

GUIDE GRATUIT · ÉDITION 2026

Cybersécurité pour TPE arnaques, piratage, sauvegardes

Les arnaques qui visent les petites entreprises, les 10 gestes qui protègent l'essentiel, et quoi faire en cas d'attaque. Simple, concret, sans jargon.

Les 10 gestes | Les arnaques | Réagir

Growth System Experts
GROWTHSYSTEMEXPERTS.COM

SOMMAIRE

Ce que contient ce guide

01 Pourquoi les TPE sont visées p. 03
02 L'hameçonnage p. 04
03 Le faux fournisseur et le faux patron p. 05
04 Le rançongiciel p. 06
05 Les mots de passe p. 07
06 La double vérification p. 08
07 Les sauvegardes p. 09
08 Les mises à jour et les appareils p. 10
09 Le Wi-Fi et le travail mobile p. 11
10 Réagir en cas d'attaque p. 12
11 Les 10 gestes essentiels p. 13
12 Former et vérifier p. 14
13 Automatiser p. 15

L'ESSENTIEL EN 30 SECONDES

Se méfier des urgences

La plupart des arnaques jouent sur la pression et la peur.

Des mots de passe solides

Longs, uniques, rangés dans un gestionnaire.

La double vérification

Un code en plus du mot de passe sur les comptes clés.

Des sauvegardes testées

Une copie hors ligne qui permet de tout récupérer.

LE PRINCIPE DE CE GUIDE

Pas besoin d'être expert pour se protéger. Une poignée de gestes simples **réduit fortement le risque face aux attaques courantes**. Ce guide vous les donne, dans l'ordre.

01 · COMPRENDRE

Pourquoi les TPE sont visées

Les pirates ne visent pas seulement les grandes entreprises. Les petites sont souvent moins protégées.

Des attaques automatiques

Les pirates envoient des milliers de messages et attendent qu'un seul clique.

De l'argent facile

Virements frauduleux, rançons, revente de données.

Le facteur humain

Un clic pressé, un mot de passe réutilisé, une pièce jointe ouverte.

EXEMPLE

Une agence reçoit un faux e-mail de son hébergeur. Elle saisit son mot de passe sur une fausse page. Le lendemain, sa boîte mail envoie des arnaques à tous ses clients.

02 · L'HAMEÇONNAGE

L'hameçonnage

Un faux message qui imite une banque, un fournisseur ou une administration, pour voler vos accès.

Les signes d'alerte

- ☐ Une urgence ou une menace
- ☐ Une adresse d'expéditeur étrange
- ☐ Un lien qui ne mène pas au vrai site
- ☐ Une demande de mot de passe ou de code
- ☐ Des fautes ou un ton inhabituel

Le bon réflexe

- ☐ Ne pas cliquer
- ☐ Aller sur le site en tapant soi-même l'adresse
- ☐ Appeler l'organisme à un numéro connu
- ☐ Signaler le message
- ☐ Supprimer

ATTENTION

Aucune banque ni administration ne vous demande votre mot de passe ou un code reçu par SMS, ni par e-mail ni par téléphone.

03 · LES VIREMENTS

Le faux fournisseur et le faux patron

Deux arnaques qui visent directement vos virements.

Le faux changement de RIB

Un « fournisseur » annonce un nouveau compte bancaire. Le paiement part chez l'escroc.

Le faux dirigeant

Un message urgent et confidentiel demande un virement exceptionnel.

La règle d'or

Tout changement de coordonnées bancaires ou toute demande de virement inhabituelle se vérifie **par téléphone, à un numéro déjà connu**, jamais celui indiqué dans le message.

À RETENIR

Mettez cette règle par écrit et partagez-la avec toute personne qui peut faire des paiements dans l'entreprise.

04 · LE RANÇONGICIEL

Le rançongiciel

Un programme qui bloque vos fichiers et réclame une rançon pour les débloquer.



La meilleure protection

Une sauvegarde récente, hors ligne, qui permet de tout restaurer sans payer.

Ne pas payer

Payer ne garantit pas de récupérer vos fichiers et finance les attaques suivantes.

05 · LES ACCÈS

Les mots de passe

Beaucoup de piratages commencent par un mot de passe faible ou réutilisé.

Un bon mot de passe

- ☐ Long : au moins 12 caractères, plus pour les comptes clés
- ☐ Unique : un par service
- ☐ Une phrase de passe facile à retenir
- ☐ Rangé dans un gestionnaire de mots de passe

À bannir

- ☐ Le même mot de passe partout
- ☐ Un nom, une date de naissance
- ☐ Un fichier « mots de passe » sur le bureau
- ☐ Les mots de passe partagés par message

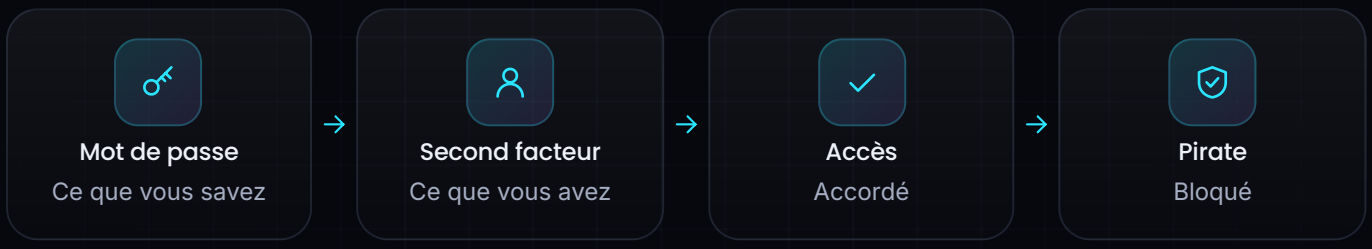
LE GESTIONNAIRE DE MOTS DE PASSE

Un coffre-fort chiffré qui retient tous vos mots de passe. Vous n'en retenez plus qu'un seul, très solide.

06 · LA DOUBLE VÉRIFICATION

La double vérification

Même avec votre mot de passe, un pirate a beaucoup plus de mal à entrer sans le second facteur.



À activer en priorité

- ☐ Votre messagerie
- ☐ Votre banque
- ☐ Votre hébergeur et nom de domaine
- ☐ Vos comptes de paiement
- ☐ Vos réseaux sociaux professionnels
- ☐ Votre stockage en ligne

✓ BONNE PRATIQUE

Une application d'authentification ou une clé de sécurité est en général plus sûre qu'un code par SMS.

07 · LES SAUVEGARDES

Les sauvegardes

Votre assurance contre le piratage, la panne et le vol.

LA RÈGLE 3-2-1

3 copies · **2 supports différents** · **1 copie hors ligne ou hors site**

Une copie déconnectée échappe à un rançongiciel.

Automatique

Une sauvegarde programmée, qui ne dépend pas de votre mémoire.

Testée

Restaurez un fichier de temps en temps pour vérifier que ça marche.

08 · LE MATÉRIEL

Mises à jour et appareils

Les mises à jour ferment les failles connues. Les ignorer laisse la porte ouverte.

Mises à jour automatiques

Ordinateurs, téléphones, logiciels, site internet.

Un antivirus actif

Celui du système suffit souvent, s'il est à jour.

Un écran verrouillé

Code ou empreinte, verrouillage automatique.

APPAREIL PERDU OU VOLÉ

Activez la localisation et l'effacement à distance. Chiffrez les ordinateurs portables : un disque chiffré est illisible sans votre code.

09 · EN DÉPLACEMENT

Le Wi-Fi et le travail mobile

Travailler de partout, oui, mais avec quelques précautions.

Les Wi-Fi publics

- [ ] Éviter les opérations sensibles
- [ ] Préférer le partage de connexion du téléphone
- [ ] Vérifier le cadenas du site
- [ ] Oublier le réseau après usage

Au bureau ou à la maison

- [ ] Changer le mot de passe de la box
- [ ] Un réseau invité pour les visiteurs
- [ ] Mettre à jour la box
- [ ] Séparer usage perso et pro si possible

10 · RÉAGIR

Réagir en cas d'attaque

Les premières heures comptent. Gardez cette page à portée de main.

1. **Isoler** — Débrancher l'appareil d'internet, sans l'éteindre. — TOUT DE SUITE
2. **Changer les mots de passe** — Depuis un autre appareil sain, en commençant par la messagerie. — VITE
3. **Prévenir la banque** — En cas de virement frauduleux, le plus tôt possible. — URGENT
4. **Se faire aider** — Le dispositif officiel cybermalveillance.gouv.fr oriente vers des professionnels. En urgence : 17Cyber. — AIDE
5. **Porter plainte** — Garder les preuves : messages, captures, relevés. — PLAINTE
6. **Prévenir la CNIL si besoin** — Si des données personnelles sont touchées : sous 72 heures, sauf risque improbable. — RGPD

11 · L'ESSENTIEL

Les 10 gestes essentiels

Si vous ne faites que ça, vous êtes déjà nettement mieux protégé.

- ☐ Mots de passe longs et uniques
- ☐ Gestionnaire de mots de passe
- ☐ Double vérification sur les comptes clés
- ☐ Sauvegarde automatique
- ☐ Une copie hors ligne
- ☐ Mises à jour automatiques
- ☐ Écrans verrouillés
- ☐ Vérifier tout changement de RIB par téléphone
- ☐ Méfiance face aux urgences
- ☐ Plan de réaction connu de tous

✓ BONNE PRATIQUE

Commencez par les trois premiers cette semaine : mots de passe, gestionnaire et double vérification. C'est l'essentiel.

12 · DURER

Former et vérifier

La sécurité est une habitude, pas un réglage unique.

CHAQUE MOIS

10 minutes

- [ ] Vérifier les sauvegardes
- [ ] Installer les mises à jour

CHAQUE TRIMESTRE

30 minutes

- [ ] Retirer les accès inutiles
- [ ] Tester une restauration

CHAQUE ANNÉE

1 heure

- [ ] Sensibiliser l'équipe
- [ ] Revoir le plan de réaction

POUR ALLER PLUS LOIN

Nos guides **RGPD pour TPE : la checklist simple** et **Compte bloqué ou suspendu : les recours**.

13 · AUTOMATISER

La sécurité en automatique

Les meilleures protections sont celles qui fonctionnent sans y penser.

Sauvegardes
Programmées

→

Mises à jour
Automatiques

→

Alertes
Connexions suspectes

→

Rappels
Vérifications

Ce qui s'automatise

- ☐ Les sauvegardes et leur contrôle
- ☐ Les mises à jour
- ☐ Les alertes de connexion
- ☐ Les rappels de vérification

Ce que vous gardez

- ☐ La vigilance
- ☐ Le choix des accès
- ☐ La vérification des virements
- ☐ La formation de l'équipe

Des automatisations pensées sécurité

Vos données restent sur vos comptes, avec des accès limités et des sauvegardes. Sur devis gratuit.

Demander mon devis gratuit → **WhatsApp**

growthsystemexperts.com · WhatsApp +34 663 29 49 52 · contact@growthsystemexperts.com

PASSER À L'ACTION

Protégez votre activité

Nous mettons en place vos automatisations avec des accès limités, des sauvegardes et vos données chez vous.

Devis gratuit
Par écrit, sous 24 h ouvrées

Acompte de 50 %
Solde à la livraison

Tout est écrit
Devis et contrat clairs

Vos données chez vous
Installé sur vos comptes

Parlons de vos outils

Dites-nous comment vous travaillez aujourd'hui. Nous vous proposons une mise en place simple, avec un prix clair.

Demander mon devis gratuit → **WhatsApp**

contact@growthsystemexperts.com

growthsystemexperts.com · WhatsApp +34 663 29 49 52 · contact@growthsystemexperts.com

Sources

Recommandations du dispositif national d'assistance aux victimes de cybermalveillance (cybermalveillance.gouv.fr) · Guide des bonnes pratiques de l'ANSSI pour les TPE et PME · RGPD : articles 32 et 33.

Guide d'information générale, à jour en octobre 2026. En cas d'attaque grave, faites-vous accompagner par un professionnel. © 2026 Growth System Experts. Usage personnel, reproduction et revente interdites.