13. PAIEMENT ÉLECTRONIQUE ET EN LIGNE

1. Les moyens de paiement électroniques

Les paiements électroniques se sont développés à partir des années 1970 avec l'introduction des cartes de crédit, puis de débit. Adoptés massivement par les consommateurs et entreprises, leur croissance est exponentielle. Il existe aujourd'hui une multitude de possibilités de paiement électronique.

Le développement des réseaux de télécommunication et d'Internet ont ouvert la voie à une panoplie de nouvelles méthodes de paiement électronique : **virements bancaires**, **transferts d'argent en ligne**, **porte-monnaie électroniques ou e-wallets**, **paiements avec son smartphone**, **cartes prépayées**, **cryptomonnaies**...

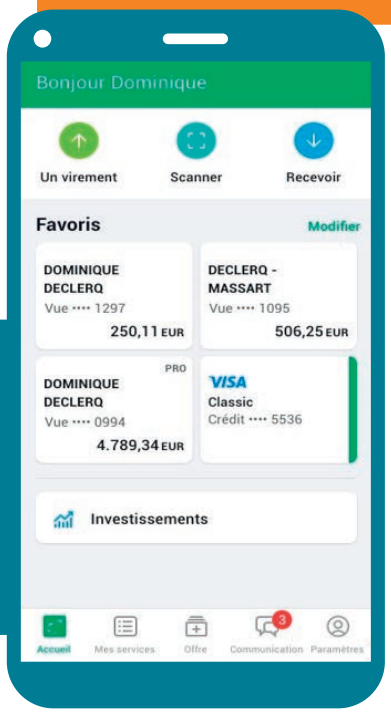
1. Les applications bancaires

Développées par les banques, les applications bancaires permettent aux clients d'accéder à leurs services financiers depuis un smartphone ou tablette. Elles permettent de réaliser des opérations telles que :

- la consultation de solde
- le virement ou le paiement mobile
- la gestion des cartes bancaires
- la souscription à des produits financiers...

Après avoir téléchargé l'application de votre banque (voir fiche 1.14.), vous devez configurer votre compte (voir fiche 13.3.) avec un **lecteur de carte de votre banque** ou **digipass**. Vous pourrez par la suite changer de méthode de connexion : empreinte digitale, code PIN...

Les **cryptomonnaies**, comme le Bitcoin, sont des monnaies numériques sécurisées par la cryptographie et fonctionnant indépendamment des banques.



Si une personne doit vous verser une somme d'argent, vous pouvez, via l'application de votre banque, générer un **QRCode** que la personne **scanne depuis son application de paiement** (celle de sa banque ou une application comme Payconiq - voir fiche 13.2.) pour effectuer le paiement. Un message vous indique si l'opération a réussi.

Le système est similaire pour vos achats en ligne. Au moment de payer, le site génère un **QRCode** que vous devez scanner pour payer.

2. Les porte-monnaie électroniques

Les **e-wallets**, **porte-monnaie ou portefeuilles électroniques** sont des plateformes numériques qui stockent et gèrent de l'argent en ligne pour faciliter les paiements, les transferts et les achats.
Les plus connus sont : **PayPal**, **Apple Pay**, **Google Wallet**.

Ils offrent une alternative rapide et sécurisée. Ils peuvent être associés à une carte de crédit ou de débit, ou même à des cryptomonnaies.

D'une plateforme à l'autre, le principe est assez similaire :

- soit vous liez une carte de crédit et la plateforme sert d'intermédiaire sécurisé cryptant vos données bancaires,
- soit vous **« chargez »** de l'argent à utiliser pour vos achats en ligne, limitant ainsi la dépense possible au montant chargé.

3. Les cartes prépayées

Une carte pré-payée offre les mêmes fonctionnalités pour des paiements en ligne qu'une carte de crédit type **Visa** ou **Mastercard**, à la différence qu'il est nécessaire de mettre de l'argent sur celle-ci avant de l'utiliser. **Il n'y a donc pas de crédit, ni d'intérêts prélevés.** Ce service de carte prépayée est un service payant proposé la Bpost ou certaines banques.

Payer avec une carte prépayée n'engendre généralement pas de frais supplémentaires.
Mais, des frais peuvent être appliqués lors du retrait d'argent à un distributeur automatique de billets.

4. Payconiq by Bancontact (voir fiche 13.2.)

L'application Payconiq (voir fiche 13.2.) permet de payer en magasin, chez un prestataire de services ou en ligne. Pour l'utiliser, il est indispensable de configurer l'application et de **relier un ou plusieurs compte(s) bancaire(s) à l'application**.

L'application permet également de :

- utiliser des chèques repas si ceux-ci sont fournis électroniquement - Sodexo, Monizze...
- acheter ses billets de tram, train ou bus
- faire des dons à des associations
- rassembler une collecte de fond...

5. NFC

Le **NFC**, pour Near Field Communication en anglais, est une technologie qui permet l'échange d'informations entre dispositifs compatibles rapprochés à une distance très courte, généralement quelques centimètres.

Le NFC est souvent utilisé pour faciliter des interactions rapides et sécurisées, telles que les **paiements sans contact** avec des cartes bancaires, des smartphones ou d'autres dispositifs équipés de cette technologie.

Afin d'effectuer des paiements sans contact avec son téléphone, il est conseillé de **se créer un compte sur un portefeuille électronique** bien sécurisé tel que **Google Pay**, **Apple Pay**... La puce NFC du téléphone est ensuite associée à ce compte et la fonctionnalité doit être activée.

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

2. Payconiq

Payconiq by Bancontact est une application mobile de paiement et de transfert d'argent. L'application, disponible en Europe, est sécurisée et pratique. Elle permet aux utilisateurs de payer rapidement et facilement en scannant un QR code ou en utilisant le NFC (paiement sans contact).

Avec **Payconiq**, les paiements sont effectués sans avoir à saisir manuellement les détails de paiement et **sans nécessiter de carte de crédit**. L'application permet de :

- payer en ligne ou en magasin,
- transférer d'argent ou remboursement entre proches
- gérer des dépenses lors d'une sortie en divisant facilement les coûts entre participants

Les transactions sont protégées par des mesures de sécurité avancées, telles que **la vérification d'empreinte digitale** et **la protection des données**.

1. Installation

Installez l'application via **Google Play** (voir fiche 1.14.).

1. A la première utilisation, vous devez accepter les conditions générales.
2. Encodez **votre numéro de téléphone**.
   Un code est envoyé par SMS afin de confirmer votre inscription.
3. Entrez ensuite **votre prénom** et **votre nom**.
4. Puis saisissez **votre adresse mail**.
5. Choisissez **un code à 4 chiffres (code PIN)** qui vous servira pour valider vos paiements.

Possibilité d'activer l'authentification biométrique (empreinte ou reconnaissance faciale).

6. Ajoutez une **carte bancaire** en sélectionnant votre banque dans la liste.
7. Une confirmation vous est alors demandée différente selon votre banque (Digipass, etc.).
8. Appuyez sur **« Relier votre compte bancaire »**.
9. Pour finaliser l'opération, appuyez sur **le lien de confirmation envoyé par e-mail**.
10. Votre compte bancaire est désormais lié à votre appli Payconiq.

2. Paiement

1. Ouvrez l'application **Payconiq**
2. Vous pouvez au choix :
   - scanner **un QR code** à la caisse d'un établissement (sur un autocollant, sur l'écran de la caisse ou sur le terminal de paiement) ou généré par l'application sur le smartphone d'une autre personne (ami, famille,...).
   - sélectionner dans « **la liste des magasins** ».
   - choisir un ami dans « **vos contacts** ».
3. Saisissez vous-même le montant ou contrôlez le montant qui s'affiche.
4. Si possible et si vous le souhaitez, ajoutez une communication.
5. Appuyez sur le bouton de paiement et confirmez avec **votre code PIN** (voir recto), **votre empreinte digitale** ou **par reconnaissance faciale**.
6. L'application envoie une confirmation pour indiquer que le paiement a bien été effectué.

Pour aller plus loin et vous tenir informé·e de l'actualité ou des nouveautés concernant l'appli, **rendez-vous sur :** www.payconiq.be

Et aussi, profitez des démos disponibles pour payer en magasin, rembourser des amis, payer des additions et des factures...

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

13. PAIEMENT ÉLECTRONIQUE ET EN LIGNE

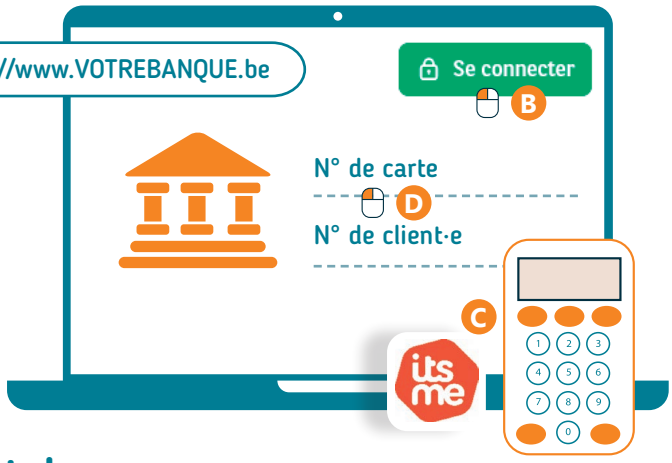
3. Accéder à sa banque en ligne

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.).

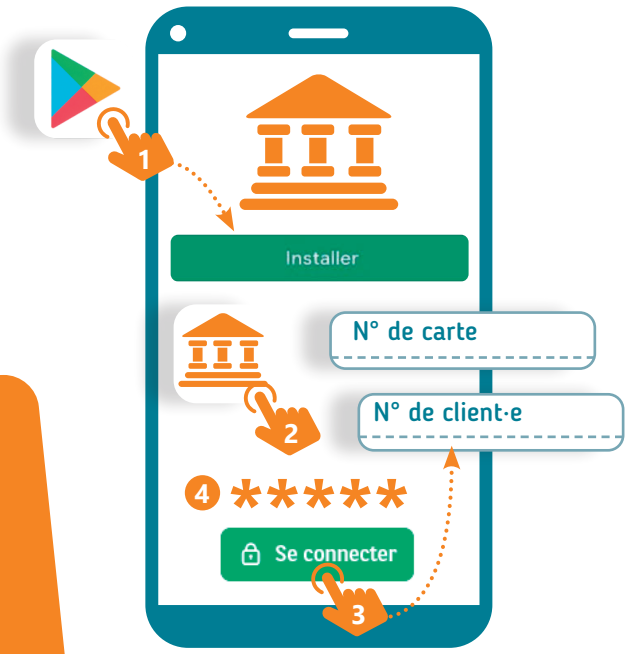
B. Trouvez le bouton permettant de **vous connecter**. En général, il se trouve **en haut à droite** de la page.

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

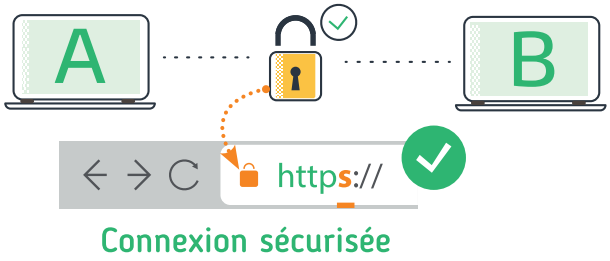
4. Sécuriser ses achats en ligne

Un achat en ligne sécurisé signifie que vos informations personnelles et financières sont protégées lors de l'achat d'un produit ou d'un service sur Internet. Cela signifie également que le produit ou service est tel qu'il est décrit et que l'entreprise ou le site Web auprès duquel vous faites votre achat respecte vos droits en tant que consommateur·trice.

1. Comment sécuriser ses achats en ligne ?

A. Choisissez des sites sécurisés

Avant de saisir vos informations personnelles, recherchez **le cadenas dans la barre d'adresse** de votre navigateur, qui indique que le site utilise le protocole **HTTPS**, plus sûr que **HTTP** (voir fiche 3.6.), pour protéger vos données.



Connexion sécurisée

B. Choisissez des sites de confiance

Optez pour des sites de vente en ligne réputés et bien établis. Vérifiez les avis et les retours d'autres clients pour évaluer leur fiabilité.

C. Ne partagez pas trop d'informations personnelles :

Un site de vente en ligne n'a pas besoin de connaître des détails tels que votre orientation sexuelle ou votre numéro nationale. Prudence avec les informations que vous partagez.

D. Utilisez une connexion sécurisée

Évitez d'effectuer des achats sensibles lorsque vous êtes connecté·e à un réseau **Wi-Fi public**, plus vulnérable aux attaques (voir fiche 2.5.).

E. Utilisez des moyens de paiement sécurisés

Utilisez des cartes prépayées ou des services de paiement en ligne réputés, des portefeuilles électroniques, tels que **PayPal**, qui offrent une protection supplémentaire (voir fiche 13.1.).

Ne cochez pas les cases pour conserver vos informations de paiement. Entrez-les à chaque fois pour réduire les risques de vol de données.

2. Méfiez-vous des arnaques courantes

Les arnaques en ligne sont malheureusement courantes et de plus en plus imaginatives, n'hésitant pas à s'inspirer et à profiter de vos habitudes de consommation ou de l'actualité pour vous manipuler (voir fiche 9.2. et 13.5.).

Avant de faire vos achats, vérifiez les conditions de vente et les possibilités de contact du service client. Privilégiez des plateformes européennes.

Méfiez-vous des :

- Offres trop belles pour être vraies ou promotions très alléchantes (voir fiches 3.4.), surtout de sites moins connus. Les escrocs peuvent utiliser de telles offres pour vous attirer et voler vos informations.
- E-mails non sollicités vous demandant vos informations personnelles (voir fiche 4.4.) et évitez de cliquer sur les liens.
- Sites Web qui ne semblent pas professionnels ou ne disposant pas de protocole de connexion sécurisée **HTTPS** (voir fiche 3.6.).

3. Les recours en cas de problème

Si vous rencontrez un problème avec un achat en ligne, comme un produit non livré, abimé ou non conforme à la description :

1. **Contactez d'abord**, le ou la vendeur·euse pour essayer de résoudre le problème.
2. Si cela ne fonctionne pas, vous pouvez contacter le service client de votre banque pour bloquer le paiement.
3. Ou le service de paiement que vous avez utilisé, qui peut être en mesure de vous aider.

Il existe également des organismes de protection des consommateurs en Belgique, comme le **SPF Economie**, qui peuvent vous aider en cas de litige avec un vendeur.
https://economie.fgov.be/fr

economie

N'oubliez pas : Acheter en ligne peut être pratique, mais c'est aussi important de le faire prudemment. **Soyez vigilant·e et protégez vos informations personnelles.**

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

Se prémunir des arnaques en ligne est essentiel pour protéger vos informations personnelles, votre argent, vos appareils, votre réputation, votre bien-être émotionnel et ceux de vos proches. La vigilance et l'adoption de bonnes pratiques sont cruciales pour minimiser les risques d'être victime d'une arnaque.

1. Qu'est-ce qu'une arnaque en ligne ?

Une arnaque en ligne, ou **cyberarnaque**, est une opération trompeuse **pour obtenir** des **informations**, de l'**argent**, des biens ou d'autres **avantages** de **manière illégale** et/ou **malveillante**. Des tactiques sophistiquées et manipulatrices sont souvent utilisées **pour inciter à agir de manière contraire à nos intérêts**.

Quelques signes peuvent indiquer une possible arnaque en ligne :

- Des offres trop belles pour être vraies.
- Des demandes d'informations personnelles ou financières non sollicitées.
- Des e-mails provenant d'adresses inconnues ou suspectes.
- Des gains à des concours ou loteries sans y avoir participé.

2. Exemples d'arnaques

E-mails et sms frauduleux : Souvent **urgents et alarmistes**, avec **des pièces jointes véhiculant des virus, des liens vers des pages web non sécurisées** ou **des formulaires** demandant vos informations... Les fraudeurs se font passer pour des entités de confiance, comme une banque, pour obtenir vos données bancaires ou vous incitent à utiliser votre lecteur de carte en prétextant des problèmes avec vos comptes ou votre carte.

Un e-mail de la Banque ???

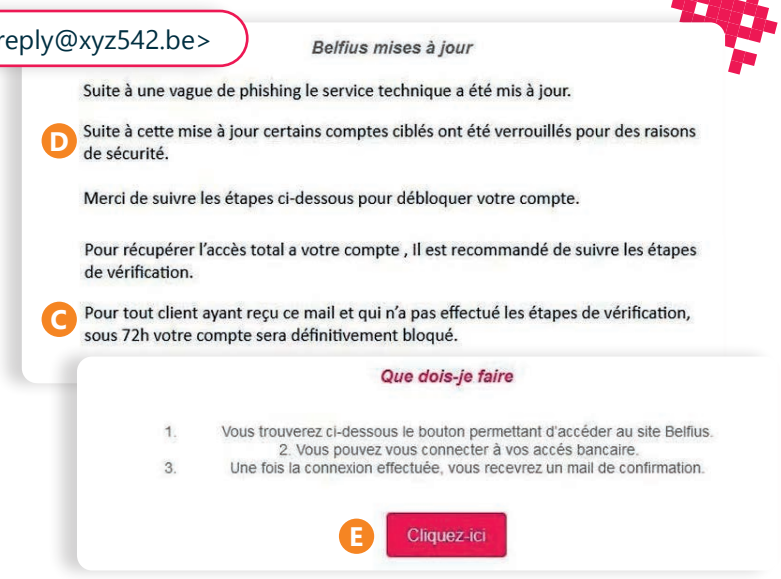
A. Si je ne suis pas client·e de cette banque l'information est plus que douteuse.

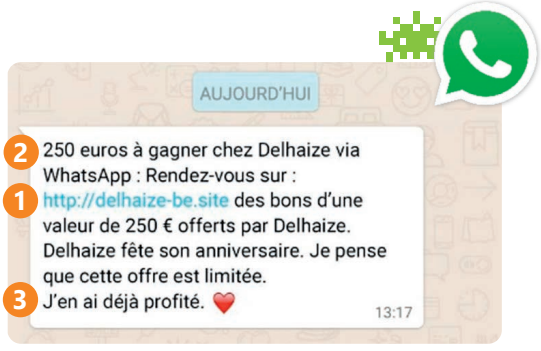
B. Vérifiez l'adresse e-mail. Si elle est étrange(@xyz542.be), **supprimez l'e-mail**.

C. **Urgence :** L'e-mail met une pression pour agir rapidement (et sans réfléchir). **Prenez le temps de réfléchir**.

D. Mail impersonnel (pas de nom).

E. **Lien douteux ?** Rendez-vous **sur le site** de la banque ou **utilisez l'application**.





Un message d'un supermarché reçu sur WhatsApp ???

1. Lien renvoyant vers un site web louche et non sécurisé (http://delhaize-be.site).
2. Bizarre pour Delhaize d'utiliser une messagerie instantanée.
3. Attention aux intermédiaires prétendant en avoir profité
   Qui est cette personne et pourquoi transmet-elle l'information ?
4. La promotion est trop belle pour être vraie.

Achats et ventes en ligne sur des sites d'annonces (objets d'occasion, Marketplace...)

Vous mettez en vente un canapé. Une personne vous contacte. Voici quelques signes qui doivent vous mettre en alerte :

1. Prise de contact rapide, discours impersonnel et utilisation de termes généraux pour décrire l'objet. Le message pourrait être repris pour n'importe quel **«article»**.
2. Un numéro de téléphone étranger (+225 = indicatif étranger).
3. L'acheteur·euse prétend vouloir vous envoyer l'argent par **« un transporteur »** (soit DPD, Mondial Relay, DHL, Fedex, etc.), pour gagner votre confiance – illusion de la sécurité en passant par des professionnels du transport de marchandises.
4. Ensuite, utilisation d'un stratagème, comme se faire passer pour la société de transport en demandant plus d'informations (personnelles et bancaires) **via un lien**, un **autre numéro** ou encore un **formulaire** pour soi-disant **« lancer la livraison »**.
5. C'est une arnaque au transporteur ! Les sociétés de livraison ne sont pas des intermédiaires financiers.

3. Comment se prémunir des arnaques en ligne ?

- **Vigilance :** Ne communiquez pas d'informations personnelles ou financières sans vérifier l'authenticité de la demande. (voir fiche 9.2. , 13.3. et 13.4.).
- **Faites preuve de prudence :** Si une offre semble trop belle pour être vraie, elle est probablement fausse (voir fiche 3.4.).
- **Mise à jour de vos logiciels :** Assurez-vous que tous vos logiciels, y compris votre antivirus, sont à jour (voir fiche 9.5. et 9.8.).
- **Protégez vos informations personnelles :** Utilisez des mots de passe forts (voir verso fiche 4.2.) et changez-les régulièrement. Ne partagez JAMAIS vos mots de passe.

4. Que faire si vous êtes victime d'une arnaque en ligne ?

Si vous pensez être victime d'une arnaque en ligne, **contactez immédiatement votre banque** si vous avez partagé des informations financières. Signalez l'incident à la police locale et au **Centre pour la Cybersécurité** via leur site web : https://cert.be/fr

CERT.be
The Federal Cyber Emergency Team

Police Fédérale

Safeonweb.be
Indice de Santé digitale

Prudence : en cas de doute, jouez la prudence. **Restez vigilant·e pour rester en sécurité en ligne !** Pour plus d'informations sur les arnaques en ligne et comment les prévenir, vous pouvez consulter :

- **le site de la Police Fédérale Belge** ou **safeonweb.be**
- **les contenus Surfons Tranquille**

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