POLICE NATIONALE

Hautes Terres tourisme
Volcan - Cantal

OFAC
OFFICE ANTI-CYBERCRIMINALITÉ

UNE RÉPONSE AMBITIEUSE POUR LUTTER CONTRE TOUTES LES FORMES DE CYBERCRIMINALITÉ

RECYM
RÉSEAU DES EXPERTS CYBER-MENACES DE LA DIRECTION NATIONALE DE LA POLICE JUDICIAIRE

Locations saisonnières : comment éviter les arnaques et les cyber-risques ?

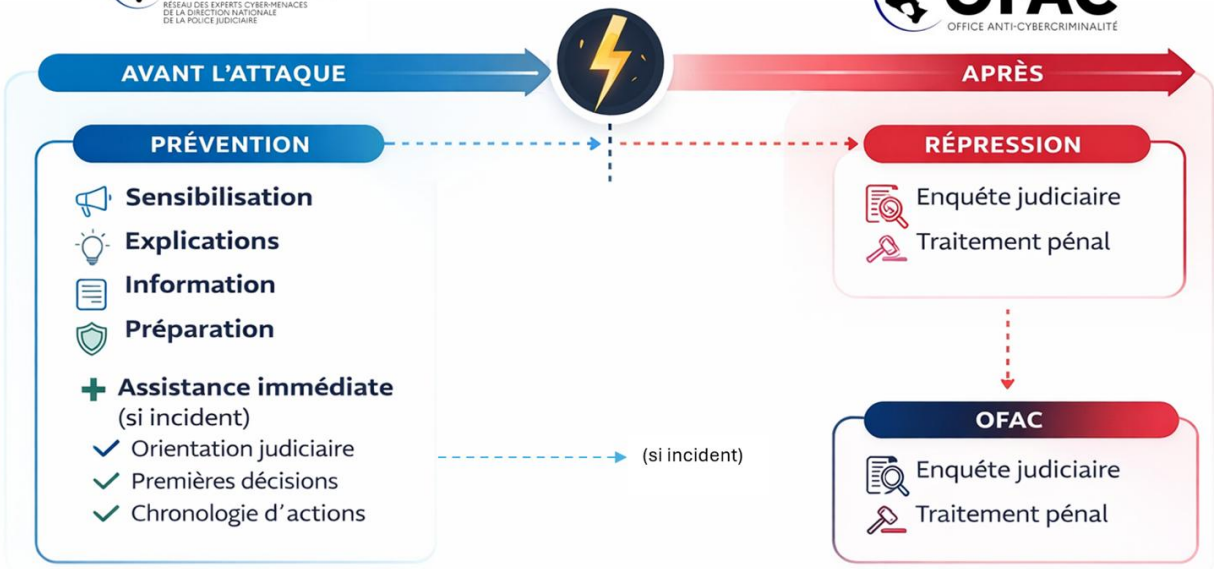
Comprendre,
Prévenir
Réagir

POLICE
NATIONALE

DNPJ
DIRECTION NATIONALE
DE LA POLICE JUDICIAIRE

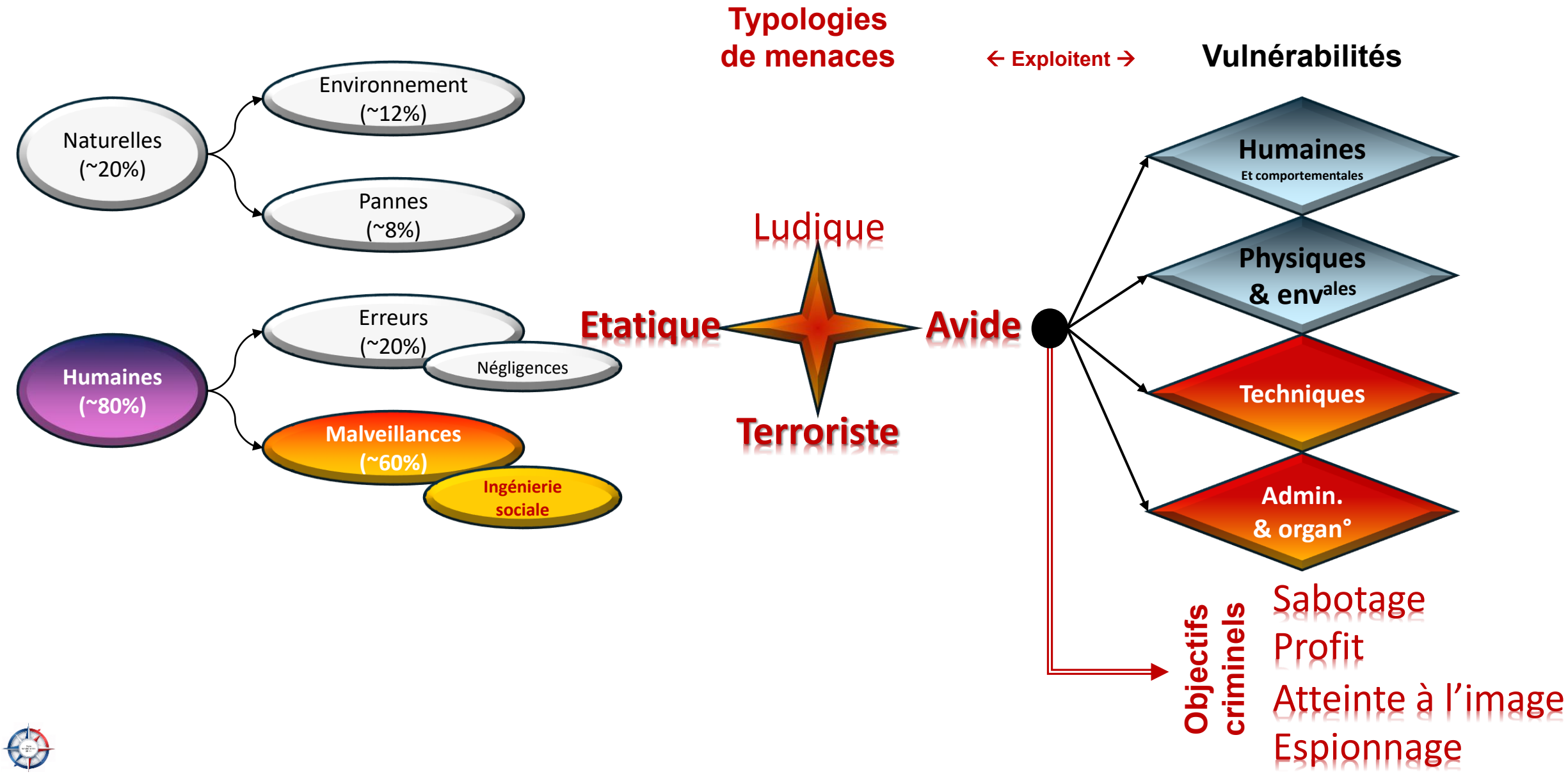
RECYM
RÉSEAU DES EXPERTS CYBER-MENACES
DE LA DIRECTION NATIONALE
DE LA POLICE JUDICIAIRE

OFAC
OFFICE ANTI-CYBERCRIMINALITÉ



RECYM
RÉSEAU DES EXPERTS CYBER-MENACES
DE LA DIRECTION NATIONALE
DE LA POLICE JUDICIAIRE

MENACES : UN EVENEMENT INTERNATIONAL GENERE UNE FORTE VISIBILITE ET ATTIRE DES ACTEURS MALVEILLANTS



RECYM
ZONE SUD-EST

VIOLATIONS DE DONNÉES EN FRANCE : NIVEAU RECORD EN 2025

2026 : plus de contrôles, plus de sanctions, zéro tolérance

DES RECORDS QUI S'ACCÉLÈRENT

6 167
violations de données notifiées à la CNIL en 2025

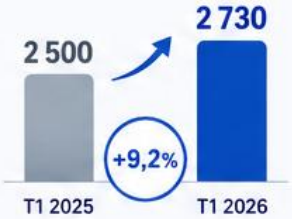
+9,5 %
par rapport à 2024

+50 %
en trois ans

TENDANCE 2026 : L'ACCÉLÉRATION CONTINUE

1er TRIMESTRE 2026

2 730
violations de données



NATURE DES VIOLATIONS

1 fuite sur 2
est liée à un piratage

Secteurs les plus touchés

- Administration publique
- Santé
- Finance / Assurance

DONNÉES MASSIVES : UN RISQUE CROISSANT

~40
violations ont concerné des bases de plus d'1 million de personnes

soit **+10** violations massives en un an

CAS EMBLÉMATIQUES

ATTAQUE CONTRE L'ANTS
(Agence nationale des titres sécurisés)

près de **12 MILLIONS** de particuliers et professionnels concernés

ATTAQUES WEDA + HARVEST

WEDA (santé) + harvest (conseil patrimonial)

Un seul incident technique
+ 11 600
notifications CNIL via les entreprises clientes impactées

- Risque fournisseur
- Effet domino
- Supply chain cyber

LE RISQUE FOURNISSEUR EN CHIFFRES

Fournisseur compromis → Nombreuses entreprises clientes impactées → Effet domino massif

SANCTIONS CNIL : CHANGEMENT D'ÉCHELLE

MONTANT DES AMENDES

NOMBRE DE SANCTIONS

87 en 2024 — 83 en 2025

Moins de sanctions, mais beaucoup plus lourdes financièrement

DES MESSAGES FORTS

« Personne n'est épargné »
Marie-Laure Denis, présidente de la CNIL

« Les violations sont de plus en plus massives »

« L'intelligence artificielle automatise, industrialise et démocratise les attaques »

TENDANCES STRATÉGIQUES

LE PRESTATAIRE, MAILLON FAIBLE

Sous-traitants, PME techniques, éditeurs logiciels, hébergeurs...

Une petite structure vulnérable peut contaminer tout un écosystème.

LA DONNÉE DE SANTÉ, CIBLE PRIORITAIRE

- Forte valeur sur les marchés criminels
- Données durables
- Risques d'extorsion, de fraude, d'usurpation et de ciblage social

DURCISSEMENT ANNONCÉ EN 2026

- Plus de contrôles
- Plus de sanctions
- Focus sur les grandes bases de données, la cybersécurité et les violations massives

BONNE HYGIÈNE NUMÉRIQUE : LES BONS RÉFLEXES

- Ne pas cliquer sur les liens douteux
- Adopter des mots de passe robustes
- Mettre à jour régulièrement ses logiciels
- Être vigilant : les conséquences d'une fuite de données peuvent survenir plusieurs semaines voire mois plus tard

LA CYBERSÉCURITÉ EST L'AFFAIRE DE TOUS : VIGILANCE, ANTICIPATION, PROTECTION

METHODES D'ATTAQUES

⚠ IMPACTS CONCRETS POSSIBLES ⚠

1. FINANCIERS

FOVI - escroqueries (deepfakes)

- Fraude au virement (FOVI)
- Usurpation d'identité de dirigeants
- Escroqueries par deepfakes (audio / vidéo)
- Perte financière, vol de données, chantage

2. TECHNIQUES

DDOS

- Saturation des sites et services en ligne
- Indisponibilité des plateformes et applicatifs
- Perturbation des activités critiques
- Atteinte à la réputation

3. VECTEURS

Piratage de messageries

Emails frauduleux, liens ou pièces jointes malveillantes pour voler identifiants et données sensibles.

Rançongiciels

Chiffrement des données et demande de rançon. Arrêt de l'activité et pertes importantes.

Faux QR Code

Redirection vers des sites malveillants pour voler des données ou installer des logiciels malveillants.

APPELS TÉLÉPHONIQUES ET DEEPFAKES VIDÉO ET AUDIO

Usurpation de voix ou d'image pour demander des actions ou des virements frauduleux.

ATTENTION AUX DIFFUSIONS « SOURCES OUVERTES » VIA LES RÉSEAUX SOCIAUX

Informations en temps réel exploitables par des attaquants (localisation, organisation, vulnérabilités...).

LOCATION SAISONNIÈRE : TOUS LES RISQUES POUR LES LOUEURS

Des menaces multiples, des impacts réels.

airbnb | Booking.com | Abritel

et autres plateformes ou location directe

LES BONS RÉFLEXES À ADOPTER

- Rester sur les plateformes officielles
- Utiliser des mots de passe forts et uniques + 2FA
- Vérifier l'identité et les paiements
- Sécuriser Wi-Fi et objets connectés
- Ne conserver que les données nécessaires
- Être vigilant et se méfier des urgences
- Conserver les preuves (échanges, paiements...)
- En cas de doute : se renseigner et signaler

EN CAS D'INCIDENT

- Conserver les preuves
- Contacter la plateforme / votre banque
- Signaler sur 17Cyber.gouv.fr ou Cybermalveillance.gouv.fr

FUITE DE DONNÉES DANS LE TOURISME : DES ATTAQUES MASSIVES EN 2026

De plus en plus de plateformes et d'acteurs du tourisme ciblés par les cybercriminels

⚠ Plus une plateforme est populaire, plus elle devient une cible attractive pour les cybercriminels.

1. DEUX ACTEURS MAJEURS TOUCHÉS EN MAI 2026

PIERRE & VACANCES CENTER PARCS

Pierre & Vacances

CenterParcs

1,6 MILLION de réservations concernées

Données avec un historique potentiel pouvant remonter jusqu'à **10 ANS** (2005–2026)

DONNÉES POTENTIELLEMENT EXPOSÉES

- Numéro de réservation
- Numéro de téléphone
- Dates et lieu de séjour
- Date de naissance
- Nom des occupants de l'hébergement

BELAMBRA

Annonce le 16 mai 2026

Belambra clubs

44 clubs de vacances en France

DONNÉES POTENTIELLEMENT EXPOSÉES

- Plus de **41 000** réservations détaillées
- Plus de **42 000** réservations clients
- Environ **360 000** données liées à des **mineurs et enfants**

CE QUI N'A PAS ÉTÉ EXPOSÉ

- Aucune donnée bancaire
- Aucun document d'identité
- Aucun mot de passe

2. D'AUTRES PLATEFORMES TRÈS CIBLÉES

Booking.com

Plusieurs incidents et campagnes ciblées

- Accès non autorisé à certaines données de réservation (avril 2026).
- Exposition possible : noms, emails, téléphones, détails de réservation, messages avec les hébergements.
- Données utilisées ensuite pour des campagnes de phishing ultra crédibles (faux messages d'hôtels, fausses demandes de paiement).
- Comptes d'hôtels partenaires parfois compromis, permettant l'envoi de faux messages depuis des messageries apparemment légitimes.

leboncoin

Plateforme historiquement très ciblée

Principales attaques observées :

- **Faux paiements** (faux liens, faux mails de paiement).
- **Faux livreurs / faux transporteurs** (faux liens pour "récupérer l'argent").
- **Faux support Le Bon Coin** (usurpation du service sécurité ou du support client).
- **Usurpation de comptes** pour publier de fausses annonces crédibles.
- **Phishing massif** (SMS, mails, faux retraits d'argent, faux paiements).

3. L'AMPLEUR DES FAITS

+ de 4,5 MILLIONS

de clients potentiellement concernés au total (PVCP + autres acteurs)

2005 à 2026

Période des données potentiellement exposées

Des hackers contactent directement les sites spécialisés (ex : French Breches) et fournissent des échantillons de données.

D'autres services touristiques et plateformes français signalés, mais non encore confirmés.

RISQUES PHYSIQUES POUR LES LOUEURS

Protégez votre logement, votre tranquillité et votre sécurité

6.1 ATTENTION AUX INFORMATIONS PUBLIÉES

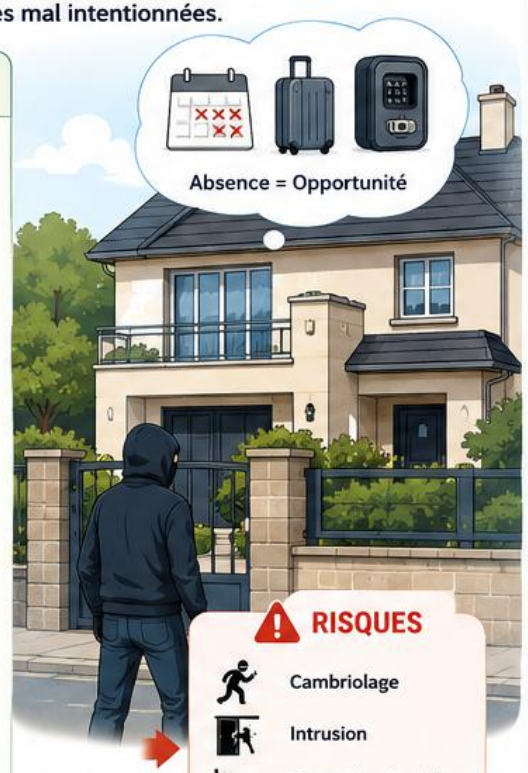
Trop d'informations en ligne peuvent révéler vos absences et attirer les personnes mal intentionnées.

EXEMPLES DANGEREUX

Annoncer publiquement les périodes d'absence

Publier les départs en vacances en direct

Montrer les accès ou équipements de sécurité



RISQUES

- Cambriolage
- Intrusion
- Occupation frauduleuse

BONS RÉFLEXES

- Ne partagez pas vos absences
- Paramétrez vos publications en privé
- Évitez de montrer vos équipements de sécurité
- Réfléchissez avant de publier
- Moins d'infos publiques = plus de sécurité

6.2 BOÎTES À CLÉS ET ACCÈS

Une mauvaise gestion des accès peut faciliter les intrusions et les occupations frauduleuses.

MAUVAISES PRATIQUES

- Code identique permanent (jamais changé)
- Code visible facilement repérable (1234)
- Transmission non sécurisée (SMS, WhatsApp, mail, appel...)

CONSEILS

- Changer régulièrement les codes
- Limiter les accès aux personnes nécessaires
- Éviter les informations visibles sur place (CODE 1234)

BONS RÉFLEXES

- Changez les codes régulièrement
- Donnez les accès uniquement aux voyageurs concernés
- Transmettez les codes via la messagerie sécurisée de la plateforme
- Vérifiez qu'aucune info n'est visible de l'extérieur
- En cas de doute : sécurisez immédiatement

MOINS D'INFORMATIONS ET DES ACCÈS MIEUX CONTRÔLÉS = MOINS DE RISQUES !

CYBERFRAUDES ET ARNAQUES EN FRANCE EN 2025 : LES CHIFFRES CLÉS

Un risque massif et en forte progression, qui touche chacun d'entre nous, y compris lors des locations saisonnières.

1. CHIFFRES GÉNÉRAUX SUR LES CYBERFRAUDES ET ESCROQUERIES

EXPOSITION MASSIVE DES INTERNAUTES

73 %
des internautes français déclarent avoir été confrontés à une cybermalveillance.

39 %
déclarent avoir été victimes d'au moins une escroquerie ou attaque numérique.

PROGRESSION DU PHISHING ET DES ESCROQUERIES

+70 %
de phishing

+170 %
d'escroqueries commerciales liées aux faux sites, faux paiements et usurpations de plateformes.

Source : Cybermalveillance.gouv.fr (2025)

SIGNALEMENTS MASSIFS

1,6 million
de signalements de phishing en France en 2025

310 millions d'€
de pertes estimées

NOMBRE DE VICTIMES

+ 500 000
personnes auraient été victimes de cyberattaques ou cyberescroqueries en France en 2025.

Sources : synthèses de données publiques 2025.

EXPLOSION DES VIOLATIONS DE DONNÉES

6 167
violations de données enregistrées par la CNIL en 2025 (niveau le plus élevé jamais atteint)

Environ la moitié résultent de piratages informatiques.

Près de 80 violations ont touché chacune plus d'un million de personnes sur les deux dernières années.

Source : CNIL (2025)

2. CHIFFRES SPÉCIFIQUES AUX LOCATIONS SAISONNIÈRES

MULTIPLICATION DES ARNAQUES AUX LOCATIONS

+30 %
de signalements d'arnaques à la location saisonnière sur un an.

Sources : études et organismes spécialisés (2025)

IMPACT RÉEL SUR LES FRANÇAIS

48 %
des Français déclarent avoir déjà été victimes, ou connaître quelqu'un victime, d'une arnaque à la location de vacances.

Pertes moyennes : ~ 2 700 €

Sources : Étude OpinionWay (2024–2025)

FAUSSES ANNONCES DÉTECTÉES

2 500
fausses annonces supprimées par Airbnb entre mars 2023 et mars 2024.

Source : Airbnb (2024)

PRINCIPALES FRAUDES OBSERVÉES DANS LES LOCATIONS SAISONNIÈRES

- Paiements hors plateforme
- Faux propriétaires
- Usurpation d'annonce
- Phishing
- Faux supports techniques
- Piratage de compte
- Fraude au remboursement
- Faux voyageurs

3. CHIFFRES TRÈS UTILES POUR "MARQUER" LE PUBLIC

"1 FRANÇAIS SUR 2"
« Près d'un Français sur deux déclare avoir déjà été confronté directement ou indirectement à une arnaque à la location de vacances. »

"73 % DES INTERNAUTES"
« Aujourd'hui, près des trois quarts des internautes français ont déjà été confrontés à une cybermalveillance. »

"6 000 VIOLATIONS DE DONNÉES"
« En 2025, la France a dépassé les 6 000 violations de données déclarées à la CNIL. »

"+170 %"
« Les escroqueries commerciales en ligne ont explosé avec une hausse de 170 %. »

EN RÉSUMÉ

- La cybercriminalité touche massivement tous les Français.
- Les escroqueries et le phishing explosent d'année en année.
- Les pertes financières sont considérables : des centaines de millions d'euros en 2025.
- Les locations saisonnières sont particulièrement ciblées, et le phénomène s'accélère.

LA VIGILANCE RESTE LA MEILLEURE PROTECTION : méfiez-vous des offres trop belles pour être vraies, restez dans les plateformes, vérifiez toujours.

SCÉNARIO TYPE : L'ARNAQUE AU FAUX VOYAGEUR

1 PRISE DE CONTACT RASSURANTE

Le fraudeur contacte le propriétaire via la plateforme avec un message poli, crédible et détaillé.

2 CONSTRUCTION DE LA CONFIANCE

Le fraudeur personnalise l'échange, parle de sa famille, rassure et crée un lien humain pour baisser la vigilance.

3 SORTIE DE LA PLATEFORME

Le fraudeur propose de continuer la discussion sur WhatsApp, SMS ou mail pour sortir de la plateforme et de ses protections.

4 LA RÉSERVATION PARAÎT CONFIRMÉE

Le fraudeur envoie un faux virement, un faux mail bancaire ou une capture d'écran qur semble crédible.

5 PRESSION PSYCHOLOGIQUE

Le fraudeur crée de l'urgence, met la pression, évoque des enfants, un retard, pour pousser le propriétaire à agir vite et à faire confiance.

6 OBTENTION DES ACCÈS

Le propriétaire transmet les codes d'accès (boîte à clés, serrure connectée, Wi-Fi...) convaincu que tout est en régle.

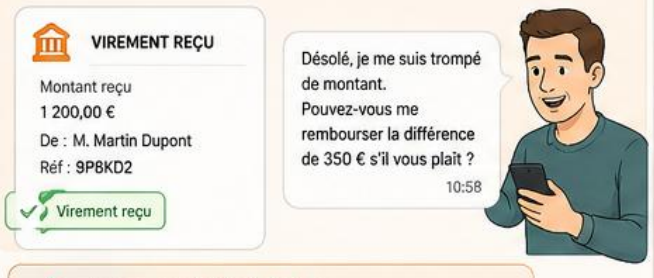
7 DISPARITION OU ESCALADE

⚠ Aucun paiement réel n'a été effectué.
Le fraudeur disparaît ou occupe le logement frauduleusement.

Le fraudeur disparaît, occupe le logement, demande un remboursement ou exploite les informations obtenues.

VARIANTES FRÉQUENTES

VARIANTE 1 : FAUX TROP-PERCU



⚠ Le paiement initial est faux.
Le propriétaire envoie l'argent réel au fraudeur.

VARIANTE 2 : FAUX SUPPORT CLIENT

⚠ Le faux conseiller récupère le code SMS et prend le contrôle du compte.

VARIANTE 3 : PIRATAGE DU COMPTE PROPRIÉTAIRE

⚠ Le propriétaire saisit ses identifiants sur un faux site :
le compte est compromis et le fraudeur peut tout contrôler.

SIGNAUX D'ALERTE À REPÉRER

- Demande de sortir de la plateforme
- Urgence et pression
- Paiement "en attente"
- Liens suspects ou inconnus
- Fautes d'orthographe inhabituelles
- Refus des procédures normales
- Demande de remboursement rapide

BONS RÉFLEXES

- Rester dans la messagerie officielle
- Vérifier le paiement sur votre compte bancaire
- Ne jamais envoyer les clés avant confirmation réelle
- Ne jamais cliquer sur un lien reçu par message
- Activer la double authentification
- Conserver tous les échanges et preuves

LOCATION SAISONNIÈRE : LES STRATÉGIES À DÉPLOYER POUR PRÉVENIR LES RISQUES

Anticiper, sécuriser, vérifier, protéger : adoptez les bons réflexes au quotidien.

1. SÉCURISER SES COMPTES

- Utiliser des mots de passe forts et uniques pour chaque compte
- Activer la double authentification (2FA) partout où c'est possible
- Ne jamais partager ses identifiants
- Vérifier régulièrement les connexions et appareils connectés

OBJECTIF :
Empêcher le piratage de vos comptes et la prise de contrôle de vos annonces.

2. ÊTRE VIGILANT FACE AUX RÉSERVATIONS

- Rester dans la messagerie de la plateforme
- Se méfier des demandes de contact en dehors de la plateforme
- Vérifier le profil et les avis du voyageur
- Se méfier de l'urgence et des demandes inhabituelles

OBJECTIF :
Éviter les arnaques aux faux voyageurs et les paiements frauduleux.

3. VÉRIFIER LES PAIEMENTS

- Ne jamais se fier à une capture d'écran ou à un email de confirmation
- Vérifier le paiement directement sur votre compte bancaire
- Ne jamais envoyer les codes ou clés avant réception du paiement réel
- Se méfier des trop-perçus et des remboursements demandés

OBJECTIF :
S'assurer que l'argent est bien réel avant toute remise d'accès.

UNE DÉFENSE EN 3 ÉTAPES

ANTICIPER les menaces

SÉCURISER vos accès et vos équipements

VÉRIFIER chaque demande et chaque paiement

4. SE PROTÉGER CONTRE LE PHISHING

- Se méfier des emails/SMS inattendus
- Ne jamais cliquer sur un lien suspect
- Vérifier l'adresse de l'expéditeur
- Contacter directement la plateforme en cas de doute

OBJECTIF :
Éviter le vol de vos identifiants et les fraudes.

5. PROTÉGER LES DONNÉES PERSONNELLES

- Collecter uniquement les données nécessaires
- Ne conserver les pièces d'identité que le temps nécessaire
- Stocker les documents de façon sécurisée
- Supprimer régulièrement les données inutiles

OBJECTIF :
Respecter la vie privée des voyageurs et éviter les fuites de données.

6. SÉCURISER LE LOGEMENT ET LES ACCÈS

- Changer régulièrement les codes des boîtes à clés et serrures connectées
- Ne pas laisser d'indices visibles sur les accès
- Séparer le réseau Wi-Fi invité du réseau principal
- Mettre à jour les équipements (box, caméras, objets connectés)

OBJECTIF :
Protéger votre logement, vos équipements et la sécurité de vos occupants.

7. MAÎTRISER SA RÉPUTATION EN LIGNE

- Surveiller régulièrement vos annonces et les avis publiés
- Signaler rapidement toute usurpation d'annonce ou avis frauduleux
- Utiliser vos propres photos et descriptions originales
- Être réactif et professionnel dans vos échanges

OBJECTIF :
Protéger votre réputation et renforcer la confiance des voyageurs.

LES 10 COMMANDEMENTS DU LOUEUR PRUDENT

1. Je sécurise mes comptes
2. Je reste toujours dans la plateforme
3. Je vérifie mes voyageurs
4. Je confirme les paiements
5. Je me méfie des liens et pièces jointes
6. Je sécurise mon Wi-Fi et mes équipements
7. Je protège les données personnelles
8. Je gère les accès avec prudence
9. Je reste discret sur mes absences et mes biens
10. Je conserve toutes les preuves des échanges

EN CAS DE DOUTE OU D'INCIDENT

- Conservez toutes les preuves (captures, messages, emails...)
- Changez immédiatement vos mots de passe
- Contactez la plateforme et/ou votre banque
- Signalez sur 17Cyber.gouv.fr ou Cybermalveillance.gouv.fr

17 CYBER

MESURES PRIORITAIRES DE PREVENTION

Encadrement des usages numériques : 6 points clés pouvant être rapidement mis en œuvre

- Diffuser un message de vigilance à tous les collaborateurs
- Réaliser des sensibilisations flash (5 à 10 min)
- Rappeler les réflexes face aux emails et appels suspects
- Distribuer les supports OFAC / Cybermalveillance.gouv.fr
- Désigner un point de contact interne en cas de doute

MESURES PRIORITAIRES DE PREVENTION

Encadrement des usages numériques : 6 points clés pouvant être rapidement mis en œuvre

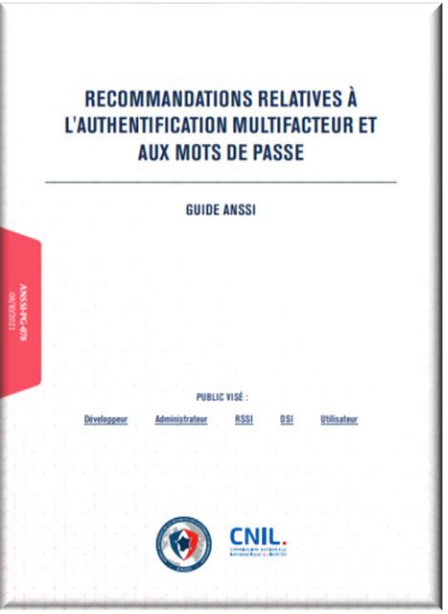
- Activer la double authentification (MFA) sur les comptes sensibles, quand cela est possible
- Changer les mots de passe faibles ou réutilisés
- Désactiver les comptes inutilisés
- Vérifier les droits d’accès des prestataires et partenaires

RECYM ZONE SUD-EST

MESURES PRIORITAIRES DE PREVENTION

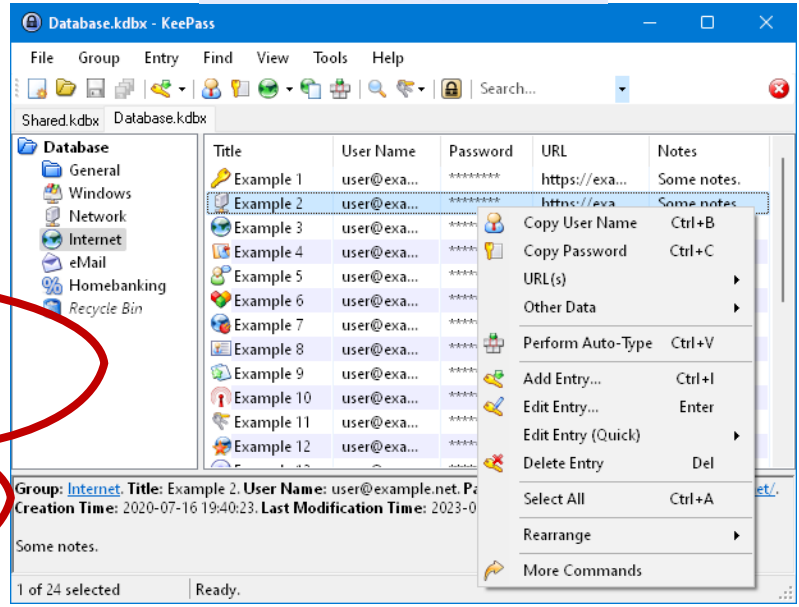
Sécurisation des accès : mots de passe et authentification forte

Les coffres forts de mots de passe



Un bon coffre-fort de mots de passe est un système où même l'éditeur du logiciel ne peut pas lire vos mots de passe. Si ce n'est pas le cas, ce n'est pas un coffre-fort, c'est une armoire grande ouverte !!

KeePass



MESURES PRIORITAIRES DE PREVENTION

Encadrement des usages numériques : 6 points clés pouvant être rapidement mis en œuvre

La vigilance opérationnelle consiste à la mise en place de règles simples, applicables, et comprises. Elles viseront par exemple à :

- Renforcer les contrôles sur les virements et demandes urgentes
- Mettre en place une double validation pour les opérations sensibles
- Sensibiliser aux faux QR codes et aux faux supports G7
- Vérifier systématiquement l'identité des interlocuteurs inhabituels

MESURES PRIORITAIRES DE PREVENTION
Grande vigilance sur les emails et demandes inhabituelles

Les bonnes pratiques pour se protéger

Les cybercriminels utilisent des emails frauduleux (phishing) pour voler vos informations, installer des logiciels malveillants ou vous inciter à réaliser des actions dangereuses.

Restez vigilant : quelques réflexes simples font la différence !

LES BONNES PRATIQUES

VÉRIFIEZ L'EXPÉDITEUR
Contrôlez l'adresse email complète. Méfiez-vous des adresses inhabituelles ou approximatives.

SOYEZ ATTENTIF AUX PIÈCES JOINTES
N'ouvrez jamais une pièce jointe inattendue ou suspecte. Privilégiez les formats sûrs (PDF).

VÉRIFIEZ LES LIENS
Ne cliquez pas directement sur les liens. Passez votre souris dessus pour vérifier l'URL réelle.

MÉFIEZ-VOUS DES DEMANDES URGENTES
Les emails qui créent un sentiment d'urgence visent souvent à vous faire agir sans réfléchir.

NE COMMUNIQUEZ PAS D'INFORMATIONS SENSIBLES
Aucune organisation sérieuse ne vous demandera vos mots de passe ou données personnelles par email.

EN CAS DE DOUTE, CONTACTEZ L'EXPÉDITEUR
Utilisez un autre moyen de contact (téléphone, site officiel) pour vérifier la légitimité du message.

EXEMPLE D'EMAIL SUSPECT
Les signaux d'alerte à repérer

EXPÉDITEUR SUSPECT
Adresse inhabituelle, orthographe approximative ou domaine étrange.

OBJET ALARMISTE
Crée un sentiment d'urgence pour vous pousser à agir.

LIEN SUSPECT
Ne cliquez pas ! Vérifiez l'URL réelle (survolez le lien).

PIÈCE JOINTE DANGEREUSE
Fichier exécutable (.exe, .scr, .bat...) potentiellement malveillant.

QUE FAIRE EN CAS DE DOUTE ?

NE RÉPONDEZ PAS
Ne répondez pas à l'email suspect.

NE CLIQUEZ PAS
Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe.

SIGNALEZ
Signalez l'email à votre service informatique ou via l'outil de signalement de votre organisation.

SUPPRIMEZ
Supprimez l'email de votre boîte de réception.

PROTÉGEZ-VOUS
Maintenez vos logiciels et antivirus à jour.

À RETENIR

- **Observer** — Prenez le temps d'analyser l'email.
- **Douter** — En cas de doute, restez prudent.
- **Vérifier** — Vérifiez l'expéditeur, les liens et les pièces jointes.
- **Protéger** — Adoptez les bons réflexes au quotidien.

Un clic peut tout changer.
Votre vigilance est votre meilleure protection !

NB : supprimer les anciens appareils non utilisés et ne laissez jamais un compte de messagerie inutilisé, sinon clôturez-le.

MESURES PRIORITAIRES DE PREVENTION

Encadrement des usages numériques : 6 points clés pouvant être rapidement mis en œuvre

- Vérifier que les sauvegardes fonctionnent réellement
- Tester une restauration simple
- Isoler au moins une sauvegarde (offline ou immuable)
- Identifier les systèmes critiques à redémarrer en priorité

MESURES PRIORITAIRES DE PREVENTION

Encadrement des usages numériques : 6 points clés pouvant être rapidement mis en œuvre

- Sensibiliser aux risques de diffusion d'informations sensibles
- Éviter la publication d'informations logistiques ou organisationnelles
- Rappeler les règles de communication externe
- Surveiller les faux comptes ou usurpations

Point de vigilance

MESURES PRIORITAIRES DE PREVENTION

Encadrement des usages numériques : 6 points clés pouvant être rapidement mis en œuvre

- Identifier les personnes à contacter en cas d'incident
- Préparer une procédure simple d'alerte interne (dont cellule de crise, slide suivante)
- Prévoir un circuit court de décision
- Conserver les numéros et plateformes utiles listés un peu plus loin dans cette présentation.

RECYM ZONE SUD-EST

MESURES PRIORITAIRES DE PREVENTION

PRÉPARER UNE CELLULE DE GESTION DE CRISE

SIMPLE, RAPIDE ET CONFORME AUX PRESCRIPTIONS DE L'ANSSI

ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

1 DÉSIGNER UN RÉFÉRENT INCIDENT

Une personne identifiable et joignable.
Elle coordonne et décide qui alerter.

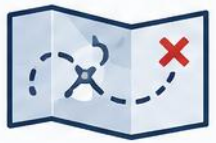
2 CONSTITUER UNE ÉQUIPE MINIMALE

3 à 6 personnes max représentant les fonctions essentielles de l'entreprise (IT, direction, métier, com, juridique/RH si possible).

3 DÉFINIR LES RÔLES ET RESPONSABILITÉS

Rédiger une fiche rôles : qui décide, qui communique, qui gère la technique, qui contacte les autorités, qui informe en interne.

4 PRÉPARER UN PLAN DE CRISE SIMPLE



1 à 2 pages avec : les scénarios possibles, les actions immédiates, les contacts, les outils, les escalades.

5 LISTER LES CONTACTS CLÉS ET OUTILS

Créer une liste à jour : interne + externe (prestataires, assureur, autorités, ANSSI/17Cyber, fournisseurs critiques).

6 PRÉPARER LES CANAUX DE COMMUNICATION DE SECOURS

Prévoir un moyen alternatif si les outils habituels sont indisponibles (téléphone, SMS, messagerie sécurisée, radio, etc.).

7 SAUVEGARDER ET ISOLER

Vérifier les sauvegardes, leur mode de restauration et s'assurer qu'au moins une copie est isolée (offline ou immuable).

8 PRÉPARER LES MODÈLES DE COMMUNICATION

Préparer des messages types pour : collaborateurs, clients, partenaires, prestataires, médias (si nécessaire).

9 TESTER LE DISPOSITIF

Organiser un mini-exercice (30-60 min) pour vérifier les contacts, les accès, la compréhension des rôles.

10 TENIR À JOUR ET AMÉLIORER

Mettre à jour régulièrement le plan, les contacts et les procédures après chaque incident ou test.

À RETENIR

- **L'objectif :** être prêt à réagir vite, décider juste et limiter l'impact.
- **Mieux vaut** un dispositif simple et connu de tous qu'un plan parfait oublié.
- **La préparation** aujourd'hui réduit les dégâts demain.

CONTACTS NATIONAUX UTILES

17 CYBER
Assistance et signalement en cas d'incident

THÉSÉE
Plateforme de signalement des entreprises

PHAROS
Signalement de contenus illicites en ligne

BON À SAVOIR : L'ANSSI met à disposition des guides et modèles sur **cyber.gouv.fr** pour vous aider à structurer votre dispositif.

cyber.gouv.fr

PRESERVER LES PREUVES : conseils essentiels en cas de cyberattaque

Objectif

Permettre l'exploitation technique et judiciaire de l'incident sans détruire les éléments utiles à l' enquête.

Les bons réflexes immédiats

1. Ne pas supprimer les fichiers suspects

Ne pas :

- supprimer les emails frauduleux,
- vider les corbeilles,
- effacer des journaux,
- "faire le ménage".
- un simple email peut contenir des éléments techniques exploitables.

2. Éviter les redémarrages inutiles

Ne pas :

- éteindre brutalement,
- redémarrer plusieurs fois,
- réinstaller immédiatement.

Certaines traces utiles disparaissent après extinction.

3. Isoler sans détruire

Si nécessaire :

- déconnecter du réseau,
- couper le Wi-Fi,
- isoler la machine.

Mais éviter les actions irréversibles.

4. Conserver les journaux et traces

Préserver :

- logs systèmes,
- journaux firewall,
- VPN,
- messagerie,
- sauvegardes,
- captures d'écran,
- horaires des événements.

5. Documenter chronologiquement

Noter :

- heure de découverte,
- premiers symptômes,
- actions réalisées,
- personnes contactées,
- décisions prises.

Une chronologie claire aide énormément les enquêteurs.

6. Conserver les supports et messages

Garder :

- SMS, messages vocaux, appels suspects,
- QR codes,
- emails, pièces jointes,
- liens frauduleux.

7. Ne pas communiquer d'informations techniques publiquement

Éviter sur :

- réseaux sociaux,
- communiqués improvisés,
- groupes publics.
- Certaines informations peuvent :
- compliquer l'enquête,
- aider les attaquants,
- nuire à la remédiation.

LE DEPOT DE PLAINTE

1 OÙ DÉPOSER VOTRE PLAINTE ?

En présentiel

- Dans un commissariat de police
- Dans une brigade de gendarmerie
- Ou par courrier au procureur de la République du tribunal judiciaire

En ligne

Vous pouvez aussi déposer plainte en ligne avec l'application THÉSEE Police Judiciaire

Disponible sur ordinateur et smartphone

2 COMMENT ÇA SE PASSE ?

- Vous exposez les faits
- Un agent ou un officier de police judiciaire (OPJ) prend votre plainte
- Un récépissé vous est remis

Le récépissé de dépôt de plainte est la preuve de votre démarche. Conservez-le précieusement.

3 QUELS DOCUMENTS FOURNIR ?

- Une pièce d'identité
- Tous éléments utiles : preuves, documents, courriels, captures d'écran, etc.

Plus vous fournissez d'éléments, plus l'enquête pourra être efficace.

4 APRÈS LE DÉPÔT DE PLAINTE

- Votre plainte est transmise au procureur de la République
- Une enquête peut être ouverte
- Vous serez informé(e) des suites données à votre plainte

À RETENIR

- Déposez plainte le plus rapidement possible.
- Conservez toutes les preuves en votre possession.
- Le dépôt de plainte est gratuit.
- Besoin d'aide ? Contactez 17Cyber

POLICE NATIONALE

RECYM
RÉSEAU DES EXPERTS CYBER-MENACES DE LA DIRECTION NATIONALE DE LA POLICE JUDICIAIRE

DNPJ
DIRECTION NATIONALE DE LA POLICE JUDICIAIRE

Qu'est-ce que le Module 17 Cyber ?

TROIS PARTENAIRES **UN GUICHET UNIQUE** **POUR TOUTES LES VICTIMES**