

Digital Identity Usage

An AdNovum Insights Study



swiss made
software



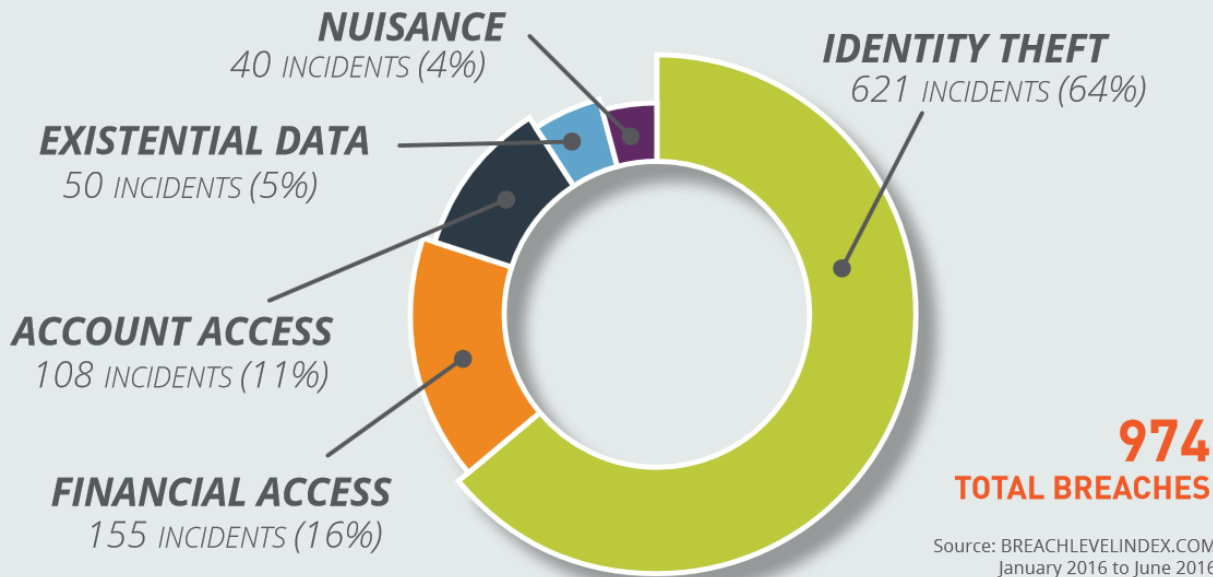
About the Survey

AdNovum conducted an informal survey to better understand consumers' usage of digital identities. The survey was sent to selected contacts within AdNovum's database. Contacts include IT department heads, CIOs and senior IT personnel.

Findings were obtained from approximately 300 **complete** responses
The survey was conducted in **June, 2016**

ID Theft – Most Prevalent Security Breach

NUMBER OF BREACH INCIDENTS BY TYPE



Identity theft accounts for **over 60%** of all known security breach incidents.

This is within the **first 6 months** of 2016

Survey Findings

Number of Digital Identities

- The average user has approximately 30 identities
- He uses at least 10 of these accounts every day



The highest reported was over 80 digital identities per user



Source: AdNovum Digital Identities Survey, June 2016

Takeaway

More accounts may lead to higher chances of identity theft, especially if the same password/credentials are **re-used across multiple accounts.**

Authentication Methods



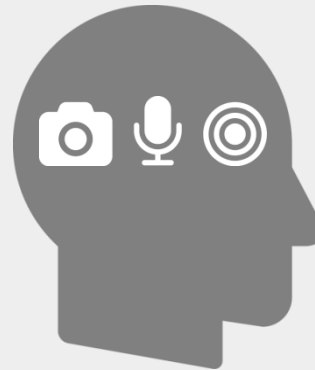
77%

have access to
fingerprint readers

- The average user has access to biometrics and is already using it for access authentication

50% Currently Use

BIOMETRICS



6% are already looking to adopt new forms of biometrics for 2fa*

*2fa = Two-factor authentication

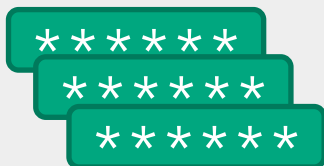
Takeaway

Mobile devices equipped with biometrics are becoming increasingly common. This has contributed to consumers **willingly embracing strong authentication** via mobile devices

Strength of Identity



90% use at least one identity with strong authentication



33% admit to re-using the same password across all identities



66% do not trust social media logins to use as universal IDs

Takeaway

Most users understand the need for enhanced security. The tendency to re-use passwords may be due to **convenience instead of ignorance.**

Conclusion

- When designing authentication solutions for products, organizations would do well to prioritise mobility and convenience.
- New forms of biometric authentication like keystroke analysis, face and voice recognition, etc. are potential solutions to review. They are likely to gain traction as they deliver good UX through security and convenience.

Copyright notice

©Copyright AdNovum 2016. This report is published by AdNovum. Reproduction of any material from this report, in whole or in part, is strictly forbidden without the prior consent of AdNovum. Furthermore, any data, ratings or rankings in this report may not be used in any corporate materials or promotional activities without the prior consent of AdNovum.



AdNovum Singapore

info@adnovum.sg www.adnovum.sg



IT Consulting



Software Solutions



NEVIS



IT Security



Application
Management