

Aspects importants relatifs à la sécurité

Chez BBVA, nous sommes conscients du besoin de **garantir la sécurité** au cours du transfert de données entre la banque et nos clients. C'est pour cette raison que nous disposons des mesures de sécurité les plus élevées pour garantir la **confidentialité des communications**.

Vérifiez toujours que vos données sont saisies sur une **page sécurisée**.

NORMES DE SÉCURITÉ

Il est important que vous suiviez les **normes de sécurité** suivantes à chaque fois que des données à caractère personnel vous sont demandées par Internet :

1. Vérifiez que la **connexion** est établie à travers un **serveur sécurisé** en vérifiant certains des aspects suivants :

- Grâce à l'adresse (URL) du serveur, puisque l'adresse d'un serveur sécurisé commence par https et non par http.
- Grâce à une indication de votre navigateur, qui se trouve sur l'un des coins inférieurs de votre fenêtre : une **clé entière** (au lieu d'être cassée, comme pour n'importe quel serveur non sécurisé) ou un **cadenas fermé** (au lieu d'être ouvert, comme pour n'importe quel serveur non sécurisé).

2. **Contrôlez les certificats de sécurité** de la page :

- Pour ce faire, cliquez sur l'icône du cadenas qui apparaît lorsque vous accédez à une zone sécurisée, sur la partie inférieure droite de votre navigateur, et vérifiez que la date d'expiration et le domaine du certificat sont en vigueur. Parmi les informations détaillées, vous trouverez l'émetteur, la période de validité et pour qui le certificat a été émis.

Pour que les mesures suivantes soient effectives, il est nécessaire d'utiliser les versions les plus récemment mises à jour des navigateurs suivants :

- Internet Explorer
- Firefox
- Chrome

De plus, le site Web a été optimisé pour une résolution d'écran de 1280 x 800 pixels ou supérieurs, pour un meilleur affichage.

SERVEUR SÉCURISÉ

Les systèmes transactionnels de services fonctionnent sur un serveur sécurisé qui utilise le **protocole SSL** (Secure Socket Layer), qui est toujours activé au moment de l'entrée dans le système de services. Le serveur transmet **les données cryptées** grâce aux algorithmes 128 bits, qui assurent qu'elles ne soient **intelligibles que pour l'ordinateur du client et le serveur de la banque.**

En utilisant le protocole SSL, nous garantissons :

- Que le client communique ses données au centre serveur du BBVA.
- Qu'entre le client et le centre serveur du BBVA, les données sont cryptées lors de leur transfert, évitant ainsi leur éventuelle lecture ou manipulation par des tiers.

ACCÈS À BBVA.BE

Chez BBVA, nous recommandons à tous nos utilisateurs de suivre ces conseils simples pour maintenir la sécurité absolue de leur session à travers notre service de Banque à distance.

Pour fermer votre session sur BBVA.BE, vous devrez toujours utiliser le bouton « Déconnexion » de la barre d'outils de BBVA.BE et cliquer sur « Ok » dans la fenêtre qui apparaîtra ensuite.

Ainsi, vous aurez fermé votre session BBVA.BE en toute sécurité et lors de votre prochaine connexion à BBVA.BE votre numéro d'utilisateur et votre code d'accès vous seront de nouveau demandés.

Si vous ne vous **déconnectez pas correctement**, le serveur ne considèrera la session comme fermée qu'une fois la période déterminée de temps (time-out) expirée, ce qui activera la **déconnexion automatique**. Si vous changez de page sur Internet sans suivre ces étapes, il sera possible d'accéder directement à votre espace personnel sur BBVA.BE sans saisir vos codes d'accès tant que la période de temps nécessaire pour la déconnexion automatique ne se soit écoulée.

MÉMOIRE CACHE

La mémoire cache du navigateur permet d'accéder de manière presque immédiate aux pages Web que vous avez récemment visitées.

Parfois, cette possibilité peut provoquer certains **petits incidents** dans le fonctionnement correct des pages. Il est possible qu'à travers votre ordinateur personnel, **la dernière version affichée soit la dernière version stockée dans la mémoire cache** et non la dernière version stockée sur le serveur de ce site Web.

Pour éviter ces inconvénients, nous vous recommandons de cocher dans votre navigateur l'option de **mise à jour des contenus à chaque visite de la page** et qu'à une certaine fréquence tous les fichiers du dossier des **fichiers temporaires d'Internet** soient éliminés.

SÉCURITÉ DE VOS CODES

Conseils

- **Ne communiquez à personne** les codes que vous utilisez sur BBVA.BE.
- L'identifiant et le code d'accès doivent être différents. De cette façon, il sera plus difficile pour un tiers de les connaître et de les deviner.
- Si vous pensez que quelqu'un a pu deviner votre code d'accès, vous devez le modifier le plus vite possible.

Stockage des codes d'accès sur les ordinateurs

- Actuellement, les navigateurs offrent la possibilité d'**enregistrer les codes et les mots de passe** des sites Web qui les demandent, ces derniers étant stockés dans la mémoire de votre ordinateur. **Cette pratique**, bien qu'elle rende plus facile l'accès aux sites sur lesquels le nom d'utilisateur et le mot de passe sont demandés, est fortement **déconseillée** lorsque les codes stockés sont ceux des banques ou autres services qui, en cas de perte ou de soustraction, peuvent provoquer **de graves dommages aux utilisateurs**.
- Chez BBVA, nous vous recommandons de **n'enregistrer aucun de vos codes d'accès** à notre service de Banque à distance sur votre ordinateur. Celui-ci peut faire l'objet de certaines **attaques** qui peuvent **envoyer les codes vers d'autres** ordinateurs connectés à Internet.

Pour **effacer les codes stockés** sur un ordinateur, il suffit de suivre une série d'étapes simples que vous pouvez consulter sur le **manuel d'aide de votre navigateur**.

Prévention et détection des attaques de virus

Les **virus** sont des logiciels dont l'objectif est celui **d'être installés** sur l'ordinateur d'un utilisateur **sans que celui-ci ait donné son autorisation et/ou le sache**. Il existe plusieurs types de virus, mais tous ont en commun de se propager et de se diffuser, à l'intérieur du même équipement et à travers le réseau.

Il est facile de contribuer sans le savoir à la diffusion d'un virus, en transférant des e-mails contenant des fichiers joints infectés par un virus. **La collaboration de tous** les utilisateurs d'Internet est fondamentale pour **éviter la diffusion** de virus à travers le réseau.

Il existe plusieurs types de fichiers qui peuvent être infectés par un virus : nous vous recommandons de ne pas faire confiance aux extensions de fichiers telles que .exe, .com, .bat et de **n'exécuter** sur votre ordinateur personnel **que les fichiers** provenant d'un expéditeur **de confiance**.

Nous vous recommandons **de ne pas télécharger** sur votre ordinateur les **fichiers n'étant pas vérifiés et certifiés** et **de ne pas ouvrir les e-mails de destinataires inconnus**.

Précautions

- Paramétrez correctement la **sécurité du système et de la connexion** à Internet et vérifiez régulièrement le niveau de sécurité de connexion. Ne modifiez pas les paramètres de sécurité de votre équipement, sauf si vous possédez les connaissances appropriées. Dans ce cas, paramétrez l'équipement et tous vos logiciels avec les niveaux de sécurité les plus élevés possibles.
- Assurez-vous en permanence que votre système d'exploitation, votre navigateur et les logiciels que vous utilisez régulièrement **sont mis à jour**.
- Installez un **pare-feu** et un logiciel **anti-virus** et assurez-vous qu'ils sont mis à jour régulièrement.
- Procéder à des **sauvegardes** régulières des fichiers.
- Si vous utilisez des connexions avec **Forfait** (par exemple, ADSL et câble), **éteignez votre ordinateur** une fois votre session fermée, vous éviterez ainsi l'exposition de votre équipement à d'éventuelles attaques.
- Vérifiez que les pages Web sur lesquelles vous devez saisir des données confidentielles sont **sécurisées** : avec les icônes du cadenas et de la clé et dont l'adresse commence par https.
- Avant de sélectionner un **lien** sur une page Web, **vérifiez** qu'il vous renvoie à l'adresse souhaitée. Il est également fréquent d'inclure dans un e-mail des liens qui semblent renvoyer vers un site Web légitime, mais qui renvoient vers un site Web n'ayant rien à voir avec l'entreprise dont le message provient, s'ils sont examinés plus rigoureusement. Restez vigilant même lorsque le design du site Web semble légitime.
- Faites preuve d'une attention particulière et de précautions lorsque vous **téléchargez des logiciels** : en cas de doute, ne permettez pas les téléchargements sur les sites auxquels vous ne faites pas entièrement confiance
- Paramétrez votre **messagerie** pour ne recevoir que les messages en format texte. N'exécutez pas un fichier joint à partir d'un e-mail qui vous a été transféré, essayez d'enregistrer ce fichier sur votre disque dur et si celui-ci est infecté, votre anti-virus le détectera. Refusez les fichiers des chats ou groupes de discussion que vous n'avez pas sollicités au préalable. Cryptez les messages et les fichiers les plus importants.

PROTECTION DES DONNÉES

Chez BBVA, nous garantissons la protection des données de nos clients.

Le cachet de l'Association espagnole de certification électronique (ACE) nous accorde la place de **première entité financière** adhérente à son **Code éthique de protection des données sur Internet**.

Le site Web du BBVA (Banco Bilbao Vizcaya Argentaria) en Belgique, sur www.bbva.be, ne reconnaît automatiquement aucune donnée relative à l'identité des visiteurs de ses pages. Pour les services de Banque à distance, dans le **but de garantir la sécurité et la confidentialité** des transactions, l'utilisateur doit **s'identifier et s'authentifier** au préalable sur le système à travers la **demande de saisie des codes d'accès**. Dans le cas où l'utilisateur demande des renseignements sur nos services ou nos produits ou bien souhaite suivre une procédure de réclamations ou d'incidences, à travers l'envoi de formulaires résidents des pages Web du BBVA, il sera nécessaire, dans tous les cas, de collecter les données à caractère personnel indispensables pour nous permettre de répondre à sa requête.

Toutes les données sont transférées dans la confidentialité absolue, **n'étant pas accessibles par des tiers** à des fins autres que celles pour lesquelles elles ont été sollicitées. Pour tout renseignement ou commentaire personnel concernant l'exécution des droits d'accès, d'annulation, de rectification ou d'opposition prévus par la loi belge sur la protection des données personnelles, vous pouvez nous contacter à travers :

bbvabe@bbva.com, n° de téléphone +32 (0)2 512.32.62, ou par courrier à BBVA, succursale en Belgique, Service Clientèle, Avenue des Arts 43, 1040 Bruxelles.