

## ITAnalysis – Avoiding common password perils

By Rob Bamforth, Principal analyst, Quocirca Ltd

'Tis the season to be jolly.....careful online. Not only is there a huge amount of digital commerce traffic in the run up to the Christmas holiday season, but there are various nefarious 'cyber' activities affecting major websites and the cracking of passwords on some social networking sites.

From phone hacking (phreaking) to social engineering, hacking and malware, there have always been those wishing to exploit network and individual vulnerabilities. Passwords, the first line of personal protection for any computer user, have been in use for several decades, but the internet opened up new risks, especially now that so many destinations require user registration. Not only do people do more online, they are signing up to a multitude of services from retail and social media to dealing with government bodies and utility providers, each service requiring a user name of some sort and a password.

Managing this is becoming a nightmare and as news stories such as the recent breach in social networking service Gawker revealed, too many people have too simplistic passwords. So the slowdown and holiday season presents an ideal opportunity for reviewing and changing a few.

So what are the recommended good practices:

- Make sure the password is sufficiently long - 8 characters is a good minimum
- Use a mix of upper and lower case letter, numbers and other symbols.
- Have different passwords for different websites or services
- Change passwords regularly, (or better still, at random times)
- Avoid names, date of births or other memorable numbers like car registrations, national insurance etc
- Make substitutions eg '3' for 'e' or '\$' for 's'
- Add related suffixes or prefixes - eg 'shop' to the front of an e-commerce password

Of course this is not infallible; passwords can still be cracked with brute force algorithms or can be intercepted if transmitted in 'clear text' and are vulnerable to the visible eavesdropping of 'shoulder surfers'. It should also be remembered that a 'Colt 45 beats four aces' and real security requires more than just a clever password or two.

There is also the problem of user forgetfulness, and laziness. Many systems that force regular password changes find that the users either shuttle between two favourites or simply increment a counter at the end of the password. Passwords that are too difficult to remember might need continual resetting and this process is vulnerable to interception.

Writing passwords down used to be frowned upon, and certainly the case of a user at a major telecoms company writing a password on a sticky note then attached to the side of his PC did not go un-noticed. However, if the written passwords are physically protected and kept safely out of sight, this may not be as bad an idea as first thought. It certainly is better than storing them all in a word processing document, and is probably at least on a par with other forms of electronic password key safes since it is at least a separate mode of storage to digital.

If memorable without crack-able is the goal, then a decent starting point is a one-liner with substitution. Eg Take a memorable film, book or music title or quote ("Do they know it's Christmas time at all"), use only the first character in each word ("DtkiCtaa"), add a prefix for use on a mobile carrier's website (tel:DtkiCtaa), then substitute in your preferred way ("t3£:Dtk1Ctaa"). It might look a bit long, but after typing a few times it will sink it and it might be rather difficult for someone to snoop and remember over your shoulder on a train.

Stick with the same idea, but with different prefixes and perhaps one-liners along the way and that should be more secure and less forgettable.

## About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at

<http://www.quocirca.com>