

ASOS Data Breach: Are Your Details Safe? - Panda Security

By Emil Bachev

Published: 2026-10-12 · Archived: 2026-10-30 02:01:15 UTC

Hackers breached ASOS, a UK-based global online fashion retailer with many customers in the USA, earlier this month. The [hackers](#) stole the names, addresses, DOBs, and contact information of millions of ASOS customers. While the exact number of affected customers remains unknown, the fashion powerhouse has tens of millions of customers, with about 20% of its traffic coming from the USA. The ASOS leadership acknowledged the breach after many customers sounded the alarm on **social media after receiving unauthorized push notifications** on their smartphones. The cybercriminals used the notification to wreak havoc and to disclose that they had compromised customers' details. The hackers threatened to leak the stolen information unless ASOS agreed to "engage with them," likely **demanding a ransom in return**.

Key takeaways

- ASOS suffered a data breach in which hackers stole the names, addresses, DOBs, and contact details of millions of customers.
- ASOS affected millions of Americans, as the company serves millions of US customers and operates a warehouse in Dallas, Texas.
- Attackers used social engineering to steal employee credentials and demanded a ransom.
- Stolen data can enable future phishing attacks and may appear on the dark web.

Were any Americans affected by the ASOS data breach?

Yes, **Americans were affected**. The online fashion retailer has a fulfillment warehouse in Texas and millions of customers in the USA, who use its US website and recently launched app. The fashion app is on both the Google Play Store and the App Store, ranks in the top **40 most-downloaded apps on the App Store** shopping chart, and has 10+ million downloads on the Google Play Store. The online fashion retailer also has a strong presence in other countries, including its home country, the United Kingdom, and Australia.

How did the criminals compromise ASOS, and who is behind the attack?

The hackers penetrated ASOS through [social engineering](#). ASOS admitted that the fraudsters successfully impersonated a **trusted contact and obtained login credentials** to its systems. Once inside, they downloaded sensitive information and approached the fashion company for ransom. The cybercriminal group **Xuanyewen** (@xuanyegroup), which has previously used the names JohnCZ (@JohnCzwartacki) and Moon Transfers (@NFTmoonstock) on Telegram, appears to be behind the attack. However, while the motive is clear, as the **fraudsters are after monetary gains**, the exact location of the attackers and their real identity remain unknown.

What can the criminals do with the stolen information?

Criminals can use the **stolen information for future attacks**. Data from company leaks and breaches often remains on the internet forever, and many data points rarely change, such as names and DOBs, meaning that years from now people might receive highly personalized, hard-to-spot malicious emails, [text messages](#), or even phone calls that could cause trouble.

Even if ASOS satisfied the hackers' requests, there is no guarantee those details won't end up on the [dark web](#), since cyber thieves have no moral compass. Data breaches happen often, and hackers use **stolen information for nefarious purposes**. Smartphone users should protect their devices by installing [antivirus software](#) on all connected devices. An **extra layer of security is often what deters hackers** from successfully utilizing stolen data to commit fraud.

- [cybersecurity](#)
- [privacy](#)
- [protection](#)

Emil Bachev is a tech communications expert specializing in cybersecurity and technology. With nearly two decades of experience, he creates content and campaigns that make complex tech topics clear and engaging.

He has worked with leading brands such as NVIDIA, Fortinet, ASUS, and Panda Security, helping communicate technology to global audiences.

Source: <https://www.pandasecurity.com/en/mediacenter/global-online-retailer-asos-hacked/>