COMMISSION NATIONALE
DE L'INFORMATIQUE
ET DES LIBERTÉS

OPERATION
AUDIT DE LA BANQUE EN LIGNE

Règles de bonnes pratiques pour les internautes et les professionnels

Les services de banque en ligne se sont considérablement développés. Ils permettent désormais aux particuliers de consulter leurs comptes bancaires, effectuer des virements, commander des chéquiers, simuler des propositions de crédit, etc.

Cette nouvelle manière d'envisager la relation bancaire n'est pas sans susciter de nouvelles interrogations de la part des internautes sur la protection de leurs données personnelles (sécurité des échanges d'information, collecte de nouvelles données, modalités d'information des personnes, prospection par voie électronique, etc.).

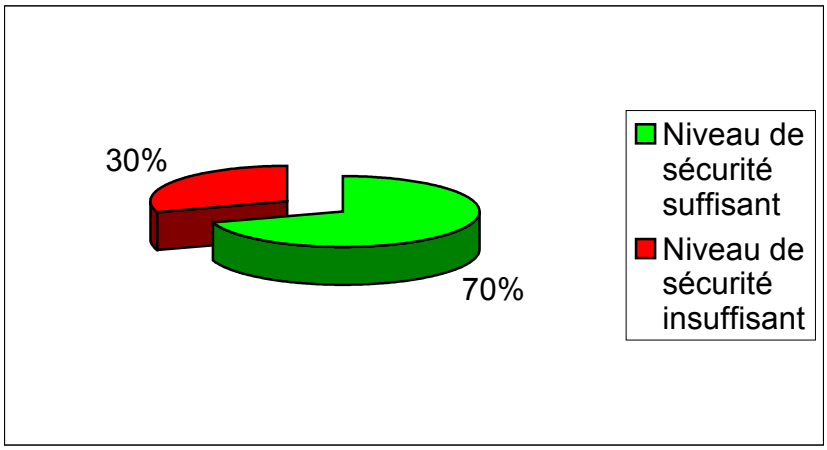
Au cours du 1er semestre 2005, la CNIL a par conséquent décidé de procéder à une série de missions de contrôle dans le secteur de la banque en ligne. Ces missions, effectuées auprès de 10 sites Internet bancaires, ont eu pour objet de vérifier le respect des dispositions de la loi « Informatique et Libertés » concernant les questions relatives à la sécurité et à la prospection commerciale.

Les contrôles ont été effectués sur la base de deux grilles d'audit de 64 questions au total portant sur la sécurité du site et les pratiques en matière de prospection commerciale. Ces contrôles ont consisté en un recensement et un dépouillement exhaustifs des réponses formulées par les banques, puis en une analyse comparative de ces réponses avec les documents techniques recueillis par la CNIL auprès de chaque organisme financier.

Ce document fait la synthèse, de façon anonymisée, des principaux résultats obtenus et enseignements tirés des contrôles diligentés par la CNIL. Des actions complémentaires sont actuellement menées auprès de certains établissements bancaires.

1-Les résultats de l'audit

Résultats « sécurité »



Sur les 10 sites contrôlés, la CNIL considère que 7 sites sur 10 respectent globalement la confidentialité et la sécurité des données (plus de 60% de réponses de ces établissements sont satisfaisantes au regard de la protection des données des clients), même si, dans certains cas, des améliorations permettraient d'augmenter le niveau de confidentialité et de sécurité des données.

Les 3 sites Internet restant présentent en revanche moins de 60 % de réponses satisfaisantes au regard de la protection des données des clients.

 Les points considérés comme satisfaisants par la CNIL

- Les internautes disposent, sur la plupart des sites, d'un bon niveau d'information : recommandations, aide en ligne, affichage du mode sécurisé ou du passage en mode sécurisé ;
- La sécurité relative à la « connexion » est globalement satisfaisante : protocole sécurisé (HTTPS), vérification possible de la date et de l'heure de la dernière connexion, déconnexion automatique après un délai de non utilisation ;
- Il existe pour l'internaute, le plus souvent, la possibilité de vérifier le bon déroulement des opérations bancaires effectuées par Internet, à l'écran ou par impression papier ;
- Enfin, si la quasi totalité des sites ne se réfère pas à des normes officielles de sécurité, nombreux sont ceux qui s'en inspirent.

 Les points considérés comme améliorables ou insuffisants

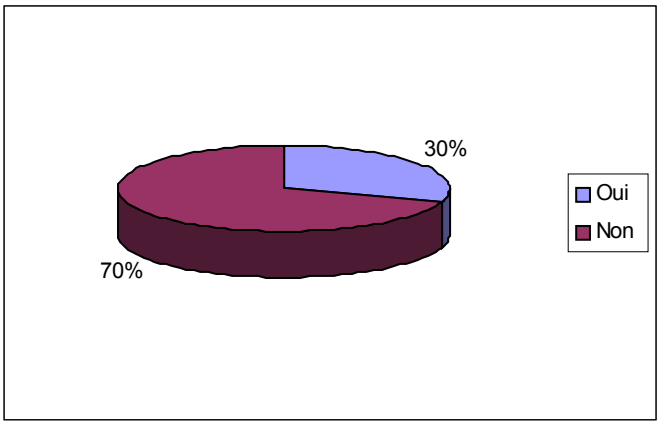
- Aucune authentification forte et incontestable des clients internautes n'est mise en œuvre, par exemple par carte à puce ou clé électronique unique. Seuls les identifiants et mot de passe ouvrent les portes des banques en ligne ;
- La gestion des cookies n'est satisfaisante (effacement après utilisation) que pour la moitié des sites audités ;

- Seule la moitié des sites effectuent une mise en garde concernant la question de la sécurité préalablement à la première connexion et disposent d'une aide en ligne permanente.

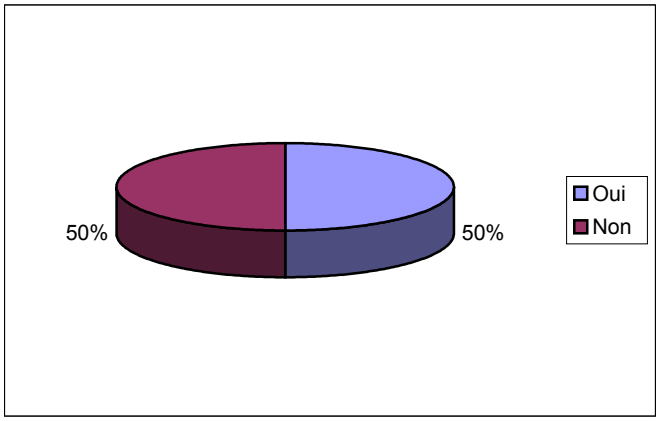
- S'agissant du mot de passe, il est rarement remis sous pli confidentiel ou envoyé en recommandé avec accusé de réception lorsqu'il est transmis par courrier postal. Il est souvent inférieur à 7 caractères alphanumériques et sa durée de validité est illimitée ;
- Quatre sites de banques en ligne ne sont pas en transaction sécurisée « https » lors de l'échange des identifiant et mot de passe, la bascule en mode sécurisé ne se faisant qu'après l'envoi de ces informations en clair sur le net ;
- Peu de sites permettent la consultation d'un historique des dernières connexions ou la réception d'un accusé de réception des opérations effectuées ;
- Enfin, la quasi totalité des sites n'offre pas la possibilité aux internautes :
    - de tester leur poste de travail (test du système d'exploitation, du navigateur, des cookies, etc.),
    - d'être informés des mises à jour régulières des règles de sécurité à suivre.

Principaux résultats « prospection commerciale »

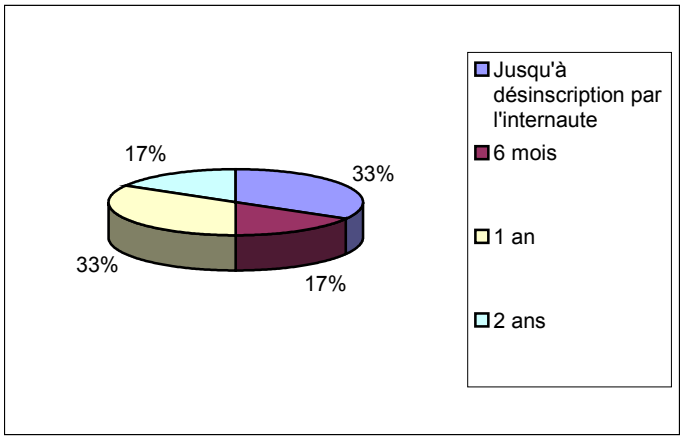
Les données collectées sur votre site font-elles l'objet d'une exploitation à des fins marketing ?



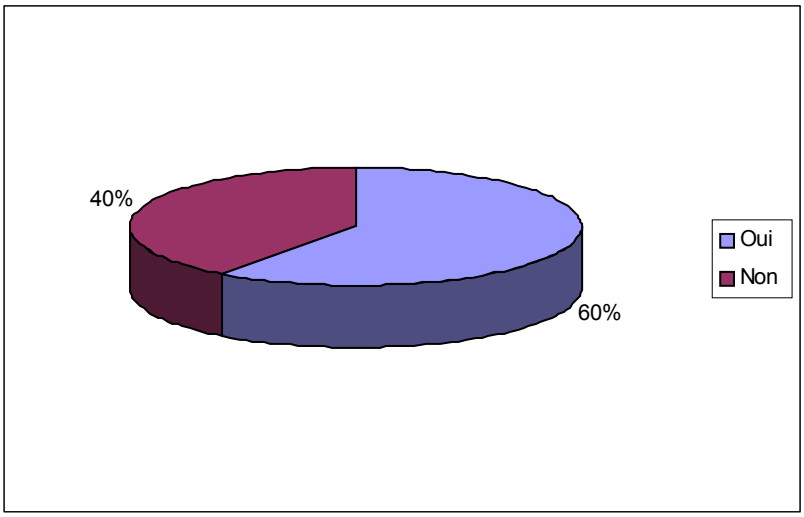
Est-ce que vous louez des fichiers externes auprès de sociétés spécialisées?



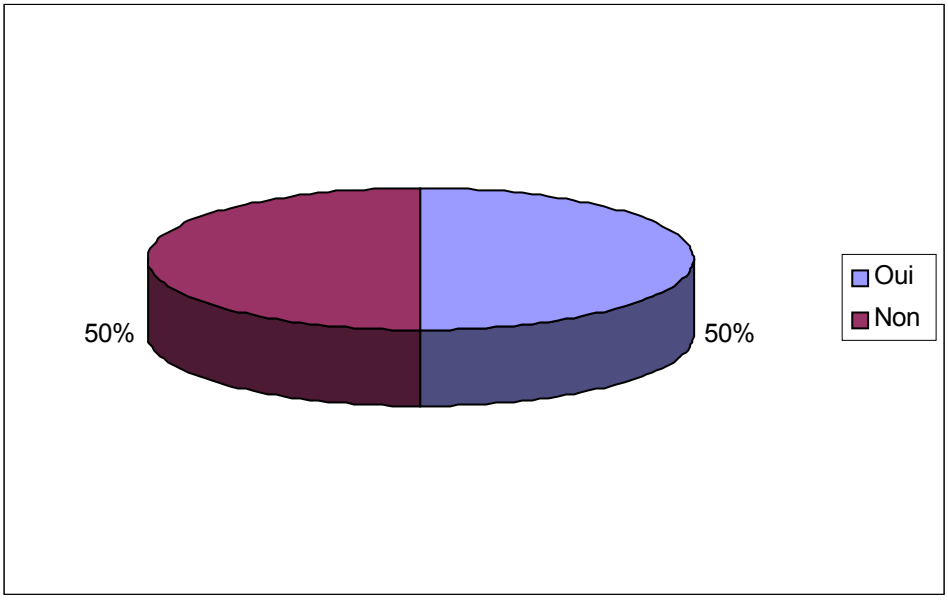
Pendant combien temps conservez-vous les informations relatives aux prospects ?



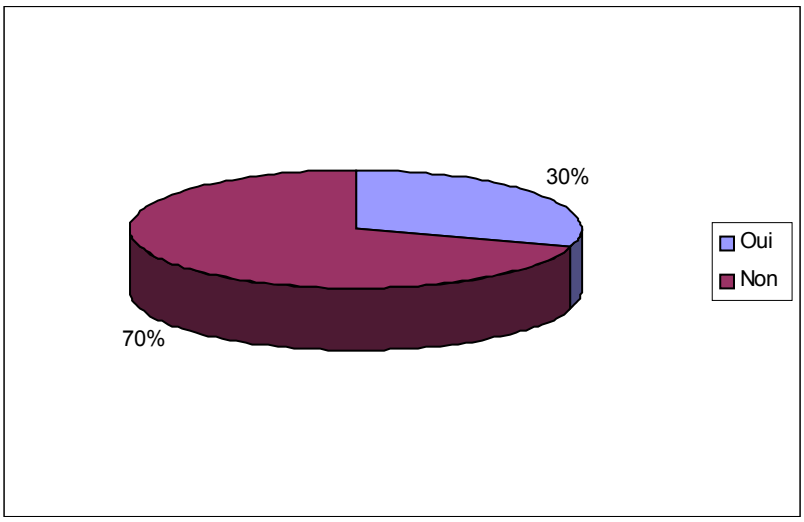
Avez-vous choisi d'appliquer le régime du consentement préalable (« opt-in » quel que soit le canal de prospection utilisé (prospection électronique ou non) ?



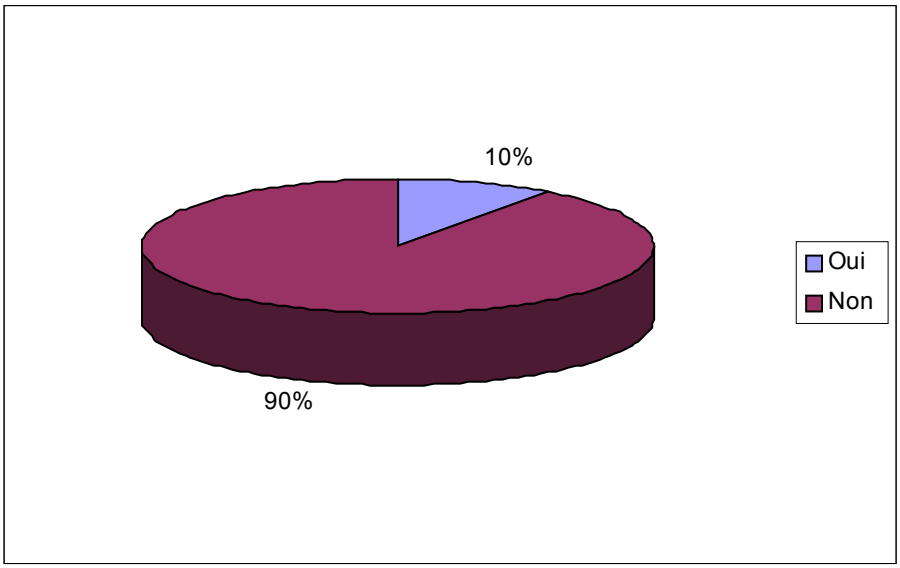
S'agissant de la prospection commerciale par courrier électronique, le consentement des personnes à recevoir de la prospection commerciale est-il formalisé par une case à cocher ?



Avez vous également soumis la prospection commerciale par courrier électronique sur des produits ou services analogues au régime de « l'opt in » ?



Le droit d'opposition à recevoir de la prospection commerciale (non électronique) peut-il s'exercer en ligne par le biais d'une case à cocher ?



Les points considérés comme satisfaisants par la CNIL :

- Dans 100 % des cas, il existe une mention relative à la loi « Informatique et libertés » sur les formulaires de collecte de données et dans les conditions générales d'utilisation ;
- Hormis les cas où il existe un dispositif de désinscription en ligne par l'internaute lui-même, les données relatives aux prospects ne sont jamais conservées plus de deux ans ;
- 60 % des sites ont choisi d'appliquer le régime de « l'opt-in » (i.e. : consentement de la personne à recevoir des informations à caractère commercial) à tous les canaux de prospection utilisés (prospection électronique ou non) ;
- Dans 30 % des cas, les banques déclarent également soumettre au régime de « l'opt-in » la prospection commerciale par courrier électronique sur des « produits ou services analogues ». Ce résultat est satisfaisant mais aucune banque n'a été en mesure de communiquer à la CNIL une définition précise de la notion de « produits ou services analogues ».

Les points considérés comme insuffisants :

- Dans 90% des cas, le droit d'opposition à recevoir de la prospection par courrier postal ne peut pas s'exercer en ligne ;
- Dans 50 % des cas, les sites ont formalisé le consentement des clients / prospects à recevoir de la prospection commerciale par une case à cocher. Bien que la case à cocher ne soit pas le seul moyen de recueillir le consentement des personnes de façon satisfaisante (d'autres techniques existent telles que des menus déroulants par exemple), aucune banque n'a évoqué d'autres techniques de recueil du consentement.

2- Les enseignements de l'audit

1- Réserver une place importante à la sensibilisation des utilisateurs aux principes de sécurité

Une meilleure sensibilisation et information des utilisateurs sur les moyens de préserver la sécurité et la confidentialité des informations lorsqu'ils effectuent des opérations bancaires à distance pourraient être opérées. Il pourrait s'agir, par exemple, de :

- n'autoriser l'internaute à utiliser les fonctionnalités offertes par le site qu'après avoir pris connaissance des mesures de sécurité, en validant lors de sa première connexion une case d'acceptation des modalités d'accès aux services de banque à domicile ;
- donner accès à une page d'information sur la sécurité depuis chaque page du site visitée en mode sécurisé ;
- rappeler les recommandations de la CNIL pour choisir un mot de passe (7 caractères alphanumériques au minimum, mot peu courant, non trivial, etc.) ;
- procéder à des rappels de sécurités dans les courriers envoyés à l'abonné internaute (relevé de compte, mailing…).

2.Assurer la sécurité lors de la transmission des codes et mots de passe, et lors de l'accès aux services

Lors de l'accès aux services de banque en ligne, le client doit s'identifier auprès de l'établissement teneur de compte. Cette identification nécessite généralement la saisie d'un login associé à un mot de passe. Elle constitue la garantie pour l'établissement bancaire que la personne qui demande l'accès aux comptes en est bien le titulaire. Ces éléments permettant l'accès aux comptes, il est primordial qu'ils soient transmis de façon sécurisée mais aussi que ces identifiants ne soient pas aisément accessibles ou déterminables.

Ainsi, il paraît souhaitable de **prévoir la transmission des codes d'accès et mots de passe au client par courrier postal et non par courrier électronique, mais aussi d'inciter l'internaute à leur changement à la première connexion sur le site** . En tout état de cause, un mot de passe oublié ne devrait pas être communiqué à son détenteur (les mots de passe doivent être cryptés dans les systèmes informatiques de la banque détentrice, et donc illisibles même aux administrateurs du système) ; la banque devrait appliquer dans ces cas la même procédure qu'au moment de l'adhésion au service (envoi de nouveaux login et mot de passe).

S'agissant des **mots de passe, ceux-ci devraient être alphanumériques, d'une longueur de 7 caractères minimum, peu courants (éviter les nom, prénom, initiales, etc.), changés périodiquement (par exemple tous les 3 mois ou à partir d'un certain nombre de connexions) et conservés confidentiellement.**

Il paraît souhaitable que l'accès soit bloqué dans le cas où un code d'accès erroné a été saisi plus de trois fois consécutivement et d'en informer l'internaute par courrier électronique, SMS, etc.

Par ailleurs, lors de la connexion du client à son service de banque en ligne **il est impératif que le mode sécurisé (https) soit actif dès l'accès à la page d'accueil du site bancaire,**

avant la saisie du login et du mot de passe (certains sites ne basculent en « https » qu'après l'envoi par l'internaute de ses login et mot de passe).

De plus, un service d'assistance devrait être mis à la disposition des clients internautes.

3- Assurer la sécurité lors de l'utilisation du service en permettant la traçabilité des actions réalisées

Le client devrait pouvoir être informé de toute action réalisée à partir des services de banque en ligne. Ainsi l'organisme bancaire devrait en particulier **offrir la possibilité de faire parvenir à l'adresse électronique déclarée lors de l'abonnement au service, pour chaque opération effectuée depuis le compte bancaire vers un compte de tiers, un courriel indiquant qu'une opération a été enregistrée.**

Par ailleurs, lors de sa connexion au service, le client devrait voir affichées **la date et l'heure de la dernière connexion au service et avoir la possibilité de consulter un historique des connexions précédentes** (date, heure et durée de connexion).

En outre, les sites de banque en ligne devraient permettre de :

- S'assurer, qu'à la déconnexion du site par l'internaute, la suppression de tous les cookies et traces diverses soit effective ;
- Mettre en place un contrôle de sécurité renforcé (carte de clés personnelles, token) pour toutes les opérations réputées à risque (virements externes, etc.) ;
- Mettre à disposition des internautes abonnés un outil permettant de tester et de révéler des failles de sécurité sur leur ordinateur personnel, tout en proposant des solutions correctives ;
- procéder à une déconnexion automatique de tout abonné connecté et inactif (par exemple, au-delà de 10mn) ;

Enfin, les sites de banque en ligne pourraient faire l'objet d'une certification ISO.

4- Faciliter l'exercice du droit d'opposition en ligne

S'agissant de la prospection commerciale par voie « classique » (courrier postal ou opérations de télémarketing), il serait souhaitable que les dispositifs de banque en ligne puisse permettre aux clients d'exercer leur droit d'opposition directement sur le site par le biais d'une case à cocher. A l'heure actuelle, l'exercice du droit d'opposition doit généralement s'exercer par l'envoi d'un courrier écrit à la banque.

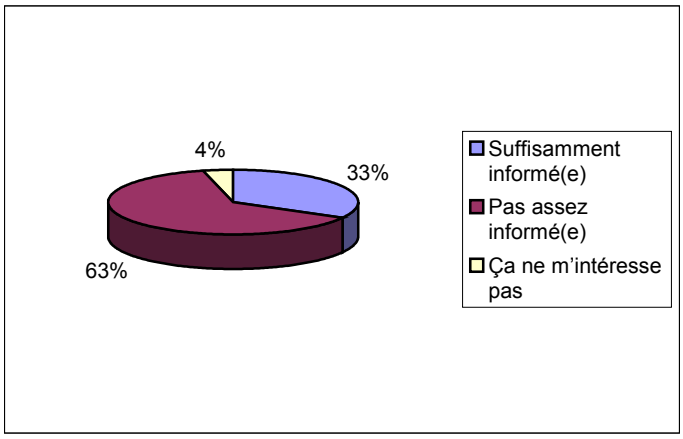
S'agissant de la prospection par voie électronique, une concertation est actuellement en cours entre la CNIL et la profession bancaire dans le but de définir certaines modalités pratiques relatives à la mise en œuvre de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

3- Internautes : les règles d'or pour utiliser les services bancaires en toute sécurité

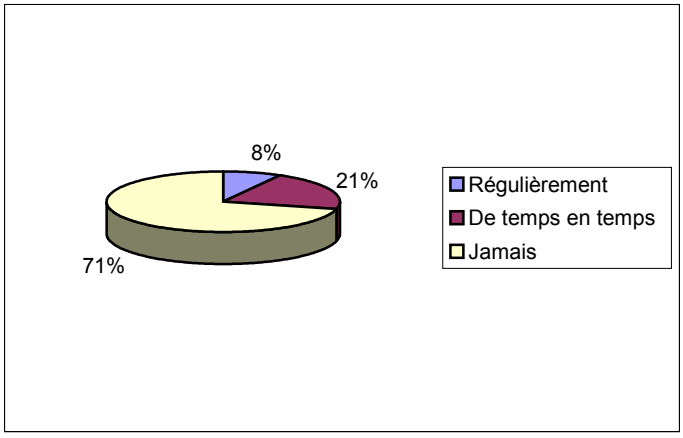
Lors du second semestre 2004, la CNIL a réalisé sur son site Internet un sondage auquel près de 1900 internautes ont répondu. Les résultats reproduits ci-après plaident pour une meilleure sensibilisation des internautes à la nécessaire vigilance dont ils doivent faire preuve lorsqu'ils utilisent des services de banque en ligne.

- Les résultats du sondage

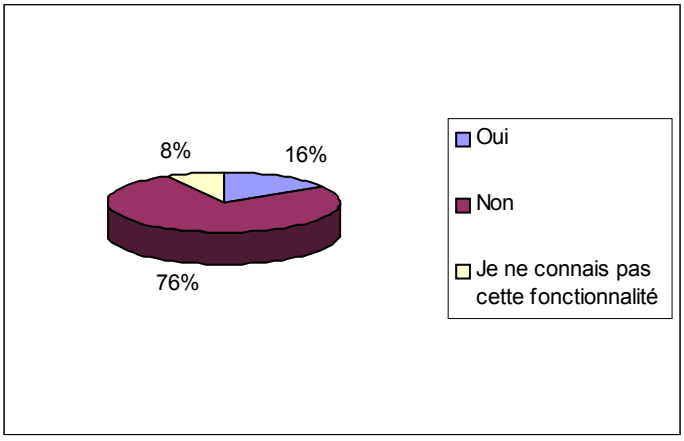
S'agissant du niveau de sécurité de votre service de banque en ligne, vous estimez-vous ?



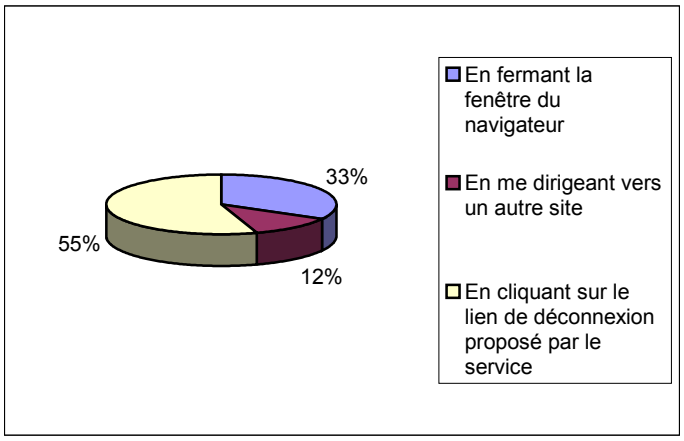
A quelle fréquence changez vous le mot de passe vous permettant d'accéder à votre service de banque en ligne ?



Pour vous authentifier sur votre banque en ligne, utilisez- vous la fonctionnalité de saisie automatique des mots de passe de votre navigateur ?



Après avoir consulté vos comptes, vous quittez votre espace personnel :



- **<u>Adopter une « Internet attitude »</u>**

Vous êtes client d'un service de banque en ligne, vous accédez à vos comptes par Internet, vous êtes par conséquent exposé à des risques importants de fraudes. Il ne s'agit pas d'une fatalité, des techniques et procédures simples peuvent être mises en œuvre pour protéger vos informations personnelles et votre ordinateur, et ainsi réduire les risques.

➢ **<u>Les moyens informatiques à mettre en œuvre</u>**

1) Vous devez assurer la sécurité de votre ordinateur ;
2) Installez les mises à jour récentes de votre système d'exploitation pour bénéficier des derniers correctifs de sécurité mis en place par l'éditeur ;
3) Équipez impérativement votre ordinateur d'un logiciel anti-virus et d'un logiciel pare-feu (fire-wall) ;
4) Attention également aux « spyware » (espiogiciel ou encore mouchard) ;
5) Paramétrez correctement votre ordinateur.

Le logiciel anti-virus

Mis à jour régulièrement et activé, il apporte une protection contre les infections par des virus, les vers ou chevaux de Troie.

Le logiciel pare-feu

Il limite ou empêche les accès non autorisés de tiers à votre ordinateur et aux informations qu'il contient.

L'espiogiciel

Il s'agit d'un petit programme mouchard installé à votre insu sur votre ordinateur. Une de ses fonctions peut être de transmettre vers l'extérieur (Internet) des informations contenues dans votre ordinateur, ou même tout simplement ce que vous tapez au clavier. Ce recueil et cette transmission d'informations indiscrètes sont effectués évidemment à votre insu et sans votre accord ou consentement préalable. Ce type de programme peut arriver dans votre ordinateur par de nombreux chemins.

Le plus fréquent est lorsque vous installez sur votre ordinateur des logiciels dont vous n'êtes pas sûr à 100 % comme les logiciels freeware[1], shareware[1], et plus particulièrement les logiciels d'échanges de fichiers appelés communément logiciels de « peer to peer »[1]. Dans la pratique, ce n'est qu'en surveillant les entrées dans la base de registres ou les processus actifs suspects que l'on peut détecter la présence d' « **espiogiciel ».**

Comment s'en protéger ?

Il existe une solution, les logiciels « anti-espiogiciel » ou « anti-spyware » qui permettent de détecter et supprimer les fichiers, processus et entrées dans la base de registres créés par les « spywares ». De plus, la présence d'un pare-feu personnel peut également permettre de détecter la présence d'espiogiciels, mais aussi de les empêcher de communiquer avec internet, et donc de divulguer les informations enregistrées dans votre ordinateur.

NOTA : Il est relativement aisé de trouver de l'information et des conseils d'utilisation en ligne sur Internet, à partir de moteurs de recherche, concernant les anti-virus, pare-feux, espiogiciels, etc.

Quelques règles de paramétrage de votre ordinateur

1) Désactivez la saisie semi-automatique et l'enregistrement automatique des mots de passe dans votre navigateur Internet. Dans le cas contraire, ces informations sont enregistrées dans votre ordinateur et peuvent devenir accessibles à toute personne pouvant y accéder.

2) Interdisez le stockage des pages sécurisées.

Par exemple pour Internet Explorer 6 :

menu "Outils" -> "Options internet" -> onglet "Avancé", puis dans la rubrique "Sécurité" cochez l'option "Ne pas enregistrer les pages cryptées sur le disque"

3) Supprimez automatiquement les fichiers Internet temporaires à chaque fermeture de votre navigateur Internet. (vous pouvez également les supprimer manuellement).

Internet Explorer 6
menu "Outils" -> "Options internet" -> onglet "Avancé", puis dans la rubrique "Sécurité" cochez l'option "Vider le dossier Temporary Internet Files lorsque le navigateur est fermé" ; pensez alors à fermer votre navigateur après chaque connexion

ou bien
menu "Outils" -> "Options internet" -> onglet "Général", puis dans la rubrique "Fichiers Internet temporaires" cliquez sur le bouton "Supprimer les fichiers".

Interdisez-vous l'installation de logiciels de type « freeware », « shareware » ou encore « peer to peer » dont vous n'êtes pas sûr.

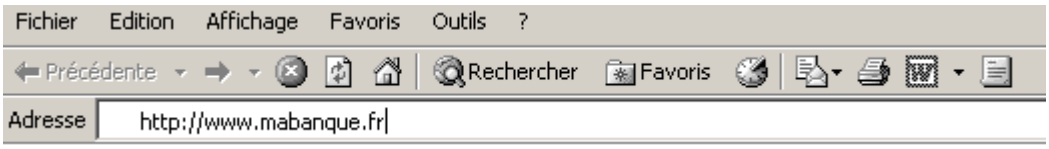
NOTA : Ces différentes barrières logicielles ne sont pas tout. Le comportement de l'internaute peut aussi constituer un facteur risque important.

➢ **Les bonnes pratiques à adopter**

1) Accéder à votre site de banque de manière sécurisée et vérifiez l'orthographe de l'adresse

Accédez à votre site de banque en tapant directement dans la barre d'adresse de votre navigateur l'adresse Internet que vous a fourni votre banque lors de votre abonnement. Créez un raccourci ou placez la page obtenue dans vos favoris. Veillez à toujours utiliser ce raccourci ou le favori pour vos accès ultérieurs.

Avant de saisir votre identifiant et votre mot de passe, assurez-vous que l'adresse du site sur lequel vous vous situez est conforme à celle de votre banque en ligne. En effet, une légère différence dans l'orthographe de l'adresse de votre site habituel révèle le plus souvent une tentative de fraude.



2) Vérifiez vos connexions

Chaque fois que vous accédez à votre banque en ligne, et lorsque cette fonctionnalité est disponible sur votre site de banque en ligne, contrôlez la date et l'heure de votre dernière connexion ainsi que la durée. Vous serez ainsi aussitôt avisé d'une connexion effectuée à votre insu.

3) Vérifiez que la connexion est sécurisée

Assurez-vous que le protocole figurant dans la barre d'adresse est « HTTPS » et qu'au bas de la fenêtre de votre navigateur figure le cryptogramme représentant un cadenas ou une clé indiquant que la page visitée du site est sécurisée.

4) Déconnectez-vous correctement.

Terminez obligatoirement votre connexion à votre site bancaire en utilisant le bouton « déconnexion ».

5) Attention au « phishing»

Vous ne devez jamais cliquer sur un lien dans un courriel reçu pour accéder à votre site de banque en ligne, même si ce courriel semble authentique et provenir de votre banque. Ce principe est fréquemment utilisé par des pirates pour tenter de récupérer à votre insu vos identifiant et mot de passe, et ainsi usurper votre identité pour accéder à vos comptes.

Le courriel envoyé par ces pirates usurpe le plus souvent l'identité d'une banque, et invite l'internaute à se connecter en ligne, par le biais d'un lien hypertexte, à un site web factice, copie conforme du site original. Pour ce faire, il vous est demandé de saisir vos identifiant et mot de passe. Par cette action, les pirates parviennent à obtenir des informations personnelles (identifiant et mot de passe, informations bancaires telles que numéro de compte en banque, etc.), et peuvent ainsi procéder à des mouvements de compte, achats sur internet, etc.

Supprimez sans les ouvrir (et videz la corbeille) tout courriel douteux. N'ouvrez jamais les pièces jointes qui peuvent contenir des virus, chevaux de Troie, particulièrement celles des dossiers exécutables ou des fichiers comportant une extension .exe, .vbs ou .com.

Enfin, pensez à activer les sécurités proposées par votre logiciel de messagerie électronique.

6) Vos identifiant et mot de passe

Ne communiquez jamais vos identifiant et mot de passe.

Si vous recevez un courriel, un appel téléphonique, un écrit (ou tout autre moyen) de votre banque (ou tout autre organisme) vous demandant de communiquer ces informations confidentielles, ignorez ces sollicitations ou, au minimum, assurez-vous auprès de votre banque, par exemple par téléphone, de la sincérité de la demande. Aucun organisme ou banque ne vous demandera ce type d'informations pour une soi-disant maintenance informatique, technique, ou pour une adhésion à un quelconque service.

Le mot de passe

- Lors de votre première connexion, changez-le ;
- Ensuite changez le régulièrement ;
- Si vous avez un doute sur son utilisation, changez le immédiatement, prévenez votre agence.

Ce mot de passe, pour être efficace, doit répondre à un certain nombre de règles :

- Il ne doit pas correspondre à un élément courant de votre vie pour ne pas être facilement déductible ;
- Il doit avoir une longueur suffisante (au moins sept caractères alphanumériques) ;
- Il ne doit absolument pas être écrit à côté de l'identifiant, et, si possible, ne pas être écrit du tout (post-it, fichier, etc.).

7) Les cybercafés et autres points d'accès

Réservez vos accès banque en ligne à votre domicile à l'exclusion de tout autre lieu. Toutes les traces informatiques que vous pourrez laisser sur un ordinateur dont vous n'avez pas la maîtrise sont susceptibles d'être utilisées à votre insu.

Si vous n'êtes pas propriétaire (ou administrateur) de l'ordinateur à partir duquel vous accédez à Internet (cybercafé, club, etc.), prohibez tout accès à vos comptes bancaires en ligne. En effet, si vous n'avez pas la maîtrise totale sur les différents paramètres de configuration de l'ordinateur (accès aux fichiers temporaires Internet, aux cookies, aux fichiers « logs » et autres traces résiduelles en machine), il est tout à fait possible d'enregistrer, à votre insu, vos identifiant, mots de passe, numéros de comptes et autres données à caractère personnel.

Enfin

Certaines banques offrent de vous informer par courriel ou SMS des opérations effectuées sur votre compte. Cette option peut se révéler intéressante, les mouvements anormaux étant ainsi rapidement détectés.

Consultez régulièrement les informations de sécurité de votre site de banque en ligne.

Au moindre doute, contactez votre agence.