# Formation Cybersécurité pour Journalistes

Formation de 4 jours - 2h par jour

75% pratique - 25% théorie

# Pourquoi cette formation ?

### Vous êtes une cible prioritaire

Sources sensibles, accès privilégiés, information confidentielle

### Menaces en constante évolution

Outils d'espionnage sophistiqués ciblant spécifiquement les médias

### Protection pratique accessible

Solutions simples pour renforcer significativement votre sécurité

# Programme de la formation

**Jour 1**

Bases de sécurité numérique

**Jour 2**

Communications sécurisées

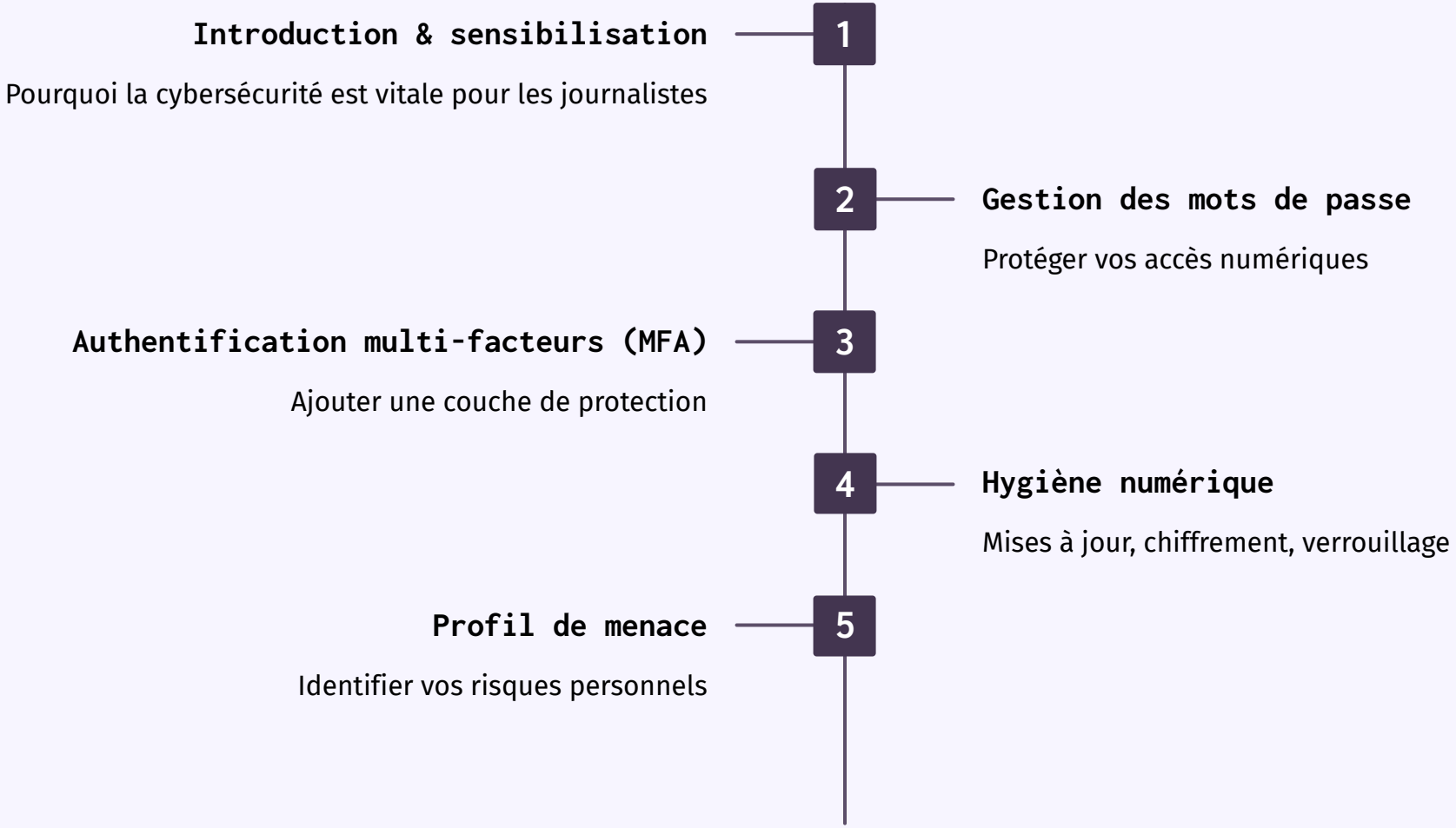
**Jour 3**

Protection des sources

**Jour 4**

Sécurité sur le terrain

# Jour 1 : Les bases essentielles



# Les journalistes : cibles privilégiées

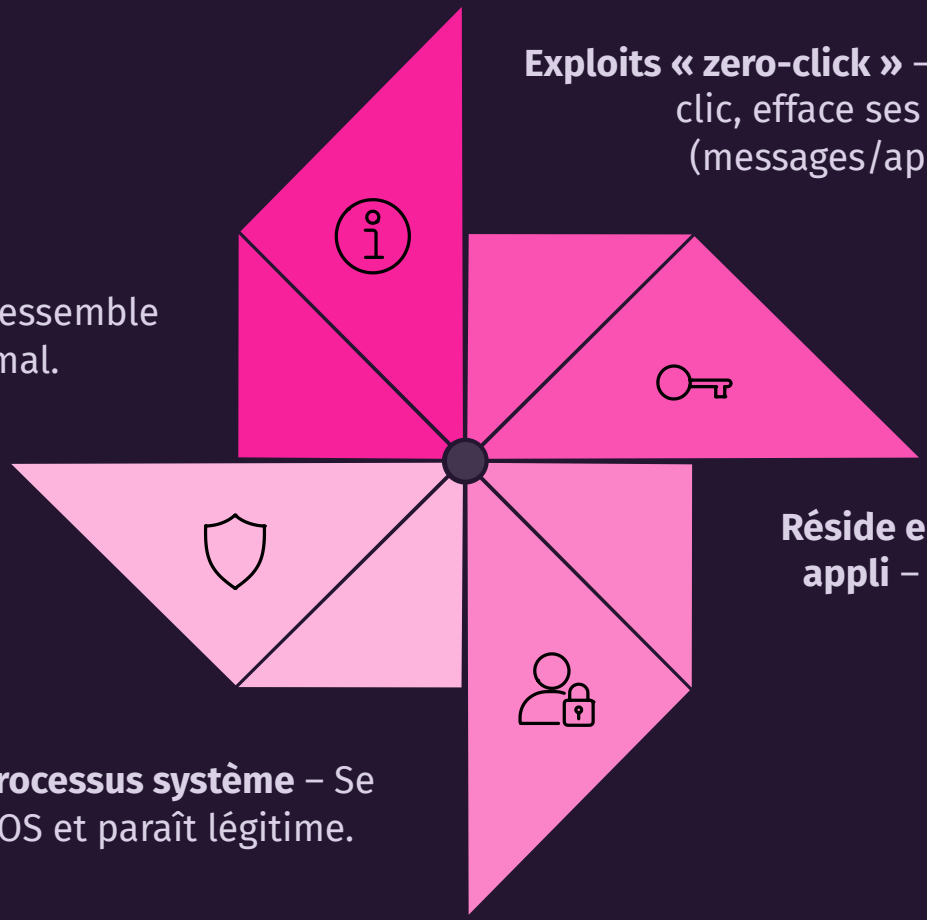
⚠ Cas réel : Logiciel espion Pegasus utilisé contre des journalistes marocains en 2021 (eg. Edwy Plenel, Mediapart founder)

Réfléchissez : "Si mon téléphone est compromis demain, quelles informations sensibles sont exposées ?"

# Pourquoi Pegasus échappe à la détection

**Exploits « zero-click »** – S'installe sans clic, efface ses traces (messages/appels).

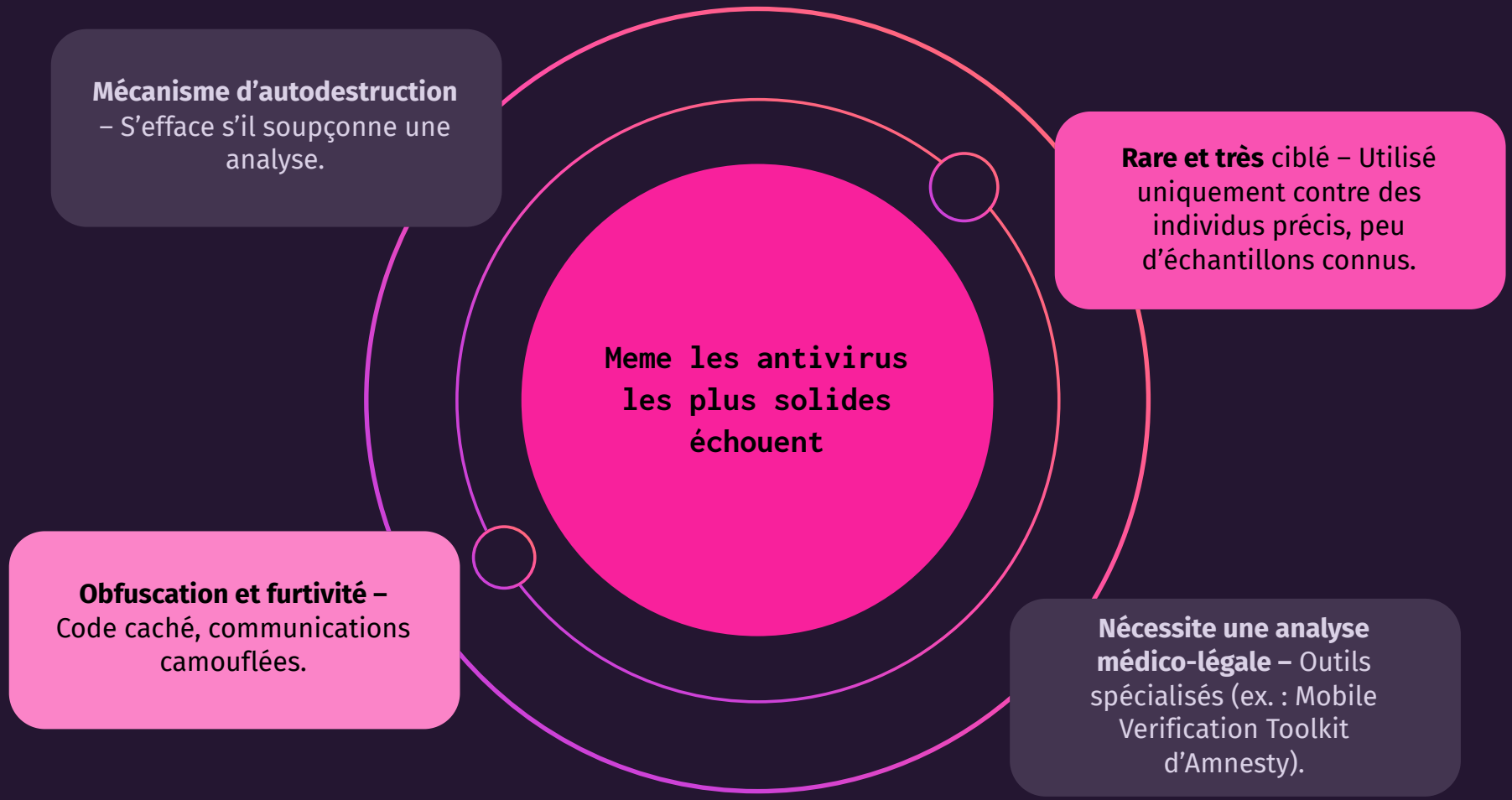
**Trafic chiffré et masqué** – Ressemble au trafic internet normal.



**Réside en mémoire, pas comme une appli** – Pas de fichiers ni d'icônes visibles.

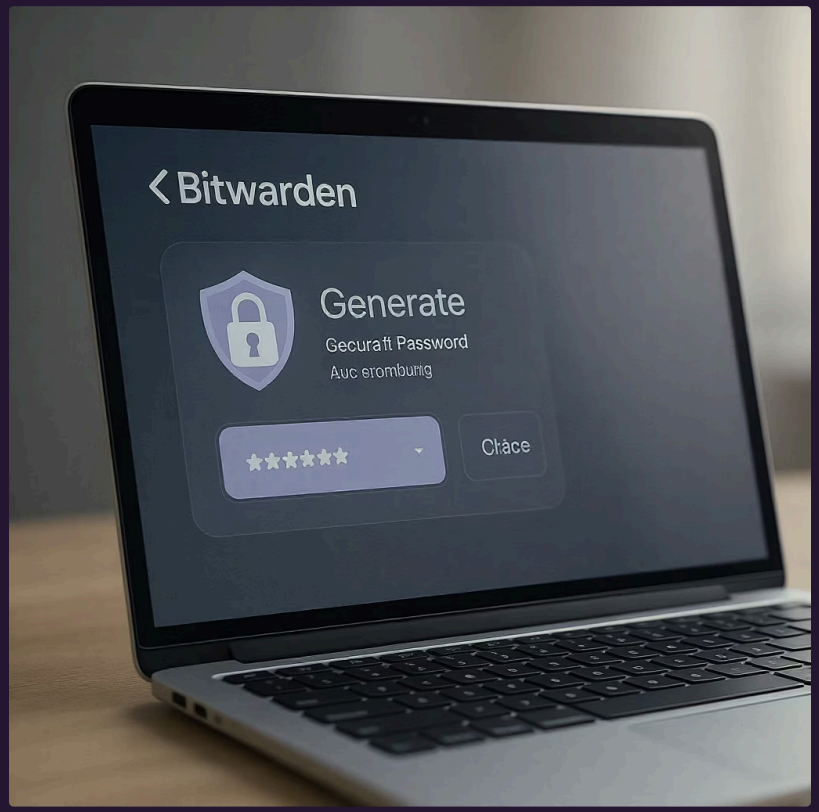
**Déguisé en processus système** – Se fond dans l'OS et paraît légitime.

# Pourquoi les antivirus ne détectent pas Pegasus



# Les mots de passe : première ligne de défense

1. Utilisez des phrases complexes (15+ caractères)
2. Jamais de réutilisation entre comptes
3. Adoptez un gestionnaire de mots de passe



# Exercice pratique : Bitwarden

### Installation

Téléchargez et configurez Bitwarden sur votre appareil

### Génération

Créez 3 mots de passe forts et uniques

### Importation

Ajoutez au moins 2 comptes existants

Le piratage du New York Times a commencé par un simple mot de passe faible

# L'authentification à deux facteurs (2FA)

**Seconde Barrière**

Ajoute une deuxième barrière après mot de passe

**Risk Reduction**

Reduit le rique d'exposition de données à 80%

**Comptes critiques**

Protège email, social, et cloud

**Two-Factor**

Use 2FA or multi-factor methods

**Authenticator Apps**

Plus solides et securisées que les codes par SMS

# Exercice pratique : Activer la 2FA

1

### Installer Authy

Application de codes d'authentification sur votre smartphone

2

### Sécuriser Gmail

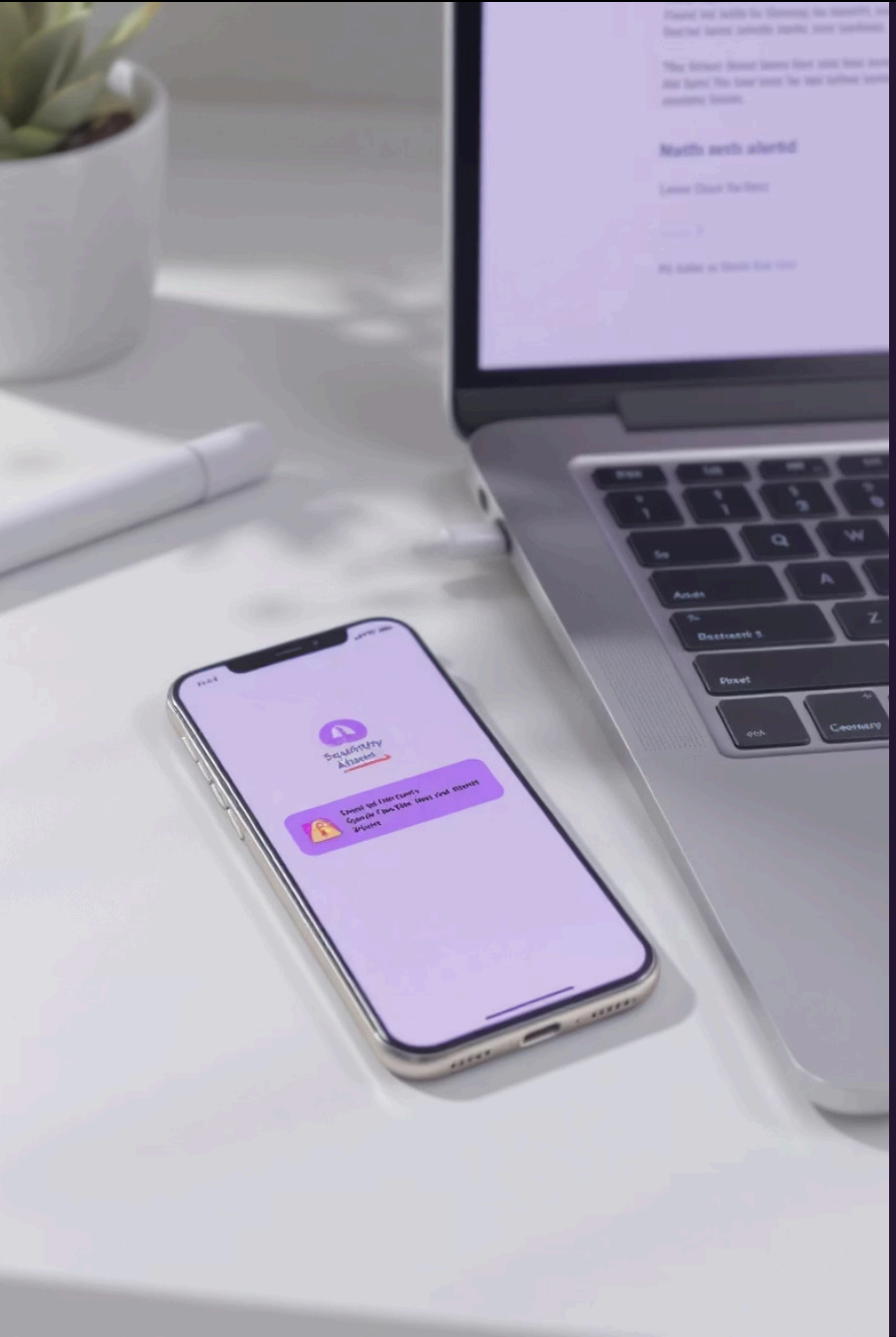
Activer la 2FA dans les paramètres de sécurité

3

### Protéger Twitter/X

Configurer l'authentification dans Paramètres → Sécurité

Un journaliste kényan a perdu l'accès à son WhatsApp faute de 2FA



# Hygiène numérique de base

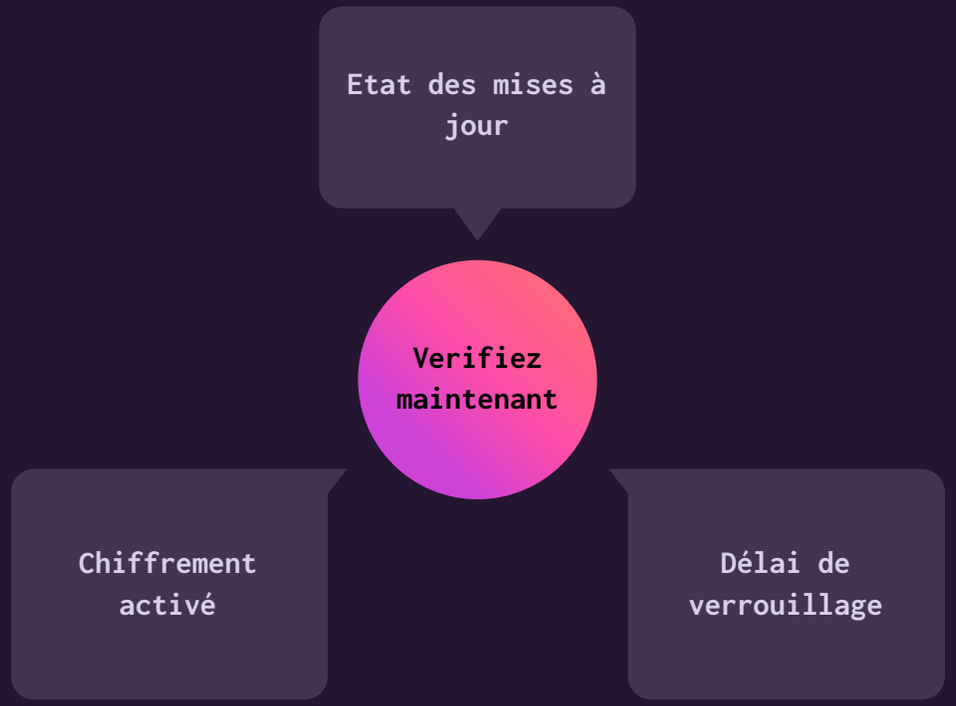
Mises à jour : installez-les immédiatement (corrigent vulnérabilités)

Chiffrement : activez-le sur tous vos appareils et disques

Verrouillage : configurez verrouillage automatique (1-5 minutes)

# Cas réel : Saisie d'équipement

> "L'iPhone d'un reporter a été saisi à l'aéroport. Sans verrouillage ni chiffrement, toutes ses sources ont été compromises."




# Comprendre votre profil de menace

### Qui pourrait vous cibler ?

- Gouvernements
- Entreprises
- Criminels
- Hacktivistes

### Quelles sont vos vulnérabilités ?

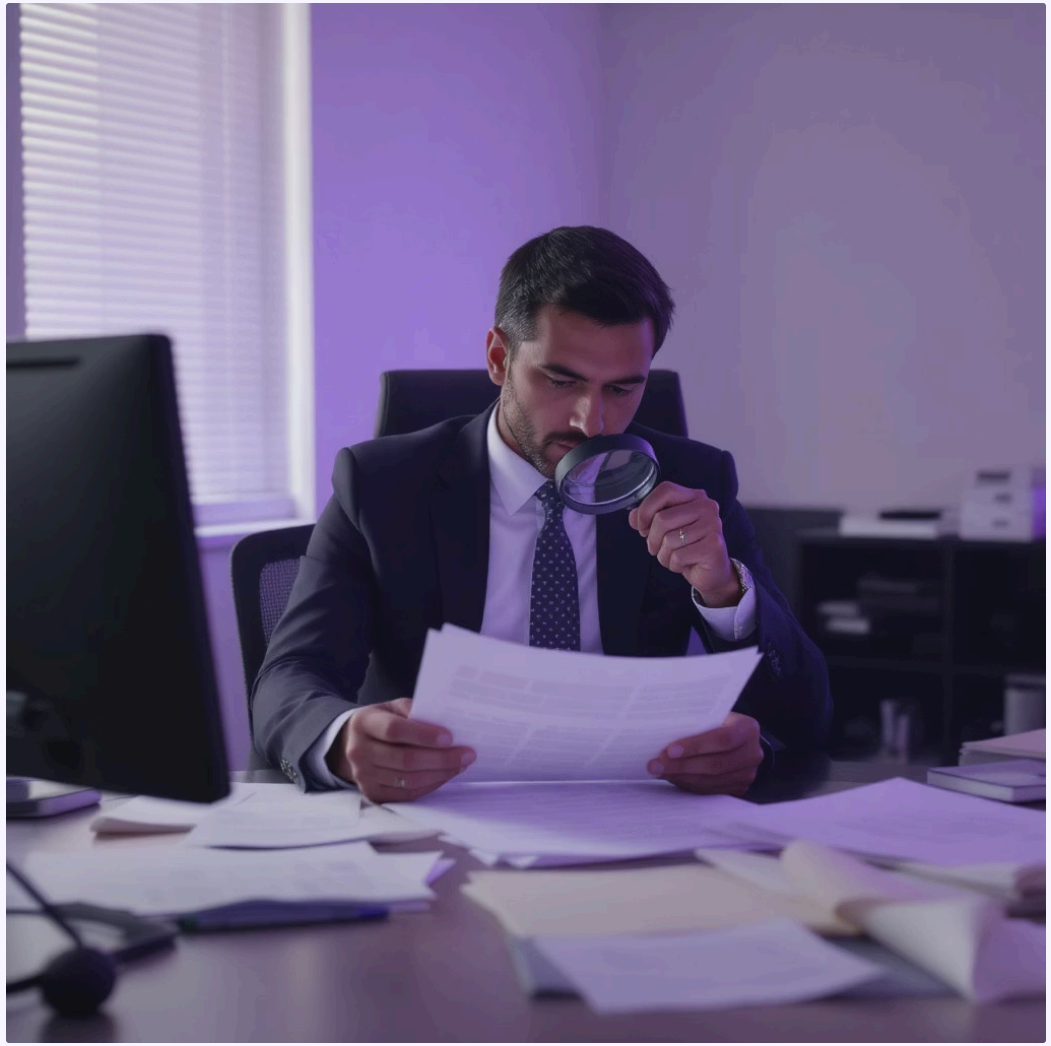
- Appareils
- Communications
- Comportements
- Données stockées

### Que cherchent-ils ?

- Sources
- Documents sensibles
- Communications privées
- Informations personnelles

# Le risque dépend de votre travail

### Journaliste d'investigation



Risque élevé : corruption, crime organisé, sujets politiques sensibles

### Journaliste sportif

Risque modéré : fraude sportive, paris illégaux, transferts confidentiels


# Exercice : Cartographie de menaces

Complétez le tableau :

- Qui pourrait vouloir m'attaquer ?
- Quelles méthodes utiliseraient-ils ?
- Quelles sont mes informations les plus sensibles ?
- Quelles seraient les conséquences d'une compromission ?

# Plan d'action personnel

### Identifiez vos 3 priorités

Concentrez-vous sur les risques les plus immédiats

### Fixez un calendrier

Planifiez des actions concrètes sur 30 jours

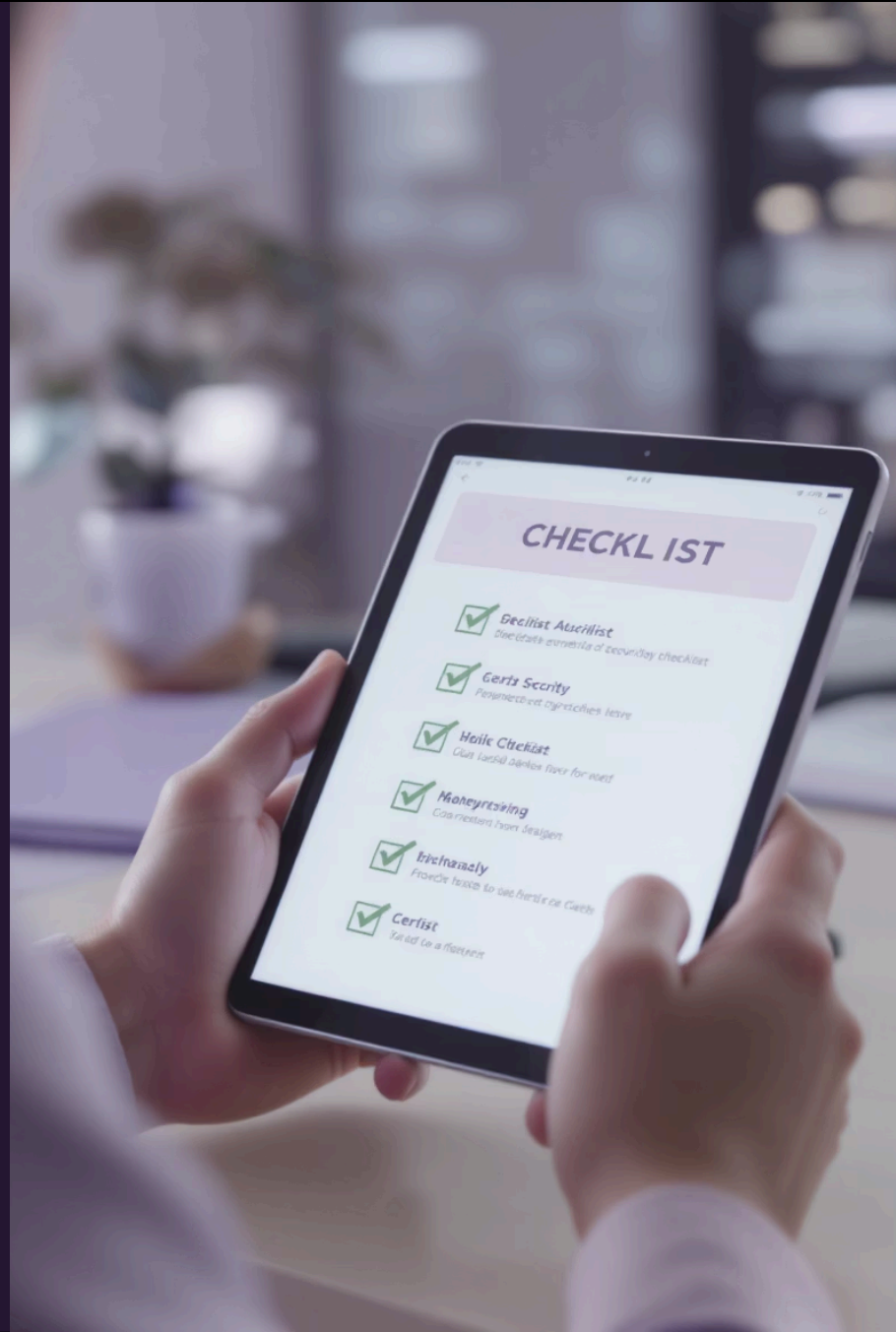
### Mettez en œuvre

Commencez par les solutions simples et efficaces

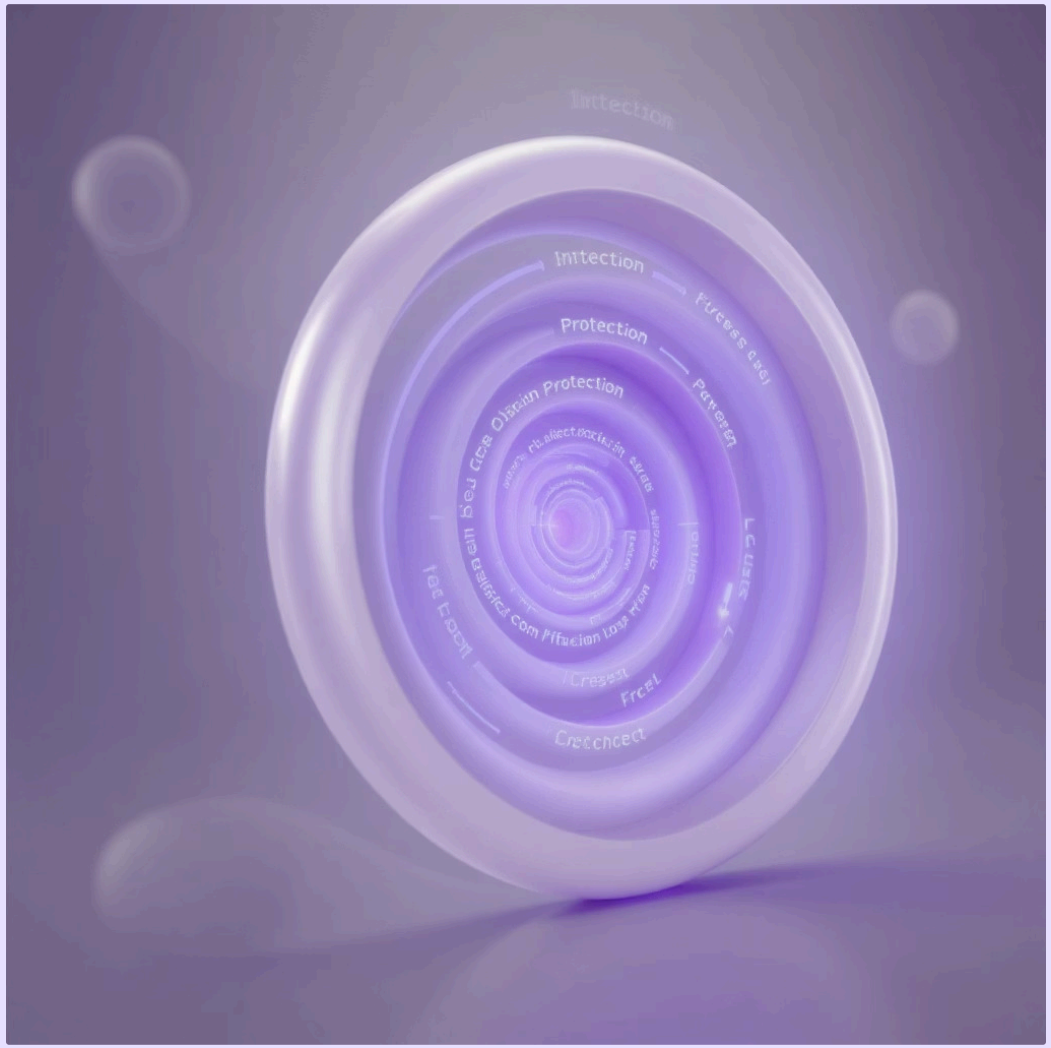
# Résultats attendus - Jour 1

À la fin de cette session, chaque participant aura :

- [ ] Un gestionnaire de mots de passe installé et configuré
- [ ] L'authentification à 2 facteurs activée sur comptes critiques
- [ ] Vérifié les mises à jour et le chiffrement de ses appareils



# La sécurité, c'est comme un oignon




## Chaque couche ajoute une protection supplémentaire

- Pas de solution magique unique
- La défense en profondeur est essentielle
- Chaque barrière réduit significativement les risques

# Ce qui vous attend pour la suite...

**Jour 2**

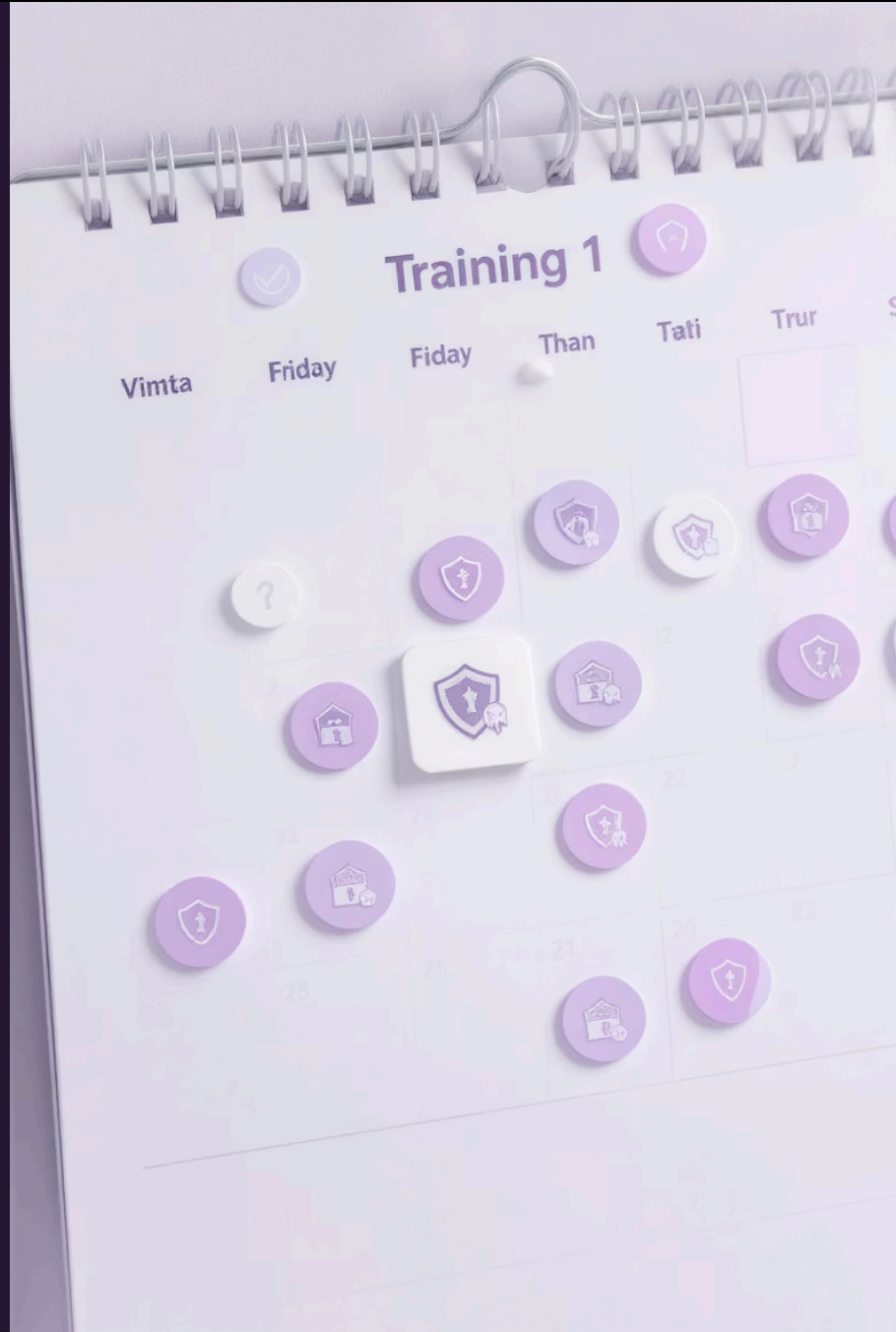
Communications sécurisées : Signal, ProtonMail, VPN

**Jour 3**

Protection des sources : Tor, SecureDrop, techniques d'anonymat

**Jour 4**

Sécurité sur le terrain : dispositifs de secours, cloud sécurisé



# Ressources à consulter

**Guide de sécurité numérique pour journalistes (RSF)**

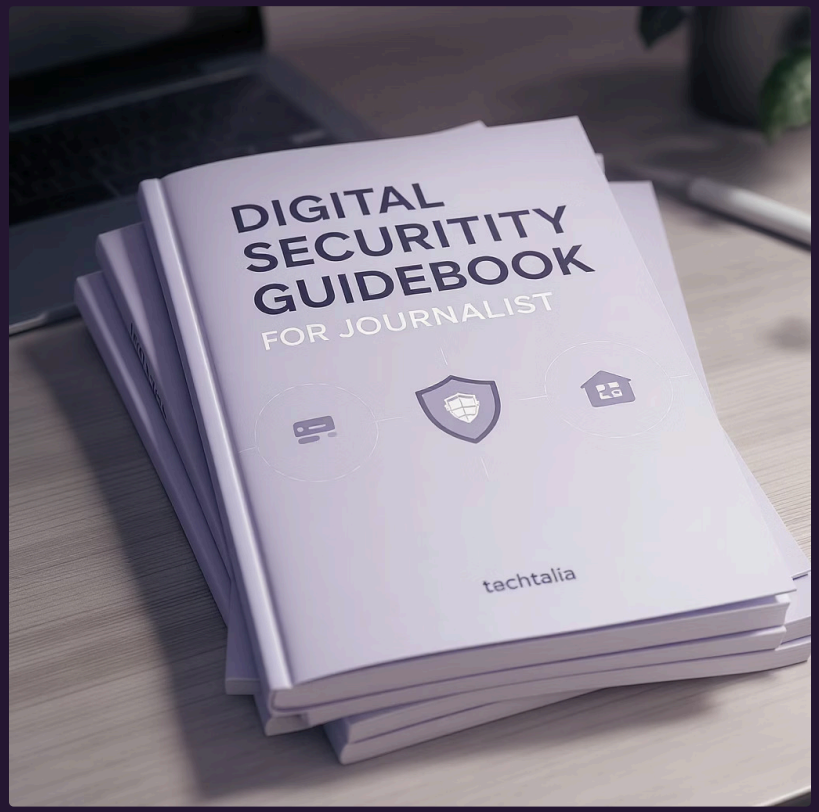
rsf.org/securite-numerique

**Security in a Box (Tactical Tech)**

securityinabox.org/fr

**Centre de ressources CPJ**

cpj.org/fr/technology



# Des questions ?

Formation présentée par **Othniel Pilipili**

Merci de votre attention