13. PAIEMENT ÉLECTRONIQUE ET EN LIGNE

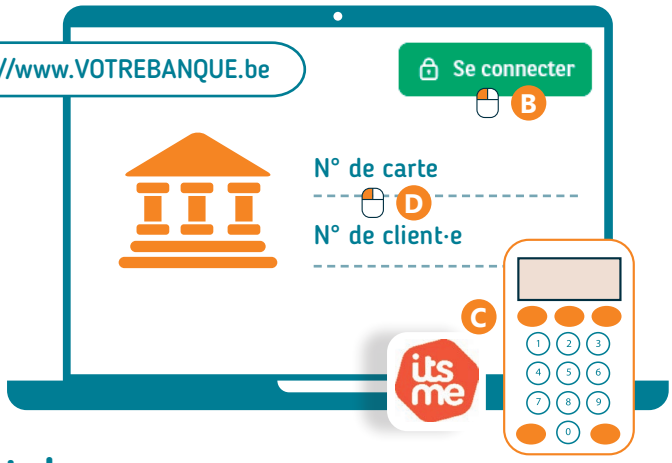
3. Accéder à sa banque en ligne

Avec le développement des outils numériques, les clients ont eu accès à de nouveaux outils pour gérer leur compte en banque. Il est possible de gérer toutes ses opérations depuis son ordinateur via un navigateur ou depuis son smartphone ou sa tablette via une application.

Sur demande, votre banque vous fournit **un lecteur de carte**, un **Digipass**. C'est un appareil électronique qui génère des codes de sécurité uniques. Cela permet en quelques étapes de vous authentifier et connecter à votre compte de manière sécurisée :

1. Identification de l'utilisateur
   - avec le code de la carte de banque par exemple
2. Génération d'un code sécurisé unique à chaque utilisation
3. Saisie du code par l'utilisateur
4. Vérification du code saisi

1. Sur PC via un navigateur



A. Rendez-vous sur la page web de votre banque (voir fiche 3.2.).

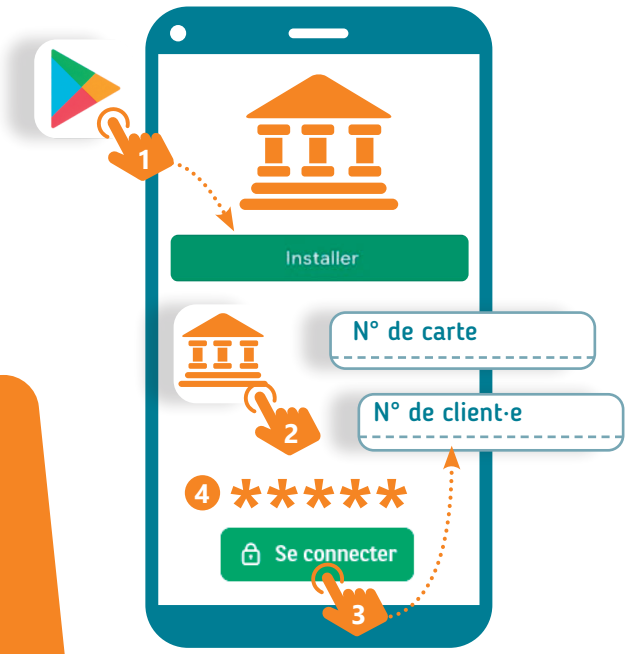
B. Trouvez le bouton permettant de **vous connecter**. En général, il se trouve **en haut à droite** de la page.

C. Plusieurs manières de vous connecter vous seront proposées : **itsme** (voir fiche 7.3.), **lecteur de carte...**

D. Entrez les données demandées pour accéder à votre compte.

2. Via l'application sur smartphone

1. Installez l'application de votre banque via le **Play Store** (voir fiche 1.14.).
2. Une fois installée, ouvrez l'application.
3. Suivez les instructions pour vous connecter à votre compte.
4. Vous pourrez configurer la méthode de connexion à utiliser la prochaine fois. Cela peut être **un code secret**, **l'utilisation du Digipass** ou même **une empreinte digitale** ou la reconnaissance faciale si votre smartphone dispose de ces options.



En cas de soucis lors de votre connexion, il y a souvent **un numéro de téléphone** affiché qui vous permettra d'obtenir de l'aide.

Une recherche sur internet (voir fiche 3.3.) des termes « **utilisation de** » suivi du nom de **votre banque** + **mobile** (ex: Utilisation de Fortis mobile, utilisation de ING mobile) vous donnera accès à des ressources d'aide écrite ou vidéo.

3. Sécurité des banques en ligne

L'utilisation des services en ligne est très sécurisée. Les principaux risques concernent **l'usurpation d'identité** et **le vol des données de paiement** (voir fiche 9.2.).

Voici les principales techniques de piratage et quelques conseils pour les éviter :

Le Phishing : technique utilisée pour tromper les utilisateurs en leur faisant croire qu'ils communiquent avec une source de confiance, comme leur banque, dans le but de voler des informations sensibles telles que des mots de passe, des informations financières...

- La banque ne demande **JAMAIS** ce genre d'informations.
  Pour être rassuré·e et obtenir plus de renseignements, le mieux est de contacter rapidement un·e conseiller·ère de votre banque.
- **Dans tous les cas, ne transmettez JAMAIS vos identifiants bancaires par mail ou après avoir cliqué sur un lien de l'e-mail.**

Le Pharming : Faux site web, ressemblant au portail officiel de l'établissement bancaire, mais enregistrant les identifiants et les codes personnels de l'utilisateur·rice dans un objectif de revente des données.

- Vérifiez l'adresse du site Web sur lequel vous êtes pour vous assurer que vous êtes sur le site de la banque (voir fiche 3.2.).
- **Ne désactivez pas le firewall** du PC.

Le Spyware : Logiciel espion qui s'installe à l'insu de l'internaute sur son ordinateur et qui enregistre ses faits et gestes (voir fiche 9.2.).

- Mettez à jour votre smartphone (voir fiche 9.5.) ou PC (voir fiche 9.8.).
- Ayez une navigation responsable et attentive sur Internet (voir fiche 3.4. et 3.6.).

Pour protéger votre compte bancaire en ligne, il vous faut surtout vous protéger vous-même en adoptant un comportement **prudent** et **attentif** :

- **Ne divulguez JAMAIS vos identifiants bancaires.**
- Sécurisez et protégez vos équipements connectés, PC ou smartphone. Veillez à ce qu'ils soient régulièrement mis à jour (voir fiche 9.5. et 9.8.).
- Ne vous connectez pas depuis des espaces non protégés (wifi public par exemple - voir fiche 2.5.) ou un PC qui ne vous appartient pas ou avec une session partagée avec d'autres personnes.
- **Ne répondez pas à des e-mails douteux** et **supprimez-les** : émetteur inconnu, fautes d'orthographe et de syntaxe, demande de codes confidentiels... (voir fiche 4.4.)
- Choisissez **un code secret efficace** pour vous connecter à votre espace bancaire en ligne et renouvelez-le fréquemment.
- Utilisez de préférence l'application smartphone plutôt que le site internet de votre banque **(sécurité en +)**.

interface3 namur
www.interface3namur.be/box-numerique

Projet réalisé avec le soutien du Fonds "ING Fund for a more Digital Society", géré par la Fondation Roi Baudouin