Club informatique menneçois
Le numérique pour tous
Newsletter
Janvier 2023 | 61

Le conseil d'Administration vous présente ses meilleurs vœux de bonne et heureuse année 2023.

Les arnaques liées aux cartes bancaires sont malheureusement fréquentes. Cette Newsletter fait le point sur le sujet et vous donne quelques conseils.

Denis GELIN

Les arnaques aux cartes bancaires

La France est au-dessus de la moyenne européenne sur l'utilisation de la carte bancaire. Elle est, depuis 2003, le moyen de paiement préféré des français avec plus de 60 % des transactions. Tout comme pour les chèques, elle est couramment ciblée par les escrocs et autres filous ! Quelles sont les arnaques couramment rencontrées ? Comment s'en prémunir ?

Les techniques des escrocs pour vous voler

Le phishing : la méthode « classique » pour récupérer les infos de votre carte

Le meilleur moyen que les escrocs ont trouvé pour récupérer vos données bancaires est tout simplement de vous les demander. Mais attention, pas de n'importe quelle manière : en utilisant la ruse et en se faisant passer pour un organisme de confiance (votre fournisseur d'énergie, de téléphone ou encore des impôts…).

Voici une vidéo qui résume parfaitement le fonctionnement du phishing (l'hameçonnage) :

https://youtu.be/PzPcWgkyPTE

La consigne est donc simple : ne répondez jamais à un e-mail ou à un appel téléphonique vous demandant des informations bancaires, notamment les données de votre carte. L'objectif pour les fraudeurs étant d'obtenir des renseignements personnels comme vos mots de passe, numéros de carte de crédit, vos codes secrets, adresse et date de naissance en vous faisant croire que vous vous adressez à un tiers de confiance (Banque, Assurance, assurance maladie… et même la police…) avec dans le pire des scénarii l'usurpation d'identité.

L'arnaque aux faux touristes : à connaître !

Il s'agit d'une technique bien rodée et particulièrement efficace qui est même parfois le fait d'enfants exploités par des réseaux mafieux. En deux temps, trois mouvements vous êtes dépouillé !

La méthode reste quasi identique à chaque fois : Un faux touriste attend le moment ou vous avez tapé votre code. Il interrompt votre transaction en vous demandant son chemin par exemple et peut même poser un plan ou un journal sur le clavier. Un complice arrive alors, et en une seconde il tape un montant de retrait et prend les billets… les deux compères s'enfuient ensuite en courant.

Si généralement c'est sans violence, il arrive qu'il y ait agression physique si vous intervenez… Alors méfiance !

En plus de vérifier si personne ne vous « colle » au distributeur de billet, un rapide contrôle de la machine s'impose avant d'effectuer toutes transactions.

Le skimming : le hacking des distributeurs automatiques

Une des fraudes les plus connues consiste à trafiquer les distributeurs afin de copier ou de retenir votre carte lors du retrait ou même de bloquer l'argent ! En effet, il est très facile pour les apprentis voleurs de se procurer du matériel…

Il faut regarder en premier lieu le distributeur d'une manière globale pour vérifier s'il n'y a pas une façade superposée au distributeur

Dans un deuxième temps il faut s'assurer qu'il n'y a pas un faux clavier qui est collé sur le vrai afin d'enregistrer le code que vous allez taper. Autre tactique des pirates pour récupérer le code, une petite webcam. Un petit trou est alors visible au -dessus du clavier….

Dans un troisième vérifiez au niveau du lecteur de carte la présence d'une excroissance significative d'un lecteur pirate. Cette technique permet de copier la piste magnétique de la carte au moment du retrait et d'en faire un clone.

Pour finir, vérifiez bien au niveau de la fente de distribution des billets… l'arnaque consiste à placer une languette qui bloque la sortie des billets.

D'une manière générale :

- vérifiez autour de vous et assurez-vous que personne ne se montre trop pres-

Quelques chiffres

La fraude touchant les cartes bancaires a repris son ascension avec des chiffres éloquents :

- elle représente la quasi-totalité du nombre de transactions frauduleuses (92,4%),
- elle a augmenté de 13,4 % en un an,
- la fraude atteint le chiffre record de 439 millions d'euros avec un montant moyen de 70,5 euros par opération.

Les arnaques aux cartes bancaires *(suite)*

sant ou regarde la saisie de votre code.

- lors de la saisie du code, vous pouvez également placer votre main au-dessus du clavier.
- privilégiez les distributeurs équipés de caméras de surveillance.
- si la banque en est équipée préférez les automates situés à l'intérieur des agences.
- et attention aux stations-services en libre-service ! Celles-ci, comme les distributeurs, font l'objet de malversations pour vous voler les coordonnées de votre carte !

Le vol de trottinette : un cas de skimming connu...

La fraude, dite du « Skimming » ou clonage, consiste, via des complices, comme des commerçants ou des serveurs de restaurants, à copier la bande magnétique de votre carte bancaire via un lecteur à mémoire.

Ces données sont ensuite revendues a de très jeunes adolescents, qui les retranscrivent ensuite sur n'importe quel support comme les cartes de fidélité ou même des cartes d'accès à des chambres d'hôtel ! le seul impératif étant que ces cartes aient une bande magnétique… ensuite le tour est joué ! Un vrai jeu d'enfant !

Les fraudeurs peuvent alors l'utiliser pour acheter sur des sites marchands (souvent étrangers), chez des commerçants complices, s'en servir pour se commander des repas, acheter des jeux en ligne, de la musique, etc.

Comment limiter les risques de vol ou de fraude de votre carte bancaire ?

Dans la vie réelle

Demandez à recevoir votre carte bancaire en AR ou directement au guichet de votre banque.

La carte bancaire, appartient et ne doit être utilisée que par une seule personne.

Apprenez votre code confidentiel par cœur et ne l'écrivez jamais (et surtout pas derrière la carte ! (Oui, des personnes le font…).

Détruisez le code secret reçu que vous avez reçu sous pli séparé.

Signez votre carte bancaire au dos dès réception. Vous éviterez qu'un fraudeur inscrive sa propre signature en cas de vol.

Conservez votre carte dans un lieu sûr.

Ne la laissez jamais « traîner » dans votre sac ou dans votre véhicule.

Ne perdez jamais votre carte de vue lors d'un paiement : ne la confiez pas à un serveur de restaurant par exemple, certains commerçants voyous copient la carte bancaire avant de vous la restituer. Il est ensuite alors possible de réaliser des achats sur Internet ou pire de revendre les données sur le DarkWeb ! Ce conseil est particulièrement approprié quand vous êtes en voyage à l'étranger : des vendeurs utilisent encore une vieille technique des années 80 pour réaliser des transactions de cartes bancaires. Ils se servent de « sabots » qui permettent de copier les données affichées sur la carte (le code secret n'est donc pas nécessaire) : Il est impératif de limiter votre exposition à ce genre de pratiques. Privilégiez les grandes enseignes pour cela !

Surveillez vos relevés de compte pour détecter les opérations suspectes

Notez votre numéro de carte et sa date d'expiration et conservez ces informations dans un lieu sûr, c'est très utile pour faire opposition !

Sur Internet

Vérifier avant tout achat que vous êtes sur un site sécurisé symbolisé non seulement pas la présence d'un « s » après le « http » dans la barre d'adresse mais aussi par un petit cadenas fermé qui apparaît lors du règlement de vos achats. Attention cependant : le protocole HTTPS garantit que vos données bancaires ne seront pas interceptées entre votre ordinateur et le site distant mais en aucun cas que le site marchand est fiable !

Vérifiez la fiabilité du site marchand. Afin de réduire le risque d'utilisation frauduleuse de vos informations de carte bancaire, il est intéressant d'estimer le risque. L'outil ScamDoc est fait pour ça ! Il vous affiche instantanément un score de confiance d'un site marchand inconnu. Passez votre chemin si le site analysé est dans le rouge...

Ne JAMAIS saisir votre code confidentiel à 4 chiffres sur un site. Seul le cryptogramme (code à 3 chiffres au dos de la carte) est obligatoirement demandé.

Privilégiez les commerçants proposant le 3DSecure. Cela limite considérablement l'utilisation frauduleuse de votre carte. Ce système permet d'authentifier le porteur d'une carte de paiement via un code d'authentification à usage unique, reçu le plus souvent par SMS. Ce code permet de valider le paiement et doit être saisi sur une page sécurisée.

Zoom sur le 3D Sécure

Il s'agit d'un protocole de paiement proposé entre autres par le GIE des cartes bancaires, permettant d'identifier le porteur de la carte et ainsi de sécuriser les transactions sur internet.

Afin de limiter la fraude, il a été adopté en 2015 par l'union Européenne, une obligation avec mise en œuvre au 14 septembre 2019, de déployer pour tous les paiements supérieurs à 30 euros une double identification.

L'UE a finalement accordé un délai supplémentaire (2022) pour permettre aux sites marchands de plus de 20 pays de se mettre en règle dont la France... Pour information, certains sites marchands restent réfractaires à ce système car il diminue le taux de ventes.

Carte bancaire perdue ou volée : que faire ?

Bien entendu, et même si la réglementation des opérations non autorisées par carte bancaire est plutôt pro-

Les arnaques aux cartes bancaires *(suite et fin)*

tectrice et en votre faveur, il n'en demeure pas moins que vous ne disposez pas « d'un droit inconditionnel au remboursement ».

Vous vous devez de rester vigilant et de bien vérifier les opérations de cartes et vos comptes bancaires.

Dès que vous vous apercevez de la perte, du vol ou de l'utilisation frauduleuse de votre carte, vous devez immédiatement faire procéder au blocage de votre carte de paiement !

Cette démarche est aujourd'hui grandement simplifiée par la mise en place de services dédiés par les banques et par le centre national de mise en opposition.

Et le paiement sans contact ?

Depuis son lancement en 2010 le paiement sans-contact est en constante augmentation.

Comment ça marche ?

Il s'agit de la technologie « NFC » (Near Field Communication) : une puce couplée à une mini antenne dans la carte bancaire permet de communiquer via des ondes radio avec un terminal de paiement. Ce système équipe aujourd'hui plus de 67 % des cartes en circulation. Le montant des transactions est limité, pour des raisons de sécurité, à 50 euros maximum et très souvent dans la limite d'un plafond mensuel.

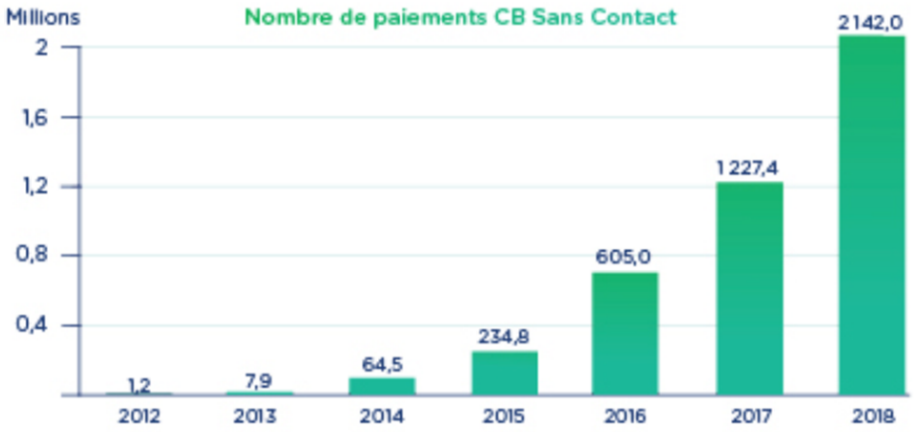
La faille de sécurité détectée en 2012 a été corrigée et la fraude sur les cartes sans-contact reste marginale et particulièrement faible, et ce, malgré que, tous les ans, des articles de presse alarmistes sur les « fraudes du sans contact à la plage ». L'observatoire de la sécurité des moyens de paiement a démontré que le taux de fraude sur le sans-contact en 2017 était de 0,02 %...

Cela n'empêche pas d'être vigilant et, soit de refuser que votre carte soit équipée de cette technologie, soit d'investir dans un étui spécifique sécurisé pour bloquer toutes transactions via un terminal de paiement « pirate ». Votre banque doit pouvoir vous en proposer.

Par contre, il existe un gros point d'alerte plus préoccupant que le piratage de la puce des cartes sans contact : le cas des oppositions.

En effet, l'opposition en cas de perte ou de vol ne bloque pas la fonctionnalité du sans-contact car dans ce type de transaction, le terminal de paiement n'entre pas en contact avec la banque... Une personne mal intentionnée ne pourrait pas utiliser la carte bancaire pour des achats sur internet par exemple, mais pourrait l'utiliser pour du sans-contact !

Mais rassurez-vous ! C'est ensuite considéré comme une utilisation frauduleuse et vous seriez remboursé . Ouf !



Les colonnes de la Newsletter vous sont ouvertes : faites-nous parvenir les articles que vous souhaitez voir publiés.

Distributeurs de billets : que faire si vous oubliez de prendre votre argent ?

Vous pensiez à autre chose et, en rentrant chez vous, vous vous apercevez que vous avez oublié de prendre vos billets de banque après un retrait. Pas de panique, il existe des solutions pour les récupérer, mais sous certaines conditions.

Oublier de prendre son argent après avoir effectué un retrait au distributeur n'est pas si rare. Il existe fort heureusement des moyens pour le récupérer. Vous vous en doutez probablement : il est plus facile de régler le problème aux heures d'ouverture de l'établissement bancaire car les billets sont généralement ravalés par le distributeur au bout de 20 à 30 secondes, tout comme votre carte bancaire. A ce moment-là, il vous suffit d'entrer dans l'agence et d'exposer votre problème. L'argent vous sera alors restitué immédiatement.

Comment récupérer vos billets si la banque est fermée ?

Cependant, si le retrait a eu lieu après l'heure de fermeture ou dans un distributeur non attaché à une banque, les choses sont plus compliquées. Si la banque est fermée, il vous faudra envoyer rapidement un courrier en recommandé à l'établissement en expliquant la situation.

Pour pouvoir être crédité, vous devrez y joindre le ticket de retrait, si vous l'avez, mais surtout un relevé de compte qui prouve que vous avez bien retiré l'argent. Si les faits sont constatés, vous serez remboursé dans les semaines qui suivent la réception de la lettre. Pour prévenir de ce type de problème, les distributeurs possèdent un système de "boîte noire" qui permet de mémoriser toutes les opérations.

Pourquoi ma carte bancaire a-t-elle été avalée ?

Si votre carte est avalée par le distributeur automatique, vous avez deux options : vous rendre à l'intérieur de la banque, ou faire opposition. Voici toutes les raisons qui peuvent expliquer l'aspiration de votre carte bleue :

- votre carte bancaire est déclarée perdue ou volée,
- vous avez composé un code erroné à trois reprises,
- vous avez oublié de reprendre votre carte,
- la date limite de votre carte bancaire est dépassée,
- un usage abusif de la carte bancaire a été détecté,
- le distributeur est défaillant.

Conseils et astuces Smartphones

Un éclairage sur la gamme des Smartphones Samsung ?

Vous savez bien évidemment qu'il existe 2 grandes familles de Smartphones qui se différencient par leur système d'exploitation : iOS ou Android. Le premier ne concerne qu'une seule marque bien connue puisqu'il s'agit d'Apple, tandis que pour le second il existe désormais une multitude de fabricants, et de nouveaux apparaissent régulièrement. La notoriété, la qualité et l'intuitivité des produits Apple ne sont plus à démontrer, tandis que du côté Android on va trouver de tout avec des produits qui sont parfois difficiles à maitriser. Nous faisons régulièrement ce constat dans l'atelier Smartphone et c'est la raison pour laquelle nous avons choisi aujourd'hui de vous aider à décrypter une gamme de Smartphones de la marque Samsung, dont le sérieux, l'innovation, et la facilité d'utilisation s'apparentent désormais à celui de Apple.

Cet article ne constitue pas une publicité pour Samsung mais un guide explicatif de la gamme d'appareils de cette marque.

Les Smartphones **Samsung Galaxy** sont actuellement regroupés en cinq gammes principales : les gammes **Galaxy S** et **Galaxy Note**, les plus haut de gamme, la gamme **Galaxy Z**, très récente pour les Smartphones pliables, la gamme **Galaxy A** pour le milieu de gamme et la gamme **Galaxy M** pour l'entrée de gamme.

La gamme M, l'entrée de gamme est pour ceux qui cherchent un Smartphone entre 100 et 250 €. La gamme A, la plus répandue, représente le milieu de gamme et les prix se situent entre 240 et 500 €. La gamme S, représente le haut de gamme, dont les prix se situent entre 500 à plus de 950€.

Samsung Galaxy est une marque appartenant à la société Samsung Electronics, qui vend des produits d'électronique grand-public. Aujourd'hui, c'est la marque la plus connue du Groupe Samsung. Elle est d'ailleurs souvent appelée par erreur ou par simplification « Samsung ». Cette marque est surtout connue pour ses Smartphones et tablettes, et plus récemment, pour ses objets connectés tels que les montres ou les écouteurs sans fils.

Créée en 2009 pour la sortie du téléphone du même nom, la marque s'est aujourd'hui diversifiée et a permis à Samsung de se positionner à la première place du marché des Smartphones depuis 2011, à la deuxième place du marché des tablettes, et à la deuxième place du marché des montres connectées depuis 2019.

En 2015, après une baisse importante de son bénéfice, le constructeur supprime 30 % de sa gamme en changeant la nomenclature de ses appareils. Les appareils bas de gamme se retrouvant principalement sous la série J (abandonnée en 2019), les milieux de gamme principalement sous la série A, puis le haut de gamme sous les séries Note et S. Actuellement, seules les gammes Galaxy et Z sont mises en vente et maintenues par Samsung. La gamme Galaxy désigne l'ensemble des Smartphones de Samsung tournant sous Android, alors, que la gamme Z désigne l'ensemble des appareils de Samsung tournant sous Tizen, un autre système d'exploitation open source, principalement utilisé dans les téléviseurs et montres intelligentes de Samsung.

Cette liste regroupe les différentes séries de téléphones ainsi que de tablettes mises en vente par la marque Samsung Electronics accompagnées d'une description pour chacune d'entre elles. Chaque série comporte une liste des Smartphones avec leurs caractéristiques et une description de chaque Smartphone.

Smartphones

La marque Samsung Galaxy est surtout connue du grand-public pour ses téléphones Android. Le premier appareil commercialisé sous cette dénomination fut le Samsung Galaxy i7500 sorti en 2009. Depuis, presque tous les Smartphones de Samsung Galaxy sont présentés sous la marque Galaxy. Depuis 2011, Samsung est le leader mondial de la téléphonie mobile, grâce à ses Smartphones Samsung Galaxy. Entre 2010 et 2020, 2 milliards de Smartphones Samsung Galaxy ont été vendus.

Les Smartphones Samsung Galaxy sont actuellement regroupés en cinq gammes principales : les gammes Galaxy S et Galaxy Note, les plus haut de gamme, la gamme Galaxy Z, très récente pour les Smartphones pliables, la gamme Galaxy A pour le milieu de gamme et la gamme Galaxy M pour l'entrée de gamme.

Galaxy S

La gamme Samsung Galaxy S est une série de Smartphones grand-public produite et vendue par Samsung Electronics. Elle constitue, avec les Galaxy Note, et plus récemment, les Galaxy Z, les fleurons de la marque, c'est-à-dire les appareils haut de gamme les plus performants et avancés tournant sous Android. La gamme Galaxy S est de loin la plus connue du grand public et aussi l'une des plus populaires. Depuis sa création en 2010 avec le Samsung Galaxy S, la gamme est renouvelée tous les ans lors d'un évènement se tenant généralement en

Conseils et astuces Smartphones *(suite et fin)*

février.

Les derniers appareils de la gamme sont les Galaxy S22 5G, S22+ 5G et S22 Ultra 5G, qui ont été présentés en février 2022.

Galaxy Z

La gamme Samsung Galaxy Z est une série de Smartphones pliables commercialisée par Samsung. Le premier appareil de la gamme, le Galaxy Fold, est présenté en février 2019, au côté des Galaxy S10. Il sort en septembre 2019, à la suite de différents problèmes liés à l'écran. Il possède un écran pliable interne se refermant comme un livre et un écran externe, plus petit, pour effectuer des actions rapides sans déplier le Smartphone. Il est équipé de six caméras au total et sera commercialisé jusqu'en décembre 2019, avant son retrait du marché.

En février 2020, Samsung présente le Galaxy Z Flip, qui contrairement au Fold, se plie dans la longueur afin de rentrer dans de petites poches. Il possède aussi un écran externe de 1,1 pouce destiné à l'affichage des notifications.

Le 1er septembre 2020, le Galaxy Z Fold 2, successeur du Galaxy Fold, est dévoilé lors d'une conférence dédiée. Le téléphone possède une charnière améliorée, un écran externe plus grand et une nouvelle dalle OLED 120 Hz. En août 2021, Samsung lance le Galaxy Z Fold 3.

Galaxy A

La gamme Samsung Galaxy A est une série de Smartphones grand-public produite et vendue par Samsung. Elle est composée de Smartphones Android milieu de gamme, et depuis 2018, d'appareils d'entrée de gamme plus compétitifs sur le plan tarifaire. Elle est, avec l'iPhone, l'une des séries de Smartphones les plus vendues dans le monde : en 2019, trois des Smartphones du top 5 en nombre de ventes étaient des Galaxy A. La gamme est composée d'environ 10 Smartphones, aux prix allant de 100 à 900 €, avec de nouvelles versions présentées chaque année.

L'un des derniers appareils de la gamme est le Galaxy A51 5G, lancé en 2020, équipé d'un processeur Exynos haut de gamme et compatible 5G.

Galaxy M

La gamme Samsung Galaxy M est une série de Smartphones grand-public produite et vendue par Samsung. Elle est composée de Smartphones Android d'entrée de gamme, avec des tarifs très compétitifs, visant surtout les marchés d'Asie et d'Afrique. La gamme est composée d'environ 10 Smartphones, à des prix inférieurs à 200 €, avec de nouvelles versions présentées chaque année.

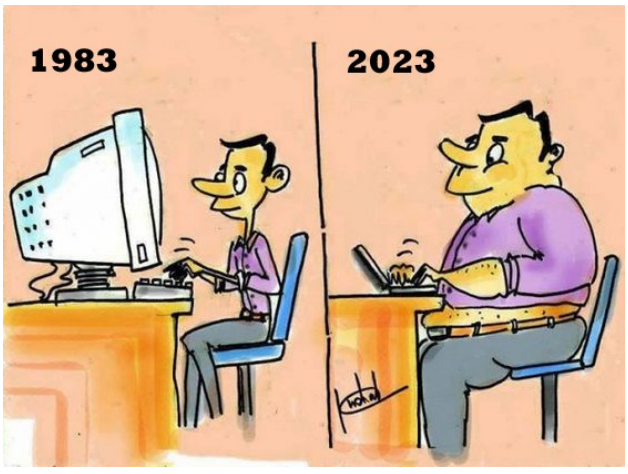
Les derniers appareils de la gamme sont les Galaxy M21 et M31, présentés en mars 2020, qui embarquent des batteries de 6 000 mAh et trois ou quatre capteurs photos.

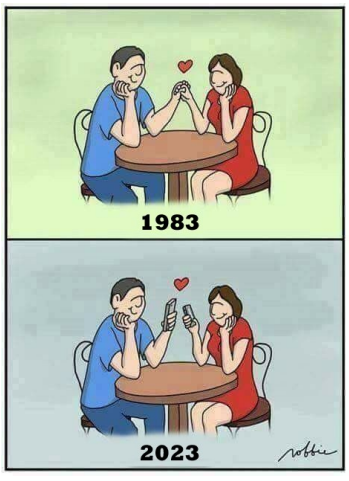
Le choix d'un Smartphone est souvent déterminé par le prix et par le conseil orienté et intéressé du vendeur, aussi nous ne saurons trop vous conseiller de vous renseigner autant que possible sur les caractéristiques et la facilité d'utilisation de ce dernier avant de valider un choix que vous pourriez regretter. Notez aussi qu'il est maintenant possible de trouver de très bonnes affaires sur des Smartphones reconditionnés et remis à l'état neuf.

Nous vous souhaitons une très bonne année 2023 et nous restons à votre disposition les jeudis après-midi sur rendez-vous de 14h30 à 16h30.

Rédacteurs : Monique WEBER, Jacques GOURDON, Thierry DELAPORTE

Humour...



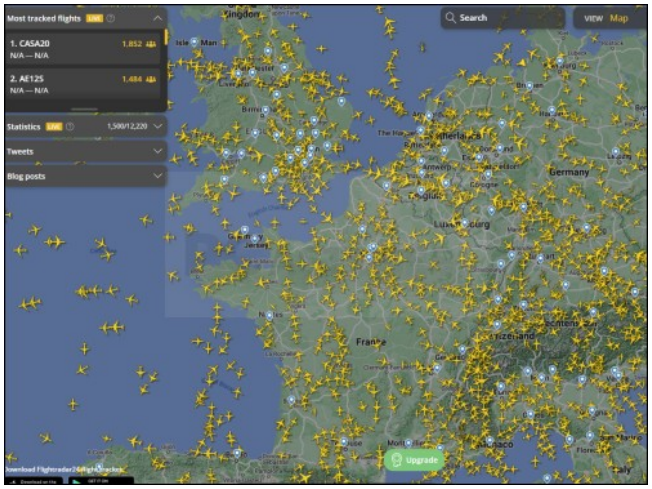


Conseils et astuces

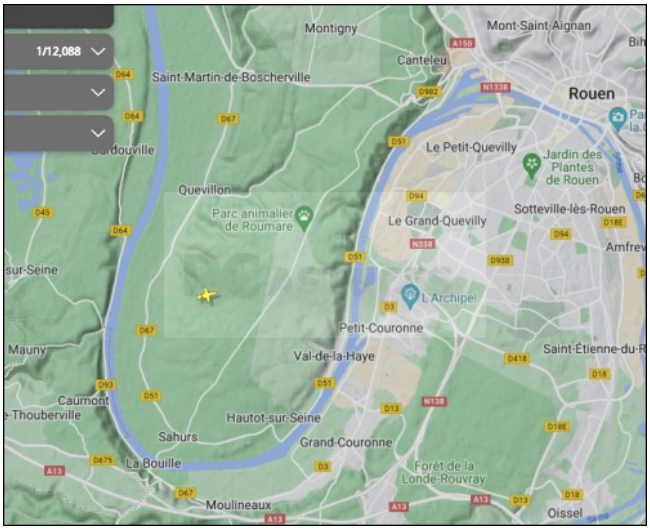
Suivre le trafic aérien en temps réel

Vous vous demandez d'où vient et où va un avion que vous voyez dans le ciel ? Flightradar24 a la réponse.

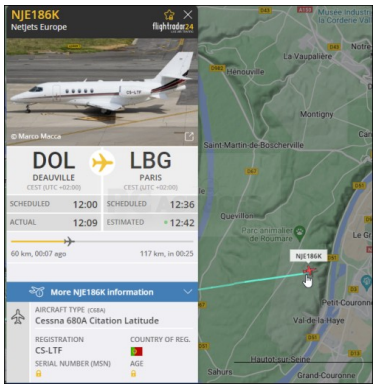
1. Dans votre navigateur Web, rendez-vous sur le site https://www.flightradar24.com/. Le trafic aérien mondial est alors affiché en temps réel.



2. Zoomez à l'endroit où vous êtes avec la molette de la souris ou avec votre doigt.

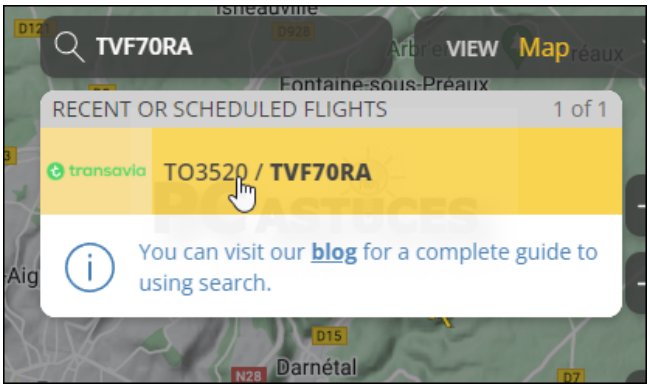


3. Cliquez sur l'avion que vous souhaitez identifier : vous avez alors des informations sur le modèle d'avion, sa provenance et sa destination.



5. Enfin, si vous êtes sur mobile, vous pouvez aussi utiliser l'application gratuite Flightradar24.

4. Notez que si vous connaissez un numéro de vol, vous pouvez le saisir dans le champ de recherche pour savoir où se trouve l'avion.



Actualité du club

Réunion du Conseil d'Administration

Le Conseil d'Administration du club s'est réuni le 6 décembre pour évoquer les sujets suivants :

- préparation de l'Assemblée Générale,
- point sur les projets en cours,
- projet de Maison de la Culture et des Savoirs,
- contenu de la Newsletter,
- changement de nom du club,
- Téléthon 2022,
- point financier,
- questions diverses.

Pourquoi changer le nom du club ?

L'idée avait germé en 2020 mais le Conseil d'Administration ne l'avait pas mise dans ses priorités.

Aujourd'hui, la demande des adhérents évolue de l'informatique vers le numérique (photo, vidéo, diaporama, généalogie, etc.).

Il existe aussi une vraie méconnaissance de nos activités à l'extérieur qui peut conduire à la perte d'adhérents potentiels. Pour preuve, lors d'une réunion à la Mairie à laquelle participait notre Président, un participant a été surpris que nous ne fassions pas de programmation. Si c'est l'image que renvoie le club, il est alors temps d'en changer.

Atelier diaporama du 1er décembre 2022

Le nouveau nom associera informatique (pour ne pas perdre nos racines) et numérique. Il sera soumis à l'avis d'une Assemblée Générale extraordinaire.

L'Assemblée Générale 2023

L'Assemblée Générale 2023 se tiendra le samedi 21 janvier à 14 H 30 dans la salle Marianne.
Elle sera suivie d'une Assemblée Générale extraordinaire pour décider du changement de nom du club.
Attention ! Vous devez être à jour de votre cotisation 2023 pour participer à ces réunions.