AI-JE ÉTÉ PIRATÉ ? — ARBRE DE DÉCISION

Répondez aux questions suivantes pour identifier votre situation et les actions à mener

FICHE RÉFLEXE
1 PAGE A4

Comment utiliser cet arbre ? Répondez à chaque question par OUI ou NON. Suivez les flèches correspondantes pour identifier votre situation et les premières mesures à prendre. En cas de doute, passez à la question suivante. Ce guide ne remplace pas une analyse technique par un professionnel.

Q1

✉

Mon compte envoie des messages à mon insu ?

Vos contacts vous signalent avoir reçu des messages bizarres de votre part. Votre messagerie montre des envois que vous n'avez pas faits. Votre compte publie du contenu que vous n'avez pas créé.

↗ OUI — COMPTE COMPROMIS

ACTION IMMÉDIATE

- → Changez le mot de passe depuis un autre appareil
- → Activez le MFA / 2FA immédiatement
- → Déconnectez toutes les sessions actives
- → Vérifiez les règles de redirection email
- → Prévenez vos contacts que le compte a été piraté
- → Signalez l'incident au service concerné

↘ NON — CONTINUEZ

Pas de signal d'alerte sur ce point

- → Vérifiez tout de même vos envois récents
- → Continuez avec la question Q2

Q2

💻

Mon ordinateur est anormalement lent / j'ai des pop-ups intempestifs ?

Votre PC démarre lentement, rame sans raison. Des fenêtres publicitaires s'ouvrent sans que vous ne cliquiez. Votre navigateur redirige vers des sites inconnus. Votre antivirus est désactivé sans votre action.

↗ OUI — MALWARE PROBABLE

ACTIONS ANTI-MALWARE

- → Déconnectez le PC d'Internet (câble ou Wi-Fi)
- → Lancez un scan complet avec Malwarebytes (gratuit)
- → En cas de ransomware : ne pas payer, appeler le RSSI
- → Vérifiez les programmes démarrés automatiquement
- → Consultez un professionnel si le problème persiste
- → Signalement : cybermalveillance.gouv.fr

↘ NON — CONTINUEZ

Système a priori sain

- → Maintenez votre antivirus à jour
- → Continuez avec la question Q3

Q3

💰

J'ai reçu une demande de rançon / mes fichiers sont chiffrés ?

Un message s'affiche indiquant que vos fichiers ont été chiffrés et qu'il faut payer pour les récupérer. Vos documents ont une extension inconnue (.locked, .encrypted, .WNCRY...). Des fichiers README.txt apparaissent dans vos dossiers.

↗ OUI — RANSOMWARE

PROCÉDURE D'URGENCE RANSOMWARE

- → ISOLEZ immédiatement : coupez tout réseau (Wi-Fi, câble)
- → NE PAYEZ PAS la rançon (ne garantit pas la restauration)
- → Alertez votre RSSI / IT et votre direction
- → Déclenchez votre plan de réponse à incident
- → Vérifiez les sauvegardes hors ligne (non chiffrées ?)
- → Identifiez le ransomware sur : id-ransomware.malwarehunterteam.com
- → Cherchez un déchiffreur gratuit : nomoreransom.org
- → Déposez plainte : cyberplainte.fr ou gendarmerie
- → Notifiez la CNIL si données personnelles concernées (72h)

↘ NON — CONTINUEZ

Pas de rançongiciel détecté

- → Assurez-vous que vos sauvegardes sont à jour
- → Continuez avec la question Q4

Q4

🪪

Mon identité est utilisée sans mon consentement ?

Vous recevez des confirmations de commandes que vous n'avez pas passées. Des crédits ont été souscrits à votre nom. Des comptes ont été ouverts sans votre accord. Des profils faux vous usurpent sur les réseaux sociaux.

↗ OUI — USURPATION D'IDENTITÉ

PROCÉDURE USURPATION D'IDENTITÉ

- → Déposez plainte sans délai : commissariat / gendarmerie ou cyberplainte.fr
- → Alertez les organismes concernés (banque, opérateur, CAF...)
- → Contactez la CNIL pour exercer vos droits RGPD
- → Signalez les faux profils sur les plateformes concernées
- → Consultez le dossier de crédit sur FICOBA (banque de France)
- → Informez France Identité Numérique si applicable
- → Conservez toutes les preuves (captures, emails, courriers)

↘ NON — BONNE NOUVELLE

Pas d'usurpation détectée

- → Vérifiez quand même sur haveibeenpwned.com
- → Activez des alertes Google sur votre nom
- → Continuez avec les bonnes pratiques ci-dessous

CYBERMALVEILLANCE
cybermalveillance.gouv.fr
Assistance + trouver un prestataire

POLICE / GENDARMERIE
17 — cyberplainte.fr
Dépôt de plainte 24h/24

ANSSI / CERT-FR
cert.ssi.gouv.fr
Incidents graves, organisations

CNIL
cnil.fr — notifications.cnil.fr
Violation données (72h)

NO MORE RANSOM
nomoreransom.org
Déchiffreurs ransomware gratuits

INFO ESCROQUERIES
0 805 805 817
Signalement escroqueries (gratuit)

RÉFLEXE GÉNÉRAL SI VOUS PENSEZ AVOIR ÉTÉ PIRATÉ — DANS TOUS LES CAS

1 — ISOLER
Coupez la connexion réseau du système concerné (Wi-Fi ou câble). Ne pas éteindre la machine (préservation des preuves).

2 — ALERTER
Prévenez votre RSSI, votre responsable ou votre prestataire informatique. Documentez les symptômes avec des captures d'écran.

3 — SÉCURISER
Changez vos mots de passe depuis un appareil sain. Activez le MFA sur tous vos comptes importants. Vérifiez vos sessions actives.

4 — SIGNALER
Déposez plainte sur cyberplainte.fr. Notifiez la CNIL si données personnelles concernées (72h). Contactez votre assurance cyber.

5 — NE PAS PAYER
En cas de ransomware, ne payez jamais la rançon. Consultez nomoreransom.org pour un déchiffreur gratuit. Restaurez depuis vos sauvegardes.

Vous pensez avoir été victime d'une cyberattaque ? Faites-vous accompagner par un expert.
ayinedjimi-consultants.fr/contact