Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Password Guidance

Published: 12/10/2018

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-47/2018E-PDF
ISBN: 978-0-660-29077-5

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Orientation sur les mots de passe

Password Guidance

On this page

Executive summary

Studies on extensive sets of breached passwords have led to a better understanding of user-generated passwords and, in turn, new best practices in password-based authentication.

To cope with the complexity and the growing number of passwords they have to manage, users often resort to practices that inadvertently undermine the security that password rules set out to achieve. The Government of Canada (GC) therefore needs a new approach to ensure strong authentication measures yet reduce the burden on users.

This guidance is for GC system owners and aims to promote user behaviours that improve rather than undermine system security.

This guidance recommends that GC system owners:

- remove password complexity requirements and increase password length requirements
- eliminate password expiry
- place the burden on the system rather than on users by implementing:
    - blacklisting of poor and breached passwords
    - online attack countermeasures
    - offline attack countermeasures

Two appendices contain guidance for GC system users: Appendix C covers passwords; Appendix D covers password managers.

1. Introduction

In this section

1.1 Purpose and scope

The purpose of this guidance is to establish best practices to securely manage passwords in the Government of Canada (GC). This guidance sets out advice and direction for GC system owners to consider when implementing password-based authentication systems for level of assurance 2. [1]

1.2 Intended audience

This document is primarily for GC system owners.

Appendices C and D contain guidance for GC system users:

- Appendix C covers passwords.
- Appendix D covers password managers.

1.3 Background

With its increasing in reliance on digital technology, the GC must continue to strengthen its defences against unauthorized access to its data and to its information technology (IT) assets and systems.

Passwords remain the most prevalent authentication mechanism. By controlling access, they help ensure that networks are secure and information is protected. Weak and compromised passwords are a leading cause of breaches.

Though keystroke logging and social engineering can undermine even the strongest of passwords, good password practice is nonetheless a critical part of an overall IT security strategy.

A system or network is only as strong as its weakest link, and the weakest link is often poorly secured user accounts. Poorly secured user accounts can give an attacker the foothold they need to compromise a system. By infiltrating even a basic user account, an attacker may be able to infiltrate an entire system by, for example, launching phishing attacks or installing malware. The attacker can then more readily access privileged accounts such as system administrator accounts.

To keep systems secure, users are typically required to create complex passwords. To cope with the complexity and the growing number of passwords they have to manage, users often resort to practices that inadvertently undermine the security that password rules set out to achieve. The Government of Canada (GC) therefore needs a new approach to ensure strong authentication measures yet reduce the burden on users.

2. Help users help you

In this section

2.1 Favour length over complexity

Forcing users to compose complex passwords that include lowercase, uppercase, a digit, and special characters was intended to lead to stronger passwords. It has, in fact, done just the opposite. Struggling to remember a growing number of complex, expiring

passwords, users often do the bare minimum to meet the complexity requirements. For instance, one of the most common passwords is “password”. To meet complexity requirements, an alarming number of users use “Password1” or “Password1!”.

To help users create better passwords, GC system owners are encouraged to:

- disable or reduce complexity policies (for example, allow all-lowercase passwords in which users can, if they like, include uppercase letters and other characters)
- require longer passwords (at **least** 12 characters) and have no limit on length
    - System owners should permit pass**phrases**, and users should use a phrase of at least 4 or 5 random words that meets the minimum 12-character length requirement.
    - In Windows environments, GC system owners should consider having a 15-character minimum to prevent weak LAN manager password storage. [2]

See Appendix B for recommended minimum password length for situations where some degree of password complexity is still required (for example, in legacy systems or because of technological limitations).

2.2 Eliminate password expiry

Forcing users to change their password at regular intervals puts a significant burden on users and has little effect on security. Typical password validity periods do little to prevent password cracking and, once a password is cracked, an attacker still has ample time to exploit the system. Also, users tend to select weak passwords that differ only slightly, and predictably.

GC system owners are therefore encouraged to require users to change passwords only when there is a good reason to do so, for example, in case of a known or suspected compromise.

2.3 Blacklist certain passwords

Past breaches have revealed that an astonishing number of users use passwords such as “password” or “123456”. Blacklisting, or blocking, passwords that are common or obvious or that appear in wordlists from previous password breaches can reduce the likelihood of a successful wordlist attack.

When GC system owners use blacklisting, they should make sure that systems tell users why a password is being denied when users try to select a blacklisted password.

3. Implement measures to counter online attacks

In this section

Online password attacks happen when an attacker interacts with a system's login screen and inputs password guesses for one or more accounts. These attacks may be automated and may originate from multiple, distributed sources (for example, a botnet).

Measures to defend against online guessing attacks include:

- throttling
- lockout
- monitoring
- two-factor or multi-factor authentication

3.1 Throttling

Throttling limits the number of attempts that can be made to login to a given account in a given period of time.

When used with blacklisting, throttling can render online password attacks largely ineffective.

3.2 Lockout

Lockout blocks access to an account after a predetermined number of incorrect password guesses. For example, a system might lock an account after 10 failed attempts.

A balance must be struck between the need to prevent an online guessing attack and the need to address the reality that legitimate users will, from time to time, type their password incorrectly.

3.3 Monitoring and risk-based authentication

Monitoring login attempts (for example, based on IP address and time of day) to detect

anomalies is another way to prevent online guessing attacks.

Monitoring mechanisms should be able to detect:

- large numbers of failed logins on an individual account
- large numbers of failed logins across many accounts

Risk-based authentication can provide an adaptable response to monitoring by computing a risk score and applying authentication controls based on the score. Risk-based authentication would analyze an authentication attempt from an unusual IP address or at an unusual time, or both, and either apply additional controls such as asking a security question or simply denying access.

3.4 Two-factor or multi-factor authentication

Two-factor or multi-factor authentication makes accounts more secure by requiring at least two steps in the basic login procedure.

When possible, GC system owners should use two-factor authentication (2FA). See Recommendations for Two-factor User Authentication within the GC Enterprise Domain for more information. As computational power continues to increase and offensive tools improve (including password-cracking tools that are driven by artificial intelligence), 2FA will become more and more important. Without 2FA, passwords will need to be longer and longer, which will add to the burden on users.

4. Implement measures to counter offline attacks

In this section

An offline attack happens when an attacker obtains the password database for a system and conducts an attack against the stored passwords.

Because this approach circumvents the online attack countermeasures listed above and gives an attacker access to greater computation power that permits, for example, many billions of guesses per second, an offline attack can rapidly expose numerous system passwords if system owners have not taken specific countermeasures.

Measures to protect against offline attacks include:

- hashing
- salting
- keyed-hashing

Password length is of particular importance in protecting against offline attacks.

4.1 Hashing

Passwords must never be stored in plain text. Systems must hash passwords using a hash encryption function approved by Communications Security Establishment Canada (for example, PBKDF2). They should also use hash iteration to increase the “cost” per guess to an attacker. A minimum of 10,000 iterations is recommended.

4.2 Salting

To protect against pre-computed rainbow table attacks, passwords should be combined with a salt when hashed. Salt values can be unique to users (for example, based on usernames) or be assigned to a group of users. When salting is not possible, it is all the more important to use the other countermeasures.

4.3 Keyed-hashing

A further password storage protection measure is to combine the password with a secret key before hashing. Although this measure is not available for all systems, it provides the highest level of password protection that is practically available.

5. References

1. Communications Security Establishment Canada, User Authentication Guidance for Information Technology Systems (CSE ITSP.30.031 v3), April 2018.
2. United Kingdom National Cyber Security Centre, Password Guidance: Simplifying Your Approach.
3. United States, National Institute of Standards and Technology Special Publication 800-63-3, Digital Identity Guidelines: Authentication and Lifecycle Management, June 2017.
4. Australian Cyber Security Centre, Passphrase Requirements, November 2017.
5. Robyn Hicock, Microsoft Identity Protection Team, Microsoft Password Guidance (PDF, 1 MB).

6. J. Bonneau, C. Herley, P.C. van Oorschot, F. Stajano. Passwords and the Evolution of Imperfect Authentication. Communications of the ACM, Vol. 58, No. 7, July 2015), pages 78 to 87.
7. D. Florêncio, C. Herley, and P.C. van Oorschot. An Administrator's Guide to Internet Password Research (PDF, 676 KB), USENIX LISA, November 2014.

6. Enquiries

For more information or for clarification of this guidance, contact ZZTBSCYBERS@tbs-sct.gc.ca.

Appendix A: Glossary

Botnet

A collection of compromised computers or devices (bots) that run malicious applications without the user's knowledge by means of a command and control infrastructure.

Hashing

A function that maps a bit string of arbitrary length to a bit string of fixed length.

Phishing

An attempt by a third party to solicit confidential information from an individual, group or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers or online banking credentials, which they may then use to commit fraudulent acts.

Rainbow table

A precomputed table for reversing cryptographic hash functions, usually for cracking password hashes.

Salting

A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

Spear phishing

Using spoof emails to persuade people in an organization to reveal their usernames or passwords. Unlike phishing, which involves mass mailing, spear phishing is done on a small scale and is targeted.

Appendix B: Password complexity equivalency

Although the recommendation is that password complexity requirements be eliminated and that a minimum password length of 12 characters be adopted, this may not always be possible (for example, in legacy systems or because of technological limitations).

Table 1 shows the minimum recommended password length for situations where some degree of password complexity is still required.

Table 1. Minimum recommended password length for different degrees of complexity

Complexity	Minimum password length
Upper, lower case letters	10 characters
Alphanumeric characters	9 characters
Alphanumeric characters **and** special characters	8 characters

Appendix C: Password guidance for GC users

Password length and complexity

Longer and simpler passwords are better than shorter, more complex ones.

“Password complexity” refers to the mixture of characters in a password. A password that contains just lowercase letters is not complex; one that contains lowercase and uppercase letters, as well as numbers, and special characters is complex.

On the surface, requiring users to use complex passwords strengthens passwords; however, because complex passwords are harder to remember, users often reuse passwords, which actually reduces overall security.

In addition, analyses of users’ passwords from past breaches show that users choose predictable patterns when they have to make a password more complex. For example, they will uppercase the first letter and use an exclamation mark as the last character.

Longer, less complex passwords, such as those composed of 4 or 5 random words, are therefore better. The extra length makes up for the reduced complexity and the reduced complexity means that users can create passwords that are easier to remember.

When a simple, all lowercase password is used, it should have at least 12 letters.

Password reuse

Past system breaches have given attackers access to over 3 billion passwords. These compromised passwords are a good starting point for password-guessing attacks. Users should therefore avoid reusing passwords. A compromised password obtained from the breach of one system may open the door to breaching other systems.

Ideally, passwords should be unique to each system. At a minimum, users should not use the same passwords for their personal accounts and their GC accounts. Users should also consider using unique passwords for their most important accounts, particularly for accounts that are used to recover passwords.

Two-factor authentication and multi-factor authentication

Many systems now offer users optional two-factor authentication (2FA) by, for example, sending a one-time code or prompt to the user by text message or through an app. Using 2FA can help prevent accounts from being compromised. Users are encouraged to use 2FA, particularly when using untrusted networks such as the Internet. They should also consider using 2FA on their personal accounts, such as Google, Apple, Facebook, LinkedIn and Twitter accounts, to help prevent their personal accounts from being used to devise spear phishing attacks against GC user accounts.

Password tips

The following tips can help users create and manage secure passwords.

- Use a passphrase. Passphrases are easier to remember and can be just as secure as shorter, more complex passwords.
    - Choose 4 or 5 randomly selected words (for example, correct horse battery staple).
    - Include words from another language (for example, correct cheval battery staple).
    - Try the Schneier scheme (for example, “I like to eat pizza every Thursday for dinner” becomes something like “IltepzevThfd”).
    - Don’t use common expressions, song titles or lyrics, movie titles, quotes, and so on.
- Give a possible password the “20-guess test”: would someone who knows the user well or has access to the user’s social media content be able to guess their password in 20 attempts? Users should not include obvious facts about their life (for example, dates of birth, marriage, names of family members).

- Add complexity to a password, as long as it is still memorable. In general, every additional character or word strengthens a password or passphrase, as long as the password is still memorable.
- Use a password manager to generate a strong password (see Appendix D for guidance on password managers).
- Don’t use predictable techniques such as transposing “E” to “3” or “a” to “@”. Such techniques provide a false sense of security and are highly susceptible to automated guessing attacks.
- If complexity is required, don’t simply capitalize the first letter and use a punctuation mark (especially an exclamation mark) as the last character (for example, “password” becomes “Password!”). Passwords like this are easy to guess.
- Don’t use a season combined with the year as a password (for example, “Summer2018”). This a common password strategy, so such passwords area easily guessed.
- Don’t store passwords in plain text or unencrypted (for example, in a text document or notes app).
- Don’t use any of the password examples given above.

Appendix D: Guidance on password managers for GC users

Password managers are applications that, at a minimum, store passwords securely. They can also, for example, generate strong, random passwords; automate authentication by directly interacting with login prompts; support populating common fields in forms such as name and address.

Password managers are an excellent tool for helping users cope with password overload. They also promote the use of strong, complex passwords and discourage password reuse.

Although password managers offer many benefits, they also present many risks. The greatest risk is that, if they are compromised, all the accounts associated with the passwords stored in them are potentially compromised as well. In a sense, a password manager holds the “keys to the kingdom” for a user.

Tips for using password managers:

- Don’t store GC passwords on personal devices.
- Only use password managers from reputable vendors.
- Use a password manager with 2FA capability, if possible.
- Consider omitting your most important passwords.
- Never store passwords for privileged accounts.

- Select a master password for the password manager that is at least as strong as the strongest password stored in it.
- Be diligent in installing updates for the password manager.

Footnotes

1 Standard on Identity and Credential Assurance

2 The recommendation of 15 characters is based on the recommendations in Microsoft's Passwords Technical Overview. Although that document dates from 2014, it remains an authoritative source on this topic.

[ISBN: 978-0-660-29077-5]

Date modified:
2018-12-24