www.makeuseof.com /amazon-scam-calls-stay-safe/

# Les appels frauduleux sur Amazon vous coûteront des milliers et voici comment rester en sécurité

***Les fraudeurs peuvent se faire passer pour Amazon de plusieurs manières. Voici comment les repousser, quelle que soit la méthode qu'ils utilisent.***

Simon Batt :


## Liens rapides



## Points clés à retenir

- Les appels frauduleux sur Amazon impliquent des escrocs prétendant provenir d'Amazon pour accéder à votre compte Amazon ou bancaire.
- Les fraudeurs peuvent réclamer un colis perdu ou des achats coûteux pour vous inciter à leur fournir votre compte ou vos coordonnées bancaires.
- Méfiez-vous de toute personne demandant des informations personnelles par téléphone, raccrochez et contactez directement Amazon pour confirmer si l'appel était légitime.

Les fraudeurs adorent se faire passer pour de grandes entreprises bien connues, et Amazon ne fait pas exception.

Vous pouvez recevoir un appel d'une personne prétendant appartenir à Amazon et faire des déclarations

effrayantes à propos de votre compte.
Alors, que sont les appels frauduleux sur Amazon et comment les identifier ?

## Que sont les appels frauduleux sur Amazon ?


Un appel frauduleux sur Amazon se produit lorsqu'un escroc qui n'est pas d'Amazon vous appelle et prétend travailler pour l'entreprise.
Il existe de nombreux types d'appels frauduleux sur Amazon, mais ils souhaitent généralement accéder à votre compte Amazon ou à votre compte bancaire.

L'escroc obtient vos informations de deux manières.
Soit vous donnez les détails vous-même, soit l'escroc vous convainc d'installer une application d'accès à distance et il accède à vos comptes via votre propre PC.

Une fois que l'escroc a accès à l'un de ces comptes (ou parfois aux deux), il peut effectuer d'énormes achats en utilisant votre argent.
En tant que tel, il est très important de savoir à quoi ressemble un appel frauduleux sur Amazon et comment l'éviter.

## Comment se présente un appel frauduleux sur Amazon ?

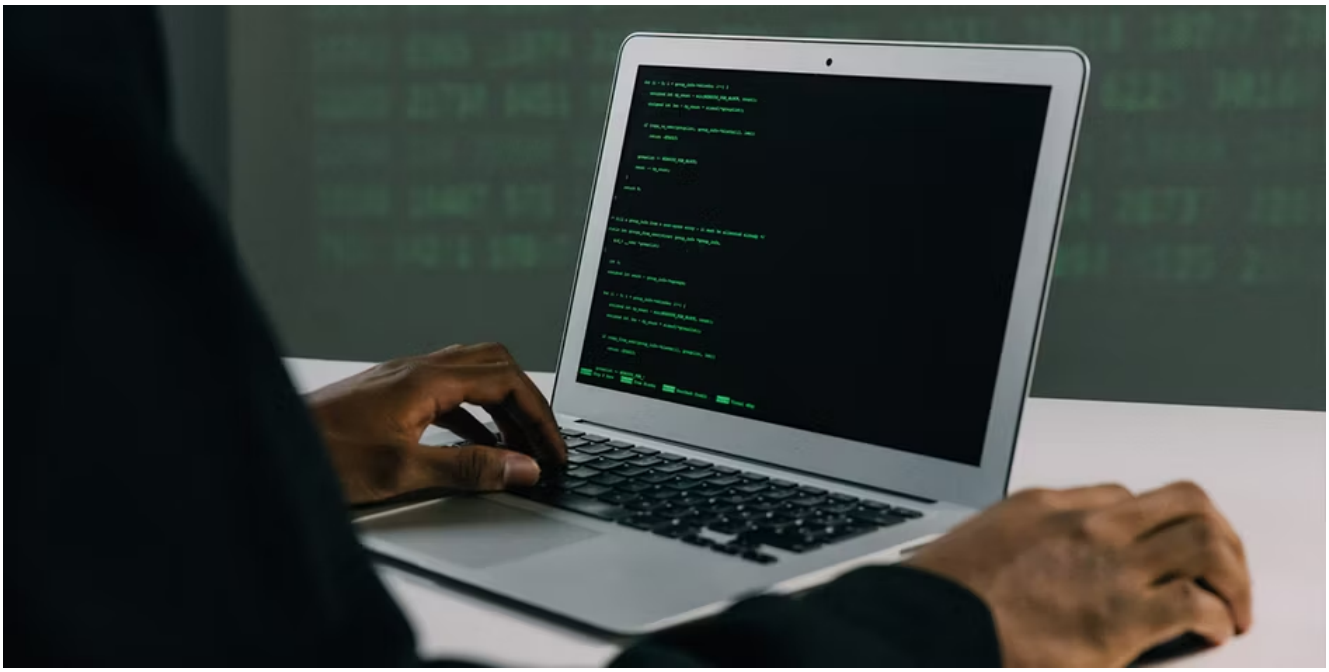
Les appels frauduleux sur Amazon peuvent se produire de différentes manières. Voici les méthodes les plus courantes utilisées par les fraudeurs.

### 1. Réclamer une livraison Amazon perdue


L'escroc pourrait prétendre qu'un colis que vous avez commandé sur Amazon s'est perdu dans le courrier. Il existe déjà un système en place pour gérer si votre commande Amazon n'arrive jamais, mais l'escroc proposera sa propre solution.

Ils peuvent soit demander les détails de votre compte Amazon afin de « suivre le colis », soit demander les détails de votre compte Amazon afin de « suivre le colis ». ou ils peuvent demander vos coordonnées bancaires afin de pouvoir « traiter un remboursement » ; pour l'objet perdu.

## 2. Réclamer qu'un pirate informatique a effectué des achats coûteux sur votre compte

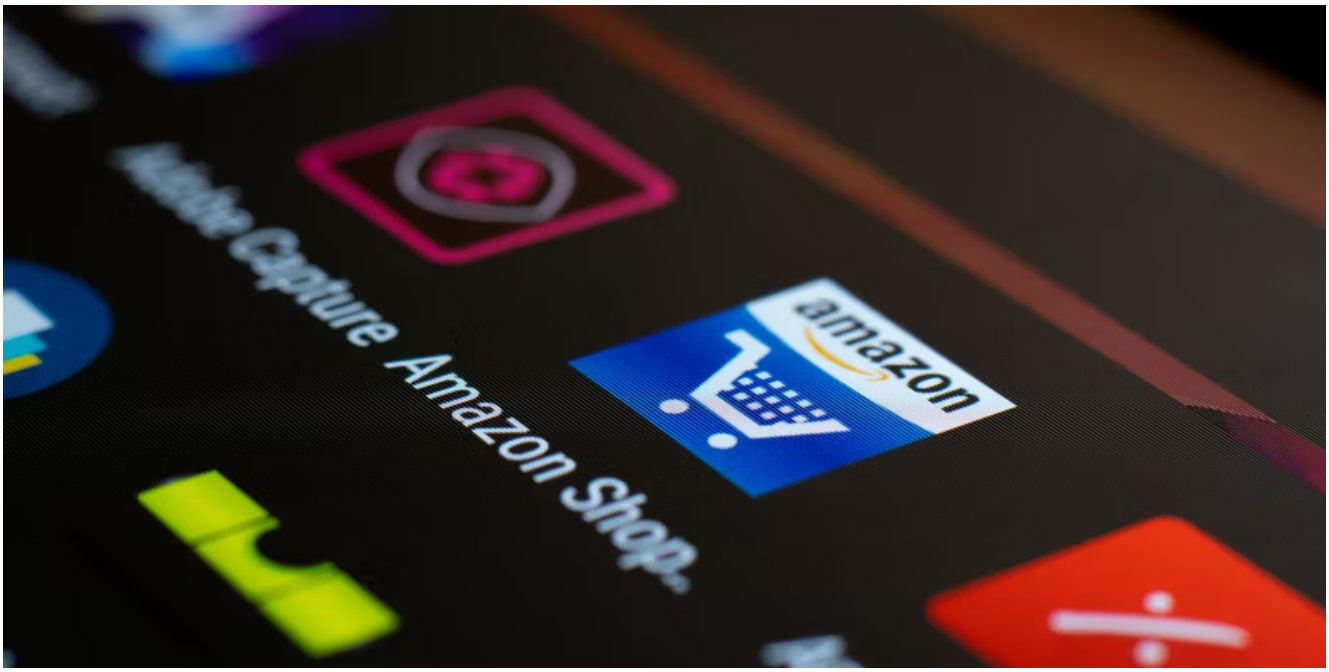


Un appel frauduleux sur Amazon peut prétendre qu'un pirate informatique a violé votre compte Amazon et dépensé votre argent en biens.
Ils mentionneront généralement un article coûteux, comme un iPhone.

Bien entendu, vos comptes sont en sécurité et personne n’a rien commandé sur votre compte.
L’arnaque repose sur votre panique et votre acceptation de leur solution.
Cela peut inclure l'autorisation d'accéder à votre compte Amazon pour annuler la commande ou l'obtention des coordonnées de votre compte bancaire afin qu'ils puissent « rembourser ». l'argent.

Dans certains cas signalés, l'escroc vous demandera d'installer un outil d'accès à distance afin que le « spécialiste de la fraude » puisse accéder à votre compte. peut annuler la commande de votre côté.
Si vous faites cela, l'escroc peut alors accéder à vos autres comptes via votre PC et effectuer des achats indésirables.

## 3. Affirmer que quelque chose ne va pas avec votre compte




Parfois, l'escroc prétendra que quelque chose ne va pas avec votre compte Amazon.
Ils vous demanderont ensuite vos coordonnées pour vous aider à résoudre le problème.

Dans certains cas, l’escroc prétend devoir mettre à jour vos informations personnelles. D'autres fois, ils prétendront qu'un pirate informatique a tenté d'accéder à votre compte. Ils doivent donc effectuer un contrôle de sécurité pour s'assurer que vous êtes le propriétaire légitime du compte.

Quelle que soit la méthode utilisée, l’escroc vous demandera alors vos informations personnelles, telles que vos informations de connexion, vos coordonnées bancaires et votre adresse.

## 4. Le prix de la réclamation de votre abonnement Amazon Prime augmentera


Dans cette arnaque, un escroc vous appelle et prétend que le prix de votre abonnement Amazon Prime est sur le point d'augmenter.
Ils proposent généralement une augmentation drastique du prix, en espérant que vous demanderez l'annulation de votre abonnement.

Si vous le faites, l'escroc "guidera" alors votre entreprise. vous tout au long du processus d'annulation de votre abonnement Amazon Prime.
Cela implique soit de demander les détails de votre compte afin qu'ils puissent l'annuler, soit de vous demander de télécharger une application d'accès à distance afin qu'ils puissent le faire pour vous.

## Comment identifier un véritable appel Amazon

Ces escroqueries peuvent sembler effrayantes, mais certains signes révélateurs vous indiqueront si quelqu'un vient d'Amazon ou non.

### Ne faites jamais aveuglément confiance aux affirmations d'un escroc

Si quelqu'un vous parle d'une commande Amazon et prétend que vous l'avez passée, mais que vous n'attendez pas de commande d'Amazon, c'est un signe évident que vous parlez à un escroc.
Ne présumez pas que vous avez simplement oublié une commande que vous avez déjà passée ; raccrochez simplement le téléphone et ignorez-le.

### Amazon ne demandera jamais d'informations sensibles

Amazon n'a pas besoin de vous demander le mot de passe de votre compte.
Votre mot de passe vous est fourni pour accéder à votre compte ; **Amazon n'a pas besoin de votre mot de passe pour accéder à vos données ou mettre à jour quelque chose sur votre compte.**

De même, Amazon ne vous demandera jamais vos coordonnées bancaires.
Si vous achetez des choses sur Amazon, vos informations de paiement sont déjà enregistrées sur votre compte.
Si Amazon souhaite vous rembourser quelque chose, il vous renverra généralement le paiement via la méthode que vous lui avez fournie.

Ainsi, si quelqu'un au téléphone vous demande le mot de passe de votre compte Amazon ou vos coordonnées bancaires, il s'agit bien d'une arnaque.
Ne leur donnez aucune information et raccrochez immédiatement.

## En cas de doute, raccrochez et vérifiez auprès d'Amazon

Les escrocs sont experts dans l'art de semer la panique. Ils utiliseront des tactiques de peur pour vous faire penser de manière irrationnelle et faire des choses que vous ne feriez pas normalement.

Si vous avez identifié les signes révélateurs, vous êtes au téléphone avec un escroc, mais vous êtes au téléphone.
Si vous avez peur de raccrocher (au cas où ils seraient légitimes), faites-le quand même. Ensuite, visitez l'Support Amazon et parlez-y à un professionnel.
Expliquez le sujet de l'appel et ce qui a été dit.

Si l'appel était légitime, l'agent d'assistance peut identifier le problème et vous aider dans les étapes.
Si ce n'était pas le cas, l'agent devrait vous rassurer sur le fait qu'il s'agissait d'une arnaque et vous rassurer.

Grâce à ces conseils, vous êtes désormais plus que prêt à faire face à tout appel frauduleux sur Amazon. Gardez la tête froide, ne divulguez pas d'informations personnelles et vous devriez vous en sortir contre les fraudeurs.

*Recherche et mise en page par:*
*Michel Cloutier*
*CIVBDL*
*20240116*
*"C'est ensemble qu'on avance"*