Discord Data Breach Exposes Sensitive User Information in Thirdâ€‘Party Hack

December 30, 2025 - Discord, a popular chat app used by about 150 million people every month, has confirmed a data breach that exposed personal information from thousands of users. The breach happened not through Discordâ€™s own servers, but through a third party company that helps handle customer support. The hackers were able to access messages between users and support agents, usernames, email addresses, IP addresses, and in some cases, images of government-issued IDs.

Discord is best known among gamers, but today it is used by many different communities, including sports fans, students, and online hobby groups. It lets users communicate by text, voice, or video, and create private or public chat groups called servers.

The breach happened in October when Discord found out that hackers had gained access to a customer support partner's system. About 70,000 users were affected. Many of them had uploaded ID photos as part of an age verification process. These documents are especially sensitive and can be used in identity theft scams.

Security experts say this is an example of a growing problem in cybercrime. Even if a company has strong security, hackers may go after third party services that are not as well protected. In this case, the attackers reportedly tried to pressure Discord by threatening to leak the stolen data.

Discord responded by cutting off access to the third party vendor, launching an investigation with cybersecurity experts, and notifying law enforcement. They also began emailing users whose information was exposed.

The company said that passwords and full credit card numbers were not taken. Still, even partial billing data and ID images can be dangerous in the wrong hands. Criminals often use this kind of information to open fake accounts or steal money from victims.

If you use Discord and submitted an ID for any reason, check your email for a notice from the company. Experts recommend changing your password, turning on two-factor authentication, and watching for any suspicious activity in your accounts.

by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS