axelites

DIFFUSION LIBRE



CAHIER DE SÉCURITÉ NUMÉRIQUE

# Sécurisez vos accès avant qu'on vous les vole.

Le guide pratique pour protéger votre e-mail, vos réseaux sociaux, votre banque et votre site internet. Sans jargon technique.


| VERSION | DATE | DESTINÉ À | ÉDITEUR |
| --- | --- | --- | --- |
| 1.0 | Octobre 2026 | Dirigeants, équipes et clients | Axelites SARL |

ALERTE · ÉTAT DE LA MENACE EN FRANCE

# Vos comptes en ligne sont devenus la cible n°1 des cybercriminels.

Il suffit d'une seule erreur : un clic sur un faux message, un mot de passe réutilisé, un code donné au téléphone. Et ce n'est plus réservé aux grandes entreprises.

**500 000+**

**victimes accompagnées en 2025** par le dispositif national d'assistance, soit +20 % en un an.

**N°1**

**Le piratage de compte** est la première menace pour les entreprises en 2025 (21 % des demandes d'assistance).

**+70 %**

**d'hameçonnage en un an.** Les faux messages sont la première menace, tous publics confondus.

**+159 %**

**de fraudes au faux conseiller bancaire** en un an. Chez les professionnels, la fraude au virement a progressé de 93 %.

## Ce qui arrive concrètement quand un accès est volé

- Votre boîte e-mail est lue, et **vos clients reçoivent de fausses factures** envoyées en votre nom.
- Votre page Facebook ou Instagram est **confisquée** et votre budget publicitaire est dépensé.
- Un **virement part vers le compte d'un escroc**, souvent sans possibilité de le récupérer.
- Votre site internet affiche de fausses pages ou **laisse fuir les données de vos clients**.
- Récupérer l'accès prend **des semaines**… quand c'est encore possible.

LA BONNE NOUVELLE

La double authentification réduit à elle seule **de 99,2 % le risque de piratage** d'un compte. Avec quelques réflexes simples, vous bloquez la grande majorité des attaques. **Ils tiennent sur la page suivante.**

Sources : Cybermalveillance.gouv.fr, rapport d'activité 2025 et Top 10 des cybermalveillances 2025 (professionnels) · Microsoft Research, *How effective is multifactor authentication at deterring cyberattacks?*, 2023.

L'ESSENTIEL EN 2 MINUTES

# Un seul mot à retenir : STOP

Avant de cliquer, de vous connecter ou de valider quoi que ce soit, faites STOP.

**S** — **Source**
Je passe par **mes favoris** ou l'application officielle. Jamais par un lien reçu, jamais par un moteur de recherche.
p. 7–8

**T** — **Temps**
Urgence, menace, délai de 24 h ? C'est le signe d'une arnaque. **Je prends le temps** de vérifier.
p. 6

**O** — **Origine**
Avant de taper un mot de passe ou un code, **je vérifie l'adresse** de la page.
p. 9

**P** — **Personne**
Je ne donne **mes mots de passe et mes codes à personne** : ni au téléphone, ni par message, ni à un collègue.
p. 12 et 18

## Et une fois pour toutes : 5 actions à faire cette semaine

| # | Action | Temps | Détails |
|---|---|---|---|
| 1 | **Activer la double authentification** sur votre e-mail, vos réseaux sociaux, votre banque et votre site, avec une clé d'accès (empreinte, Face ID) si possible. | 15 min | p. 11 |
| 2 | **Ranger vos codes de secours** en lieu sûr : imprimés ou dans votre gestionnaire de mots de passe. | 5 min | p. 12 |
| 3 | **Créer un dossier « Mes accès »** dans les favoris de votre navigateur. | 5 min | p. 7 |
| 4 | **Installer un gestionnaire de mots de passe**, un outil qui les stocke en lieu sûr, et remplacer les mots de passe réutilisés. | 30 min | p. 10 |
| 5 | **Faire le ménage dans les accès** : un compte par personne, retirer les anciens salariés et prestataires. | 20 min | p. 18 |

↓ **Regardez les détails dans les pages suivantes.**
D'abord le résumé de toutes les actions page 4, puis chaque point expliqué pas à pas, avec des exemples concrets.

RÉSUMÉ DES ACTIONS

# Ce que vous devez faire

Onze actions, en deux temps. Si vous ne gardez qu'une page de ce guide, gardez celle-ci.

## À CHAQUE FOIS — Les réflexes du quotidien

| | |
|---|---|
| **Favoris** | Je passe par mes favoris, **jamais par un lien reçu**. |
| **Adresse** | Je **vérifie l'adresse** de la page avant de me connecter. |
| **Refus** | Je **refuse** toute demande que je n'ai pas lancée moi-même. |
| **Secret** | Je ne donne **jamais** mes mots de passe ni mes codes. |
| **Doute** | Dans le doute, **je m'arrête et je demande**. |

## UNE FOIS POUR TOUTES — Les réglages, à faire cette semaine

| | | |
|---|---|---|
| **Double authentification** | Je l'**active partout**, avec une clé d'accès si possible. | p. 11 |
| **Secours** | Je range mes **codes de secours** en lieu sûr. | p. 12 |
| **Gestionnaire** | Je range mes mots de passe dans **un outil sécurisé**. | p. 10 |
| **Unique** | Un **mot de passe différent** pour chaque service. | p. 10 |
| **Accès** | **Un compte par personne**, jamais d'accès partagé. | p. 18 |
| **Mises à jour** | Mes appareils et mon site sont **toujours à jour**. | p. 17 |

↓ **Passons aux détails.**
Chaque action est expliquée pas à pas.
Sommaire page suivante.

**Besoin d'aide pour tout mettre en place ?**
contact@axelites.com · +33 1 87 66 36 82
axelites.com

SOMMAIRE

# Le détail, étape par étape

## NIVEAU 1 · LES BASES


01 Comprendre les arnaques par faux message 6

02 Le réflexe « favoris » 7

03 Ne jamais cliquer sur un lien reçu 8

04 Vérifier l'adresse d'une page 9


## NIVEAU 2 · PROTÉGER SES COMPTES


05 Les mots de passe 10

06 La double authentification 11

07 Sécuriser votre boîte e-mail 13

08 Facebook, Instagram, Meta Business et autres réseaux 14

09 Banque et paiements 15

10 Votre ordinateur et votre téléphone 16


## NIVEAU 3 · ENTREPRISE ET SITE INTERNET


11 Travailler en équipe : ne jamais partager les accès 18

12 Votre site internet : WordPress, Magento, Shopify… 19


## À GARDER SOUS LA MAIN


13 En cas de doute ou de problème 20

✓ Ma check-list sécurité 21

i À propos de ce document et avertissement 22


**i Comment utiliser ce guide**

- Lisez d'abord les **pages 2 à 4** : la menace, l'essentiel à retenir et le résumé des actions.
- Consultez ensuite les chapitres dont vous avez besoin. Ils vont du plus simple au plus avancé.
- Terminez par la **check-list**, à refaire tous les trois mois.

NIVEAU 1 · SIMPLE

# 01 Comprendre les arnaques par faux message

L'hameçonnage (en anglais *phishing*) consiste à vous envoyer un faux message qui imite un service connu (Google, Meta, votre banque, La Poste, les impôts…) pour vous pousser à cliquer et à saisir vos identifiants sur une fausse page.

## Comment ça marche

1. Vous recevez un message alarmant ou alléchant : *« Votre compte sera fermé »*, *« Paiement refusé »*, *« Colis en attente »*, *« Votre page a enfreint nos règles »*.
2. Le lien vous amène sur une page **identique au vrai site** : même logo, mêmes couleurs.
3. Vous tapez votre e-mail, votre mot de passe, parfois même le code reçu par SMS.
4. L'arnaqueur récupère tout **en direct** et se connecte à votre place. Il change le mot de passe : vous perdez l'accès.

## Exemple d'un faux e-mail

**De :** Google Security ‹no-reply@google-accounts-support.com›
**Objet :** ⚠ Votre compte sera fermé sous 24h

Bonjour,
Nous avons détecté une activité inhabituelle. Sans action de votre part, votre compte Google sera **définitivement fermé dans 24 heures**. Merci de confirmer votre identité et de nous donner votre avis.

Confirmer mon compte

- L'adresse de l'expéditeur n'est pas celle de Google (google-accounts-support.com).
- Une menace et un délai très court pour vous faire paniquer.
- Un bouton qui vous demande de vous connecter : c'est le piège.

### Les signaux d'alerte

- Urgence, menace ou récompense
- Demande de mot de passe, de code ou de coordonnées bancaires
- Expéditeur ou adresse de site étrange
- Message inattendu, même s'il semble venir d'un proche

### Bon à savoir en 2026

Grâce à l'intelligence artificielle, les faux messages sont désormais **sans faute d'orthographe** et parfaitement imités. On peut même imiter une voix au téléphone. Ne vous fiez plus à l'apparence : **fiez-vous à vos réflexes**.

NIVEAU 1 · SIMPLE

# 02 Le réflexe « favoris »

Taper « Google Cloud » ou « ma banque » dans un moteur de recherche puis cliquer sur le premier résultat est risqué : les arnaqueurs **achètent des publicités** qui apparaissent tout en haut et mènent vers de fausses pages.

**À éviter**

Chercher le nom du service dans Google ou Bing, puis cliquer sur le premier lien (souvent un lien « Sponsorisé »).

**Le bon réflexe**

Enregistrer **une fois pour toutes** l'adresse officielle de chaque service dans les favoris, et toujours passer par là.

## Créer vos favoris en 3 étapes

1. Ouvrez le site officiel une première fois, en tapant vous-même l'adresse indiquée ci-dessous.
2. Appuyez sur **Ctrl + D** (Windows) ou **Cmd + D** (Mac), ou cliquez sur l'étoile ☆.
3. Rangez-le dans un dossier « **Mes accès** » affiché dans la barre de favoris.

## Les adresses officielles à mettre en favoris

| | |
|---|---|
| Gmail<br>`mail.google.com` | Compte Google (sécurité)<br>`myaccount.google.com` |
| Google Cloud<br>`console.cloud.google.com` | Google Ads<br>`ads.google.com` |
| Outlook / Microsoft 365<br>`outlook.office.com` | LinkedIn<br>`www.linkedin.com` |
| Facebook<br>`www.facebook.com` | Meta Business Suite<br>`business.facebook.com` |
| Instagram<br>`www.instagram.com` | Impôts · Urssaf<br>`impots.gouv.fr · urssaf.fr` |
| Votre banque<br>**Adresse indiquée sur votre contrat** | Votre site (administration)<br>**Adresse fournie par votre prestataire** |

**Sur le téléphone**

Utilisez les **applications officielles** (Gmail, Instagram, votre banque…) installées depuis l'App Store ou Google Play : elles jouent le rôle des favoris.

NIVEAU 1 · SIMPLE

# 03 Ne jamais cliquer sur un lien reçu

C'est **la règle la plus importante** de ce guide. Quel que soit le message, même s'il semble officiel, même s'il est urgent : on ne clique pas sur le lien.

## La méthode en 3 temps

1. **Je ferme le message.** Je ne clique sur rien, je ne réponds pas.
2. **J'ouvre le service moi-même**, depuis mes favoris ou l'application officielle.
3. **Je cherche la notification sur place.** Si l'alerte est vraie, elle apparaît aussi dans mon compte (rubrique notifications, sécurité ou messages). Je fais l'action depuis là. Si je ne trouve rien, c'était une arnaque.

**? Exemple**

Vous recevez : *« Votre compte Google sera fermé, cliquez ici pour donner votre avis. »*
→ Vous fermez l'e-mail, vous ouvrez `myaccount.google.com` depuis vos favoris, puis la rubrique **Sécurité**. Aucune alerte ? Le message était faux : supprimez-le.

## Cela vaut pour tous les canaux

| Canal | Exemples fréquents |
|---|---|
| E-mail | Compte bloqué, facture impayée, document partagé, mot de passe expiré |
| SMS | Colis en attente, amende, remboursement, carte Vitale, compte bancaire suspendu |
| WhatsApp / Messenger | « Maman, j'ai changé de numéro », faux support Meta, faux recruteur |
| QR code | QR code collé sur un parking ou reçu par courrier, qui mène vers une fausse page de paiement |
| Pièce jointe | Fausse facture, faux bon de commande : ne l'ouvrez pas si vous ne l'attendiez pas |

**✕ Banques et paiements : tolérance zéro**

Votre banque ne vous demandera **jamais** vos codes, votre mot de passe ou de valider une opération par e-mail, SMS ou téléphone. Un appel de votre « conseiller » ou du « service fraude » ? Raccrochez et rappelez le numéro inscrit au dos de votre carte.

NIVEAU 1 · SIMPLE

# 04 Vérifier l'adresse d'une page

Avant de saisir un mot de passe ou un code, jetez un œil à la barre d'adresse, tout en haut du navigateur. Une fausse page peut être parfaite visuellement, mais **son adresse la trahit toujours**.

## La règle simple

Le vrai nom du site est **le dernier mot avant le premier « / »** (avec son .com, .fr…). Tout ce qui est écrit avant peut être inventé par l'arnaqueur.

| | |
|---|---|
| https://accounts.**google.com**/signin | ✓ Vrai |
| https://accounts.google.com.**secure-login.io**/signin | ✗ Faux |
| https://**g00gle.com**/login | ✗ Faux (deux zéros) |
| https://business.**facebook.com**/settings | ✓ Vrai |
| https://**meta-support-center.com**/appeal | ✗ Faux |
| https://**instagram-verify.help**/account | ✗ Faux |

**Le cadenas ne prouve rien**

Le petit cadenas signifie seulement que la connexion est chiffrée. **Les faux sites ont aussi un cadenas.** Il ne garantit pas que vous êtes sur le bon site.

**L'astuce qui règle tout**

Si vous êtes arrivé sur la page **par vos favoris**, l'adresse est forcément la bonne. C'est pour ça que le réflexe n°2 est si efficace.

NIVEAU 2 · ESSENTIEL

# 05 Les mots de passe

Quand un site se fait pirater, les mots de passe de ses utilisateurs circulent sur internet. Si vous utilisez le même partout, **une seule fuite ouvre toutes vos portes**.

### ✓ Un bon mot de passe

- **Unique** : un par service, sans exception
- **Long** : 14 caractères minimum
- Idéalement une phrase facile à retenir, par exemple `Mon-Chat-Mange-3-Croissants!`

### ✗ À bannir

- Le même mot de passe sur plusieurs sites
- Prénom, date de naissance, nom de l'entreprise
- Un post-it sur l'écran ou un fichier « mdp.xlsx »
- L'envoyer par e-mail, SMS ou WhatsApp

## Utilisez un gestionnaire de mots de passe

Personne ne peut retenir 50 mots de passe différents. Un gestionnaire de mots de passe est un **coffre-fort numérique** : vous ne retenez qu'un seul mot de passe principal, il se souvient de tous les autres et les remplit pour vous.

**Nos recommandations :**

POUR TOUS

### Bitwarden

- Fonctionne sur **tous les appareils** : Windows, Mac, iPhone, Android, et tous les navigateurs.
- **Gratuit** pour un usage personnel. Une offre payante permet de partager des accès en équipe.
- À télécharger uniquement depuis `bitwarden.com` ou les boutiques officielles.

SI VOUS ÊTES ÉQUIPÉ APPLE

### Mots de passe d'Apple

- L'app **« Mots de passe »** est déjà installée sur iPhone, iPad et Mac : rien à acheter.
- Synchronisée par iCloud, et utilisable sur un PC Windows avec l'application iCloud.
- Gère aussi vos **clés d'accès** et vos codes de validation.

### ? Un bonus anti-arnaque

Le gestionnaire ne remplit votre mot de passe **que sur le vrai site**. S'il ne vous propose rien alors qu'il le fait d'habitude, méfiance : vous êtes peut-être sur une fausse page.

### i Le mot de passe principal

Celui de votre gestionnaire et celui de votre boîte e-mail sont les deux plus importants. Faites-en de longues phrases que vous n'utilisez nulle part ailleurs, et protégez-les par la double authentification.

NIVEAU 2 · ESSENTIEL

# 06 La double authentification

La double authentification (ou « validation en deux étapes », « 2FA ») demande une deuxième preuve en plus du mot de passe. Même si un arnaqueur vole votre mot de passe, il reste bloqué. **Elle est désormais obligatoire** sur tous vos comptes importants.

## Toutes les méthodes ne se valent pas

**1**
IDÉAL

### Les clés d'accès (passkeys) À PRIVILÉGIER

Vous vous connectez avec **votre empreinte, Face ID ou le code de votre ordinateur** (Windows Hello, Touch ID). Pas de mot de passe à taper, pas de code à recopier.

Pourquoi c'est le meilleur choix : la clé d'accès est liée au vrai site. **Sur une fausse page, elle ne fonctionne tout simplement pas**, même si vous vous faites avoir.

**2**
TRÈS BIEN

### La validation sur le téléphone BONNE OPTION

Au moment de vous connecter, votre téléphone affiche *« Est-ce bien vous qui essayez de vous connecter ? »* et vous répondez **Oui** ou **Non** (Google, Microsoft, Meta proposent cette option).

La règle d'or : **vous ne validez que si c'est vous qui venez de lancer la connexion.** Une demande surprise, même répétée plusieurs fois ? Répondez **Non** et changez votre mot de passe.

**3**
EN DERNIER RECOURS

### Le code (application Authenticator ou SMS) AVEC PRUDENCE

Vous recopiez un code à 6 chiffres reçu par SMS ou affiché par une application (Google Authenticator, Microsoft Authenticator…). C'est mieux que rien, mais **c'est exactement ce que les fausses pages cherchent à récupérer** : l'arnaqueur vous demande le code et l'utilise dans la seconde.

Avant de taper un code : **suis-je arrivé ici par mes favoris ? L'adresse de la page est-elle la bonne ?** Si vous avez le moindre doute, ne tapez rien. Et ne donnez jamais un code à quelqu'un, même au téléphone.

## Où l'activer ?

Passez toujours par vos favoris, puis suivez ce chemin. Profitez-en pour ajouter une clé d'accès si le service le propose.

| Service | Chemin |
|---|---|
| Google / Gmail | `myaccount.google.com` → Sécurité → Validation en deux étapes · Clés d'accès |
| Microsoft / Outlook | `account.microsoft.com` → Sécurité → Options de connexion |
| Facebook et Instagram | Espace Comptes → Mot de passe et sécurité → Authentification à deux facteurs |
| Meta Business | Paramètres de l'entreprise → Centre de sécurité → Exiger la double authentification |
| LinkedIn | Préférences → Connexion et sécurité → Vérification en deux étapes |
| Votre banque | Déjà en place dans l'application officielle : gardez-la à jour |
| Votre site, hébergeur, nom de domaine | Demandez à votre prestataire de l'activer pour chaque utilisateur |

Les intitulés exacts peuvent légèrement changer selon les mises à jour des services.

## Les codes de secours : votre roue de secours

Lors de l'activation, le service vous propose une liste de **codes de secours** (souvent 8 ou 10). Ils vous permettent de récupérer votre compte si vous perdez ou changez de téléphone.

### ✓ À faire

- Les **imprimer** et les ranger en lieu sûr, ou les enregistrer dans votre gestionnaire de mots de passe
- En générer de nouveaux après en avoir utilisé un (chaque code ne sert qu'une fois)
- Ajouter **une deuxième méthode** (un deuxième téléphone, une clé de sécurité) pour ne jamais être bloqué

### ✗ À ne jamais faire

- Les prendre en photo dans la galerie de votre téléphone
- Les envoyer par e-mail ou messagerie
- Les communiquer à qui que ce soit, même à un « support technique »

### ! Vous changez de téléphone ?

Avant de vous séparer de l'ancien, vérifiez que vos clés d'accès et votre application Authenticator ont bien été transférées sur le nouveau, et que vous savez où sont vos codes de secours.

NIVEAU 2 · ESSENTIEL

# 07 Sécuriser votre boîte e-mail

Votre adresse e-mail est **la clé maîtresse** de tous vos comptes : c'est elle qui reçoit les liens « mot de passe oublié ». Qui contrôle votre e-mail peut prendre le contrôle de tout le reste.

## Les 6 actions à faire dès aujourd'hui

1. **Un mot de passe long et unique**, utilisé nulle part ailleurs.
2. **La double authentification**, avec une clé d'accès de préférence (voir chapitre 06), et vos codes de secours en lieu sûr.
3. **Un téléphone et une adresse de secours à jour**, pour pouvoir récupérer votre compte.
4. **Vérifier les appareils connectés** : dans les paramètres de sécurité, déconnectez tout appareil que vous ne reconnaissez pas.
5. **Vérifier les transferts automatiques et les filtres** : un pirate en ajoute souvent un pour recevoir une copie de vos e-mails en toute discrétion. Supprimez ceux que vous n'avez pas créés.
6. **Faire le bilan de sécurité** proposé par votre messagerie, une fois par trimestre.

| Messagerie | Où faire le point |
|---|---|
| Gmail / Google Workspace | `myaccount.google.com` → Sécurité → « Check-up Sécurité » |
| Outlook / Microsoft 365 | `account.microsoft.com` → Sécurité |
| Autres (OVH, Orange, iCloud…) | Rubrique « Sécurité » ou « Connexion » des paramètres de votre compte |

**Séparez pro et perso**

Utilisez une adresse professionnelle pour l'entreprise (Google Workspace, Microsoft 365…) et une adresse personnelle pour le reste. Si l'une est compromise, l'autre reste protégée.

**Alerte de connexion reçue ?**

« Nouvelle connexion depuis un appareil inconnu » : ne cliquez pas dans l'e-mail. Ouvrez votre compte depuis vos favoris et vérifiez l'activité récente.

# 08 Facebook, Instagram, Meta Business et autres réseaux

Les pages Facebook et comptes Instagram d'entreprise sont très ciblés : une fois volés, ils servent à diffuser des arnaques à vos abonnés ou à dépenser votre budget publicitaire.

## Pour chaque compte personnel qui gère une page

- **Double authentification activée** sur Facebook et Instagram (Espace Comptes Meta → Mot de passe et sécurité).
- Un mot de passe unique, différent de celui de votre e-mail.
- Vérifiez régulièrement les **appareils connectés** et déconnectez ceux que vous ne reconnaissez pas.

## Pour votre portefeuille Meta Business

- **Exigez la double authentification** pour tous les membres (Paramètres de l'entreprise → Centre de sécurité).
- Gardez **au moins deux administrateurs de confiance** : si l'un perd son accès, l'autre peut le rétablir.
- Donnez à chacun **le minimum de droits nécessaires** (accès partiel plutôt que contrôle total).
- Pour une agence, utilisez l'option **« Partenaires »** : elle accède à vos pages sans jamais connaître vos identifiants.
- Retirez immédiatement les anciens salariés, stagiaires et prestataires.

**L'arnaque la plus fréquente**

Un message Messenger ou un e-mail « Meta » vous annonce que votre page **enfreint les droits d'auteur** ou **sera supprimée**, avec un lien pour « faire appel ». C'est faux. Meta ne vous contacte jamais par Messenger avec un lien. Les vraies alertes se trouvent dans **Meta Business Suite → Assistance aux comptes professionnels**.

**Vérifier qu'un e-mail vient bien de Facebook ou Instagram**

Dans les paramètres de sécurité de Facebook et d'Instagram, une rubrique liste **les e-mails récents réellement envoyés** par le service. Si l'e-mail que vous avez reçu n'y figure pas, c'est une arnaque.

Les mêmes principes s'appliquent à LinkedIn, TikTok, YouTube, X, Google Business Profile… : double authentification, un compte par personne, droits minimum, et aucun clic sur les liens reçus.

NIVEAU 2 · ESSENTIEL

# 09 Banque et paiements

Les arnaques financières visent autant les particuliers que les entreprises. Les règles des chapitres précédents s'appliquent, avec quelques réflexes en plus.

**Les bons réflexes**

- Accédez à votre banque **uniquement par l'application officielle** ou vos favoris.
- **Lisez ce que vous validez** dans l'application : montant, bénéficiaire. Ne validez que ce que vous avez vous-même lancé.
- Activez les notifications de paiement pour repérer vite une opération anormale.

**Jamais, sous aucun prétexte**

- Donner un code reçu par SMS, même à un « conseiller »
- Valider une opération pour « annuler une fraude »
- Installer une application à la demande d'un interlocuteur au téléphone

## Deux arnaques qui visent les entreprises

**Le faux changement de RIB**

Un « fournisseur » vous écrit : *« Nous avons changé de banque, merci d'utiliser ce nouveau RIB. »* Le message peut même venir de sa vraie adresse si sa boîte a été piratée.
**Réflexe : appelez votre contact au numéro que vous connaissez déjà** (pas celui indiqué dans le message) avant tout virement.

**La fraude au président**

Un e-mail ou un appel du « dirigeant » demande un virement urgent et confidentiel. La voix peut être imitée par intelligence artificielle.
**Réflexe : aucune urgence ne justifie de sauter les vérifications.** Rappelez la personne sur son numéro habituel et faites valider par une deuxième personne.

NIVEAU 2 · ESSENTIEL

# 10 Votre ordinateur et votre téléphone

Vos appareils sont la porte d'entrée de tous vos comptes. Quelques réglages suffisent à les protéger.

| Réflexe | Pourquoi |
|---|---|
| **Faire les mises à jour** dès qu'elles sont proposées | Elles corrigent des failles déjà connues des pirates. Activez les mises à jour automatiques. |
| **Verrouiller l'écran** (code, empreinte, Face ID) | Un téléphone perdu ou un ordinateur laissé ouvert donne accès à tout. |
| **Installer uniquement depuis les boutiques officielles** | App Store, Google Play, Microsoft Store, ou le site officiel de l'éditeur. Pas de logiciel « gratuit » d'origine douteuse. |
| **Limiter les extensions du navigateur** | Certaines extensions lisent tout ce que vous tapez. Gardez seulement celles que vous utilisez vraiment. |
| **Éviter les Wi-Fi publics** pour les opérations sensibles | Préférez le partage de connexion de votre téléphone pour la banque ou l'administration de votre site. |
| **Une session par personne** | Ne partagez pas votre session d'ordinateur. Chaque collaborateur a la sienne. |
| **Sauvegarder vos fichiers** | Une copie régulière (cloud ou disque externe) vous protège en cas de panne, de vol ou de rançongiciel. |

**Antivirus**

Sur Windows, Microsoft Defender (inclus et gratuit) suffit dans la plupart des cas, à condition qu'il soit activé et à jour. Sur Mac, iPhone et Android, les protections intégrées et les mises à jour sont l'essentiel.

NIVEAU 2 · ESSENTIEL · SUITE

## Les mises à jour, appareil par appareil

Une mise à jour corrige des failles que les pirates connaissent déjà. **Activez les mises à jour automatiques partout**, puis vérifiez une fois par mois avec ce tableau.

| Appareil / logiciel | Où faire la mise à jour |
|---|---|
| **Windows** | Paramètres → Windows Update → Rechercher des mises à jour |
| **Mac (macOS)** | Réglages Système → Général → Mise à jour de logiciels → activer les mises à jour automatiques |
| **iPhone / iPad** | Réglages → Général → Mise à jour logicielle → Mises à jour automatiques |
| **Android** | Paramètres → Système → Mise à jour du système (sur Samsung : Paramètres → Mise à jour du logiciel) |
| **Google Chrome** | Menu ⋮ → Aide → À propos de Google Chrome, puis cliquer sur « Relancer » |
| **Microsoft Edge** | Menu … → Aide et commentaires → À propos de Microsoft Edge |
| **Firefox** | Menu ≡ → Aide → À propos de Firefox |
| **Safari** | Mis à jour en même temps que macOS, iOS et iPadOS |
| **Applications** | App Store, Google Play ou Microsoft Store → rubrique « Mises à jour » |

Les intitulés peuvent varier légèrement selon la version et la marque de l'appareil.

**Redémarrez**

Une mise à jour ne protège qu'**après le redémarrage** de l'appareil ou du navigateur. Ne repoussez pas un redémarrage pendant des semaines.

**Les fausses mises à jour**

Une fenêtre sur un site web qui vous demande de « mettre à jour Chrome » ou d'« installer un lecteur » est une arnaque. **Les vraies mises à jour se font uniquement depuis les réglages.**

**Un appareil trop ancien n'est plus protégé**

Quand le fabricant arrête les mises à jour, les failles ne sont plus corrigées. C'est le cas de **Windows 10**, qui ne reçoit plus de correctifs de sécurité gratuits : passez à Windows 11 ou remplacez l'ordinateur. Un téléphone qui ne propose plus de mise à jour doit aussi être remplacé pour un usage professionnel.

NIVEAU 3 · AVANCÉ

# 11 Travailler en équipe : ne jamais partager les accès

« Je te donne mon mot de passe, c'est plus simple. » C'est l'une des premières causes de piratage en entreprise. **Un accès, une personne.**

**? Pourquoi ne jamais partager un compte**

- **On ne sait plus qui fait quoi** : impossible de savoir qui a supprimé un produit ou modifié un paramètre.
- **On ne peut pas retirer l'accès** à une seule personne sans bloquer tout le monde.
- **La double authentification devient impossible** ou est désactivée « pour que tout le monde puisse se connecter ».
- **Le mot de passe circule** dans des e-mails, des SMS, des fichiers… et finit par fuiter.

## Les bonnes pratiques

1. **Créez un compte nominatif** pour chaque collaborateur ou prestataire, avec son adresse e-mail à lui.
2. **Utilisez les invitations** prévues par chaque outil (Google Workspace, Meta Business, Google Ads, WordPress, Shopify…) plutôt que de donner vos identifiants.
3. **Donnez le minimum de droits nécessaires** : un rédacteur n'a pas besoin d'être administrateur.
4. **Si un partage est vraiment inévitable**, utilisez la fonction de partage sécurisé de votre gestionnaire de mots de passe, jamais un e-mail ou un message.
5. **Le jour d'un départ**, retirez tous les accès de la personne et changez les mots de passe qu'elle connaissait.
6. **Une fois par trimestre**, faites la liste des personnes qui ont accès à chaque outil et supprimez celles qui n'en ont plus besoin.

**i Et avec Axelites SARL ?**

Nous ne vous demanderons jamais votre mot de passe personnel. Pour intervenir sur vos outils, nous vous demanderons de nous **inviter avec un compte à notre nom**, que vous pourrez retirer à tout moment.

NIVEAU 3 · AVANCÉ

# 12 Votre site internet : WordPress, Magento, Shopify…

Un site piraté peut afficher de fausses pages, voler les données de vos clients ou être retiré des résultats Google. La plupart des intrusions passent par **un accès administrateur mal protégé** ou **un module pas à jour**.

## Vos accès à l'administration du site

- **Un compte par personne**, jamais de compte « admin » partagé.
- **Le bon rôle pour chacun** : sur WordPress, « Éditeur » ou « Auteur » suffit pour publier du contenu. Réservez « Administrateur » à une ou deux personnes.
- **La double authentification activée** : intégrée à Magento, Shopify et PrestaShop récents, ajoutée par une extension sur WordPress. Demandez à votre prestataire de l'activer.
- **L'adresse de l'administration dans vos favoris**, comme pour vos autres services.
- **Supprimez les comptes inutilisés** : anciens salariés, stagiaires, agences précédentes.

## Les accès « de l'ombre » à ne pas oublier

Votre site dépend aussi de comptes que l'on oublie souvent. Ils méritent la même protection (mot de passe unique + double authentification) :

| Compte | Ce qu'un pirate peut faire avec |
|---|---|
| Nom de domaine (OVH, Gandi, GoDaddy…) | Détourner votre site **et vos e-mails** vers ses serveurs |
| Hébergeur | Modifier ou supprimer votre site et vos sauvegardes |
| Moyens de paiement (Stripe, PayPal…) | Détourner vos encaissements |
| Google Search Console / Analytics | Faire désindexer votre site, accéder à vos statistiques |

### ✕ À ne jamais faire

- Installer un thème ou une extension téléchargé hors du site officiel (versions « gratuites » de modules payants)
- Garder des extensions désactivées « au cas où »
- Ignorer les alertes de mises à jour

### ✓ À demander à votre prestataire

- Les mises à jour régulières du site et des modules
- Des sauvegardes automatiques, stockées ailleurs que sur le site
- La liste des comptes administrateurs actifs

Axelites SARL s'en charge avec sa **TMA**.

# 13 En cas de doute ou de problème

Vous avez cliqué sur un lien suspect, tapé votre mot de passe sur une page douteuse, ou vous n'arrivez plus à vous connecter ? **Pas de panique, et pas de honte** : cela arrive à tout le monde. Ce qui compte, c'est d'agir vite.

## Les premiers gestes

1. **Changez immédiatement le mot de passe** du compte concerné, en passant par vos favoris. Faites de même partout où vous utilisiez ce mot de passe.
2. **Déconnectez toutes les sessions** depuis les paramètres de sécurité du compte (« Se déconnecter de tous les appareils »).
3. **Vérifiez la double authentification** : elle doit toujours être active, avec vos propres méthodes (un pirate peut ajouter son téléphone).
4. **Banque : faites opposition** sans attendre si vous avez donné des informations de carte ou validé une opération suspecte.
5. **Prévenez votre entourage** professionnel si votre e-mail ou votre page a pu envoyer des messages en votre nom.
6. **Contactez-nous** : nous vous aidons à reprendre la main et à vérifier qu'il ne reste aucun accès indésirable.

## Signaler une arnaque

| Situation | Où signaler |
|---|---|
| E-mail frauduleux | `signal-spam.fr` |
| SMS frauduleux | Transférez-le gratuitement au **33700** |
| Victime d'une cyberattaque | `17cyber.gouv.fr` (aide officielle de l'État) |
| Conseils et assistance | `cybermalveillance.gouv.fr` |
| Compte Facebook / Instagram piraté | `facebook.com/hacked` · `instagram.com/hacked` |

**Une question, un doute ?**

Avant de cliquer, demandez. Il n'y a pas de question bête en sécurité.

contact@axelites.com
+33 1 87 66 36 82
axelites.com · LinkedIn

À COCHER

# Ma check-list sécurité

Cochez chaque ligne une fois l'action réalisée. Refaites le point tous les trois mois.

## LES RÉFLEXES

- [ ] J'ai créé un dossier « Mes accès » dans mes favoris avec tous mes services importants.
- [ ] Je ne clique plus sur les liens reçus par e-mail, SMS ou messagerie.

## MOTS DE PASSE ET DOUBLE AUTHENTIFICATION

- [ ] J'utilise un gestionnaire de mots de passe pour stocker mes mots de passe en lieu sûr.
- [ ] Chaque service a un mot de passe unique.
- [ ] La double authentification est active sur mon e-mail.
- [ ] La double authentification est active sur Facebook, Instagram et mes autres réseaux.
- [ ] La double authentification est active sur ma banque, mon site et mon nom de domaine.
- [ ] J'ai activé une clé d'accès (empreinte, Face ID) là où c'est possible.
- [ ] Mes codes de secours sont imprimés ou rangés dans mon gestionnaire.

## COMPTES ET ÉQUIPE

- [ ] Mon téléphone et mon adresse de secours sont à jour.
- [ ] J'ai vérifié les appareils connectés et les transferts automatiques de ma boîte e-mail.
- [ ] Mon portefeuille Meta Business exige la double authentification et compte au moins deux administrateurs.
- [ ] Chaque collaborateur et prestataire a son propre compte, avec les droits minimum.
- [ ] Les anciens salariés et prestataires n'ont plus aucun accès.

## APPAREILS ET SITE

- [ ] Mon ordinateur, mon téléphone et mon navigateur se mettent à jour automatiquement, et mes écrans sont verrouillés.
- [ ] Mon site est mis à jour régulièrement et sauvegardé automatiquement.

INFORMATIONS

# À propos de ce document

Ce guide est conçu par **Axelites SARL** pour sensibiliser ses clients et leurs propres clients aux bons réflexes de sécurité numérique. Il est volontairement non technique.

**Libre de diffusion** : vous pouvez le transmettre à vos équipes, vos partenaires et vos clients, à condition de ne pas le modifier et de conserver la mention d'Axelites SARL.

Les menaces évoluent vite : ce guide est mis à jour régulièrement. Assurez-vous de disposer de la dernière version.

> **Avertissement**
>
> Ce guide est fourni à titre informatif. Il présente des bonnes pratiques générales et ne garantit pas une protection totale contre les attaques. Axelites SARL n'est pas responsable des incidents de sécurité, pertes ou dommages pouvant survenir, que ces conseils aient été appliqués ou non. Les services cités le sont à titre d'exemple et leurs menus peuvent évoluer.

## Retrouvez-nous

| | |
|---|---|
| Notre site | `axelites.com` |
| Maintenance et TMA de votre site | `axelites.com/services/maintenance-tma-magento` |
| LinkedIn | `linkedin.com/company/axelites` |

Axelites SARL · contact@axelites.com · +33 1 87 66 36 82 · axelites.com