



What Actually Happened?



On September 20, 2025, attackers accessed a third-party customer support provider, not Discord's core systems.

Discord disclosed the breach on Oct 3 and updated on Oct 8, confirming that passwords and authentication tokens were not affected.



What's at Risk (and What's Not)

Exposed data includes names, usernames, emails, IP addresses, payment type, last 4 digits of cards, support chat messages, and some internal materials. A small subset of age-verification IDs may have been exposed.

Safe data includes full card numbers, CVVs, private DMs, and passwords.

RISK / EXPOSED



SAFE





Am I Impacted?

Here's How to Know



Users most impacted are those who opened support tickets or contacted Trust & Safety, especially for age-verification.

Discord will only contact users via noreply@discord.com, and media reports indicate Zendesk as the affected vendor.

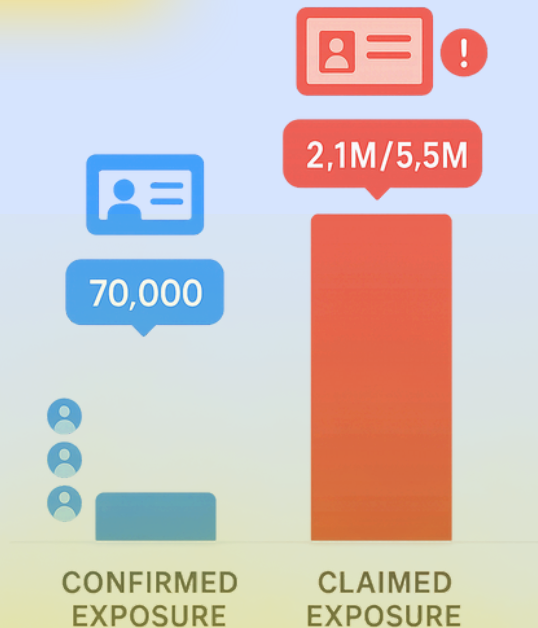


Reality Check: Confirmed vs. Claimed

Discord confirmed that
~70,000 users may have
had ID photos exposed.

Attackers claimed 2.1M
photos and 5.5M users, likely
exaggerated for ransom.

Discord has notified all
affected users and ended
work with the compromised
vendor.

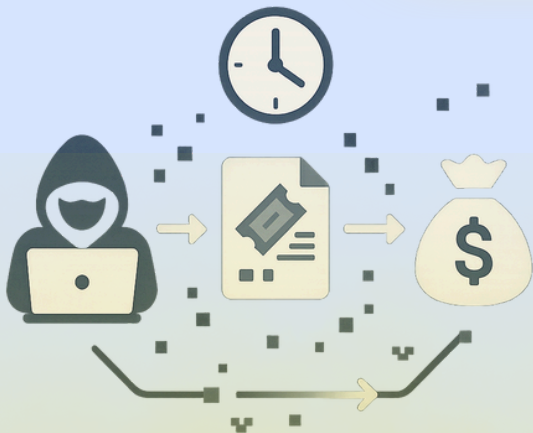




Inside the Attack (From Early Reporting)

The breach reportedly started through a compromised Zendesk support account, lasting approximately 58 hours.

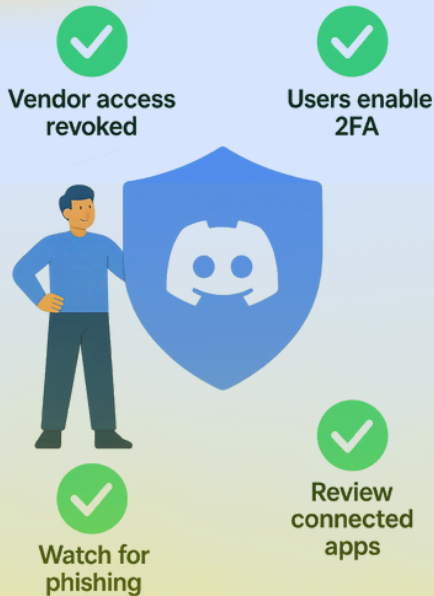
Attackers allegedly accessed support tickets and attachments, demanding a \$5M ransom, later reduced to \$3.5M. Details remain unconfirmed by Discord.





Discord's Response and Your Next Steps

Discord revoked the vendor's access, engaged forensics, notified authorities, and reviewed third-party controls. Users should enable 2FA, monitor accounts, watch for phishing, and review connected apps or bots.





Thank you!