

JULY 2008 · WHITEPAPER

THE PASSING OF PASSWORDS

FFIEC*-compliant user login authentication
*Federal Financial Institutions Examination Council



vidoop

Vidloop LLC © 2008

EXECUTIVE SUMMARY



Web passwords play a large role in confirming the identity of those who use the Internet. However, people simply have too many passwords and often choose ones that are simple to remember yet easy to steal. Internet statistics show that more people are online and taking advantage of e-commerce in increasing numbers.

The need for a login solution that is more secure than passwords has emerged, and stronger ways to authenticate logins have become a focus in the industry. Requiring increased complexity of passwords has proven to be a quick fix. Unfortunately, this method tends to impede users from remembering their passwords and often leads to a feeling of indifference regarding the need for security and ignored security threats. A paradigm shift in login authentication aimed at replacing passwords is described.

Cyber crime in the U.S. and Canada cost businesses an estimated 1.4 percent of online revenue in 2007, amounting to roughly **\$3.6 billion** in online payment fraud.

THE PASSING OF PASSWORDS

Passwords play a large role in confirming the identity of internet users. In 2008, the Pew Internet & American Life Project found that approximately three-fourths of the U.S. population is online (215 million users), and according to Internet World Stats (2008) one out of every five people on Earth is online (1.4 billion users).

Utilizing passwords to confirm identity among that many people is a formidable task and a growing problem. People simply have too many passwords and have trouble remembering them. Since passwords that are hard to guess are often hard to remember, users tend to pick passwords that can be easily remembered and guessed.¹

Typical user behavior with passwords:²

- 64% of end users report that they have written down their password at least once
- 65% of workers use the same password for different applications or services
- 70% of people do not use a unique password for each Web site
- One third of Internet users have shared their log-in information with their partner
- One third of Internet users have shared their password with others in the last month
- Around 82% of people have forgotten a password used on a Web site
- 40% of online banking customers use the same password multiple times

Respondents to a recent Internet user survey³ indicated that they use an average of 5.4 different passwords to access sites on the Internet. In the same study, seven out of ten respondents indicated that they have trouble remembering their Internet passwords.

¹ Marshall, 2004a; Suo, Shu, & Owen, 2005; Manly, 2006; Forget, Chiasson, & Biddle, 2007; VeriSign, 2008; IT Business Edge, 2008

² Marshall, 2004b

³ Flexo, S., 2008

Correspondingly, another study published by the Association for Computing Machinery⁴ found that the average Internet user has 6.5 passwords. Each user has roughly 25 password protected accounts and has to recall about eight passwords per day. The average password in a user's arsenal is eventually used at just under six distinct login sites.

Required password complexity accompanied by the need to frequently update passwords entices users to meet only the bare minimum standards for complexity or resort to keeping a list. To compensate, people often repeat patterns that are easy to remember. They are likely to write passwords on notepads and even directly on the case of the computer.⁵

The National Cyber Security Alliance reported in 2008 that **nearly half of consumers** are entirely unsure of what to do if they fall victim to a cyber crime. In turn, they do not know how to protect themselves from cyber criminals. In 2008, Christiansen & Burke warned that, "The Web is the new threat vector of choice for hackers and cybercriminals to distribute malware and perpetrate identity theft, financial fraud, and corporate espionage."

This raises the issue of the effectiveness of passwords and what can be done to replace them. Many of the deficiencies of password authentication systems arise from the limitations of human memory as discussed in a 2008 Vidoop LLC white paper. In 2000, a study by the Cambridge Computer Laboratory ideally stated that "A good password should consist of mixed characters or special characters, and should not consist of words found in the dictionary. It should not be written down in an easily accessible place and especially not next to login."⁶ However, "Requirements for length, complexity, frequency of change, restrictions on re-use, and exclusion of dictionary terms enhance the security of passwords but make them more cumbersome for end-users who, in response, tend to write them down and/or rely more on the help desk for assistance" (*Derek Brink, CISSP, Vice President of IT Security for Aberdeen Group*).⁷

⁴ Florencio & Herley, 2007. The Association for Computing Machinery is the world's largest educational and scientific computing society and delivers resources that advance computing as a science and a profession.

⁵ Espenschied, 2008

⁶ <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf>

⁷ <http://www.aberdeen.com/summary/report/benchmark/4660-RA-password-lifecycle-management.asp>

Given the limitations of human memory, Delbert Hart declared in the Journal of Computing

Sciences in Colleges in 2008 that, "There often is talk of biometrics replacing passwords, (but) for the foreseeable future passwords will remain central to how we verify that a person is who they say they are." Be that as it may, passwords are useless if security risks are ignored by end users.

Out of 67 participants who entered a website authentication study conducted in 2007 by Schechter, Dhamija, Ozment, & Fisher, 85 percent ignored absent HTTPS indicators, 92 percent of the users entered their passwords even if their site authentication images were missing, and 53 percent disregarded simulated attack clues and entered their passwords on all tasks. If user apathy and poor password construction continue to be the leading points of breach on security systems, what is the solution to both verifying identity and providing secure authentication?

Vidooop has created a ground-breaking solution that provides authentication strong enough for banking, finance, and e-commerce that also maintains a usable, stress-free experience. Vidooop fixes the password problem by validating users with a matrix of random images that belong to static categories chosen by the user during registration.

The solution eases the strain on a user's memory by asking them to simply recognize categories as opposed to recall a long, complex password. Bona fide security coupled with the intrinsic ease of recognition provides a convenient, intuitive experience that drives online participation and earns consumer trust. The solution also cuts support calls, reduces failed logins, and increases customer confidence.



VeriSign stressed in a 2008 study that, "A time is fast approaching when passwords will not and cannot be an effective security mechanism for our enterprise environments."



A 2008 Information Week study found that **70 percent** of IT professionals acknowledge that user names and passwords do not provide an adequate level of security.

If old-fashioned password security can't stop the modern cyber criminal – and most of the alternatives are cumbersome and expensive – then delivering easy and cost-effective strong authentication such as that offered by Vidoop makes sense. It also makes dollars and cents.

A 2007 survey by InternetRetailer.com revealed that 45 percent of U.S. adults shop online. In 2008, John Horrigan, Associate Director of the Pew Internet & American Life Project, found that the growing number of e-shoppers fosters widespread concern about the safety of financial and personal data online. As early as 2004, a study conducted by the Center for the Digital Future found that “purchasers and nonpurchasers alike report extraordinarily high levels of concern about online security and privacy.”

Merchants in the U.S. and Canada lost an estimated 1.4 percent of e-commerce revenue (approximately \$3.6 billion) to online payment fraud in 2007, according to CyberSource Corp.'s 9th Annual Online Fraud Report. In the report, Rob Trout of InternetRetailer.com warned that some merchants may actually be underestimating the impact of fraudulent activities on their revenue and profit picture.

If you, like Information Week and Verisign, are concerned with the diminishing efficiency of passwords and recognize the growing need for stronger user authentication due to increased Internet security threats, a paradigm shift in solutions is needed. The Vidoop's authentication solution fixes the password problem with a solution that is strong enough for banking, finance, and e-commerce while providing a uniquely usable, stress-free experience for users.

References

- 45% of U.S. adults shop online, but security concerns hold others back. (2007). *Internet Retailer*. Retrieved June 22, 2008 from <http://www.internetretailer.com/internet/marketing-conference/72196-45-us-adults-shop-online-but-security-concerns-hold-others-back.html>.
- Brink, D. (2008). Passwords, Privileged Passwords and Password Lifecycle Management. *Aberdeen Group*. Retrieved June 18, 2008, from <http://www.aberdeen.com/summary/report/benchmark/4660-RA-password-lifecycle-management.asp> database.
- Christiansen C.A. & Burke, B.E. (2008). Web Security SaaS: The Next Generation of Web Security. *IDC*. Retrieved June 9, 2008, from <http://www.idc.com>.
- Cisco & Ironport Inc. (2008). 2008 *Internet security trends*. Retrieved June 18, 2008, from <http://webforms.ironport.com/go/ironportinc/trends2008>.
- Espenschied, J. (2008). *Four signs your security program's gone too far*. Retrieved June 24, 2008, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=education_training&articleId=9103099&taxonomyId=56&intsrc=kc_feat.
- Flexo, S. (2008). Internet Passwords, User Ids, and Other Personal Identity , *Omni Business Study # 803161*.
- Florencio , D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International Conference on World Wide Web*, 657-666.
- Forget, A., Chiasson, S., & Biddle, R. (2007). Helping users create better passwords: is this the right approach?. *ACM Symposium on Usable Privacy and Security (SOUPS)*.
- Hart, D. (2008). Attitudes and practices of students towards password security. *Journal of Computing Sciences in Colleges*, 23(5), 169-174.
- Horrigan, J. (2008). Online Shopping. *Pew internet & american life project*. Retrieved June 22, 2008, from http://www.pewinternet.org/pdfs/PIP_Online%20Shopping.pdf database.
- Information Week. (2008). *Closing the Gap Between Two-Factor Security and User Adoption*. Retrieved June 18, 2008, from <http://www.techwebonlineevents.com/ars/eventregistration.do?mode=eventreg&F=1000993&K=4TW>.
- Internet World Stats. (2008). *World Internet Users*. Retrieved June 23, 2008, from <http://www.internetworldstats.com/stats.htm>.
- IT Business Edge. (2008). *Too Many Passwords as Web Apps Proliferate*. Retrieved June 21, 2008 from <http://www.itbusinessedge.com/item/?ci=39743>.
- Manly, R., (2006). Password security is her game. *California State University, Long Beach*. Retrieved June 9, 2008, from <http://www.csulb.edu/misc/inside/archives/v58n5/2.htm>.
- Marshall , B. K., (2004a). Core Characteristics for Evaluating Authenticators. *PasswordResearch.com*. Retrieved June 10, 2008, from <http://www.passwordresearch.com/core.html>.
- Marshall , B. K., (2004b). User Password Practices. *PasswordResearch.com*. Retrieved June 10, 2008, from <http://passwordresearch.com/stats/statindex.html#User%20Password%20Practices>.
- National Cyber Security Alliance, (2008). *Overview of NSCA Consumer Research Study*. Retrieved June 18, 2008, from http://www.staysafeonline.org/pdf/NSCA_quickquery_survey.pdf.
- Pew Internet & American Life Project. (2008). *Demographics of internet users*. Retrieved June 23, 2008, from <http://www.pewinternet.org/trends.asp>.
- Schechter, S., Dhamija, R., Ozment, A. & Fisher, I., (2007). The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. *IEEE Symposium on Security and Privacy*. Retrieved June 15, 2008, from <http://www.usablesecurity.org/emperor/emperor.pdf> database.
- Suo, X., Shu, Y., & Owen, G.S. (2005). Graphical passwords: a survey. *21st Annual Computer Security Applications Conference* , (), 463-472 . Retrieved June 24, 2008, from <http://www.acsac.org/2005/papers/89.pdf> database.
- Surveying the Digital Future: Year Four. (2004). *Center for the Digital Future*. Retrieved June 23, 2008 from <http://www.digitalcenter.org/downloads/DigitalFutureReport-Year4-2004.pdf> database.
- Trout R., (2008). Safety payoff. *Internet Retailer*. Retrieved June 22, 2008, from <http://www.internetretailer.com/article.asp?id=26259>.
- VeriSign. (2008). The security risks of using passwords. Retrieved June 23, 2008, from http://cnscenter.future.co.kr/resource/security/hacking/password_whitepaper.pdf.
- Vidoop. (2008). *The one thing you should know*. Retrieved June xx, 2008, from <http://www.confidenttechnologies.com/>.
- Yan, J., Blackwell, A., Anderson, R. & Grant, A. (2000). The memorability and security of passwords – some empirical results. *Cambridge University*. Retrieved June 20, 2008 from <http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf>.