Passwords: The Human-defined Firewall

Why using 'P@55w0rd' may not be as effective as you think and how to set better passwords

DAYBLINK

Information Security

In 2018, British Airways announced that a major security breach had exposed the personal data of 565,000 customers. The airline confirmed that over a two-week period, hackers were able to gain access to names, addresses, email addresses, credit card numbers, expiry dates and security codes. Then, in 2019, a data breach at Capital One resulted in the exposure of 106 million similar personally identifiable information (PII). These attacks are just a few examples of large scale hackings and the detrimental results that they incur. Aside from the more well-known or large scale attacks, hackers often prey on individuals or small businesses as their security systems are easier hacking targets and usually guarded by a simple password.

Since the creation of internet accounts, passwords have been the front line of defense for individual account protection. While the initial passwords only required a short pincode or a random dictionary word, passwords have evolved to include special characters, upper and lower-case letters, and numbers.

According to Moore's law, processor speeds, or overall processing power for computers, will double every two years. As processing speed increases, the ability for attackers to more quickly cycle through potential passwords therefore reducing the barrier to hacking. Information security must be continually amplified in order to protect against evolving external threats. However, inadequate online password security often severely threatens the security of information.

Basic Requirements

Companies have various strategies to protect your personal information by requiring different sets of parameters when creating passwords. Examples of these required parameters include a minimum number of characters, the addition of a digit or special characters, or the capitalization of one or more characters. Although it is seemingly logical to believe that using special characters and numbers will make a password significantly more secure, it has only a minimal effect.

54%

54% of all people on the internet use 5 or fewer passwords across their entire online footprint

9.6

The average password length is 9.6 characters and has an average of 1.1 upper-case letters, 6.1 lower-case letters, 2.2 numbers and 0.2 special characters

40%

Last year, 2 out of 5 people either received notice that their personal information was compromised, an account had been hacked, or a password had been stolen

73%

73% of all online accounts are guarded by duplicated passwords

Sources

https://www.entrepreneur.com/article/246902
https://resources.infosecinstitute.com/beyond-password-length-complexity/#gref

Hackability

There are two major determinants of the ease with which a hacker can access an account: password length and password complexity. 61% of all passwords used only meet the minimum amount of characters required by online accounts, and because password requirements are fairly synonymous across sites, many people create simple passwords and use them their entire online presence. The average internet user has anywhere from 80-100 accounts, and remembering a unique and complex password for each is not feasible without devising a system of recording or maintaining. However, having one single password for all of your accounts is extremely risky as it may lead to a "domino effect". If a hacker is able to acquire the password to one of your accounts, perhaps one with lesser security, the hacker can have access to all of your accounts within seconds. Passwords used across accounts with only slight character changes are similarly vulnerable to those that are identical. Human nature is predictable, and a hacker would certainly attempt this sequence while trying to access an account. However, a randomly sequenced password is not the silver bullet; it is merely a step in ensuring that an account is well-protected.

Most Common Password Attacks

Brute Force Attack

Brute force attacks rely on hackers bombarding a system with guesses until something sticks. As a result of sheer effort and repetition, they are able to detect non-dictionary terms, such as alphanumeric combinations.

Spidering

Hackers have realized that corporate passwords are often comprised of words that are connected to the business itself. By going to the company's website or studying literature and other sales materials, hackers can build a custom word list to use in a brute force attack.

Rainbow Table Attack

A rainbow table, which is a pre-computed database of passwords and their corresponding hash values, can be used as an index by a hacker, who can cross-reference it with hashes found on a given computer.

Phishing

A phishing email will appear as a legitimate message from a company and will typically ask a user to access their account through a link in the email. After clicking on the link, the unsuspecting reader is directed to a fake login page. Once they enter their password, the hacker is able to see it. The hacker will then use that password to access the user's legitimate account.

Social Engineering

Social engineering uses psychological manipulation to gain access to an account. For example, a hacker could call an office posing as an IT security technician, and simply ask for the network access password.

Keyloggers

Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.

Sources

https://www.betterbuys.com/estimating-password-cracking-times/
https://www.itpro.co.uk/security/34616/the-top-ten-password-cracking-techniques-used-by-hackersy/#gref

Complexity vs Length

When creating a sturdy and unique password, it is important that it has stochastic behavior as that lessens the chances of a hacker guessing it. If the password has such behavior, it becomes less predictable to a threat actor. However, complexity plays a relatively small role in the creation of an ironclad password. One of the most important factors in protecting an online account is the passwords length. Increasing the length of the password allows for more variability to take place in the password, which results in an exponential increase in available password configurations. The greater number of possible passwords, the more secure your account is.

By creating a password of a certain length that includes a specific combination of elements, the choice will fit into the realm of all unique options that conform to the website requirements. Each character in a password has a limited number of possible parameters; if you choose a random lowercase letter as a character, your available options result in a 1/26 (~4%) chance of choosing any given lowercase letter.

For example, if you were asked to enter a 6-character password comprised of all lower case letters, such as "***cosmos***", the space would contain 26^6 or 308,915,776, possibilities. There are 26 possible lower case letters in the English language, and there are 6 independent spaces that make up the password "***cosmos***". While the hacker's probability of a 1 in ~300 million chance of correctly guessing your password seems improbable, attacks such as the dictionary attack make known words fairly easy to uncover.

Because the choice of lower case letters in each space is independent, the size of the password space is the product of the possibilities, i.e. 26 * 26 * 26 * 26 * 26 * 26 = $26^6 \cong$ 3.1E8. Whereas if you take "***blackholes***", a ten character lowercase letter password, it produces 26^{10} possibilities which well surpases "***cosmos***", indicating the the true power of length. If you were to follow the normal guidelines for making a password, as in the next case, then the number of possible passwords dramatically increases. For example, if you make a 10-character password that includes a random selection of upper and lowercase letters (52 total possibilities), all 10 digits, and 10 commonly used symbols (!, @, #, $, %, ^, &, ?, / and +), you would have 72 possibilities for each character space in your password. This would give you a possibility space of $72^{10} \cong$ 3.7E18, which is substantially larger than the aforementioned example, which resulted in $26^{10} \cong$ 1.4E14 .

Computer engineers and IT professionals describe the strength and complexity of a password as its "entropy". The strength of a random password as measured by the information entropy is merely the base-2 logarithm of the number of possible combinations used for a password, assuming each symbol in the password is produced independently. Thus, a random password's entropy, E, is given by the formula: $E = log_2(R^L)$.

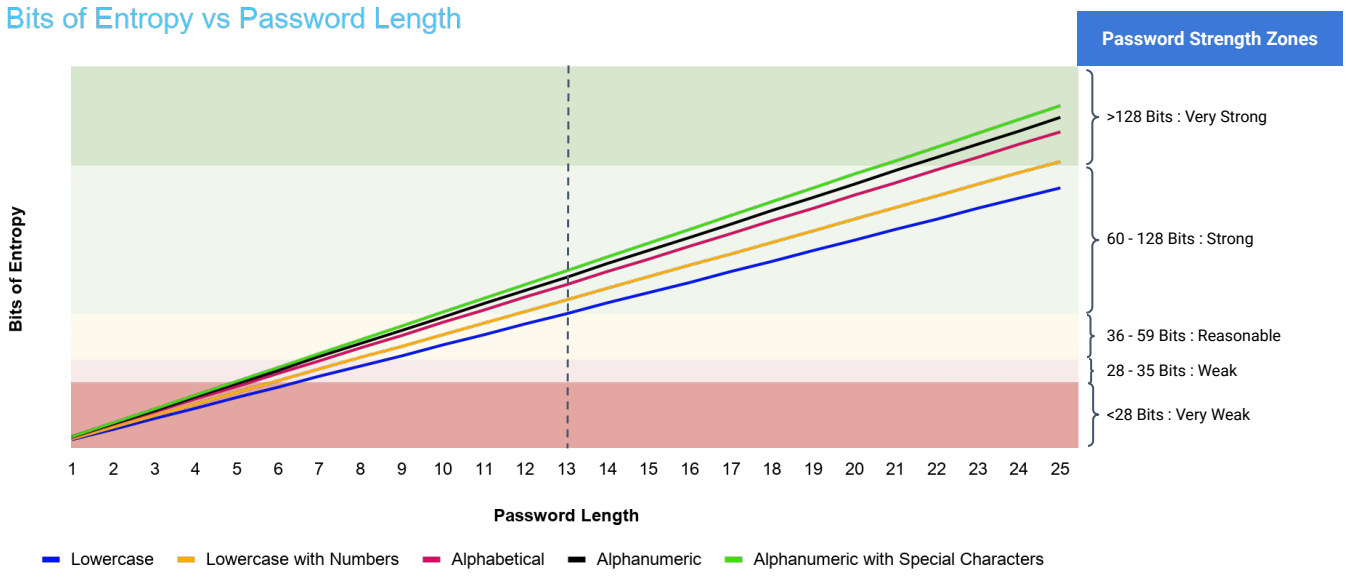
Case Study: Amazon.com – amazon.com enforces the following rules for a password while registration of a user account

- Must have a minimum of **6 characters**
- *Recommends* a combination of upper and lower case and/or a combination of letters and numbers.

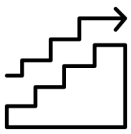
In this formula, 'E' is the password entropy in bits, 'R' is the number of unique available characters that can be included in the password, and 'L' is the number of characters in your password. In our previous example, the password "cosmos," we have a character length of 6 (L = 6, as there are 6 letters) and we have only lower case letters (R = 26, letters of the lowercase alphabet). This leads us to an equation of ***E = $log_2(26^6)$ = 20.3 bits of entropy.*** Such a password would perhaps keep a family member from accessing your account, but it would not pose a challenge for a hacker as it is a 6-letter, lowercase, dictionary word. As we have shown above, we can clearly see that length increases the possibilities of a password at a faster rate than complexity, i.e. having a higher 'L' will better increase the strength of your password than having a high 'R' would. Ultimately, choosing a high 'L' and maximizing your 'R' will create the most secure password. Determining the bits of entropy for a password is useful in demonstrating its true efficacy.

Companies and online accounts typically require users to provide a 36 - 59 bit password, while financial institutions require at least 60 bits. Although a 128+ bit password is often considered overkill, some companies do require it to protect company information. According to the aforementioned equation for password entropy, R^L should be optimized in order to achieve the required amount of bits for a password. **To amplify the entropy, you can increase the pool of characters (R), but it will increase even faster if you lengthen your password (L).**

Password Entropy



Example Lowercase	Example Lowercase with Numbers	Example Alphabetical	Example Alphanumeric	Example Alphanumeric with Special Characters
"cosmos" - 28 Bits	**"c0sm0s" - 31 Bits**	**"COSmos" - 34 Bits**	**"30Smos" - 36 Bits**	**"CO$m0$" - 37 Bits**



Password strength reaches "Strong" with **10 characters** for Alphanumeric; however, adding only 3 characters (**13 total**) to a Lowercase-only string reaches the same tier of strength

The rate of change for Lowercase-only is Alphanumeric with special characters is **6.2 bits** while Lowercase-only is a comparable **4.7 bits**

In the previous figure we can see the existence of a threshold that separates instances in which it is a necessity to incorporate complexity from those in which it is not.For example, if you have a password with **13>** characters, it is recommended that you incorporate some complexity as that will drive up your password strength. However, it seems that if you choose a password with **≥13** characters, complexity isn't as vital as it is with shorter passwords. Having an all lowercase password with 18 characters is significantly stronger than a 10 character alphanumeric with special characters password. This begs the question, is it easier to create and remember an alphanumeric with special characters password or a lengthy lowercase password?

If you create an all lowercase password, you can simply make it into a passphrase, which is, simply put, a password that is comprised of a string of words tied together. From the preceding example, an 18 character passphrase, such as "***holepenroseprocess***", is much easier to remember and more secure than a 10 alphanumeric with special characters password such as "***8^Pnn23#wW***".

Password Managers

On any given day, we interact with multiple websites, tools, and systems that require password authentication. At scale, remembering and storing passwords can become extremely burdensome. This is why some users are turning toward password managers. Used properly, a password manager, paired with two factor security, will help you efficiently orchestrate all of your online unique passwords.

Primary Benefits of Password Managers

1. **Password Storage and Encryption** - Password managers store your login information for websites you use and auto-populate your credentials when you visit the login screen. Your passwords are encrypted in a database with a master password, thus reducing the number of passwords you need to remember to just one.
2. **Unique Password Generation** - Password managers also generate and house strong, unique passwords when you sign up for new websites.
3. **Credential Capture Protection** - Password managers will only populate the usernames and passwords for domains that you saved within the tool. This protects you from entering your credentials on (sometimes) identical looking, but malicious phishing sites that attackers create to steal your credentials.
4. **Multi-device Compatibility** - Many password managers have an encrypted syncing feature across devices, you can access account information anywhere, even on your phone.

Moving Forward

When devising passwords for online accounts, one should consider the value of the personal information within the account and the level of security that makes you feel secure. For user safety, it is advised to avoid using old or repeated passwords to help prevent the hacking of multiple accounts. In order to create a secure password, one should aim to make the password longer than the minimum as lengthening a password will increase your bits of entropy faster than just simply changing an "A" for an "@".

Storing and remembering passwords has been an issue with some individuals as it's easier to create simpler and pre-existing passwords for multiple accounts, which will inevitably lead to stolen personal information. With the need for creating longer and more complex passwords increasingly apparent, using a password manager to house and generate all unique passwords is a promising solution.

ABOUT THE AUTHORS

Preston Bradham M.S. is a Analyst within DayBlink's Cybersecurity Center of Excellence

Justin Whitaker is a Partner and Practice Lead of DayBlink's Cybersecurity Center of Excellence

ABOUT DAYBLINK

In today's cybersecurity environment, the threat landscape is rapidly evolving. It's outpacing the current defensive resources and skill sets of most corporations – meaning many companies are falling victim to attacks by malicious agents. The way we do business is also changing – with more data stored, living in the cloud, and constantly demand on the go. Breaches can mean losing clients and customers overnight.

DayBlink works with clients to improve their security posture. We assess threats and vulnerabilities, identify organizational risk, prioritize remediation efforts, and implement solutions to secure IT environments and critical assets from sophisticated cyber-attacks.

For more information:
Visit: www.dayblink.com/services/technology/cybersecurity
Email: cybersecurity@dayblink.com
Call: 1 (866) 281-4403