Data Breach Notice Research

Summary

The Identity Theft Resource Center (ITRC) and DIG.Works surveyed 1,050 U.S. adult consumers on topics related to data compromises, data breach notices, and the actions taken, if any, in response to both events. The findings fall into three primary categories:

- Most consumers have been the victim of a data breach; more than half of social media users have had their accounts compromised.
- Few consumers take strong actions to protect themselves after receiving a breach notice, including the most effective protection, a credit freeze.
- Most consumers do not follow secure password practices, with more than half saying it's too difficult to keep up with all their credentials.

Analysis

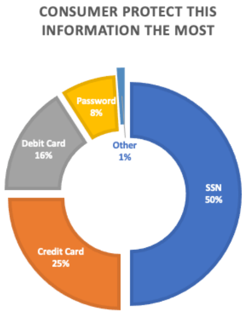
The DIG.Works research, performed pro-bono for the ITRC, explored several issues related to data and account compromises, as well as data breach notices.

Overall, consumers report a high level of awareness of data compromises and the range of actions they can take to protect themselves before and after a data breach. However, there is a significant gap between the level of awareness and the actions taken by consumers that leave most people vulnerable to additional attacks and a continuing risk of identity crimes.

In other words, most people know what they should do, but choose not to do so in two key areas: Data Protection and Password Practices.

- **Data Protection**
  - A shockingly high 16 percent of respondents took no action following a data breach notice, leaving those consumers open to identity fraud or their employers vulnerable to cyberattacks, including ransomware and Business Email Compromise (BEC). Less than half (48 percent) changed the passwords on the breached account, while only 22 percent changed all of their passwords.
  - Only three (3) percent of respondents said they put a credit freeze in place to block the creation of new accounts that require credit checks such as new loans, credit cards and other major purchases. This compares to 11 percent who took advantage of free data/credit monitoring services after a data breach but do not block new credit accounts from being opened.
  - **Recommendation:** ***Organizations should review how they notify consumers of data breaches with the goal of reducing the level of inaction and improving the rates of credit freeze adoption.***

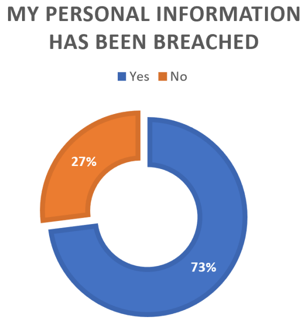
- **Password Practices**
    - Only 15 percent of respondents claim to use unique passwords for each of their accounts. The remaining 85 percent admitted to reusing passwords on multiple accounts, although some claimed a still risky practice of using variations of the same password on different accounts.
    - Only eight (8) percent of respondents say they closely guard their passwords as a way of preventing identity theft and fraud. Half of the respondents (50 percent) say they protect their Social Security number (SSN) the most, despite the fact email credentials are 40x more valuable in identity marketplaces than SSNs ($2 USD for SSNs vs. $80 USD for Gmail credentials).

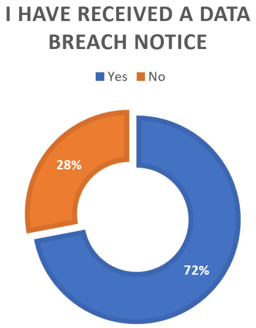


    - **Recommendation:** ***Businesses should strongly recommend consumers reset any password that is not unique and offer Multi-factor Authentication (MFA) using a mobile app. Consumers should follow password best practices, including long, unique passwords on every account. For more recommendations on secure passwords, visit www.idtheftcenter.org.***

Specific Findings

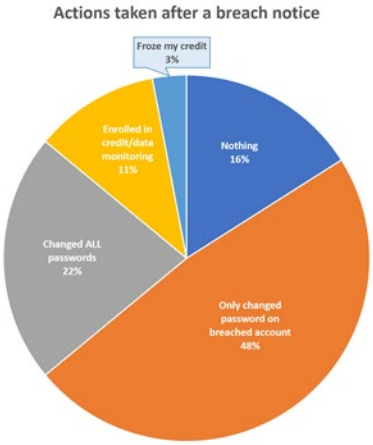
- Seventy-three (73) percent of respondents believe their personal information has been impacted by a data breach; 72 percent have received a data breach notification letter.



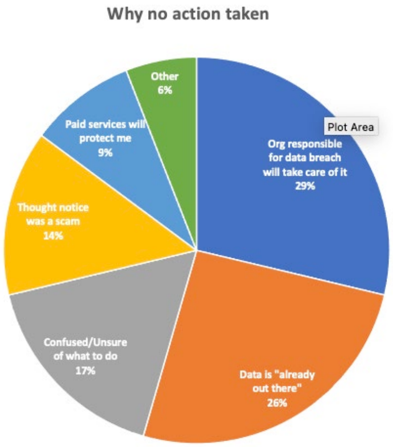


- Fifty-five (55) percent of social media accounts have been compromised, including 42 percent of Facebook users and 32 percent of Instagram users.

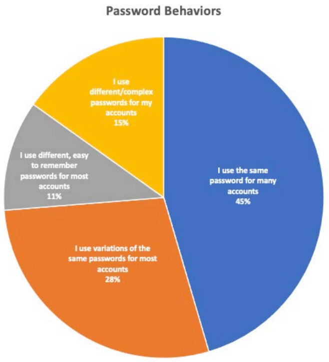
- Only three (3) percent of respondents froze their credit after receiving a data breach notice; 16 percent took no action at all; 22 percent changed all of their account passwords; however, 48 percent only changed the breached account password.



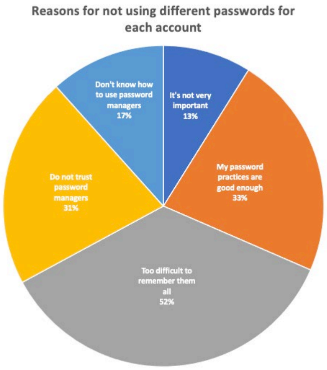
- When asked why they didn't act after receiving a breach notice, 26 percent said "my data is already out there;" 29 percent believed organizations responsible for protecting their data would address the issue; 17 percent did not know what to do; 14 percent thought the notice was a scam.



- Approximately 85 percent admit to using the same password on multiple accounts to one degree or another.
- When asked why they don't use unique passwords, 52 percent said it's too difficult to remember their passwords: 48 percent don't trust or know how to use password managers; 46 percent don't think it's important or believe their password practices are good enough.



Password Behaviors



Reasons for not using different passwords for each account

Acknowledgment: The ITRC thanks Jonathon Sasse and Anders Steele for their donation of this research project on behalf of the ITRC and identity crime victims. Please visit DIG.Works to learn more.