Intro to passwords

In our current day and age, passwords are one of the most common and often our best means of security within the digital world so it goes without saying how integral it is to ensure that those passwords remain strong and that no one other than yourself would be capable of easily guessing it. But as for what makes a strong password, there are some details to consider, such as how complex it is so that it cannot be broken through brute force, how easily guessable it is with enough prior knowledge such as birthdates or names of pets, how much of a well kept secret it is to where hackers cannot be able to find it, and finally just how different it is to your other passwords in the off chance that a data leak was to occur. By reviewing the standards behind good passwords from different authors, I aim to understand what exactly is needed to form a secure password by comparing the guidelines between these authors to see what comparisons and contrasts I can make and use as a summarised guideline to form your secure passwords.

Company Standards

Starting with Mark Burnett who is one of the authors of *Perfect Passwords: Selection, Protection, Authentication*, they made sure to provide both pointers and general rules to follow for forming passwords. Starting with the rule, the first is The Rule of Complexity, which consists of the length and variety of characters used in a password, and it helps resist brute-force attacks. Complexity can be attained through the use of one or two numbers placed in random locations that are not the front or back of the password, letters that are capitalized not at the front, the use of special characters again in the middle of the password when available, and the by having between 15-20 characters.[1] The second is The Rule of Uniqueness, which is about how different your passwords are between different systems. To make passwords unique, you would need to avoid common words/phrases/passwords, avoid reusing the same or similar passwords between different systems, use names/words/numbers that relate to yourself or your environment, and avoid predictable patterns/sequences.[2] You can help maintain your passwords' uniqueness by updating them every three to six months, and if you feel like there has been a security incident then change all of your passwords at once[3], by making your passwords unique it helps you become less vulnerable when a data leak occurs and make you better prepared for them. The third is The Rule of Secrecy which is, as the name suggests, about keeping your passwords secret so no one can easily find it and easily log in as you. To best maintain secrecy, you should never share your passwords with anyone (which includes friends and family), avoid saving your passwords onto your web browser or on insecure applications, always change passwords that were automatically assigned to you, delete emails that contain your passwords and use one password to set up your system and then change it into another password. For being secretive you make it difficult for hackers or any malicious

---

[1] Burnett, Mark (Mark M.)., and Dave Kleiman. *Perfect Passwords : Selection, Protection, Authentication*. 1st edition, Syngress, 2006. 122

[2] Burnett, Mark (Mark M.)., and Dave Kleiman. *Perfect Passwords : Selection, Protection, Authentication*. 1st edition, Syngress, 2006. 123

[3] Burnett, Mark (Mark M.)., and Dave Kleiman. *Perfect Passwords : Selection, Protection, Authentication*. 1st edition, Syngress, 2006. 123

passerby to be able to obtain your login details through less effort than guessing or by brute force.

Moving onto the next author, we have Ryan C. Williams who wrote *Passwords and Internet Addresses Journal for Dummies,* he listed a few solutions to a decent password and some important factors to consider. Starting with the solutions, you shouldn't pick obvious passwords that can be easily guessable such as names, birthdays, and common words.[4] Next, the longer your passwords the better as it raises the number of possible combinations and just how long it takes for someone to brute force it, and to further make it difficult to break, using a random combination of numbers, letters, and symbols when available can also help aid in the complexity of the password.[5] Moving onto the important factors, the first being how to remember passwords, while it is discouraged to keep your passwords saved onto your browser to prevent people who can gain access to your laptop from being able to immediately log into your bank accounts, and write down passwords on sticky notes or note taking apps is just as insecure, using applications designed to hold passwords that require a password to access so that you only really need to remember one password.[6] Second would be the use of encryption to make either your passwords or files only legible to you as the owner of the decryption key, you can also make use of password enhancements such as two-factor authentication, passphrases, captcha, or a VPN.[7]

Comparisons of company standards

(Conclusion) Summary of guidelines for forming a password

Citation

Burnett, Mark (Mark M.)., and Dave Kleiman. *Perfect Passwords : Selection, Protection, Authentication*. 1st edition, Syngress, 2006. https://ebookcentral.proquest.com/lib/carleton-ebooks/reader.action?docID=254851

Williams, Ryan C., et al. *Passwords and Internet Addresses Journal for Dummies*. 1st edition, For Dummies Imprint, 2013. https://learning.oreilly.com/library/view/passwords-internet/9781118828366/08_chapter-02.html#ch002-sec002

[4] Williams, Ryan C., et al. *Passwords and Internet Addresses Journal for Dummies*. 1st edition, For Dummies Imprint, 2013. Chapter 2

[5] Williams, Ryan C., et al. *Passwords and Internet Addresses Journal for Dummies*. 1st edition, For Dummies Imprint, 2013. Chapter 2

[6] Williams, Ryan C., et al. *Passwords and Internet Addresses Journal for Dummies*. 1st edition, For Dummies Imprint, 2013. Chapter 2

[7] Williams, Ryan C., et al. *Passwords and Internet Addresses Journal for Dummies*. 1st edition, For Dummies Imprint, 2013. Chapter 2