AIRNITE

# ZERO DAY

NUMÉRO 15/2026 · MARKETING & SEO

# Qui tient le compte tient l’argent : comment les escrocs visent les comptes Amazon

En 2025, Amazon a fait fermer plus de 70 000 sites de phishing, et plus d’une arnaque signalée sur quatre visait l’accès aux comptes. Dès 2018, des attaquants ont détourné une centaine de comptes vendeurs. Les leçons pour vendeurs et clients.

Publié le: 21 novembre 2026 Temps de lecture: 5 min Auteur: Rédaction Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUATION EN CHIFFRES

**28 %**
**arnaques visant l'accès au compte**
part des usurpations d'Amazon signalées en 2025 (Amazon)

**70 000+**
**sites de phishing fermés**
fermetures engagées par Amazon en 2025

**14 000+**
**numéros de téléphone bloqués**
en 2025, selon Amazon

**≈ 100**
**comptes vendeurs détournés**
de mai à octobre 2018 (Engadget d'après Bloomberg)

Un compte Amazon, c'est plus qu'une liste de commandes. Pour les clients, il contient des moyens de paiement ; pour les vendeurs, tout leur chiffre d'affaires. Pas étonnant que des escrocs se fassent passer pour Amazon afin d'obtenir des identifiants.

## // Que s'est-il passé ?

Amazon publie lui-même des chiffres : parmi toutes les arnaques usurpant l'identité d'Amazon signalées par ses clients dans le monde en 2025, **28 %** visaient à accéder à des comptes clients. Selon Amazon, l'entreprise a fait fermer en 2025 **plus de 70 000 sites de phishing** et **plus de 14 000 numéros de téléphone** ; un site de phishing signalé peut souvent être supprimé en quelques heures.

Un cas plus ancien montre que les vendeurs sont aussi visés. Selon Engadget, qui s'appuyait sur Bloomberg et des documents judiciaires, Amazon a signalé en 2019 une campagne « sérieuse » : entre mai et octobre 2018, **une centaine de comptes vendeurs** ont été compromis. Les attaquants ont modifié des coordonnées et détourné de l'argent issu des ventes et de prêts. Amazon n'a pas commenté les détails, mais a rappelé que ce type d'incident peut résulter de phishing.

## // Comment fonctionne l'attaque ?

Le schéma est classique : un e-mail, un SMS ou un appel se fait passer pour Amazon – avec un prétendu problème de commande, de paiement ou de compte. Un lien mène à une page de connexion trompeusement authentique. Quiconque y saisit ses identifiants les livre aux escrocs.

Pour les comptes vendeurs, le préjudice est particulièrement lourd. Une fois connectés, les attaquants peuvent modifier les coordonnées bancaires de versement, manipuler les offres ou utiliser le compte pour escroquer des acheteurs. La réutilisation des mots de passe les aide souvent : un mot de passe volé ailleurs ouvre alors aussi le compte Amazon.

## // Qui est concerné ?

Les clients d'Amazon sont concernés, tout comme les vendeurs de la place de marché – de l'entrepreneur individuel à la marque disposant de sa propre agence. Pour les vendeurs s'ajoute un facteur : plusieurs personnes accèdent souvent au compte – salariés, prestataires, agences. Chacun de ces accès est une porte d'entrée possible s'il n'est pas bien protégé.

## // Que faire maintenant ?

Amazon conseille de vérifier les messages via ses propres comptes et applications plutôt que par des liens, et de signaler les cas suspects. Pour les vendeurs s'y ajoutent la vérification en deux étapes pour tous les accès, des utilisateurs distincts au lieu de mots de passe partagés et un contrôle régulier des coordonnées bancaires. La check-list ci-dessous résume les étapes.

## // Comment Airnite vous aide-t-il ?

Airnite gère des **présences sur Amazon** – comme pour notre référence Caribee – et sécurise le compte vendeur dès le départ : accès, rôles, notifications. En **formation**, votre équipe apprend à reconnaître les faux messages Amazon. En **conseil**, nous vérifions qui a aujourd'hui accès à votre compte et faisons le ménage.

> Remarque : le cas de 2018 provient d'articles de presse sur des documents judiciaires ; selon nos recherches, Amazon ne publie pas de chiffres actuels sur les comptes vendeurs détournés. État de la recherche : 21 novembre 2026.

## Check-list : ce qu'il faut faire maintenant

[+] Activer la vérification en deux étapes pour tous les comptes Amazon – clients et vendeurs.

[+] N'ouvrir Seller Central que via un favori, jamais via des liens reçus par e-mail ou SMS.

[+] Créer des utilisateurs distincts avec les droits adaptés pour les équipes et agences au lieu de partager les identifiants.

[+] Vérifier régulièrement les coordonnées bancaires et de versement et activer les notifications de modification.

[+] Vérifier les messages prétendument envoyés par Amazon uniquement dans le compte lui-même et signaler les cas suspects à Amazon.

[+] Utiliser un mot de passe fort et unique par compte – les mots de passe réutilisés sont une porte d'entrée fréquente.

## Comment Airnite vous aide

- Gestion Amazon – Fiches produits, univers visuel et suivi de votre présence Amazon.
- Formations – Votre équipe apprend nos outils et méthodes.
- Conseil – Un regard extérieur sur vos projets.

## Votre compte vendeur est-il aussi protégé que votre chiffre d’affaires ?

Airnite gère votre présence sur Amazon et sécurise en même temps le compte vendeur : vérification en deux étapes, droits utilisateurs propres pour l’équipe et les agences, coordonnées bancaires contrôlées et alertes en cas de modification. Nous formons votre équipe à repérer les faux messages Amazon.

**Demander un premier échange · Écrire un e-mail · Par WhatsApp**

### Contact

Des questions sur cet article ? Écrivez-nous sur WhatsApp : +49 174 6834842

Lire en ligne: https://airnite.de/fr/magazine/comptes-amazon-phishing-protection-vendeurs/

## Sources

Chaque fait de cet article repose sur les sources ci-dessous. Les sources primaires sont signalées.


1. **Amazon · 6 tips to help you spot and avoid scams impersonating Amazon** · 07/07/2025, mise à jour 20/11/2026 · SOURCE PRIMAIRE
   Source primaire : 28 % des arnaques signalées visant l’accès au compte, plus de 70 000 sites de phishing, plus de 14 000 numéros, conseils
   https://www.aboutamazon.com/news/retail/how-to-avoid-amazon-scams

2. **Engadget · Hackers stole cash from 100 Amazon sellers in 'serious' fraud** · 08/05/2019
   Presse spécialisée (d’après Bloomberg et des documents judiciaires) : une centaine de comptes vendeurs détournés en 2018
   https://www.engadget.com/2019/05/08/amazon-seller-hack/


*Information éditoriale générale, sans conseil juridique ni examen individuel de vos systèmes. État : date de publication.*


Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de