

2013 YEAR OF THE MEGA BREACH

Cybercriminals unleashed the most damaging series of cyber attacks in history

The total number of breaches in 2013 was

2012



DATA BREACH
156



IDENTITIES EXPOSED
93M



MEAG BREACHES
>10M
1

62%
greater than in
2012

2013



DATA BREACH
253



IDENTITIES EXPOSED
552M



MEAG BREACHES
>10M
8

Each of the **eight** top data breaches in **2013** resulted in the loss of **tens of millions** of data records



What's Stolen?

Consumers' credit card information, birth dates, government ID numbers, home address, medical records, phone numbers, financial information, email addresses, login, password, and other personal information.

PROTECTION TIPS

FOR BUSINESS

Know your data: Protection must focus on the information – not the device or data center. Understand where your sensitive data resides and where it is flowing to help identify the best policies and procedures to protect it.

Educate employees: Provide guidance on information protection, including company policies and procedures for protecting sensitive data on personal and corporate devices.

Implement a strong security posture: Strengthen your security infrastructure with data loss prevention, network security, endpoint security, encryption, strong authentication and defensive measures, including reputation-based technologies.

FOR CONSUMERS

Exercise tech savvy: Passwords are the keys to your kingdom. Use password management software to create strong, unique passwords for each site you visit and keep your devices – including smartphones – updated with the latest security software.

Be vigilant: Review bank and credit card statements for irregularities, be cautious when handling unsolicited or unexpected emails and be wary of online offers that seem too good to be true – they usually are.

Know who you work with: Familiarize yourself with policies from retailers and online services that may request your banking or personal information. As a best practice, visit the company's official website directly (as opposed to clicking on an emailed link) if you must share sensitive information.

#ISTR
@Symantec

