



25 "Worst Passwords" of 2011 Revealed

Source: Forbes.com

If you see your password below, STOP!

Do not finish reading this post and immediately go change your password -- before you forget. You will probably make changes in several places since passwords tend to be reused for multiple accounts.

Here are two lists, the first compiled by SplashData:

1. password
2. 123456
- 3.12345678
4. qwerty
5. abc123
6. monkey
7. 1234567
8. letmein
9. trustno1
10. dragon
11. baseball

12. 111111
13. iloveyou
14. master
15. sunshine
16. ashley
17. bailey
18. passwOrd
19. shadow
20. 123123
21. 654321
22. superman
23. qazwsx
24. michael
25. football

Last year, Imperva looked at 32 million passwords stolen from RockYou, a hacked website, and released its own Top 10 "worst" list:

1. 123456
2. 12345
3. 123456789
4. Password
5. iloveyou
6. princess
7. rockyou
8. 1234567

9. 12345678

10. abc123

If you've gotten this far and don't see any of your passwords, that's good news. But, note that complex passwords combining letters and numbers, such as passw0rd (with the "o" replaced by a zero) are starting to get onto the 2011 list. abc123 is a mixed password that showed up on both lists.

Last year, Imperva provided a list of password best practices, created by NASA to help its users protect their rocket science, they include:

It should contain at least eight characters

It should contain a mix of four different types of characters - upper case letters, lower case letters, numbers, and special characters such as !@#\$%^&*;" If there is only one letter or special character, it should not be either the first or last character in the password.

It should not be a name, a slang word, or any word in the dictionary. It should not include any part of your name or your e-mail address.

Following that advice, of course, means you'll create a password that will be impossible, unless you try a trick credited to security guru Bruce Schneir: Turn a sentence into a password.

For example, "Now I lay me down to sleep" might become nilmDOWN2s, a 10-character password that won't be found in any dictionary.

Can't remember that password? Schneir says it's OK to write it down and put it in your wallet, or better yet keep a hint in your wallet. Just don't also include a list of the sites and services that password works with. Try to use a different password on every service, but if you can't do that, at least develop a set of passwords that you use at different sites.

Someday, we will use authentication schemes, perhaps biometrics, that don't require so much jumping through hoops to protect our data. But, in the meantime, passwords are all most of us have, so they ought to be strong enough to do the job.