



Chick-fil-A Cyberattack Potentially Exposes Customer Data

Description

Chick-fil-A confirmed on Wednesday that a recent security breach may have compromised the personal information of a limited number of customer loyalty accounts. The Atlanta-based fast-food chain acted swiftly to secure the affected accounts and inform the customers potentially impacted by this incident.

A spokesperson for Chick-fil-A stated, "We recently identified a security incident that may have affected a limited number of Chick-fil-A One Loyalty accounts." Upon realising the breach, the company took immediate measures to secure and restore the affected accounts and has been communicating directly with those impacted.

The chain expressed regret for any inconvenience and reaffirmed its commitment to maintaining customer trust. Notification to potentially impacted customers began on Monday following the discovery of suspicious login activity tied to specific Chick-fil-A One accounts.

USA Today reported that unauthorized entities targeted the company's website and mobile app between June 17 and June 19, allegedly utilising login credentials obtained from a third-party source. The breach has reportedly affected customers in several states, including Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, Vermont, and Washington, D.C.

The data potentially compromised includes customers' names, email addresses, details of Chick-fil-A One memberships, mobile payment information, the last four digits of payment cards, and the amount of Chick-fil-A credit available in their accounts. In response to the breach, Chick-fil-A reset passwords for the affected accounts, restored any impacted loyalty balances, and provided additional rewards to customers. The company has not disclosed the total number of accounts affected.

Vocabulary List:

1. **breach** //bri:tʃ// (noun): a failure that lets others get private information
2. **compromised** //ˈkɑ:mprə,maɪzd// (verb): made less safe or put at risk
3. **credentials** //krəˈdɛnʃəlz// (noun): information used to log in to accounts
4. **unauthorized** //ʌnˈɔ:θə,raɪzd// (adjective): not allowed or approved by the account owner
5. **suspicious** //səˈspɪʃəs// (adjective): looks likely to be wrong or dangerous
6. **loyalty** //ˈlɔɪəlti// (noun): support and repeat buying from a company

Comprehension Questions



Multiple Choice

1. When did Chick-fil-A confirm the security breach?
 - Option: Monday
 - Option: Wednesday
 - Option: Friday
 - Option: Tuesday

2. What may have been compromised in the security breach?
 - Option: Customer loyalty accounts
 - Option: Employee information
 - Option: Franchise agreements
 - Option: Company profits

3. How did Chick-fil-A respond to the security incident?
 - Option: Ignored it
 - Option: Took immediate measures
 - Option: Outsourced it
 - Option: Filed a lawsuit

4. Which of the following states was NOT mentioned as affected?
 - Option: Iowa
 - Option: California
 - Option: New Mexico
 - Option: Rhode Island

5. What type of information was potentially compromised?
 - Option: Credit scores
 - Option: Physical addresses
 - Option: Mobile payment information
 - Option: Birthdays

6. What actions did Chick-fil-A take in response to the breach?
 - Option: Reset passwords
 - Option: Offered free meals
 - Option: Closed stores
 - Option: Increased prices



True-False

- 7. Chick-fil-A is based in New York.
- 8. The breach affected customer loyalty accounts only in Iowa.
- 9. Chick-fil-A expressed regret over the security incident.
- 10. The company has disclosed the total number of accounts affected.
- 11. Suspicious login activity was discovered after June 19.
- 12. Chick-fil-A One memberships were part of the compromised data.

Gap-Fill

- 13. The security breach was confirmed on _____.
- 14. Chick-fil-A took immediate measures to secure the affected accounts and inform the _____.
- 15. Unauthorized entities targeted the company's website and mobile app between June 17 and _____.
- 16. The data potentially compromised includes customers' names, email addresses, and mobile payment _____.
- 17. Chick-fil-A reset _____ for the affected accounts in response to the breach.
- 18. The company has not disclosed the total number of accounts _____.

Answer

Multiple Choice: 1. Wednesday 2. Customer loyalty accounts 3. Took immediate measures 4. California
5. Mobile payment information 6. Reset passwords

True-False: 7. False 8. False 9. True 10. False 11. False 12. True

Gap-Fill: 13. Wednesday



14. customers 15. June 19 16. information 17. passwords 18. affected

CATEGORY

1. Business - LEVEL6

POST TAG

1. chick-fil-a
2. customer data
3. cyberattack
4. ESL learning
5. esl news
6. Level 6

Tags

1. chick-fil-a
2. customer data
3. cyberattack
4. ESL learning
5. esl news
6. Level 6

Date Created

2026/07/23

Author

aimeeyoung99

ESL-NEWS.COM