MANUFACTURE UNIQUE PASSWORDS

Create a strong and unique password always.

PHOTOGRAPHY: ISTOCKPHOTO

Every person who has had to create or change a password has experienced password exhaustion. To battle this exhaustion, it is common to repeatedly use the same password or make simple variations of the same. While this may help you to remember the password better, it doesn't always keep information secure. Because one single breach will expose you to every other site (Fleishman). The days of hacking in a stuffy basement are over. Hackers, more sophisticated now, use various tools to steal passwords. They know that people will add the least amount of complexity and the simplest choices needed to select passwords (Fleishman). In effect, by making the password unforgettable you end up making it vulnerable. This section presents a single solution with multiple steps for creating a strong and unique password every single time.

PHOTOGRAPHY: PEREZ, TONY

Roll a dice

Most popular passwords are chosen for their simplicity. In the same context, simple passphrases can replace passwords to make them more secure. A passphrase containing 5 to 7 words is virtually uncrackable (Fleishman). All websites require a minimum of 8 characters in their passwords and often there is no higher limit. It is a popular misconception to stick to the afore mentioned 8 characters when a longer password is the most secure. Diceware is a unique method for creating passphrases using the roll of a die. To create a Diceware passphrase follow these steps:

1. The die is rolled five to six times to create a hardware generated random number. Assemble the die rolls as a five or six-digit number, e.g. 45162. A simple alternate is to use five dices.
2. Find the word corresponding to the number in the Diceware list of words. This list is available at *http://world.std.com/~reinhold/dicewarewordlist.pdf.*
3. The word corresponding to 45162 is paste.
4. Repeat, steps 1 - 3, five to seven times to create a unique passphrase. E.g.: paste jazzy grip tap keys. Or you can come up with your own 5 unique unrelated words. Sometimes you can even mix up languages.
5. Once you have the passphrase, it's time to add capitalization, numbers and special characters, e.g. pAst3 jAssy gr!p tAp k3ys. In this example, the vowels are replaced thus: A for a, 3 for e, ! for i, 0(zero) for o and U for u.
6. The final passphrase is **pAst3jAssygr!ptApk3ys.**

Buy a passphrase

It's tedious to come up with one of your own passphrase all the time. If you still wish to use a Diceware password, then Mira Modi might be able to help. Modi is a young New Yorker, who sells Diceware passphrases. Her website is *www.diceware passwords.com.* She rolls dices to generate a random, six-word phrase, which she mails to each customer (Sorcher). Now all you must do with the phrase is add capitalization, numbers and special characters to make it exclusively your own Diceware password.

Use a Password Manager

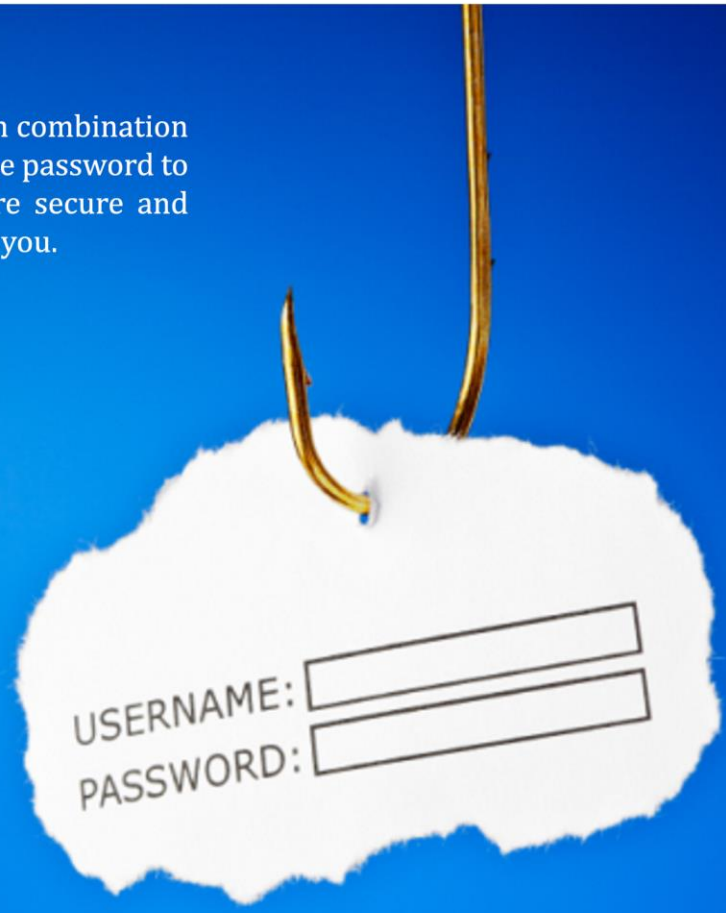
How many such Diceware passwords can be created and remembered? Not to worry, technology is here with another solution. Using a password manager, presents a simple solution for creating multiple unique passwords.

A password manager is a software service that stores all your unique passwords securely in one location. E.g. 1Password. 1Password is a password manager that generates and stores a unique password for every account. This is then locked under one strong unique password you should remember. This unique password can be your Diceware passphrase. Now every time you need to open a website your 1Password will do it.

Conclusion

By using a Diceware password in combination with 1Password, there is only one password to remember. Now all accounts are secure and only one person has access to it, you.
Sharanya Sudhakar

[word count: 630]



PHOTOGRAPHY: "AN INSIDE"

Sources:

"An Inside Look at Password Security". *Volusion.* Digital Image. 27 Aug. 2014. https://www.volusion.com/ecommerce-blog/articles/an-inside-look-at-password-security/. Accessed 16 Mar. 2017

Fleishman, Glenn."Why a Strong Password Doesn't Help as Much as a Unique One." *Macworld - Digital Edition,* vol. 32, no. 9, Sept. 2015, p. 94. *EBSCOhost*, offcampus.lib.washington.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=f5h&AN=110129450&site=ehost-live. Accessed 16 Mar. 2017

iStockPhoto. Digital Image. "Do Frequent Password Changes Increase Security?". *Parade Magazine.* https://parade.com/22396/marilynvossavant/do-frequent-password-changes-increase-security/. Accessed 16 Mar. 2017

Perez, Tony. "Thinking Through the Password Expiration Discussion". *PerezBox.* Digital Image. https://perezbox.com/2016/08/thinking-through-the-password-expiration-discussion/. Accessed 16 Mar. 2017

Sorcher, Sara. Ann Hermes Staff Photographer. "Video: How to Create a Secure Password, as Told by a 12 Year Old." *Christian Science Monitor,* 23 Jan. 2017. *EBSCOhost*, offcampus.lib.washington.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=120890526&site=ehost-live. Accessed 16 Mar. 2017