JAVELIN

In Search of a Better Password Policy

04 December 2014 By: Al Pascual

Despite claims by security experts and popular media that passwords are dead, this method of authentication remains firmly entrenched across the financial industry and elsewhere. The simplicity and familiarity of passwords has helped them retain a role in securing online accounts, despite vulnerabilities that are significant and universally known. Yet suggestions for creating and securely managing passwords are largely ignored by accountholders who deem them impractical. Typically supplemented by other forms of authentication when used to secure financial accounts, passwords are considered by bank executives to be only the most cursory of deterrents. And cybercriminals have proven successful at circumventing this deterrent, effectively misusing compromised credentials to access online financial accounts. Bolstering the security of passwords will require strategies that address vulnerabilities such as password reuse, targeted malware, data breaches, and social engineering without sacrificing convenience for accountholders. Stakeholders generally anticipate a future free of passwords, but a balanced approach to improving their security in the interim could have a noticeable effect on the rate of fraud while preserving the experience of accountholders.

Primary Questions:

- What are the security threats and vulnerabilities specific to passwords?
- What is the relationship between passwords and identity fraud?
- How often do leading financial institutions update their customer-facing password policies?
- What are the factors that financial institutions consider when deciding on customer-facing password policies?
- Which industries and what credentials do criminals currently target with their efforts?
- What can financial institutions do to improve the security of customer accounts?

Despite claims by security experts and popular media that passwords are dead, this method of authentication remains firmly entrenched across the financial industry and elsewhere. The simplicity and familiarity of passwords has helped them retain a role in securing online accounts, despite vulnerabilities that are significant and universally known. This report examines the security threats and vulnerabilities specific to passwords and gives recommendations on what financial institutions can do to improve the security of customer accounts.

Companies Mentioned

Adobe, Ally, Amazon, Bank of America, Bank of the West, Capital One, Comerica, eBay, Facebook, Google, LinkedIn, Mozilla, Sony, and SunTrust

2013 Identity Fraud Survey Data Collection

Javelin's Identity Fraud Survey was historically fielded as a landline survey using computer-assisted telephone interviewing (CATI). At the survey's inception in 2003, landlines provided relatively comprehensive coverage of the U.S. population. However, with the advent of time and technology, landline coverage has been shrinking, and thus the survey has had increasingly less penetration into the younger, more mobile population. Cognizant of this shift, Javelin fielded the fraud survey in 2011 through the KnowledgePanel®. Javelin continued to use KnowledgePanel for the 2013 survey in order to obtain the most representative sample of U.S. adults.

KnowledgePanel is the only probability-based online panel in the U.S. Through mail, the panel recruits households with no access to the Internet (at the time of recruitment), as well as cell phone-only households. The panel offers a mix of RDD-based recruitment (1999–present) and address-based sampling (introduced in 2008 and rolled out in full in 2009).

The 2013 ID Fraud Survey was conducted among 5,634 U.S. adults over age 18 on KnowledgePanel; this sample is representative of the U.S. census demographics distribution, recruited from the Knowledge Networks panel. Data collection took place Oct. 9–30, 2013. The final data was weighted by Knowledge Networks, while Javelin was responsible for data cleaning, processing, and reporting. Data is weighted using 18+ U.S. population benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets.

Margin of Error

For questions answered by all 5,634 respondents, the maximum margin of sampling error is +/- 1.31 percentage points at the 95% confidence level. For questions answered by all 936 identity-fraud victims, the maximum margin of sampling error is +/- 3.20 percentage points at the 95% confidence level.

Password Policies

The public-facing password policies of six financial institutions and four consumer-oriented non-banking websites were examined by Javelin. This process included identifying the allowed and disallowed password components and length, along with those features of a password that are not recommended for use.

As part of this process, Javelin calculated the entropy of each organization's minimum password requirements using the following formula:

Nmin log2 Cmin

Where Cmin is the cardinality of the minimum character set required and Nmin is the minimum length.

Executive Interviews

Javelin interviewed several financial industry fraud and security executives in an effort to understand their perspectives on passwords and the broader authentication landscape, along with the factors that influence the development of FI password policies.

ENDNOTES

Heuristic password cracking software deciphers encrypted passwords more quickly than traditional brute-force guessing methods by leveraging complex algorithms "trained" with lists of common passwords or password components.
2 http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/, accessed Nov. 25, 2014.
3 http://www.reuters.com/article/2012/06/06/net-us-linkedin-breach-idUSBRE85511820120606, accessed Nov. 25, 2014.
4 http://arstechnica.com/tech-policy/2011/06/sony-hacked-yet-again-plaintext-passwords-posted/, accessed Nov. 25, 2014.
5 https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet, accessed Nov. 25, 2014.
6 http://www.wired.co.uk/news/archive/2013-03/25/cracking-passwords, accessed Nov. 25, 2014.
7 http://www.bankinfosecurity.com/blogs/account-takeovers-get-automated-p-1538, accessed Nov. 23, 2014.
8 http://blog.trendmicro.com/trendlabs-security-intelligence/predator-pain-and-limitless-behind-the-fraud/, accessed Nov. 23, 2014.
9 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf, accessed Nov. 24, 2014.
10 https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab13013.pdf, accessed Nov. 24, 2014.
11 http://www.cnet.com/how-to/how-to-enable-two-factor-authentication-on-popular-sites/, accessed Nov. 24, 2014.
1 2 http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/access-control-/authentication.aspx, accessed Nov. 24, 2014.
13 http://repository.cmu.edu/cgi/viewcontent.cgi?article=1086&context=cylab, accessed Nov. 23, 2014.
1 4 http://www.americanbanker.com/news/technology/consumers-reuse-of-passwords-will-speed-adoption-of-biometrics-report-1071183-1.html, accessed Nov. 24, 2014.
15 https://www.bankofthewest.com/personal-banking/mobile-banking/mobile-tablet-apps.html, accessed Nov. 24, 2014.
16 https://www.charterone.com/online-banking/mobile-banking/fast-balance/agreement.aspx, accessed Nov. 24, 2014.
17 http://www.digitaltrends.com/computing/lay-off-chrome-firefox-has-the-same-password-security-flaw/, accessed Nov. 24, 2014.
18 https://forums.lastpass.com/viewtopic.php?f=13&t=62, accessed Nov. 24, 2014.
1 9 http://www.darkreading.com/operations/identity-and-access-management/new-citadel-attack-targets-password-managers/d/d-id/1317642, accessed Nov. 24, 2014.

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100