

Les 5 réflexes face à une **cyberattaque**

Déposez plainte dans les 72 h

- ✓ Le délai de 72 heures commence après avoir eu connaissance de l'intrusion.
- ✓ Déposez plainte au commissariat ou à la gendarmerie et demandez le procès-verbal, ou écrivez au procureur de la République par lettre recommandée.
- ✓ Conservez le procès-verbal ou la preuve de dépôt du recommandé.



Attention : la pré-plainte en ligne n'est pas une plainte. Elle ne répond pas au délai de 72h. Déposez plainte au commissariat ou écrivez au procureur par lettre recommandée.

Activez immédiatement votre **assistance cyber**

- ✓ En cas de dommages, contactez votre assistance cyber au numéro prévu dans votre contrat.
- ✓ N'attendez pas d'avoir identifié l'origine de l'attaque pour demander de l'aide.
- ✓ L'assistance vous accompagne pour contenir l'incident, limiter les dommages et organiser la reprise d'activité.



Notre conseil : n'agissez pas seul sur les systèmes compromis et ne répondez jamais aux attaquants avant d'avoir reçu les consignes de l'assistance.

Préservez les **preuves** de l'attaque

- ✓ Conservez les emails frauduleux, messages, demandes de rançon, liens suspects.
- ✓ Faites des captures d'écran et conservez les journaux d'événements (logs).
- ✓ Notez les informations essentielles : date, heure, systèmes touchés et impacts.



Conseil d'expert : ne supprimez pas les éléments liés à l'attaque. Ils pourront être utiles aux experts cyber, aux autorités et à votre assureur.

Contactez votre courtier **Onlynnov**

- ✓ Transmettez-nous le procès-verbal ou la preuve de dépôt dès que possible.
- ✓ Nous vous accompagnons dans la déclaration et le suivi du sinistre auprès de l'assureur.
- ✓ Conservez les justificatifs : factures, dépenses engagées, pertes constatées, échanges.



Notre conseil : centralisez tous les documents liés à l'incident dans un dossier dédié, hors du système touché.

Effectuez les **signalements** nécessaires

- ✓ En cas de violation de données personnelles, la CNIL doit être notifiée (RGPD).
- ✓ Selon l'incident, signalez-le aussi à l'ANSSI ou sur cybermalveillance.gouv.fr.
- ✓ Une fois l'urgence maîtrisée, documentez l'incident et les actions menées.



Notre conseil : faites-vous accompagner par votre assistance cyber et votre courtier pour identifier les démarches adaptées à votre situation.

Imprimez cette fiche et partagez-la à tous vos salariés.

En cas d'attaque, vous n'aurez plus accès à vos fichiers. Tout salarié qui constate un incident ou clique sur un lien suspect prévient immédiatement son responsable informatique.

