DROIT ET RÉGLEMENTATION

DÉPOSER PLAINTE
après une cyber attaque



CLUSIF

DROIT ET RÉGLEMENTATION

DÉPOSER PLAINTE
après une cyber attaque

Pourquoi déposer plainte ?

4 RAISONS DE DÉPOSER PLAINTE

→ Déclencher une enquête

Le dépôt de plainte permet l'ouverture d'une enquête pénale, indispensable à l'identification et la sanction des auteurs ; dans de nombreuses situations où seule la victime a connaissance de l'incident, cet acte est de facto le seul permettant une réponse judiciaire.

→ Être reconnu comme victime

Le dépôt de plainte est la condition juridique pour accéder à une indemnisation, constituer partie civile, et tenter de récupérer des fonds volés (recall SEPA possible sous 10 jours, chances fortement réduites après 72h).

→ Protéger l'organisation

Preuve d'une réaction responsable vis-à-vis des partenaires ; possibilité de faire révoquer des documents d'identité volés ou de bloquer l'exploitation de données stratégiques.

→ Satisfaire à l'obligation assurantielle

Depuis la loi LOPMI (2023), l'indemnisation par l'assureur est conditionnée à un dépôt de plainte dans les 72 heures suivant la découverte de l'incident. Le dépôt en ligne n'est pas accepté par les compagnies.

Le saviez-vous ?

Certains acteurs sont tenus à des obligations légales de signalement : fonctionnaires (article 40 du Code de procédure pénale), professionnels de secteurs réglementés (banques, opérateurs télécom, experts-comptables, avocats, notaires).

comment déposer plainte ?

→ Anticiper avant l'événement

Ne pas attendre l'incident pour identifier le service de police ou de gendarmerie compétent à proximité.

Un contact préalable permet d'obtenir les bons interlocuteurs pour la prise de plainte et, le cas échéant, d'être orienté vers les unités spécialisées (BEFTI, C3N, ICC…).

→ Qui, quand, où

Qui

Le représentant légal de la personne morale, ou toute personne munie d'un pouvoir spécial de représentation.

Quand

Le plus tôt possible. Délai légal : 6 ans pour les délits, mais la volatilité des preuves numériques impose d'agir dans les premiers jours. Délai critique LOPMI : 72h.

Où

Auprès d'un service de police / gendarmerie (dépôt en main propre obligatoire, même en cas de pré-plainte en ligne) ou auprès du procureur de la République (de préférence, par dépôt en main propre au Tribunal, ou, à défaut, par courrier postal ou électronique). Le dépôt en main propre garantit la rapidité de la prise en compte de la plainte car il permet d'ouvrir l'enquête et de signaler l'éventuelle urgence à traiter les faits.

Les bons réflexes

Déposer une première plainte avec un minimum d'éléments pour obtenir le récépissé, puis compléter ultérieurement par audition ou complément de plainte.

Préparer les éléments utiles : logs, captures d'écran, rapports d'analyse, contacts prestataires, mandat de représentation si délégation.

CE QU'IL FAUT SAVOIR SUR L'ENQUÊTE

L'enquête cyber est par nature longue et complexe : preuves numériques volatiles, auteurs souvent à l'étranger, cycles d'investigation itératifs. L'absence de nouvelles n'est pas un classement sans suite. La qualité et la rapidité du signalement conditionnent directement les chances d'aboutissement.

LE GROUPE DE TRAVAIL *Dépôt de plainte suite à une cyberattaque* DU CLUSIF

Le GT du Clusif consacré au dépôt de plainte publiera d'ici la fin de l'année 2026 plusieurs fiches thématiques : chaîne pénale, éléments de facilitation d'une enquête, modèles de main courante et de délégation de signature ou encore recommandations pour anticiper et simplifier le dépôt de plainte.

Ce groupe réunit des RSSI, avocats et juristes, anciens enquêteurs ou encore des acteurs du monde de l'assurance.

La présente plaquette représente un point d'étape très synthétique des avancées du groupe.

Toutes les publications de l'association :
clusif.fr/publications/

CLUSIF

Tour Eria, 5 Rue Bellini, 92800 Puteaux
clusif@clusif.fr - https://clusif.fr