



RÉFLEXES EN CAS D'ATTAQUE D'ORIGINE CYBER

ÉTAPE 1

Arrêter l'hémorragie

 Coupez physiquement l'accès Internet :
Débranchez les câbles réseau et le Wi-Fi.

 **N'ÉTEIGNEZ PAS les ordinateurs et les serveurs afin de conserver les preuves numériques.**

ÉTAPE 2

Alerter : 17CYBER

Connectez-vous immédiatement pour le diagnostic et l'orientation.

 **www.17cyber.gouv.fr**

Accessible 24h/24 et 7j/7

RÉPONSE TECHNIQUE
(MESURE RÉFLEXE)

 Audio avec Campus Cyber

PROCÉDURE JUDICIAIRE
(DÉPÔT DE PLAINTE)

 Forces de l'ordre

ÉTAPE 3

Faites appel à des spécialistes

En cas de virement suspect :

- Appeler la banque.
- Exiger un **RAPPEL DE FONDS**.
- **Urgence absolue.**

Appelez votre prestataire informatique :

- Demandez la **remédiation**.
- **Attention : Ne rien effacer !**
- Il doit copier les preuves avant de réinstaller.
- Trouver l'origine de l'intrusion

ÉTAPE 4

Dépôt de Plainte

1. PRÉPARATION

17CYBER (Tchat)



2. VALIDATION

Commissariat / gendarmerie

*Le déplacement physique est obligatoire pour signer la plainte.
Gardez la copie pour l'assurance.*

ÉTAPE 5

Protégez-vous des obligations Légales & Clients



CNIL
(Données personnelles)

Déclaration sous **72h** sur cnil.fr.



Tiers
(Clients/Fournisseurs.)

Obligation d'informer s'il y a un vol d'informations personnelles.

En résumé

 **ATTAQUE DÉTECTÉE**



ISOLATION

On débranche tout, on n'éteint rien.

17CYBER.GOUV.FR

Point d'entrée unique & diagnostic



TECHNIQUE



ENQUÊTE



BANQUE

"Rappel de fonds"



PRESTATAIRE

Sauvegarde preuves



- ☒ Dépôt de plainte
- ☒ Déclaration CNIL (72h)
- ☒ Informer le prestataire et les clients



REPRISE D'ACTIVITÉ