GUIDE D'HYGIÈNE NUMÉRIQUE

Se protéger au quotidien contre le phishing, les messages piégés et les arnaques téléphoniques

ÉDITION BELGIQUE / UNION EUROPÉENNE · 2026

Les 3 signaux d'alarme universels

Presque toutes les arnaques — par téléphone, e-mail, SMS ou messagerie — combinent au moins un de ces trois leviers psychologiques. **Deux à la fois = raccrochez / supprimez immédiatement.**

L'URGENCE

« Vous avez 10 minutes ! »

« Compte bloqué », « dernier rappel », « colis retourné aujourd'hui », « virement en cours ». L'urgence vise à court-circuiter votre réflexion.

L'AUTORITÉ

« Police, banque, Card Stop… »

L'appelant se dit de votre banque, de la police, de Card Stop, du SPF Finances, d'itsme ou du « support technique ». Le numéro affiché peut être falsifié (spoofing).

LE CODE / SECRET

« Donnez le code reçu par SMS »

On vous demande un code SMS, un mot de passe, un code itsme, les données de votre carte, ou d'installer une application « de protection ». Personne de légitime ne demande cela.

Les 7 règles d'or

1. **Un code de confirmation ne se partage JAMAIS** — ni par téléphone, ni par SMS, ni « au support ». Un code sert à autoriser une opération : le donner, c'est signer.
2. **On raccroche, on rappelle soi-même** le numéro officiel (dos de la carte bancaire, site officiel tapé à la main).
3. **Jamais de lien cliqué dans un message non sollicité** — on ouvre l'application ou le site officiel soi-même.
4. **Peur + pression = arnaque.** Une administration ou une banque belge ne menace jamais par téléphone et laisse toujours le temps de vérifier.
5. **Ni la banque, ni Card Stop, ni la police** ne demandent codes, mots de passe ou transferts vers un « compte sécurisé ». Le « compte sécurisé » n'existe pas.
6. **Mot de passe unique + double authentification (2FA)** sur chaque compte important (e-mail, banque, itsme, messageries).
7. **Vérifier par un autre canal.** « Maman, nouveau numéro » ? Message vocal d'un proche ? Rappelez l'ancien numéro. Convenez d'un **mot de passe familial** secret.

Réflexes belges essentiels

Message suspect → transférez à **suspect@safeonweb.be** puis supprimez

Carte compromise → **Card Stop** **078 170 170** (24h/24) · Document d'identité → **Doc Stop** **00800 2123 2123**

Sources : Safeonweb / Centre pour la Cybersécurité Belgique, SPF Économie, Police Fédérale, Test-Achats, Banque de Russie & MVD (typologie des schémas), Kaspersky. Document informatif — 2026.

1 · Hygiène numérique quotidienne

🔑 Mots de passe & accès

- **12 caractères minimum**, unique pour chaque compte. Utilisez un **gestionnaire de mots de passe** (Bitwarden, KeePass, 1Password…) : une seule phrase maîtresse longue à retenir.
- **2FA partout** : e-mail, banque, itsme, Tax-on-web/CSAM, messageries, réseaux sociaux. Préférez une application d'authentification ou une clé physique au SMS.
- Vérifiez régulièrement les **sessions actives** de vos comptes et déconnectez les appareils inconnus.
- Compte e-mail principal = clé de tout le reste. Protégez-le en priorité.

📱 Appareils & logiciels

- **Mises à jour immédiates** du système, du navigateur et des applications : la plupart des infections exploitent des failles déjà corrigées.
- Applications **uniquement** depuis App Store / Google Play. Un fichier `.apk` reçu par messagerie n'est pas une photo : c'est un programme qui peut prendre le contrôle du téléphone (SMS, banque, clavier).
- **Sauvegardes régulières** (disque externe ou cloud chiffré) : votre assurance contre les rançongiciels et la perte du téléphone.
- Antivirus sur les téléphones des proches moins à l'aise : il bloque l'installation d'applications piégées.
- Verrouillage d'écran + chiffrement activés ; codes PIN différents pour le téléphone et la carte SIM.

🛡 Données personnelles

- **Minimisez votre empreinte** : pas de numéro de téléphone, d'adresse, de photos de documents (carte d'identité, billets, plaques) ni de géolocalisation en temps réel sur les réseaux sociaux. Les fraudeurs personnalisent leurs attaques avec ces données et les fuites de bases de données.
- Créez une **adresse e-mail secondaire** (et si possible un second numéro virtuel) pour les boutiques en ligne et inscriptions diverses.
- Le RGPD vous donne le droit de demander la **suppression de vos données** auprès de tout site européen.
- Google Alerts sur votre propre nom : détection précoce d'usurpation.

🌐 Réseaux & navigation

- Wi-Fi public : jamais d'opération bancaire ; utilisez un VPN de confiance (les VPN « gratuits » se paient souvent avec vos données).
- Tapez vous-même l'adresse de votre banque ou utilisez ses **favoris / application officielle** — jamais via un résultat sponsorisé ou un lien reçu.
- Vérifiez l'orthographe du domaine : `be1fius.be`, `arqenta.be`… un caractère change tout. Le cadenas HTTPS ne prouve **pas** qu'un site est honnête.
- Installez l'application **Safeonweb** : alertes officielles belges sur les campagnes de phishing en cours.

✅ Routine « 10 minutes par mois »

- Mises à jour faites ? Sauvegarde récente ?
- Sessions actives inconnues (e-mail, banque, Telegram/WhatsApp) ?
- Relevés bancaires : petits débits inconnus ?
- Un mot de passe faible remplacé.

2 · E-mails : reconnaître et neutraliser le phishing

Anatomie d'un e-mail piégé

Attention : l'IA a changé la donne — plus de fautes d'orthographe grossières. Un français parfait, un logo correct et même votre nom ne prouvent plus rien : seuls comptent **le domaine réel, le lien réel et la nature de la demande**.

✓ Les bons réflexes

- **Ne cliquez pas** : ouvrez vous-même le site ou l'app officielle (banque, bpost, eBox, MyPension…) pour vérifier si l'action existe vraiment.
- Une organisation légitime ne demande **jamais** mot de passe, code PIN, code de sécurité complet ou code à usage unique par e-mail ou téléphone.
- Doute sur un « collègue » ou « fournisseur » qui change de compte bancaire ? **Vérifiez par téléphone** au numéro connu (fraude au faux virement/CEO).
- Transférez le message à `suspect@safeonweb.be` puis supprimez-le : votre signalement fait bloquer les sites frauduleux.
- Sur smartphone, l'adresse complète et les liens sont masqués : en cas de doute, revérifiez sur un ordinateur avant d'agir.

✕ Si vous avez cliqué / répondu

- **Données de carte communiquées** → Card Stop **078 170 170** immédiatement, puis prévenez votre banque.
- **Mot de passe saisi** → changez-le partout où il est réutilisé, en commençant par l'e-mail ; déconnectez toutes les sessions ; activez la 2FA.
- **Pièce jointe ouverte** → antivirus complet ; en cas de doute, ne plus utiliser l'appareil pour la banque.
- **Argent débité** → banque + plainte à la police locale (voir page 6). En vertu des règles européennes (PSD2), les paiements **non autorisés** doivent en principe être remboursés (franchise max. 50 €) — sauf négligence grave, d'où l'importance de ne jamais donner ses codes.

3 · WhatsApp, Telegram, SMS : sécuriser ses messageries

⚙ Réglages indispensables (5 minutes)

- **Vérification en deux étapes** : WhatsApp → Compte → Vérification en deux étapes ; Telegram → Confidentialité → Mot de passe cloud. C'est LA protection contre le vol de compte.
- **Masquez** votre numéro, photo de profil et « vu à » pour les inconnus (Confidentialité).
- Interdisez l'**ajout automatique aux groupes** par des inconnus — c'est un canal d'arnaque majeur.
- Contrôlez la liste des **appareils connectés** et fermez les sessions inconnues.
- Filtrez / rendez silencieux les appels de numéros inconnus.

⚠ Le « quishing » (QR codes)

Les voleurs de comptes ne cherchent plus le code SMS : ils vous font **scanner un QR code** qui connecte LEUR appareil à VOTRE compte (affiches, faux chats de quartier, faux « Telegram Premium offert »). Scannez uniquement avec la fonction interne du messager et lisez l'avertissement : « rejoindre un groupe » ≠ « connecter un appareil ».

⊘ Pièges classiques en messagerie

- **« Mon code SMS est arrivé chez toi par erreur, renvoie-le »** → vol de compte instantané. Un code ne se transfère jamais.
- **« Maman/Papa, c'est mon nouveau numéro »** + demande d'argent urgente : rappelez l'ancien numéro. Très répandu en Belgique.
- Message d'un ami piraté : ton inhabituel, vouvoiement soudain, demande d'argent ou « vote pour moi » avec lien → appelez-le pour vérifier.
- « Support Telegram/WhatsApp Security » qui écrit en privé : les équipes officielles ne contactent jamais ainsi.
- Fichier « Photo » ou « Invitation » en `.apk` : malware de prise de contrôle.
- SMS « colis bloqué », « amende à payer », « eBox : nouveau message » avec lien : passez toujours par l'application ou le site officiel.

🔒 Compte volé ? Réagissez

Changez le mot de passe → fermez toutes les sessions → activez la 2FA → prévenez vos contacts (ils recevront des arnaques « de votre part ») → contactez le support du messager.

Deepfakes : la menace 2026

Une voix ou une vidéo **parfaitement imitée** d'un proche ou d'un chef peut être générée à partir de quelques secondes d'audio publié en ligne. Scénario type : message vocal paniqué, « pas le temps d'expliquer, ne me rappelle pas, vire l'argent ici ». Parade : **toujours rappeler soi-même** sur le numéro habituel, poser une question que seul le vrai proche connaît, et convenir en famille d'un **mot code secret** (« Dis-moi notre mot » — et ne jamais le divulguer ailleurs).

4 · Arnaques téléphoniques (vishing) : les schémas courants

Le vishing explose en Belgique : Safeonweb reçoit des vagues de signalements. Les centres d'appels frauduleux travaillent avec des scénarios écrits, des rôles multiples (« banquier », « policier », « technicien ») et des numéros falsifiés. Voici leur répertoire :

N°1 Le faux appel de la banque / Card Stop

« Transaction suspecte détectée, confirmez vos codes » ou message automatisé « Card Stop ». Variante finale : transférer l'argent vers un **« compte sécurisé »**. Réalité : Card Stop et les banques ne demandent **jamais** codes ou transferts. Le compte sécurisé n'existe pas — c'est le compte du voleur.

N°2 Le faux policier / la fausse fraude

« Votre compte est utilisé pour du blanchiment, collaborez à l'enquête, n'en parlez à personne (secret de l'instruction) ». On vous fait « protéger » votre argent en le déplaçant, ou remettre cartes/cash à un « coursier ». La police ne mène **aucune** enquête financière par téléphone et n'envoie personne chercher vos cartes.

N°3 Le colis / la livraison

Appel ou SMS « bpost/DPD » : frais de douane, adresse à confirmer, code à donner au « livreur ». Le code demandé ouvre en réalité votre compte (banque, itsme, boutique en ligne). Deuxième acte fréquent : rappel d'un « service anti-fraude » qui « constate » un piratage.

N°4 Le faux support technique

« Microsoft/votre opérateur » détecte un virus et fait installer un outil de prise en main à distance (AnyDesk, TeamViewer…). Une fois connectés, ils vident le compte bancaire. N'installez **jamais** un logiciel à la demande d'un appelant.

N°5 Le proche en détresse (+ deepfake)

« Grand-mère, j'ai eu un accident, il faut payer l'avocat » — parfois avec la **vraie voix clonée**. Pression émotionnelle maximale, demande de discrétion. Parade : raccrocher, rappeler le proche sur son numéro habituel, mot code familial.

N°6 Le faux investissement

« Plateforme crypto/actions » avec rendements garantis, faux tableaux de bord, « conseiller » attitré. Les gains sont fictifs ; pour « retirer », on exige des taxes et commissions sans fin. Vérifiez toute plateforme sur les **listes d'alerte de la FSMA** (fsma.be). Promesse de rendement garanti = fraude.

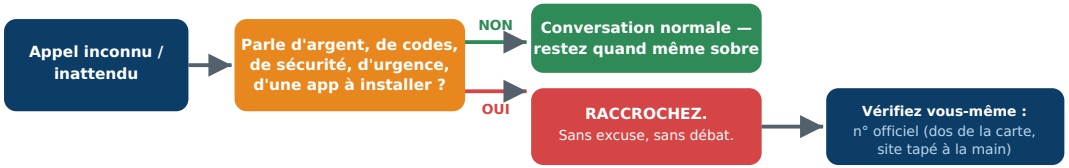
N°7 La mise en scène à étapes

Nouvelle génération : plusieurs appels successifs qui se « confirment » l'un l'autre (livreur → « Roskomnadzor »/« SPF » → « banquier » → « policier »), SMS en rafale pour créer la panique, fausse conversation de groupe très crédible. Plus le scénario est complexe et cohérent, plus il est suspect : les vraies administrations ne fonctionnent pas ainsi.

N°8 Divers : SIM swap, NFC, enquêtes

Duplication de votre carte SIM pour intercepter vos codes (protégez votre compte opérateur par mot de passe) ; « sondages » qui enregistrent votre voix (« dites oui ») ; demande d'approcher votre carte/téléphone d'un terminal. En cas de perte soudaine de réseau mobile sans raison : contactez votre opérateur immédiatement.

5 · Protocole de conduite : un appel inattendu arrive



- **Raccrocher n'est pas impoli** — c'est la réponse professionnelle recommandée par la Police Fédérale et Safeonweb. Ne rappelez jamais le numéro donné par l'appelant : cherchez-le vous-même.
- Ne dites pas « oui », ne « confirmez » rien, ne discutez pas : chaque minute de conversation donne aux fraudeurs des informations et un échantillon de votre voix.
- Le numéro affiché prouve rien (spoofing) : même « votre banque » à l'écran peut être un faux.
- Bloquez le numéro, activez le filtre anti-spam de votre opérateur ou une app de filtrage d'appels.
- Avec les proches vulnérables, instaurez la règle : **« tout appel qui parle d'argent → on raccroche et on m'appelle d'abord »**. Cette seule règle neutralise 90 % des schémas.

6 · Victime ou tentative ? Plan d'action Belgique

1. **Bloquez** : cartes → **Card Stop 078 170 170** (24h/24) ; accès banque en ligne → via votre banque ; carte d'identité/passeport perdu ou utilisé → **Doc Stop 00800 2123 2123**.
2. **Documentez** : captures d'écran, numéros, e-mails, extraits de compte, heures des appels.
3. **Contestez** auprès de votre banque toute opération non autorisée, par écrit et sans délai (droits PSD2 ; litige non résolu → médiateur Ombudsfin).
4. **Portez plainte** à la police locale (indispensable pour le remboursement et l'enquête). Certains faits se déclarent en ligne via Police-on-web.
5. **Signalez** : message frauduleux → `suspect@safeonweb.be` ; pratique commerciale trompeuse → SPF Économie (pointdecontact.belgique.be) ; fraude à l'investissement → FSMA.
6. **Nettoyez** : mots de passe changés (e-mail d'abord), sessions fermées, 2FA activée, appareil scanné, opérateur prévenu si SIM compromise.

NUMÉROS & ADRESSES À AFFICHER

Card Stop (cartes bancaires)
078 170 170

Doc Stop (documents d'identité)
00800 2123 2123

Phishing / messages suspects
suspect@safeonweb.be

Infos officielles : **safeonweb.be**
Arnaques conso : **pointdecontact.belgique.be**
Investissements : **fsma.be**
Urgence : **112** · Police : **101**

Sans honte. Ingénieurs, juristes, banquiers : tout le monde se fait piéger. Ce n'est pas un manque d'intelligence, c'est de la manipulation professionnelle. Signaler vite = limiter les dégâts et protéger les suivants.