Fiches imprimables

Protégez votre vie privée numérique — édition 2026

Ces fiches complètent le livre. Les exemples sont fictifs. N’y inscrivez jamais un mot de passe, un code bancaire ou un code de récupération.

Annexe A - Diagnostic personnel en 20 questions

Répondez par **oui**, **non** ou **à vérifier**. Un « non » n’est pas une faute : il signale seulement une action possible. Ne notez aucun mot de passe, code bancaire ou secret sur cette fiche.

Comptes et récupération

1. Ma messagerie principale utilise un mot de passe unique.
2. Elle possède un second facteur que je sais récupérer.
3. Mes codes de secours se trouvent hors du téléphone principal.
4. Mon gestionnaire de mots de passe possède une sauvegarde ou une récupération testée.
5. Les numéros et adresses de récupération m’appartiennent encore.

Appareils

1. Le contenu sensible est masqué sur l’écran verrouillé.
2. Le téléphone et l’ordinateur reçoivent encore des mises à jour de sécurité.
3. Le chiffrement de l’ordinateur est confirmé et sa clé est retrouvable.
4. Je peux localiser ou verrouiller le téléphone depuis un autre appareil.
5. Une restauration de fichier a été testée au cours des douze derniers mois.

Diffusion

1. Mon adresse électronique principale n’est pas utilisée pour toutes les inscriptions.
2. Je sais quelles informations apparaissent lorsque je recherche mon nom.
3. Les anciens partages d’agenda, de fichiers et de photos ont été revus.
4. L’adresse du domicile n’est pas publiée sans nécessité.
5. Je distingue le compte professionnel de mes comptes personnels.

Continuité

1. Trois numéros utiles existent aussi sur papier.
2. Je peux passer vingt-quatre heures sans mon téléphone principal.
3. Une personne autorisée sait où commencent mes consignes numériques.
4. Mes documents indispensables possèdent une copie séparée.
5. Une date de révision est inscrite dans mon agenda.

Comptez les réponses « à vérifier ». Choisissez-en trois seulement pour les sept prochains jours : une concernant les comptes, une concernant un appareil et une concernant la continuité.

Annexe B - Plan d’action sur 7 jours et 30 jours

Les sept premiers jours

- **Jour 1 :** recherchez votre nom, votre adresse électronique publique et un pseudonyme. Notez trois expositions.
- **Jour 2 :** protégez la messagerie principale et vérifiez ses moyens de récupération.
- **Jour 3 :** masquez les notifications sensibles et examinez les autorisations récentes du téléphone.
- **Jour 4 :** séparez une inscription commerciale avec un alias ou une adresse dédiée.
- **Jour 5 :** vérifiez le chiffrement de l’ordinateur et retrouvez la récupération hors de l’appareil.
- **Jour 6 :** restaurez un fichier de test depuis votre sauvegarde.
- **Jour 7 :** écrivez trois numéros, un lieu de rendez-vous et la date du prochain contrôle.

Chaque journée doit rester inférieure à vingt minutes. Si une action exige une migration, arrêtez-vous après l’inventaire et planifiez-la.

Les trente jours

Pendant les trois semaines suivantes, corrigez un seul mélange à la fois : compte personnel sur appareil professionnel, document partagé sans date de fin, ancien réseau Wi-Fi, application oubliée, adresse publique ou récupération fragile. Conservez une période de chevauchement avant de fermer une adresse, un numéro ou un compte.

Au trentième jour, reprenez le diagnostic. Gardez cinq protections qui fonctionnent réellement. Abandonnez les organisations trop complexes et inscrivez une révision semestrielle ou annuelle.

Annexe C - Matrice « information, personne, canal, durée »

Utilisez une ligne par situation. Ne recopiez pas le contenu sensible : décrivez seulement sa catégorie.

Information	Personne ou organisme	Canal retenu	Durée utile	Suppression ou révision
Exemple : justificatif de domicile	Organisme identifié	Espace authentifié	Jusqu'à validation	Retirer la copie locale temporaire

Posez cinq questions : cette personne doit-elle vraiment recevoir l'information ? Le canal confirme-t-il son identité ? Une copie moins détaillée suffit-elle ? Combien de temps l'accès doit-il durer ? Qui devra le retirer ?

Annexe D - Fiche de récupération des comptes critiques

Créez une fiche par compte critique et conservez-la dans un lieu protégé. N'y inscrivez pas le mot de passe.

Champ	Votre réponse
Service	
Rôle : messagerie, stockage, banque, administration, travail ou autre	
Adresse officielle du service	
Identifiant utilisé, seulement si la conservation est adaptée	
Second facteur : application, passkey, clé physique, SMS ou autre	
Moyen de secours : type et emplacement, jamais le code	
Adresse ou numéro de récupération	
Appareil de confiance	
Date du dernier test	
Action en cas de perte du téléphone	

Exemple fictif : service « Messagerie principale » ; rôle « récupération des autres comptes » ; second facteur « clé d'accès et application » ; secours « enveloppe dans le coffre familial, sans recopier le code ici » ; dernier test « 15 août 2026 » ; perte du téléphone « utiliser la seconde clé depuis l'ordinateur connu, puis révoquer le téléphone ».

Testez la présence du moyen de secours depuis une seconde session, sans provoquer un blocage. Pour une clé physique, connectez-vous avec chacune des deux clés. Pour un code de secours, vérifiez qu'il est lisible et que le service indique encore où en générer de nouveaux.

Annexe E - Checklist Android, iPhone, Windows et macOS

Android

- [ ] Notifications sensibles masquées.
- [ ] Tableau de bord de confidentialité examiné.
- [ ] Protection contre le vol et localisation activées.
- [ ] Applications inutilisées mises en veille ou supprimées.
- [ ] Protection USB et méthode de charge en déplacement testées.

iPhone

- [ ] Protection en cas de vol réglée.
- [ ] Contrôle de sécurité consulté.
- [ ] Rapport de confidentialité des apps examiné.
- [ ] Localisation retirée d'une photo test.
- [ ] Accessoires filaires et récupération iCloud réglés consciemment.

Windows

- [ ] Presse-papiers local, synchronisé et épinglé vérifié.
- [ ] Autorisations et logiciels de bureau examinés.
- [ ] Recall absent, désactivé ou réglé consciemment.
- [ ] Chiffrement confirmé et clé de récupération séparée.
- [ ] Adresse matérielle aléatoire testée sur un réseau public.

macOS

- [ ] FileVault actif et récupération séparée.
- [ ] Chaque accès complet au disque est justifié.
- [ ] Partage d’écran, accès distant et partage de fichiers contrôlés.
- [ ] Autorisation des nouveaux accessoires réglée.
- [ ] Restauration Time Machine ou autre sauvegarde testée.

Annexe F - Modèles courts pour exercer vos droits

Adaptez ces modèles au contexte et envoyez-les au responsable identifié. Une demande précise est souvent plus exploitable qu'une demande générale.

Accès

« Je souhaite obtenir confirmation que vous traitez des données me concernant ainsi qu'une copie des données relatives à [compte, achat ou période]. Merci d'indiquer leurs catégories, leur origine, leurs destinataires et la durée de conservation prévue. »

Rectification

« L'information suivante est inexacte : [description]. Je vous demande de la rectifier ainsi : [information correcte]. Vous trouverez le justificatif strictement nécessaire en pièce jointe. »

Effacement

« Je demande l'effacement de [donnée ou contenu précis] pour le motif suivant : [finalité terminée, consentement retiré ou autre motif applicable]. Merci de me confirmer l'action réalisée ou de m'indiquer la justification d'un éventuel refus. »

Opposition à la prospection

« Je m'oppose à l'utilisation de mes coordonnées à des fins de prospection. Merci d'enregistrer cette opposition sans me réinscrire à une communication commerciale. »

Conservez la demande, sa date, l'accusé de réception et la réponse. Ne joignez pas spontanément une pièce d'identité complète si une vérification moins intrusive suffit. Les droits connaissent des conditions et des exceptions ; utilisez les modèles de la CNIL et demandez un conseil compétent pour une situation complexe.

Annexe G - Fiche « 24 heures sans mon téléphone »

Conservez cette fiche sur papier, séparée du téléphone. Elle ne doit contenir aucun mot de passe.

Information	Votre réponse
Trois numéros de proches	
Numéros d'urgence et d'opposition du territoire	
Lieu de rendez-vous principal et solution de repli	
Adresse de l'hébergement ou du domicile	
Moyen de transport et horaires indispensables	
Nom de l'opérateur téléphonique	
Emplacement des codes de récupération, jamais les codes	
Information médicale strictement nécessaire	
Moyen de paiement de secours	
Personne autorisée à intervenir	

Exemple fictif : contacts « Camille, Samir, médecin » ; rendez-vous « mairie, puis domicile de Camille » ; opérateur « opérateur mobile A » ; récupération « enveloppe scellée chez Camille » ; donnée médicale « allergie grave à la pénicilline » ; aucun mot de passe ni code.

Testez la fiche pendant une heure : éteignez le téléphone, puis cherchez un trajet, un contact et la procédure de récupération. Corrigez ce qui manque sans transformer la fiche en copie de toute votre vie.

Annexe H - Inventaire de continuité et volontés numériques

L'inventaire explique les dépendances ; il ne contient pas les secrets.

Service ou équipement	Rôle	Personne autorisée	Action attendue	Document ou récupération
Messagerie principale	Récupération des comptes		Maintenir temporairement puis fermer	
Téléphone et numéro	Communications et codes		Bloquer, transférer ou résilier	
Stockage	Documents et photos		Transmettre, archiver ou supprimer	
Abonnements	Paiements récurrents		Résilier ou transférer	
Domaine ou site	Présence publique		Maintenir, rediriger ou fermer	

Exemple fictif : « nom de domaine familial » ; rôle « adresse du site et courriels » ; personne autorisée « Camille » ; action « renouveler six mois puis transférer » ; document « contrat et procédure chez le notaire, récupération dans le coffre ». Aucun mot de passe n'apparaît dans l'inventaire.

Ajoutez la personne à prévenir, les justificatifs probables, l'emplacement de la lettre d'instructions et la date de révision. Séparez cette lettre des clés de récupération. Utilisez les mécanismes officiels de contact légataire ou de compte inactif lorsqu'ils conviennent, puis vérifiez leur périmètre.

Annexe I - Glossaire sans jargon

- **Adresse IP :** numéro utilisé pour acheminer une connexion sur un réseau. La changer ne supprime pas les cookies, les comptes ni l'empreinte du navigateur.
- **Alias :** adresse ou nom intermédiaire qui redirige vers une destination réelle. Il sépare les usages sans garantir l'anonymat.
- **Authentification multifacteur :** combinaison de plusieurs preuves, par exemple mot de passe et clé physique.
- **Chiffrement :** transformation rendant une donnée illisible sans la clé prévue. Il ne protège pas forcément le document lorsqu'il est déjà ouvert.
- **DNS :** service qui traduit un nom de site en adresse technique. Un DNS chiffré ne chiffre pas toute la navigation.
- **Donnée personnelle :** information concernant une personne identifiée ou identifiable, directement ou par recoupement.
- **Espace privé ou profil séparé :** zone isolant certaines applications et données sur un appareil. Son existence peut rester détectable.
- **Métadonnée :** information décrivant un fichier ou une action, comme auteur, date, lieu ou destinataire.
- **Passkey ou clé d'accès :** moyen cryptographique de connexion lié au vrai service, souvent synchronisé ou conservé sur un appareil.
- **Pseudonyme :** nom utilisé publiquement à la place du nom civil. Sa réutilisation peut relier plusieurs activités.
- **Récupération :** procédure permettant de reprendre un compte après la perte d'un mot de passe, d'un téléphone ou d'une clé.
- **Synchronisation :** reproduction de changements entre appareils. Une suppression ou un fichier chiffré par un logiciel malveillant peut se propager ; ce n'est pas toujours une sauvegarde.
- **VPN :** tunnel chiffré jusqu'à un fournisseur intermédiaire. Il déplace une partie de la confiance et ne rend pas anonyme.

Annexe J - Le petit matériel qui mérite vraiment sa place

Vous n’avez pas besoin de tout acheter. Commencez par votre propre chargeur, un câble connu et une pochette déjà disponible. Ajoutez un accessoire seulement s’il répond à une situation que vous rencontrez réellement.

Les coûts ci-dessous sont relatifs : € désigne généralement un petit accessoire, €€ un achat plus conséquent ou deux exemplaires nécessaires.

Matériel	Priorité	Quand il est utile	Test avant de lui faire confiance	Limite à connaître
Chargeur secteur et câble personnels	Essentiel · €	Hôtel, gare, salle d’attente, véhicule de location	Charger le téléphone verrouillé pendant dix minutes	Ne protège pas un appareil déverrouillé ou compromis
Batterie externe	Utile en déplacement · €€	Journée sans prise fiable ou risque de perte du téléphone principal	Vérifier niveau, câble, puissance et recharge une semaine avant le départ	Se décharge au stockage et doit voyager selon les règles du transporteur
Filtre de confidentialité amovible	Utile selon les lieux · €	Train, avion, accueil, espace partagé	Demander à une personne de lire l’écran depuis le côté puis l’arrière	Assombrit parfois l’écran et ne protège pas tous les angles
Câble de charge uniquement ou bloqueur de données USB	Utile en secours · €	Prise USB inconnue lorsqu’aucune prise secteur n’est disponible	Tester charge normale, charge rapide et retrait avant le voyage	Bloque les données compatibles, pas la qualité du chargeur ni l’appareil déverrouillé
Obturateur intégré ou cache de webcam compatible	Utile selon l’appareil · €	Ordinateur utilisé dans une chambre, un bureau partagé ou pour des réunions	Fermer doucement l’écran et vérifier caméra, capteur de lumière et adhésif	Un cache trop épais peut endommager l’écran ; préférer l’obturateur intégré
Deux clés physiques FIDO compatibles	Sensible ou renforcé · €€	Courriel principal, gestionnaire de mots de passe ou compte professionnel compatible	Enregistrer et tester les deux clés, puis simuler la perte de la première	Un service peut ne pas les accepter ; conserver la seconde séparément
Pochette opaque pour la récupération	Essentiel · €	Codes de secours, copie de récupération ou consignes d’urgence	Faire retrouver l’information par la personne autorisée sans révéler le contenu	Cache à la vue, mais ne résiste ni au vol ni à l’ouverture
Témoin d’ouverture numéroté	Situation sensible · €	Sac ou appareil laissé temporairement hors de vue	Photographier le numéro et vérifier l’état au retour	Signale une manipulation possible ; ne l’empêche pas et

Matériel	Priorité	Quand il est utile	Test avant de lui faire confiance	Limite à connaître
				n’identifie pas son auteur

Le choix simple

Pour la plupart des lecteurs, le kit de départ tient en quatre éléments : chargeur secteur, câble personnel, batterie externe entretenue et pochette opaque. Le filtre d’écran dépend des lieux fréquentés. Le bloqueur USB répond à un cas de secours, pas à un besoin quotidien. Les clés physiques deviennent pertinentes lorsque la perte d’un compte critique aurait des conséquences importantes.

Avant d’acheter

- [ ] Je peux nommer la situation précise dans laquelle l’accessoire sera utilisé.
- [ ] J’ai vérifié les dimensions, le connecteur et la compatibilité avec mon appareil.
- [ ] Je connais une solution de secours si l’accessoire est perdu ou incompatible.
- [ ] Je l’ai testé avec des données fictives ou un usage sans conséquence.
- [ ] Je sais ce qu’il ne protège pas.

Références : [P1], [P2], [P3], [P4], [P5].

Annexe K - Fiche réflexe en cas d’incident

Remplissez cette fiche avec des catégories et des références, jamais avec des mots de passe. Conservez-la près du plan de récupération. Le chapitre 20 explique l’ordre des actions.

Heure	Fait observé, sans interprétation	Preuve conservée	Action effectuée	Interlocuteur et référence
Exemple fictif : 08 h 15	Alerte de connexion depuis un appareil inconnu	Capture et courriel original	Mot de passe changé depuis l’adresse officielle ; sessions révoquées	Assistance, dossier EX-204

Les cinq premières décisions

- [ ] Je vérifie d’abord la sécurité physique et l’urgence réelle.
- [ ] Je conserve les originaux sans repartager le contenu exposé.
- [ ] Je protège la messagerie de récupération depuis un appareil de confiance.
- [ ] Je ferme les sessions et préviens les personnes concernées par un autre canal.
- [ ] Je note chaque action, son heure et la référence reçue.

Contacts à préparer

Catégorie	Canal officiel ou emplacement
Banque ou moyen de paiement	
Opérateur téléphonique	
Employeur ou responsable sécurité	
Plateforme ou hébergeur	
Assurance	
Aide aux victimes, police ou gendarmerie	

En danger immédiat, la sécurité des personnes prime sur le remplissage de cette fiche. Ne négociez pas seul avec un harceleur ou un maître-chanteur. Ne payez pas dans l’urgence et n’effacez pas l’appareil avant d’avoir apprécié la nécessité de préserver les preuves.