MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

*Liberté*
*Égalité*
*Fraternité*

POLICE
NATIONALE

*Direction générale de la police nationale*

*Direction interdépartementale de la police nationale de Seine-et-Marne*

*Circonscription de Police Nationale de Melun Val de Seine*

# LA POLICE NATIONALE VOUS INFORME

**Soyez vigilants en cette période de rentrée, de nouvelles escroqueries et arnaques sont au rendez-vous, depuis des années les escrocs doivent se réinventer fréquemment, et ils redoublent d'inventivité pour tenter de vous soutirer vos données personnelles et données bancaires.**

**- Nouvelle arnaque en lien avec la rentrée scolaire 2024:**
Cette dernière vise de nombreux parents, plusieurs sites frauduleux reprenant les codes des sites officiels du gouvernement, vous promettent de dévoiler la classe ou sera admis votre enfant, en compagnie de quels camarades et avec quels enseignants.
Tout cela est faux et loin d'être anodin, le seul but étant de capter vos données personnelles, pour un usage frauduleux futur.

**- Arnaque aux cartes de transports gratuites:**
Cette dernière a déjà fait de nombreuses victimes.
De fausses publicités sur les réseaux sociaux principalement, reprenant les codes de sites officiels, promettent l'obtention d'une carte de transport à usage illimité et gratuite pendant une certaine période.
Tout cela est faux, et l'escroc aura alors à sa disposition vos données personnelles et vos coordonnées bancaires qu'il pourra utiliser à des fins frauduleuses puis revendre à d'autres escrocs.

**- Arnaque à l'Intelligence Artificielle:**
- Cette arnaque est apparue cet été et se multiplie principalement dans les domaines de la réservation de voyage, l'hôtellerie et la restauration.
- Soyez très vigilants lors de vos réservations dans ces domaines, régulièrement et obligatoirement lors de la réservation de voyage vous devez communiquer les détails de votre carte de crédit et ou télécharger une pièce d'identité.
- Si le lien parait suspect, ne cliquez pas et vous avez le moindre doute, appelez la propriété, les hôtes et le service clientèle.
- Pour rester le plus en sécurité privilégiez l'authentification à deux facteurs, ce qui rend l'accès à vos informations beaucoup plus difficiles. En plus du mot de passe, vous faites vérifier votre identité grâce à un code à usage unique.

**- Arnaque au «re-scram» cette nouvelle arnaque vise des personnes déjà arnaquées:**
Des escrocs s'attaquent maintenant aux personnes déjà victimes d'arnaques, en se faisant passer pour des avocats ou des personnes travaillant sur ce genre de dossiers.
Vous venez d'être victime d'une arnaque ? Ils vous contactent directement en vous faisant miroiter une solution pour récupérer votre argent.

Leur intention est bien évidemment de vous arnaquer une seconde fois ! En se présentant comme un avocat ou un spécialiste de ce genre d'affaires. Après avoir perdu des sommes très importantes pour certaines victimes, l'escroc revient sans état d'âme, vous assurer qu'il peut vous aider concrètement à récupérer une partie de vos pertes, moyennant une somme d'argent. Problème, une fois le paiement effectué, votre argent s'envole de nouveau.

**- Nouvelle arnaque par SMS: « Bonjour, c'est le coursier, votre paquet ne rentrait pas dans votre boîte aux lettres»**

Ce message est suivi d'un lien frauduleux qui, si vous cliquez dessus et remplissez, aspirera vos données personnelles voir bancaires.

**Rappel Info Escroquerie**: 0 805 805 817 (gratuit)

**Source:** Divers médias.

# Comment vérifier la fiabilité d'un site web conseils et astuces

Avant de visiter un site web, d'en accepter les cookies, d'y réaliser un téléchargement ou un achat, il convient d'en vérifier la fiabilité, afin de ne pas être la cible d'actes malveillants.
S'assurer qu'un site est sécurisé préservera la confidentialité de vos données et vous évitera d'en télécharger un fichier compromis ou de subir une escroquerie.

## Les critères de fiabilité d'un site web:

**URL et nom de domaine :** la première étape consister à vérifier que l'URL commence bien par "**https://**", ce qui indique, a priori, une connexion sécurisée. Par exemple, sur le navigateur de Google, Chrome, vous pouvez cliquer sur l'icône tout de suite à gauche de l'URL pour obtenir des informations sur la sécurisation d'un site. Il est important de se méfier des noms de domaine qui contiennent des fautes ou des caractères inhabituels, souvent utilisés par des sites frauduleux pour tromper les utilisateurs.

**Certificats de sécurité :** un certificat SSL valide est essentiel pour la sécurité des échanges de données. En cliquant sur l'icône à côté de l'URL sur la plupart des navigateurs (souvent sous la forme d'un cadenas), il est possible de vérifier la validité du certificat SSL. Assurez-vous ainsi que celui-ci est émis par une autorité de certification reconnue, comme DigiCert ou Comodo.

**Informations de contact :** un site fiable doit afficher des informations de contact détaillées, comme une adresse mail, un numéro de téléphone ou une adresse physique. Par exemple, des sites comme Amazon ou Fnac fournissent des moyens de contact clairs, qu'il est possible de trouver dans le footer ou les mentions légales.

**Politiques de confidentialité :** pour comprendre comment vos données personnelles seront collectées, exploitées et protégées, il est judicieux de prendre soin de lire les politiques de confidentialité d'un site web. Une plateforme sérieuse détaillera ses pratiques de manière transparente.

**Réputation en ligne :** des recherches d'avis sur des plateformes comme Trustpilot ou SiteJabber permettent de connaître la réputation d'un site. Si vous envisagez d'acheter sur une boutique en ligne, les avis clients peuvent notamment vous informer de la bonne qualité du service.

## Conseils pratiques pour vérifier la fiabilité d'un site web:

Une fois compris les éléments constitutifs d'un site web fiable et sécurisé, certaines actions peuvent renforcer la protection de votre identité en ligne ou de vos appareils lorsque vous visitez différentes plateformes. En voici quelques-unes :

**Utiliser des outils de vérification :** des outils tels que Google Safe Browsing, Norton Safe Web peuvent vous aider à vérifier si un site est sécurisé, en entrant simplement l'URL à évaluer, ce qui permet d'accéder à un rapport de sécurité détaillé.

**Analyser le contenu :** un site fiable présente a minima un contenu bien rédigé et régulièrement mis à jour. Il convient de se méfier des sites avec du contenu bourré de fautes et rarement actualisé.

**Vérifier les liens et téléchargements :** en passant votre curseur sur les liens avant de cliquer dessus, vous obtiendrez un aperçu de l'URL complète. Celle-ci vous permet de vérifier en amont que la redirection ne semble pas malveillante. Quant aux téléchargements, il est préférable de s'orienter vers des sites réputés et officiels, notamment ceux des fournisseurs de solutions.

**Utiliser un bloqueur de publicité et un antivirus :** ces outils, bloqueurs de publicité et antivirus, permettent respectivement d'éviter les pop-ups intrusifs et potentiellement dangereux, et de se protéger contre des logiciels malveillants et les tentatives de phishing.

**Éviter de partager des informations sensibles :** bien sûr, ne partagez jamais vos informations personnelles ou financières sur un site dont vous ne vous êtes pas assuré de la fiabilité. Pour les paiements en ligne, il est important d'utiliser des plateformes sécurisées, qui offrent une couche de protection supplémentaire, tout comme les cartes bancaires virtuelles et temporaires.

***Lorsque vous naviguez sur le web, la vigilance reste votre meilleure alliée pour éviter d'être victime d'escroqueries ou de cyberattaques.***

**Source :** B D M  Média des professionnels du digital.