ARBORESCENCE STUDIO

GUIDE PRATIQUE

arborescence.studio

Sécurité numérique pour petites structures

Mots de passe, sauvegardes, hameçonnage : le kit opérationnel complet pour une petite entreprise ou une association, sans service informatique dédié.

01 — LE CONSTAT

La sécurité d’une petite structure ne se joue pas sur des outils chers

La grande majorité des incidents subis par les petites structures — perte de données, compte piraté, rançongiciel — ne viennent pas d’une attaque sophistiquée : ils viennent de l’absence de trois réflexes simples, gratuits ou presque, jamais mis en place faute de temps. Ce guide traite ces trois réflexes en priorité, avant tout investissement en outil de sécurité payant.

> **Le principe.** Trois habitudes bien tenues (mots de passe, sauvegardes, vigilance au hameçonnage) éliminent la grande majorité des incidents réels rencontrés par les structures de cette taille — bien avant qu’un pare-feu ou un antivirus payant ne fasse une différence.

02 — MOTS DE PASSE

Ce qui protège vraiment, ce qui ne sert à rien

PRATIQUE	UTILE OU INUTILE ?
Un mot de passe différent par service important	Utile — indispensable
Un gestionnaire de mots de passe (Bitwarden, KeePass)	Utile — élimine le besoin de mémoriser
La double authentification (code envoyé par SMS ou application)	Utile — bloque la plupart des piratages de compte
Changer son mot de passe tous les 3 mois sans raison	Inutile — pousse à des mots de passe plus faibles et prévisibles
Un mot de passe complexe mais réutilisé partout	Dangereux — une seule fuite compromet tous les comptes

> **La priorité n°1.** Activer la double authentification sur la messagerie professionnelle avant toute autre mesure : c’est par la messagerie que transitent la plupart des réinitialisations de mot de passe des autres services.

03 — SAUVEGARDES

La règle 3-2-1, expliquée simplement

- **3 copies** de toute donnée importante — l'originale, plus deux copies.
- **2 supports différents** — par exemple le disque de l'ordinateur et un service en ligne, jamais deux fois le même type de support.
- **1 copie hors site** — hors des locaux physiques, pour survivre à un vol, un incendie ou un dégât des eaux.

Une sauvegarde automatique et programmée vaut infiniment mieux qu'une sauvegarde manuelle "quand on y pense" — dans la pratique, elle n'est presque jamais faite à temps.

> **Le test qui manque presque toujours.** Une sauvegarde qui n'a jamais été restaurée pour de vrai n'est pas une sauvegarde vérifiée. Tester une restauration complète au moins une fois par an, sur un fichier sans importance, pour être certain que ça fonctionne le jour où ça compte.

04 — HAMEÇONNAGE

Reconnaître un message frauduleux

SIGNAL D'ALERTE	POURQUOI
Urgence artificielle ("votre compte sera fermé dans 24h")	Technique classique pour empêcher de réfléchir avant de cliquer
Adresse d'expéditeur qui ressemble à s'y méprendre à la vraie	Toujours vérifier l'adresse complète, pas seulement le nom affiché
Lien qui ne mène pas où le texte le laisse penser	Survoler le lien sans cliquer pour voir la vraie destination
Demande de mot de passe ou de coordonnées bancaires par message	Aucun service sérieux ne le demande jamais de cette façon

> **Le réflexe qui protège toute une équipe.** En cas de doute, ne jamais cliquer — vérifier directement en tapant l'adresse du service dans le navigateur, ou en appelant l'expéditeur par un canal déjà connu. Un seul clic évité arrête l'incident avant qu'il ne commence.

05 — RÉAGIR À UN INCIDENT

Les premiers gestes, dans l’ordre

1. Débrancher l’appareil concerné du réseau (câble ou Wi-Fi), sans l’éteindre si possible.
2. Changer immédiatement les mots de passe des comptes sensibles, depuis un autre appareil.
3. Prévenir les personnes concernées si des données personnelles ont pu être exposées.
4. Si des données personnelles sont concernées, évaluer l’obligation de notification à la CNIL sous 72 heures.
5. Restaurer depuis la sauvegarde la plus récente vérifiée saine, jamais depuis une copie potentiellement déjà compromise.

06 — CHECKLIST

À mettre en place, dans l’ordre de priorité

- ☐ Double authentification activée sur la messagerie professionnelle
- ☐ Gestionnaire de mots de passe adopté par toute l’équipe
- ☐ Sauvegarde automatique programmée, sur un support hors site
- ☐ Une restauration test effectuée dans l’année
- ☐ Une personne référente identifiée en cas de doute sur un message reçu
- ☐ Une procédure écrite, même courte, pour les 24 premières heures d’un incident