A security notice from Ultrahuman about your account

ULTRAHUMAN

Hi there,

I’m Mohit, founder & CEO of Ultrahuman. On 27 March 2026, we had a security incident, but the most important facts first: no passwords, card details, or payment data were involved, and we have found no evidence of misuse. Here is the full account what occurred, the information involved, and the steps we have taken in response.

WHAT HAPPENED

On 27 March 2026, an unauthorised third-party gained read-only access to an internal system used for internal analytics. The access was constrained in scope by the system's design, which did not permit modification or deletion of data. We identified the incident promptly, took the affected system offline, and revoked all access.

WHAT INFORMATION WAS AND WAS NOT INVOLVED

For your account, the affected dataset contained your contact and account details, your order and transaction history, and some fitness related data associated with your product usage and purchases.

No passwords, payment or credit card information were accessible or affected by this incident. Your Ultrahuman Ring continues to operate normally and to record accurate wellness information.

STEPS WE HAVE TAKEN

After identifying the incident, we immediately took the affected system offline and revoked all access. We have since implemented the following remediation measures:

1. Strengthened access control policies across internal systems, including least-privilege access reviews.
2. Hardened endpoint security on all employee devices, with stricter configuration controls and continuous monitoring.
3. Increased the frequency of periodic access audits across internal tooling.
4. Deployed export-volume anomaly detection and alerting on internal systems.

We have also conducted active monitoring of public and other internet channels for any evidence of the publication or further misuse of the accessed information. To date, we have not identified any such publication or misuse.

WHAT YOU SHOULD DO

As a precaution, and as is standard practice after any incident, be alert to phishing attempts. If you receive any unexpected email, SMS, or telephone call referencing Ultrahuman, your orders, or your personal data, please treat it with caution, particularly where it conveys urgency or requests that you click a link.

Ultrahuman will not ask you to confirm your password, payment details, or any other personal information by email or SMS.

CONTACT US

For questions, write to security-2026@ultrahuman.com with the subject line "Security Incident." Our team is standing by. More information at ultrahuman.com/legal/notice-march-2026.

We take this incident seriously. The measures we have taken are designed to prevent a recurrence, and we remain committed to earning your trust every day.

Mohit Kumar
Founder & CEO, Ultrahuman