



Hackers gain unauthorized access to data of Santander employees and millions of customers

Description

Hackers are allegedly attempting to sell confidential information belonging to millions of Santander staff and customers, sparking concerns about data security. The bank, which employs 200,000 people globally, including 20,000 in the UK, has confirmed that data has indeed been stolen. Santander has issued an apology for the potential anxiety this may cause and is actively reaching out to affected customers and employees.

According to a statement from the bank, information from customers of Santander in Chile, Spain, and Uruguay, as well as current and former employees, has been compromised. However, the bank reassures that no transactional data or credentials enabling account transactions were part of the breach.

The group behind the alleged hack, known as ShinyHunters, claims to possess data such as bank account details for 30 million people, 6 million account numbers with balances, and 28 million credit card numbers, along with HR information for staff. While Santander has not verified the accuracy of these claims, concerns over data security remain high.

It has been reported that ShinyHunters previously sold data from US telecoms firm AT&T and is now offering private data allegedly obtained from Ticketmaster for sale. The Australian government and FBI are involved in addressing the Ticketmaster data breach.

Cybersecurity experts caution that ShinyHunters' claims should be taken with scrutiny. Researchers suggest that the Santander breach and the Ticketmaster incident may be linked to a larger hack of a cloud storage company, Snowflake. Snowflake has acknowledged unauthorized access to a limited number of customer accounts, possibly resulting from stolen login details from a former employee's demo account. Despite this, Snowflake asserts that no sensitive data was compromised.

The interconnectedness of these cyber threats underscores the ongoing challenges in safeguarding personal and corporate data. Security measures and protocols need to adapt swiftly to prevent such incidents from occurring in the future.

Warning: Trying to access array offset on false in `/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-questions.php` on line 76

Warning: Trying to access array offset on false in `/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-questions.php` on line 76

Warning: Trying to access array offset on false in `/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-questions.php`



on line **76**

Warning: Trying to access array offset on false in `/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-questions.php` on line **76**

Warning: Trying to access array offset on false in `/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-questions.php` on line **76**

Warning: Trying to access array offset on false in `/home/u750883576/domains/esl-news.com/public_html/wp-content/plugins/gpt-post-quiz/includes/admin/forms/gpoq-post-pdf-questions.php` on line **76**

Vocabulary List:

1. **Confidential** // (adjective): Private or secret intended to be kept secret.
2. **Allegedly** // (adverb): Used to convey that something is claimed to be the case or have taken place although there is no proof.
3. **Spark** // (verb): To give off an electric current briefly or in small bursts.
4. **Credentials** // (noun): Evidence of authority status or rights.
5. **Compromised** // (adjective): Exposed to risk or harm especially by failure to maintain security.
6. **Reassures** // (verb): To say or do something to remove doubts or fears.

Vocabulary quizzes

Multiple Choice (Select the Correct answer for each question.)

1. What term is used to describe a significant stage or point in development?

- Option: Robustness
- Option: Milestone
- Option: Enticing
- Option: Popularity

2. What term refers to the state or condition of being liked or admired by many people or the general public?



- Option: Surpassing
- Option: Popularity
- Option: Benchmark
- Option: Ecosystem

3. What term describes the capability of a system to handle a growing amount of work or its potential to be enlarged to accommodate that growth?

- Option: Consistent
- Option: Gas fees
- Option: Scalability
- Option: Innovative

4. Which term refers to gaps or violations especially related to security or protocols?

- Option: Credentials
- Option: Malware
- Option: Breaches
- Option: Vulnerabilities

5. What term is used to signify a pact coalition or partnership between individuals or groups?

- Option: Exploratory
- Option: Alliance
- Option: Robust
- Option: Sentiment

6. Who are individuals usually consulted for advice or guidance especially in decision-making processes?

- Option: Traumatic
- Option: Apologized
- Option: Advisers
- Option: Bias

7. What legal action is started by a plaintiff against a defendant based on a complaint or allegations?

- Option: Confidential
- Option: Allegedly
- Option: Lawsuit
- Option: Discrimination

8. What term describes something attractive or tempting usually encouraging engagement or participation?

- Option: Credentials
- Option: Compromised
- Option: Reassures
- Option: Enticing

9. Which term describes an event or experience that is emotionally disturbing or distressing?



- Option: Spark
- Option: Traumatic
- Option: Surged
- Option: Alliance

10. What term is used to describe malicious software designed to harm or disable computer systems?

- Option: Insights
- Option: Malware
- Option: Surged
- Option: Discrimination

Gap-Fill (Fill in the blanks with the correct word from the vocabulary list.)

11. _____ focuses on meeting the needs of the present without compromising the ability of future generations to meet their own needs.

12. The company entered into a _____ with a leading tech firm to develop innovative solutions.

13. Regular physical _____ is essential for maintaining good health and well-being.

14. The software's _____ allowed it to handle large amounts of data without crashing.

15. The field of _____ involves the application of scientific and mathematical principles to design and develop structures machines and systems.

16. The company denied the _____ of corruption made by the whistleblower.

17. Sales of the new product _____ after receiving positive reviews from consumers.

18. The company prides itself on its _____ approach to product development.

19. Public _____ towards the new policy was largely negative.

20. Users complained about the high _____ associated with using the platform.

Matching Sentences (Match each definition to the correct word from the vocabulary list.)



21. The new smartphone set a high for performance and features in its price range.
22. The social media campaign led to awareness of the charity's mission.
23. The singer's latest album gained immense among fans and critics alike.
24. The organization implemented strict policies against any form of in the workplace.
25. Following the public backlash the company for the product defect and offered refunds.
26. Candidates must provide valid to be considered for the job.
27. The cybersecurity analyst identified several in the network's defenses.
28. It is crucial to ensure that the information provided is accurate and before making decisions.
29. Proper authentication protocols are essential to verify the identity of users.
30. All employees are required to keep sensitive information to maintain data security.

Answer

Multiple Choice: 1. Milestone 2. Popularity 3. Scalability 4. Breaches 5. Alliance 6. Advisers 7. Lawsuit
8. Enticing 9. Traumatic 10. Malware

Gap-Fill: 11. Sustainability 12. partnership 13. activity 14. robustness 15. engineering 16. allegations 17.
surged 18. innovative 19. sentiment 20. gas fees

Matching sentence: 1. benchmark 2. widespread 3. popularity 4. discrimination 5. apologized 6. credentials
7. vulnerabilities 8. trustworthy 9. authenticate 10. confidential

CATEGORY

1. Business - LEVEL5

Date Created

2024/06/01

Author

aimeeyoung99