Sécurité Numérique pour Journalistes

Communication avec les Sources & Protection des Données

Formation Pratique - Jour 2

Programme du Jour

1. **Communication chiffrée avec Signal**
   Messagerie sécurisée pour sources sensibles
2. **Emails sécurisés**
   ProtonMail et correspondance protégée
3. **Navigation anonyme**
   Utilisation de Tor pour l'anonymat
4. **Phishing & Social Engineering**
   Identifier les menaces
5. **Cas pratique en groupe**
   Plan de communication sécurisée

Objectifs de la journée

Choisir le bon canal

Adapter l'outil au niveau de risque

Maîtriser les outils

Signal, ProtonMail, Tor Browser

Identifier les menaces

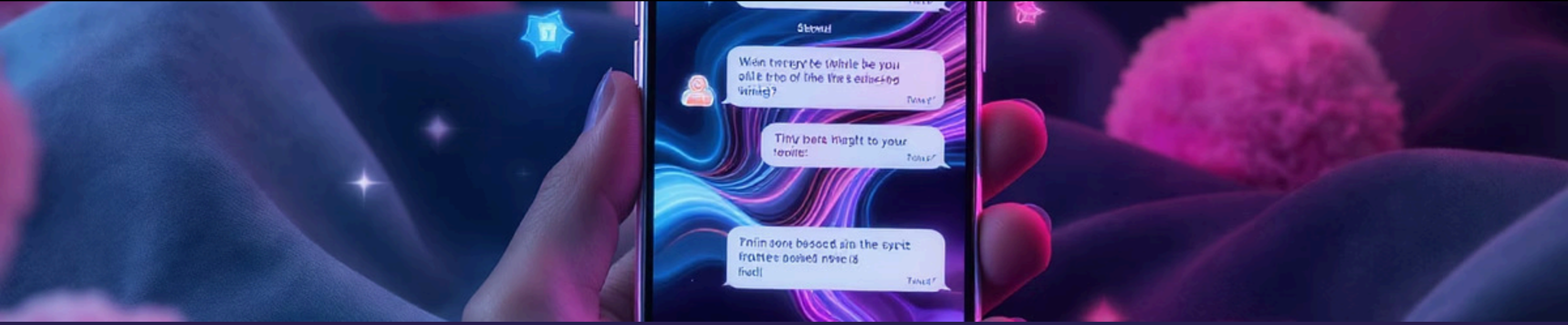
Reconnaître tentatives de phishing

Créer un protocole

Applicable en rédaction

Retour sur le Jour 1

- Qu'avez-vous mis en pratique ?
- Quelles questions sont apparues ?
- Quelles difficultés avez-vous rencontrées?



Signal

La messagerie chiffrée de référence

Pourquoi Signal ?

Chiffrement de bout en bout

Messages illisibles, même par Signal

Open source

Code vérifiable par experts indépendants

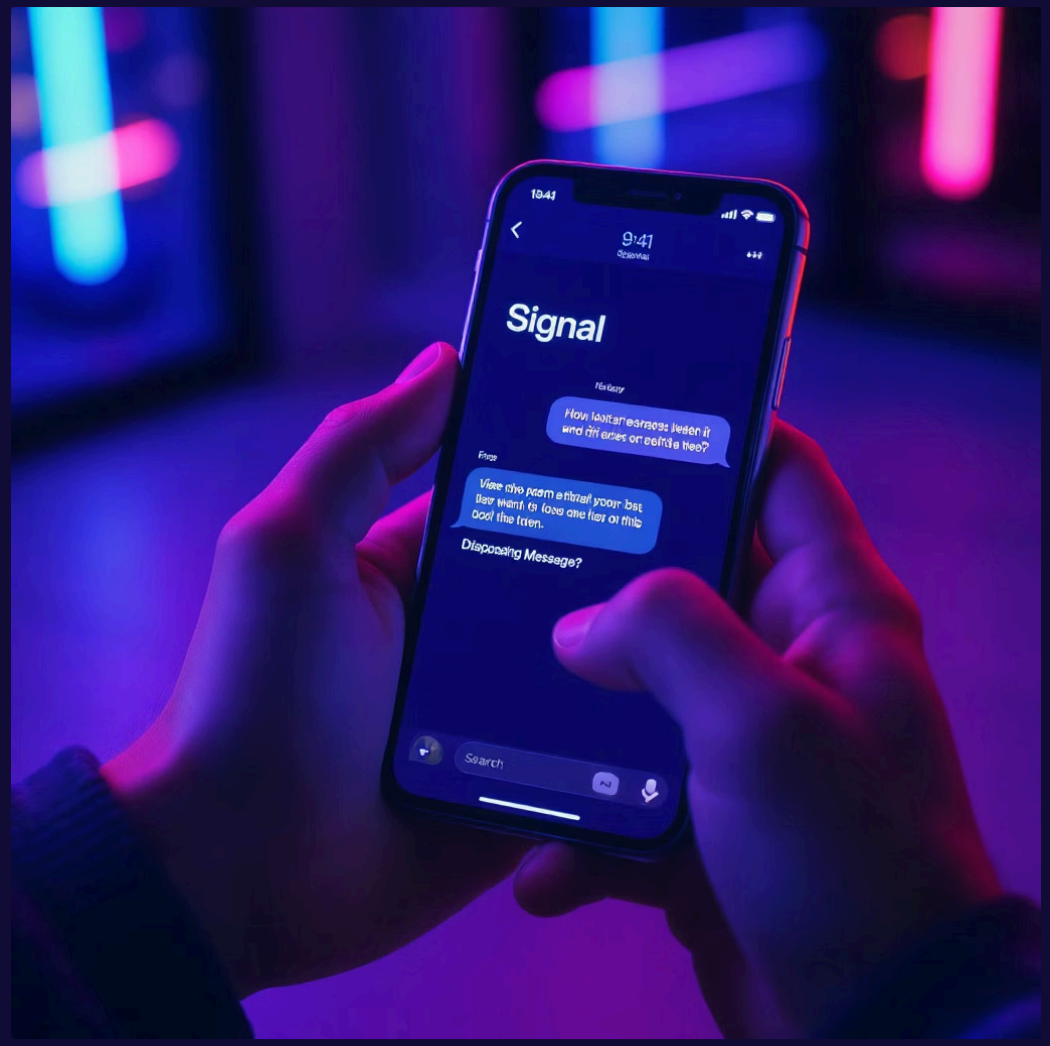
Messages éphémères

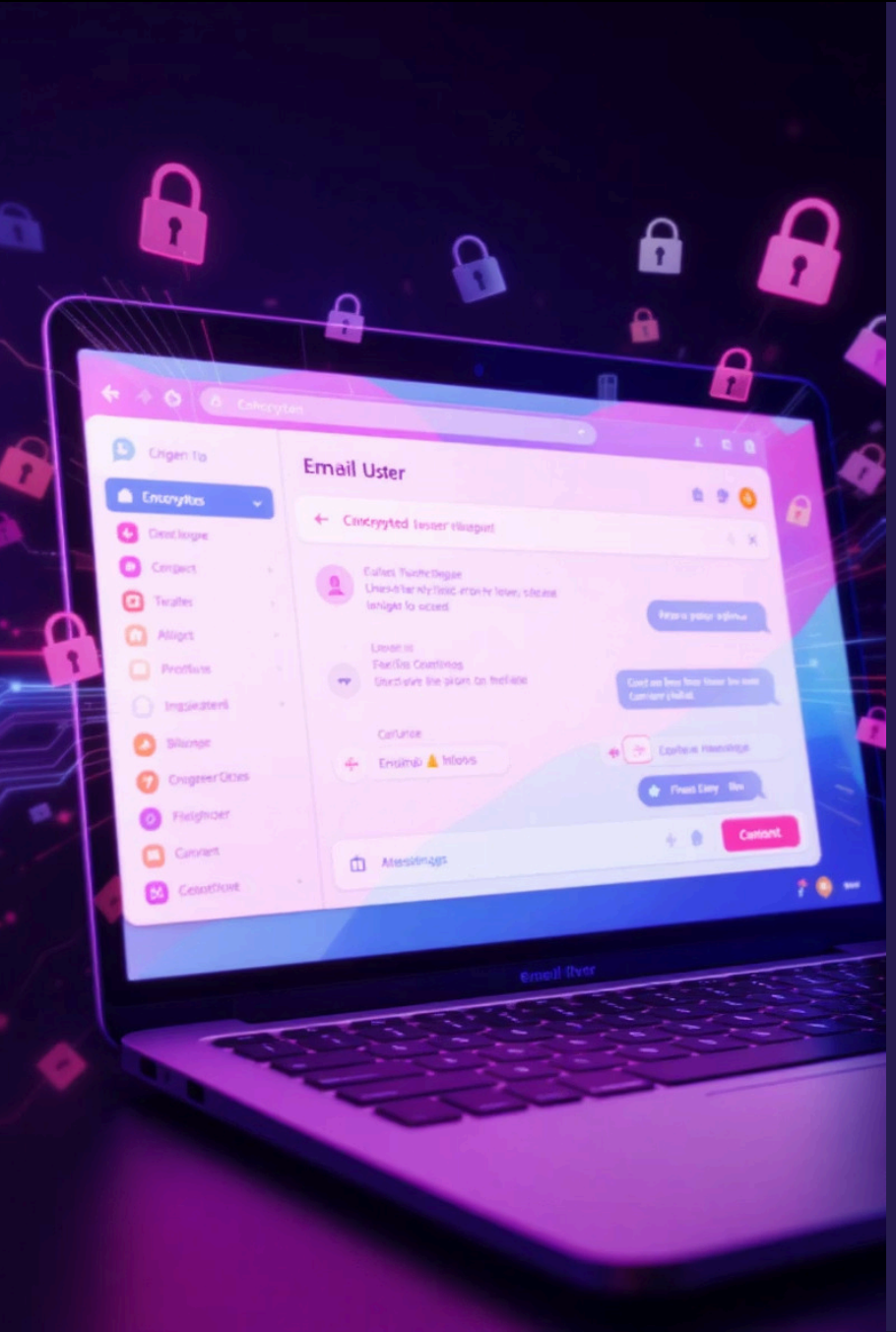
Disparition programmée des messages

Cas concret : Reporters mexicains communiquant avec sources au sein des cartels

Exercice Signal

- Installer Signal
- Créer un compte
- Envoyer un message
- Appel test chiffré





Emails Sécurisés

ProtonMail & Tutanota

Email chiffré : principes clés

Contenu chiffré

Message illisible en transit

Authentification

Vérification d'identité

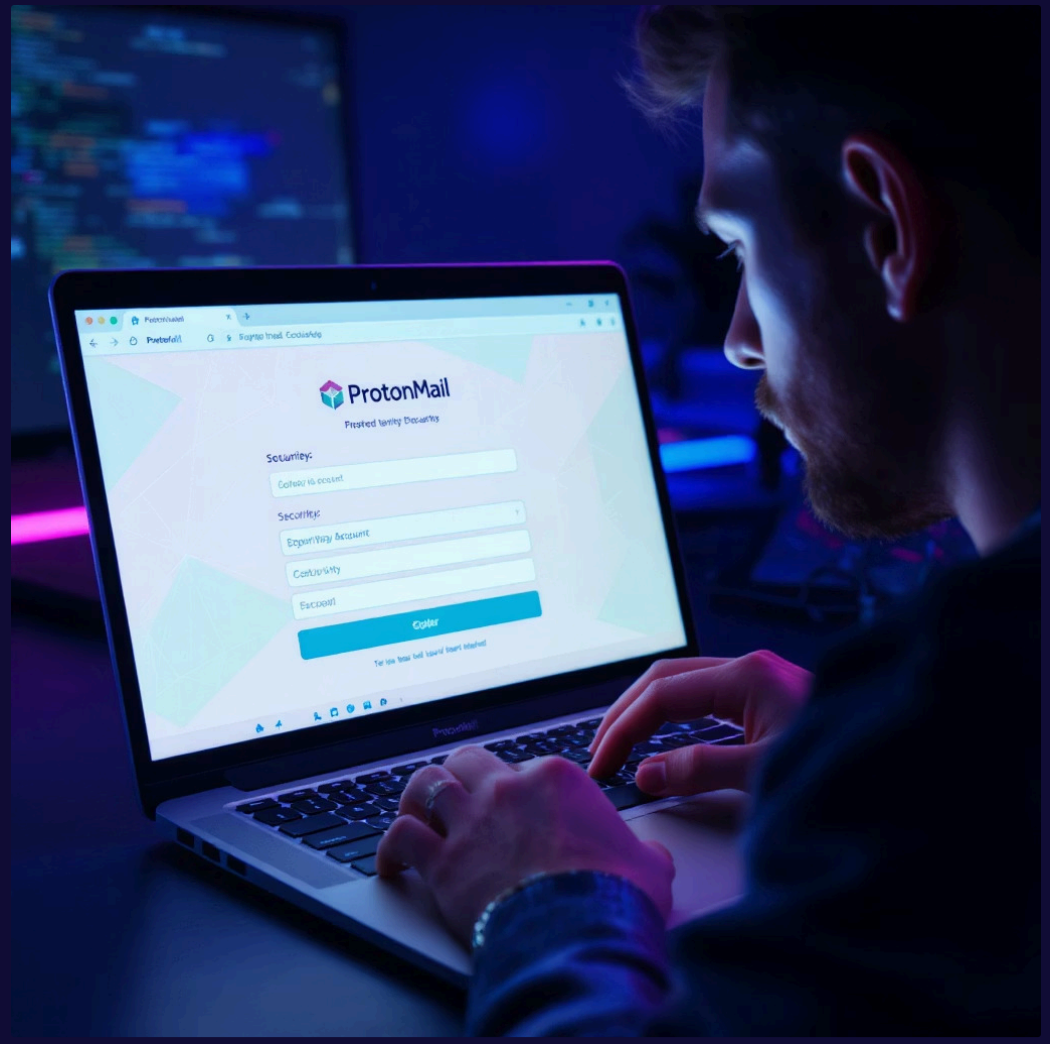
Zéro connaissance

Fournisseur ne peut lire

Cas historique : Edward Snowden communiquant avec les journalistes du Guardian

Exercice ProtonMail

1. Créer un compte ProtonMail
2. Configurer la récupération
3. Envoyer un email chiffré à un partenaire
4. Utiliser un mot de passe partagé
5. Envoyer un PDF verouillé



Navigation Anonyme

Tor Browser + Duckduckgo

Comment fonctionne Tor

Votre ordinateur

Point de départ

Nœud d'entrée

Premier relais

Nœud de sortie

Connexion au site

Nœud intermédiaire

Relais central

Cas réel : Journalistes birmans accédant aux médias bloqués par la junte

Exercice Tor Browser

- Installer Tor Browser
- Vérifier son adresse IP
- Visiter un site .onion
- Comparer avec navigation normale

Phishing & Social Engineering

Reconnaître les menaces

Signes de phishing

Urgence suspecte

"Réagissez immédiatement" ou "Compte bloqué"

Fautes d'orthographe

Erreurs dans le texte ou l'adresse email

URL trompeuses

Domaines similaires mais différents

Pièces jointes suspectes

Fichiers .exe, .zip ou .doc non attendus

Cas réel : Faux emails PayPal ciblant des journalistes AFP

Exercice Détection de Phishing

Analyse
Analyze 5 example emails

Spot Clues
Identifier les indicateurs de phishing

Note Techniques
Notez les methods utilisées par les attaqueurs

Check Liens
Inspectez les URLs and redirects

Verifer l'expediteur
Confirmez l'authenticité de l'expediteur

Verifiez l'urgence
Cherchez les tactiques de pression

Notez les resultats
Synthetisez les observations clé

Cas Pratique

Communication avec un lanceur d'alerte

Scénario

⚠ Un employé d'une grande entreprise pharmaceutique souhaite vous révéler des documents sur des essais cliniques falsifiés.

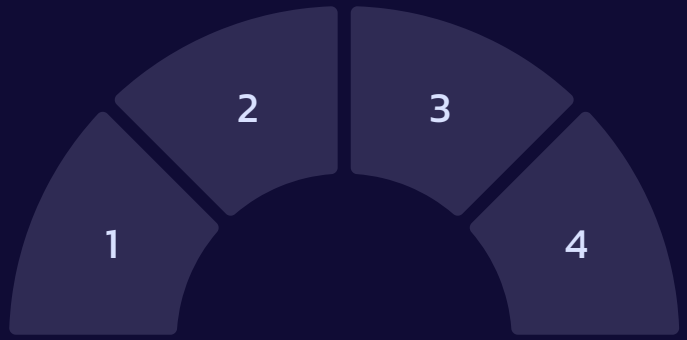
Vous devez établir une communication sécurisée pour :

- Échanger des messages
- Recevoir des documents
- Planifier une rencontre
- Protéger son identité

Risque : surveillance possible par entreprise disposant de moyens importants

Travail en groupe

À définir en 10 minutes :



1. Canaux de communication à utiliser
2. Protocole de vérification d'identité
3. Méthode d'échange de documents
4. Précautions pour rencontre physique

Conclusion

Évaluez les risques

Adaptez vos outils au niveau de menace

Pratiquez régulièrement

La sécurité s'entretient

Formez votre équipe

La chaîne n'est forte que par son maillon le plus faible

Votre outil préféré aujourd'hui ?

Merci !

Présenté par Othniel Pilipili