LA LETTRE DU CYBER CONSEILLER

n° 22606 NOVEMBRE et DÉCEMBRE 2026 19e année





Au sommaire : *En 2027, ça va bouger grave - En 2027, autre chose ? - Allez, on se détend avec les ordinateurs - Nouveau décodeur TV d'Orange - Fin du support OFFICE 2021 - ANDROID : lutter contre les SMS frauduleux - L'espionnage via les voitures électriques et connectées.*

EN 2027, ÇA VA BOUGER GRAVE !

Ce dimanche 25 octobre, à 3h du matin, il sera de nouveau 2h : la France repasse à l'heure d'hiver, et les logs horodatés en heure locale vont voir passer deux fois 2h30.
Ce casse-tête-là n'a toujours pas de date de fin, mais les développeurs vont bientôt pouvoir rayer un autre cas limite de leur liste.
Réunie mi-octobre à Versailles, la Conférence générale des poids et mesures (les gardiens officiels du mètre, du kilo et de la seconde, ça plaisante pas 😤) a adopté une résolution qui acte la fin des secondes intercalaires.
En conséquence, à partir du 20 mai 2027, l'heure de référence mondiale (UTC) deviendra continue : plus aucune seconde ne lui sera ajoutée ni retirée pour la garder calée sur la rotation de la Terre.

Minute, papillon

L'UTC, l'heure sur laquelle vos serveurs se synchronisent, est calculée à partir d'horloges atomiques d'une régularité quasi parfaite. La Terre, elle, tourne de façon bien moins régulière, et les deux finissent par diverger au fil des années.
Pour garder l'écart sous la seconde, on ajoute donc depuis 1972 une seconde de temps en temps, à la fin d'un 30 juin ou d'un 31 décembre. La dernière minute de la journée compte alors 61 secondes et l'horloge affiche 23:59:60 avant de passer à minuit.
Ce genre de détail, le logiciel le digère très mal.
Le temps Unix, par exemple, part du principe qu'une journée dure toujours 86.400 secondes : sur beaucoup de machines, l'horloge système revient alors une seconde en arrière pour caser l'intruse.

Retour vers le passé

UTC a encaissé 27 secondes intercalaires depuis sa création, et la dernière, ajoutée fin 2016, a pourri le réveillon du réseau internet Cloudflare, le plus important du monde. Le 1er janvier 2017 à minuit pile (heure UTC), son service DNS, écrit en langage Go, s'est mis à mesurer des durées négatives. Il a fini par en refiler à une fonction de tirage aléatoire, qui bugue dès qu'on lui passe un nombre négatif.
Une partie des résolutions DNS de ses clients a échoué, et son post-mortem résume la cause profonde du bug en une phrase : avoir cru que le temps ne pouvait pas reculer.
Doc Brown de Retour vers le futur, lunettes de soudeur sur le nez, tenant deux pinces crocodiles et portant deux montres.

Certains ont préféré ruser : Google étale la seconde en trop sur une vingtaine d'heures, en rallongeant chaque seconde de la période d'un peu plus de dix microsecondes. L'horloge n'affiche ainsi jamais de 23:59:60 et ne recule jamais.

➤➤

Sauf que chacun étale à sa façon, et la résolution pointe les limites de ces bricolages : pendant l'opération, deux horloges peuvent afficher des heures différentes, et une seconde n'y dure plus tout à fait une seconde.

C'était moins une

Jusqu'à la fin des années 2010, la Terre tournait un poil trop lentement et on ajoutait des secondes. Mais depuis 2020, elle tourne un poil trop vite.
Depuis 2020, les journées raccourcissent.
Au point que des spécialistes de la rotation terrestre évaluent à 30 % le risque d'une seconde intercalaire négative d'ici 2035. Il faudrait alors retirer une seconde : l'horloge sauterait directement de 23:59:58 à minuit.
Aucun système n'a encore eu à traiter ce cas de figure grandeur nature. Selon la résolution, s'y préparer pourrait coûter cher aux industries qui dépendent d'une heure précise.
La résolution redoute aussi que, si la réforme tardait à se mettre en place, certaines organisations lâchent UTC comme heure de référence au profit de celle d'un système de navigation par satellite, comme le GPS.
La même conférence avait déjà voté en 2022 la fin des secondes intercalaires, au plus tard pour 2035.
Ce sera finalement le 20 mai 2027, Journée mondiale de la métrologie, la science de la mesure (rien à voir avec la météo). Eh ouais, les métrologues ont le sens de la fête.

On a tout le temps

Pour justifier qu'on laisse l'heure officielle s'éloigner du soleil, la résolution sort un argument imparable : à cause du découpage des fuseaux horaires, l'heure légale de nombreux pays s'écarte déjà de plus d'une heure du temps solaire.
C'est d'ailleurs le cas de la France : le méridien de Greenwich la traverse (elle devrait donc être sur le même fuseau que Londres), mais elle vit à l'heure de Berlin. À Brest, l'heure d'hiver a déjà plus d'une heure d'avance sur le soleil.
Le passage à l'heure d'hiver nous rapprochera bien du soleil le dimanche 25/10, mais seulement jusqu'au printemps : à l'heure d'été (cette grande pourvoyeuse de bugs), Brest a plus de deux heures d'avance sur lui. Alors on n'est plus à quelques secondes près, hein.
Jusqu'ici, l'écart toléré entre UTC et la rotation de la Terre était inférieur à une seconde. La résolution le porte à une heure, de quoi tenir plusieurs siècles. Ce qu'on fera le jour où cette limite sera atteinte, le texte ne le dit pas.
Ce sera le problème de développeurs qui ne sont pas encore nés (ou des IA qui nous auront tous remplacés d'ici là). Pas mal la feinte pour repousser le problème.

source : la Convention du Mètre

EN 2027, AUTRE CHOSE ?

En marge de cette réforme du temps mondial, l'année 2027 sera marquée par deux autres transitions technologiques d'envergure :

1\. L'expiration des certificats Windows Update :

Une première échéance fixée au 17 mai 2027 va bloquer les mises à jour automatiques de certains serveurs et PC Windows plus anciens qui n'auront pas migré leurs protocoles de sécurité à temps.

2\. L'IA obligatoire à l'école :

En France, la rentrée scolaire de septembre 2027 concrétise un virage numérique majeur avec l'introduction d'une heure d'enseignement hebdomadaire dédiée à l'intelligence artificielle pour tous les élèves de seconde.

L'expiration des certificats de sécurité de Windows Update en 2027 est un sujet technique crucial. Si une machine n'est pas à jour à cette échéance, elle perdra définitivement tout accès automatique à Windows Update, devenant incapable de télécharger le moindre correctif de sécurité ou même les définitions de Microsoft Defender.
Voici le détail complet des systèmes concernés, des dates limites et de la solution.

Les deux vagues d'expiration en 2027

Microsoft procède à une rotation majeure de ses certificats numériques. Selon la version du système d'exploitation, l'accès aux serveurs sera coupé à l'une de ces deux dates si le correctif minimal n'est pas présent :

-Windows Server 2019 Mise à jour de sécurité de juillet 2026 (ou ultérieure) 17 mai 2027
-Windows Server 2022 Mise à jour de sécurité de juillet 2026 (ou ultérieure) 19 juin 2027
-Windows Server 2025 Mise à jour de sécurité de septembre 2025 (ou ultérieure) 19 juin 2027
-Windows 10 Grand Public (sous abonnement ESU) Patchs ESU de juillet 2026 (ou ultérieurs) 19 juin 2027

Note : Les futures versions (comme Windows 11 25H2 ou supérieures) intègrent déjà nativement les nouveaux certificats et ne nécessitent aucune action particulière.

Qui est réellement en danger ?

Dans la pratique, cette situation concerne principalement deux profils :
1\. Les ordinateurs des particuliers ou d'entreprises "figés" : Les machines déconnectées d'Internet ou sur lesquelles les mises à jour automatiques ont été volontairement bloquées ou suspendues depuis 2025 ou 2026.
2\. Les infrastructures d'entreprise mal synchronisées : Si un serveur WSUS (Windows Server Update Services) local distribue les mises à jour sans être lui-même mis à jour, les postes clients finiront par être bloqués. Si votre système effectue ses mises à jour mensuelles (les fameux Patch Tuesdays) de manière totalement classique et régulière, les nouveaux certificats s'installeront bien avant les échéances de 2027.

Que faire si un PC se retrouve bloqué

Si une machine rate le coche et dépasse la date limite sans avoir reçu son correctif, Windows Update affichera une erreur de connexion en boucle (le PC ne pourra plus valider l'authenticité des serveurs Microsoft). La solution consistera à effectuer une mise à jour manuelle hors-ligne :
1\. Télécharger le correctif requis (le package .msu cumulatif de juillet 2026 ou ultérieur) depuis un autre ordinateur connecté sur le Catalogue Microsoft Update.
2\. Transférer le fichier sur la machine bloquée via une clé USB.
3\. Installer le patch manuellement et redémarrer le système pour injecter les nouveaux certificats valides.

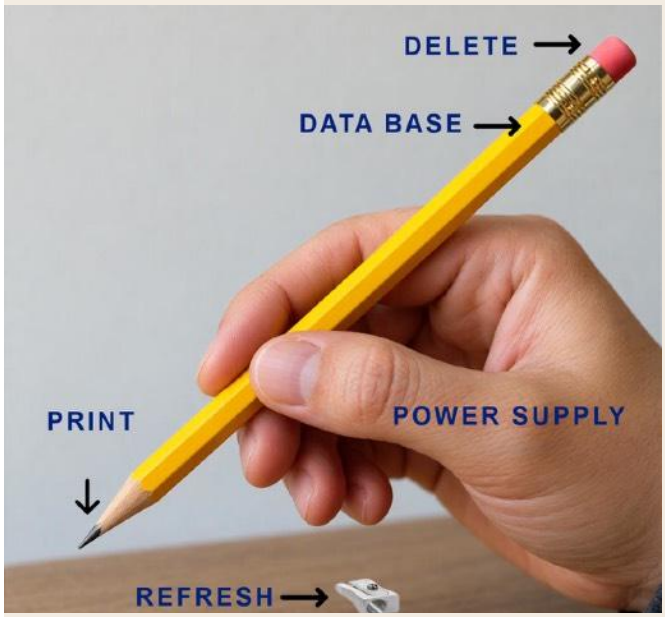
source : Microsoft

ALLEZ, ON SE DÉTEND AVEC LES ORDINATEURS

Le **tout premier ordinateur** date du Paradis Perdu d'ADAM et ÈVE ? si, si …Il possédait un seul octet. C'était une pomme (Apple) … Ils l'ont branché et ça s'est très mal passé !



Mon **premier ordinateur familial**



Le **DIGI-COMP 1,** L'ordinateur sans électricité



DIGI-COMP 1 est un ordinateur mécanique numérique à 3 bits conçu pour enseigner les bases de l'informatique binaire via des leviers et des élastiques.

Fonctionnement mécanique :
Il utilise des leviers et des élastiques pour effectuer des opérations binaires, fonctionnant à une vitesse d'environ 1 Hz.

Kit à monter soi-même :
Il était vendu sous forme de kit à assembler, permettant aux utilisateurs de comprendre son fonctionnement interne. « J'ai eu le premier ordinateur personnel numérique (à ne pas confondre avec le premier ordinateur personnel numérique électronique), ce DIGI-COMP 1, en kit en 1963 », nous révèle l'auteur de ce texte.

Outil pédagogique :
Il est décrit comme un jouet et une démonstration de la manière dont un ordinateur numérique binaire mécanique fonctionne, conçu pour initier les utilisateurs aux principes informatiques. « C'était autant une démonstration du fonctionnement d'un ordinateur numérique binaire mécanique qu'un joue »..

Utilisation et applications Jeu NIM :
Le DIGI-COMP 1 peut jouer au jeu NIM, une application courante pour les premiers ordinateurs simples.

Inspiration pour les carrières :
Pour certains, l'utilisation du DIGI-COMP 1 a été un point de départ pour une carrière dans la programmation ou l'informatique. « C'était mon premier ordinateur, menant à une vie professionnelle de programmation », nous dit l'auteur.

Accessibilité moderne
Réplications et versions imprimables en 3D : Des reproductions du DIGI-COMP 1 existent aujourd'hui, y compris des versions en carton et des modèles imprimables en 3D, rendant son concept accessible. Quelqu'un a également mis au point une version imprimable en 3D, qui semble plus abordable en termes de coût (en supposant que vous ayez déjà une imprimante 3D).

source : GIF

NOUVEAU DÉCODEUR TV D'ORANGE

Orange vient d'annoncer le 7 octobre 2026 le lancement d'un nouveau décodeur TV, sobrement intitulé Home Cinema.

Si ce nom manque d'un brin d'humilité, il faut constater que l'opérateur a tout fait pour se rapprocher de l'expérience qu'il promet, notamment avec la prise en charge du Dolby Atmos.

Son nom donne déjà le ton : Home Cinema. Que lui vaut un tel sobriquet ? L'opérateur historique met un point d'honneur dans son communiqué à insister sur les capacités audio de son boîtier. Sans oublier qu'il s'agit avant tout d'un boîtier, avec quelques innovations logicielles qui valent d'être soulignées.

Commençons donc par la partie image. De ce côté, pas de doute possible, on se situe bien dans la division haut de gamme. Orange a tout mis en place pour obtenir la meilleure qualité possible. Le décodeur Home Cinema prend ainsi en charge la 4K, mais également la plage HDR 10+ ainsi que le Dolby Vision, ce qui lui assurera d'afficher des palettes de couleurs plus profondes et réalistes.

Comme à son habitude depuis quelques années, Orange intègre dès l'installation la plupart des services de streaming les plus populaires, dès lors accessibles d'un simple coup de télécommande. Mais ce n'est pas tout. L'opérateur a aussi rattrapé son (immense) retard par rapport à la concurrence. Son nouveau boîtier est le premier à s'ouvrir à l'écosystème Android, en permettant notamment l'accès au Google Play Store, et donc à toutes les applications qu'il contient.



Il s'agit là d'avancées notables dans la gamme de décodeurs TV d'Orange, mais son principal argument de vente ne se trouve pas là. Passons donc à la partie audio, véritable chef de file de cette nouvelle offre. Afin d'assurer un son de qualité premium, l'opérateur s'est associé aux experts danois de chez Bang & Olufsen. Pour le dire simplement, Orange veut faire de son décodeur une barre de son à lui tout seul.

À cet effet, ce dernier embarque donc toutes les technologies audio haut de gamme, en premier lieu le Dolby Atmos, dont Orange est le premier opérateur à offrir l'accès sans équipement supplémentaire. Ce dernier sera chargé de spatialiser le son en fonction non seulement du contexte, mais aussi de la pièce dans laquelle le boîtier se trouve.
Pour servir au mieux la technologie, le décodeur embarque 4 haut-parleurs, notamment deux latéraux qui serviront justement à diffuser le son là où le Dolby Atmos les envoie. Les utilisateurs auront l'opportunité d'améliorer encore un peu plus leur installation avec deux enceintes sans fil supplémentaires. L'idée ici est de pouvoir les positionner où on le souhaite dans l'espace où se trouve le téléviseur, pour une spatialisation du son vraiment complète. Celles-ci utilisent la technologie Dolby Atmos FlexConnect, qui leur permet de se configurer automatiquement, peu importe où elles se situent.
Il vous faudra souscrire à l'abonnement Livebox Max à 47,99 €/mois pendant un an pour les nouveaux clients, avant de passer à 57,99 €/mois pour un engagement de douze mois. Ajoutez à cela 50 € pour le décodeur en lui-même et 80 € pour les enceintes optionnelles.

source : Phonandroid

FIN DU SUPPORT OFFICE-2021

Vous utilisez Word, Excel, Outlook ou PowerPoint sur votre ordinateur ?
Attention, une étape importante vient d'être franchie : depuis le **13 octobre 2026**, Microsoft ne prend plus en charge Office 2021 !
Mais êtes-vous concerné ? Voici comment le vérifier en quelques secondes.



🔍 **Quelle version d'Office utilisez-vous ?**
C'est très simple :
1. Ouvrez Word ou Excel.
2. Cliquez sur Fichier, puis sur Compte.
3. Regardez la rubrique Informations sur le produit. Vous y trouverez le nom de votre version : Office 2019, Office 2021, Office 2024…

Si vous utilisez Office 2021 (ou une version plus ancienne), la suite devrait vous intéresser !

Que signifie la fin du support d'Office 2021 ?
Rassurez-vous : vos logiciels ne vont pas s'arrêter de fonctionner du jour au lendemain ! Vous pourrez toujours rédiger vos documents Word, utiliser Excel ou consulter vos anciens emails Outlook. En revanche, Microsoft ne fournit désormais plus de mises à jour de sécurité ni de corrections de bugs pour Office 2021. Avec le temps, cette absence de mises à jour peut devenir problématique. En effet, de nouvelles failles de sécurité peuvent être découvertes, sans qu'aucun correctif ne soit proposé. L'ouverture de documents ou de pièces jointes provenant d'Internet pourrait alors présenter davantage de risques.

Faut-il absolument changer de version ?
Pas de panique ! Vous pouvez continuer à utiliser Office 2021. Cependant, pour profiter d'une version toujours prise en charge et bénéficier des mises à jour de sécurité, il est préférable d'envisager une évolution vers Office 2024.

Ou se procurer Office 2024 à bon compte ?
- Pack Office 2024 en version complète et officielle, pas d'abonnement.
- Valable pour un seul poste PC Windows 10 ou Windows 11
- Comprend Word, Excel, PowerPoint, Outlook, Access, OneNote...
- ✔ Installation ultra simple La procédure a été largement simplifiée et est très facile à mettre en oeuvre quel que soit votre âge ou votre niveau d'informatique.

➳

- ✔ Livraison INSTANTANÉE Votre clé de produit officielle, le lien de téléchargement et les instructions d'installation vous seront envoyés dans les 24h après votre paiement.
- ✔ Conseils et Service après-vente GRATUITS sur toutes les commandes Le pas à pas pour installer Office 2024 et activer votre clé de licence vous seront envoyés après votre commande. Si vous avez une difficulté d'installation, nous vous viendrons en aide.
- ✔ Garantie de service Après l'achat, nous vous fournissons une clé de produit authentique et un lien de téléchargement du site officiel de Microsoft Office. Une fois que Microsoft a vérifié avec succès votre clé de produit, il sera lié à votre compte Microsoft à vie.
- Compatible uniquement avec Windows 10 et Windows 11.
- Comprend Word, Excel, PowerPoint, Outlook, Access, OneNote...
- Mise à niveau sans perte de documents.
- Publisher a été supprimé dans cette version 2024, remplacé par des fonctions supplémentaires dans PowerPoint.
- Langue : Français.
- Un seul poste PC (la licence n'est pas transférable)
- coût de la licence : **24,90 €** TTC chez Facilepc.

FACILE PC serviceclients@facilepc.fr

source : communiqué de facilepc

ANDROÏD : LUTTER CONTRE LES SMS FRAUDULEUX

Google renforce son arsenal contre les SMS frauduleux (qui ne cessent de se multiplier) au sein de Google Messages. Si certaines fonctions sont exclusives aux modèles Pixel, d'autres concernent les appareils Android. Et il en existe même une probablement déjà présente sur votre smartphone, sans



même que vous ne le sachiez. On vous la présente.

Il est aujourd'hui difficile de repérer les arnaques tant les escrocs ne cessent de sophistiquer leurs techniques et diversifier leurs canaux – et il est, en revanche, aisé de développer une méfiance excessive et désagréable. Les constructeurs de smartphones, notamment, ont conscience de ce fléau et développent des solutions pour protéger leurs utilisateurs.
Google est l'un des acteurs les plus notables en la matière.
Face à la multiplication des SMS frauduleux, Google redouble d'efforts.
La détection des arnaques par messages est maintenant disponible sur les Pixels en France, tandis qu'un mode de protection renforcée s'appuyant sur Gemini arrive dans Google Messages.
Mais votre smartphone Android dispose déjà d'une fonctionnalité pour détecter les arnaques par SMS : **Circle to Search.**

Circle to Search détecte les arnaques par SMS
En mai dernier, Google a introduit une nouvelle fonction de sécurité au sein de Circle to Search : la détection de SMS frauduleux. Face à la multiplication du phishing par SMS, l'entreprise l'a mise de nouveau en avant dans un billet de blog officiel publié hier. Pour l'utiliser, rien de plus simple :

- Appuyez longuement sur le bouton d'accueil ou la barre de navigation pour déclencher Circle to Search,
- Entourez le SMS qui vous paraît suspect

La fonction se charge d'analyser la formulation, le contenu du texte sélectionné, les coordonnées de l'expéditeur. Si elle détecte un schéma d'escroquerie courant, l'aperçu IA souligne les éléments suspects (faux avis de livraison, urgence bancaire…) et vous conseille de bloquer l'expéditeur. Autrement, elle vous rassure en confirmant qu'il s'agit d'une alerte légitime – et cela fonctionne également avec les alertes de sécurité officielles entrantes.
Cette fonctionnalité de Circle to Search est très pratique à bien des égards :

- Elle est disponible sur les smartphones Android compatibles avec Circle to Search – et ils sont nombreux.
- Son fonctionnement est fluide avec Google Messages, l'application de messagerie par défaut sur les téléphones de bien des constructeurs Android (Google évidemment, Oppo, Samsung qui encourage ses utilisateurs à passer dessus…)
- Elle ne nécessite aucune configuration supplémentaire.
- Le processus est facile en plus d'être rapide.

Évidemment que cette fonction est la bienvenue puisqu'elle agit comme un premier filtre de sécurité très pratique pour toutes les raisons évoquées ci-dessus. Il est toutefois recommandé de toujours faire preuve de vigilance et de discernement. Ainsi, évitez de faire aveuglément confiance à Circle to Search.
Si le moindre doute persiste dans votre esprit, suivez les conseils habituels :

- Ne cédez jamais à la pression : le sentiment d'urgence est souvent un signal qu'il n'y en a pas
- Ne donnez jamais vos codes confidentiels, à quiconque.
- Ne cliquez jamais sur un lien qui vous paraît suspect ou non sollicité.
- Composez vous-même le numéro du service dont prétend émaner le message : votre banque, votre assurance…
- Rendez-vous dans l'application ou le site web officiel en saisissant vous-même l'adresse dans la barre de recherche de votre navigateur (et en vérifiant les fautes de frappe qui peuvent suffire à un hacker pour voler vos identifiants).

Avec ces différents outils de protection et ces astuces pour repérer les signaux d'alarme, vous devriez réduire considérablement les risques de tomber dans le piège des escrocs.

source : Phonandroid

L'ESPIONNAGE VIA LES VOITURES ÉLECTRIQUES ET CONNECTÉES



L'espionnage et la collecte massive de données via les voitures électriques et connectées constituent un enjeu géopolitique et de cybersécurité majeur. Souvent qualifiées de « smartphones sur roues », ces voitures intègrent une multitude de capteurs, de caméras, de micros et de systèmes GPS qui enregistrent en permanence l'activité des utilisateurs et de leur environnement

Cette problématique se divise en trois risques principaux :

- 1- **Les tensions géopolitiques et la peur de l'espionnage d'État** Les véhicules électriques, particulièrement ceux fabriqués par des constructeurs chinois, subissent une surveillance stricte des autorités occidentales par crainte que les données collectées (vidéos de l'environnement, cartographie GPS précise) ne soient transmises à des services de renseignement étrangers.
  I**nterdictions militaires** : L'armée américaine interdit l'accès aux bases militaires (notamment la base aérienne de Kadena au Japon) aux véhicules du constructeur chinois BYD. Le Département de la défense suisse (DDPS) restreint également l'accès des voitures connectées près d'infrastructures sensibles.
  Bannissements logiciels et matériels : Les États-Unis ont initié des interdictions strictes concernant l'importation de véhicules et de logiciels connectés en provenance de Chine et de Russie.

- 2- **L'intrusion dans la vie privée des conducteurs** Les constructeurs automobiles ne se contentent pas de collecter des données techniques ; ils accumulent des informations extrêmement intimes.
  Clonage de smartphones : Connecter son téléphone via câble ou Bluetooth permet à l'ordinateur de bord de copier les journaux d'appels, SMS et fichiers, des données qui restent en mémoire même après une déconnexion et extinction des appareils.
  Données comportementales et intimes : Les micros et caméras captent les conversations de l'habitacle (parfois revendues à des fins publicitaires). Des rapports ont même révélé que des marques collectaient des informations allant jusqu'aux habitudes de vie privée et parfois très privée ! .

- **Abus internes** : Par le passé, des salariés de Tesla ont été épinglés pour avoir partagé en interne des vidéos intimes ou insolites enregistrées par les caméras embarquées des clients.

- 3- **Les failles de cybersécurité et le piratage** L'écosystème de la recharge et de la connectivité expose les utilisateurs à des cyberattaques.
  Piratage via les bornes de recharge : Les hackers exploitent de plus en plus les failles des bornes de recharge publiques pour intercepter des données ou tenter de prendre le contrôle de fonctionnalités du véhicule, ce qui peut s'avérer extrêmement dangereux.
  Espionnage industriel : Les constructeurs eux-mêmes sont des cibles. Volkswagen a par exemple subi des campagnes de cyberpiratage d'envergure menant au vol de milliers de documents confidentiels liés à la mobilité et à la technologie du véhicule.

Le piratage des bornes de recharge pour véhicules électriques est devenu une réalité cybercriminelle concrète. Les infrastructures de recharge, souvent gérées à distance et connectées à internet sans protection suffisante, présentent plusieurs failles majeures. Une étude a révélé que près de 72 % des bornes accessibles en ligne acceptent des connexions sans chiffrement, transmettant les informations en clair. Les attaques se matérialisent principalement sous quatre formes :

Le vol de données personnelles et la fraude Pour utiliser une borne publique, les automobilistes utilisent des applications ou des cartes RFID associées à des comptes clients.
Piratage des bases de données : Récemment, le spécialiste de la recharge Plenitude On The Road a subi une intrusion informatique massive, exposant les noms, numéros d'identification fiscale, e-mails et historiques précis de recharge de ses clients.
Le Quishing (Faux QR codes) : Les pirates collent de faux autocollants QR code sur l'écran des bornes physiques. En les scannant pour payer, l'utilisateur est redirigé vers un site miroir frauduleux qui subtilise ses coordonnées bancaires.
Duplication RFID : Les cartes de recharge utilisant des protocoles anciens peuvent être copiées à distance par des hackers pour recharger leur propre véhicule gratuitement aux frais de la victime.
Le blocage et les demandes de rançon (Ransomwares) Les opérateurs de recharge (CPO) gèrent des parcs de milliers de bornes via des serveurs cloud. En s'infiltrant dans ces systèmes d'exploitation (souvent via des failles du protocole de communication OCPP), les rançonneurs peuvent verrouiller à distance des réseaux entiers de bornes. Ils exigent alors des rançons financières pour débloquer les chargeurs, menaçant de paralyser la mobilité d'une région entière.
L'accès direct au véhicule (Le point d'entrée) Le câble reliant la borne à la voiture ne transmet pas que de l'électricité, il échange également des flux massifs de données informatiques pour réguler la charge.
Des failles de sécurité critiques (comme CVE-2025-27071) permettent à un pirate d'exécuter du code malveillant directement à travers le port de charge.
En modifiant les paramètres via la borne, un hacker peut théoriquement tenter de pirater le système électronique de bord ou déclencher un dysfonctionnement de la batterie (surchauffe).

source : RTS Suisse