The anatomy of a credit card breach

Pete Woodward
Co-founder and CTO

SECURIOUS
The South West's leading cyber security company

UK credit card breaches

- Over 5m individuals affected
- Over £1b stolen

Overview

- The Payment Card Industry (PCI) Data Security Standard
- Attacks that are happening right now
- Tips on staying protected

SECURIOUS
The South West's leading cyber security company

Pete Woodward

- Co-founder and CTO of Securious
- Qualified Security Assessor (QSA) for PCI DSS
- Prevent and fix credit card data breaches

SECURIOUS
The South West's leading cyber security company

The Payment Card Industry (PCI DSS) Standard

- Technical and operational requirements
- Apply to all who store, process or transmit cardholder data
- Set up by five leading credit card companies

3 common attack vectors for ecommerce sites

- SQL injection
- Cross-site scripting (XSS)
- Credentials stuffing

SECURIOUS
The South West's leading cyber security company

SQL injection

- Enables access to website database
- E.g. contact forms, payment details
- Responsible for leaks of multiple data records

SQL injection

TalkTalk data breach customer details found online

22 May 2019 Share

TalkTalk failed to inform 4,545 customers their personal information, including bank account details, were stolen as part of the 2015 data breach.

SQL injection - how to protect from it

- Keep databases up to date
- Layered security approach
- Admin access and user access control

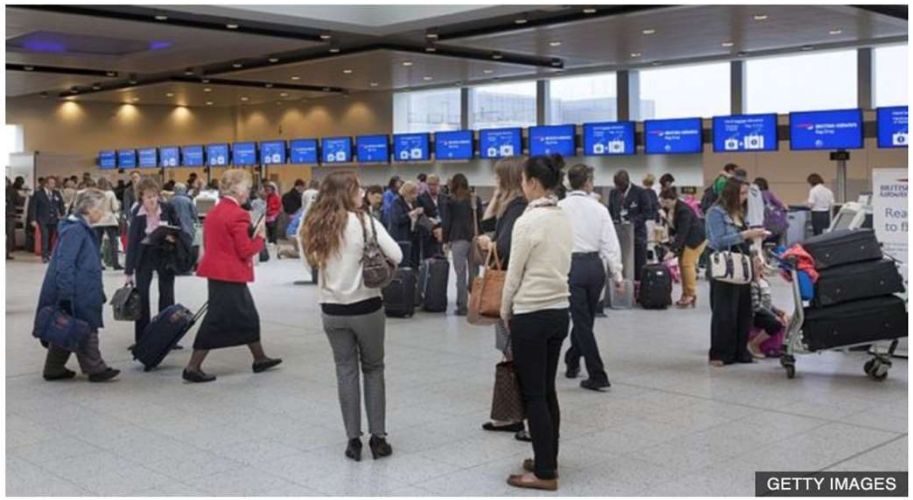
Cross-site scripting (XSS)

- Injection of malicious code
- Visitor sees something other than intended
- May reveal sensitive data or even take over their machine

Cross-site scripting (XSS)

British Airways faces record £183m fine for data breach

8 July 2019 Share



British Airways is facing a record fine of £183m for last year's breach of its security systems.

Cross-site scripting (XSS) - how to protect from it

- Implement access controls
- Force strong passwords
- Continually check for vulnerabilities

SECURIOUS
The South West's leading cyber security company

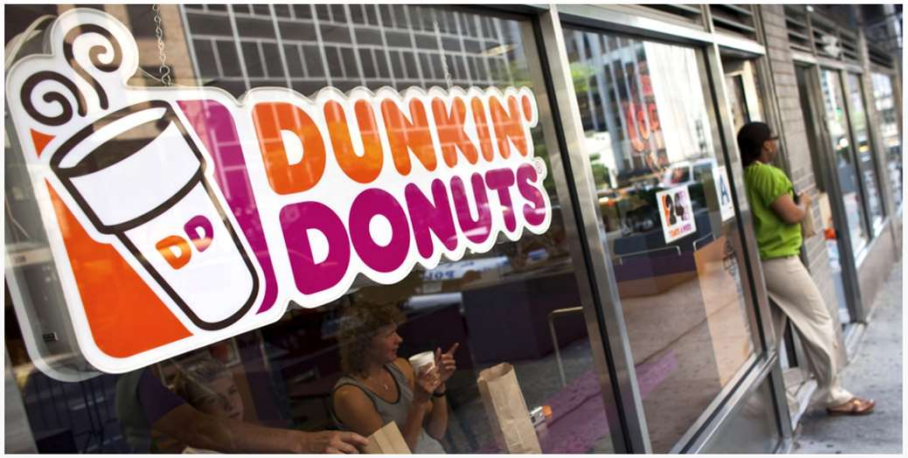
Credentials stuffing

- Gain access to website control panel
- Can result in complete loss of site control
- Exposes site data to attacker

Credentials stuffing

Dunkin' Donuts reveals consumer security breach – here's what it may mean for you

The coffee chain says hackers were after customers' information through its DD Perks program.



Dunkin Donuts Getty Images

Nov. 29, 2018, 7:56 PM GMT / Source: TODAY

By Drew Weisholtz

Some people in America aren't too pleased to be running on Dunkin' right now.

Credentials stuffing - how to protect from it

- Use multi-factor authentication
- Use ‘captchas’
- Limit login attempts

11 tips to protect your ecommerce site

1. Switch to HTTPS
2. Ensure software/plugins up to date
3. Change default login page url
4. Enforce strong passwords
5. Don’t use default admin username
6. Limit login attempts

SECURIOUS
The South West's leading cyber security company

11 tips to protect your ecommerce site

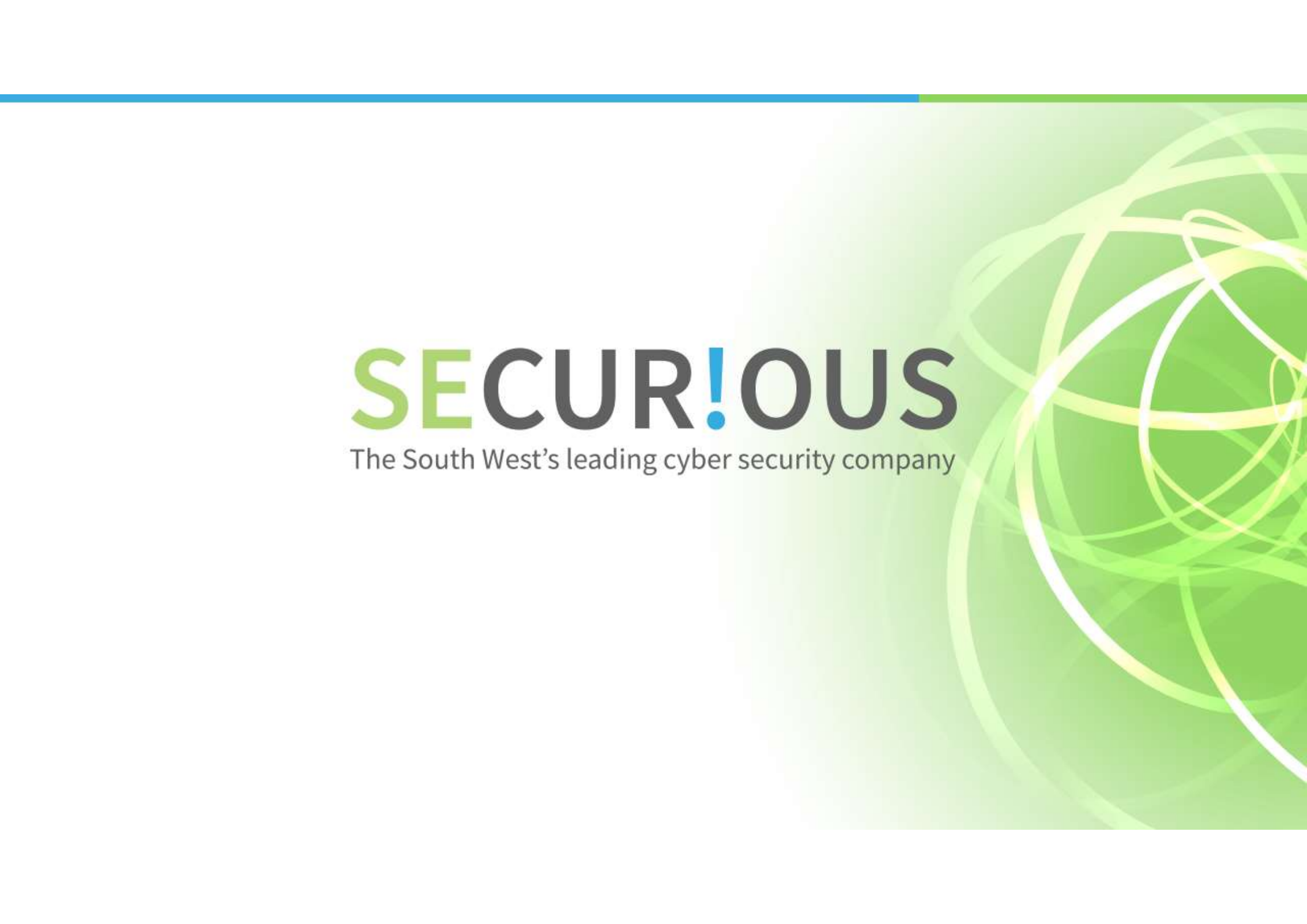
7. Commission regular vulnerability scans
8. Consider two-factor authentication
9. Use a secure ecommerce payment platform
10. Use a content delivery network (CDN)
11. Take regular backups

SECURIOUS
The South West's leading cyber security company

Summary

- The cost of a payment card data breach is substantial
- Ensure you are PCI compliant and take regular action
- Have a plan in place in case the worst happens

SECURIOUS
The South West's leading cyber security company


SECUR!OUS
The South West's leading cyber security company