FICHE RÉFLEXE CYBERSÉCURITÉ

RANSOMWARE

INCIDENT CRITIQUE

Mes fichiers sont chiffrés — Que faire ?

LES 10 ÉTAPES À SUIVRE IMMÉDIATEMENT, DANS L'ORDRE

1 Ne pas éteindre le poste
Les preuves en mémoire vive sont précieuses pour l'investigation.

2 Déconnecter du réseau
Débrancher le câble Ethernet et désactiver le Wi-Fi immédiatement.

3 Ne pas payer la rançon
Aucune garantie de récupération, finance les criminels, illégal dans certains cas.

4 Photographier le message
Avec votre smartphone : le message de rançon, l'écran de blocage, les erreurs.

5 Noter l'heure et la date
Heure exacte de découverte, postes/serveurs touchés, nature des fichiers chiffrés.

6 Prévenir le DSI / RSSI
Ou votre prestataire informatique. Ne pas attendre, alerter par téléphone.

7 Déposer plainte
Gendarmerie ou Police nationale. Conserver le récépissé de plainte (assurance).

8 Contacter cybermalveillance.gouv.fr
Assistance gratuite, mise en relation avec un expert agréé.

9 Préserver les preuves
Ne pas supprimer les fichiers chiffrés, ne pas réinstaller avant expertise.

10 Communiquer en interne
Informer les équipes via un canal de secours (téléphone), éviter l'affolement.

⚠ NE JAMAIS FAIRE

- ✕ **Payer la rançon — aucune garantie, vous financez les attaquants**
- ✕ **Supprimer les fichiers chiffrés — destruction de preuves, récupération impossible**
- ✕ **Négocier seul avec les attaquants — risque d'aggravation, contacter des experts d'abord**

ASSISTANCE CYBERMALVEILLANCE	ANSSI — URGENCES CYBER	GENDARMERIE / POLICE
cybermalveillance.gouv.fr	**cert.ssi.gouv.fr**	**17 ou 3114 (numérique)**
Dépôt de signalement en ligne	Grandes organisations / OIV	Dépôt de plainte obligatoire

Besoin d'un accompagnement post-incident ou d'un plan de reprise d'activité ?
ayinedjimi-consultants.fr/contact