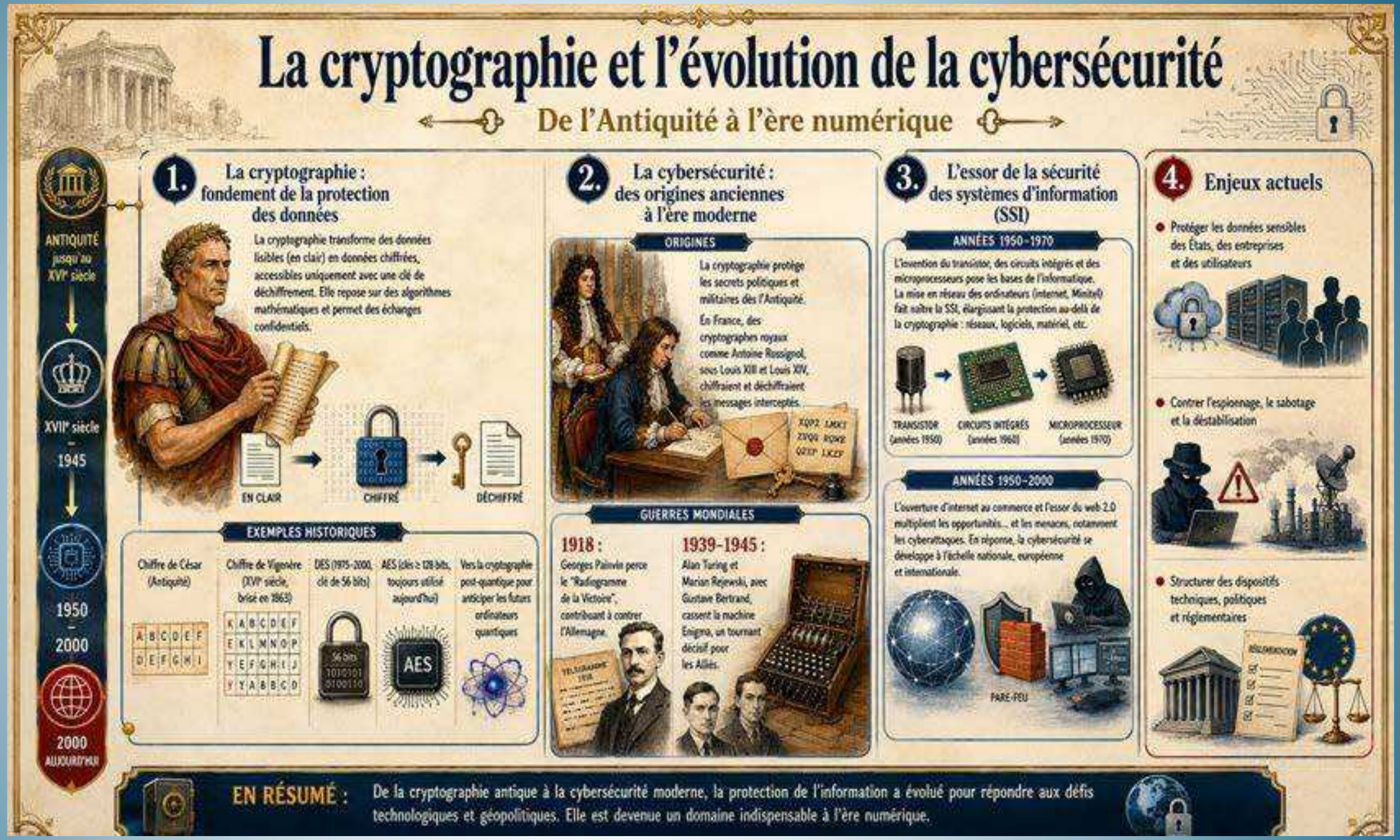


Mois du cyber 2026

Résilience en santé numérique





webinaire cyber résilience 2026 - Dr SALLIOT Adeline- URPS
CD ARA- visuel généré par IA

CYBERCRIMINALITÉ EN SANTÉ : LE PLUS CIBLÉ EN 2025

Les données de santé sont devenues l'une des cibles principales des cybercriminels en 2025, plus précieuses et plus durables que les données bancaires.

LA SANTÉ : LE SECTEUR LE PLUS CIBLÉ EN 2025



- Attaques en forte hausse (+35% en 2025*)
- Rançongiciels, vol de données, extorsion
- Interruption des soins et services critiques
- Données sensibles à forte valeur sur le dark web

*Source : Rapports cybersécurité 2025 (Santé)

40% DES DONNÉES SONT REVENDUES



Environ 40% des données de santé volées sont **revendues** sur le dark web ou des forums clandestins.

Le reste est utilisé pour des fraudes, usurpations ou extorsions.

PRIX DES DONNÉES DE SANTÉ SUR LE DARK WEB

Informations médicales basiques (nom, adresse, date de naissance, mutuelle...)	50 £ à 150 £
Dossier médical avec historique complet d'assurance maladie	≈ 500 £
Informations très complètes (diagnostics, traitements, imagerie, contacts...)	250 £ à 1 000 £

UN DOSSIER PEUT ÊTRE RECONSTITUÉ AVEC DES BRIBES D'INFORMATIONS

Même des informations apparemment anodines peuvent être assemblées pour reconstituer un dossier médical complet.

Accès à un rendez-vous en ligne + Paiement de parking + Emails / SMS de rappel + Achats en pharmacie + Résultats d'examens + Informations administratives (diverses sources) = Dossier médical reconstitué

DONNÉES D'ENFANTS ET DE MINEURS : TRÈS RECHERCHÉES



- Données valides plus longtemps (ouverture de crédit future)
- Moins susceptibles d'être surveillées
- Utilisées pour créer des identités synthétiques
- Très demandées sur le dark web

NOS EXAMENS PEUVENT RELEVER DE LA BIOMÉTRIE : RISQUE D'USURPATION D'IDENTITÉ

Imagerie médicale (IRM, scanner, radio)

Signaux biologiques (ECG, voix, empreintes numériques, ADN...)

Données biométriques visage, iris, empreintes, reconnaissance vocale...

Risque majeur d'usurpation d'identité
Difficulté à changer ces données uniques si elles sont compromises.

POURQUOI C'EST SI GRAVE ?

- Données sensibles, personnelles et permanentes
- Usurpation d'identité et fraudes financières
- Extorsion, chantage et revente en masse
- Impact direct sur la santé et la vie des patients

POURQUOI LA PROTECTION DES DONNÉES DE SANTÉ EST ESSENTIELLE

- Protéger la vie privée et la dignité des patients
- Garantir la continuité des soins et services
- Respecter les obligations légales (RGPD, NIS2, etc.)
- Maintenir la confiance des patients et usagers
- Éviter les pertes financières et atteintes à la réputation

À RETENIR

La donnée de santé a une valeur élevée, durable et personnelle.
Chaque information compte.
Chaque protection fait la différence.

CABINET DENTAIRE / MÉDICAL : TOUS LES PRESTATAIRES, TOUS CONCERNÉS

Un écosystème connecté au service des soins… et de votre sécurité

VOS PRESTATAIRES AU QUOTIDIEN

- **FOURNISSEUR DE MESSAGERIE SÉCURISÉE** — Hébergement professionnel, messagerie et outils sensibles (données patients)
- **FOURNISSEUR D'ANTIVIRUS / EDR** — Protection des postes, serveurs et périphériques
- **FOURNISSEUR D'ACCÈS INTERNET** — Connexion du cabinet (Internet, messagerie, téléservices)
- **ÉDITEUR DE LOGICIELS MÉTIERS** — Logiciel de gestion du cabinet, dossiers patients, comptabilité
- **MAINTENANCE INFORMATIQUE (MSP)** — Maintenance, mises à jour, support et assistance
- **HÉBERGEUR / CLOUD** — Hébergement des données du cabinet (logiciel métier, imagerie, sauvegardes)

VOS COLLABORATEURS ET SOUS-TRAITANTS

- **INFORMATICIEN** — Prestataire IT, infogérance, support à distance
- **LABORATOIRE DE PROTHÈSES FIXES** — Couronnes, bridges, inlays, onlays, etc.
- **LABORATOIRE DE PROTHÈSES NUMÉRIQUES** — Conception et usinage (CFAO, impression 3D)
- **LABORATOIRE D'ORTHÈSE MANDIBULAIRE** — Gouttières, contentions, appareils sur mesure
- **ORGANISME DE FORMATION** — Formations du personnel et des praticiens
- **MÉDECINE DU TRAVAIL** — Suivi médical et prévention en santé au travail
- **EXPERT-COMPTABLE / GESTIONNAIRE PAIE** — Comptabilité, paie, déclarations sociales et fiscales
- **FOURNISSEUR DE CONSOMMABLES** — Matériel dentaire, produits d'hygiène, médicaments
- **SOCIÉTÉ DE NETTOYAGE** — Entretien des locaux et gestion des déchets
- **PRESTATAIRE DE STÉRILISATION** — Contrôle et maintenance des autoclaves et instruments



L'UNIVERS DE SANTÉ NUMÉRIQUE

- **e-PRESCRIPTION** — Logiciels de prescription et plateformes sécurisées
- **AGENCE NUMÉRIQUE EN SANTÉ (ANS)** — Opérateur des services numériques de santé (MSSanté, ApCV, …)
- **RÉPERTOIRES DE PROFESSIONNELS DE SANTÉ (RPPS/FINESS)** — Édition des cartes professionnelles CPS
- **CARTE CPS** (Carte de Professionnel de Santé) — Authentification forte et signature électronique
- **CARTE CPE** (Carte de Personnel d'Établissement) — Pour les salariés des établissements de santé
- **INS** (Identité Nationale de Santé) — Référentiel d'identité partagé pour une meilleure prise en charge

VOS ÉCHANGES AVEC D'AUTRES PROFESSIONNELS DE SANTÉ

- **MÉDECINS TRAITANTS** — Partage d'informations et coordination des soins
- **CORRESPONDANTS SPÉCIALISÉS** — Échanges de comptes rendus et d'imagerie sécurisés
- **PHARMACIENS** — Échanges d'ordonnances, plans de traitement, interactions médicamenteuses
- **HÔPITAUX / CLINIQUES** — Échanges de données, compte rendu, hospitalisation, imagerie
- **IMAGERIE MÉDICALE** — Partage d'images et de comptes rendus sécurisés
- **AUTRES PROFESSIONNELS DE SANTÉ** — Kinésithérapeutes, orthophonistes, infirmiers, sages-femmes, diététiciens, psychologues, etc.
- **STRUCTURES SÉCURISÉES** — EHPAD, centres de soins, services à domicile, à domicile, etc.
- **ET BIEN D'AUTRES…** — Réseau de soins, URPS, ARS, CPAM, mutuelles, etc.

MA CYBERSÉCURITÉ COMMENCE LÀ OÙ COMMENCE CELLE… DE MON ÉQUIPE … DE MES PRESTATAIRES … DE MES OUTILS … DE MES DONNÉES … DE MES PATIENTS = **LA CONFIANCE ET LA CONTINUITÉ DES SOINS**

Ensemble, construisons un environnement numérique de confiance, pour vous, votre équipe et vos patients.

La sécurité n'est pas une option, c'est notre responsabilité à tous.

Cybersécurité : un contexte qui se durcit

Des évolutions réglementaires et opérationnelles qui concernent les cabinets dentaires



1 France : retard sur NIS 2

- La France n'a pas encore **transposé** la directive NIS 2.
- La Commission européenne a saisi la Cour de justice de l'UE et demande des sanctions financières.

2 Des fuites de données de plus en plus fréquentes

- Multiplication des cyberattaques.
- Début 2026 : en moyenne **3 vols de données par jour** au sein des services de l'État.

3 Cabinets dentaires : un impact surtout indirect

- Un cabinet n'est pas automatiquement soumis à NIS 2.
- La directive concerne notamment les **éditeurs, hébergeurs et prestataires numériques** (secteur santé). Leurs nouvelles exigences de sécurité se répercutent sur les cabinets.

4 Le gouvernement hausse le ton

- Plan annoncé le 30 avril 2026 : renforcer la gouvernance numérique de l'État, sécuriser les systèmes d'information et **200 M€ supplémentaires** pour la cybersécurité.
- Dispositif **REACTIV**, piloté par l'ANSSI : capacité renforcée de réaction, d'intervention et d'assistance aux ministères concernés.

5 La CNIL applique des sanctions importantes

- Le RGPD s'applique déjà pleinement.
- Des amendes significatives :
  - **42 M€** à Free / Free Mobile (janvier 2026)
  - **500 000 €** à un hôpital (septembre 2026)
- La CNIL contrôle et sanctionne les manquements à la sécurité des données.

Logiciel métier : points à vérifier

- Hébergement certifié HDS ?
- Certifications de sécurité (ex. ISO 27001) ?
- DPO ou référent RGPD clairement identifié ?

À retenir

NIS 2 arrive, les cyberattaques se multiplient,
le RGPD est déjà appliqué et les contrôles se renforcent.
La sécurisation de votre cabinet et de vos prestataires devient un enjeu concret.

Des données protégées pour des soins en toute confiance.

12 règles ANSSI adaptées à la santé

Priorités essentielles de cybersécurité pour les structures et professionnels de santé

Objectif : protéger la disponibilité, l'intégrité et la confidentialité des données et services de santé.

1 Sauvegardes

Sauvegardes quotidiennes et testées des données critiques (DPI, imagerie médicale).

Solutions certifiées HDS recommandées.

Règle des 3 -2 – 1

2 Mises à jour

Correctifs de sécurité sous 48 h pour les systèmes critiques.

Automatiser les mises à jour lorsque c'est possible.

3 Authentification forte

Double facteur (2FA) pour tous les accès au SI santé.

Utiliser des moyens d'authentification renforcés adaptés au secteur.

4 Gestion des mots de passe

Mots de passe d'au moins 12 caractères ou phrases de passe.

Interdire tout mot de passe par défaut.

Gestionnaire de mot de passe

5 Segmentation du réseau

Isoler les réseaux médicaux des réseaux administratifs.

Utiliser VLAN, cloisonnement et pare-feu internes.

6 Sensibilisation

Former 100 % des professionnels aux risques cyber.

Réaliser des exercices et simulations de phishing ou rançongiciel.

7 Contrôle des accès

Appliquer le principe du moindre privilège.

Gérer les droits par rôles avec des matrices d'accès.

8 Chiffrement

Chiffrement fort des données de santé au repos et en transit.

Utiliser des solutions d'hébergement conformes et sécurisées.

9 Surveillance

Centraliser les journaux et surveiller les événements de sécurité.

Détecter rapidement les comportements anormaux.

journal

10 Réponse aux incidents

Disposer d'un plan de réponse aux cyberattaques, testé chaque année.

Prévoir des scénarios de rançongiciel et de reprise.

registre

https://signalement.social-sante.gouv.fr/

11 Sécurité physique

Restreindre l'accès aux salles serveurs et postes sensibles.

Mettre en place badges et protection des locaux.

Principe de Bureau vide physique ET numérique

12 Sécurité des terminaux

Protéger tous les postes et appareils médicaux connectés.

Déployer antivirus ou EDR sur l'ensemble du parc.

Recommandations transversales

- Tester régulièrement
- Documenter les procédures
- Former les équipes
- Contrôler les accès
- Anticiper les incidents

Référence : bonnes pratiques ANSSI adaptées au secteur santé



IDENTITOVIGILANCE ET AUTHENTIFICATION

Des outils complémentaires pour des soins plus sûrs

La bonne information,
au bon patient,
au bon moment.

1 IDENTIFIER LE PATIENT

Identitovigilance – INS (obligatoire depuis 2021)

ins Identité Nationale de Santé

Bien identifié-e, bien soigné-e

- Une identité unique et pérenne pour chaque patient
- Réduit les erreurs d'identification
- Sécurise le partage des données de santé

Depuis 2021, l'utilisation de l'INS est obligatoire pour référencer le patient dans son parcours de soins.

2 LES PRINCIPAUX DOSSIERS

DUI
Dossier Usager Informatisé
Suivi de l'accompagnement dans le secteur social et médico-social.

DPI
Dossier Patient Informatisé
Dossier de soins tenu par l'établissement ou la structure de santé.

DMP
Dossier Médical Partagé
Dossier numérique intégré à Mon espace santé. Alimenté et consultable selon les règles en vigueur.

Dossier européen de santé (EEDS)
Projet européen pour faciliter l'accès et l'échange des données de santé dans l'UE.

3 S'AUTHENTIFIER EN TANT QUE PROFESSIONNEL

Des accès sécurisés pour protéger les données de santé

PRO SANTÉ CONNECT (PSC)

- Accès sécurisé aux services numériques de santé
- Garantie de l'identité du professionnel de santé

Authentification forte obligatoire dès 2026

- Renforce la sécurité des accès
- Double vérification de l'identité de l'utilisateur

La CPS, notre signature

- Elle authentifie votre identité professionnelle (équivalent d'une signature).
- **Elle ne se prête pas.**
- Il existe des CPE pour nos salarié(e)s (personnels non professionnels de santé).

ASTUCE

L'appli carte Vitale sur smartphone

= INS déjà qualifiée

- Récupération par QR code ou NFC
- Pour le titulaire de l'application, pas besoin de requalifier l'INS via INSi
- Pas besoin de redemander une pièce d'identité

Des outils numériques au service de la qualité des soins

Sécurité des données
Confiance des patients

Une coordination renforcée entre professionnels



Authentification multifacteur (MFA)

Des accès plus sûrs pour protéger vos patients et votre cabinet

Un compte bien protégé,
des données de santé en sécurité.

1 Aujourd'hui



Fin du SMS et des appels vocaux

Ces méthodes ne sont plus suffisantes : trop facilement usurpables (phishing, SIM swap…).

2 Demain



Activation obligatoire de méthodes MFA modernes pour les accès professionnels (Microsoft Entra ID).

3 Attention aux arnaques eSIM



Les cybercriminels peuvent détourner votre numéro de téléphone via une eSIM et recevoir vos codes d'authentification.

Ne comptez plus sur le SMS ou les appels pour vous protéger !

Les méthodes MFA à privilégier

Plusieurs options, à utiliser selon vos accès et vos outils.



Clé de sécurité FIDO2

- Très sécurisée
- Résistante au phishing
- Simple d'utilisation



Application d'authentification

- Codes temporaires
- Fonctionne sans réseau
- Ex. : Microsoft Authenticator, Google Authenticator



Carte professionnelle (CPS)

- Pour certains accès de santé
- Authentification forte
- Usage professionnel



Biométrie

- Empreinte digitale ou reconnaissance faciale
- Simple et rapide
- À utiliser en complément d'une autre méthode

Nos conseils

- Activez dès maintenant une méthode MFA moderne.
- Enregistrez plusieurs méthodes (ex. : clé + appli).
- Vérifiez régulièrement vos informations de récupération.
- Restez vigilant face aux tentatives de phishing.
- Formez toute l'équipe.

À retenir

Un seul compte compromis peut exposer les données de vos patients.

Des accès sécurisés
pour des soins en toute confiance.

La cybersécurité, l'affaire de tous au service de la santé.

PCRA EN CABINET DENTAIRE

Anticiper • Réagir • Continuer à soigner

Un plan simple pour assurer la continuité des soins et protéger les données de vos patients.

Être prêt aujourd'hui
pour continuer à soigner demain.

1 ANTICIPER
Connaître ses risques et se préparer

Identifier les risques
Panne, cyberattaque, vol, sinistre (locaux, matériel), indisponibilité du logiciel.

Protéger l'essentiel
Sauvegardes, accès sécurisés, mises à jour, prestataires fiables.

Définir l'organisation
Qui fait quoi ? Contacts utiles, procédures simples.

Préparer les ressources
Matériel de secours, accès de secours, documents clés (sans données sensibles).

Objectif : limiter l'impact d'un incident.

2 RÉAGIR
En cas d'incident

Détecter et qualifier
Identifier rapidement la nature et la gravité de l'incident.

Activer la procédure
Alerter les personnes concernées (équipe, prestataire, autorités si nécessaire).

Mettre en œuvre les mesures
Isoler, sécuriser, basculer si besoin (mode dégradé).

Communiquer
Informer l'équipe et, si nécessaire, les patients.

Objectif : une réponse rapide et organisée.

3 CONTINUER À SOIGNER
Revenir à la normale

Assurer la continuité des soins
Utiliser les solutions de secours et les procédures prévues.

Restaurer et vérifier
Remettre en service les systèmes et contrôler l'intégrité des données.

Tirer les enseignements
Analyser l'incident et améliorer les procédures.

Objectif : reprendre une activité normale et plus résiliente.

EXEMPLES D'INCIDENTS

- **Cyberattaque** (ransomware, hameçonnage...)
- **Panne informatique ou matérielle**
- **Sinistre dans les locaux** (incendie, dégât des eaux...)
- **Vol ou perte de matériel** (ordinateur, téléphone...)

LES BÉNÉFICES

- **Des soins maintenus pour vos patients**
- **Une équipe sereine et des rôles clairs**
- **Des données protégées et une reprise plus rapide**

Un cabinet préparé est un cabinet qui continue de soigner.

« Anticiper aujourd'hui, c'est protéger vos patients, votre équipe et la pérennité de votre activité. »

webinaire cyber résilience 2026 - Dr SALLIOT Adeline- URPS CD ARA- visuel généré par IA

CYBERSÉCURITÉ – LES 7 OUTILS ESSENTIELS

Pour un cabinet médical sécurisé

Connexion à distance
(Contrôle à distance)



À quoi ça sert ?

- Dépannage / assistance technique
- Collaboration
- Accès ponctuel à un poste

Règles clés

- Sessions ponctuelles
- Permissions limitées
- Vérifier l'identité
- Logs des sessions
- Déconnexion après usage

- Accès permanent
- Partage d'identifiants

Machine virtuelle (VM)
(Environnement isolé)



À quoi ça sert ?

- Tester des logiciels
- Isoler des applications
- Protéger le système principal

Règles clés

- Isoler le réseau (NAT/Host-only)
- Chiffrer les données
- Sauvegardes régulières
- Mises à jour systématiques
- Accès restreint

- Partage de fichiers non contrôlé
- Logiciels non approuvés

VPN
(Tunnel sécurisé)



À quoi ça sert ?

- Accès sécurisé au réseau du cabinet
- Chiffrement des échanges
- Travail à distance sécurisé

Règles clés

- Chiffrement fort (AES-256)
- Authentification 2FA
- Accès limité aux autorisés
- Logs des connexions
- Mises à jour régulières

- VPN grand public pour accès aux dossiers patients
- Identifiants partagés

Pare-feu
(Mur de protection)



À quoi ça sert ?

- Filtrer le trafic réseau
- Bloquer les intrusions
- Limiter les accès

Règles clés

- Bloquer par défaut
- Autoriser uniquement les ports nécessaires
- Segmenter le réseau (VLAN)
- Surveiller les logs
- Mises à jour régulières

- Ouvrir tous les ports
- Ignorer les alertes

Règles de base Cyber
(transversales)



- Utiliser des **mots de passe** forts et uniques
- Activer la **double authentification** (2FA)
- Mettre à jour régulièrement logiciels et systèmes
- **Sauvegarder** selon la règle 3-2-1 (3 copies, 2 supports, 1 hors ligne/cloud)
- **Sensibiliser** le personnel au phishing
- Conformité RGPD / HDS

Objectif unique :

Protéger les données patients et garantir la continuité des soins.

EDR
(Détection & Réponse)



À quoi ça sert ?

- Détecter les menaces avancées
- Surveiller les comportements suspects
- Réagir et contenir rapidement

Règles clés

- Surveillance en temps réel
- Analyse comportementale
- Isolement automatique des menaces
- Mises à jour régulières
- Tableaux de bord et alertes

- Désactiver les alertes
- Ignorer les incidents

Antispam
(Filtrage des emails)



À quoi ça sert ?

- Bloquer les emails indésirables
- Empêcher le phishing et les malwares
- Protéger la messagerie du cabinet

Règles clés

- Filtrage en amont
- Analyse des pièces jointes et liens
- Listes blanches / noires
- Signalement des spams
- Mises à jour régulières

- Ouvrir les pièces jointes inconnues
- Cliquer sur des liens suspects

7 réflexes à retenir

- **Protéger les accès** (moins de privilèges)
- **Mettre à jour régulièrement**
- **Sauvegarder et tester**
- **Surveiller et contrôler**
- **Former et sensibiliser**
- **Détecter et réagir vite**
- **Filtrer et prévenir**

⚠ En cas de doute : **arrêter – vérifier – isoler – contacter** votre prestataire / DPO / support



En cas d'hébergement des données de santé recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi réalisé dans le cadre social et médico-social sur les serveurs d'un tiers (ex. informatique en nuage/cloud), ce dernier devra être certifié hébergeur de données de santé. La prestation réalisée et le contrat conclu devront respecter les obligations imposées à l'article le L. 1111-8 et aux articles R. 1111-8-8 et suivants du code de la santé publique (CSP).

En synthèse, quelles sont les obligations du déployeur ?

- mettre en place une gouvernance adaptée ;
- tenir un registre des traitements en application de l'article 30 du RGPD ;
- réaliser une AIPD en application de l'article 35 du RGPD ;
- réaliser une AIDF, le cas échéant, en application de l'article 27 du RIA ;
- informer les autorités de surveillance en cas d'incidents ou dysfonctionnements.

AIPD: Analyse d Impact Protection des Données.
AIDF : analyse d Impact sur Droits fondamentaux,

Les réflexes à adopter systématiquement :

Il est conseillé **de ne pas contractualiser** avec un fournisseur si :

- la conformité réglementaire pour l'usage prévu ne semble pas assurée ;
- les principes de fonctionnement, d'explicabilité ou d'apprentissage du SIA restent opaques pour l'établissement ou le professionnel utilisateur ;
- il n'existe pas de preuves de validation dans la population d'usage prévu ;
- le circuit des données n'est pas clairement explicité.

SIA: Système d'Intelligence Artificielle

- **Hébergeur de données de santé HDS**
- **Contrôle humain**
- **La norme ISO 27001 est la norme internationale de référence pour la sécurité des systèmes d'information,**
- **Coordonnées du DPO**



L'IA NOUS AIDE AU QUOTIDIEN, MAIS RESTONS MAÎTRES DE NOS DÉCISIONS !

UTILISER L'IA AU CABINET MÉDICAL : SIMPLE, SÛR ET RESPONSABLE !



IA ACT : LES RÈGLES CHANGENT EN 2026

Le règlement européen IA Act est pleinement applicable à partir de 2026. Il impose des règles strictes pour une IA sûre, transparente et respectueuse des droits.

1 CAS CONCRETS : L'IA AU SERVICE DU QUOTIDIEN DU CABINET

LECTURE DES MAILS
- Trier, résumer et prioriser les mails professionnels (compte-rendus, résultats, courriers...).
- Gain de temps et vigilance sur l'important.

RÉDACTION MAILS
- Rédiger des mails professionnels (compte-rendus, résultats, courriers...).
- Gain de temps et qualité des écrits.

SCRIPTS COMPTE RENDU
- Générer un brouillon de compte rendu de consultation à partir de vos notes.
- À relire, vérifier et valider avant signature.

PANIER CONSOMMABLES
- Suggérer les consommables à commander selon votre historique et vos besoins.
- Optimiser les stocks et éviter les ruptures.

LECTURE RADIO
- Aider à la détection d'anomalies sur les examens d'imagerie (radio, scanner, IRM...).
- Toujours confirmer le contexte clinique et votre expertise.

RECHERCHE
- Accélérer la recherche d'articles, données médicales, recommandations ou guidelines.
- Vérifier les sources, la date et la pertinence.

CRÉATION CONTENU
- Créer des supports patients, affiches, posts réseaux sociaux, présentations...
- Adapter, personnaliser et respecter la déontologie.

L'IA est un outil au service des soins et de l'organisation, pas un décideur. Toujours en toute transparence vis-à-vis des patients et de l'équipe.

2 CHARTE IA DU CABINET : 5 ENGAGEMENTS À DÉFINIR COLLECTIVEMENT

1. BON UTILISATEUR POUR BON USAGE
Définir qui utilise quels outils d'IA et pour quels usages adaptés à nos missions et compétences.

2. FINALITÉ CLAIRE ET LÉGITIME
Chaque usage de l'IA répond à un objectif précis, utile au soin, à l'organisation ou à l'amélioration continue.

3. PROTÉGER LES DONNÉES
Garantir la confidentialité et la sécurité des données de santé à chaque étape. Aucun usage n'est légitime sans protection des données.

4. CONTRÔLE HUMAIN À CHAQUE ÉTAPE
L'humain reste responsable : l'IA assiste, mais ne décide pas. Chaque résultat est vérifié, validé et assumé par un professionnel.

5. TOUJOURS EN TOUTE TRANSPARENCE
Informer clairement les patients et l'équipe des usages de l'IA, de ses limites et des résultats proposés.

Ces engagements guident toutes nos pratiques et sont réévalués régulièrement ensemble.

3 CONFORMITÉ LÉGALE : CADRE ET RESPONSABILITÉS

VÉRIFIER LE RESPECT DU RGPD
Assurer la protection des données personnelles des patients.

STOCKAGE AVEC CERTIFICAT HDS
Stocker les données de santé sur des hébergeurs certifiés (HDS).

SIGNER DES CHARTES (DPA SI NÉCESSAIRE)
Signer des chartes conformes. Un DPA (Data Processing Agreement) est requis si nécessaire.

CONSULTER TOUJOURS LES CLAUSES LÉGALES
Consulter systématiquement les clauses légales de l'outil IA utilisé et vérifier les conditions d'utilisation.

S'INFORMER SUR LE FOURNISSEUR
S'assurer de l'existence d'une charte RGPD, d'un DPO ou d'un correspondant dédié et connaître les responsabilités du fournisseur.

4 RÈGLES CYBER À APPLIQUER AVEC L'IA ACT

NE PAS PARTAGER DE DONNÉES SENSIBLES
Aucune donnée de santé nominative ne doit être partagée dans l'outil IA.

NE PAS ENTRAÎNER L'IA
Ne pas autoriser l'utilisation de nos données pour entraîner les modèles d'IA.

USAGE CLOS
Utiliser l'IA dans un cadre clos et maîtrisé : aucune fuite de données en dehors du cabinet.

SUPPRIMER RÉGULIÈREMENT LES HISTORIQUES
Supprimer régulièrement les historiques de conversation et les données temporaires.

ACCÈS SÉCURISÉS
Utiliser des comptes dédiés, des mots de passe robustes et l'authentification à deux facteurs.

SENSIBILISER L'ÉQUIPE
Former et rappeler les bonnes pratiques cyber à toute l'équipe.

RAPPEL : IA ACT – DATES CLÉS
- 2 FÉVRIER 2025 : entrée en vigueur de l'IA Act.
- 2 AOÛT 2026 : application des premières obligations pour la majorité des systèmes d'IA.

AMENDES POSSIBLES
- Jusqu'à 7,5 M€ ou 1 % du chiffre d'affaires mondial pour les violations les plus graves.
- Jusqu'à 15 M€ ou 3 % du chiffre d'affaires mondial en cas de récidive ou de fausse information.

LA SÉCURITÉ DE NOS DONNÉES ET LE RESPECT DU CADRE LÉGAL SONT LA GARANTIE DE LA CONFIANCE DE NOS PATIENTS ET DE LA QUALITÉ DE NOS SOINS.

NOTRE PRIORITÉ : LE BON USAGE AU SERVICE DU SOIN ET DE LA CONFIANCE

Compléments des logiciels métiers

Outils numériques pour le cabinet dentaire

Des solutions européennes et françaises pour travailler en toute confiance

Besoin	Outils courants	Alternatives recommandées	Informations clés
Suite bureautique Présentations, tableurs, documents	PowerPoint, Excel, Word	OnlyOffice ou KSuite	• OnlyOffice : suite bureautique développée en Lettonie, gratuite sur ordinateur • KSuite : suite en ligne d'Infomaniaque, hébergée en Suisse
Messagerie instantanée Équipe, échanges rapides	WhatsApp, Teams, Signal	Olvid	• Messagerie française • Certifiée par l'ANSSI • Recommandée par le gouvernement à ses ministres depuis 2023 • Gratuite • Pas de numéro de téléphone • Pas d'e-mail • Pas d'annuaire central
Envoi de données aux patients Résultats, documents	Gmail	MS Santé	• Gratuite pour tous les professionnels • Messagerie sécurisée dédiée au secteur de la santé
Moteur de recherche Recherche générale	Google Chrome	Qwant	• Moteur de recherche européen • Ne trace pas vos données
Intelligence artificielle générative Rédaction, synthèse, idées	ChatGPT, Claude	Mistral AI	• IA européenne, développée en France • Alternative performante et souveraine
Recherche médicale Littérature scientifique		Vera Health	• Solution développée par deux chercheurs français • Recherches médicales tout en respectant l'anonymisation
Information pour les patients Conseils, informations santé	ChatGPT, Doctissimo	Gustave	• Solution fiable à recommander à vos patients • Informations de santé vérifiées et compréhensibles
Questions juridiques Réglementation, droit de la santé, vie du cabinet		Juribot	• Assistant juridique français • Réponses fiables sur les questions juridiques • Spécialisé en droit français

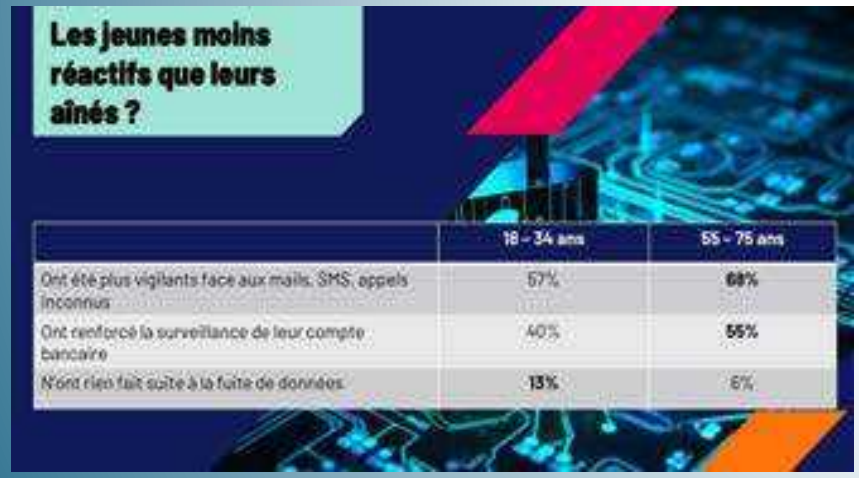
Logos et noms cités à titre d'identification de solutions. Informations issues des sites officiels.



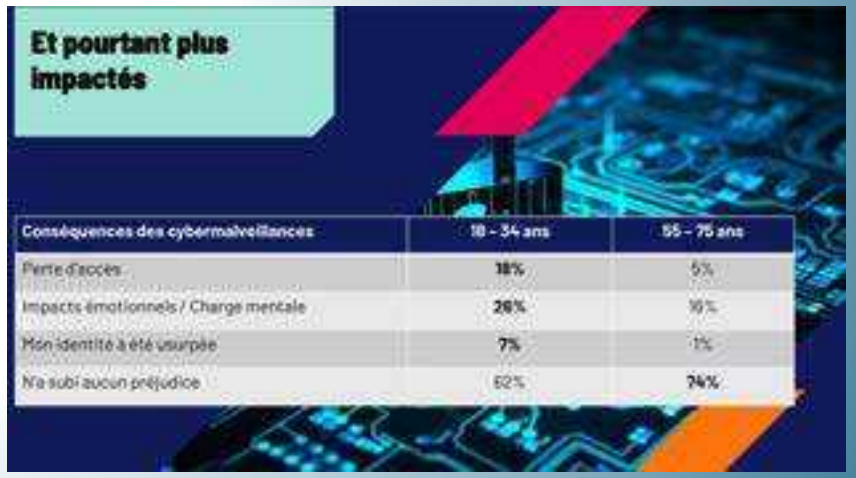




Sensibiliser









CYBER-RÉSILIENCE : SÉPARER VIE PRO & VIE PERSO

Deux mondes différents, les mêmes bonnes pratiques !

VIE PRO

VIE PERSO

OBJECTIF

- Protéger les données professionnelles et personnelles
- Limiter les risques juridiques (RGPD, Code du travail...)
- Éviter les contaminations croisées et les fuites
- Préserver la vie privée et la réputation

1 ÉQUIPEMENTS & TERMINAUX

Idéal : séparer les équipements

- **PRO** — Administré par l'entreprise ; Données pro uniquement
- **PERSO** — Loisirs, achats, réseaux sociaux, photos, documents personnels

Si un seul appareil :

- Comptes utilisateurs distincts (pro/perso)
- Ne jamais mélanger les fichiers
- Pas de clés USB perso pour le travail
- Respecter la politique BYOD de l'entreprise

Mises à jour automatiques | Antivirus & pare-feu actifs | Chiffrement des appareils | Effacement sécurisé avant vente/recyclage

2 RÉSEAUX & CONNEXIONS

Au travail

Appareils perso uniquement sur le réseau invité autorisé

Réseau pro réservé aux usages professionnels

À la maison

- Séparer les réseaux :
  - Travail (sécurisé)
  - Famille / invités
  - Objets connectés (IoT)

Changer le mot de passe du routeur, désactiver le WPS

En déplacement

Éviter le Wi-Fi public pour les activités sensibles

Utiliser un VPN professionnel si nécessaire

Évitez les Wi-Fi publics. Privilégiez le partage de connexion mobile ou le VPN.

3 COMPTES & AUTHENTIFICATION

Boites e-mail distinctes

- PRO — Travail uniquement
- PERSO — Vie privée uniquement
- Ne pas transférer de mails pro vers une boite perso
- Ne pas utiliser la boite pro pour des services personnels

Mots de passe

- Mots de passe uniques et complexes
- Activer la double authentification (2FA)
- Utiliser un gestionnaire de mots de passe

Connexion pro depuis un appareil perso (si nécessaire)

- Navigateur privé / session invitée
- Se déconnecter dès la fin
- Ne pas enregistrer les identifiants
- Effacer l'historique / cache

CLÉS ANTI-DATA : se connecter en toute sécurité

Utilisez une clé anti-data (USB de charge uniquement) pour recharger vos appareils sur des ports publics (bornes, aéroports, cafés...).

Bloque le transfert de données, autorise seulement l'alimentation.

À utiliser pour :

- Charge seulement
- Pas de transfert de données

AU QUOTIDIEN AYEZ LES BONS RÉFLEXES

- Méfiez-vous des e-mails, pièces jointes et liens
- Ne mélangez pas les canaux de communication (pro/perso)
- Ne parlez pas de votre travail sur les réseaux sociaux
- Verrouillez vos profils perso et limitez les informations partagées
- Avant de publier : regardez aussi l'arrière-plan !

4 DONNÉES & STOCKAGE

Stockage

- Données pro : solutions validées par l'entreprise
- Données perso : services personnels

Jamais de données pro sur un cloud perso

Partage

Utiliser les outils professionnels pour partager les fichiers.

Éviter les outils grand public pour les données sensibles

Sauvegardes

Sauvegardes régulières et testées

- Données pro : supports chiffrés et gérés par l'entreprise
- Données perso : disque externe déconnecté

Suppression

Effacer ou réinitialiser les appareils et objets connectés avant de les céder

6 EN ENTREPRISE : RÔLE DE CHACUN

Employeur

- Fournir une charte informatique claire
- Mettre à disposition des outils sécurisés
- Former et sensibiliser les salariés
- Mettre en place des solutions de sécurité (VPN, antivirus, EDR, sauvegardes...)
- Prévoir un réseau invité isolé

Salarié

- Respecter la charte et les règles
- Adopter les bonnes pratiques
- Signaler tout incident ou comportement suspect immédiatement
- Ne pas tenter de résoudre seul un incident

7 VOYAGES & VACANCES

N'emportez que le strict nécessaire | Chiffrer les appareils | Évitez les réseaux inconnus | Attention aux contrôles et aux pertes/vols

La douane peut demander l'accès à vos appareils. N'emportez pas de données sensibles inutiles.

LES 5 RÈGLES D'OR POUR SÉPARER PRO & PERSO

1. SÉPARER LES ÉQUIPEMENTS
2. SÉPARER LES RÉSEAUX
3. SÉPARER LES COMPTES
4. SÉPARER LES DONNÉES
5. SÉPARER LES COMPORTEMENTS

EN CAS D'INCIDENT

1. ARRÊTER l'action suspecte
2. ALERTER IT / RSSI / Manager
3. PRÉSERVER les preuves
4. SUIVRE les consignes

SÉPARER · PROTÉGER · SAUVEGARDER · VÉRIFIER · SIGNALER

Des gestes simples aujourd'hui, une sécurité renforcée demain !



webinaire cyber résilience 2026 - Dr SALLIOT Adeline- URPS CD ARA- visuel généré par IA





webinaire cyber résilience 2026 - dr SALLIOT Adeline- URPS CD ARA- visuel généré par IA



INGÉNIERIE SOCIALE ET CYBERCRIMINALITÉ

Ne vous laissez pas manipuler !

Les cybercriminels exploitent la psychologie humaine pour voler vos informations ou accéder à vos systèmes.

Votre vigilance, c'est votre meilleure protection !

INGÉNIERIE SOCIALE

Technique utilisée par les cybercriminels pour manipuler des individus et leur soutirer des informations sensibles (mots de passe, données bancaires, accès à des systèmes...).
Elle exploite la confiance, la peur, l'urgence ou l'ignorance.

CYBERCRIMINALITÉ

Ensemble d'activités illégales menées via des réseaux informatiques, combinant méthodes techniques (malwares, piratage) et stratégies d'ingénierie sociale.

6 EXEMPLS CONCRETS

1 PHISHING (HAMEÇONNAGE)

Un message (email, SMS...) vous incite à cliquer sur un lien ou à ouvrir une pièce jointe pour voler vos identifiants ou installer un malware.

Ex. : « Votre compte est bloqué. Cliquez ici pour le débloquer. »

2 PRÉTEXTE (PRETEXTING)

Je suis du service IT, j'ai besoin de votre mot de passe pour une maintenance urgente.

Le criminel invente un scénario crédible (faux technicien, faux collègue...) pour obtenir des informations.

Ex. : Demande de mot de passe par téléphone.

3 USURPATION D'IDENTITÉ (CEO FRAUD / BEC)

URGENT

Transférez 50 000 € sur ce compte pour une opération confidentielle. Ne parlez à personne.

Le pirate se fait passer pour un cadre supérieur ou un partenaire et demande un virement ou des données sensibles.

Ex. : Faux email du PDG demandant un virement urgent.

4 ARNAQUE AU SUPPORT TECHNIQUE

Votre PC est infecté ! Appelez le 01 23 45 67 89

Le criminel prétend être du support technique et fait croire à un problème pour obtenir un accès ou un paiement.

Ex. : Pop-up ou appel alarmant pour vous faire paniquer.

5 BAITING (LEURRES)

SALAIRES 2026

Une clé USB ?

Le pirate utilise un appât (clé USB, faux concours...) pour vous inciter à agir.

Ex. : Clé USB abandonnée contenant un malware.

6 QUID PRO QUO

Répondez à ce sondage et recevez un cadeau !

Le criminel propose un service, un gain ou une réduction en échange d'informations ou d'un accès.

Ex. : Sondage, offre promotionnelle ou faux cadeau.

COMMENT S'EN PROTÉGER ?

VÉRIFIER LES SOURCES
Ne cliquez pas sur les liens ou pièces jointes sans vérifier l'expéditeur. Contactez l'organisme par un canal officiel.

NE JAMAIS PARTAGER SES IDENTIFIANTS
Aucune entreprise sérieuse ne demande votre mot de passe par email, SMS ou téléphone.

SENSIBILISER LES ÉQUIPES
Formez vos équipes aux techniques d'ingénierie sociale (simulations de phishing).

UTILISER L'AUTHENTIFICATION MULTIFACTORIELLE (MFA)
Même si un mot de passe est volé, le MFA ajoute une couche de sécurité.

METTRE À JOUR LES SYSTÈMES
Corrigez les failles et maintenez vos logiciels et systèmes à jour.

POURQUOI ÇA MARCHE ?

- **URGENCE** : « Agissez maintenant ! »
- **PEUR** : « Votre compte sera bloqué ! »
- **CURIOSITÉ** : « Découvrez qui a consulté votre profil ! »
- **AUTORITÉ** : « Votre patron vous le demande ! »

?

LA MEILLEURE DÉFENSE, C'EST LA VIGILANCE DE CHACUN !

Restez informé, restez attentif, restez protégé !



Boite à outils
kit de communication





RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR

Cybermalveillance.gouv.fr
Assistance et prévention en cybersécurité





Avec la campagne « Citoyen numérique », les avocats rappellent que vos droits existent, même en ligne.



webinaire cyber résilience 2026 - Dr SALLIOT Adeline- URPS CD ARA- visuel généré par IA

CYBERSÉCURITÉ

LES ASTUCES QUI COMPTENT !

PROTÉGEZ vos accès · RESTEZ vigilant · PROTÉGEZ vos données · RÉAGISSEZ rapidement

ALIAS D'EMAIL

Protégez votre vie privée, évitez le spam !

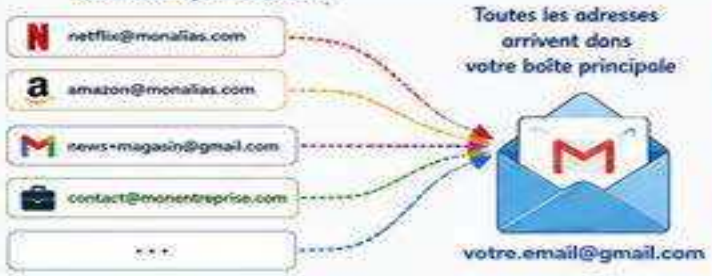
C'EST QUOI ?

Une adresse email secondaire qui redirige automatiquement les messages vers votre boîte principale.

À QUOI ÇA SERT ?

- Protéger votre vie privée
- Éviter le spam
- Organiser vos emails
- Tester des services
- Partager une adresse sans donner votre vrai email

COMMENT ÇA MARCHE ?



COMMENT CRÉER UN ALIAS AVEC GMAIL ?

1 Utiliser le +

votre.email+amazon@gmail.com
votre.email+news@gmail.com

Astuce : créez un filtre dans Gmail pour trier automatiquement.

2 Utiliser les points (.)

votre.email@gmail.com
v.otre.email@gmail.com
vo.tre.email@gmail.com

Gmail ignore les points : toutes ces variantes arrivent dans la même boîte.

OÙ CRÉER DES ALIAS ?

Gmail (+)	Gratuit
ProtonMail	Gratuit (limité) / Illimité
SimpleLogin	Gratuit
Firefox Relay	Gratuit
DuckDuckGo Email Protection	Gratuit
FastMail	Payant
Votre nom de domaine	Payant (via hébergeur)

Moins de spam, plus de sécurité : un alias par service !
Si un alias est compromis, supprimez-le sans changer votre email principal.

INFO PIXEL : DÉSACTIVEZ LE SUIVI

Les pixels (images invisibles 1x1) intégrés dans les emails indiquent à l'expéditeur que vous avez ouvert le message.



COMMENT SE PROTÉGER ?

- Désactivez le chargement automatique des images dans vos emails.
- N'ouvrez pas les emails suspects.
- Supprimez les expéditeurs inconnus.
- Utilisez un filtre anti-spam.

La plupart des services modernes bloquent déjà beaucoup de pixels, mais cette précaution reste utile.

NUMÉROS UTILES POUR SIGNALER

33700	SMS frauduleux (smishing) Envoyez le SMS au 33700 (service gratuit, tous opérateurs).
Signal Spam	Emails frauduleux (spam, phishing) Signalez un email frauduleux sur www.signal-spam.fr
Phishing Initiative	Sites de phishing Signalez un site de phishing pour le faire bloquer : phishing-initiative.fr
PHAROS	Contenus illicites, arnaques, phishing Signalez sur : internet-signalement.gouv.fr
Info Escroqueries	Escroqueries, arnaques (appel gratuit) 0 805 805 817 (Lun-Ven, 9h-18h)

En cas d'urgence : contactez le 17

cyber.gouv.fr

OUTILS UTILES À CONNAÎTRE

Have I Been Pwned	**DeHashed**	**VirusTotal**	**URLScan**	**Firefox Monitor**	**SimpleLogin**	**Firefox Relay**	**DuckDuckGo Email Protection**
Vérifiez si votre email ou mot de passe a été exposé dans une fuite de données.	Découvrez quelles données (email, tel, adresse...) ont été exposées.	Analysez des fichiers ou des liens pour détecter des menaces.	Analysez un site web suspect (capture, comportement, technologies...).	Vérifiez si vos données ont été compromises dans des fuites.	Créez des alias jetables ou permanents pour protéger votre email.	Créez des alias jetables gratuits pour vous inscrire en ligne.	Générez des alias automatiquement et bloquez les traceurs.
haveibeenpwned.com	dehashed.com	virustotal.com	urlscan.io	monitor.firefox.com	simplelogin.io	relay.firefox.com	duckduckgo.com/email

LES BONS RÉFLEXES AU QUOTIDIEN

- Utilisez des mots de passe forts et uniques
- Activez la double authentification (2FA)
- Faites vos mises à jour régulièrement
- Sauvegardez vos données importantes

UN PEU DE VIGILANCE AUJOURD'HUI, BEAUCOUP DE SÉRÉNITÉ DEMAIN ! 😊

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FiligraneFacile

Sécurisez vos documents, luttez contre la fraude

Le service gratuit de l'État pour ajouter un filigrane numérique à vos documents sensibles



Qu'est-ce que FiligraneFacile ?

FiligraneFacile est un service en ligne gratuit proposé par l'État français.

Il permet d'ajouter **un filigrane numérique personnalisé (ou tatouage** numérique) sur vos documents sensibles avant de les transmettre.

Objectif : lutter contre l'utilisation frauduleuse des documents et l'usurpation d'identité.



Comment ça fonctionne ? (exemple)



Document original

Filigrane personnalisé (visible en transparence)

Document filigrané prêt à être transmis

Comment l'utiliser ?

1. Déposez votre document sur la plateforme.
2. Choisissez le texte du filigrane.
   Ex. : « Copie pour [Nom du destinataire] – [Date] ».
3. Appliquez le filigrane et téléchargez votre document sécurisé.





Utilité en cybersécurité

Protection contre la fraude
Le filigrane rend plus difficile la réutilisation malveillante de vos documents, car il atteste de leur propriété ou limite leur usage à un destinataire précis (ex. : nom du destinataire, date d'envoi, raison de l'envoi).

Dissuasion
Même si les filigranes ne sont pas infaillibles (ils peuvent parfois être retirés avec des logiciels ou l'IA), leur présence complique la tâche des fraudeurs et peut en dissuader certains.

Confiance
FiligraneFacile est opéré par un acteur de confiance (l'État) : vos documents ne sont pas exploités à des fins malveillantes pendant le processus.

Acceptation administrative
Les administrations françaises acceptent généralement les documents filigranés, à condition que le filigrane ne rende pas le document illisible ou n'altère pas les dispositifs de sécurité (QR code, 2D-Doc).

Limites
Le filigrane n'est pas une protection absolue : il peut être supprimé par des outils avancés. Mais il reste un levier efficace de prévention et de traçabilité.



Un service public de confiance
FiligraneFacile est développé et hébergé en France par l'État. Vos documents ne sont ni stockés ni partagés au-delà du traitement nécessaire à l'application du filigrane.

Protégez vos documents, protégez votre identité.

Application France identité:

L'utilisateur a la possibilité de produire un justificatif d'identité exploitable par une seule et unique personne/entité/société, avec un motif spécifique (optionnelle) et une durée définie.


RÉPUBLIQUE FRANÇAISE

Justificatif d'identité à usage unique







SENSIBILISATION & APPRENTISSAGE

APPRENDRE EN S'AMUSANT, C'EST RESTER CYBER VIGILANT !

DES OUTILS LUDIQUES POUR ADOPTER LES BONS RÉFLEXES CYBER !

LA CNIL ET CYBERMALVEILLANCE.GOUV.FR PROPOSENT DES JEUX, KITS ET RESSOURCES POUR SENSIBILISER TOUTES LES ÉQUIPES !

CYBERSÉCURITÉ NOTRE AFFAIRE À TOUS !

1. KITS DE JEUX CNIL

DES JEUX POUR COMPRENDRE ET ADOPTER LES BONS RÉFLEXES !

PROTECTION DES DONNÉES (KIT)
Des jeux pour comprendre ce que sont les données personnelles et comment les protéger au quotidien.
cnil.fr/fr/jeux

UN JEU POUR RESTER NET (KIT)
Un jeu pédagogique pour aborder les enjeux du numérique de manière ludique (vie privée, identité numérique, réseaux sociaux...).
cnil.fr/fr/jeux

DIS-MOI DIX MOTS SUR LES DONNÉES (KIT)
Un jeu de cartes pour découvrir et définir 10 notions clés autour des données personnelles.
cnil.fr/fr/jeux

CYBER HÉROS (KIT)
Un serious game pour devenir un héros du numérique et relever des défis en équipe !
cnil.fr/fr/jeux

CYBER ENQUÊTE
Mènes l'enquête pour identifier les risques numériques et trouver les bonnes solutions.
cnil.fr/fr/jeux

ATELIERS & ESCAPE GAMES
Kits d'animation prêts à l'emploi pour organiser des ateliers ou escape games en équipe (supports, scénarios, fiches animateur).
cnil.fr/fr/jeux

À RETENIR !
- Comprendre les enjeux numériques
- Adopter les bons réflexes au quotidien
- Protéger les données et la vie privée
- Être acteur de la sécurité numérique

POSTERS & SUPPORTS PÉDAGOGIQUES
AFFICHER, EXPLIQUER, RAPPELER !



Affiches et supports prêts à l'emploi pour animer vos espaces et rappeler les bons réflexes.

2. RESSOURCES & JEUX SUR CYBERMALVEILLANCE.GOUV.FR

DES OUTILS PRATIQUES ET LUDIQUES TOUTE L'ANNÉE, ET UN RENDEZ-VOUS INCONTOURNABLE : LE CYBERMOIS !

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

JEUX & QUIZ
Quiz, jeux d'énigmes et challenges pour tester ses connaissances et adopter les bons réflexes.

EXERCICES INTERACTIFS
Exercices pratiques pour apprendre à repérer les menaces (phishing, mots de passe, arnaques...).

PARCOURS THÉMATIQUES
Parcours ludiques sur les grands thèmes de la cybersécurité pour tous les niveaux.

CYBERMOIS
LE RENDEZ-VOUS NATIONAL DE LA CYBERSÉCURITÉ — OCTOBRE
Chaque année en octobre : des jeux inédits, des défis, des webinaires et des ressources spéciales pour se mobiliser !

KITS DE SENSIBILISATION
Supports clés en main (affiches, présentations, fiches pratiques...) pour animer vos temps de sensibilisation.

www.cybermalveillance.gouv.fr

RÉFLÉCHIR avant de cliquer · VÉRIFIER avant de partager · PROTÉGER nos données · SIGNALER en cas de doute

DES OUTILS LUDIQUES, DES ÉQUIPES INFORMÉES, UNE ENTREPRISE PLUS SÛRE !

ENSEMBLE, ADOPTONS LES BONS RÉFLEXES ET FAISONS DE LA CYBERSÉCURITÉ UNE FORCE COLLECTIVE !







Épisode 5 Ralala trouver un mot de passe robuste, quel casse tête ! Dans cet épisode,...
13,2K vues · 2 juil. 2024
Facebook · Gendarmerie de la Charente Maritime

webinaire cyber résilience 2026 - Dr SALLIOT Adeline- URPS CD ARA- visuel généré par IA

CYBERRESILIENCE

Les 5 R pour une organisation plus sûre

CYBER MOIS — NOUS SOMMES #CYBER ENGAGÉS — 1er au 31 octobre

urPS CHIRURGIENS DENTISTES AUVERGNE RHÔNE-ALPES

REPÉRER — RÉAGIR — RÉPARER — RÉSILIENCE — RÉFLEXE

1. HIÉRARCHIE DES DROITS

ADMINISTRATEUR
- Contrôle total du système
- Gestion des utilisateurs
- Gestion des droits

GESTIONNAIRE
- Gestion des ressources
- Gestion des membres
- Accès étendus

UTILISATEUR
- Accès aux ressources nécessaires
- Droits limités

INVITÉ
- Accès restreint
- Lecture uniquement
- Aucune modification

MOINS DE DROITS = MOINS DE RISQUES

2. RÉDUIRE LA SURFACE D'ATTAQUE

- Chiffrement
- Séparer l'usage pro et perso
- Installer des filtres de confidentialité sur les écrans visibles du public
- Cartographier le parc informatique pour mieux connaître les actifs et les protéger
- Sensibiliser les équipes
- Supprimer régulièrement les données de navigation et les historiques
- Checker les paramètres de sécurité de ses outils numériques
- Installer VPN et pare feu
- Sécuriser le WiFi
- Emploi sécurisé et raisonné de l'IA : définir des règles claires d'utilisation et d'encadrement

3. SAUVEGARDES ET CLÉS

SAUVEGARDE RÈGLE DES 3-2-1

- 3 copies de vos données
- 2 supports différents
- 1 copie hors site

Disque dur externe — Clé USB — Sauvegarde cloud

CLÉ ANTI-DATA
- Bloque les transferts de données
- Recharge uniquement

CLÉ SÉCURITÉ
- Authentification 2FA
- Connexion sécurisée

4. SOUVERAINETÉ NUMÉRIQUE

Utiliser en priorité des solutions conformes aux recommandations et à l'ANSSI et de la CNIL, hébergées en France.

Mots de passe
Utiliser un gestionnaire de mots de passe sécurisé et souverain.

Messagerie sécurisée
Privilégier une messagerie sécurisée et souveraine pour toutes les communications sensibles.

Hébergement souverain
Héberger les données en France en priorité sur des serveurs français reconnus pour leur fiabilité et leur conformité.

EXEMPLES DE SOLUTIONS SOUVERAINES

KoriBus	Olvid	OVHcloud
Gestionnaire de mots de passe	Messagerie sécurisée	Hébergement cloud français

5. LES BONS RÉFLEXES

- Alerter immédiatement le support informatique
- Ne pas éteindre ou redémarrer avant expertise du support informatique.
- Isoler les appareils touchés : couper Internet, Wi-Fi et réseau
- Conserver les preuves : mails, captures, journaux
- Noter les événements et les actions réalisées
- Activer les solutions de secours / PCA-PRA
- Contacter assureur, banque si besoin, puis déposer plainte
- CNIL : notifier sous 72 h si des données personnelles sont concernées
- En cas de fuite avérée
  Informer les personnes concernées au plus tôt si le risque est élevé (arnaque, fraude, vol d'identité…), avec des infos claires, vérifiées.

5 POINTS CLÉS POUR SIGNALER UN ÉVÉNEMENT CYBER ET OBTENIR DE L'AIDE EN FRANCE

CYBERMALVEILLANCE.GOUV.FR
Plateforme officielle pour signaler une cyberattaque (rançongiciel, piratage, etc.) et recevoir des conseils, envoyer à tous particuliers, entreprises, collectivités)
www.cybermalveillance.gouv.fr

17CYBER
Outil de diagnostic en ligne, soutenu par la Police et la Gendarmerie, pour identifier le type d'attaque et accéder à des recommandations.
17cyber.gouv.fr

CERT-FR (ANSSI)
Pour les entreprises et administrations, afin de déclarer un incident ou une vulnérabilité (logiciel, attaque, etc.).
cert.ssi.gouv.fr OU cert-fr@ssi.gouv.fr

CERT Santé
Spécifique au secteur santé (hôpitaux, EHPAD, etc.) avec un numéro d'urgence 24/7.
+ 33 (0)9 72 43 91 25
certsante@esante.gouv.fr

THESEE
Plateforme nationale de signalement des contenus illicites en ligne (escroqueries, phishing, arnaques, etc.)
www.thesee.gouv.fr

SIGNALEMENT SANTÉ
Pour déclarer un cyberincident en tant que professionnel de santé, utiliser le portail officiel de signalement des événements sanitaires indésirables.
Choisir l'espace "professionnels de santé" puis "Cybersécurité / Incident de sécurité des systèmes d'information".
signalement.social-sante.gouv.fr

EN CAS DE DOUTE, ISOLEZ L'APPAREIL ET CONTACTEZ : 04 72 40 56 56

NUMÉRO D'URGENCE : CYBER ASSISTANCE AUVERGNE-RHÔNE-ALPES
Assistance téléphonique gratuite 24h/24 et 7j/7 pour les entreprises et associations de la région victimes d'une cyberattaque.

CYBER MOIS