# The Hackability of your Cyber Security Password: Great Minds Think Alike, Fools Seldom Differ

Futures Law Faculty – Kristi Erasmus
30 September 2019
https://www.golegal.co.za/cybersecurity-breaches-hack/

Today when browsing any website, filling in any online order or purchase, you are requested to enter some personal information, usually your name, email address and contact details. We seldom think much of it beyond having thought out a password which we honestly believe to offer the same level of security as Fort Knox, marvelling at our wit and intelligence in having thought of an exceptional password consisting of our or our child's/pets birthday and some inimitable lettering combination which only we would ever be able to understand. However, the truth of the matter is that most passwords are short, simple and super easy to crack. People are predictable, we think along the same lines about the same obvious words or numbers and combine them in the same simple ways to create, what we trust to be an unguessable password (Hickey, 2015), however, as the saying goes : "Great minds think alike, but fools seldom differ."

Recent research shows that the most used passwords are simple, easy, if not obvious, combinations of numbers and letters such as "123456789" as is clearly displayed on the right side of you keyboard or "QWERTY", presented at the top left side of your keyboard. Others also include the very obvious, if not thoughtless "password" ; "123"; "1q2w3e4r5t"; "00000"or "iloveyou, with popular fictional characters including Superman, Naruto, Tigger, Pokemon and Batman, acting as the cybersecurity heroes of the digital realm together with common names such Daniel, Ashely, Jessica and Charlie and well known football teams also used as popular passwords. (O'Flaherty, 2019)

We seldom if ever give our password a second thought, forgetting the intrinsic value it serves to protect and using the same password across various devices, websites, portals and login's.

Today, our personal or company data is the currency of the Fourth Industrial Revolution, used as a medium of exchange for obtaining access to a certain site, for downloading a flyer or brochure or to obtain recommendations, insights or opinions. (Ng, 2018) What it all comes down to is that personal data has an economic value which can be stored, bought, exchanged and traded – an intrinsic value, making all things possible. (Eggers, Hamill, & Ali, 2013)

This intrinsic value fosters a risk, a danger, a plausible threat of theft, unauthorised access and prohibited use of our data, the hacking of our personal information, tastes, preferences and history, with or without our knowledge, the true owners and creators of the valued data.

Although we believe we are aware of the potential risk of cyber hacking and that we , with our very unique passwords, have put sufficient cybersecurity measures in place, many of us are blind to the reality of cybersecurity breaches within South Africa. South Africa has on average over 13000 attempted cyber security attacks per day. This means that there is just under 577 attempted attacks every 60 minutes, or just over 9 per second. (Smith, 2019) Mobile malware has increased by 17%, (Smith, 2019) with a 50% increase in cyberattacks on smartphones and the android phone being ranked the second most targeted in South Africa in respect of banking malware. (Palmer, 2019)

South Africa companies that have fallen prey to cyberattacks and hacking in the last couple of years include, Liberty Life during June 2018; ViewFines during May 2018, the South African Deeds Office during November 2017, Buffalo City Municipality and Eastern Cape Educational Department during June 2017, Ster-Kinekor during May 2017, Old Mutual during 2017, KFC during December 2016 and well in to 2017, University of Limpopo during 2016, the SABC during July 2016, Armscor during July 2016, Standard Bank of South Africa during June 2016, Postbank during January 2012 and the South African Government during December 2012 (Grove, 2018) (Niselow, 2018).

These are only the high profile cybersecurity breaches that were reported in the media. There are numerous, less evident, more frequent, cybersecurity breaches and hacking occurring on a daily basis, normally discovered only when its already too late and sensitive data has been compromised and millions of Rands lost, which are not always reported on or made publicly known given the fear of public outrage and the outdated knowledge and the laissez faire approach of regulators.