PAYPAL ACCOUNTS BREACHED

Published By Bleepingcomputer.com I Bill Toulas I Jan. 19, 2023

PayPal accounts breached in large-scale credential stuffing attack. Close to 35,000 users impacted.

PayPal is sending out data breach notifications to thousands of users who had their accounts accessed through credential stuffing attacks that exposed some personal data.

Credential stuffing are attacks where hackers attempt to access an account by trying out username and password pairs sourced from data leaks on various websites. This type of attack relies on an automated approach with bots running lists of credentials to "stuff" into login portals for various services. Credential stuffing targets users that employ the same password for multiple online accounts, which is known as "password recycling."

PayPal explains that the credential stuffing attack occurred between December 6 and December 8, 2022. The company detected and mitigated it at the time but also started an internal investigation to find out how the hackers obtained access to the accounts. By December 20, 2022, PayPal concluded its investigation, confirming that unauthorized third parties logged into the accounts with valid credentials.

The electronic payments platform claims that this was not due to a breach on its systems and has no evidence that the user credentials were obtained directly from them. According to the data breach reporting from PayPal, 34,942 of its users have been impacted by the incident. During the two days, hackers had access to account holders' full names, dates of birth, postal addresses, social security numbers, and individual tax identification numbers.

Transaction histories, connected credit or debit card details, and PayPal invoicing data are also accessible on PayPal accounts. PayPal says it took timely action to limit the intruders' access to the platform and reset the passwords of accounts confirmed to have been breached. Also, the notification claims that the attackers have not attempted or did not manage to perform any transactions from the breached PayPal accounts.

Impacted users will receive a free-of-charge two-year identity monitoring service from Equifax.

The company strongly recommends that recipients of the notices change the passwords for other online accounts using a unique and long string. A good password is at least 12-characters long and includes alphanumeric characters and symbols.

Moreover, PayPal advises users to activate two-factor authentication (2FA) protection from the 'Account Settings' menu, which can prevent an unauthorized party from accessing an account, even if they have a valid username and password.

What should I do if my identity is stolen?

Contact your financial institution immediately and alert it to the situation.
Visit IdentityTheft.gov to see if your identity has been misused, and how to report
and recover from identity theft.