The top 50 passwords you should never use
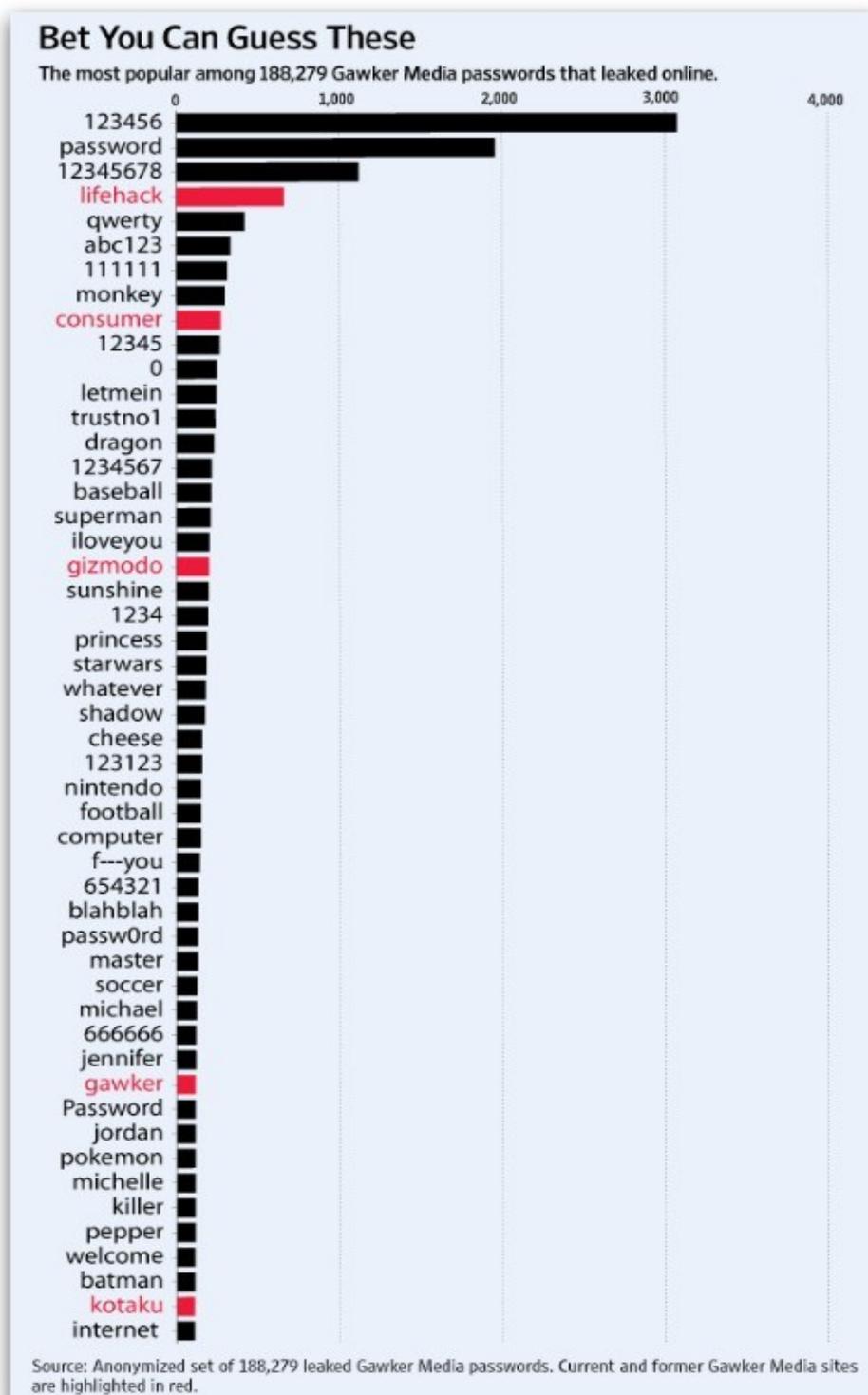
by Graham Cluley on December 15, 2010

Are you one of the many people who is using a dangerously easy-to-guess password?

Maybe now's the time to fix that before it's too late.

Twitter, LinkedIn, World of Warcraft and Yahoo are amongst the popular websites which are advising users to change their passwords in light of the recent security breach at the Gawker Media family of sites.

The issue is that many people (33% in our research) use the same password on every single website. That means that if your password gets stolen in one place (like Gawker's Gizmodo or Lifehacker websites), it can be used to unlock access to other sites too.

Bet You Can Guess These
The most popular among 188,279 Gawker Media passwords that leaked online.

Source: Anonymized set of 188,279 leaked Gawker Media passwords. Current and former Gawker Media sites are highlighted in red.

Unfortunately, an analysis of the passwords stolen in the Gawker incident show that many people are choosing very poor passwords, that are easy for intruders to guess:

Disturbing isn't it? Too many of us are choosing risible passwords - and trust me, the hackers know about the most commonly chosen passwords and are quick to try them out when trying to break into your accounts. Malware like the infamous Conficker worm have even had lists of commonly-used passwords built into them - and have used them to try to spread further.

So, clearly people need to get out of the habit of using the same password everywhere, and they also need to ensure that their passwords are not easy to guess or crack.

But another thought springs to my mind. Why don't more websites test the password that you've chosen to ensure that it's strong enough?

It would be fairly simple, for instance, when a new user creates an account for the website to run the password they submit against a database of commonly used passwords and a dictionary. If the password you offer is a dictionary word, or is too easy to crack then it should be rejected by the website.

If websites simply tell users to change their passwords after the Gawker incident what's to stop folks changing their "123456" password to the just as bad "password" password?

We need to not just drum into users heads about the importance of password safety, but also police submitted passwords better to ensure weak ones *can't* easily be chosen.

Here's a YouTube video I made a while back showing how to choose a hard-to-crack but easy-to-remember password. It also explains how password management software programs like 1Password, KeePass and LastPass can help you remember all your different passwords.