UC San Diego Health discloses data breach after phishing attack

bleepingcomputer.com/news/security/uc-san-diego-health-discloses-data-breach-after-phishing-attack/

Sergiu Gatlan

By
Sergiu Gatlan

- July 27, 2021
- 04:06 PM
- 0

UC San Diego Health, the academic health system of the University of California, San Diego, has disclosed a data breach after the compromise of some employees' email accounts.

UC San Diego Health is one of the nation's best hospitals, being repeatedly ranked as the best health care system in San Diego, according to the 2021-2022 U.S. News & World Report survey.

The health system operates UC San Diego Medical Center, Jacobs Medical Center, and Sulpizio Cardiovascular Center under one license, with a total capacity of 808 beds.

When asked for additional details regarding the data breach, UC San Diego Health's Executive Director of Communications and Media Relations Jacqueline Carr told BleepingComputer that the breach was the result of a phishing attack.

Personal info of patients, students, and employees exposed

UC San Diego Health discovered unauthorized access to some of its employees' email accounts on April 8, after being initially alerted to suspicious activity on March 12.

After discovering the breach, UC San Diego Health terminated the unauthorized access to the compromised accounts and reported the event to law enforcement and the FBI.

The attackers may have accessed or acquired the personal information of patients, employees, and students between December 2, 2020, and April 8, 2021, after breaching the email accounts in a phishing attack.

While the threat actors had access to the email accounts for more than four months, an ongoing investigation by its security teams and external cybersecurity experts has not found any evidence that this information has been misused since the attack.

The personal information accessed during the incident could potentially include: full name, address, date of birth, email, fax number, claims information (date and cost of health care services and claims identifiers), laboratory results, medical diagnosis and conditions, Medical Record Number and other medical identifiers, prescription information, treatment information, medical information, Social Security number, government identification number, payment card number or financial account number and security code, student ID number, and username and password.

There is no "no evidence that other UC San Diego Health systems were impacted, nor do we have any evidence at this time that the information has been misused," the academic health system explained.

"In addition to notifying individuals whose personal information may have been involved, UC San Diego Health has taken remediation measures which have included, among other steps, changing employee credentials, disabling access points, and enhancing our security processes and procedures."

Potentially impacted individuals warned of identity theft risks

UC San Diego Health also warned community members and potentially affected individuals to keep an eye out for identity theft or fraud attempts.

"You can do this by regularly reviewing and monitoring your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity," UC San Diego Health added.

UC San Diego Health also advises rotating credentials and enabling multifactor authentication (MFA) for personal online accounts whenever possible.

After the ongoing investigation ends (likely around September 30), UC San Diego Health will send individual breach notification letters to students, employees, and patients affected by the data breach.

In June 2018, UC San Diego Health also informed 619 patients that they might have been affected by an external data breach involving Nuance Communications, a third-party medical transcription provider.

The breach alert came after Nuance's medical transcription platforms were breached between November 20, 2017, and December 9, 2017.

Related Articles:

Fake Trezor data breach emails used to steal cryptocurrency wallets

Intuit warns of QuickBooks phishing threatening to suspend accounts

General Motors credential stuffing attack exposes car owners info

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

Ransomware attack exposes data of 500,000 Chicago students

- Data Breach
- Health Care
- Health Services
- Healthcare
- Phishing

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

You may also like: