AIRNITE

ZERO DAY

ISSUE 15/2026 · MARKETING & SEO

Whoever has the account has the money: how fraudsters target Amazon accounts

In 2025, Amazon had more than 70,000 phishing websites taken down, and more than one in four reported scams targeted account access. Back in 2018, attackers hijacked around 100 seller accounts. What sellers and customers can learn.

Published: 21 November 2026 Reading time: 5 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

28%
scams targeting account access
share of reported Amazon impersonation scams in 2025 (Amazon)

70,000+
phishing websites taken down
takedowns initiated by Amazon in 2025

14,000+
phone numbers taken down
2025, according to Amazon

≈ 100
seller accounts hijacked
May to October 2018 (Engadget, citing Bloomberg)

An Amazon account is more than an order list. For customers it holds payment details; for sellers, their entire revenue. No wonder fraudsters deliberately pose as Amazon to get hold of credentials.

// What happened?

Amazon itself publishes figures on this: of all scams impersonating Amazon reported by customers worldwide in 2025, **28%** involved attempts to gain access to customer accounts. According to Amazon, in 2025 it initiated the takedown of **more than 70,000 phishing websites** and **more than 14,000 phone numbers**; reported phishing sites can often be taken down within a few hours.

An older case shows that sellers are targeted too. According to Engadget, citing Bloomberg and court filings, Amazon reported a "serious" campaign in 2019: between May and October 2018, **around 100 seller accounts** were compromised. The attackers changed account details and drained money from sales and loans. Amazon declined to comment on the details but pointed out that such incidents can happen through phishing.

// How does the attack work?

The pattern is classic: an email, text message or call poses as Amazon – with a supposed problem with an order, a payment or the account. A link leads to a deceptively genuine login page. Anyone entering credentials there hands them to the perpetrators.

The damage is particularly large for seller accounts. Once inside, attackers can change payout bank details, manipulate listings or misuse the account to defraud buyers. Password reuse often helps the perpetrators: a password stolen from another service then also opens the Amazon account.

// Who is affected?

Amazon customers are affected as well as sellers on the marketplace – from sole traders to brands with their own agency. For sellers there is an extra factor: often several people access the account – staff, service providers, agencies. Each of these accesses is a potential way in if it is not properly protected.

// What should you do now?

Amazon advises verifying messages through its own accounts and apps rather than via links, and reporting suspicious cases. For sellers, add two-step verification for all access, separate users instead of shared passwords and regular checks of stored bank details. The checklist below sums up the steps.

// How does Airnite help?

Airnite manages **Amazon presences** – as with our reference Caribee – and secures the seller account from the start: access, roles, notifications. In **training**, your team learns to recognise fake Amazon messages. In **consulting**, we check who currently has access to your account and clean up.

> Note: the 2018 case comes from press reports on court filings; according to our research, Amazon does not publish current figures on hijacked seller accounts. Research status: 21 November 2026.

Checklist: what to do now

[+] Enable two-step verification for all Amazon accounts – customer and seller accounts.

[+] Open Seller Central only via a bookmark, never via links in emails or text messages.

[+] Set up staff and agencies as separate users with appropriate permissions instead of sharing credentials.

[+] Regularly check stored bank details and payout data and enable change notifications.

[+] Verify messages that supposedly come from Amazon only within the account itself and report suspicious cases to Amazon.

[+] Use a separate, strong password for each account – reused passwords are a common way in.

How Airnite helps

- Amazon Management – Product pages, imagery and care for your Amazon presence.
- Training – Your team learns our tools and processes.
- Consulting – An outside view of your plans and projects.

Is your seller account as protected as your revenue?

Airnite manages your Amazon presence and secures the seller account at the same time: two-step verification, clean user permissions for team and agencies, verified bank details and alerts on changes. We train your team to spot fake Amazon messages.

Request an initial call · Send an email · Via WhatsApp

Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/amazon-accounts-phishing-seller-protection/

Sources

Every fact in this article is based on the sources below. Primary sources are marked.

1. **Amazon · 6 tips to help you spot and avoid scams impersonating Amazon** · 7 Jul 2025, updated 20 Nov 2026 · PRIMARY SOURCE
   Primary source: 28% of reported scams targeting account access, 70,000+ phishing sites, 14,000+ phone numbers, tips
   https://www.aboutamazon.com/news/retail/how-to-avoid-amazon-scams
2. **Engadget · Hackers stole cash from 100 Amazon sellers in 'serious' fraud** · 8 May 2019
   Trade press (citing Bloomberg and court filings): around 100 hijacked seller accounts in 2018
   https://www.engadget.com/2019/05/08/amazon-seller-hack/

General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.

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