FICHE PRATIQUE

Que faire en cas de piratage

Les premières heures sont décisives. Voici la marche à suivre, étape par étape.

Étape 1 : isoler

- **Débranchez** l'appareil concerné du réseau (câble Ethernet, Wi-Fi coupé).
- Ne l'éteignez **pas** tout de suite : des éléments d'enquête peuvent disparaître.
- Identifiez ce qui semble compromis : un poste, une boîte mail, un serveur, tout le réseau ?

Étape 2 : contenir

- Changez les mots de passe des comptes critiques **depuis un appareil sain**.
- Révoquez les sessions actives (email, cloud, réseaux sociaux).
- Coupez l'accès aux comptes des collaborateurs concernés si nécessaire.

Étape 3 : alerter

- Prévenez votre **dirigeant** ou DPO.
- Contactez votre **assurance cyber** (si vous en avez une) : elle peut financer la remédiation.
- Prévenez votre **banque** si des comptes financiers sont touchés.

Étape 4 : signaler officiellement

- **cybermalveillance.gouv.fr** : diagnostic gratuit + mise en relation avec un expert local.
- **Plainte** en gendarmerie ou commissariat (ou via la plateforme THESEE pour les particuliers).
- **CNIL** si des données personnelles ont fuité (notification sous 72 h).

Étape 5 : restaurer

- Repartez d'une **sauvegarde saine**, antérieure à la compromission.
- Réinstallez l'OS si nécessaire (un nettoyage simple ne suffit pas pour un ransomware).
- Faites un **retour d'expérience** écrit pour éviter la récidive.

Ce qu'il ne faut PAS faire

- Payer une rançon (aucune garantie, et financement de la criminalité).
- Communiquer publiquement avant d'avoir mesuré l'impact.
- Effacer des traces utiles à l'enquête.

Vous êtes touché ?
BigFamily Accompagnement intervient en gestion de crise pour les TPE/PME, sur engagement projet.