

Cyberattaque : les premiers gestes qui sauvent

Les 24 premières heures décident de l'ampleur des dégâts. Le plan d'action minute par minute.

11 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/reponse-incident

Face à un incident de sécurité — poste chiffré, compte piraté, fuite de données — la panique fait commettre des erreurs irréversibles. Un plan simple, connu de tous et affiché quelque part, change tout.

1. Réflexes immédiats (première heure)

- Isoler : débrancher le câble réseau et couper le Wi-Fi des machines suspectes — sans les éteindre (les traces en mémoire aident l'analyse)
- Alerter : prévenir le référent informatique ou votre prestataire, même le soir ou le week-end
- Préserver : ne rien supprimer, ne pas se reconnecter « pour vérifier », photographier les écrans de rançon
- Recenser : quelles machines, quels comptes, quelles données semblent touchés ?

2. Dans les 24 à 72 heures

- Changer les mots de passe des comptes potentiellement compromis, depuis un poste sain
- Déposer plainte (commissariat, gendarmerie ou plainte en ligne) — indispensable pour l'assurance
- Notifier la CNIL sous 72 h en cas de violation de données personnelles
- Contacter votre assureur si vous avez une couverture cyber
- Communiquer sobrement auprès des clients ou partenaires concernés

3. Préparer avant l'incident

Le meilleur plan de réponse s'écrit à froid. Une page suffit : les contacts d'urgence (prestataire IT, assureur, banque), la localisation des sauvegardes, la liste des systèmes critiques et l'ordre de priorité pour les restaurer. Imprimez-la — si le réseau est chiffré, le PDF sur le serveur ne servira à rien.

4. Vers qui se tourner

- Votre prestataire informatique : le premier appel, pour contenir et analyser
- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) : diagnostic en ligne et mise en relation avec des intervenants qualifiés près de chez vous — gratuit
- Votre assureur cyber : la plupart des contrats incluent une hotline de crise (experts techniques, juristes) — appelez tôt, c'est souvent leur meilleure prestation
- La police ou la gendarmerie : dépôt de plainte, indispensable pour l'assurance ; les sections cyber savent traiter ces dossiers

- La CNIL : notification en ligne sous 72 h si des données personnelles sont violées
- Votre banque : en cas de fraude financière, chaque minute compte pour le rappel des fonds

ATTENTION

Les erreurs classiques qui aggravent tout : éteindre les machines (destruction des preuves en mémoire), restaurer les sauvegardes sur un réseau encore compromis (elles se font chiffrer à leur tour), tout réinstaller avant l'analyse (impossible de savoir comment l'attaquant est entré — il reviendra), et garder le silence en interne (l'attaque continue pendant ce temps).

5. Après la crise : transformer l'incident en progrès

- Analyse à froid, sans chasse aux coupables : chronologie, porte d'entrée, ce qui a fonctionné, ce qui a manqué
- Corriger la cause racine en priorité — pas seulement les symptômes
- Mettre à jour la fiche réflexe avec ce que l'incident a appris
- Informer l'équipe du déroulé : rien ne sensibilise mieux qu'un incident réel bien débriefé
- Réévaluer la couverture d'assurance et les contrats prestataires à la lumière de l'expérience

L'essentiel à retenir

- 01 Rédiger une fiche réflexe d'une page et l'imprimer
- 02 Afficher les contacts d'urgence IT accessibles hors ligne
- 03 Former l'équipe au réflexe « isoler sans éteindre »
- 04 Vérifier la couverture cyber de votre assurance
- 05 Connaître la procédure de notification CNIL (72 h)
- 06 Prévoir un canal de communication de secours si la messagerie tombe

Questions fréquentes

Pourquoi ne faut-il pas éteindre un ordinateur compromis ?

La mémoire vive contient des traces précieuses : processus malveillants en cours, connexions actives, parfois des clés de chiffrement du ransomware. Éteindre efface tout cela et complique l'analyse — voire la récupération. Isoler du réseau (câble débranché, Wi-Fi coupé) stoppe la propagation sans détruire les preuves.

Que dire aux clients si l'incident les concerne ?

La transparence maîtrisée : ce qui s'est passé, ce qui est fait, ce qu'ils doivent faire (changer un mot de passe, surveiller leurs comptes), sans minimiser ni dramatiser. Un message honnête préserve la confiance ; un silence découvert plus tard la détruit. Si des données personnelles à risque élevé sont touchées, l'information des personnes est de toute façon une obligation RGPD.

Comment travailler pendant que les systèmes sont bloqués ?

C'est le rôle du plan de continuité, préparé à froid : téléphones 4G pour l'essentiel, adresses email de secours, liste papier des contacts clients, procédures manuelles pour les opérations vitales. Même modeste, ce plan B change tout — improviser en pleine crise coûte des jours.

Un incident « mineur » (un seul poste, un compte) mérite-t-il tout ce protocole ?

Version allégée, mais oui : isoler, changer les mots de passe, vérifier qu'il n'y a pas de propagation, documenter. Beaucoup d'attaques majeures commencent par un « petit » incident négligé trois semaines plus tôt. Et la documentation systématique des incidents, même mineurs, est une obligation RGPD dès que des données personnelles sont en jeu.

Pour aller plus loin

Cybermalveillance.gouv.fr — assistance aux victimes — www.cybermalveillance.gouv.fr/diagnostic/accueil

ANSSI — les bons réflexes en cas d'incident — cyber.gouv.fr/en-cas-dincident

CNIL — notifier une violation de données — www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaulé pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr