FICHE PRATIQUE

RGPD pour les nuls

Le règlement européen sur les données personnelles, expliqué simplement aux TPE/PME.

À quoi sert le RGPD ?

Le RGPD protège les données personnelles des personnes physiques : clients, prospects, salariés, fournisseurs. Il s'applique dès que vous traitez la moindre donnée identifiante (nom, email, IP, photo, etc.), même via un simple fichier Excel.

Les 6 principes à retenir

- **Licéité** : un traitement = une base légale (contrat, consentement, obligation légale, intérêt légitime…).
- **Minimisation** : ne collectez que ce qui est strictement utile.
- **Exactitude** : tenez les données à jour, corrigez-les sur demande.
- **Limitation** : fixez une durée de conservation et purgez ensuite.
- **Sécurité** : protégez l'accès (mots de passe, sauvegardes, chiffrement).
- **Transparence** : informez clairement les personnes concernées.

Vos obligations concrètes

- Tenir un **registre des traitements** (modèle CNIL gratuit).
- Publier une **politique de confidentialité** sur votre site.
- Recueillir un consentement valable pour les newsletters et cookies.
- Signer des accords de sous-traitance avec vos prestataires (hébergeur, CRM, paie).
- Notifier toute fuite de données à la CNIL sous **72 h**.

Les pièges classiques

- Demander la date de naissance « par habitude » sans usage réel.
- Conserver les CV non retenus pendant des années.
- Utiliser une boîte mail générique partagée pour gérer les clients.
- Oublier que Google Analytics, Mailchimp ou un CRM US sont des transferts hors UE.

Besoin d'aller plus loin ?
Un DPO externalisé ou un audit RGPD pour structurer votre conformité, sans surcharger vos équipes.

FICHE PRATIQUE

Vérifier un site marchand

8 réflexes avant de saisir votre carte bancaire sur un site inconnu.

Les vérifications express

- L'adresse commence par **https://** et le nom de domaine est exact (méfiez-vous de amaz0n.com, paypa1.fr…).
- Une page **« Mentions légales »** nomme une société, une adresse, un numéro SIREN.
- Les **CGV** existent et précisent : prix, livraison, rétractation de 14 jours, SAV.
- Un moyen de contact **autre qu'un formulaire** (téléphone fixe, email pro).

Les signaux qui doivent alerter

- Promotions à -80 % sur des produits high-tech ou de luxe.
- Paiement uniquement par virement, crypto, ou cartes cadeaux.
- Avis clients tous datés du même mois, écrits dans un français approximatif.
- Site créé il y a moins de 6 mois (vérifiable sur **whois.com**).
- Logos de confiance (Visa, Trusted Shops…) **non cliquables**.

Les bons outils

- **signal-arnaques.com** et **scamadviser.com** : avis et score de confiance.
- **cybermalveillance.gouv.fr** : signalement officiel.
- Votre banque : activez la confirmation par appli (3D Secure) pour chaque paiement.

Si vous avez déjà payé

- Faites **opposition** immédiatement auprès de votre banque.
- Conservez tous les échanges et captures d'écran.
- Déposez plainte en gendarmerie ou via la plateforme THESEE.

FICHE PRATIQUE

Reconnaître un email de phishing

Le phishing reste la porte d'entrée n°1 des cyberattaques contre les TPE/PME.

Les 5 signaux rouges

- **Urgence** : « Votre compte sera bloqué sous 24 h ».
- **Émetteur étrange** : un email qui prétend venir de votre banque mais finit par @gmail.com.
- **Lien suspect** : survolez-le, l'URL réelle s'affiche en bas du navigateur.
- **Pièce jointe inattendue** : facture, CV, ZIP… surtout d'un inconnu.
- **Demande inhabituelle** : virement « urgent » du dirigeant, changement d'IBAN fournisseur.

Le réflexe en 3 temps

- **Stop** : ne cliquez sur rien, ne répondez pas.
- **Vérifiez** par un autre canal : appelez votre interlocuteur sur son numéro habituel.
- **Signalez** à **signal-spam.fr** ou **phishing-initiative.fr**, puis supprimez.

Les arnaques du moment

- Faux mail Ameli, Impôts, Chronopost, Vinted, Netflix.
- Fausse alerte « connexion suspecte Microsoft 365 ».
- Fraude au président : usurpation du dirigeant pour déclencher un virement.

Côté entreprise

- Activez la **double authentification** sur tous les comptes pro.
- Mettez en place **SPF, DKIM, DMARC** sur votre nom de domaine.
- Formez vos équipes au moins **1 fois par an** avec des cas concrets.

Tester vos équipes ?
BigFamily organise des simulations de phishing pédagogiques, sans piège ni honte.

FICHE PRATIQUE

Hygiène numérique au quotidien

10 gestes simples qui suffisent à neutraliser la majorité des risques.

Les 10 réflexes essentiels

- **Mises à jour** activées automatiquement (OS, navigateurs, applis).
- **Mots de passe uniques** par site, gérés dans un coffre.
- **Double authentification** sur email, banque, réseaux sociaux.
- **Sauvegarde** hebdomadaire de vos fichiers importants.
- **Antivirus** à jour, y compris Windows Defender (suffisant pour beaucoup d'usages).
- **Verrouillage** automatique de l'écran après 5 minutes.
- **Wi-Fi public** : pas d'achat, pas de connexion banque sans VPN.
- **Pièces jointes** : on ne clique pas si l'on n'attend pas.
- **Réseaux sociaux** : profil verrouillé, infos personnelles limitées.
- **Données pro / perso** : séparées sur des comptes différents.

Côté smartphone

- N'installez que des applis depuis les **stores officiels**.
- Vérifiez les permissions (micro, contacts, localisation).
- Activez la **localisation à distance** et l'effacement en cas de vol.

Ce qu'il ne faut JAMAIS faire

- Réutiliser le même mot de passe sur plusieurs sites.
- Brancher une clé USB inconnue trouvée au bureau.
- Communiquer un code reçu par SMS, même au « support technique ».

Un état des lieux complet ?
Audit d'hygiène numérique BigFamily : une demi-journée pour cartographier vos risques.

FICHE PRATIQUE

Sécuriser ses mots de passe

Le mot de passe reste votre première ligne de défense. Voici comment bien faire.

La recette d'un bon mot de passe

- **12 caractères minimum**, idéalement 16+.
- Mélange de majuscules, minuscules, chiffres et symboles.
- **Aucun mot du dictionnaire**, aucune donnée personnelle (nom, date, prénom enfant).
- **Unique** pour chaque service.

La méthode des 3 mots

- Choisissez 3 mots sans rapport : poireau / orage / cravate.
- Ajoutez un symbole et un chiffre : poireau!orage7cravate.
- Mémorisable, long, robuste.

Utilisez un gestionnaire de mots de passe

- Vous ne retenez plus qu'un mot de passe maître.
- Solutions reconnues : **Bitwarden** (gratuit, open source), **1Password**, **Dashlane**, **KeePass**.
- Synchronisé entre tous vos appareils.

La double authentification (2FA)

- Activez-la **partout** : email, banque, réseaux sociaux, cloud.
- Préférez une **appli** (Authy, Google Authenticator) au SMS.
- Pour les comptes critiques : **clé physique** type YubiKey.

Que faire si un mot de passe a fuité ?

- Vérifiez sur **haveibeenpwned.com**.
- Changez-le immédiatement, ainsi que tous les sites qui le partageaient.
- Activez la 2FA sur les comptes concernés.

Déployer un coffre pour votre équipe ?
BigFamily installe et accompagne la prise en main d'un gestionnaire pour vos collaborateurs.

FICHE PRATIQUE

Protéger ses données personnelles

Reprendre le contrôle de ce que les services en ligne savent de vous.

Faites le ménage dans vos comptes

- Listez vos comptes (gestionnaire de mots de passe, recherche dans vos emails).
- Supprimez ceux que vous n'utilisez plus (**justdeleteme.xyz** aide à trouver les procédures).
- Désactivez la publicité personnalisée sur Google, Facebook, Apple.

Réduisez votre empreinte

- Utilisez un **email d'alias** pour les inscriptions secondaires (SimpleLogin, Firefox Relay).
- Vérifiez régulièrement les **autorisations d'applis** sur votre téléphone.
- Sur les réseaux sociaux : profil privé, listes d'amis cachées, photos limitées.

Vos droits RGPD

- **Droit d'accès** : demander toutes les données qu'une entreprise a sur vous.
- **Droit à l'effacement** : être supprimé des fichiers.
- **Droit d'opposition** : refuser la prospection commerciale.
- Réponse obligatoire **sous 1 mois**. À défaut : plainte CNIL gratuite.

Smartphone : les bons réglages

- iPhone : Réglages › Confidentialité & sécurité.
- Android : Paramètres › Confidentialité.
- Désactivez la géolocalisation des applis qui n'en ont pas besoin.
- Refusez le suivi publicitaire (« App Tracking Transparency »).

Et votre entreprise, que sait-on d'elle ?
Un audit d'empreinte numérique BigFamily révèle ce qui circule sur vous et vos collaborateurs.

FICHE PRATIQUE

Sauvegarder son téléphone

Photos, contacts, conversations : tout récupérer en cas de perte, vol ou casse.

Pourquoi sauvegarder ?

- 1 smartphone sur 5 finit perdu, volé ou cassé dans sa vie utile.
- Une sauvegarde permet de tout retrouver sur un nouveau téléphone en quelques minutes.

iPhone : la sauvegarde iCloud

- Réglages › [votre nom] › iCloud › Sauvegarde iCloud activer.
- 5 Go gratuits, souvent insuffisants : abonnement iCloud+ à 0,99 €/mois (50 Go).
- Sauvegarde automatique chaque nuit quand l'iPhone est branché et en Wi-Fi.
- Alternative locale : **Finder** (Mac) ou **iTunes** (PC) en USB.

Android : la sauvegarde Google

- Paramètres › Google › Sauvegarde activer.
- Stocke contacts, SMS, applis, paramètres dans Google Drive (15 Go gratuits partagés).
- Photos : activez la **sauvegarde Google Photos** séparément.
- Alternative : Samsung Cloud, Mi Cloud, OneDrive selon la marque.

WhatsApp et messageries

- WhatsApp : Réglages › Discussions › Sauvegarde activer (iCloud ou Google Drive).
- Signal et Telegram : sauvegardes manuelles depuis les paramètres.
- Pensez à **chiffrer** la sauvegarde (mot de passe ou clé).

Bonne pratique

- Vérifiez la date de la dernière sauvegarde **une fois par mois**.
- Testez la restauration sur un appareil de test si possible.
- Conservez un export local des photos importantes (disque externe).

Famille, équipe, association ?
BigFamily met en place une routine de sauvegarde claire, qui tourne toute seule.

FICHE PRATIQUE

Sauvegarder son ordinateur

La règle d'or 3-2-1, traduite en pratique pour un PC ou un Mac.

La règle du 3-2-1

- **3 copies** de vos données.
- **2 supports différents** (ex. disque interne + disque externe).
- **1 copie hors site** (cloud ou disque chez un proche).

Sur Windows

- **Historique des fichiers** sur un disque externe (intégré à Windows).
- Outil de **sauvegarde système** (image complète) via Panneau de configuration.
- Cloud : OneDrive (5 Go gratuits, 1 To avec Microsoft 365).

Sur Mac

- **Time Machine** sur un disque externe : sauvegardes horaires automatiques.
- iCloud Drive pour les fichiers du Bureau et Documents.
- Pour une image complète : **Carbon Copy Cloner** ou **SuperDuper!**.

Le cloud chiffré (hors site)

- **pCloud**, **Proton Drive**, **kDrive Infomaniak** : hébergement en Europe.
- **Backblaze** : sauvegarde illimitée pour 9 €/mois, idéal pour gros volumes.
- Vérifiez que **le chiffrement** est activé (clé maître côté utilisateur).

Ce que beaucoup oublient

- Une sauvegarde non testée = pas une sauvegarde. **Testez la restauration** 1 fois par an.
- Un disque externe branché en permanence subit aussi un ransomware. Débranchez-le entre 2 sauvegardes.
- Documents pro : pensez à sauvegarder aussi vos **boîtes mail** et vos **SaaS**.

FICHE PRATIQUE

Sécuriser son Wi-Fi domestique

Votre box est la porte d'entrée de tous vos appareils. Voici comment bien la fermer.

Les réglages incontournables

- Changez le **mot de passe administrateur** de la box (≠ mot de passe Wi-Fi).
- Choisissez un **mot de passe Wi-Fi long** (16 caractères) en chiffrement **WPA3** (ou WPA2 à défaut).
- Renommez le SSID sans révéler votre identité (ex. : « FreeBox-Martin » « ColibriRouge »).
- Désactivez le **WPS** (bouton d'appairage facile = faille).
- Maintenez le **firmware** de la box à jour (souvent automatique chez les FAI).

Un réseau invité pour les visiteurs

- Activez le **Wi-Fi invité** pour les amis et la famille élargie.
- Sépare leurs appareils de vos imprimantes, NAS et caméras.

Pour les objets connectés (IoT)

- Ampoules, enceintes, caméras : mettez-les sur le **réseau invité** ou un VLAN dédié.
- Changez les mots de passe par défaut.
- Désactivez les services UPnP, accès distant et P2P inutilisés.

Vérifier qui est connecté

- Interface de la box (192.168.1.1) liste des appareils connectés.
- Appli mobile de votre FAI (Freebox, Orange, SFR…).

En déplacement

- Ne faites jamais de paiement ni de connexion banque sur un Wi-Fi public sans **VPN**.
- Préférez le **partage de connexion** 4G/5G de votre téléphone.

> **Pro à domicile ou télétravail ?**
> BigFamily audite votre Wi-Fi et installe un routeur pro segmenté si nécessaire.

FICHE PRATIQUE

Bien choisir son antivirus

Ce qu'un antivirus fait (et ne fait pas) en 2026, et comment choisir le bon.

Ce qu'un antivirus moderne fait

- Détection des virus, ransomwares, chevaux de Troie.
- Analyse en temps réel des fichiers et téléchargements.
- Filtrage web : blocage des sites malveillants.
- Protection contre le phishing dans les navigateurs.
- Souvent inclus : pare-feu, contrôle parental, gestionnaire de mots de passe.

Ce qu'il ne fait PAS

- Vous protéger de vos propres erreurs (clic sur un lien, divulgation de mot de passe).
- Sécuriser un compte mal configuré (mot de passe faible, pas de 2FA).
- Remplacer les sauvegardes.

Windows Defender suffit-il ?

- Pour un usage personnel courant : **oui**, dans la majorité des cas.
- Pour une TPE qui manipule beaucoup d'emails et de fichiers clients : un EDR pro est plus adapté.
- Sur Mac : la protection intégrée est solide, un antivirus tiers reste optionnel.

Comment choisir

- Consultez les tests indépendants : **AV-TEST**, **AV-Comparatives**.
- Évitez les antivirus gratuits qui vendent vos données ou affichent de la pub.
- Vérifiez l'impact sur les performances de votre machine.
- Privilégiez un éditeur européen pour les données sensibles.

Pour les pros : passer à l'EDR

- EDR = Endpoint Detection and Response : antivirus + détection comportementale + console centralisée.
- Solutions courantes : Microsoft Defender for Business, Bitdefender, ESET, SentinelOne.

FICHE PRATIQUE

Mettre à jour ses appareils

80 % des cyberattaques exploitent une faille déjà corrigée. Ne soyez pas victime d'un correctif oublié.

Pourquoi c'est critique

- Chaque mise à jour comble des failles découvertes depuis la précédente.
- Les attaquants scannent en permanence Internet à la recherche d'appareils non à jour.
- Un appareil non patché reste vulnérable **indéfiniment**.

Ce qu'il faut mettre à jour

- **Système d'exploitation** : Windows, macOS, iOS, Android, Linux.
- **Navigateurs** : Chrome, Firefox, Edge, Safari.
- **Applications** : suite bureautique, lecteur PDF, messageries.
- **Box internet et routeurs** : firmware.
- **Objets connectés** : caméras, imprimantes, NAS, enceintes.

Activer la mise à jour automatique

- Windows : Paramètres › Windows Update › Options avancées.
- macOS : Réglages Système › Général › Mise à jour de logiciels.
- iOS / Android : activer les MAJ auto dans les paramètres système et store.
- Box : la plupart des FAI font ces MAJ automatiquement, vérifiez quand même.

Fin de support : le piège

- Windows 10 : fin du support en octobre 2025 migrer vers Windows 11 ou Linux.
- Smartphones : 2 à 5 ans de MAJ selon les marques. Au-delà, à remplacer.
- Objets connectés : vérifiez la durée de support promise par le fabricant.

Pour les pros

- Tenez un **inventaire** de vos appareils, OS et logiciels.
- Définissez une **fenêtre de maintenance** mensuelle.
- Pour les serveurs : testez les MAJ sur un environnement de pré-production.

FICHE PRATIQUE

Sensibiliser ses collaborateurs

Comment transformer vos équipes en première ligne de défense, sans les noyer.

Pourquoi former vos équipes

- 9 incidents sur 10 commencent par une erreur humaine (clic, partage, négligence).
- Un salarié formé identifie un phishing en moyenne 3× mieux qu'un salarié non formé.
- C'est une **obligation** de moyens pour le RGPD.

Les thèmes à couvrir en priorité

- Mots de passe et double authentification.
- Phishing et fraude au président.
- Données personnelles et RGPD au quotidien.
- Télétravail et Wi-Fi hors bureau.
- Réflexe en cas de doute (qui contacter ?).

Le format qui marche

- **Sessions courtes** (30 à 45 min) plutôt qu'une grosse journée par an.
- **Cas concrets** tirés de votre secteur d'activité.
- **Quizz** et mises en situation interactives.
- **Simulations de phishing** régulières (1 par trimestre).

Le rythme idéal

- Une session d'**onboarding** pour chaque nouvel arrivant.
- Un **rappel annuel** pour tout le monde.
- Des **communications courtes** (1 fois par mois) sur l'actualité cyber.

Mesurer l'impact

- Taux de clic sur les simulations de phishing.
- Nombre de signalements spontanés par les salariés.
- Quizz avant/après formation.

Sessions d'1 heure, à la carte ?
BigFamily Académie propose des modules courts, ludiques et adaptés à votre secteur.

FICHE PRATIQUE

Bonnes pratiques en télétravail

Travailler de chez soi sans ouvrir la porte aux risques de l'entreprise.

Votre poste de travail

- Utilisez de préférence un **ordinateur fourni par l'entreprise**, séparé du familial.
- Verrouillez l'écran dès que vous quittez la pièce (Win+L ou Ctrl+Cmd+Q).
- Pas de famille ni de visiteurs sur votre poste pro.
- Filtre de confidentialité d'écran si vous travaillez en lieu public.

Votre réseau

- Wi-Fi domestique en WPA3 ou WPA2, mot de passe long.
- **VPN** de l'entreprise systématiquement activé avant tout accès aux ressources internes.
- Jamais de Wi-Fi public sans VPN (gare, hôtel, café).

Partage de fichiers

- Uniquement via les **outils validés** par l'entreprise (SharePoint, Drive, Nextcloud…).
- Jamais de pièce jointe sensible par email perso ou WeTransfer non chiffré.
- Pas de clé USB personnelle sur le poste pro.

Visioconférences

- Vérifiez l'arrière-plan ou utilisez un fond virtuel.
- Coupez le micro et la caméra entre les réunions.
- Ne partagez votre écran qu'après avoir fermé les fenêtres sensibles.

Côté hygiène de vie numérique

- Plages horaires définies : la cybersécurité fatigue moins quand vous êtes reposé.
- Signalez immédiatement tout incident, même mineur, à votre référent.
- Effacez les données pro de vos appareils quand vous changez de poste.

Charte télétravail à formaliser ?
BigFamily aide les TPE à rédiger une charte simple, lisible, applicable.

FICHE PRATIQUE

Sécurité sur les réseaux sociaux

Profiter des réseaux sans en payer le prix fort en données ou en réputation.

Réglages de confidentialité

- Profil privé par défaut sur Instagram, Facebook, TikTok, X.
- Listes d'amis et abonnements **cachés**.
- Géolocalisation désactivée pour les photos.
- Visibilité du téléphone et de l'email : amis uniquement, ou personne.

Ce qu'on ne publie pas

- Photos d'enfants identifiables (école, prénom + nom).
- Plaque d'immatriculation, carte d'embarquement, billets de spectacle.
- Vacances en temps réel (signal qu'il n'y a personne à la maison).
- Informations professionnelles confidentielles, organigrammes.

Sécurité du compte

- Mot de passe unique et long.
- **Double authentification** activée (appli plutôt que SMS).
- Vérifiez régulièrement les **sessions actives** et les applis tierces autorisées.
- Email de récupération sécurisé.

Reconnaître les arnaques

- Faux profils qui tentent de devenir « ami » pour collecter des infos.
- Faux jeux concours, faux SAV de marque, faux livreurs.
- Investissements en crypto ou en trading « miraculeux ».

Pour les pros

- Comptes pro et perso bien séparés.
- Sur LinkedIn : attention aux fausses demandes de recruteurs (collecte d'infos).

Ateliers pour ados ou seniors ?
BigFamily Académie intervient aussi en milieu scolaire, associatif, et en entreprise.

FICHE PRATIQUE

Protéger ses enfants en ligne

Accompagner les 6-17 ans dans un monde numérique qu'ils maîtrisent souvent mieux… techniquement.

La règle d'or : dialoguer

- Posez des règles claires, expliquées, et révisées avec l'âge.
- Établissez un climat où l'enfant peut **signaler** un souci sans peur d'être puni.
- Connaissez les applis qu'il utilise avant de les interdire.

Contrôle parental

- **iPhone / iPad** : Temps d'écran (limites par appli, restrictions de contenu).
- **Android** : Google Family Link.
- **PC / Mac** : comptes enfant avec filtres.
- **Box internet** : la plupart des FAI proposent un filtre Internet familial gratuit.

Réseaux sociaux et messageries

- Aucun réseau social en théorie avant **13 ans** (15 ans pour TikTok et Snap).
- Comptes en privé, listes d'amis fermées.
- Pas de prénom + nom + école dans le pseudo ou la bio.

Cyberharcèlement : reconnaître les signaux

- Repli, perte de sommeil, refus d'aller à l'école.
- Suppression brutale des comptes ou changement de pseudo.
- Évitement du téléphone ou hypervigilance.

Quoi faire en cas de problème

- Numéro **3018** (gratuit, anonyme, harcèlement et violences numériques).
- Plateforme **pharos.gouv.fr** pour signaler des contenus illégaux.
- Conservez les captures d'écran avant de bloquer ou supprimer.

Ateliers parents-enfants ?
BigFamily Académie propose des sessions en école, MJC et associations familiales.

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.

FICHE PRATIQUE

Réagir à un vol de téléphone

Les 30 premières minutes qui font la différence entre simple perte matérielle et catastrophe.

Dans les 30 minutes

- **Localisez** et verrouillez à distance : Localiser (Apple), Find My Device (Google).
- Si récupération impossible : déclenchez l'**effacement à distance**.
- Appelez votre **opérateur** pour suspendre la ligne et bloquer la carte SIM.
- Fournissez l'**IMEI** à l'opérateur (sur l'emballage, ou via *#06# sur un autre appareil).

Dans les heures qui suivent

- Changez les **mots de passe** des comptes accessibles depuis le téléphone : email, banque, réseaux sociaux.
- Vérifiez les **sessions actives** et déconnectez les appareils inconnus.
- Bloquez les **moyens de paiement** mobiles (Apple Pay, Google Pay).

Démarches administratives

- **Déclaration de vol** en gendarmerie ou commissariat (à présenter à l'assurance).
- Informez votre **assurance** (responsabilité civile, multirisque habitation, ou contrat dédié).
- Si une carte d'identité ou un permis numérique étaient stockés : signalez à France Identité.

Préparer l'éventualité (avant le vol)

- Activez **Localiser** et la **sauvegarde cloud** dès l'achat.
- Notez l'**IMEI** dans un endroit sûr (carnet, gestionnaire de mots de passe).
- Configurez un **code PIN** sur la carte SIM en plus du verrouillage de l'écran.

Besoin d'être guidé pas à pas ?
BigFamily Accompagnement vous épaule dans les 24 h suivant un vol — démarches, comptes, assurance.

FICHE PRATIQUE

Récupérer ses comptes compromis

Email, Facebook, Google, Instagram : procédures officielles et bons réflexes.

Réflexes communs à tous les services

- Tentez d'abord la procédure de **récupération de mot de passe** standard.
- Si l'email associé a aussi été changé : passez par les formulaires de récupération avancée.
- Préparez : preuves d'identité, ancien mot de passe, dates et lieux de connexion habituels.

Compte Google

- **g.co/recover** : assistant guidé, peut prendre 24 à 72 h.
- Une fois récupéré : changez le mot de passe, activez la 2FA, vérifiez les filtres de redirection des emails.

Compte Microsoft / Outlook

- **account.live.com/acsr** : formulaire de récupération.
- Préparez des éléments de preuve : contacts récents, sujets de mails envoyés.

Facebook et Instagram

- **facebook.com/hacked** : procédure dédiée.
- Instagram : Aide à la connexion vérification d'identité par selfie vidéo.
- Activez ensuite la 2FA et révoquez les applis tierces.

Banque

- Appelez immédiatement votre conseiller ou le numéro d'urgence figurant au dos de la carte.
- Faites opposition, contestez par écrit toute opération frauduleuse sous 13 mois maximum.
- Déposez plainte (la banque vous le demandera pour vous rembourser).

Après récupération

- Vérifiez les **règles de transfert** automatique d'emails.
- Examinez les **applis autorisées** et révoquez celles que vous ne reconnaissez pas.
- Mettez en place la **2FA** (par appli ou clé physique).

Démarches fastidieuses ?
BigFamily Accompagnement prend en charge la coordination de la récupération de vos comptes.

FICHE PRATIQUE

Signaler une cyberattaque

Tous les bons interlocuteurs, avec leur rôle exact, pour ne rien oublier.

cybermalveillance.gouv.fr

- Diagnostic en ligne **gratuit** en quelques minutes.
- Mise en relation avec des prestataires labellisés près de chez vous.
- Conseils personnalisés selon le type d'incident.
- Pour particuliers, TPE/PME et collectivités.

La plainte pénale

- Gendarmerie ou commissariat (dépôt physique).
- **Plateforme THESEE** (service-public.fr) : pour les particuliers victimes d'arnaque en ligne.
- **Pré-plainte en ligne** sur le portail national : gain de temps.

La CNIL

- Obligatoire **sous 72 h** en cas de violation de données personnelles.
- Formulaire dédié sur **cnil.fr**.
- Documenter même les violations non notifiées dans un registre interne.

L'ANSSI (selon les cas)

- Opérateurs d'importance vitale, administrations, et incidents de grande ampleur.
- **cert.ssi.gouv.fr** pour les signalements techniques.

Pharos (contenus illégaux)

- **internet-signalement.gouv.fr** : pour signaler des contenus illicites en ligne.
- Harcèlement, escroqueries, contenus haineux ou pédopornographiques.

Votre assureur

- Si vous avez une **cyber-assurance**, déclarez l'incident dans les délais contractuels (souvent 5 jours).
- L'assureur peut financer expertise, communication de crise, restauration des données.

Pris dans la crise ?
BigFamily Accompagnement coordonne ces démarches à votre place pour vous laisser gérer le reste.

FICHE PRATIQUE

Préparer un plan de continuité

Anticiper l'inacceptable : 6 questions pour ne pas mettre la clé sous la porte après un incident.

1. Qu'est-ce qui est vital ?

- Listez vos **5 à 10 processus** sans lesquels l'activité s'arrête (facturation, paie, production...).
- Pour chacun : quels logiciels, fichiers, accès, personnes ?
- Combien de temps pouvez-vous tenir sans (RTO) et combien de données pouvez-vous perdre (RPO) ?

2. Vos données sont-elles vraiment sauvegardées ?

- Sauvegardes **3-2-1** sur tous les systèmes critiques.
- Testez la **restauration** au moins 1 fois par an.
- Sauvegardez aussi vos SaaS (CRM, comptabilité, emails).

3. Qui appelle qui ?

- Annuaire de crise (papier + cloud) : équipe, prestataires IT, banque, assureur, CNIL.
- Numéros directs, pas seulement standards.
- Désignez un **responsable communication** en cas d'incident.

4. Où travaillez-vous si vos locaux sont inaccessibles ?

- Solution de repli (télétravail, espace de coworking, locaux partenaires).
- Accès distants aux outils déjà testés.

5. Que dit-on aux clients ?

- Message-type prêt à envoyer en cas d'incident, validé en amont.
- Canaux alternatifs si email indisponible (site, réseaux sociaux, SMS).

6. Comment apprend-on de l'incident ?

- Retour d'expérience formalisé dans les 30 jours.
- Plan d'actions concrètes priorisées.
- Mise à jour du plan de continuité en conséquence.

Co-construire votre PCA ?

BigFamily Accompagnement structure votre plan de continuité en 2 ou 3 ateliers.