L'OCTET

Édition
Octobre 2026

Le droit et le numérique décodés.

22

À LA UNE

IA pour tous, tous pour IA ?

LE DÉCRYPTAGE

Cybermois : la sensibilisation face aux menaces numériques

Retrouvez d'autres éditions sur notre site web.

IA pour tous, tous pour IA ?

Il y a encore peu, l'intelligence artificielle était une technologie que l'on observait à distance, réservée à certains secteurs, certains métiers ou quelques usages spécialisés. Ce temps paraît déjà loin. En 2025, 48 % de la population utilisaient l'IA générative, contre seulement 20 % deux ans auparavant. Chez les 18-24 ans, cette proportion atteint même 85 %. Et le phénomène ne s'arrête pas aux usages personnels : en 2026, quatre TPE-PME françaises sur dix déclarent déjà utiliser au moins une solution d'intelligence artificielle. L'IA devient accessible à tous. Mais, à mesure qu'elle se démocratise, une autre question apparaît : allons-nous vers une « IA pour tous » ou vers un monde où chacun serait, d'une certaine manière, sommé de se rallier au « tous pour l'IA » ?

L'accès généralisé à ces technologies constitue évidemment une formidable opportunité. L'IA peut faciliter certaines tâches, améliorer l'accès à l'information, assister la création, automatiser des opérations répétitives ou encore accompagner la prise de décision. Elle permet à des structures modestes d'accéder à des capacités autrefois réservées à de grandes organisations. À ce titre, l'enjeu de démocratisation est réel : chacun doit pouvoir comprendre ces outils, les expérimenter et, lorsqu'ils répondent à un besoin, en tirer parti.
Mais la démocratisation ne doit pas se transformer en injonction. Utiliser l'IA parce qu'elle améliore effectivement un service est une chose ; l'intégrer simplement parce qu'elle est disponible, parce qu'elle est devenue un argument commercial ou parce que « tout le monde le fait » en est une autre. L'apparition systématique de fonctionnalités d'IA dans les outils du quotidien pose ainsi une question plus profonde : conservons-nous réellement la liberté de choisir quand nous souhaitons l'utiliser, pour quelle finalité et avec quelles données ?

Cette question dépasse d'ailleurs le seul utilisateur. Derrière chaque usage se trouvent des choix de conception, des traitements de données, des infrastructures, des coûts environnementaux, des risques de sécurité et parfois des décisions susceptibles d'affecter directement des personnes. Généraliser l'IA suppose donc aussi de généraliser une culture de son usage : savoir ce qu'elle fait, connaître ses limites, vérifier ses résultats et déterminer les situations dans lesquelles une intervention humaine demeure nécessaire. L'enjeu n'est plus seulement d'apprendre à se servir de l'IA, mais aussi d'apprendre à ne pas lui confier ce qu'elle ne devrait pas décider à notre place.

« IA pour tous » ne devrait donc pas signifier « IA partout ». Le progrès ne se mesure pas au nombre de fonctionnalités intégrant une intelligence artificielle, mais à notre capacité à employer cette technologie lorsqu'elle apporte une réelle valeur, tout en conservant la maîtrise de nos choix. Peut-être est-ce là le véritable défi des prochaines années : faire de l'intelligence artificielle un outil accessible à tous, sans faire de son utilisation une évidence imposée à chacun.

Hébert-Marc GUSTAVE
Avocat au Barreau de Paris
Fondateur de LOCK-T

CYBERMOIS : LA SENSIBILISATION FACE AUX MENACES NUMÉRIQUES

Chaque année en octobre, le mois européen de la cybersécurité, ou Cybermois en France, vise à sensibiliser aux risques numériques et aux moyens de s'en protéger. À cette occasion, la Commission nationale de l'informatique et des libertés (ci-après la « Cnil ») rappelle notamment l'importance de prévenir les violations de données personnelles et de savoir réagir lorsqu'elles surviennent. Cette initiative contribue ainsi à faire de la cybersécurité un enjeu collectif, en encourageant l'adoption de bonnes pratiques face aux menaces numériques.

Mais qu'est-ce que la cybersécurité ? C'est l'ensemble des mesures destinées à protéger les systèmes informatiques, les réseaux et les données contre les attaques, les accès non autorisés ou les altérations. Aujourd'hui, elle concerne chacun d'entre nous, tant les outils numériques occupent une place centrale dans notre quotidien. Hameçonnage, piratage, fuites de données ou encore deepfakes : les cybermenaces peuvent entraîner des pertes financières, des atteintes à la vie privée et des conséquences importantes pour les entreprises. La prévention repose notamment sur des réflexes simples, comme la vérification des messages reçus, l'utilisation de mots de passe robustes et la mise à jour régulière des logiciels. Par ailleurs, Cybermalveillance.gouv.fr accompagne les victimes d'actes de cybermalveillance en leur proposant une assistance adaptée, tout en informant le public sur les différentes menaces et les moyens de s'en protéger.

Dans ce contexte, LOCK-T participe à la sensibilisation aux risques numériques à travers une série de vidéos consacrées au Cybermois. Ces formats courts, diffusés sur nos réseaux sociaux Instagram, LinkedIn et TikTok, présentent différentes formes de cybermalveillance, leurs mécanismes et les moyens de s'en protéger. L'objectif : rendre ces enjeux accessibles et transmettre des conseils concrets pour adopter les bons réflexes.

Toutefois, l'actualité du mois d'octobre rappelle que la sensibilisation, aussi essentielle soit-elle, ne suffit pas à faire disparaître les risques. Ce mois a notamment été marqué par une cyberattaque visant les systèmes de réfrigération de plusieurs centaines de supermarchés français, ainsi que par la découverte de deux vulnérabilités critiques affectant PHP, un langage largement utilisé pour le développement web. Ces événements rappellent que la prévention doit s'accompagner de mesures techniques et organisationnelles adaptées.

Le Cybermois est donc l'occasion d'informer et de prévenir : la cybersécurité exige une vigilance permanente, associant sensibilisation des utilisateurs, mesures de protection adaptées et anticipation des incidents. Comprendre les menaces est une première étape ; savoir les prévenir et y répondre constitue une nécessité durable.

Ce qu'il ne fallait pas louper

CYBERATTAQUE DES SUPERMARCHÉS : LES FRIGOS PRIS POUR CIBLE

Dans la nuit du 11 au 12 octobre 2026, plusieurs enseignes de la grande distribution française ont été touchées par une cyberattaque visant leurs installations frigorifiques. Des attaquants ont pris le contrôle à distance de systèmes de régulation, notamment de marque Danfoss, et modifié certains paramètres de fonctionnement, provoquant une hausse anormale des températures. Environ 700 sites auraient été concernés selon le Gouvernement. Plusieurs magasins ont ainsi dû retirer et détruire des denrées dont la chaîne du froid ne pouvait plus être garantie. Cet incident illustre la dépendance croissante des activités économiques aux systèmes numériques : une compromission informatique peut désormais avoir des effets immédiats sur des équipements physiques, les marchandises et la continuité d'activité.

Comment une telle attaque a-t-elle été possible ? Le 12 octobre, le CERT-FR, centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, a publié le bulletin CERTFR-2026-ALE-012 après avoir constaté de nombreuses compromissions de contrôleurs à distance d'installations de réfrigération. Plusieurs équipements Danfoss, puis Copeland et Dixell, étaient concernés. Si le mode opératoire précis de l'attaque n'est pas encore publiquement établi, le CERT-FR souligne que l'exposition directe d'une interface de gestion sur Internet est contraire aux bonnes pratiques. Il recommande notamment de supprimer ces accès directs et de ne les rétablir qu'au moyen d'un VPN sécurisé ou d'un réseau protégé.

Les conséquences sont à la fois économiques et sanitaires. Dès lors que la température de conservation n'est plus garantie, le respect de la chaîne du froid peut imposer la destruction des produits concernés afin d'écarter tout risque pour les consommateurs. À ces pertes de marchandises s'ajoutent les interventions techniques, la remise en état des installations et les difficultés de réapprovisionnement. L'incident pose également la question du partage des responsabilités entre exploitants, fabricants et prestataires chargés de l'installation ou de la maintenance des équipements. Une enquête a été ouverte, mais l'identité des auteurs et leurs motivations ne sont, à ce stade, pas publiquement établies.

Cette attaque met surtout en lumière une vulnérabilité parfois sous-estimée : celle des équipements connectés qui pilotent le fonctionnement physique des bâtiments. Réfrigération, chauffage, climatisation ou contrôle d'accès reposent désormais largement sur des systèmes administrables à distance. Leur cybersécurité ne peut donc plus être considérée comme secondaire par rapport à celle des réseaux informatiques traditionnels. L'incident rappelle ainsi qu'une simple prise de contrôle à distance peut entraîner des conséquences très concrètes sur la continuité d'activité d'une entreprise et, ici, sur l'ensemble de la chaîne d'approvisionnement alimentaire.

Ce qu'il ne fallait pas louper

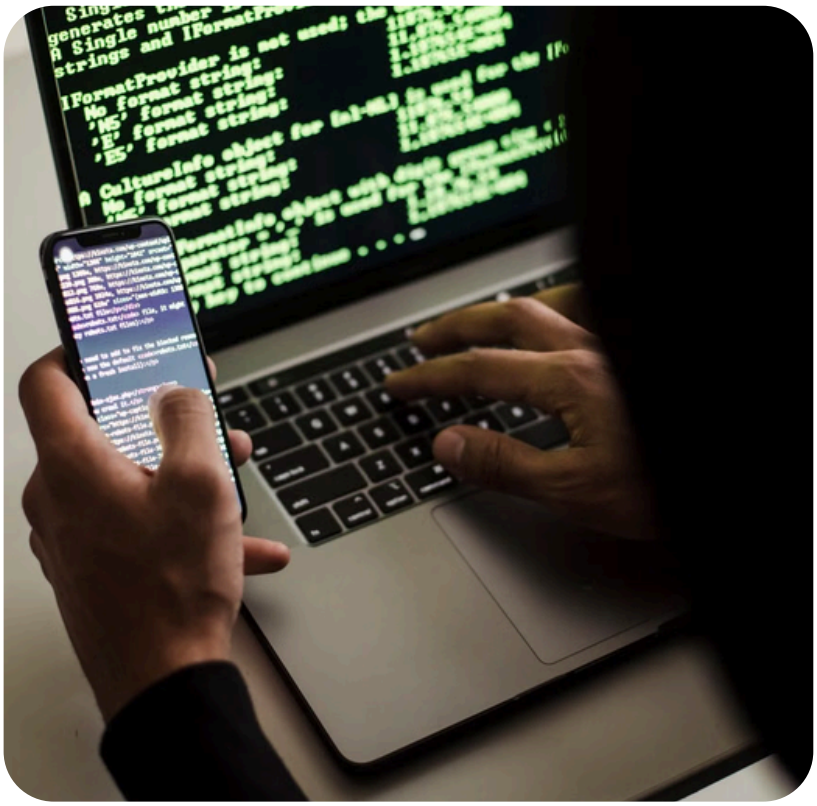
SÉCURITÉ WEB : DEUX FAILLES CRITIQUES DANS PHP

Le 21 octobre 2026, deux failles de sécurité critiques affectant PHP, langage utilisé par une grande partie des sites et applications web, ont conduit à une importante mobilisation des acteurs de la cybersécurité. Référencées sous les identifiants CVE-2026-109618 et CVE-2026-109619 et évaluées à un niveau de criticité très élevé, ces vulnérabilités peuvent, dans certaines configurations, permettre à un attaquant non authentifié d'exécuter du code à distance sur un serveur vulnérable. Des correctifs ont été publiés le jour même par PHP.

En France, la réaction a été immédiate. À la demande de l'Agence nationale de la sécurité des systèmes d'information (ci-après « l'ANSSI »), plusieurs sites publics exposés à ces vulnérabilités ont été temporairement placés en maintenance afin de permettre l'application des correctifs. Les sites des préfectures ont notamment été rendus indisponibles par mesure de précaution. Il ne s'agissait donc pas d'une cyberattaque contre ces services, mais d'une mesure préventive face à une vulnérabilité susceptible d'être rapidement exploitée.

Le 22 octobre, Cybermalveillance.gouv.fr a également publié une AlerteCyber invitant les professionnels et les organisations concernés à mettre à jour sans délai leurs installations PHP. Une exploitation réussie peut notamment permettre une prise de contrôle à distance, provoquer une interruption de service ou permettre l'accès à des données. L'alerte est d'autant plus importante que les anciennes versions de PHP qui ne sont plus maintenues ne bénéficient plus de correctifs de sécurité : leur migration vers une version toujours supportée devient donc indispensable.

L'urgence n'était d'ailleurs pas seulement théorique : des tentatives d'exploitation ont été observées avant même la publication officielle des correctifs. Cet épisode rappelle ainsi les effets que peut produire une vulnérabilité affectant un composant aussi largement utilisé du web. Pour les entreprises comme pour les administrations, la mise à jour des logiciels, la surveillance des vulnérabilités et l'abandon des versions qui ne sont plus maintenues demeurent donc des mesures essentielles de cybersécurité.



NOTION CLÉ : LE PHP

PHP, pour « PHP : Hypertext Preprocessor », est un langage de programmation libre et open source principalement utilisé pour le développement web. Il s'exécute généralement côté serveur : il permet notamment de générer dynamiquement des pages web avant de transmettre le résultat au navigateur de l'utilisateur.

Concrètement, PHP peut traiter des informations reçues par un site, interagir avec une base de données, gérer des comptes utilisateurs ou des sessions et produire du contenu en fonction des données disponibles. Il constitue ainsi l'une des technologies utilisées pour faire fonctionner des sites et applications web dynamiques.

Son rôle peut également entraîner des conséquences directes en matière de sécurité et de protection des données. Selon l'architecture du service, le code exécuté côté serveur peut notamment participer à la gestion des droits d'accès, à la sécurisation des données, à leur conservation ou encore au respect de certaines règles relatives aux données personnelles. Une vulnérabilité affectant PHP peut donc entraîner des conséquences bien au-delà du seul fonctionnement technique d'un site.



Ce qu'il faut connaître

BONNES PRATIQUES:

L'utilisation des outils numériques ne cesse de se développer et de se diversifier : ordinateurs, téléphones, montres connectées, objets connectés, etc. Cette présence croissante du numérique dans notre quotidien multiplie également les points d'entrée potentiels pour les cybercriminels.

Voici 10 pratiques essentielles de cybersécurité à appliquer aussi bien dans le cadre professionnel que personnel.

1. Protéger l'accès aves des mots de passe robustes ;
2. Sauvegardez vos données régulièrement ;
3. Appliquez les mises à jour de sécurité sur tous les appareils, dès qu'elles vous sont proposées ;
4. Utilisez des antivirus ;
5. Téléchargez vos applications uniquement sur les sites officiels ;
6. Méfiez-vous des messages inattendus ;
7. Vérifiez les sites sur lesquels vous faites des achats ;
8. Maîtrisez vos réseaux sociaux ;
9. Séparez vos usages personnels et professionnels ;
10. Évitez les réseaux Wi-Fi publics ou inconnus.



CHIFFRES CLÉS

700

C'est le nombre approximatif de supermarchés français touchés par la cyberattaque ayant visé leurs systèmes de réfrigération dans la nuit du 11 au 12 octobre 2026, sur environ 10 000 magasins à l'échelle nationale.

Une entreprise découvre qu'un équipement connecté utilisé dans ses locaux est directement accessible depuis Internet. Quelle mesure constitue la réaction la plus appropriée ?

1. Modifier uniquement le nom d'utilisateur administrateur
2. Masquer l'adresse IP de l'équipement sur le site de l'entreprise
3. Supprimer l'exposition directe à Internet et sécuriser l'accès, notamment via un VPN ou un réseau protégé
4. Conserver l'accès public mais augmenter la fréquence des sauvegardes

Réponse du mois de septembre 2026

Savez-vous quelle thématique sera mise à l'honneur au mois d'octobre ?

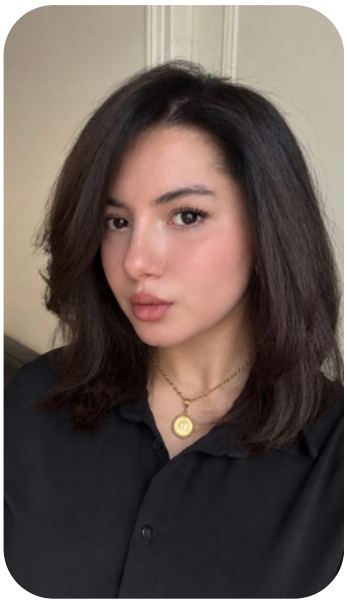
1. Le mois de la propriété intellectuelle
2. Le mois du numérique
3. Le mois de l'IA
4. Le mois de la cybersécurité

Réponse 4

ACTU

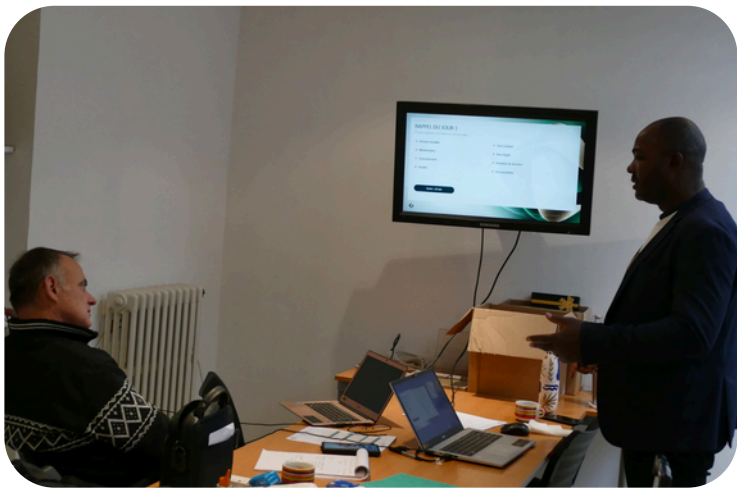
Bienvenue à Asseline !

Nous accueillons Asseline Nessiri, étudiante en troisième année de Licence de droit à Paris-Panthéon-Assas, pour un stage de deux mois. Intéressée par le droit du numérique et la propriété intellectuelle, elle contribuera notamment à notre veille juridique, nos livrables et nos contenus.



Une première pour LOCK-T Académie

LOCK-T a officiellement réalisé sa première formation professionnelle en tant qu'organisme de formation ! Consacrée à la conformité RGPD appliquée au métier commercial, cette formation de 14 heures sur deux jours marque une nouvelle étape dans le développement de LOCK-T Académie.





LOCK-T soutient CAP CYBER

LOCK-T soutient CAP CYBER, une initiative permettant aux entreprises et collectivités de bénéficier gratuitement d'un premier diagnostic de cybersécurité réalisé par des étudiants de l'IUT de La Rochelle, encadrés par des professionnels. Une belle démarche pour sensibiliser les organisations tout en formant les talents de demain !

Rendez-vous au Salon INNN

Les 4 et 5 novembre, retrouvez LOCK-T au Salon INNN à Niort, stand E31 ! Deux journées pour rencontrer notre équipe, découvrir nos nouveautés et échanger autour de vos enjeux numériques. Nous vous attendons nombreux !

LOCK-T arrive sur TikTok

LOCK-T est désormais sur TikTok ! Nous y partagerons des vidéos courtes et pédagogiques autour du RGPD, de la cybersécurité, de l'IA et plus largement des enjeux du numérique. Rejoignez-nous et abonnez-vous !

LOCK-T dévoile sa nouvelle identité

Nous avons grandi, notre identité aussi ! LOCK-T évolue pour mieux refléter l'ensemble de ses expertises, désormais organisées autour de cinq univers : Conseil & DPO, Avocat, Académie, Digital et LOCK-thèque. Une nouvelle identité, avec toujours le même engagement à vos côtés.

LOCK-T



Et votre environnement numérique est maîtrisé

+33(0)6 41 10 99 33

contact@lock-t.com

www.lock-t.com