If Your Password Is 123456, Just Make It HackMe

by Ashlee Vance
Friday, January 22, 2010

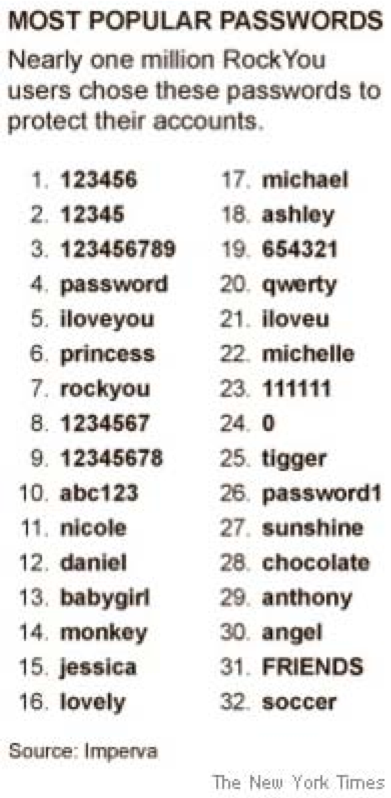
provided by
The New York Times

Back at the dawn of the Web, the most popular account password was "12345."

Today, it's one digit longer but hardly safer: "123456."

Despite all the reports of Internet security breaches over the years, including the recent attacks on Google's e-mail service, many people have reacted to the break-ins with a shrug.

According to a new analysis, one out of five Web users still decides to leave the digital equivalent of a key under the doormat: they choose a simple, easily guessed password like "abc123," "iloveyou" or even "password" to protect their data.



MOST POPULAR PASSWORDS

Nearly one million RockYou users chose these passwords to protect their accounts.

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123
11. nicole
12. daniel
13. babygirl
14. monkey
15. jessica
16. lovely
17. michael
18. ashley
19. 654321
20. qwerty
21. iloveu
22. michelle
23. 111111
24. 0
25. tigger
26. password1
27. sunshine
28. chocolate
29. anthony
30. angel
31. FRIENDS
32. soccer

Source: Imperva

The New York Times

"I guess it's just a genetic flaw in humans," said Amichai Shulman, the chief technology officer at Imperva, which makes software for blocking hackers. "We've been following the same patterns since the 1990s."

Mr. Shulman and his company examined a list of 32 million passwords that an unknown hacker stole last month from RockYou, a company that makes software for users of social networking sites like Facebook and MySpace. The list was briefly posted on the Web, and hackers and security researchers downloaded it. (RockYou, which had already been widely criticized for lax privacy practices, has advised its customers to change their passwords, as the hacker gained information about their e-mail accounts as well.)

The trove provided an unusually detailed window into computer users' password habits. Typically, only government agencies like the F.B.I. or the National Security Agency have had access to such a large password list.

"This was the mother lode," said Matt Weir, a doctoral candidate in the e-crimes and investigation technology lab at Florida State University, where researchers are also examining the data.

Imperva found that nearly 1 percent of the 32 million people it studied had used "123456" as a password. The second-most-popular password was "12345." Others in the top 20 included "qwerty," "abc123" and "princess."

More disturbing, said Mr. Shulman, was that about 20 percent of people on the RockYou list picked from the same, relatively small pool of 5,000 passwords.

That suggests that hackers could easily break into many accounts just by trying the most common passwords. Because of the prevalence of fast computers and speedy networks, hackers can fire off thousands of password guesses per minute.

"We tend to think of password guessing as a very time-consuming attack in which I take each account and try a large number of name-and-password combinations," Mr. Shulman said. "The reality is that you can be very effective by choosing a small number of common passwords."

Some Web sites try to thwart the attackers by freezing an account for a certain period of time if too many incorrect passwords are typed. But experts say that the hackers simply learn to trick the system, by making guesses at an acceptable rate, for instance.

To improve security, some Web sites are forcing users to mix letters, numbers and even symbols in their passwords. Others, like Twitter, prevent people from picking common passwords.

Still, researchers say, social networking and entertainment Web sites often try to make life simpler for their users and are reluctant to put too many controls in place.

Even commercial sites like eBay must weigh the consequences of freezing accounts, since a hacker could, say, try to win an auction by freezing the accounts of other bidders.

Overusing simple passwords is not a new phenomenon. A similar survey examined computer passwords used in the mid-1990s and found that the most popular ones at that time were "12345," "abc123" and "password."

Why do so many people continue to choose easy-to-guess passwords, despite so many warnings about the risks?

Security experts suggest that we are simply overwhelmed by the sheer number of things we have to remember in this digital age.

"Nowadays, we have to keep probably 10 times as many passwords in our head as we did 10 years ago," said Jeff Moss, who founded a popular hacking conference and is now on the Homeland Security Advisory Council. "Voice mail passwords, A.T.M. PINs and Internet passwords — it's so hard to keep track of."

In the idealized world championed by security specialists, people would have different passwords for every Web site they visit and store them in their head or, if absolutely necessary, on a piece of paper.

But bowing to the reality of our overcrowded brains, the experts suggest that everyone choose at least two different passwords — a complex one for Web sites were security is vital, such as banks and e-mail, and a simpler one for places where the stakes are lower, such as social networking and entertainment sites.

Mr. Moss relies on passwords at least 12 characters long, figuring that those make him a more difficult target than the millions of people who choose five- and six-character passwords.

"It's like the joke where the hikers run into a bear in the forest, and the hiker that survives is the one who outruns his buddy," Mr. Moss said. "You just want to run that bit faster."