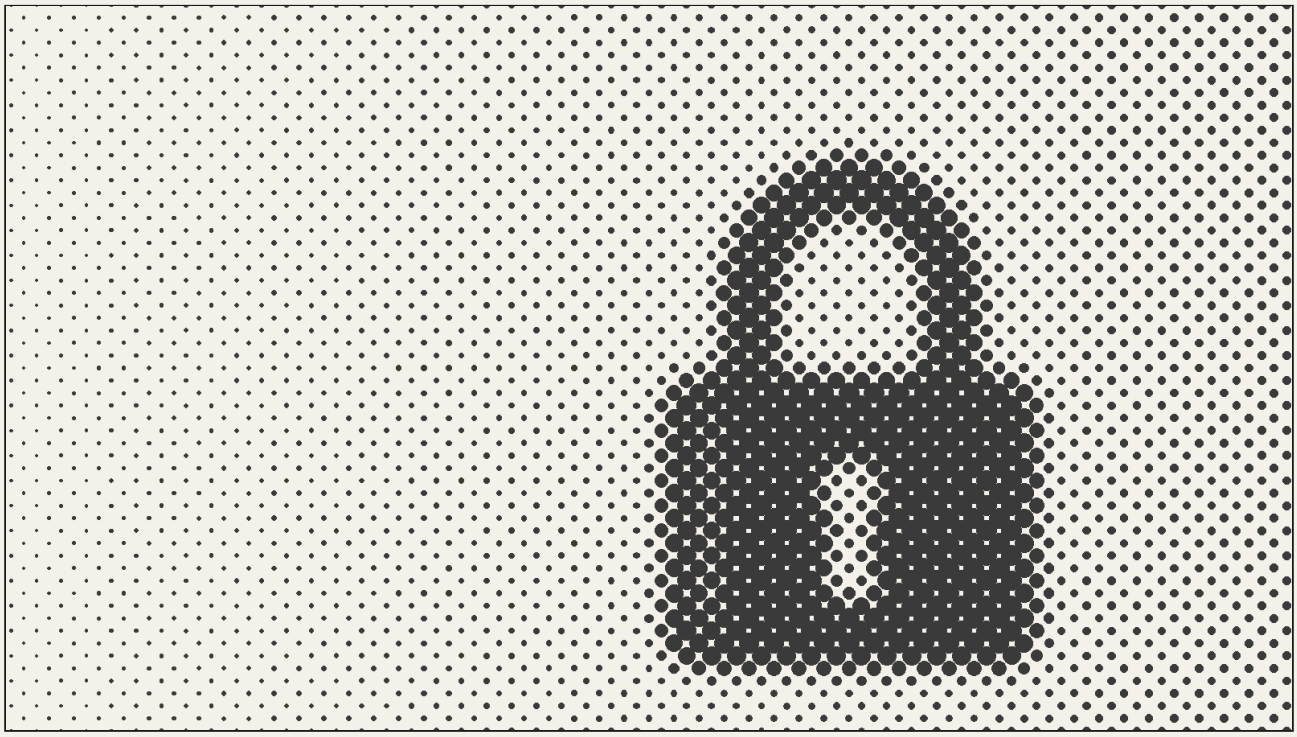


> Hygiène numérique en une heure

La checklist pour protéger l'essentiel, pas à pas, sans jargon et sans panique

En une heure, vous protégez votre adresse e-mail, votre téléphone, vos comptes les plus sensibles et vos photos. Vous n'avez besoin d'aucune connaissance technique, seulement d'un peu de temps et d'un stylo.

CARNET OFFERT

v1.0 · novembre 2026 · hu-tech.ch

> Mode d'emploi

CE GUIDE EST-IL POUR VOUS ?

Probablement, si vous vous reconnaissez dans au moins une de ces situations :

- Votre adresse e-mail a le même mot de passe que la boutique en ligne où vous avez commandé un jour une paire de chaussures.
- Votre téléphone vous propose une mise à jour depuis trois semaines, et vous appuyez chaque soir sur « Plus tard ».
- Vous avez reçu un SMS du genre « Votre colis est en attente, réglez 1,99 € de frais » et vous avez hésité une seconde avant de l'effacer.
- Vos photos de famille n'existent que sur votre téléphone.
- Vous savez que vous « devriez faire quelque chose » pour votre sécurité, mais vous ne savez pas par où commencer.

Ce guide vous donne un ordre précis : suivez les étapes une par une, sans chercher à tout comprendre d'avance.

CE QU'IL VOUS FAUT AVANT DE COMMENCER

- [ ] **Votre téléphone**, branché ou chargé à plus de la moitié. Certaines mises à jour refusent de démarrer quand la batterie est trop faible.
- [ ] **Votre ordinateur**, s'il vous sert à vos démarches en ligne, branché lui aussi.
- [ ] **Le code de déverrouillage de votre téléphone.**
- [ ] **Le mot de passe actuel de votre adresse e-mail principale.** Vérifiez-le maintenant en vous connectant depuis un navigateur. Si vous ne le connaissez plus, réglez ce point avant de commencer : l'étape 4 en dépend.
- [ ] **Un stylo et ce carnet imprimé**, ou ouvert sur une tablette où vous pouvez écrire.
- [ ] **Une heure sans interruption.** Un dimanche matin convient mieux que les dix minutes avant de partir au travail.

CE QUE CE GUIDE NE FAIT PAS

Il ne vous rend pas invulnérable. Personne ne l'est, pas même les entreprises qui dépensent des millions en sécurité. Il ferme les portes que les escrocs essaient en premier : mots de passe réutilisés, appareils pas à jour, comptes sans double vérification.

Il ne vous demande pas non plus de changer tous vos mots de passe aujourd'hui. Vous vous occupez de cinq à huit comptes importants. Les autres suivront au fil des semaines, à mesure que vous les utiliserez.

COMMENT LIRE CHAQUE ÉTAPE

Chaque étape suit la même structure, pour que vous sachiez toujours où vous en êtes :

- **Objectif** : ce que vous aurez obtenu à la fin de l'étape
- **Pourquoi** : la raison en une phrase, pour ne pas faire les choses à l'aveugle
- **Actions** : les gestes à faire, avec une case à cocher pour chacun
- **Piège à éviter** : l'erreur la plus fréquente à cette étape
- **Si vous bloquez** : quoi faire pour ne pas rester coincé

Si une étape vous prend plus de temps que prévu, notez où vous vous êtes arrêté et reprenez le lendemain. Mieux vaut sept étapes bien faites que neuf faites à la va-vite.

À PROPOS DES MENUS ET DES NOMS DE RÉGLAGES

Les chemins indiqués dans ce guide (par exemple « Réglages > Général > Mise à jour logicielle ») ont été vérifiés en novembre 2026. Les fabricants et les services en ligne renomment ou déplacent régulièrement leurs menus, et un même réglage peut porter un nom différent selon la marque de votre téléphone ou la version de votre système.

Si vous ne trouvez pas un menu, ouvrez les Réglages ou les Paramètres, touchez la loupe et tapez un mot-clé (« mise à jour », « sécurité », « mot de passe »). Vous trouverez presque toujours l'option, même si son nom diffère un peu de celui du guide.

> Sommaire

Chaque ligne est un lien : touchez ou cliquez un titre pour aller directement à sa page.

LE DÉROULÉ DE VOTRE HEURE

Étape	Ce que vous faites	Durée	Page
1	Lancer les mises à jour et vérifier le verrouillage	5 min	5
2	Lister vos comptes essentiels	5 min	7
3	Installer un gestionnaire de mots de passe	10 min	9
4	Sécuriser votre adresse e-mail principale	10 min	11
5	Sécuriser votre compte Apple ou Google	7 min	13
6	Activer la double vérification sur vos autres comptes essentiels	8 min	15
7	Vérifier si vos données ont fuité	5 min	17
8	Activer une sauvegarde automatique	5 min	19
9	Faire le tri dans vos applications	5 min	21

APRÈS LES ÉTAPES

Garder le cap : bilan et entretien	22
Je pense m'être fait pirater : la fiche réflexe	24
Reconnaître un message frauduleux	25
Ressources et mentions	26

POURQUOI CET ORDRE ?

Les mises à jour arrivent en premier parce qu'elles peuvent tourner seules pendant que vous faites le reste. Le gestionnaire de mots de passe vient avant tout changement de mot de passe, pour que vous ayez un endroit où ranger les nouveaux. Votre adresse e-mail passe avant les autres comptes, car elle sert à réinitialiser presque tous les autres : quelqu'un qui la contrôle peut faire « Mot de passe oublié » partout à votre place.

> Étape 1

Lancer les mises à jour et vérifier le verrouillage (5 min)

OBJECTIF

Vos appareils reçoivent les corrections de sécurité, et personne ne peut ouvrir votre téléphone s'il est perdu ou volé.

POURQUOI

Quand un fabricant découvre une faille, il la corrige dans une mise à jour. Tant que vous ne l'installez pas, la faille reste ouverte chez vous, alors qu'elle est désormais connue de tous, escrocs compris.

ACTIONS

- [ ] **Lancez la mise à jour du téléphone.** Laissez-le branché et passez à la suite pendant qu'il travaille.
  `iPhone : Réglages > Général > Mise à jour logicielle`
  `Samsung : Paramètres > Mise à jour du logiciel > Téléchargement et installation`
  Autre Android : ouvrez les Paramètres, touchez la loupe et tapez « mise à jour ». Les menus changent d'une marque à l'autre, mais la recherche les trouve toujours.

- [ ] **Lancez la mise à jour de l'ordinateur.**
  `Mac : menu Pomme > Réglages Système > Général > Mise à jour de logiciels`
  `Windows : Démarrer > Paramètres > Windows Update > Rechercher des mises à jour`

- [ ] **Vérifiez votre navigateur.** En ouvrant cette page, le navigateur cherche lui-même une nouvelle version. S'il en trouve une, cliquez sur « Relancer ». Safari se met à jour avec le Mac, vous n'avez rien à faire.
  `Chrome : menu ⋮ > Aide > À propos de Google Chrome`
  `Firefox : menu ≡ > Aide > À propos de Firefox`
  `Edge : menu … > Aide et commentaires > À propos de Microsoft Edge`

- [ ] **Activez les mises à jour automatiques**, pour ne plus y penser. Sur Mac et Windows, l'option se trouve sur la même page que la mise à jour.
  `iPhone : Réglages > Général > Mise à jour logicielle > Mises à jour automatiques`

- [ ] **Vérifiez le code de votre téléphone.** Il doit compter au moins 6 chiffres. Évitez ceux que tout le monde essaie en premier : 123456, 000000, 111111, 121212, votre année de naissance ou la date de naissance d'un enfant. Un code comme 4 8 2 9 1 6, tiré au hasard, s'oublie moins vite qu'on ne le croit après trois jours d'usage. Le déverrouillage par empreinte ou par visage reste un bon complément au quotidien.

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

☐ **Activez la localisation en cas de perte.**

iPhone : Réglages > touchez votre nom > Localiser > Localiser mon iPhone

Android : Paramètres, loupe, tapez « localiser »

[!] PIÈGE À ÉVITER

Éteindre ou débrancher un appareil pendant une mise à jour. Une mise à jour interrompue peut bloquer l'appareil. Si elle semble figée, attendez au moins une demi-heure avant de vous inquiéter.

[?] SI VOUS BLOQUEZ

Votre téléphone affiche qu'il est à jour alors que la dernière mise à jour date de plusieurs années ? Il ne reçoit probablement plus de mises à jour de sécurité. Notez-le dans « Ce qui reste à faire », à la fin du carnet. Vous pouvez continuer le guide, mais le remplacement de cet appareil devra entrer dans vos projets des prochains mois.

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

> Étape 2

Lister vos comptes essentiels (5 min)

OBJECTIF

Savoir exactement quels comptes protéger aujourd'hui.

POURQUOI

Vous avez sans doute des dizaines de comptes en ligne, mais une poignée d'entre eux suffit à prendre le contrôle des autres ou à vider votre compte bancaire. Vous commencez par ceux-là.

ACTIONS

Remplissez la grille. Une ligne d'exemple vous montre comment faire. Dans la dernière colonne, « Je ne sais pas » est une réponse parfaitement valable : vous vérifierez aux étapes 4 à 6.

Compte	Adresse e-mail liée	Double vérification ?
Exemple : Gmail	*marie.dupont@gmail.com*	*Je ne sais pas*
Mon adresse e-mail principale		
Mon compte Apple ou Google		
Ma banque en ligne		
Mon opérateur téléphonique		
Mon réseau social principal		
Une boutique où ma carte est enregistrée		

Pour chaque ligne, voici à quoi penser :

- **Adresse e-mail principale** : celle que vous donnez partout (Gmail, Outlook, Bluewin, Orange, Free, Proton…). Si vous en avez deux, notez les deux.
- **Compte Apple ou Google** : celui qui gère votre téléphone, vos photos et vos achats d'applications. Sur un téléphone Samsung, il peut aussi exister un compte Samsung : notez-le.
- **Banque en ligne** : l'application ou le site où vous consultez votre compte.

- **Opérateur téléphonique** : Swisscom, Sunrise, Salt, Orange, SFR, Bouygues, Free… Votre espace client compte, car un escroc qui obtient une nouvelle carte SIM à votre nom reçoit vos codes de sécurité par SMS.
- **Réseau social principal** : celui qu'un usurpateur utiliserait pour demander de l'argent à vos proches en se faisant passer pour vous.
- **Boutique avec carte enregistrée** : Amazon, Galaxus, Zalando, la Fnac… Choisissez celle où vous achetez le plus souvent.

ASTUCE

Vous ne savez plus où vous avez des comptes ? Cherchez dans votre boîte e-mail les mots « Bienvenue » ou « Confirmez votre adresse ». Vous retrouverez la plupart de vos inscriptions, même anciennes.

[!] PIÈGE À ÉVITER

Vouloir tout lister. Arrêtez-vous à huit lignes au maximum. Les autres comptes viendront plus tard.

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

> Étape 3

Installer un gestionnaire de mots de passe (10 min)

OBJECTIF

Vous avez un coffre-fort numérique où ranger tous vos mots de passe, et vous n'avez plus qu'un seul mot de passe à retenir.

POURQUOI

Quand un site se fait pirater, les escrocs essaient aussitôt le couple e-mail et mot de passe volé sur d'autres sites (Gmail, Amazon, PayPal…). Si vous utilisez le même mot de passe partout, une fuite sur un petit site de recettes peut ouvrir votre messagerie.

CHOISISSEZ VOTRE GESTIONNAIRE

	Bitwarden	Proton Pass
Prix	Version gratuite complète pour un usage personnel	Version gratuite suffisante pour commencer
Code source	Ouvert, examiné par des experts indépendants	Ouvert, examiné par des experts indépendants
Origine	Entreprise américaine, avec un hébergement possible en Europe	Entreprise suisse, basée à Genève
Pour qui	Vous voulez l'outil le plus répandu et le plus éprouvé	Vous utilisez déjà Proton Mail, ou vous préférez un acteur européen

Les deux font très bien le travail. Si vous hésitez encore au bout d'une minute, prenez Bitwarden et passez à la suite. Vous pourrez changer plus tard, car les deux permettent d'exporter vos données.

ACTIONS

- [ ] **Créez votre compte** sur bitwarden.com ou proton.me/pass. Avec Bitwarden, choisissez la région « Europe » au moment de l'inscription si vous préférez que vos données chiffrées restent en Europe.
- [ ] **Choisissez votre phrase de passe maîtresse.** Prenez quatre ou cinq mots sans aucun lien entre eux et ajoutez un chiffre, par exemple : *tulipe-girafe-fourchette-orage-27*. Une phrase de ce genre se retient en quelques jours, et un ordinateur mettrait des siècles à la deviner. À éviter : une citation connue, un vers de chanson, le nom de votre chien suivi de votre année de naissance. (N'utilisez pas l'exemple de ce guide, qui est désormais public.)

- [ ] **Écrivez cette phrase sur papier** et rangez-la chez vous, dans un endroit sûr : avec vos papiers importants, pas sur un post-it collé à l'écran. Ne la photographiez pas et ne l'enregistrez pas dans vos notes de téléphone.
- [ ] **Installez l'application sur votre téléphone** depuis l'App Store ou le Play Store, et connectez-vous.
- [ ] **Installez l'extension dans votre navigateur** sur l'ordinateur. Elle proposera de remplir vos mots de passe et d'enregistrer les nouveaux.
- [ ] **Autorisez le remplissage automatique sur le téléphone.** L'application vous guide au premier lancement. Sinon, ouvrez les Réglages ou Paramètres, touchez la loupe et tapez « remplissage » ou « mots de passe ».

[!] PIÈGE À ÉVITER

Importer et trier tous vos anciens mots de passe maintenant. Vous y passeriez la soirée. Aujourd'hui, le coffre ne contiendra que les quelques comptes de votre liste de l'étape 2. Les autres y entreront au fil de vos connexions : à chaque fois que vous vous connectez à un site, le gestionnaire vous propose d'enregistrer le mot de passe.

[?] SI VOUS BLOQUEZ

L'installation ne fonctionne pas, ou tout cela vous semble trop pour aujourd'hui ? Utilisez le gestionnaire déjà présent sur votre téléphone (l'app Mots de passe sur iPhone, le Gestionnaire de mots de passe de Google sur Android). Il vaut largement mieux que des mots de passe réutilisés. Vous pourrez passer à Bitwarden ou Proton Pass plus tard.

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

> Étape 4

Sécuriser votre adresse e-mail principale (10 min)

OBJECTIF

Votre adresse e-mail a un mot de passe unique, une double vérification et des codes de secours rangés en lieu sûr.

POURQUOI

Sur presque tous les sites, le lien « Mot de passe oublié ? » envoie un e-mail. La personne qui contrôle votre messagerie peut donc réinitialiser vos autres comptes, un par un.

Les exemples ci-dessous concernent Gmail et Outlook. Pour une autre messagerie (Bluewin, Orange, Free, Proton Mail…), cherchez la rubrique « Sécurité » de votre compte : les réglages portent des noms très proches.

ACTIONS

- [ ] **Changez le mot de passe, en commençant par le gestionnaire.** L'ordre compte ici :
    1. Dans votre gestionnaire, créez une entrée pour votre messagerie et utilisez le générateur pour créer un mot de passe d'au moins 20 caractères.
    2. Enregistrez l'entrée.
    3. Copiez ce mot de passe et collez-le dans le formulaire de changement de votre messagerie.

    `Gmail : myaccount.google.com > Sécurité > Mot de passe`
    `Outlook : account.microsoft.com > Sécurité > Modifier mon mot de passe`
    Dans cet ordre, le nouveau mot de passe ne peut pas se perdre entre deux fenêtres. Vos autres appareils vous demanderont ensuite de vous reconnecter : c'est normal, le gestionnaire remplira le mot de passe pour vous.
- [ ] **Activez la double vérification.** On l'appelle aussi « double authentification », « validation en deux étapes » ou « 2FA ». En plus du mot de passe, le service vous demande une preuve que c'est bien vous : un code à six chiffres, une confirmation sur votre téléphone, ou votre empreinte.
    `Gmail : myaccount.google.com > Sécurité > Validation en deux étapes`
    `Outlook : account.microsoft.com > Sécurité > Options de sécurité avancées`
    Si le service vous propose une **clé d'accès** (passkey), acceptez-la : vous vous connecterez avec votre empreinte ou votre visage, et aucun faux site ne pourra vous la voler. Sinon, choisissez une **application d'authentification**, de préférence séparée de votre gestionnaire de mots de passe pour ne pas mettre toutes vos clés dans le même coffre. Deux options fiables et gratuites : **Proton Authenticator**, de l'entreprise suisse

qui édite Proton Pass, et **Ente Auth**, open source. Le SMS arrive en dernier, mais il vaut toujours mieux que rien.

- [ ] **Enregistrez vos codes de secours.** Le service vous donne une série de codes à usage unique (Google en fournit dix). Ils vous permettent d'entrer dans votre compte si vous perdez votre téléphone. Copiez-les dans votre gestionnaire, dans la note de l'entrée de votre messagerie. Imprimez-les ou recopiez-les aussi sur papier, et rangez-les avec votre phrase de passe maîtresse.

- [ ] **Vérifiez vos moyens de récupération.** Le numéro de téléphone et l'adresse e-mail de secours doivent être les vôtres et toujours valables. Un ancien numéro professionnel ou l'adresse d'un ex-conjoint donne à quelqu'un d'autre une porte d'entrée sur votre compte.
  `Gmail : myaccount.google.com > Sécurité > Comment vous connecter à Google`

- [ ] **Déconnectez les appareils inconnus.** Parcourez la liste des appareils connectés à votre compte. Un « Windows, Lyon » alors que vous n'avez jamais mis les pieds à Lyon mérite une déconnexion immédiate.
  `Gmail : myaccount.google.com > Sécurité > Vos appareils`

- [ ] **Vérifiez qu'aucun transfert automatique n'a été ajouté.** Une technique d'escroc courante consiste à créer, en silence, une règle qui copie tous vos e-mails vers son adresse. Si vous y trouvez une adresse que vous ne connaissez pas, supprimez la règle et refaites le changement de mot de passe.
  `Gmail : Paramètres (roue dentée) > Voir tous les paramètres > onglets « Transfert et POP/IMAP » puis « Filtres et adresses bloquées »`

[!] PIÈGE À ÉVITER

Activer la double vérification sans garder les codes de secours. Si vous perdez ou changez de téléphone, vous risquez de ne plus jamais pouvoir entrer dans votre compte. C'est le blocage le plus fréquent, et le plus pénible à résoudre.

[?] SI VOUS BLOQUEZ

Votre messagerie ne propose pas de double vérification ? C'est le cas de certaines adresses anciennes fournies par les opérateurs. Gardez au minimum le nouveau mot de passe unique, et notez dans « Ce qui reste à faire » de réfléchir à une adresse plus moderne pour vos comptes importants.

> Étape 5

Sécuriser votre compte Apple ou Google (7 min)

OBJECTIF

Le compte qui contrôle votre téléphone, vos photos et vos achats est protégé comme votre messagerie.

POURQUOI

Ce compte permet d'effacer votre téléphone à distance, de lire vos sauvegardes et de voir vos photos. Entre de mauvaises mains, il donne accès à une bonne partie de votre vie.

SI VOUS AVEZ UN IPHONE

- [ ] **Changez le mot de passe de votre compte Apple** avec la même méthode qu'à l'étape 4 : d'abord une nouvelle entrée dans le gestionnaire, ensuite le changement.
  `Réglages > touchez votre nom > Connexion et sécurité > Changer le mot de passe`
- [ ] **Vérifiez que la double vérification est active.** Sur la même page, la ligne « Identification à deux facteurs » doit indiquer « Activée ». Sur la plupart des comptes récents, c'est déjà le cas.
- [ ] **Ajoutez un contact de récupération** : une personne de confiance (un conjoint, un frère, une amie proche) qui pourra vous aider à récupérer votre compte si vous perdez l'accès. Elle ne verra jamais vos données.
  `Réglages > touchez votre nom > Connexion et sécurité > Récupération du compte`
- [ ] **Activez la protection en cas de vol.** Si un voleur vous a vu taper votre code dans le tram puis vous arrache le téléphone, il ne pourra pas changer votre mot de passe Apple sans votre visage ou votre empreinte.
  `Réglages > Face ID et code > Protection en cas de vol de l'appareil`
- [ ] **Faites le tri dans vos appareils.** Tout en bas de la page qui s'ouvre quand vous touchez votre nom, la liste montre chaque appareil lié à votre compte. Retirez l'ancien iPad revendu en 2022 ou l'iPhone que vous avez donné à votre neveu.

SI VOUS AVEZ UN TÉLÉPHONE ANDROID

Votre compte Google est souvent le même que votre Gmail. Dans ce cas, vous avez déjà fait l'essentiel à l'étape 4 : il vous reste deux vérifications.

- [ ] **Lancez le Check-up Sécurité de Google.** En deux minutes, il vous signale les problèmes et vous propose de les corriger, un par un.
  `myaccount.google.com/security-checkup`

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

- [ ] **Retirez les applications qui n'ont plus besoin d'accéder à votre compte.** Ce jeu essayé une fois en 2020 ou ce service de cartes de vœux n'ont plus de raison de lire vos données.

  `myaccount.google.com > Sécurité > Vos connexions à des applications et services tiers`

- [ ] **Si vous avez un compte Samsung**, vérifiez le mot de passe et la double vérification de la même façon.

  `Paramètres > touchez votre nom en haut de l'écran > Sécurité et confidentialité`

[!] PIÈGE À ÉVITER

Retirer de la liste un appareil que vous utilisez encore, comme votre ordinateur ou la tablette de la cuisine. En cas de doute, ne touchez à rien : un appareil que vous reconnaissez n'est pas un danger.

[?] SI VOUS BLOQUEZ

Vous ne trouvez pas un réglage ? Tapez son nom dans la loupe des Réglages. Votre compte Apple ou Google vous demande un code envoyé sur un ancien numéro ? Arrêtez-vous là pour cette étape et notez-le dans « Ce qui reste à faire ». Ce problème se règle avec le support d'Apple ou de Google, et il prend souvent plusieurs jours.

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

> Étape 6

Activer la double vérification sur vos autres comptes essentiels (8 min)

OBJECTIF

Chaque compte de votre liste de l'étape 2 est protégé par autre chose qu'un simple mot de passe.

POURQUOI

Un mot de passe peut fuiter sans que vous le sachiez. La double vérification oblige l'escroc à avoir aussi votre téléphone, ce qu'il n'a presque jamais.

QUELLE MÉTHODE CHOISIR ?

De la plus solide à la moins solide. Prenez la méthode la plus solide que le service propose.

Méthode	Comment ça marche	Niveau
Clé d'accès (passkey)	Votre empreinte ou votre visage remplace le mot de passe	Très solide
Application d'authentification	Un code à six chiffres qui change toutes les 30 secondes	Solide
Confirmation dans l'application du service	Vous touchez « Oui, c'est moi » dans l'app de la banque, par exemple	Solide
SMS	Un code reçu par message	Correct, toujours mieux que rien

ACTIONS

Reprenez votre grille de l'étape 2 et complétez la dernière colonne au fur et à mesure.

- [ ] **Votre banque.** La double vérification y est presque toujours obligatoire. Vérifiez seulement deux choses : l'application de validation de votre banque fonctionne sur votre téléphone actuel, et le numéro de téléphone de votre banque est noté sur papier (vous le trouvez au dos de votre carte bancaire). En cas de doute sur un appel ou un message, c'est ce numéro-là que vous appelez, jamais celui qu'on vous donne. Retenez aussi cette règle : votre banque ne vous demandera jamais un code de validation par téléphone, par SMS ou par e-mail. Toute personne qui le demande est un escroc, même si elle connaît votre nom et votre numéro de compte.
- [ ] **Votre opérateur téléphonique.** Connectez-vous à votre espace client (Swisscom, Sunrise, Salt, Orange, SFR, Bouygues, Free…). Changez le mot de passe avec votre gestionnaire et activez la double vérification si elle existe. Demandez aussi au service client s'il est possible d'ajouter un mot de passe ou un code exigé avant tout

changement de carte SIM. Cette protection empêche un escroc de se faire remettre une carte SIM à votre nom, et donc de recevoir vos codes SMS.

- [ ] **Votre réseau social principal.** Pour les autres réseaux, cherchez « sécurité » ou « deux facteurs » dans les paramètres.
  `Facebook et Instagram : Paramètres > Espace Comptes > Mot de passe et sécurité > Authentification à deux facteurs`

- [ ] **Votre boutique avec carte enregistrée.** Si la boutique ne propose pas de double vérification, supprimez votre carte enregistrée et saisissez-la à chaque achat. Vous perdez trente secondes par commande, et un pirate ne pourra pas commander à vos frais.
  `Amazon : Votre compte > Connexion et sécurité > Vérification en deux étapes`

[!] PIÈGE À ÉVITER

Valider une demande de connexion que vous n'avez pas faite. Si votre téléphone affiche « Est-ce bien vous qui essayez de vous connecter ? » alors que vous regardez un film, refusez. Quelqu'un connaît votre mot de passe : changez-le dans la foulée.

[?] SI VOUS MANQUEZ DE TEMPS

Arrêtez-vous après la banque et l'opérateur. Notez le reste dans « Ce qui reste à faire » et finissez dans la semaine.

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

> Étape 7

Vérifier si vos données ont fuité (5 min)

OBJECTIF

Vous savez si votre adresse e-mail apparaît dans des fuites de données connues, et vous avez changé les mots de passe concernés.

POURQUOI

Quand un site se fait pirater, la liste de ses utilisateurs circule ensuite sur Internet, parfois pendant des années. Vous ne pouvez pas empêcher une fuite chez les autres, mais vous pouvez faire en sorte qu'elle ne vous coûte rien.

ACTIONS

- [ ] **Rendez-vous sur haveibeenpwned.com** (en anglais, gratuit, géré par un chercheur en sécurité reconnu). Tapez votre adresse e-mail principale et validez.
- [ ] **Lisez le résultat.** Le site affiche la liste des fuites où votre adresse apparaît, avec la nature des données volées. Vous y verrez par exemple « Bouygues Telecom » (2025), où les escrocs ont obtenu noms, adresses, dates de naissance et IBAN, ou « Substack » (2025), où ils ont obtenu des adresses e-mail et des numéros de téléphone.
- [ ] **Pour chaque fuite qui contient un mot de passe**, posez-vous une seule question : est-ce que j'utilise encore ce mot de passe, sur ce site ou ailleurs ? Si oui, changez-le partout où vous l'utilisez, avec votre gestionnaire. Si non, ou si vous avez supprimé ce compte depuis longtemps, vous n'avez rien à faire.
- [ ] **Si la fuite contient seulement votre adresse e-mail ou votre téléphone**, aucun changement n'est nécessaire. Attendez-vous simplement à recevoir plus de messages frauduleux, et soyez plus méfiant pendant quelques mois.
- [ ] **Activez les alertes gratuites** sur la page d'accueil du site, pour être prévenu par e-mail si votre adresse apparaît dans une nouvelle fuite.
- [ ] **Répétez l'opération** avec votre deuxième adresse, si vous en avez une.

Votre gestionnaire de mots de passe propose peut-être aussi un outil qui surveille les fuites et repère les mots de passe réutilisés. Cherchez une rubrique « Surveillance », « Rapports » ou « Santé des mots de passe » dans l'application.

CAS PARTICULIER : LES « STEALER LOGS »

Si une fuite porte un nom contenant « Stealer Logs », vos identifiants ont été volés par un logiciel espion installé sur un appareil, le plus souvent un ordinateur. Le site qui gère votre compte n'est pas en cause. Dans ce cas, changer le mot de passe ne suffit pas : faites aussi analyser l'ordinateur que vous utilisiez à l'époque par un antivirus à jour (celui intégré à Windows suffit pour commencer), ou demandez de l'aide à un professionnel. Sinon, le logiciel espion volera aussi votre nouveau mot de passe.

[!] PIÈGE À ÉVITER

Paniquer devant une longue liste. La plupart des personnes qui utilisent Internet depuis dix ans apparaissent dans plusieurs fuites. Le résultat ne dit pas que vous êtes piraté : il vous dit quels anciens mots de passe ne plus utiliser.

[?] SI VOUS BLOQUEZ

Le site est en anglais et vous gêne ? Votre navigateur peut traduire la page : un clic droit puis « Traduire en français » dans Chrome et Edge, ou l'icône de traduction dans la barre d'adresse de Firefox.

> Étape 8

Activer une sauvegarde automatique (5 min)

OBJECTIF

Vos photos et vos documents existent à au moins deux endroits, et cette copie se fait sans vous.

POURQUOI

Un téléphone tombe dans le lac, un ordinateur refuse de démarrer un lundi matin, un virus chiffre vos fichiers. Avec une sauvegarde, chacune de ces situations devient un ennui. Sans sauvegarde, vous risquez de perdre dix ans de photos de famille.

> SYNCHRONISATION OU SAUVEGARDE ?
> La différence piège beaucoup de monde. Une synchronisation (iCloud Drive, Google Drive, OneDrive, Dropbox) recopie chaque changement partout : si vous effacez un fichier sur votre ordinateur, il disparaît aussi de votre téléphone et du cloud. Une sauvegarde garde une copie à part, que vos erreurs n'atteignent pas. La synchronisation reste pratique, mais elle ne remplace pas une sauvegarde.

ACTIONS

- [ ] **Activez la sauvegarde du téléphone.**
  `iPhone : Réglages > touchez votre nom > iCloud > Sauvegarde iCloud`
  `Android : Paramètres, loupe, tapez « sauvegarde »`
  L'espace gratuit (5 Go chez Apple, 15 Go chez Google, partagés avec vos e-mails) suffit rarement si vous prenez beaucoup de photos. Le téléphone vous le signalera. Vous aurez alors le choix entre un petit abonnement et une sauvegarde de vos photos sur l'ordinateur ou sur un disque externe.
- [ ] **Choisissez une sauvegarde pour l'ordinateur.** La solution la plus simple, et qui ne dépend d'aucun cloud, reste un disque dur externe, qui coûte quelques dizaines d'euros. Sur Mac, branchez le disque : le Mac vous propose de l'utiliser avec Time Machine. Acceptez. Sur Windows, ouvrez les Paramètres, tapez « sauvegarde » dans la recherche et suivez l'outil proposé.
  Vous n'avez pas de disque sous la main ? Notez-le dans « Ce qui reste à faire » et passez à la suite. Vous ferez cette action à réception du disque.
- [ ] **Testez une restauration.** Choisissez une photo au hasard, retrouvez-la dans votre sauvegarde et ouvrez-la. Une sauvegarde que vous n'avez jamais testée reste une promesse, pas une certitude.

POUR ALLER PLUS LOIN : LA RÈGLE 3-2-1

Les professionnels conseillent 3 copies de vos données, sur 2 supports différents, dont 1 hors de chez vous. Par exemple : les photos sur votre téléphone, une copie sur un disque externe à la maison, et une copie dans le cloud ou sur un disque rangé chez un proche. Vous n'avez pas besoin d'y arriver aujourd'hui : une seule sauvegarde automatique vous protège déjà de la plupart des pertes.

[!] PIÈGE À ÉVITER

Laisser le disque de sauvegarde branché en permanence à l'ordinateur. Un virus qui chiffre vos fichiers peut aussi chiffrer le disque. Branchez-le une fois par semaine, le temps de la sauvegarde, puis débranchez-le.

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

> Étape 9

Faire le tri dans vos applications (5 min)

OBJECTIF

Votre téléphone ne garde que les applications que vous utilisez, et chacune n'accède qu'à ce dont elle a besoin.

POURQUOI

Chaque application installée peut contenir une faille, et beaucoup collectent plus de données qu'elles n'en ont besoin. Une application de lampe torche n'a aucune raison de lire vos contacts.

ACTIONS

- [ ] **Supprimez les applications inutilisées.** Bonne règle : une application que vous n'avez pas ouverte depuis six mois peut partir. Vous pourrez toujours la réinstaller.
  `iPhone : Réglages > Général > Stockage iPhone (date de dernière utilisation de chaque app)`
  Android : ouvrez le Play Store, touchez votre photo de profil, puis cherchez la gestion des applications. Certaines versions permettent de trier par « Les moins utilisées ».

- [ ] **Revoyez l'accès à votre position.**
  `iPhone : Réglages > Confidentialité et sécurité > Service de localisation`
  `Android : Paramètres, loupe, tapez « autorisations » ou « localisation »`
  Pour chaque application, choisissez la réponse la plus restrictive qui lui permet de fonctionner :
  - **Jamais** : la plupart des jeux, les applications d'achat, les réseaux sociaux
  - **Lorsque l'app est active** : les cartes, la météo, les applications de transport
  - **Toujours** : presque aucune application n'en a vraiment besoin

  Pour la météo, désactivez aussi « Position exacte » : votre ville suffit à prévoir la pluie.

- [ ] **Vérifiez le micro, la caméra et les contacts.** Dans le même menu de confidentialité, ouvrez chaque catégorie et retirez l'accès aux applications qui n'ont pas de raison évidente de l'avoir. Une application de visioconférence a besoin du micro, pas un jeu de cartes.

[!] PIÈGE À ÉVITER

Tout couper d'un coup, puis s'étonner que la carte ne trouve plus votre position ou que l'application de la banque refuse de scanner un QR code. Si une application cesse de fonctionner, elle vous redemandera l'autorisation, et vous pourrez l'accorder en connaissance de cause.

Menus vérifiés en novembre 2026. Ils peuvent différer selon votre appareil et sa version.

> Garder le cap

VOTRE BILAN

Vous avez terminé. Cochez ce que vous avez fait :

- ☐ 1. Mes appareils sont à jour et se mettent à jour seuls
- ☐ 2. J'ai listé mes comptes essentiels
- ☐ 3. J'ai un gestionnaire de mots de passe et ma phrase maîtresse est rangée sur papier
- ☐ 4. Mon adresse e-mail principale est protégée par une double vérification et mes codes de secours sont rangés
- ☐ 5. Mon compte Apple ou Google est protégé
- ☐ 6. Ma banque, mon opérateur, mon réseau social et ma boutique en ligne sont vérifiés
- ☐ 7. J'ai vérifié mes fuites et changé les mots de passe concernés
- ☐ 8. Une sauvegarde automatique tourne, et je l'ai testée
- ☐ 9. J'ai fait le tri dans mes applications

Une case vide n'a rien d'un échec. Reportez-la ci-dessous avec une date, et finissez-la dans les quinze jours.

CE QUI RESTE À FAIRE

Ce qu'il me reste à faire	D'ici le
Exemple : acheter un disque externe pour la sauvegarde	*5 décembre*

L'ENTRETIEN

Une fois en place, votre sécurité demande peu de temps. Créez dès maintenant un rappel répété dans l'agenda de votre téléphone, par exemple « Hygiène numérique », le premier dimanche de chaque mois.

Chaque mois (5 minutes)

- ☐ Installer les mises à jour en attente

- [ ] Vérifier que les mots de passe des sites utilisés ce mois-ci sont bien entrés dans le gestionnaire

Chaque trimestre (15 minutes)

- [ ] Parcourir les appareils connectés à votre e-mail et à votre compte Apple ou Google
- [ ] Revoir les permissions des applications installées depuis le dernier contrôle
- [ ] Restaurer un fichier au hasard depuis votre sauvegarde

Chaque année (30 minutes)

- [ ] Refaire toute la checklist, de l'étape 1 à l'étape 9
- [ ] Vérifier que vos codes de secours et votre phrase maîtresse sont toujours à leur place

> Je pense m'être fait pirater

Vous recevez un e-mail « Votre mot de passe a été modifié » alors que vous n'avez rien touché. Vos amis reçoivent des messages étranges envoyés depuis votre compte. Un paiement inconnu apparaît sur votre relevé. Respirez, puis suivez cet ordre :

1. **S'il y a de l'argent en jeu, appelez votre banque en premier.** Utilisez le numéro au dos de votre carte, jamais celui d'un message reçu. Faites bloquer la carte si besoin. Chaque heure compte pour contester un paiement.
2. **Reprenez le contrôle du compte.** Changez le mot de passe depuis un autre appareil que celui que vous soupçonnez, par exemple votre téléphone si votre ordinateur se comporte bizarrement. Déconnectez ensuite toutes les sessions, puis vérifiez la double vérification, les moyens de récupération et les règles de transfert (étape 4).
3. **Si vous ne pouvez plus vous connecter du tout**, utilisez le formulaire de récupération du service. Cherchez « récupérer mon compte » suivi du nom du service, et passez uniquement par le site officiel. Les « services de récupération » qui vous contactent sur les réseaux sociaux sont des escrocs.
4. **Prévenez vos proches** par un autre canal : « Mon compte Facebook a été piraté, ne répondez à aucune demande d'argent venant de lui. »
5. **Gardez des traces.** Faites des captures d'écran des messages suspects, des paiements, des e-mails de modification. Vous en aurez besoin pour la banque et pour un éventuel dépôt de plainte.
6. **Signalez l'incident.**
   - En Suisse : l'Office fédéral de la cybersécurité (OFCS) propose un formulaire de signalement : report.ncsc.admin.ch/fr
   - En France : cybermalveillance.gouv.fr vous guide selon votre situation et vous oriente vers une aide.
   - Si vous avez perdu de l'argent, déposez plainte auprès de la police ou de la gendarmerie.

> Reconnaître un message frauduleux

La plupart des piratages commencent par un message. Méfiez-vous dès que vous repérez un de ces signes :

- **L'urgence** : « Votre compte sera suspendu dans 24 heures », « Dernier rappel avant poursuites »
- **Une petite somme à payer** : « Frais de livraison de 1,99 € », « Amende de stationnement impayée »
- **Une demande de code** : aucun service sérieux ne vous demande de lui transmettre un code reçu par SMS
- **Un proche qui change soudain de numéro** : « Coucou maman, j'ai cassé mon téléphone, voici mon nouveau numéro, tu peux m'aider à payer une facture ? »
- **Un expéditeur presque juste** : « service@paypa1.com » au lieu de « paypal.com », ou un numéro de téléphone inconnu pour un message signé « La Poste »
- **Un lien inattendu**, même d'un contact connu, dont le compte a peut-être été piraté

> En cas de doute, ne cliquez pas. Ouvrez vous-même l'application ou le site officiel, ou appelez la personne sur son numéro habituel.

> Ressources et mentions

LES OUTILS CITÉS DANS CE GUIDE

- Bitwarden : bitwarden.com
- Proton Pass : proton.me/pass
- Proton Authenticator : proton.me/authenticator
- Ente Auth : ente.com/auth
- Have I Been Pwned : haveibeenpwned.com

LES RESSOURCES OFFICIELLES

- Suisse : Office fédéral de la cybersécurité (OFCS), ncsc.admin.ch. Formulaire de signalement : report.ncsc.admin.ch/fr. L'OFCS collabore aussi avec Have I Been Pwned.
- France : cybermalveillance.gouv.fr, le dispositif national d'assistance aux victimes de cybermalveillance

SUR HU-TECH.CH

Retrouvez les articles sur l'usage conscient des technologies et les prochains Carnets Hu-Tech sur hu-tech.ch.

VERSION ET MISES À JOUR

Version 1.0, novembre 2026. Les menus, les noms de réglages et les offres des services évoluent. Si vous avez téléchargé ce carnet sur hu-tech.ch, vous recevrez gratuitement ses mises à jour à l'adresse e-mail utilisée lors du téléchargement.

CONDITIONS D'UTILISATION

Ce carnet est destiné à votre usage personnel et à celui de votre foyer. Vous pouvez l'imprimer autant de fois que nécessaire. Merci de ne pas le revendre ni le diffuser en ligne : il fait vivre hu-tech.ch, un site indépendant et sans publicité.

AVERTISSEMENT

Ce guide réduit les risques les plus courants. Il ne garantit pas une protection totale et ne remplace pas l'aide d'un professionnel en cas d'incident grave. Les outils cités le sont pour leur sérieux, sans aucun lien commercial avec hu-tech.ch.