Présentation Pragmatique des Solutions de Sécurisation

🚨 TRÈS HAUTE PRIORITÉ — Déploiement Immédiat

1. **Smartphone Fantôme**

Base absolue du système de sécurisation. Un OS sécurisé, aucune collecte de données Google. Applications uniques : Signal, Proton, VPN.

2. **Tor + VPN (Onion over VPN)**

Anonymat numérique maximum en deux couches. VPN masque votre IP, Tor masque destination. Configuration : VPN d'abord, puis Tor. Traçabilité zéro même pour Fournisseur d’accès Internet.

3. **Pochette et Sac de Faraday**

Blindage métallique bloquant **tous** les signaux (GPS, WiFi, Bluetooth, RFID, GSM, NFC). Empêche tracking physique. Utilisation : déplacements sensibles, réunions, etc. Test : signal disparaît complètement à l'intérieur.

4. **Détecteur de Signal Radio et Caméra Embarquée**

Détecte mouchards RF, traceurs GPS, balises espion sur fréquences 100 MHz - 8000 MHz. Alerte précoce menaces. Scan pièce/véhicule avant réunion critique.

5. **Brouilleur GPS**

Rend tracking GPS impossible sur périmètre (10-100m selon modèle). Ideal pour empêcher un tracking dans une voiture. Rend tout équipement de tracking obsolète dans une voiture.

6. **Filtres de Confidentialité Écran**

Film protection écran limitant angle vision (30° chaque côté). Empêche lecture par-dessus épaule ou via une Camera de sécurité. Installation : 5-10 minutes. Réduction luminosité acceptable (15-20%).

7. Étuis Anti-RFID

Blindage contre lecture ID, carte bancaires sans contact + passeport. Empêche clonage carte à distance. Utilisation combinée : RFID sleeves + Pochette Faraday = protection complète.

8. Radio Numérique Cryptée (P25, DMR, Tetra)

Communication bidirectionnelle indépendante réseau GSM/Internet. Chiffrement obligatoire (pas analogique). Fonctionnement zones souterraines. Modèles : Motorola DP4400e, Hytera PD685, Icom IC-4100H. Portée 10-50 km selon terrain. Voix uniquement.

Combinaison idéale : Radio chiffrée coordination terrain + Signal/Proton documents secondaires + Smartphone éteint + Pochette Faraday repos.

📌 HAUTE PRIORITÉ

Signal + Proton Mail

Messagerie + appels + vidéo chiffrés bout-en-bout. Email sécurisé Proton. Désactiver sauvegardes cloud Google. Vérifier codes sécurité contacts critiques. Ne pas utiliser WhatsApp

VPN Sécurisé

Masquage IP + chiffrage trafic. Recommandés : ProtonVPN. Configuration : connexion auto démarrage, kill switch activé, serveur lointain, DNS chiffré.

Clés USB/Disques Cryptés

Stockage portable chiffré. Accès mot de passe long. Jamais brancher clé inconnue sur le PC.

Authentification 2FA/FIDO2

Clés ou Carte NFC FIDO2 physiques. Codes secours stockés scellés coffre. Aucun piratage possible authentification matérielle.

Sauvegardes Hors Ligne

Sauvegarde hebdomadaire disque externe. Disque **déconnecté réseau** après sauvegarde. Rotation 3 disques (prévention corruption). Vérification intégrité tous 3 mois.

📋 PRIORITÉ MOYENNE

Téléphone Basique Sans Internet

Backup communication urgence. Appels + SMS uniquement. Batterie 7-10 jours. SIM prépayée distincte. Zéro données professionnelles. Usage : urgence seulement. Si non utilisé, mettre dans pochette Faraday

Mode Avion Systématique

Désactivation réseau nuit, entre opérations, repos minière. Batterie +40% autonomie. Zéro tentative connexion suspecte. Vérifier désactivation WiFi/Bluetooth même Mode Avion.

Tails OS (Situations Exceptionnelles)

OS portable amnésique (oublie tout après extinction). Pas de trace disque dur. Tor intégré automatique. Idéal accès depuis PC public.

🚨 GESTION INCIDENTS — Procédures Urgence

Téléphone Perdu/Volé/Compromis

1. Alerter équipe sécurité immédiatement (< 5 min)
2. Déclencher effacement à distance (réinitialisation usine)
3. Révoquer sessions Signal/Proton web depuis autre appareil
4. Rotation mots de passe critiques (12h après incident)
5. Vérifier accès frauduleux historiques connexions

Email/Appel/Message Suspect

1. **NE PAS ouvrir pièce jointe** (risque malware immédiat)
2. **NE PAS cliquer lien** (phishing courant)

3. Vérifier canal alternatif : appeler personne supposée numéro connu, "tu viens me contacter?"
4. Transférer analyste sécurité : screenshot + contexte (de qui, quand, sujet), évaluation menace

Exemple alerte : Message Signal "Connecte-toi Proton urgence" avec lien proton-sécurite.net (pas proton.me) = **FAUX** appeler autre canal confirmer.