# AL2025_49 Discord Support-Ticket Breach Exposes User Data (October 7th, 2025)

## Description

Discord disclosed that an unauthorized party gained limited access to a third-party customer service/ticketing system used by Discord, exposing support tickets and associated user data for a subset of users. Exposed information may include names, usernames, email addresses, IP addresses, partial billing details (payment type and last four card digits), messages and attachments sent to support, and a small number of government ID images submitted for age verification. Discord has revoked the provider's access and is notifying impacted users.

## Attack Details

- The incident occurred on September 20, 2025, and involved a third-party customer support provider's access to Discord's ticketing system.
- The attacker attempted to extort Discord by demanding a ransom in exchange for not leaking the stolen support-ticket data.
- Data types accessed include contact details, support messages, IP addresses, purchase history and partial payment data, and a limited number of scanned government IDs for users who submitted them during age-verification appeals.
- Discord states the platform itself was not directly breached and that full credit card numbers and account passwords were not accessed.

## Remediation

- **Enable MFA:** Turn on multi-factor authentication for all important accounts (email, social, admin consoles).
- **Be vigilant for phishing/extortion:** Do not respond to ransom or extortion attempts; verify any unexpected support contact via the vendor's official channels.
- **Verify notifications:** Confirm official communications come from verified domains (e.g., noreply@discord.com) before acting.
- **Review & secure accounts:** Check active sessions/devices and sign out unknown sessions; rotate passwords and OAuth/app tokens if you suspect exposure.
- **Use unique passwords & password managers:** Ensure all accounts use strong, unique passwords.
- **Monitor financial and identity risk:** If identity documents were submitted, monitor financial accounts and consider fraud alerts with banks/credit providers.

- **Scan & patch devices:** Run anti-malware scans and ensure operating systems, browsers, and security software are up to date.
- **Audit third-party access:** Review and revoke unnecessary third-party vendor integrations; enforce least privilege for vendor accounts.
- **Rotate credentials & keys:** Immediately rotate service credentials, API keys, vendor tokens, and any shared secrets used with the affected vendor.
- **Increase monitoring & detection:** Review authentication and access logs for suspicious activity, enable alerts for anomalous logins and data-exfiltration indicators.
- **Protect backups:** Isolate and harden backup systems, ensure strong credentials and immutability where possible, and test restores.
- **Awareness & training:** Brief staff on this incident and reinforce guidance on handling PII, downloading files, and reporting suspicious contacts.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

**References**


- Ilascu, I. (2025, October 4). Discord discloses data breach after hackers steal support tickets. BleepingComputer. Retrieved from https://www.bleepingcomputer.com/news/security/discord-discloses-data-breach-after-hackers-steal-support-tickets/

- Discord. (2025, October 3). Update on a Security Incident Involving Third-Party Customer Service. Discord Press Releases. Retrieved from https://discord.com/press-releases/update-on-security-incident-involving-third-party-customer-service