



**A VOUS,  
CHER CLIENT,  
CE MESSAGE CONCERNE VOTRE SECURITE**

A la BANQUE DES MASCAREIGNES, nous accordons une extrême importance à la sécurité de vos informations. Nos systèmes et les procédures de sécurité mises en place, ont été conçus de manière à garder vos données personnelles et financières confidentielles, et ceci en toutes circonstances.

Cependant, vous avez également un rôle important à jouer et nous vous recommandons de suivre ces quelques règles de sécurité, qui vous aideront à protéger vos données personnelles et financières contre toute utilisation frauduleuse.

### **Vos codes d'accès sécurisés**

Vos codes d'accès pour le Service de Banque en Ligne constituent l'accès principal à vos comptes en ligne et doivent rester confidentiels.

### **Numéro d'Abonné**

Nous vous conseillons de choisir un Numéro d'Abonné dont vous vous rappellerez facilement, mais que d'autres ne pourront facilement deviner. Evitez de choisir les noms de famille, les dates d'anniversaire, les numéros de téléphone ou des mots qui pourront être facilement devinés. Il est plus sûr de choisir un long identifiant et qui serait difficile à deviner ou à contrefaire.

Nous vous suggérons de créer un mot de passe contenant à la fois une combinaison de lettres de l'alphabet et de chiffres- ceci dans le but d'ajouter à la complexité des codes d'accès.

### **Code Secret**

Votre Code Secret constitue la clef qui vous permet d'accéder à votre compte en ligne et nous vous conseillons vivement de :

- Protéger et de changer votre Code Secret régulièrement, par exemple tous les 1 à 2 mois, de créer un mot de passe que vous, seul, connaîtrez et que d'autres personnes ne pourront deviner.
- Créer un Code Secret contenant une combinaison de lettres de l'alphabet et de chiffres.
- Eviter d'associer votre Code Secret à des informations personnelles telles que les noms, dates de naissance, numéro de téléphone ou autres informations familiales.
- Mémoriser votre Code Secret mais ne le notez jamais ou ne le révéléz jamais à quiconque.

Nous attirons votre attention sur le fait que personne à la Banque des Mascareignes ne vous demandera jamais de révéler votre Code Secret ou PIN ( «Personal Identification Number » ou Numéro d'Identification Personnelle).


Il vous est vivement **déconseillé** de révéler toute information personnelle à quiconque au téléphone ou sur un site Web à moins que vous n'ayez, au préalable, vérifié la crédibilité de la source ou si vous avez été celui ou celle qui avez pris l'initiative de contacter une source fiable. Les sociétés dignes de confiance ne vous demanderont pas votre code secret ou votre PIN («Personal Identification Number»/ Numéro d'Identification Personnelle) par courrier électronique ou par téléphone.

Nous vous **conseillons** vivement d'informer la Banque des Mascareignes de toutes sollicitations inhabituelles à propos de vos données bancaires.

## Votre Sécurité en Ligne

### Vous êtes conseillé :

- d'installer un logiciel de pare-feu sur votre PC afin d'empêcher que toute personne non autorisée ou toute information extérieure n'accède à votre système informatique. Ceci est très important pour les PC qui utilisent une connexion à Internet à haut débit (modems câble ou DSL) ;
- de mettre régulièrement en marche votre logiciel anti-virus sur votre PC. Un logiciel anti-virus permet de filtrer tous les messages et fichiers joints entrants et sortants afin de bloquer l'accès d'éventuels virus, vers (« worms »), chevaux de Troie (« Trojan Horses ») et autres codes malicieux qui pourraient affecter vos fichiers informatiques et la bonne marche de votre ordinateur ;
- de faire l'acquisition de logiciels qui permettent la mise à jour régulière et automatique de votre protection contre les virus informatiques sur votre ordinateur ;
- de maintenir à jour le logiciel de votre PC et de faire en sorte à ce que vous appliquiez les patch de sécurité pour votre système d'exploitation afin de garder à jour les données relatives à la sécurité de votre PC ;
- d'envisager l'acquisition de logiciels anti-spam qui filtrent au préalable les courriers électroniques indésirables ou « spam » - avant de les éliminer- de votre liste de messages entrants.

Lorsque vous remplissez un formulaire d'inscription sur un site Web dont l'adresse n'affiche pas « **https://** » ou si vous ne voyez pas le symbole « cadenas »  en bas de page à droite, ne divulguez aucune donnée personnelle.

Le protocole « **https://** » et le symbole « cadenas » indiquent que la session en ligne se déroule dans un contexte « sécurisé » et que les informations personnelles que vous avez fournies sont protégées.

Protégez votre Code Secret à partir de votre PC, de tout accès à vos données personnelles par des personnes non autorisées, et changez-le tous les 1 à 2 mois.

Désactivez l'option 'Saisie Automatique' afin d'éviter que d'autres personnes ne voient les données concernant votre accès lorsque vous utilisez le Service de Banque en ligne.

Toujours terminer la session en ligne- en faisant la déconnexion- et fermer votre navigateur après chaque session sur le service de Banque en Ligne et éteindre votre ordinateur lorsque vous ne l'utilisez pas.

N'accédez pas au Service Banque en Ligne dans les cybercafés, bibliothèques ou autres endroits publics où vos données personnelles risquent d'être copiées, retracées et réutilisées après votre utilisation.

Prenez connaissance des clauses de confidentialité en lisant les chartes de confidentialité des sites Web que vous visitez, pour savoir comment elles sont appliquées à des offres commerciales,

publicités et tirages au sort. Renseignez-vous sur la manière de faire enlever votre nom des bases de données qui servent à des fins commerciales afin de ne pas recevoir de courriels (courrier électronique) indésirables ou «Spam».

Vérifiez d'où proviennent vos messages ou courriels avant de les consulter et toujours mettre en marche votre logiciel anti-virus avant de les lire. Ne soumettez jamais d'informations d'ordre privé, personnel ou financier, sauf si celles-ci sont cryptées sur un site Web qui est sécurisé par une source fiable.

Sachez qu'il existe des messages électroniques et sites Web qui ont pour intention de piéger des consommateurs et de recueillir des informations personnelles concernant ces derniers. Si vous recevez un message électronique ou un lien à une page ou à un site Web, vous demandant de confirmer les données personnelles vous concernant, ne soumettez en aucun cas ces informations- même si la page Web vous semble légitime. Ne répondez pas aux chaînes de courriels puisque certaines contiennent un virus informatique dans le ou les fichiers joints. La meilleure chose à faire est de les éliminer.

N'ouvrez pas les courriels ou fichiers joints dont vous ne connaissez pas la provenance. Filtrez au préalable le courrier électronique à l'aide d'un logiciel antivirus.

NE double-cliquez pas sur un fichier joint électronique- dont vous ne connaissez pas la provenance- contenant un ou des dossiers exécutables dont l'extension est : «.exe », «.com », ou «.vbs ».

### **Votre sécurité hors connexion**

#### **Vous êtes vivement conseillé de :**

- Ne pas divulguer –concernant le service Mascareignes Direct - votre Numéro d'Abonné, Code secret ou toute information personnelle à quiconque lors d'une communication téléphonique, sur un site Web ou autrement, à moins d'avoir vérifié la crédibilité de la source ou si vous avez été celui ou celle qui avez lancé l'appel vers une source sûre ;
- Ne pas permettre l'accès à votre ordinateur à des étrangers ;
- Désactiver l'option « Partage de fichiers et d'imprimantes pour les réseaux » sur votre PC pour ne permettre à quiconque sur Internet de chercher ou d'effacer vos fichiers informatiques ;
- Vérifier vos relevés de comptes bancaires et de cartes de crédit pour noter toute transaction non autorisée ou tout retrait non autorisé et, informer la Banque de toutes irrégularités si toutefois vous en constatez dans les relevés. Les transactions et achats effectués peuvent également être vérifiés à travers les services de Banque à Distance par Internet ;

- Rester informé sur les façons vous permettant de toujours bénéficier d'une expérience bancaire en ligne sécurisée grâce à des bulletins d'informations par messagerie.

**En cas de fraude ou de transaction illégale sur votre compte :**

Si vous pensez avoir été victime de fraude ou si vous pensez qu'une transaction suspicieuse ou illégale s'est effectuée sur vos comptes, nous vous conseillons d'en informer immédiatement la Banque en téléphonant au : **(230) 213.22.00.**

De plus, il vous est conseillé de porter plainte auprès de la Police et d'obtenir des copies du procès-verbal afin que vous puissiez les référer à vos créanciers.