



CHECKLIST IMPRIMABLE

Votre routine essentielle de sécurité numérique

Une fiche à cocher pour réduire les risques les plus courants sans compliquer votre quotidien. Commencez par vos accès les plus importants, puis adoptez le réflexe de pause face aux demandes suspectes.

Au sommaire

1. Protéger les comptes prioritaires
2. Garder les appareils et les fichiers protégés
3. Repérer les menaces et le bon réflexe
4. Les trois objectifs à garder en tête

1. Protéger les comptes prioritaires

- ☐ **Identifier ma messagerie principale comme compte prioritaire**
Elle reçoit souvent les alertes et les liens de réinitialisation des autres services.
- ☐ **Sécuriser mes comptes bancaires, mon stockage de fichiers et mes réseaux sociaux**
- ☐ **Protéger mon compte Apple, Google ou Microsoft**
- ☐ **Remplacer chaque mot de passe réutilisé par un mot de passe unique**
- ☐ **Activer l'authentification à plusieurs facteurs sur les comptes prioritaires**
Elle peut bloquer de nombreuses tentatives de connexion lorsqu'un mot de passe a fuité.

2. Garder les appareils et les fichiers protégés

- ☐ **Installer les mises à jour du système d'exploitation**
- ☐ **Mettre à jour le navigateur et les applications**
- ☐ **Conserver une copie séparée de mes documents et photos importants**
Cette sauvegarde reste utile en cas de panne, de perte, de vol ou de rançongiciel.
- ☐ **Inclure mon téléphone et ma box internet dans mes habitudes de sécurité**
La protection ne concerne pas uniquement l'ordinateur.

3. Repérer les menaces et le bon réflexe

Menace ou situation	Signaux à repérer	Réflexe utile
Hameçonnage ou faux site	Un message imite une organisation, un commerce ou un proche.	Ne pas cliquer dans la précipitation et vérifier avant de transmettre une information.
Message frauduleux	Urgence, peur, autorité ou promesse de gain.	Faire une pause avant toute action.
Demande de code ou de paiement	Le message réclame une information sensible ou pousse à payer.	Ne pas réagir par réflexe ; contrôler la demande.
Vol ou fuite de mot de passe	Une tentative de connexion vise un compte important.	Utiliser un mot de passe unique et l'authentification à plusieurs facteurs.
Panne, perte ou rançongiciel	Les fichiers ou l'appareil deviennent indisponibles.	Prévoir une sauvegarde séparée de l'appareil principal.

Vérifier une demande inhabituelle

Un réflexe simple en 3 étapes pour vous protéger et éviter les arnaques.

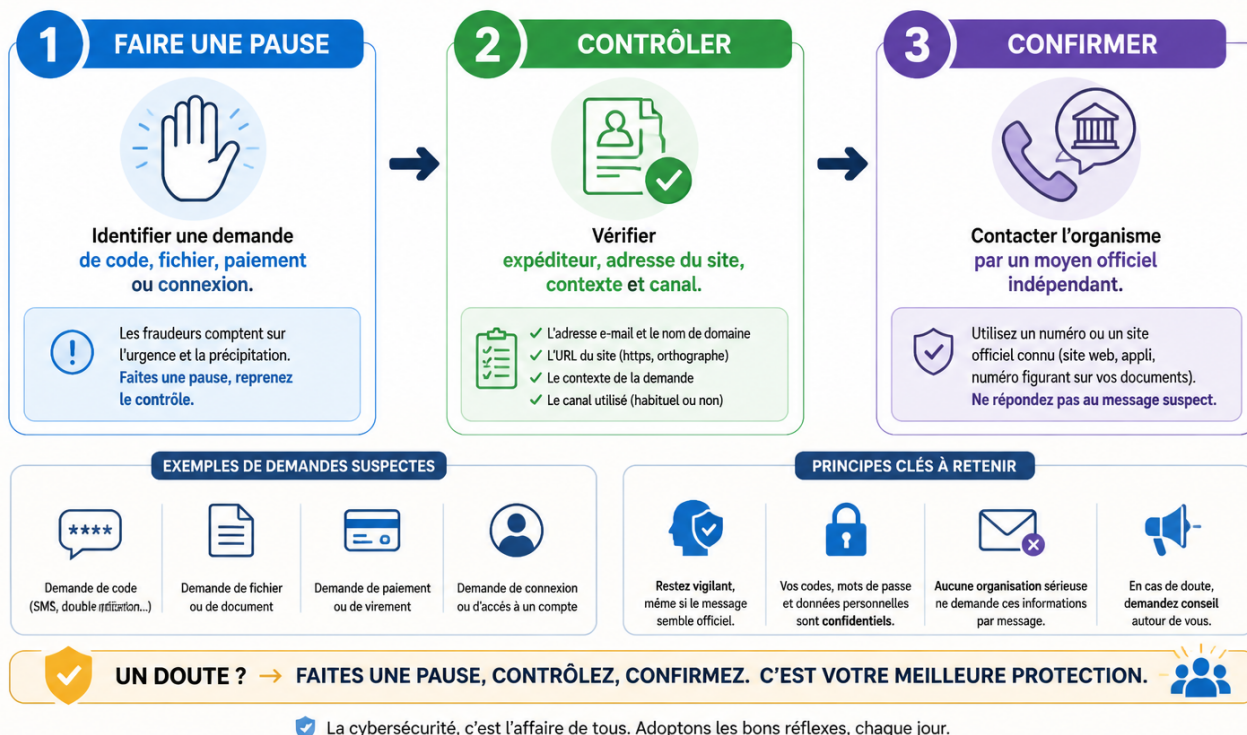


SCHÉMA Les étapes de vérification à suivre face à un message suspect.

! Le réflexe qui évite beaucoup d'erreurs

Un message qui crée l'urgence, demande un code ou vous pousse à payer doit déclencher une pause. Les arnaques exploitent souvent une décision prise trop vite plutôt qu'une faille technique complexe.

4. Les trois objectifs à garder en tête

Confidentialité : empêcher l'accès non autorisé à vos données et identifiants.

Disponibilité : pouvoir retrouver vos fichiers et vos services lorsque vous en avez besoin.

Intégrité : éviter la modification frauduleuse de vos fichiers ou de vos comptes.

La sécurité repose sur plusieurs protections qui se complètent : accès protégés, mises à jour, sauvegardes et vigilance.

À retenir : protégez d'abord les comptes qui permettent d'accéder aux autres, en particulier votre messagerie principale.