Worst Passwords of 2013: password & 123456

By Judge Herbert B. Dixon Jr.

How many of you seeing the title of this article thought to yourself, "Why is my password in the title of this technology article?" Quite a few, I suspect. SplashData, a data security and productivity software provider for smartphones and computers that also provides software for managing passwords, digital photos, financial accounts, and other sensitive data, issued a report entitled "Worst Passwords of 2013." This report is the latest update of an annual effort by SplashData to compile a list of passwords having the dubious distinction of being the most common (and, therefore, least secure) passwords of the year.[1] The report tells us that 2013's absolute worst, common password known to mankind is **123456**, which beat out the former #1 worst password for several years running, **password**. How can this be? Less than two years ago, I wrote an article on cybersecurity that included a true story about a prominent technology writer (not me) who was the victim of malicious hacking.[2] I was certain everyone would take heed, follow through, and strengthen their pitifully weak passwords. Was I ever wrong! The top five worst passwords in 2013 also included **12345678**, **qwerty** (sequential keys on the keyboard), and **abc123**. This is distressing!

How Was the List of 2013's Worst Passwords Compiled

In case you are wondering how a list of passwords is compiled, security researchers use two primary sources: (1) information revealed from big security breaches and (2) online password dumps.[3] You probably heard about both situations in the news. In many instances, researchers believe the confidential password information came from computers infected with malicious software that logged keystrokes. Not only are too many passwords too weak, but after analyzing the data, some researchers concluded that 30–40 percent of people use the same passwords on different websites. The tragedy of these findings is that users who thought they were being cleverly unique actually created predictable passwords. For example, among the most common passwords in 2013, **123123** came in at number 11, **letmein** at number 14, and **trustno1** at number 24.

There have been lots of news coverage over the past year about cybersecurity threats and online privacy breaches, especially cyberattacks against well-known tech giants, including Adobe, Google, Facebook, Twitter, and LinkedIn.[4] The Adobe breach resulted in the disclosure of over 130 million passwords created by 38 million active users of that site plus an unknown number of inactive users.[5] Researchers learned from this breach that over 1.9 million individuals on Adobe's website used the password **123456** and nearly 346,000 used the word **password** as their personal password. Also, as if to honor the cyberattack against Adobe, over 211,000 unsuspecting online users created the password **adobe123**, causing it to appear at number 10 on the worst passwords list. Would you believe that the password **photoshop** (also an Adobe product) was not far behind at number 15 on the list? How's that for carefully creating a secure password? Moreover, and consistent with the conclusions by other researchers, these researchers found that many individuals used the same username and password for all of the websites they regularly accessed, further compromising the security of their data.[6] In the words of one security commentator, "If you recognize your favorite password here, it's really time to pick something else."[7]

These revelations about common passwords in 2013 are in line with past research. In 2009, Twitter banned 370 passwords that included most of the passwords noted above, including, you guessed it, **twitter**[8]—more proof that unsuspecting individuals often create website account passwords that include the website's. Doesn't Twitter's discovery of many

individuals using **twitter** as part of their password seem eerily similar to the revelations of many Adobe website using **adobe** as part of their online password? Have you done something similar with one of your online accounts? Shouldn't you change that pathetically weak password now? Although there are various efforts to move away from passwords, namely, using biometrics such as fingerprints and iris scans, and special key and USB devices, the user-defined password is not likely to go the way of the dinosaur (or should I say floppy disk?) anytime in the near future.

How Should I Go About Creating a Strong Password

To create strong passwords, you may want to consider a password manager for assistance in creating a strong, unique password for each website. For example, you may wish to consider using a password manager service like SplashID Safe,[9] Passpack,[10] RoboForm,[11] or LastPass[12] to secure your accounts. Alternatively, you might try a password generator such as Secure Password Generator[13] or Norton's password generator.[14]

Finally, you should consult websites such as the Microsoft Safety & Security Center[15] to receive terrific suggestions on how to create a reasonably secure password and the pitfalls to avoid. For example, do not use

- Personal identity information that could be guessed or easily discovered, like pet names, nicknames, birthdate, or home or office address.
- Dictionary words in any language (including the word *password*—2013's second most common password in the English language!).
- Words spelled backward, abbreviations, and common misspellings (e.g., **repapswen**, newspaper spelled backward, or operater, a common misspelling of operator).
- Common letter-to-symbol conversions within a dictionary word, such as changing "o" to "0" or "i" to "1" or "!".
- Sequences or repeated characters. Examples: **12345678**, **222222**, **abcdefg**, or adjacent letters on your keyboard (such as **qwerty**).

The most secure type of password is one that has a random combination of upper- and lowercase letters, numbers, and symbols, such as this 12-digit password: **z^4D$1Lr9%dk**. Unfortunately, having a password with similar random characters is not practical. The password would likely end up on a "Post-it note" attached to the computer monitor or on a list in a folder kept next to the computer labeled "My Passwords."

There is another possibility that users may find more acceptable for developing a secure password. Start with a phrase, for example, "The USA is number one in the world." Eliminate the spaces and change it to **TheUSAis#1intheworld**. Another idea for a passphrase is something like "The cost of a car in 1960 was $2000." Eliminate the spaces and change it to **Thecostofacarin1960was$2000**. In both instances, these are very strong passwords, containing at least one upper- and lowercase letter, numbers, and at least one symbol. As a bonus, both of these passwords are much stronger, more secure, and easier to remember than the 12-digit random combination shown above. For additional hints at creating a secure password, review my earlier article on cybersecurity that I referenced in the first paragraph of this article.

Conclusion

In the final analysis, a weak or common password makes your data vulnerable to the cyber thief and online hacker, whether the data are your bank account and credit card information or personal family photographs. The loss of either type of data would cause financial hardship or personal anguish, or both. The readers of this column should take heed of the lessons of weak passwords already learned by others and take the necessary steps to decrease the possibility of being the next victim.

As you have heard before, a hint to the wise is sufficient. ■

Endnotes

1. *Worst Passwords of 2013—Our Annual List Updated*, SplashData News, http://splashdata.blogspot.com/2014/01/worst-passwords-of-2013-our-annual-list.html.

2. Herbert B. Dixon Jr., *Cybersecurity . . . How Important Is It?*, 51 The Judges' J., no. 4, Fall 2012, at 36.

3. *Stolen Facebook and Yahoo Passwords Dumped Online*, BBC News (Dec. 4, 2013), http://www.bbc.com/news/technology-25213846.

4. Charlie Warzel, *It's 2014 and Our Passwords Aren't Getting Better*, BuzzFeed (Jan. 22, 2014), http://www.buzzfeed.com/charliewarzel/its-2014-and-our-passwords-arent-getting-better.

5. Lorenzo Franceschi-Bicchierai, *The 20 Most Popular Passwords Stolen from Adobe*, Mashable (Nov. 5, 2013), http://mashable.com/2013/11/05/20-most-popular-passwords-adobe.

6. Julie Bort, *2 Million More Passwords for Facebook, Google, Twitter, Other Sites Were Stolen and Posted to the Net*, Bus. Insider (Dec. 4, 2013), http://www.businessinsider.com/2-million-more-passwords-stolen-2013-12?utm_source=slate&utm_medium=referral&utm_term=partner.

7. *Id.*

8. Dan Frommer, *Twitter's List of 370 Banned Passwords*, Bus. Insider (Dec. 28, 2009), http://www.businessinsider.com/twitters-list-of-370-banned-passwords-2009-12.

9. SplashID Safe, https://www.splashid.com.

10. Passpack, https://www.passpack.com.

11. RoboForm, http://www.roboform.com.

12. LastPass, https://lastpass.com.

13. *Secure Password Generator*, PasswordsGenerator, http://passwordsgenerator.net.

14. *Password Generator*, Norton Identity Safe, https://identitysafe.norton.com/password-generator.

15. *Create Strong Passwords*, Microsoft Safety & Sec. Ctr., https://www.microsoft.com/security/pc-security/password-checker.aspx.

Judge Herbert B. Dixon Jr. is the technology columnist for *The Judges' Journal*, a member of the *ABA Journal* Board of Editors, and a former chair of the National Conference of State Trial Judges. He sits on the Superior Court of the District of Columbia and can be reached at Herbert.Dixon@dcsc.gov. Follow Judge Dixon on Twitter @Jhbdixon.