUR LA SANTÉ DE VOS APPAREILS

Chaque jour, de nouvelles failles de sécurité sont découvertes dans les logiciels qui équipent nos micro-ordinateurs, nos téléphones et nos tablettes. Chacune d'elle peut permettre à des individus sans scrupule d'accéder à nos informations les plus sensibles, dont nos comptes bancaires. Afin d'éviter cette menace, pensez à **appliquer rapidement les mises à jour** qui vous sont proposées : ce geste simple suffit souvent à éviter les fraudes !

POUR TÉLÉCHARGER L'APPLICATION DE VOTRE BANQUE, PAR EXEMPLE, UTILISEZ DE PRÉFÉRENCE LES LIENS PROPOSÉS SUR SON SITE WEB

FICHE 4 À L'ÉTRANGER

1 PRENEZ QUELQUES PRÉCAUTIONS POUR PARTIR À L'ÉTRANGER L'ESPRIT LÉGER

Avant de vous rendre à l'étranger, prenez contact avec votre banque afin de connaître **les précautions et les protections possibles à activer.**

Pensez à vérifier la validité de votre carte bancaire ainsi que les clauses de votre contrat (plafond hebdomadaire et journalier des retraits et paiements) pour ne pas avoir de mauvaise surprise lorsque vous serez en voyage.

Informez-vous sur l'existence de distributeurs automatiques de billets dans le pays concerné ainsi que sur les possibilités de paiement par carte bancaire.

Renseignez-vous afin de connaître les **numéros de téléphone internationaux** de mise en opposition de votre carte bancaire.

AVANT DE VOUS RENDRE À L'ÉTRANGER, PRENEZ CONTACT AVEC VOTRE BANQUE

FICHE 5 LES JEUNES ET LES RISQUES BANCAIRES

DES JEUNES QUI SE CONSIDÈRENT TRÈS MAJORITAIREMENT VIGILANTS

Disent **faire attention** à la protection de leurs…

… données personnelles et bancaires
86 %

… moyens de paiement
85 %

… données bancaires sur leurs appareils connectés
84 %

NÉANMOINS, DANS LES FAITS, DES COMPORTEMENTS À RISQUE

Lors d'un paiement en ligne,

nombreux sont ceux qui **ne vérifient pas** si…

https://

… l'adresse du site commence par **https**
21 %

3D Secure

… le site internet possède la norme **3D Secure**
39 %

Dans les choix de mots de passe…

56 %
utilisent le ou les **mêmes mots de passe** pour plusieurs sites, plusieurs accès

31 %
n'alternent pas minuscules, majuscules, lettres, chiffres et symboles

29 %
choisissent un mot de passe **en lien avec leur identité**

Dans le stockage des données…

1 jeune sur 4
Stocke des informations bancaires ou ses codes confidentiels sur un appareil connecté

dont seulement
54 %
le protègent par un code de vérouillage

Sur la connexion wifi…

26 %
des 19-24 ans se sont déjà connectés à l'appli de leur banque via un réseau WIFI non protégé

Source : TNS Sofres / AXA prévention - janvier 2014.

AXA BANQUE S'ENGAGE POUR LES JEUNES !

LES JEUNES ET L'ARGENT
un engagement AXA Banque

Découvrez notre programme solidaire et responsable : accompagner les jeunes dans leur éducation budgétaire

LES JEUNES SE CONSIDÈRENT VIGILANTS, POURTANT IL EXISTE DES COMPORTEMENTS À RISQUE

GLOSSAIRE

Cryptogramme
Série unique de trois chiffres imprimée au dos des cartes bancaires Visa et MasterCard.

Jailbreaker (ou desimlockage)
Ajout de données supplémentaires dans l'iPhone qui permet l'accès à un centre de téléchargement d'applications développées par des personnes non-affiliées à Apple.

Phishing (ou hameçonnage)
Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but d'usurper une identité. Dans la pratique, les fraudeurs envoient un e-mail en se faisant passer pour une instance importante (une banque, le plus souvent) et demande la confirmation des coordonnées bancaires pour ensuite pirater le compte de la victime.

Skimming
Technique de piratage d'un distributeur de billet qui permet de copier les informations de la bande magnétique d'une carte bancaire et de les recopier sur une carte vierge.

Usurpation d'identité
Le fait de prendre délibérément l'identité d'une personne dans le but de réaliser des actions frauduleuses, commerciales, civiles ou pénales.

3D Secure
Système pour éviter les paiements frauduleux par carte bancaire sans présence réelle de la carte. Dans la pratique, après avoir communiqué les données habituelles de votre carte bancaire (numéro, validité et cryptogramme), vous serez redirigé vers le site de votre banque qui vous demandera des informations supplémentaires. Une fois les informations fournies, vous reviendrez sur le site du commerçant qui vous confirmera le paiement.

Guide rédigé en partenariat avec AXA Prévention, Association loi 1901
313 Terrasses de l'Arche 92727 Nanterre Cedex

AXA prévention
La prévention responsable

www.axaprevention.fr

CONTACTS UTILES

En cas de perte, de vol ou d'utilisation frauduleuse de votre carte bancaire, vous devez **très rapidement faire opposition** pour que les paiements ultérieurs soient bloqués.

Appelez dans les meilleurs délais le Centre d'Opposition (ouvert 7j/7, 24h/24) ainsi que votre banque.

- **Centre d'opposition : 0 892 705 705**
- **De l'étranger : +33 442 605 303**

AXA BANQUE,
LA BANQUE MULTI-ACCÈS

Pas encore client : 36 41
(numéro gratuit depuis un poste fixe)

Des agences & conseillers AXA,
proches de chez vous

Déjà client : 0970 808 088 (GRATUIT*)
***Hors coût de votre forfait mobile ou fixe / numéro non surtaxé**

Sur Internet : www.axabanque.fr

Applications & site mobile
iPhone, iPad, Blackberry, Android

Sur les réseaux sociaux :
facebook, Twitter, Linkedin, YouTube

AXA BANQUE

réinventons / la banque