Password Recommendations

Trinidad Faure

2020

[Introduction 2](#_Toc24914328)

[Poor Password Practices and Their Consequences 2](#_Toc24914329)

[Recommended Password Practices 3](#_Toc24914330)

[Additional Challenges 5](#_Toc24914331)

[Conclusion 5](#_Toc24914332)

[Works Cited 7](#_Toc24914333)

Password Recommendations

# Introduction

The security and privacy of electronically stored data requires that access to that data is controlled. A username and password combination continues to be the most common form of . While more secure alternatives for authentication and authorization are available, passwords are easy to use and cost-effective to implement. Unfortunately, attackers that users have limitations when choosing passwords and that those limitations introduce vulnerabilities that they can take advantage of to gain illicit access.

In this paper, common poor practices and well-known vulnerabilities created by those practices are reviewed first. Next, the consequences of such vulnerabilities are described. Then a series of recommendations for password use are presented in a form that is easily understood by end-users. Finally, additional challenges are considered and a conclusion is offered.

# Poor Password Practices and Their Consequences

Choosing a poor password has a number of potentially devastating outcomes for the security and privacy of your personal information. Users will frequently choose passwords that are short and easy to remember. (Storm, 2016)A list of the most common passwords includes *123456*, *password*, *letmein[[1]](#footnote-1)* and other well-known passwords. (Storm, 2016)

Passwords that are short or common are not only easily guessed by a human attacker, but are even more easily broken by automated tools by hackers. These tools are built to recover passwords using a variety of techniques, including dictionary searches, brute force, and . Passwords that are eight or fewer characters and contain no variations such as uppercase, digits or symbols, are cracked in a matter of seconds by ordinary computer hardware.

Another bad habit is reusing passwords. If you have created a strong password but have reused it across multiple systems, your data are at risk. This is a result of the fact that your password for a specific system is not only under your control, it’s also under the control of the system operator. A password can be considered a “shared secret.” Therefore, you implicitly rely on the system operator to take care to safeguard your password. Experience has shown that many systems handle passwords insecurely and it has led to massive caches of usernames and passwords published online. The availability of such lists provides opportunities for attackers to try to access systems whose operators protect passwords properly but are left vulnerable due to the disclosure of passwords from other systems.[[2]](#footnote-2)

# Recommended Password Practices

The first line of defense is creating long, strong, and seemingly random passwords. Passwords should never be shorter than eight characters, but longer is always better. Always include a mix of lowercase letters, uppercase letters, digits, and symbols and have them in random places. (Schneier, 2014)For example, the uppercase letter should not just be the first character and the symbol should not just be added to the end. (Schneier, 2014)

Equally important is the practice of “one system, one password.” For every user account on every system, you should have a unique password. This means that if you have user accounts on e-mail systems, banking web sites and online shopping sites, you will have as many different passwords.

Having so many complex passwords to create and track will soon become overwhelming, so the passwords and other details about the systems will inevitably need to be recorded somewhere. Writing down passwords on paper or storing them in a traditional computer file opens different avenues for abuse. To securely store passwords and other secrets, use a software application called a . In its most basic form, a password manager is a tool used to create and protect a database of usernames and passwords and information about the system they apply to, such as the URL of a web site.

Password managers are available in two broad categories: online and offline. Online password managers keep your database on Internet-connected servers operated by the maker of the password manager. Offline password managers see online save the password database on your computer. Online password managers have the advantage of providing access to your password on different devices, though those systems may themselves be targets of attackers. If you use an offline password, you can use other tools to transfer and synchronize your password database between different devices.

Many passwords managers add user-friendly features, such as mobile applications, browser plug-ins to allow automatic form filling, and the ability to remind you when a password is getting stale, for example when it hasn’t been changed in a long time. Some of these features come at a premium price, but a password manager does not have to cost a lot to be good. (Storm, 2016)Some highly regarded offline password managers are even free. (Storm, 2016)

For some purposes, relying solely on a password manager may not be feasible. This applies to the master password that protects your password database and also to passwords you may need to enter frequently, such as your computer login password. To create strong passwords for those uses, think “passphrase” instead of password. Begin by thinking of a favorite phrase, such as a movie line, song lyric, or quote. You can then choose to obfuscate this phrase by substituting regular characters for symbols or digits, removing vowels, or adding punctuation characters.

The final recommended password practice is to keep your password secure and private at all times. You should never share your password, not even with trusted individuals. After all, you may trust them, but they may not practice safe passwords habits like you do. If you ever suspect that a password has been compromised, immediately change it and review your information on the affected system for any unauthorized changes.

# Additional Challenges

No matter how conscientiously you protect your password and avoid re-use, there are times when passwords are compromised. For example, even the savviest Internet users can fall victim to . Some of the recommended practices above can limit the negative impact of being phished, but some damage will be done. Security-minded system operators offer users an additional way to authenticate. This is referred to as two-factor or multi-factor authentication. Examples include sending a text message with a one-time code or asking for a constantly changing number that is generated by a smartphone app.

Attackers can bypass password security altogether by abusing self-service password reset provisions. Often, these provisions require providing answers to questions that only the legitimate user should know. Yet, the answers are often found online as part of social media profiles or are easily guessed. Attackers will not attempt to guess a password if it’s much easier to guess the reset answers. When required to provide one or more such answers, the best approach is to create random answers and store this in the with the other information about that system.

# Conclusion

Users must be aware that the passwords they cr are keys to private information. Short or common passwords are easily recovered by automated tools. Password reuse can compromise different systems accessed by the same user. Information security can be enhanced significantly by creating random passwords using reputable password managers, which bring implementing the recommended best practices within reach of everyone.

Users should opt-in to use multi-factor authentication whenever offered by systems. The use of a second, independent authentication mechanism makes the password less sensitive and therefore less desirable for attackers.

# Works Cited

Schneier, B. (2014, March 3). *Choosing Secure Passwords*. Retrieved from Schneier on Security : https://www.schneier.com/blog/archives/2014/03/choosing\_secure\_1.html

Storm, D. (2016, January 20). Worst, Most Common Passwords for the Last 5 Years. *ComputerWorld* , p. http://www.computerworld.com/article/3024404.

A

access control, 3

P

password manager, 5, 6

phishing, 6

R

rainbow tables, 3

1. Common passwords as obtained from data breaches. [↑](#footnote-ref-1)
2. Common passwords as obtained from data breaches. [↑](#footnote-ref-2)