Weak Password Policies: A Lack of Corporate Social Responsibility

Tobi A. West, CISSP, GCFE
Dakota State University
The Beacom College of Computer and Cyber Sciences
Madison, SD, USA
Tobi.West@trojans.dsu.edu

***Abstract*—Data breaches continue to occur as weak password policies prevail on major websites, at costs reaching billions of dollars annually. Password attacks are a known cause of data breaches and abuse of user accounts. Enforcing strong password policies should be considered part of an organization's corporate social responsibility. Major technology companies are socially obligated to go beyond internal policies to strengthen their password policies for external-facing consumer accounts to help reduce the risk of data breaches or sensitive data exposure. Strong, enforceable password policies are beneficial to reduce the risk of successful network attacks and prevent unauthorized access to sensitive data stored in online consumer accounts. This study includes a compilation of current password policies for major social media sites, online streaming services, and online retailers to demonstrate the lack of strong password requirements across multiple industries and spanning decades of corporate establishment in the online environment. Recommendations are provided for organizations to strengthen their password policies to align with NIST Special Publication 800-63-3 as part of their corporate social responsibility to provide protection for sensitive consumer data for millions of customers and online marketplace sellers.**

Keywords—cybersecurity, cyber security, passwords, password policy, password management, password guidelines, password attacks, password cracking, corporate social responsibility

I. INTRODUCTION

Social media sites and online merchants have an obligation to society, a corporate social responsibility, to help raise awareness of cybersecurity issues and protect user information stored on their networks, such as securing account credentials through strong password policies. Chen (2019) refers to corporate social responsibility (CSR) as self-regulated, that organizations can use the business model to remain socially accountable to consumers and all business stakeholders. Corporate citizenship is relevant to all aspects of society to enhance social objectives, including those that have environmental, economic, and quality of life impacts (Boulouta and Pitelis, 2014).

In February 2018, The White House's Council of Economic Advisers reported that the estimated annual cost of malicious cyber activity is between $57 billion and $109 billion (Anonymous, 2018). With data breaches having such a negative financial impact on the government and private sectors, organizations have a moral and social responsibility to develop a strong security posture and to raise consumer awareness about cybersecurity topics that impact customers, including establishing strong password requirements to curtail vulnerabilities. The most widely used mechanism for user authentication to access a website is a text-based password (Han, et al., 2018). Organizations providing online services should recognize the CSR associated with strong passwords.

Password requirements are the criteria of a password policy that determine the strength and complexity of the combination of characters input when a password is setup or reset (Afonin, 2017). According to Raponi and Di Pietro (2020), poor password policies allow users (i.e., consumers) to setup weak passwords that can be cracked nearly instantly. Sophisticated cracking dictionaries can break weak hashing algorithms and reveal collections of breached passwords, leaving organizations vulnerable to network intrusion (Krasznay, 2018; Raponi and Di Pietro, 2020). The following study provides an assessment of password policy guidelines identified by the government and industry followed by an analysis of password requirements for popular websites, including streaming media, social media, and online shopping. The findings of the analyses were used to formulate recommendations for development of password policies to strengthen cybersecurity best practices relative to enforcement of password requirements.

II. ANALYSIS OF PASSWORD REQUIREMENTS OVER THE YEARS

Decades ago, prior to the World Wide Web with online shopping, the computer password was first used in 1961 to accommodate multiple users for the same computer system, known as the Compatible Time-Sharing System (Bonneau, et al., 2015; Hiscott, 2013). Soon after in 1962, the password list for that system was hacked with a simple file printing request by one of the system users for non-nefarious reasons, his intent was simply to gain access to more time using that system by entering with other user's passwords. Since then password policies have not changed dramatically even though there is significantly more sensitive information online to be protected (Hiscott, 2013).

In addition to computer password policies set by the big name companies (e.g., Microsoft, Google, Amazon) that may be considered influential in the market, there are many factors that have shaped and guided how online merchants and service providers have developed their password policies for customer accounts over the years. It appears that user convenience dominates as one of the primary reasons that password policies continue to be weak on heavy-traffic websites (Florencio and Herley, 2010; Raponi and Di Pietro, 2020). Considering that users often access more than 25 password-protected sites per day, this takes significant attention to detail on the user's part if each password is different (Hiscott, 2013; Raponi and Di Pietro, 2020).

A. Password Policy Guidelines

On many of the early operating systems developed by Microsoft Corporation, the password length can be set to any number of characters between 0 and 14 (Microsoft, 2016). This Microsoft password configuration suggests that the system administrator can change the password length to zero characters which will then require no password at all for a computer login. While this type of policy may have been considered acceptable years ago for single-user systems such as Windows 7, it is not considered best practice for multi-user systems such as Windows Server 2008 or Windows Server 2012 R2, even according to Microsoft. The recommended password configuration on the Microsoft site now is to set the password length to 14 characters and enforce the password complexity rules.

Although the National Institute of Standards and Technology (NIST) established secure password guidelines in Special Publication 800-63 published in June 2004, new guidelines have since superseded with Special Publication 800-63-3 in June 2017 (Grassi, et al.). These guidelines include several specific characteristics, the password shall be at least 8 characters, ASCII characters and the space character should be accepted, redundant spaces may be condensed, no truncation of the password shall be performed, and the password shall be compared to known compromised, commonly used, or expected passwords.

According to NIST, expected passwords to be rejected may include passwords from previous breach lists, dictionary words, username, and repetitive or sequential characters (e.g., 'eeeeeeee' or 'abcdefgh'). If the password is rejected based on the expected password criteria, a reason for the rejection shall be provided and the user shall be required to choose a different password. Additionally, a password strength meter should be provided to offer guidance to the account creator.

Attempts at raising public awareness about password strength and complexity has resulted in World Password Day, which is calendared annually for the first Thursday of May (Avast, 2019). The Avast Security News Team (2019) reported that up to 18% of United States users have never changed their password and 83% have weak passwords. With the complexity and number of passwords to be remembered for daily use, it would be beneficial to have a secure place to keep them. The multitude of passwords can be stored using a password manager that can handle the variety and complexity, which may offer some relief for users with an abundance of passwords to be entered daily on frequently visited websites.

B. Managing Passwords

An application known as a password manager can be used by consumers and business organizations to keep track of passwords for multiple sites to reduce the confusion and prevent re-use of passwords to other sites (Han, et al., 2018; Towner, 2019). According to Forbes, 60 million users find a password manager useful to maintain their passwords in an encrypted fashion (O'Flaherty, 2019). For those that do not use a password manager, they may choose to re-use the password across multiple sites and/or they may choose to use the least number of characters to make the password easier to remember (Han, et al., 2018; SpecOps, 2019).

A lengthy password known as a passphrase can be used in place of a short password to add length and complexity to the password, making it more difficult to crack compared to the types of password complexity schemes suggested by NIST back in 2003 (Clark Estes, 2017; Krasznay 2018). Additionally, Krasznay (2018) and SpecOps (2019) recommends an easily memorable passphrase of at least 20 characters. Memorizing multiple passphrases may not be easy for users, that is where a password manager could be useful.

C. Password Attacks

Passwords allow access to protected and sensitive information, in some cases it is a personal account and in other cases it may be access to entire enterprise systems (Krasznay, 2018; Spitzner, 2018). A database full of passwords is a prime target for cyber criminals and may lead to loss of credentials for all users on the system. Whether that password data is stored in a plaintext readable format or a hashed format, it is a treasure trove for an attacker because the passwords can often still be cracked even if they are hashed (Dale, 2018). Password re-use on multiple accounts could mean that if one password is compromised then the other accounts for that user may be compromised as well (Raponi and Di Pietro, 2020).

There are various attacks that can be used to gain access to a user's password, including social engineering and more technical attacks. Different types of social engineering include phishing email in which a user may simply be tricked into providing their login credentials (i.e., username and password) to a website by spoofing to look like a familiar link and leading to a familiar looking website (e.g., financial institutions). Another social engineering attack may be more personal, attempting to convince a user to provide their login credentials simply by acting as a familiar company or government organization (e.g., Internal Revenue Service) (Bisson, 2019). Technical attacks include the use of brute force, rainbow tables, and dictionary attacks in which cyber criminals can use system tools to crack passwords quickly as the password is compared to a combination of characters or a list of known passwords.

According to Dellinger (2019), the quickly stolen Disney+ accounts were already worth $3 to $11 each on the hacking forums within a couple weeks after Disney+ began its online streaming services. Passwords are a prime target for attackers because the accounts can be sold for profit. Disney claims that this was not a widespread attack but was due to the types of passwords that users setup for their accounts (Dellinger, 2019). Included in the next section is the Disney+ password policy: a minimum of 6 characters, case sensitive with at least one number or special character. This a simple password policy and does not meet the NIST guidelines noted in the prior section. Surprisingly, Disney+ required that the credentials match the account setup for the user's Disneyland annual passport.

A brute force attempt taken out on a 6-character password may take as long as 10 hours with a powerful video card, or it could be instant if that password has already been compromised or is on the list of common passwords (Afonin, 2017). Multi-factor authentication (MFA) can help to reduce the abuse of cracked passwords, such as in the Disney+ situation mentioned previously. Some sites allow users to setup an additional method of verification that may involve human interaction, perhaps a one-time passcode sent via text message that must be entered after the login credentials, or a phone call to verify that the user interacts with the system. Some believe multi-factor authentication methods can lead to a loss of convenience and privacy because of the additional steps needed and the additional data stored for verification (Hiscott, 2013).

III. Password Policy Comparisons

A comparison of password policies from popular online sellers and service providers is necessary to view the landscape of account creation and the password requirements of major online retailers with large market shares. These password policies may have broader impacts and global implications on cybersecurity, in that these policies may shape and guide how users choose to setup passwords for other sites.

In order to understand the password requirements of a variety of popular websites, 15 online organizations were selected for new account creation in December 2019, using a personal email address previously created on the Google site. New accounts were created for Streaming Media Providers: *Disney+*, *Hulu*, *YouTube*, *Twitch*, and *SmashCast*; Social Media Providers: *Facebook*, *Instagram*, *Snapchat*, *Pinterest*, and *LinkedIn*; and Online Retailers: *Target*, *Walmart*, *Etsy*, *Amazon*, and *eBay*. The accounts were created similarly to identify the type of username that was required, to check whether password requirements were initially visible on screen or required a poor password attempt for the requirements to be displayed, to identify password strength and complexity requirements, and whether a password strength indicator was available to guide users with password creation.

Customer account creation on a website may include a request for some personal information or as little as an email address and password. Typically, the login type for account creation may include either a user-generated name or an email address. If a user-generated name is allowed then it is usually compared to existing usernames for that site to reject duplicates, avoiding the possibility of a user creating the same username as one previously stored for another user.

Of the 15 accounts created for this study, 4 allowed the user to generate a login name with minimum character values ranging between 4 and 8 characters. Password requirements varied with 10 of the 15 accounts requiring 6 character minimum, and 8 of the 15 accounts accepting sequential characters such as 'abcdef' for the password. Only 2 of the 15 accounts offered a password strength meter to guide users on the strength or complexity of the password being entered for the new account.

A variety of online retailers and service providers were selected to compare password policies for websites that were created over the past 25 years and that have different target audiences. For example, LinkedIn is a social media platform for professionals while Hulu is for anyone that wants to stream movies or shows. In this study, Amazon has the longest running site, since 1994, while Disney+ is one of the newest, having launched less than one month ago in November 2019 (Sherman, 2019). All of the sites have one thing in common relative to password policies, a simple minimum of 6 characters and an email address to get an account started.

A. Password Policies on Popular Sites

Table I in Appendix provides a comparison data collected during account creation, including provider name, login type, password requirements, the inclusion of a password strength indicator on-screen, the number of users reportedly accessing the site, and the year the website was established on the World Wide Web.

Some of the websites included in this study have been in existence for decades and each one has millions or more accounts containing sensitive information. With this much time providing products and services to the community and with such heavy traffic, it would stand to reason that the organizations are aware that the password policies are weak and that there are many options available as guidelines for developing stronger password policies. These organizations have a corporate social responsibility to follow the latest password guidelines provided in NIST SP 800-63-3 and change the minimum requirements for their password policies to protect the sensitive customer information stored on their systems.

In 2018, on the Amazon Web Services (AWS) blog site, Rains included "weak, leaked, and stolen passwords" as the number three-way organizations initially get compromised. The post goes on to describe the implementation of complex password policies for AWS and the Identity and Access Management (IAM) systems, which are not currently implemented on the Amazon commercial site. The Amazon retail site still allows customer account creation with as few as six alpha characters and no complexity requirements.

According to Bocetta's Dark Reading article (2019), following are the most common passwords exposed during breaches:

```
123456 123456789 password qwerty 12345 qwerty123
1q2w3e 123123 111111 12345678 1234567 1234567890
abc123 anhyeuem iloveyou password1 123456789
123321 qwertyuiop 654321 123456 121212 asdasd
666666 zxcvbnm 987654321 112233 123456a 123123123
123qwe 11111111 aaaaaa qwe123 dragon 1234
1q2w3e4r5t reset zinch 25251325 monkey a123456
1qaz2wsx 1q2w3e4r 123654 159753 222222 asdfghjkl
147258369 999999 5201314 123abc qweqwe 456789
555555 7777777 qazwsx princess qwerty1 1111111
football j38ifUbn asdfgh 66bob 888888 163.com
147258 asd123 azerty sunshine 789456 3rJs1la7qE
159357 michael 789456123 88888888 1234qwer daniel
Password abcd1234 myspace1 computer 987654321
shadow qqqqqq 1234561 killer superman pokemon
987654 master q1w2e3r4t5y6 baseball 777777
123456789a charlie 11223344 333333 soccer
x4ivygA51F
```

The above collection of re-used, breached passwords demonstrates the simplicity of many passwords and that users are often still including many sequential characters in their passwords which allows for the password to be easily cracked or hacked. For the most part, the accounts setup in this study would all have allowed any of these passwords for account creation. Hughes (2017) notes that DashLane's examination of password policies on major websites revealed that most had failed to implement even the most rudimentary password guidelines, having given ratings of 0 to popular streaming sites such as Netflix, Pandora, and Spotify.

An online password strength indicator often reflects the characteristics of a user password in either a numeric value, a Likert-scale value, or a color-coded meter to represent the complexity of the password entered. This helps users gain visibility to whether the password they are creating could easily be compromised by an attacker. The DashLane examination reports that 76% of consumer sites failed to provide any form of on-screen password assessment (Hughes, 2017). Over 30% of consumer sites do not support two-factor authentication, according to Hughes (2017), which leaves users without the choice to take extra precautions to protect sensitive information on those accounts.

B. *Limitations of the Study*

This study included only the options for entry of the password on the account setup screen and did not continue with the login process, password reset process, or other factors affecting the form in which it may be stored or the way the user may interact further with the password (e.g., typing in the password, using a password manager or previously stored password, or multi-factor authentication).

IV. Recommendations

With Facebook boasting over 2.45 billion monthly active users worldwide, the impact of the weak password policy cannot be any more profound (Clement, 2019). Facebook has deleted billions of fake accounts in 2019 alone (Stewart, 2019). These organizations should recognize the corporate social responsibility for the weak password policies that allow the abuse of account setup because the consequences are so far reaching.

Opderbeck (2017) is of the mindset that large transnational corporations have a corporate responsibility to consider implications for cybersecurity and international security in product and service development. Due to the significant reliance on digital technology for the global economy and social processes, cybersecurity is imperative to protect sensitive data that could be used to harm others financially or physically. With that in mind, there is a high level of responsibility to protect user accounts and "to reduce the most probable cyber risks" (Christen, et al., 2017). For these reasons, organizations have a corporate social responsibility to develop strong password policies that help protect sensitive user information, maintaining user privacy and preventing fraudulent use of customer accounts.

The Microsoft Identity Protection Team reports seeing over 10 million attacks every day on username/password pairs (Hicock, 2019). Microsoft provides recommendations to IT Administrators based on this experience, including a minimum of 8 characters, a ban on common passwords, enforcement of multi-factor authentication, and risk-based multi-factor authentication challenges. Similar to recommendations from other organizations, Microsoft's policy also includes the elimination of the character-composition requirements and the elimination of the periodic password reset (Hicock, 2019).

A. *Password Policy Improvements for Organizations*

Following are the recommendations for organizations when developing a password policy, especially on heavy-traffic sites. These suggestions from NIST SP 800-63-3 (Grassi, et al., 2017) and Krasznay (2018) apply to both password setup and password reset.

- Always require the use of passwords for accounts and systems containing sensitive data
- Set minimum requirements to 14 characters
- Prevent use of known-compromised passwords
- Ban commonly used passwords
- Prevent use of passwords known to be in cracking dictionaries, especially top 10
- Do not allow the username or service name to be included in the password
- Do not require periodic password reset
- Allow multi-factor authentication

- Continuous password monitoring using known-compromised passwords and common passwords to maintain an updated dictionary
- Require input of the current password on password reset requests
- Do not require reuse of the same credentials across different systems without single sign-on

B. Strong Passwords for Users

Following are recommendations for users when setting up or resetting a password, especially on sites that store sensitive or personal data. Some of these suggestions are from NIST SP 800-63-3 (Grassi, et al., 2017).

- Use a passphrase of at least 16 characters that can easily be remembered but not easily guessed
- Enable multi-factor authentication whenever possible
- Do not choose commonly used passwords or sequential passwords that are easy to guess
- Avoid words that are related to the service being protected or yourself
- Avoid words or numbers related to pet names, children's names, phone numbers, addresses, birthdates, or anniversaries
- Avoid phishing scams and other social engineering attempts that may try to obtain your password
- Avoid using public Wi-Fi that is not encrypted to protect your password
- Avoid using public computers to log into secure websites where credentials may be retrieved by other users
- Do not re-use passwords on multiple sites
- Do not share your password with others

V. Conclusion

Many of today's major online retailers, service providers, and social media sites continue to have weak password policies despite strong password policy guidelines and recommendations from industry and government being widely available. Of those studied, most sites require only 6 characters on the password setup which can be cracked instantly by hackers to gain access to online accounts containing sensitive information, including credit card numbers. The majority of users in the United States continue to have weak passwords that go unchanged for great periods of time.

This paper included a historical look at the evolution of the password and recommendations, covered an analysis of password policies for popular heavy-traffic websites, and provided recommendations for organizations and consumer users to develop stronger password policies and passwords for use online. Of the recommendations for organizations provided, the ones to be emphasized are increased minimum character limits and multi-factor authentication to be enabled for all users. Of the user recommendations, the most emphasized are to use multi-factor authentication whenever possible, to avoid re-using the same password on multiple sites, and do not share your password with others.

Short and simple passwords can be cracked quickly by hackers with malicious intent, exposing sensitive information, leaving accounts and computer networks open to data theft. Organizations have an obligation to customers to help to protect the accounts containing sensitive information on corporate systems. Corporate social responsibility dictates that organizations help to defend customer accounts by developing appropriately strong password policies to prevent users from creating simple passwords that can potentially be easily cracked leading to account compromise.

References

[1] Afonin, O. (7 Apr 2017). How Long Does It Take to Crack Your Password? Elcomsoft: Desktop, Mobile, and Cloud Forensics. Retrieved from https://blog.elcomsoft.com/2017/04/how-long-does-it-take-to-crack-your-password/

[2] Anonymous. (2018). HINDSIGHT. Risk Management, 65(3), 54-55.

[3] Avast Security News Team. (1 May 2019). World Password Day 2019 – Is your password strong enough? Avast Blog. Retrieved from https://blog.avast.com/strengthening-passwords-on-world-password-day

[4] Bisson, D. (5 Nov 2019). 5 Social Engineering Attacks to Watch Out For. The State of Security. Retrieved from https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[5] Bocetta, S. (9 Aug 2019). It's (Still) the Password, Stupid! Dark Reading. Retrieved from https://www.darkreading.com/endpoint/its-(still)-the-password-stupid!/a/d-id/1335430?ngAction=register&ngAsset=389473

[6] Bonneau, J., Herley, C., Van Oorschot, P., & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. Communications of the ACM, 58(7), 78-87.

[7] Boulouta, I., & Pitelis, C. N. (2014). Who needs CSR? the impact of corporate social responsibility on national competitiveness. Journal of Business Ethics, 119(3), 349-364. DOI:10.1007/s10551-013-1633-2

[8] Chen, J. (27 Nov 2019). Corporate Social Responsibility (CSR). Investopedia. Retrieved from https://www.investopedia.com/terms/c/corp-social-responsibility.asp

[9] Christen, M., Gordijn, B., Weber, K., et al. (2017). A Review of Value-Conflicts in Cybersecurity. The Orbit Journal, volume 1. Retrieved from https://doi.org/10.29297/orbit.v1i1.28

[10] Clark Estes, A. (8 Aug 17). The guy who invented those annoying password rules now regrets wasting your time. Gizmodo. Retrieved from https://gizmodo.com/the-guy-who-invented-those-annoying-password-rules-now-1797643987

[11] Clement, J. (19 Nov 2019). Number of monthly active Facebook users worldwide as of 3rd quarter 2019. Statista. Retrieved from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[12] Dale, C. (27 Nov 2018). Passwords and Authentication - Get Up to Speed on Attacks and Defenses. SANS Webcasts. Retrieved from https://www.sans.org/webcasts/passwords-authentication-speed-attacks-defenses-108865

[13] Dellinger, AJ. (25 Nov 2019). Setting Up A Disney+ Account? Don't Use A Princess As Your Password. Forbes. Retrieved from https://www.forbes.com/sites/ajdellinger/2019/11/25/setting-up-a-disney-account-dont-use-a-princess-as-your-password/#6740a4c42551

[14] Florencio, D. and Herley, C. (2010). Where Do Security Policies Come From? Microsoft Research. Retrieved from https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/WhereDoSecurityPoliciesComeFrom.pdf

[15] Grassi, P., Newton, E., et al. (Jun 2017). NIST Special Publication 800-63B. Digital Identity Guidelines. National Institute for Standards and Technology (NIST), US Department of Commerce. Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html

[16] Han, W., Li, Z., Ni, M., Gu, G., & Xu, W. (2018). Shadow Attacks Based on Password Reuses: A Quantitative Empirical Analysis. IEEE Transactions on Dependable and Secure Computing, 15(2), 309-320.

[17] Hicock, R. (17 Jul 2019). Microsoft Password Guidance. Microsoft Identity Protection Team. Retrieved from https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

[18] Hiscott, R. (30 Dec 2013). The Evolution of the Password — And Why It's Still Far From Safe. Mashable. Retrieved from https://mashable.com/2013/12/30/history-of-the-password/

[19] Hughes, M. (9 Aug 2017). Study: Most major websites have dreadful basic password security. The Next Web. Retrieved from https://thenextweb.com/insider/2017/08/09/study-most-major-websites-have-dreadful-basic-password-security/

[20] Krasznay, C. (2018). Fixing the Problems with Passwords. Risk Management, 65(6), 14-15.

[21] O'Flaherty, K. (20 Feb 2019). Password Managers Have A Security Flaw -- Here's How To Avoid It. Forbes. Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2019/02/20/password-managers-have-a-security-flaw-heres-how-to-avoid-it/#246e53f84e16

[22] Opderbeck, D. (2017). Cybersecurity, Encryption, and Corporate Social Responsibility. Georgetown Journal of International Affairs, 105-111.

[23] Microsoft. (30 Aug 2016). Minimum password length. Retrieved from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994560(v%3Dws.11)

[24] Rains, T. (17 Oct 2018). The Five Ways Organizations Initially Get Compromised and Tools to Protect Yourself. AWS Public Sector Blog Team. Retrieved from https://aws.amazon.com/blogs/publicsector/the-five-ways-organizations-initially-get-compromised-and-tools-to-protect-yourself/

[25] Raponi, S., & Di Pietro, R. (2020). A Longitudinal Study on Web-sites Password Management (in)Security: Evidence and Remedies. IEEE Access, 8, 1.

[26] Sherman, A. (13 Nov 2019). Disney+ already has 10 million subscribers — here's how that compares with rivals. CNBC. Retrieved from https://www.cnbc.com/2019/11/13/disney-10-million-subscribers-vs-competition.html

[27] Specops. (30 Jul 2019). 3 best passphrase practices. Retrieved from https://specopssoft.com/blog/3-passphrase-best-practices/

[28] Spitzner, L. (2019). Security Awareness Topic #6 - Passwords. SANS Security Awareness. Retrieved from https://www.sans.org/security-awareness-training/blog/security-awareness-topic-6-passwords

[29] Stewart, E. (23 May 2019). Facebook has taken down billions of fake accounts, but the problem is still getting worse. Vox. Retrieved from https://www.vox.com/recode/2019/5/23/18637596/facebook-fake-accounts-transparency-mark-zuckerberg-report

[30] Towner, N. (1 Feb 2019). CNET Asks: Do you use a password manager? CNET. Retrieved from https://www.cnet.com/news/cnet-asks-do-you-use-a-password-manager/

APPENDIX

TABLE I. PASSWORD REQUIREMENTS OF POPULAR WEBSITES

Provider Name	Login Type	Password Requirements	Password Strength Indicator	Number of Users	Year Established
STREAMING MEDIA					
Disney+	Email address	Minimum 6 characters Case sensitive At least one number or special character	Yes	10 million	2019
Hulu	Email address	Minimum 6 characters Initially no indicators displayed	No	28.5 million	2007
YouTube	Gmail address	Uses third-party Google sign-in	N/A	110 million	2005 (purchased by Google in 2006)
Twitch	Username (4 to 25 chars)	Minimum 8 characters Must qualify as at least “Weak” At least one number and one alpha character Password creation help page	Yes	148 million	2011
SmashCast	Username (6 chars minimum)	Minimum 6 characters	No	No data	2017

Provider Name	Login Type	Password Requirements	Password Strength Indicator	Number of Users	Year Established
SOCIAL MEDIA					
Facebook	Email address	Minimum 6 characters Combination of numbers, letters, and punctuation	No	2.45 *billion* (monthly active users) and 60 million business pages	2004
Instagram	Username	Minimum 6 characters	No	1 *billion* (monthly active users) and 25 million business accounts	2010

Provider Name	**Login Type**	**Password Requirements**	**Password Strength Indicator**	**Number of Users**	**Year Established**
SOCIAL MEDIA					
Snapchat	Username (5 chars minimum and must start with a letter)	Minimum 8 characters	No	310 million (monthly active users)	2011
Pinterest	Email address	Minimum 6 characters	No	265 million (monthly active users)	2010
LinkedIn	Email address	Minimum 6 characters	No	610 million	2003

Provider Name	**Login Type**	**Password Requirements**	**Password Strength Indicator**	**Number of Users**	**Year Established**
ONLINE RETAILERS					
Target	Email address	Minimum 8-20 characters At least 2 of the following: lower case letters, uppercase letters, numbers, special characters except < >	No; but has a req. met indicator	140 million (monthly active users)	1999 (founded in 1902)
Walmart	Email address	Minimum 8-20 characters	No	132 million (monthly active users)	2000 (founded in 1962)
Etsy	Email address	Minimum 6 characters	No	54 million (2.1 million sellers)	2005
Amazon	Email address	Minimum 6 characters	No	300 million (2.5 million sellers)	1994
eBay	Email address	Minimum 6 characters At least one number or symbol	No	182 million (6.7 million sellers)	1995