



Acheter en sécurité sur internet

Faites chauffer la carte bleue sans prendre feu

Reconnaître un site fiable

- Le cadenas  ou le bouclier  est présent dans la barre d'adresse (la connexion est sécurisée)
- L'adresse commence par https:// (le "s" signifie "sécurisé")
- Le nom du site est correct, sans faute ni variante suspecte ("fnaac.com" ou "amazon-soldes.fr" sont des faux)
- L'extension est cohérente : .fr, .com, .eu... (une extension bizarre comme .xyz ou .top est un signal d'alarme)
- Les mentions légales sont accessibles (nom de l'entreprise, adresse, contact, numéro SIRET)

Pour vérifier la réputation d'un site :

- Cherchez le nom du site + "avis" sur Google
- Consultez Trustpilot
- Méfiez-vous des sites avec uniquement des avis 5 étoiles ou des avis très récents

Les pièges à éviter

Les faux sites

Des sites copient l'apparence exacte de grandes boutiques. Tapez toujours l'adresse vous-même ou passez par Google. Vérifiez l'adresse dans la barre de navigation avant de payer.

Les offres trop belles

Un super téléphone à 50€ ? C'est suspect. Ça peut être une contrefaçon, un article jamais livré ou une copie de mauvaise qualité. Ne vous laissez pas brusquer par les "ventes flash" et comparez sur plusieurs sites. Attention aussi aux frais cachés qui n'apparaissent qu'à la dernière étape.

Les abonnements piégeux

Vous achetez une fois et sans le savoir vous souscrivez un abonnement mensuel. Lisez bien ce qui est coché avant de valider. Si vous avez souscrit sans le vouloir, contactez votre banque pour opposition.

Les vendeurs tiers

Sur Amazon ou Cdiscount, n'importe qui peut vendre. Vérifiez toujours la note et les avis du vendeur, pas seulement du produit.

Sécuriser son paiement

- Payez toujours par carte bancaire (vous pouvez contester un débit auprès de votre banque). Jamais par virement, mandat cash ou carte cadeau (ces paiements sont irréversibles).
- La page de paiement peut-être différente du site : c'est normal (elle est gérée par un prestataire spécialisé).

Sur la page de paiement, vérifiez :

- Le cadenas  est présent
- Le nom du prestataire est reconnaissable (PayPal, Stripe, Paybox, Monetico...)
- Le montant affiché est correct
- On vous demande uniquement le numéro de carte, la date d'expiration et le cryptogramme (jamais votre mot de passe bancaire ou votre code PIN)
- Vous n'avez pas cliqué sur un lien reçu par mail ou SMS pour arriver là
- Votre banque peut vous envoyer un code par SMS ou notification pour confirmer l'achat. Il n'est pas systématique mais quand il apparaît, c'est une bonne chose.

Que faire si ça tourne mal ?

- Si c'est un problème de produit ou de livraison – Contactez le vendeur : cherchez ses coordonnées dans les mentions légales. Envoyez un mail en expliquant le problème et gardez une trace écrite de tous vos échanges. Donnez-lui 48 à 72h pour répondre.
- Si c'est un problème de paiement – Contactez votre banque : signalez tout débit suspect le plus vite possible. Vous pouvez demander une opposition sur votre carte et un remboursement. Plus vous réagissez vite, plus vous avez de chances d'être remboursé.
- Si c'est une arnaque – Signalez et obtenez de l'aide auprès de cybermalveillance.gouv.fr : aide aux victimes de cybermalveillance et/ou la gendarmerie ou le commissariat : pour porter plainte (conservez toutes les preuves : captures d'écran, mails, relevés bancaires).

Internet, c'est fait pour vous aussi. Avec les bons réflexes, vous pouvez profiter de tous ses avantages l'esprit tranquille. Les escrocs misent sur la précipitation donc prenez votre temps.