

WHAT IS IT WITH PEOPLE AND PASSWORDS?

The biggest problem with web security is still weak passwords, according to spokespeople from three major IT networks.

Speaking at South by South West Interactive (SXSWi), an industry panel of security engineering managers from Twitter, Facebook and Microsoft discussed the approaches they use to secure their web services.

As featured by Tech Radar, director of trust and safety at Twitter Del Harvey claimed that education of users about security is an on-going problem. Harvey said: "Everyone knows at least one person who says 'I use the same password on every site – but it's a really good one', or 'I use different passwords on every site – I take the first letter of the site and the last letter of the site and then I put my birth year in the middle'.

"It's this big wave right now of almost identity theft-based attempts at hacking, not just on Twitter but also on Facebook and on email sites and messenger sites. There's a big push towards not necessarily brute force [attacks] but more specialised. Obviously we still have brute force issues where we deal

with, OK they've tried to log into x number of accounts in y amount of time with z combinations of passwords. And then we have rounds of phishing, straight out 'haha this you?' links."

Also speaking was Ryan McGeehan, security manager for incident response at Facebook, who concurred that awareness was a major thing for Facebook too, as he said that 'the number of individuals who use the same password across multiple sites is astounding'.

He said: "So, for instance, if some

obscure web forum that you are a part of gets compromised and the database gets leaked, and the passwords are stored in clear text, then the person who stole that database decides to try all of those usernames and passwords on other sites the success rate is astounding."

Deepak Manohar, who looks after security on Windows Live products, said that user awareness is a major concern and a major part of the Windows Live security program.



Commenting, Amichai Shulman, chief technology officer at Imperva said that social networking sites need to take more responsibility for steering users in the direction of stronger passwords.

He said that the comments made fail to take in account that people can - and frequently do - choose bad passwords. He said: "Coupled with the fact that users of these sites often don't use any IT security software and can be quite gullible at times, it's down to the operators of these sites to mandate the use of strong passwords.

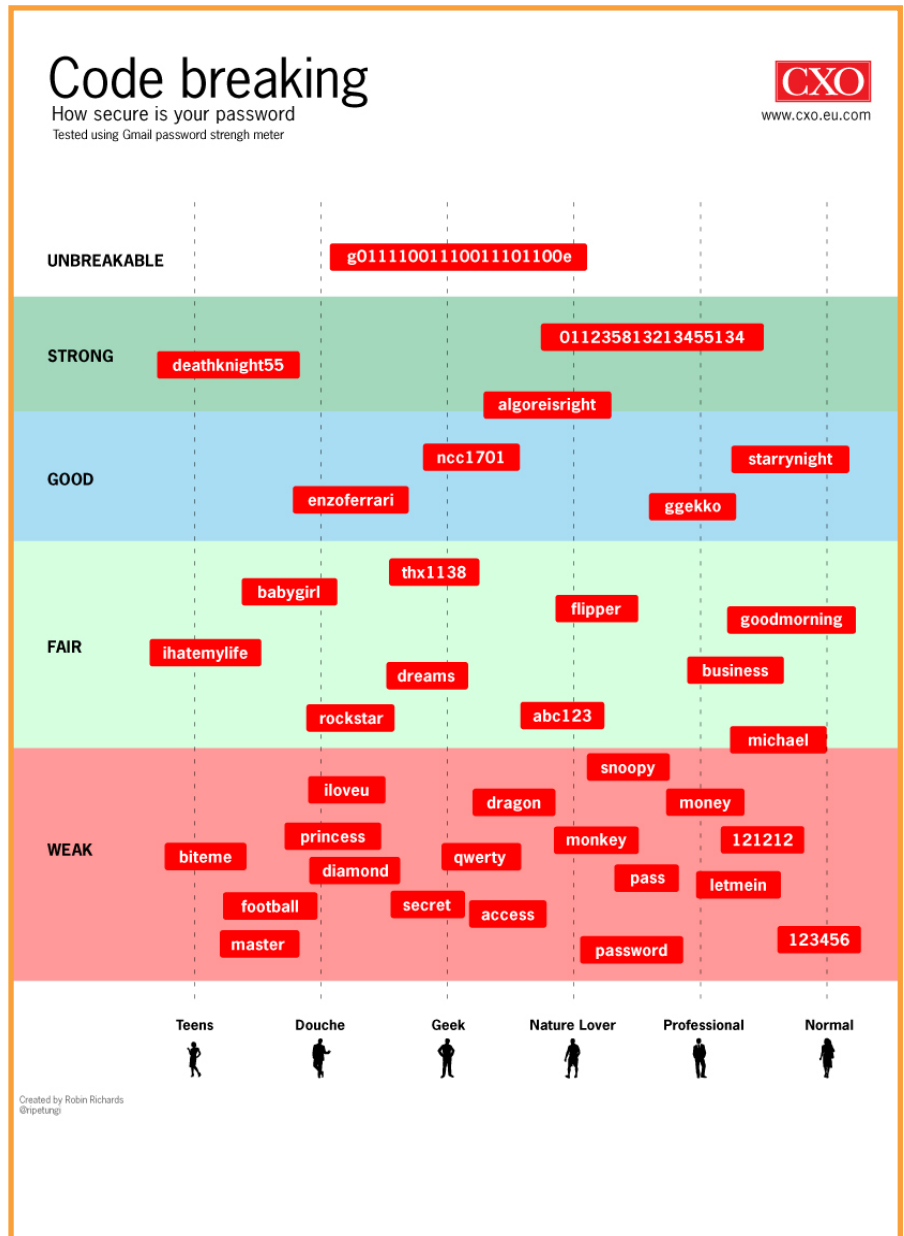
"Education as to the reasons why strong passwords are required is also useful, but far from essential. Internet history has shown that, if you mandate users to do something in return for a free service, they will do what you want - which is good news on the password front."

So what is considered a 'strong' password? Have a look at the chart below and see where you fit in to it.

Consider the following sample password combinations

- Secure = 308 million
- SeCuRe = 19 billion
- SeCuRiT_y = 53 trillion
- S3c*RI Ty = 6,095 trillion

Are you confident your data is secure?



Richard Connelly
Head of Security
Agenda Security Services
Hull, UK