Cybercriminalité
Gestes de prudence et prévention
2 ieme partie

Alain BRARD

Version du 18/09/2025

Quelle est l'importance de la Cybercriminalité

- **La cybercriminalité en France – chiffres 2024**
  - Atteintes numériques : **348 000 cas (+2 %)**
  - Hausse de **74 % en 5 ans**
  - Répartition : 65 % atteintes aux biens / 30 % personnes / 5 % institutions
  - **3 000 signalements** & **1 361 incidents** recensés par l'ANSSI (Agence nationale de la sécurité des systèmes d'information, l'autorité française chargée de la cybersécurité).
- **Principales menaces**
  - **Pour les particuliers :**
    - Phishing (hameçonnage) = menace n°1
    - Piratage de comptes en hausse (+55 %)
    - Arnaques au faux support technique
    - Violations massives de données personnelles (France Travail, FFF, Free, etc.)
  - **Pour les entreprises :**
    - 67 % ont subi au moins une cyberattaque en 2024 (vs 53 % en 2023)
    - Principaux vecteurs : **phishing (60 %)**, failles exploitées (47 %), DDoS (41 %)
- Coût estimé : **> 100 milliards €** (Chiffre tout à fait plausible — et même conservateur — quand on parle d'une zone géographique large (ex. UE) ou d'un grand pays (certains rapports nationaux récents donnent des centaines de milliards pour l'Allemagne sur 1 an).

Cyberattaques récentes en France

- **Entreprises, commerces & organismes publics**
  - Free : fuite de données (≈19 M de clients, coordonnées, IBANs)
  - FFF : compromission des données de 1,5 M de licenciés
  - Auchan : centaines de milliers de comptes clients exposés
  - France Travail : ≈340 000 demandeurs d'emploi touchés
  - Viamédis / Amerys : données de santé / assurés volées
  - SFR : fuite d'informations clients
  - Boulanger, Cultura, Truffaut, Grosbill : bases clients compromises
  - CAF : accès frauduleux à des comptes allocataires
- **Hôpitaux & organismes publics**
  - Hôpitaux publics (Normandie & Hauts-de-France) : vol de données administratives (identité, âge, coordonnées)
  - Clinique de Saint-Étienne : vol des données de ~126 000 patients
  - Centre hospitalier d'Armentières : piratage concernant ~300 000 patients
  - Hôpital Simone Veil de Cannes : attaque par ransomware, perturbation des services
  - Vol de données médicales (Mediboard) : ≈750 000 personnes affectées (allergies, prescriptions, etc.)
  - AP-HP (Paris) : fuite de données COVID (~1,4 M de personnes concernées)
- -

Nouveaux risques et techniques d'attaques.

- **Nouveaux risques en 2024**
  - **Phishing industrialisé** : automatisé, personnalisé, renforcé par l'IA. Envois massifs de courriels / messages très ciblés, souvent personnalisés, parfois automatisés par des outils IA.
  - **Deepfakes & IA générative** : usurpation de voix/vidéos pour escroqueries . Utilisation de voix, vidéos ou images synthétiques pour imiter une personne de confiance (dirigeant, collègue, client)
  - **Ingénierie sociale augmentée** : exploitation fine des données volées. Utilisation de données personnelles / fuite de données + IA pour créer des messages convaincants, personnalisés, pressants.
  - **Attaques cloud & vulnérabilités logicielles** : Exploitation de failles dans des services cloud, logiciels tiers, ou failles zero-day (vulnérabilité logicielle inconnue et non encore corrigée) Mauvais paramétrage, obsolescence logicielle.
- **Attaques évoluées**
  - **Rançongiciels (Ransomware) nouvelle génération**
    - Double extorsion: En plus du chiffrement, les attaquants exfiltrent les données (ils les copient avant de les chiffrer). S'ils ne reçoivent pas la rançon : La victime perd l'accès à ses données (chiffrement). Les pirates menacent de publier ou vendre les données sensibles (propriété intellectuelle, dossiers patients, comptes clients, données bancaires…).
    - Cela met une pression beaucoup plus forte : au risque technique s'ajoute le risque juridique (RGPD), financier (clients attaqués à leur tour), et réputationnel.
    - Pression accrue sur les victimes
- –

Nouveaux risques et techniques d'attaques.

- **Nouveaux risques en 2024, Attaques évoluées …**
  - **Contournement de l'authentification**
    - Failles dans l'usage des codes de vérification à usage unique (SMS, applis tierces), solution contournée dans certains cas, usage malveillant d'applications tierces.
    - Nécessité de clés de sécurité / MFA avancé :
      - Une clé de sécurité est un petit objet (souvent une clé USB ou un porte-clé qui se connecte en USB ou Bluetooth/NFC).Elle sert à confirmer votre identité lorsque vous vous connectez à un site ou un service. Même si un pirate a volé votre mot de passe, il ne peut pas se connecter sans la clé physique → c'est comme un "badge d'accès numérique". (La CB et le Smartphone peuvent servir).
      - MFA = authentification multi-facteurs. L'idée est d'avoir plusieurs preuves différentes que c'est bien vous, pas seulement un mot de passe.
      - 3 grandes familles de facteurs :
        - Quelque chose que vous savez → mot de passe, code PIN.
        - Quelque chose que vous avez → téléphone, clé de sécurité, badge.
        - Quelque chose que vous êtes → empreinte digitale, reconnaissance faciale, voix.

L’actualité de la Cybercriminalité

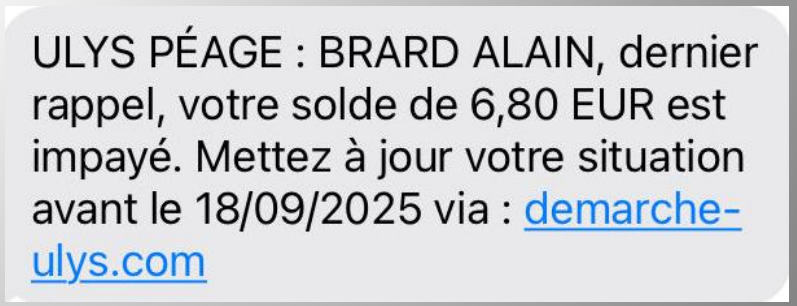
- **les dernières techniques utilisées pour pirater les comptes bancaires.**
- Méthodes classiques :
  - sites clones → emails ou SMS vers faux sites de banque
  - Smishing → SMS frauduleux (souvent avec usurpation du numéro téléphonique de la banque)
  - Vishing → faux conseillers par téléphone, parfois avec voix générée par IA.
  - Malwares bancaires → logiciels sur PC ou smartphone interceptant identifiants et codes.
- Techniques plus avancées :
  - Contrôle à distance : logiciels frauduleux de “support technique” → accès total à l’ordinateur/téléphone.
  - Modification des virements en temps réel : changement du bénéficiaire à la volée (Cheval de Troie type Zeus).
  - Usurpation d’identité numérique : réutilisation de données personnelles issues de fuites massives.
  - Attaques via IA / deepfake : faux appels crédibles, emails ou voix synthétiques imitant un conseiller
- -

Le smishing, c’est l’arnaque par SMS ; le vishing, c’est l’arnaque par téléphone.

- Sextorsion : mécanisme
  - Piratage : prise de contrôle d'une webcam ou vol de données. Via un virus ou un logiciel malveillant installé sur l'ordinateur/smartphone (souvent par phishing ou téléchargement piégé).Le pirate peut activer la webcam à distance et enregistrer des images.
  - Menace : message affirmant posséder des images/vidéos intimes. Pas toujours vrai.
  - Chantage : demande de rançon (souvent en cryptomonnaie)
- Que faire :
  - Ne jamais payer → cela encourage le cybercriminel.
  - Conserver les preuves (emails, captures d'écran, adresses de paiement).
  - Déposer plainte (police, gendarmerie, THESEE).
  - Renforcer sa sécurité numérique (mots de passe, antivirus, cache webcam).
- L'importance numérique de ces attaques
  - Les signalements de sextorsion ont fortement augmenté ces dernières années : par exemple, aux États-Unis le NCMEC (National Center for Missing & Exploited Children) a reçu 26 718 signalements en 2023, contre 10 731 en 2022 — plus du double en un an.
  - Les autorités nationales et européennes alertent sur une hausse globale des cas, en particulier parmi les jeunes (victimes souvent ciblées via applis de rencontres/ réseaux sociaux).
  - -

Deepfakes & IA : l'amélioration des outils d'IA augmente le risque de menaces reposant sur des images fabriquées.

- Divers - les principales arnaques en forte croissance:
  - Scams d’investissement / crypto → promesses de rendements élevés, plateformes frauduleuses.
  - Pig-butchering → arnaque sentimentale combinée à de faux investissements
    - arnaque par « mise en relation + faux investissement » : on gagne votre confiance pendant des semaines puis on vous pousse à déposer gros dans une plateforme frauduleuse.
  - Deepfakes & IA → imitation de voix ou d’images pour escroquer.
  - Faux sites marchands → produits jamais livrés, vols de données bancaires
  - l’arnaque liée aux péages « à flux libre » (envoi de faux SMS / e-mails réclamant un paiement) s’est beaucoup diffusée ces derniers mois.
    - Des escrocs envoient des SMS, e-mails ou courriers se faisant passer pour des opérateurs (Ulys/Vinci, SANEF, APRR, etc.) pour réclamer le paiement d’un « péage » supposé non réglé sur une portion en flux libre. Le message contient un lien vers un faux site de paiement qui imite l’officiel afin de récupérer des données bancaires ou pousser à un paiement frauduleux. La somme initiale est souvent faible (ex. ~6,80 €) pour paraître crédible avant d’ensuite tenter d’obtenir plus.



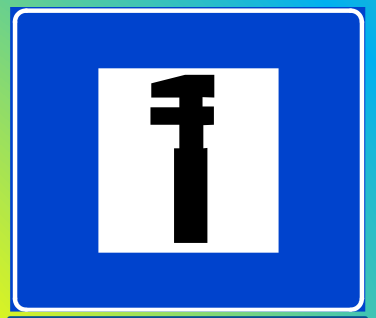
- Divers - les principales arnaques en forte croissance:
  - Faux sites ou fausses annonces de location saisonnière (Airbnb, Abritel, Booking imités)
    - Prix très attractifs pour attirer les victimes
    - Paiement demandé par virement ou lien non sécurisé.
    - Après paiement → le bien n’existe pas ou est indisponible.
    - L’escroc disparaît (annonce supprimée, site fermé).
  - Conseils de protection :
    - Vérifier l’URL, mentions légales et coordonnées du site.
    - Se méfier des prix trop attractifs.
    - Consulter les avis sur des sources indépendantes.
    - Ne jamais payer par virement direct.
    - Utiliser des plateformes reconnues et sécurisées
  - -

J'ai installé un bon logiciel anti-virus et je le met à jour quotidiennement

Je gère correctement Mes mots de passe. J'utilise l'authentification à 2 facteurs (PWD+tel)

Je fais régulièrement des sauvegardes

Je ne télécharge pas n'importe quoi, je n'accepte pas d'aide de personne que je ne connais pas



Mon système d'exploitation (Windows, IOS ...) Et mes logiciels sont à jour

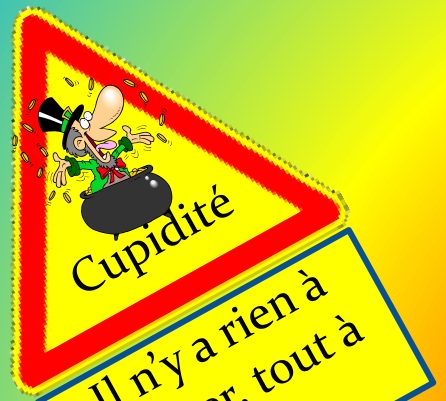
Je ne partage jamais et sous aucun prétexte mon code de CB ni mes mots de passe

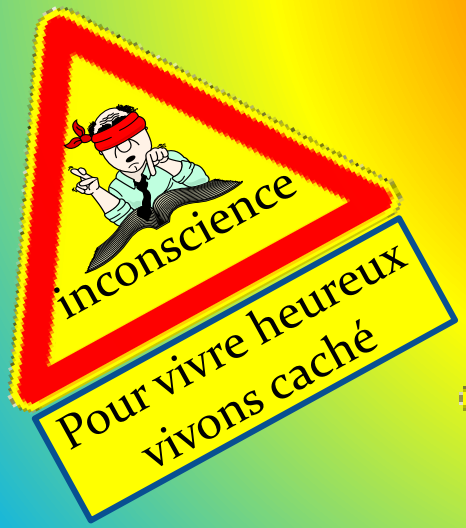
Je respecte les règles de navigation sur Internet

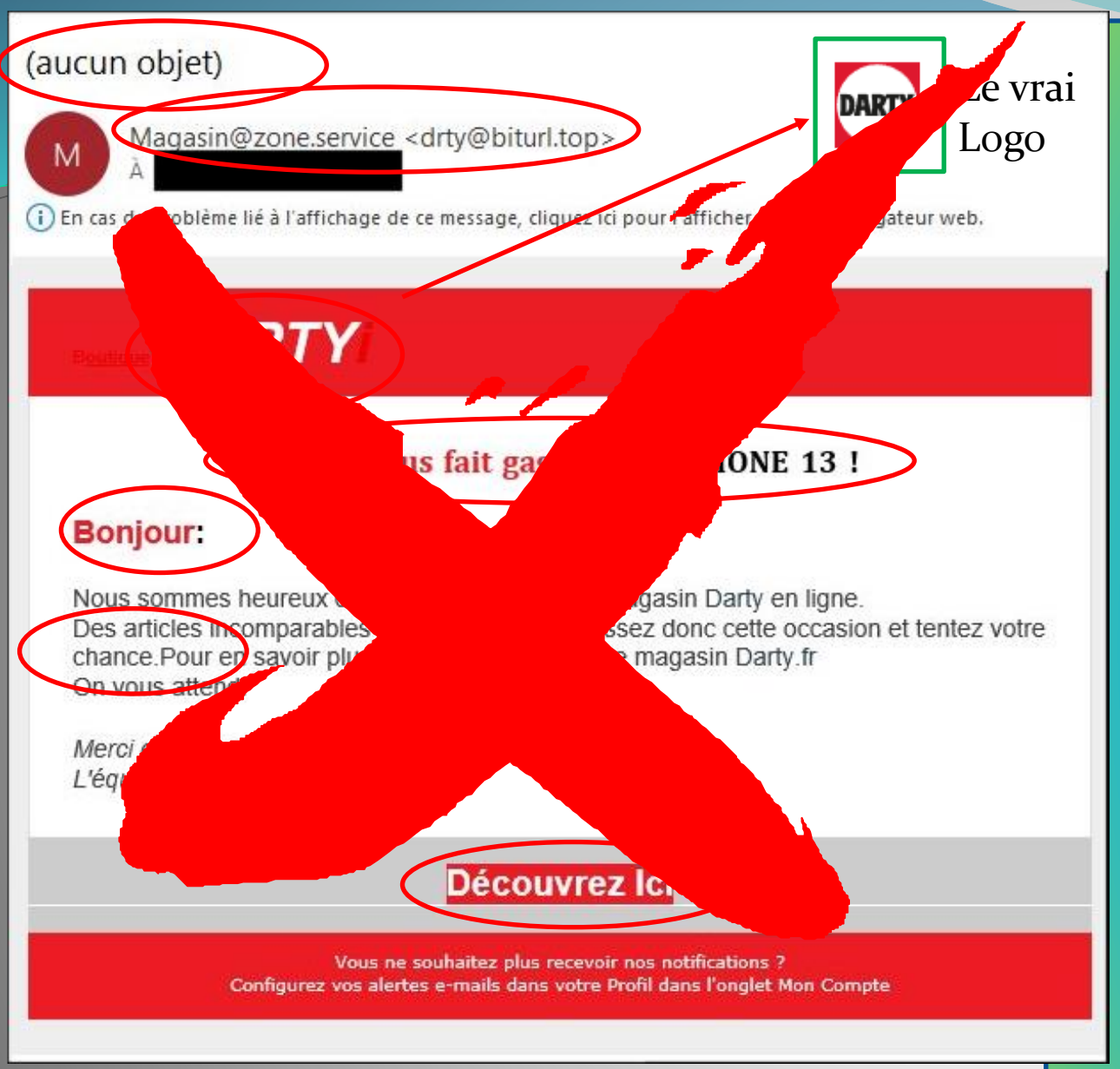
Je fais attention au Wifi partagé (public, hôtel...)

Je vais directement sur les sites « sensibles » en utilisant mes propres liens ou mieux via le moteur de recherche

Les sources de danger dans les mails, SMS et pages Internet





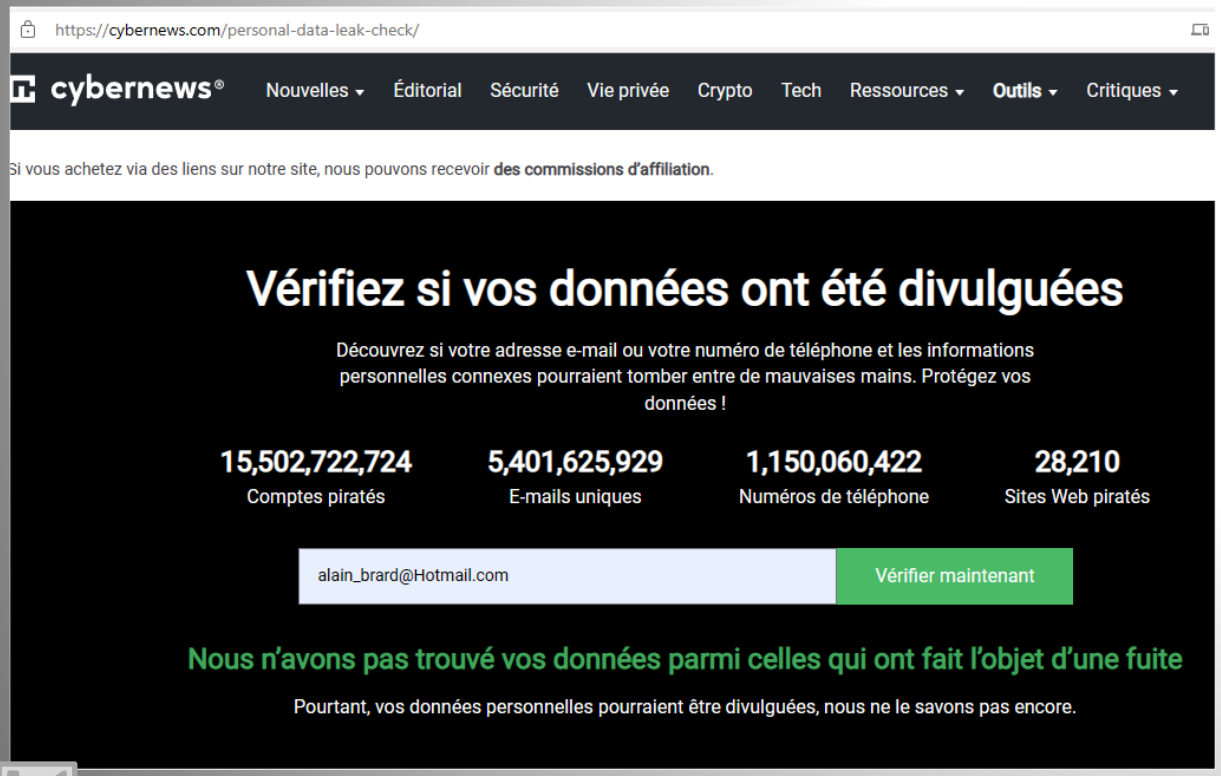


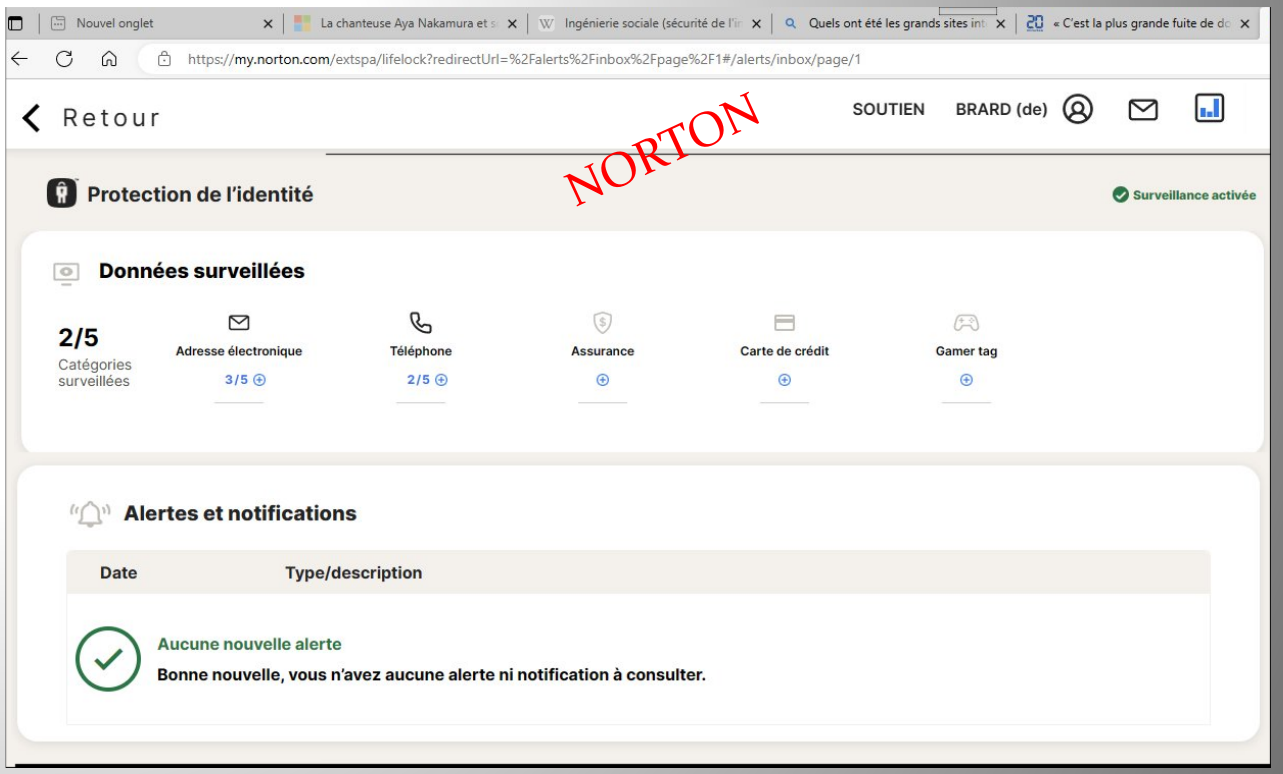
Reconnaitre les mails d'arnaque

- Absence d'objet ou objet fantaisiste ;
- Emetteur ne reprenant pas le nom de domaine de l'entreprise (Darty dans l'exemple) ou un libellé d'imitation (drty) et/ou émanent d'un particulier, ou contenant des caractères spéciaux (0, o, & %) ;
- Absence de Charte graphique de l'entreprise ou charte fantaisiste (logo) ;
- Message non personnalisé alors que vous êtes client / adhèrent / usager ...
- Langue française, grammaire, orthographe non respectée ;
- Présence de liens et/ou de pièces jointes (exe, bin, PDF, Doc ...) ;
- Emetteur dont vous n'êtes ni client, adhérent, usager ...
- Mail évoquant des gains, l'urgence, un risque, la fraude, des mises à jour à faire, la péremption de vos droits de votre carte de sécurité sociale... avec des délais courts pour réagir, de compte bloqué ;
- Absence des mentions légales ;
- ...
- -.

Vous êtes ou vous pensez être attaqué, que faire ?

- Surveillance
  - Certains Antivirus vous permettent de surveiller le « Darknet (L'internet sombre / parallèle) » à la recherche d'informations vous concernant. Idem pour certains sites :
  - Personal Data Leak Checker: Votre e-mail et vos données volés.
  - -



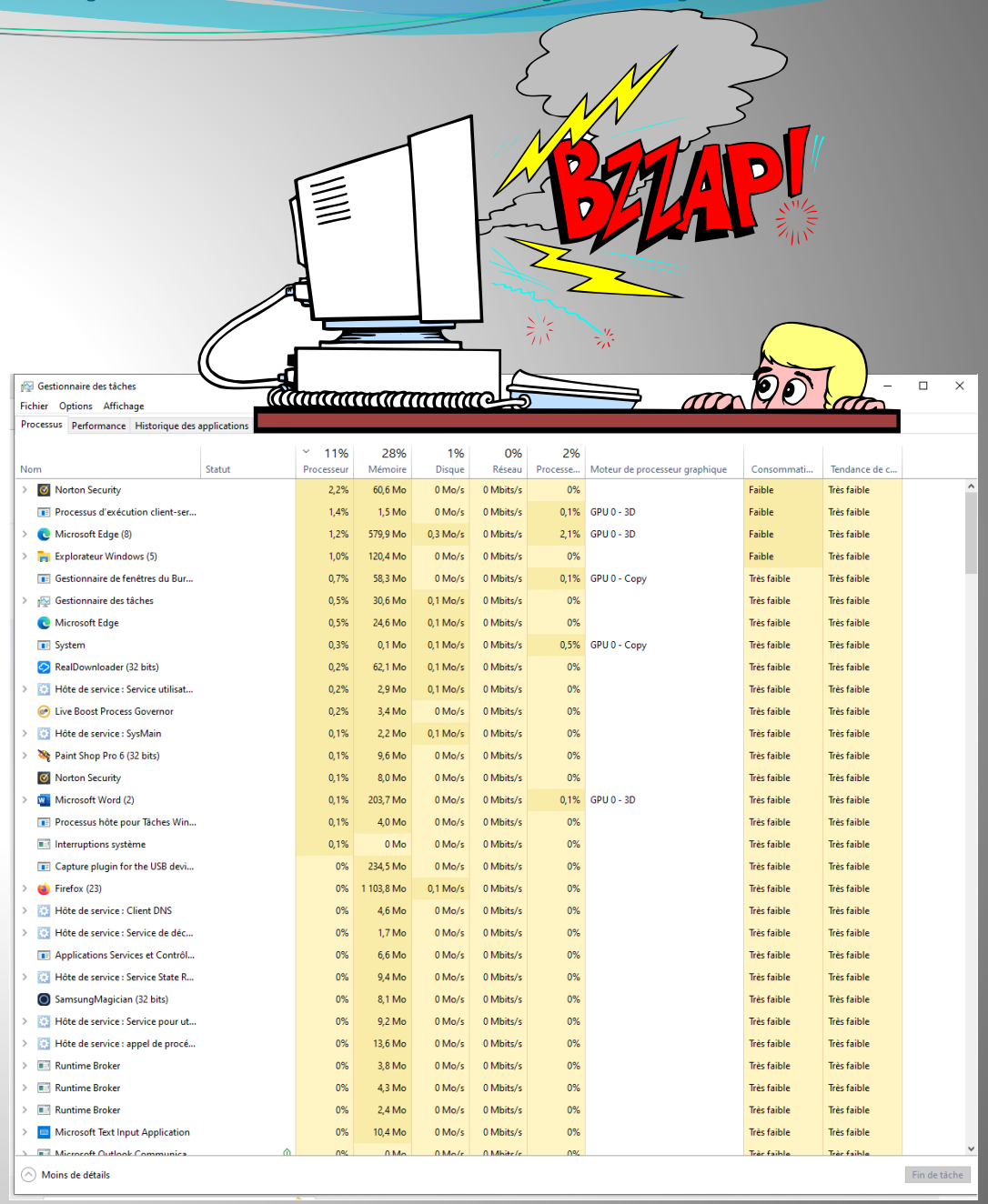


Vous êtes ou vous pensez être attaqué, que faire ?

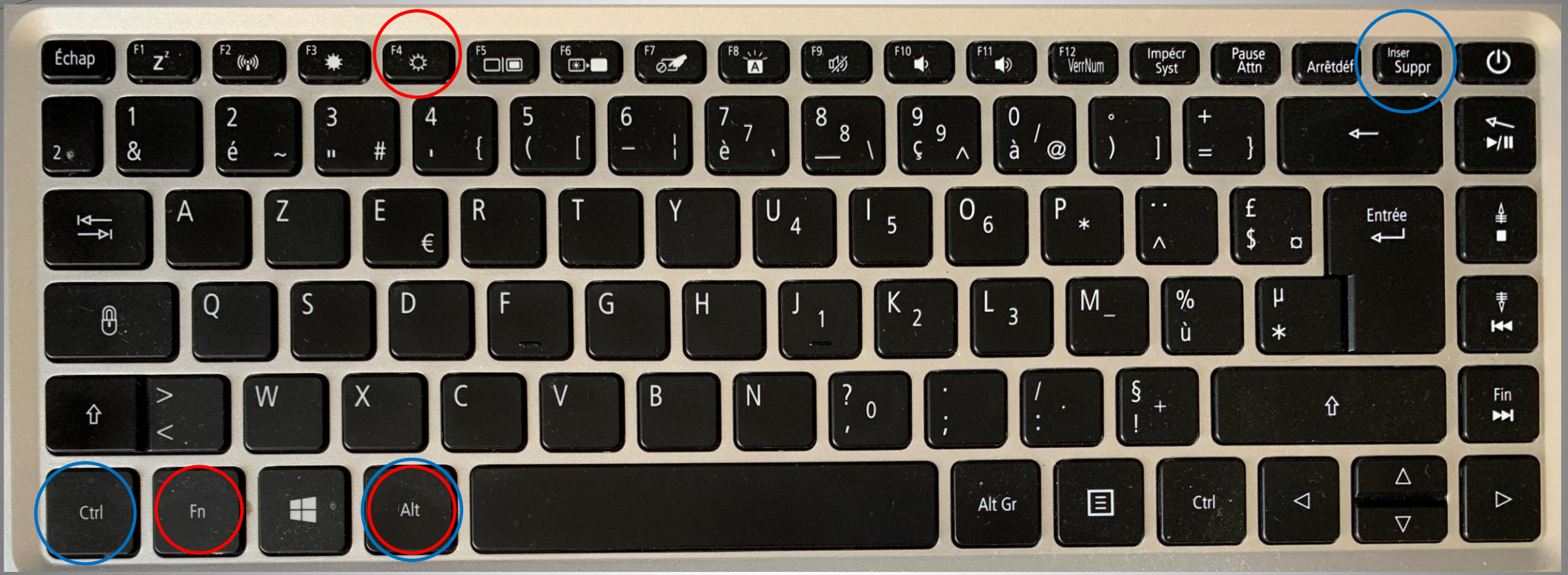
- Vous venez de subir une attaque:
  - Dans la plupart des cas, c'est votre logiciel antivirus qui vous préviendra et aura fait le nécessaire (blocage du Virus, mise en quarantaine du fichier suspect, …).
  - Par précaution, fermer votre internet, si vous ne l'aviez pas encore fait et lancer un « scan (une analyse) de votre ordinateur via votre antivirus.
  - Si nécessaire changer vos mots de passe voire votre adresse e-mail des sites sur lesquels vous étiez.
  - Vérifiez dans vos banques qu'un nouveau bénéficiaire de virement n'a pas été ajouté frauduleusement, que vos informations personnelles sont à jour en particulier votre numéro de téléphone mobile et votre adresse mail.
  - Vérifiez la liste de vos virements.
  - Restez attentif dans les jours à venir.
  - -

Vous êtes ou vous pensez être attaqué, que faire ?

- Vous êtes ou vous pensez être attaqué, que faire ?
- L'attaque au feu d'artifice
  - Si subitement un grand nombre de pages Internet s'affichent, avec une alarme sonore et des messages du type « votre ordinateur est infecté par un virus cliquez ici .... », des clignotements partout, un feu d'artifice d'écrans ...
  - En bref, tout pour vous stressez au maximum, pas de panique, ça ne va pas exploser !
    - **Ne cliquez pas sur le lien censé vous aider, vous téléchargeriez un Cheval de Troie**
    - **N'appelez pas le centre d'aide** (prétendument être Microsoft, l'éditeur de votre antivirus ou tous autres faux services), votre interlocuteur vous fera télécharger un cheval de Troie où vous vendra un abonnement « bidon » à un logiciel de pseudo-sécurité ...
    - Commencez par faire ALT+F4 (touche ALT combinée avec la touche de fonction F4) => cela permet de fermer le programme en cours : votre navigateur.
    - Si cela n'est pas suffisant (touche F4 invalidée par le hacker) tapez CTRL+ALT+Suppr cela conduit au gestionnaire de programmes, choisissez « gestionnaire des taches », vous verrez apparaitre un tableau de tous les programmes en cours d'exécution sur votre PC. Vous pouvez alors sélectionner la/les lignes(s) de programme(s) posant problème et faire « Fin de tâche ».
    - -



Fermer une application et/ou le Pc Windows lorsque l'application ne répond plus?



ALT+(Fn)+F4	Ferme une fenêtre applicative / Application
CTRL+ALT+Suppr.	Affiche le gestionnaire de programmes, gestionnaire des tâches , sélection, fin de tâche
ALT+|←	Permet de passer d'une application à une autre

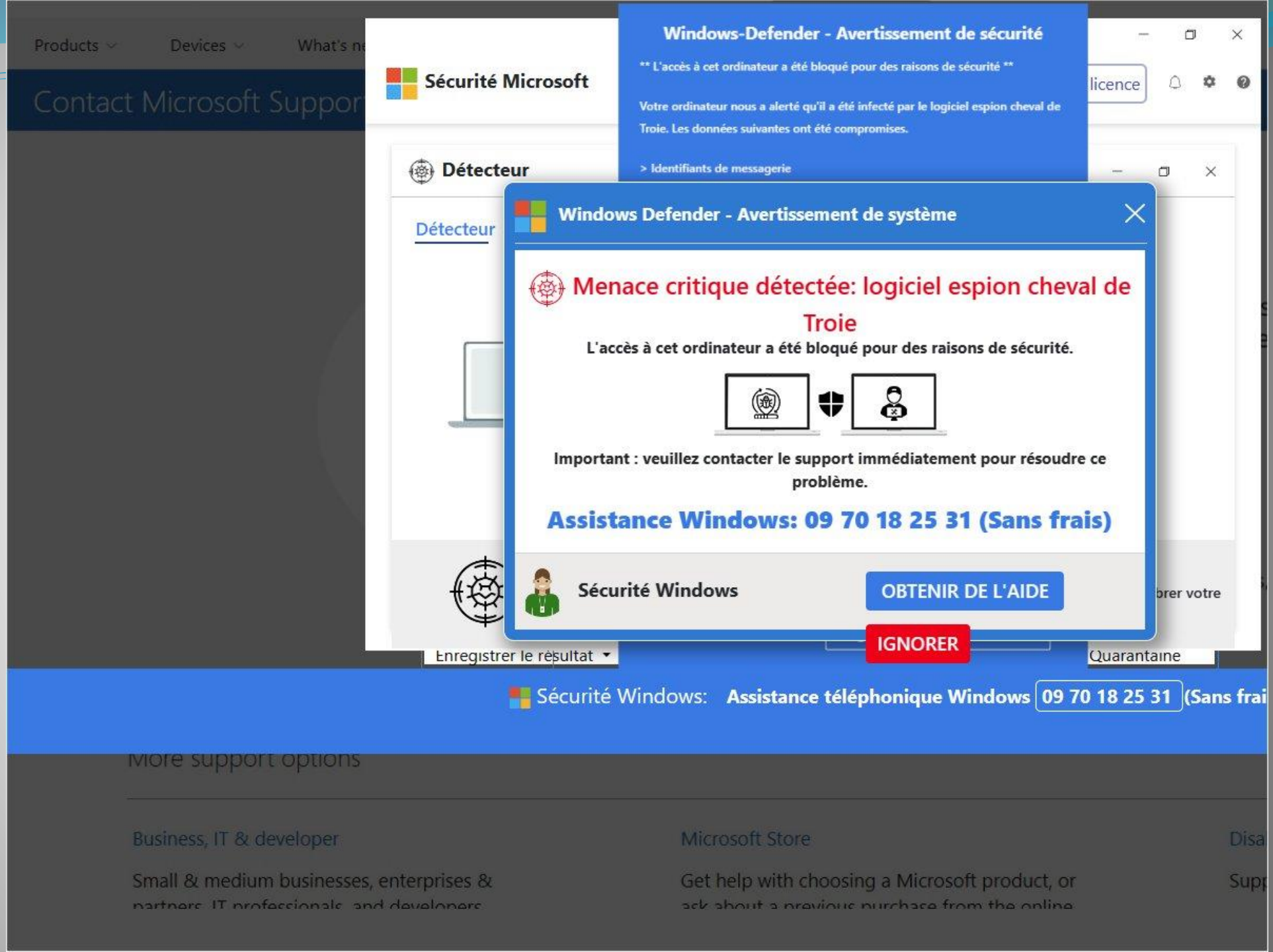
Fermer une application et/ou le MAC lorsque l'application ne répond plus?

- Forcer l'arrêt d'une application sur Mac et/ou le redémarrage de la machine:
  - Raccourcis et actions rapides : Menu Force Quit (Fenêtre "Forcer à quitter") : Apple menu > Force Quit… → sélectionnez l'application qui ne répond pas → Force Quit. (perte possible des données non enregistrées).
  - Raccourci clavier : ⌘ (Commande) + ⌥ (Option) + Esc (Appuyez en même temps pour ouvrir directement la fenêtre Force Quit Applications, sélectionnez l'app et cliquez Force Quit.
  - Forcer la fermeture d'une app depuis le Dock : Maintenez la touche Option enfoncée, faites un clic droit sur l'icône de l'app dans le Dock, puis choisissez Force Quit (pas de boîte de confirmation).
  - Moniteur d'activité pour processus récalcitrants :
  - Ouvrez Applications > Utilities > Activity Monitor, repérez le processus problématique, cliquez sur la croix (X) en haut à gauche, puis choisissez Force Quit ou Quit.

Si rien ne répond — redémarrage forcé / arrêt
Si le Mac ne redémarre pas normalement : appuyez et maintenez le bouton d'alimentation (ou le bouton Touch ID sur certains portables) pendant ~10 secondes jusqu'à extinction,

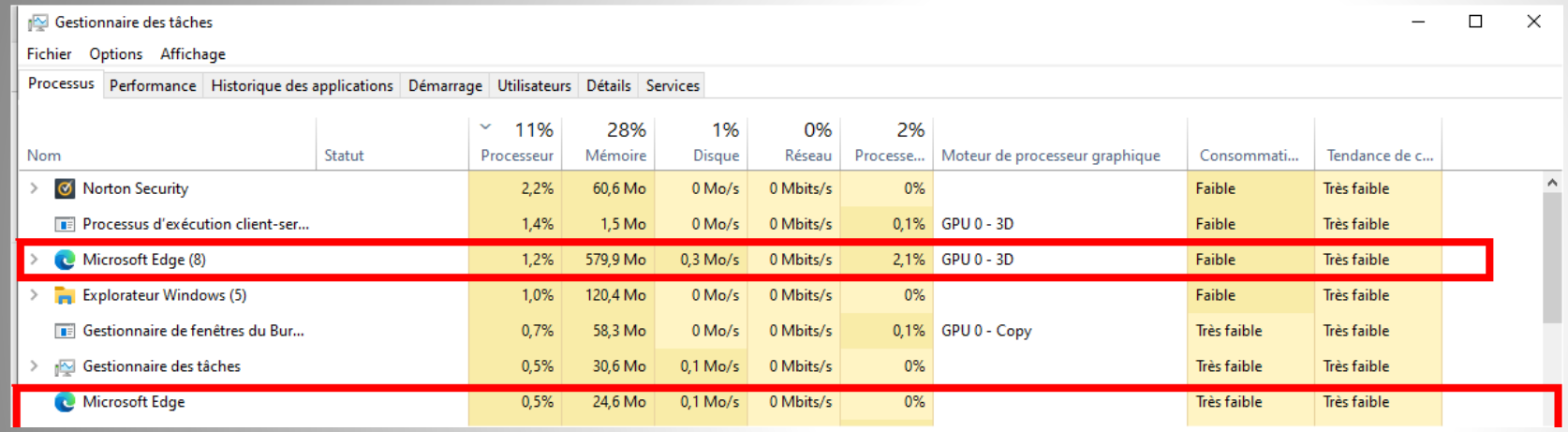
1. ⌘ (Commande / Command / cmd) — touche Command (souvent marquée d'un ⌘).
2. ⌥ (Option / Alt) — touche Option (parfois marquée alt ou option).
3. Esc (Échap / Escape) — la touche Esc en haut à gauche du clavier.

- Illustration / l’attaque au feu d’artifice
  - -

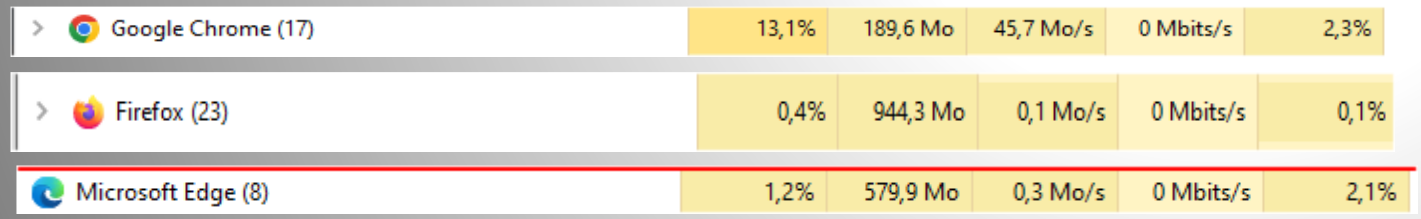


Vous êtes ou vous pensez être attaqué, que faire ?

- L'attaque au feu d'artifice (suite)
- Repérez la ligne correspondant à votre navigateur (attention il peut-y en avoir plusieurs, surtout si plusieurs pages du navigateur sont ouvertes, et le tableau évolue en permanence), cliquez sur cette/ces ligne(s),



- Et pour chacune, en bas de l'écran, appuyez sur « fin de tache » cela force l'arrêt immédiat du navigateur.



- NB : Selon votre navigateur la /les lignes seront identifiées par Firefox, Edge, Chrome ....

Vous êtes ou vous pensez être attaqué, que faire ?

- L'attaque au feu d'artifice (suite)
  - Si cela ne fonctionne toujours pas, essayez de fermer proprement en les sauvegardant vos travaux en cours. Tapez ALT + Tab (grâce aux flèches choisissez successivement toutes les fenêtres ouvertes et enregistrer vos travaux en cours avant de fermer proprement ces applications (ou tapez ALT + F4 pour les fermer plus brutalement) et lorsque vous aurez arrêté ces programmes en cours, à l'exception du navigateur que vous ne parvenez pas stopper et qui vous stresse, arrêtez l'ordinateur avec le bouton marche / arrêt.
  - **Attention : Débrancher le fil électrique brutalement risque de détruire ou au moins de détériorer votre disque dur.**
  - L'événement est stressant (des pages partout des alarmes sonores et visuelles) mais rarement risqué dans la mesure où vous ne donnez pas suite aux demandes de cliquer sur un lien ou d'appeler un numéro de téléphone. Le principale risque est de devoir arrêter brutalement le PC et de perdre des travaux en cours.
  - Au redémarrage de votre ordinateur lancez un scan complet de votre PC à partir de votre logiciel antivirus.
  - Et lorsque vous redémarrerez votre navigateur, si celui-ci vous propose de rouvrir les pages de la session précédentes ne le faites surtout pas vous auriez gagné un deuxième tour de piste !
  - -

Vous êtes ou vous pensez être attaqué, que faire ?

- Vous êtes ou vous pensez être attaqué, que faire ?
  - Fraude à la Carte Bancaire -Quel remboursement ?
    - La banque doit vous rembourser au plus tard à la fin du 1er jour ouvrable suivant votre signalement (Il n'est pas nécessaire d'avoir souscrit une assurance spécifique) sauf négligence de votre part.
    - En cas de vol ou de perte de votre carte, les dépenses réalisées avant le blocage sont à votre charge dans la limite de 50 €, excepté si l'opération a été réalisée sans votre code secret (3D sécure).
    - C'est à la banque de démontrer la négligence du client pour pourvoir refuser un remboursement (infraction avec le code monétaire et financier). Attention vous devez faire opposition dès que vous avez connaissance de la perte ou du vol de cette carte et pouvoir prouver que vous avez fait opposition.
    - Utiliser le service en ligne Perceval, pour faire un signalement de fraude à la carte bancaire.

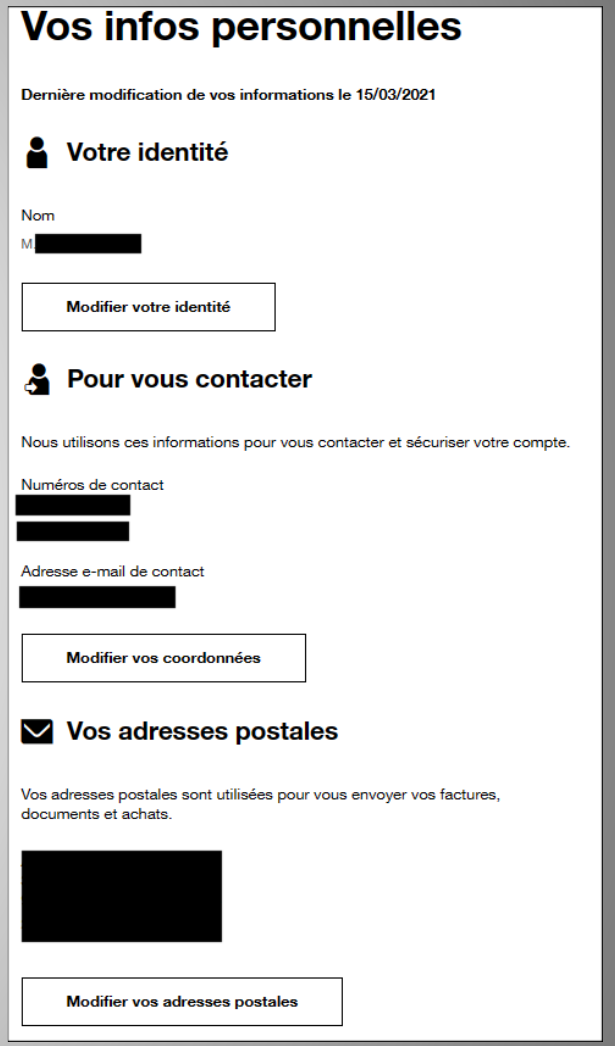
  - Détournement de fonds via Internet
    - La banque est responsable de la sécurité de vos avoir dans la mesure où vous ne commettez de votre côté pas de négligence.
    - Faite au plus vite opposition des opérations contestées.
    - Déposez plainte (le cas échéant par Internet).
    - Le phishing du client est une cause courante de refus de remboursement, c'est pourquoi il est important de savoir le détecter.
    - -

https://www.demarches.interieur.gouv.fr/particuliers/escroquerie

Vous êtes ou vous pensez être attaqué, que faire ?

- Votre messagerie est piratée
  - En préalable et en permanence, faites en sorte que vos données soient à jour (Nom, Prénom, adresses, les numéros de téléphone, adresse secondaire de messagerie, questions / réponses secrètes ….).
  - Le cas échéant si l'option est disponible activer la double-authentification (avec code sur téléphone).

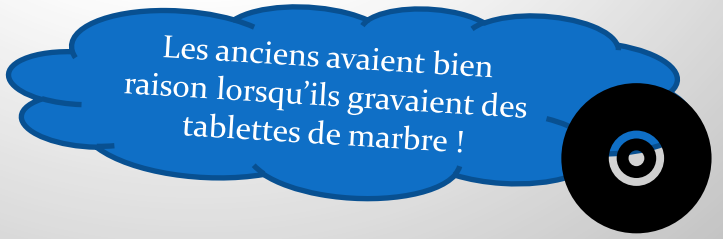
  - Le plus souvent vous découvrirez que votre messagerie a été piraté parce que vos contacts vous indiquent avoir reçu un message de votre part alors que vous n'en êtes pas l'auteur ;
  - Essayez de vous connecter à vote messagerie avec votre identifiant / mot de passe, y compris en utilisant la procédure de réinitialisation de mot de passe. NB : Vérifiez que votre clavier est position minuscule et pas bloqué en position majuscule. Si vous y parvenez changez immédiatement votre mot de passe par un complexe et mettez en place la double authentification (mot de passe + SMS).
  - Il existe des procédures de récupération de votre accès et de réinitialisation de votre mot de passe propre à chaque messagerie, certaines nécessitent que vous ayez enregistré des données connues et que vous ayez connaissance des derniers mails échangés. Dans d'autres vous pouvez appeler un service dédié.
  - S'il existe pour cette messagerie, vérifiez l'historique de connexion.
  - Dans la plupart des messageries il existe la possibilité de filtrer et/ou rediriger les messages vers une adresse e-mail tierce. Vérifiez l'absence de redirection de vos e-mails vers une boite qui ne serait pas la vôtre.
  - Vérifiez qu'aucune adresse e-mail frauduleuse n'a été créée.
  - Si certains (ou tous) vos contacts ont été supprimés, ils sont le plus souvent dans la « poubelle » des contacts et peuvent être restaurés pendant un certain temps.
  - Si vraiment vous ne pouvez plus accéder à votre messagerie : Prévenez vos principaux contacts, dont les organismes financiers et surveiller vos comptes bancaires.
  - Prévenez vos amis, afin qu'ils ne s'étonnent pas de recevoir des mails de demande d'aide, d'argent … censés venir de vous.
  - Déposer plainte : Plusieurs infractions pénales peuvent être retenues : Piratage informatique, atteinte au secret des correspondances, usurpation d'identité, escroquerie.
  - -

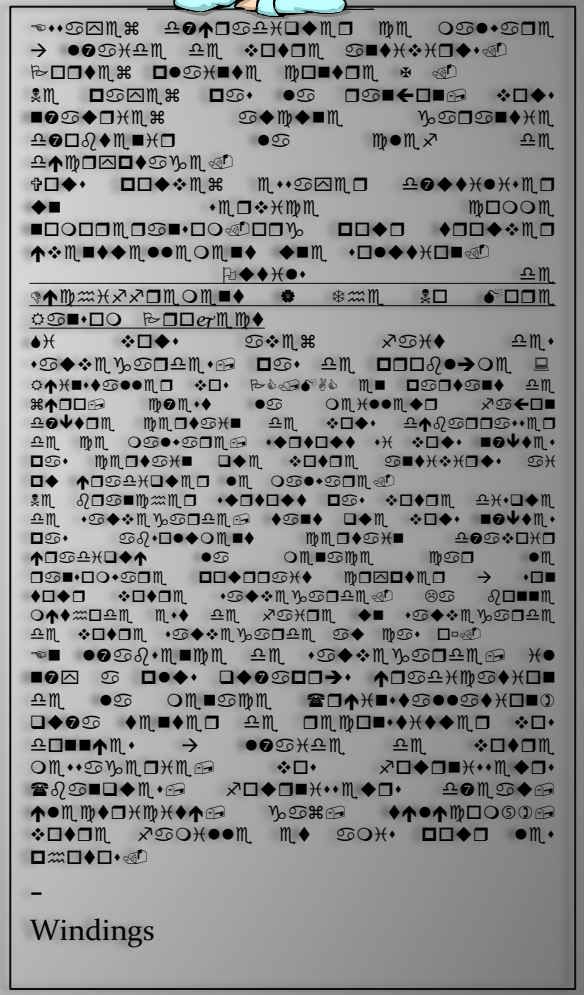


Vous êtes ou vous pensez être attaqué, que faire ?

- Vous êtes victime d'un ransomware / rançon logiciel :
  - Essayez d'éradiquer ce malware à l'aide de votre antivirus.
  - Portez plainte contre X .
  - Ne payez pas la rançon, vous n'auriez aucune garantie d'obtenir la clef de décryptage.
  - Vous pouvez essayer d'utiliser un service comme nomoreransom.org pour trouver éventuellement une solution.

    Outils de Déchiffrement | The No More Ransom Project
  - Si vous avez fait des sauvegardes, pas de problème :
    - Réinstaller vos PC/MAC en partant de zéro, c'est la meilleure façon d'être certain de vous débarrasser de ce malware, surtout si vous n'êtes pas certain que votre antivirus ait pu éradiquer ce malware.
    - Ne brancher surtout pas votre disque de sauvegarde, tant que vous n'êtes pas absolument certain d'avoir éradiqué la menace car le ransomware pourrait crypter à son tour votre sauvegarde. La bonne méthode est de faire une sauvegarde de votre sauvegarde au cas où.
  - En l'absence de sauvegarde, il n'y a plus qu'après éradication de la menace (réinstallation), qu'a tenter de reconstituer vos données à l'aide de votre messagerie, vos fournisseurs (banques, fournisseurs d'eau, électricité, gaz, télécom…), votre famille et amis pour les photos, scanner vos documents papier …
  - -



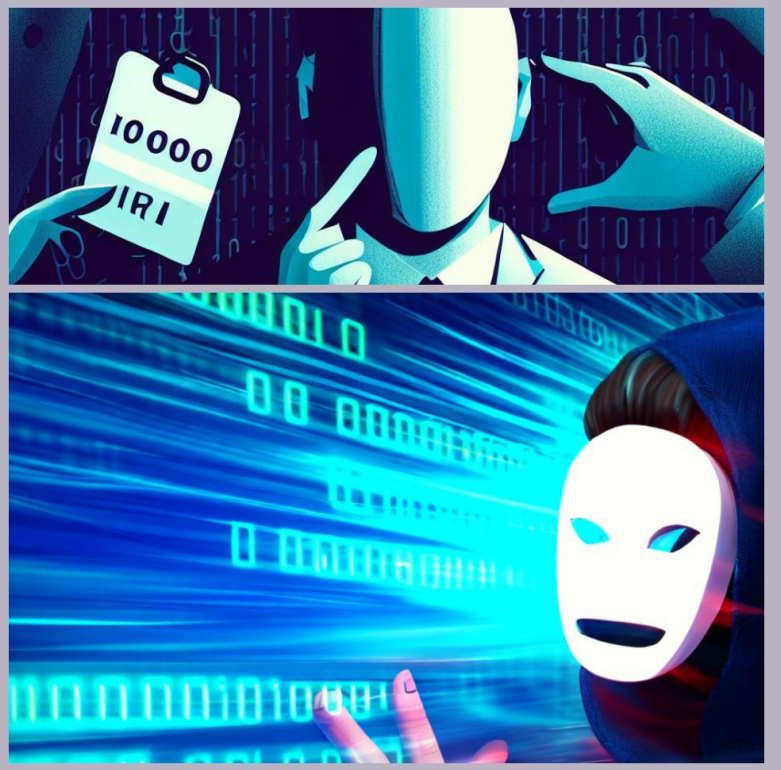


-

Windings

Vous êtes ou vous pensez être attaqué, que faire ?

- Usurpation d'identité - Agissez immédiatement :
  - Conservez les preuves : Emails, SMS, captures d'écran, relevés bancaires
  - Portez plainte contre X pour usurpation d'identité (une vraie plainte pas une main courante). La preuve est indispensable pour faire valoir votre bonne foi. Plainte au Commissariat, gendarmerie ou Procureur de la République sur la base de l'article 226-4-1 Code pénal.
  - Prévenez immédiatement vos établissements financiers et ceux qui vous gèrent et versent de l'argent (Banques, Sécurité sociale, CAF, organisme de retraite (CNAVTS, AGIRC, ARCOO…) Si cela vous arrive, il faut agir sans attendre.
    - Changez mots de passe, activez double authentification
    - Demander une nouvelle carte bancaire.
    - Verrouillez avec votre banque les prélèvements (liste blanche des émetteurs autorisés (ICS/référence de mandat) : Impôts, loyer, Electricité, Gaz, télécommunication … en fournissant les références de ces prélèvements
  - Vérifier que vous ne faites l'objet d'aucune inscription aux fichiers de la Banque de France (Fichier central des chèques (FCC) ou au Fichier des incidents de remboursement des crédits aux particuliers (FICP).
  - Signalez l'usurpation sur les sites :
    - PHAROS (internet-signalement.gouv.fr)
    - Cybermalveillance.gouv.fr
  - -



- Suivi juridique
  - Demandez la suppression des données usurpées (RGPD) ; droit prévu par le Règlement Général sur la Protection des Données : Le droit à l’effacement (“droit à l’oubli”).
  - Le RGPD (art. 17) vous donne le droit de demander à un organisme (site web, réseau social, banque, etc.) de supprimer vos données personnelles si elles sont utilisées de manière frauduleuse, illégale, ou sans votre consentement.
  - Exemple concret en cas d’usurpation d’identité : Un faux compte Facebook / Twitter / LinkedIn créé avec votre nom et photo : Vous pouvez exiger sa suppression et exiger l’effacement et le blocage.
    - "Je vous informe que mon identité est usurpée via ce compte/profil. Conformément à l’article 17 du RGPD, je demande la suppression immédiate de ces données personnelles utilisées sans mon consentement."
  - Si elles refusent ou tardent, on peut saisir la CNIL (Commission Nationale de l’Informatique et des Libertés).
  - -

Vous êtes ou vous pensez être attaqué, que faire ?

- Face aux cyberattaques : 17cyber, « le nouveau réflexe » des victimes »:
  - La France dispose d'une plateforme pour assister les particuliers, entreprises et collectivités face aux cyberattaques.
  - Objectif principal : Identifier les incidents, déposer plainte et promouvoir les bonnes pratiques contre la cybercriminalité.
  - La plateforme aide à diagnostiquer les incidents (phishing, ransomware, etc.) via un formulaire simplifié.
  - Dépôt de plainte facilité : 17cyber guide les victimes vers des outils spécialisés comme Perceval, Thesee ou Pharos.
  - Sensibilisation et prévention : Des astuces et recommandations adaptées à chaque type d'attaque sont proposées.
  - Accompagnement renforcé : Mise en relation possible avec des policiers ou gendarmes spécialisés.
  - Module intégré : Le « module 17cyber » permet d'ajouter ce service sur des sites partenaires.
  - Urgence accrue : En 2023, 278 703 infractions numériques ont été enregistrées, marquant une augmentation significative.
  - -

17Cyber - Mon assistance en ligne

Liens

- Pour renforcer votre cybersécurité, plusieurs autorités françaises proposent des ressources et des services dédiés :
  - 17Cyber : Service en ligne lancé par la Police nationale, la Gendarmerie nationale et Cybermalveillance.gouv.fr, il offre une assistance immédiate aux victimes de cyber malveillance, avec des conseils et un accompagnement personnalisé.
    https://17cyber.gouv.fr/
  - ANSSI (Agence nationale de la sécurité des systèmes d'information) : Autorité nationale en matière de cybersécurité, l'ANSSI offre des recommandations, des guides et des formations pour protéger les systèmes d'information.
    https://cyber.gouv.fr/?utm_source=chatgpt.com
  - CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) : Rattaché à l'ANSSI, le CERT-FR publie des alertes et des conseils pour faire face aux cybermenaces.
    https://www.cert.ssi.gouv.fr/?utm_source=chatgpt.com
  - Cybermalveillance.gouv.fr : Plateforme nationale d'assistance aux victimes de cyber malveillance, elle propose des outils de diagnostic, des conseils personnalisés et met en relation avec des prestataires spécialisés.
    - https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/lancement-17cyber?utm_source=chatgpt.com
  - Cyber malveillance, détection des mails frauduleux : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage
  - Thésée, Pharos ou labyrinthe / signaler des arnaques; fraudes … : https://www.plus.transformation.gouv.fr/experiences/3501349_thesee-pharos-ou-labyrinthe#:~:text=R%C3%A9ponse%20du%20service%20(THESEE)&text=Si%20vous%20souhaitez%20signalez%20un,%2Dsignalement.gouv.fr.
  - ACPR-Autorité de Contrôle Prudentiel et de Résolution https://acpr.banque-france.fr/
  - Hoaxbuster-Plateforme collaborative contre la désinformation http://www.hoaxbuster.com
  - CNIL pour savoir « comment détecter un message malveillant » https://www.cnil.fr/fr/phishing-detecter-un-message-malveillant
  - Fédération bancaire française (cybersécurité) https://www.fbf.fr/fr/mots-cles/cybersecurite/
  - AMF protection des épargnants : Page d'accueil | Protect Epargne (amf-france.org)

Ces sites officiels sont des ressources précieuses pour vous aider à prévenir et à réagir efficacement face aux cybermenaces.

Nature des Infractions pénales

- Usurpation d'identité (Art. 226-4-1 CP)
  - → 1 an prison & 15 000 € d'amende
- Accès frauduleux à un système (Art. 323-1 CP)
  - → 2 à 5 ans prison & jusqu'à 150 000 € d'amende
- Atteinte aux données (Art. 323-3 CP)
  - → 5 ans prison & 150 000 €,
  - jusqu'à 7 ans / 300 000 € en bande organisée
- Diffusion d'outils de piratage (Art. 323-3-1 CP)
  - → 5 ans prison & 150 000 € d'amende
- Escroquerie numérique / Phishing (Art. 313-1 CP)
  - → 5 ans prison & 375 000 € d'amende

- L'usurpation d'identité, piratage, fraude bancaire, phishing, escroquerie numérique, diffusion d'outils de piratage sont en droit français des **Délits.**
- Article 15-3 du Code de procédure pénale :"La police judiciaire est tenue de recevoir les plaintes déposées par les victimes d'infractions à la loi pénale et de les transmettre sans délai au procureur de la République." Cela signifie que les forces de l'ordre n'ont pas le droit de refuser une plainte.
  - Le cas échéant écrire à l'inspection générale de la Police nationale (IGPN)
  - Déposer plainte directement auprès du procureur de la République
  - Pré-plainte en ligne : Via le site officiel : www.pre-plainte-en-ligne.gouv.fr
- -

Tester vos connaissances :
https://www.cybermalveillance.gouv.fr/medias/2020/01/Quizz.pdf?utm_source=chatgpt.com

F I N

Exposé d'Alain BRARD sur la cybercriminalité en 2024, actualisé et enrichi de données et schémas générés avec l'aide de l'IA ChatGPT.