Publication: DIAMOND FIELDS ADVERTISER
Date: 2015-09-01
Page: 6

It is all in your password

Technology brings with it convenience and the benefits of making life easier on many fronts. For example, one can shop or bank from the comfort of one's own home. But it also makes life easier for criminals who prey on unsuspecting targets.

Cybersecurity firm Kaspersky Lab says that 64 percent of South Africans have faced serious threats from criminals. Security firm Wolfpack Information Risk estimates that cybercrime costs South Africans between R2.5 billion and R5.8 billion annually.

BAD HABITS

A study by researchers from Stellenbosch University found that South African password users often lack security-related knowledge, which results in users who tend to "make up their own rules" regarding passwords.

Some users overestimate their password abilities while others underestimate their vulnerability. Kaspersky Lab reported that at least 20 percent of South Africans mistakenly believe that their passwords would have no value to cybercriminals and as a result do not take the necessary protective measures.

Because some people have so many passwords to remember, they choose weaker passwords (such as their pet's name or favourite colour) that are easier to remember, but less secure. Using the same password for more than one purpose and re-using previous passwords are other examples of poor behaviour.

The study also found that 65 percent of respondents were not sure what a "strong" password was. Unsafe practices evident from this study include using personal information when creating passwords, using old passwords or the same password simultaneously for multiple sites, sharing passwords and not changing passwords regularly.

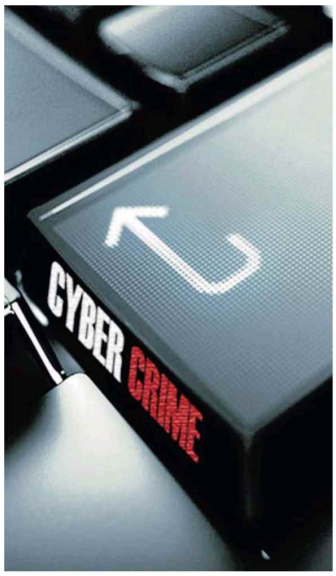
CREATING STRONG PASSWORD

The researchers make the following suggestions for improved computer password security:

• Create strong, complex passwords. Do not use information that may be associated with the user (such as personally meaningful words, numbers or dates) and use a combination of alphabetical and numerical characters.

• Do not use letters sequential in the alphabet, sequential numbers or letters, or numbers consecutive on keyboards (such as "12345" or "QWERTY"). Longer passwords are more difficult to guess. When creating passwords, keep the risk associated with the use of that password in mind. Choose even stronger, more complex passwords for high risk purposes, such as for internet banking.

• Using passphrases is a safe technique to remember passwords. Passphrases are longer and easier to remember than ordinary passwords. It can include words (or phrases or full sentences) and numbers, both upper case and lower case letters, as well as special characters, for example "Iamthe#1passwOrdcreatOr".



• Another secure habit is the use of the mnemonic method, where the user selects a phrase, extracts a letter from each word in the phrase, then adds numbers or special characters to create a password, for example using the phase "I am the #1 password creator.", the password can be "Iat#1pc".

CULTIVATE GOOD ONLINE HABITS

Use only safe techniques to store passwords. Do not write passwords down or keep them in lists that are not password-protected. Rather, use reliable password manager programs such as Dashlane or Roboform.

Also, make use of the following good password management practices:

• Do not share passwords;
• Do not re-use old passwords;
• Do not use the same password simultaneously for more than one purpose;
• Change passwords regularly.

Access to personal banking details is usually controlled by passwords. As financial gain is the cybercriminals' major motive, they use various methods to try to hack or guess passwords to gain access to individual financial accounts.

DON'T GET CAUGHT PHISHING

In the recent Ashley Madison hacking episode, passwords were part of the information that was hacked by the cybercriminals.

Phishing is a commonly used attempt in which criminals use emails to try to convince unsuspecting victims to disclose personal financial information (such as their account numbers and the passwords used to gain access to it).

While technology can provide a certain level of protection against some of these attacks, human behaviour remains "the weak link". When passwords are not properly created ("weak" passwords) or passwords (irrespective of whether they are "weak" or "strong") are not kept safe, it increases their susceptibility to being compromised.

There's good news. The study also showed that South Africans are willing to change their behaviour if they found that their password practices were deemed weak. Given the dangers, password users must realise their vulnerability and empower themselves with the knowledge and capability to make their password secure. – *The Conversation*