SplashData's annual list shows people still using easy-to-guess passwords

October 25 2012, by Bob Yirka

(Phys.org)—In what has become an annual tradition, SplashData, a company that makes productivity applications for smartphones, has released a list of passwords it claims are the most commonly used to access online applications. The list is compiled by the company using passwords that hackers have posted on various web sites to illustrate the ease with which online accounts can be cracked. SplashData refers to the top 25 passwords as the "worst passwords of the year."

The top three haven't changed from last year: "password," "123456" and "12345678." SplashData indicates that many people fear forgetting their password more than they fear hackers breaching their account. Others, perhaps responding to reports of multiple recent website hacking incidents, have resorted to trying easy-to-remember (but still easy-to-hack) passwords such as "Jesus," "mustang," "welcome" and "ninja."

In response to the posting by SplashData, several computer security companies have posted tips to users aimed at encouraging protection of accounts with stronger passwords. Most companies persist with the tried-and-true standard of suggesting users choose passwords that mix numbers and letters, are at least eight characters long, and include punctuation characters. Experts also suggest users choose different passwords for different sites to prevent hackers from accessing all of their accounts if they happen to gain access to their single-use password. A third option is for users to choose difficult-to-remember passwords and then use a password manager application (such as *SplashID Safe* made by SplashData), which tracks all passwords and then enters them

automatically when users log into to registered sites.

SplashData encourages people—especially those who use the same password for access to online entertainment sites such as Facebook and Twitter, and those sites that hold important bank and credit card information—to take the task of choosing a password more seriously. The company also suggests that people who are currently using one of the "listed" passwords change it immediately, or risk having their account compromised.