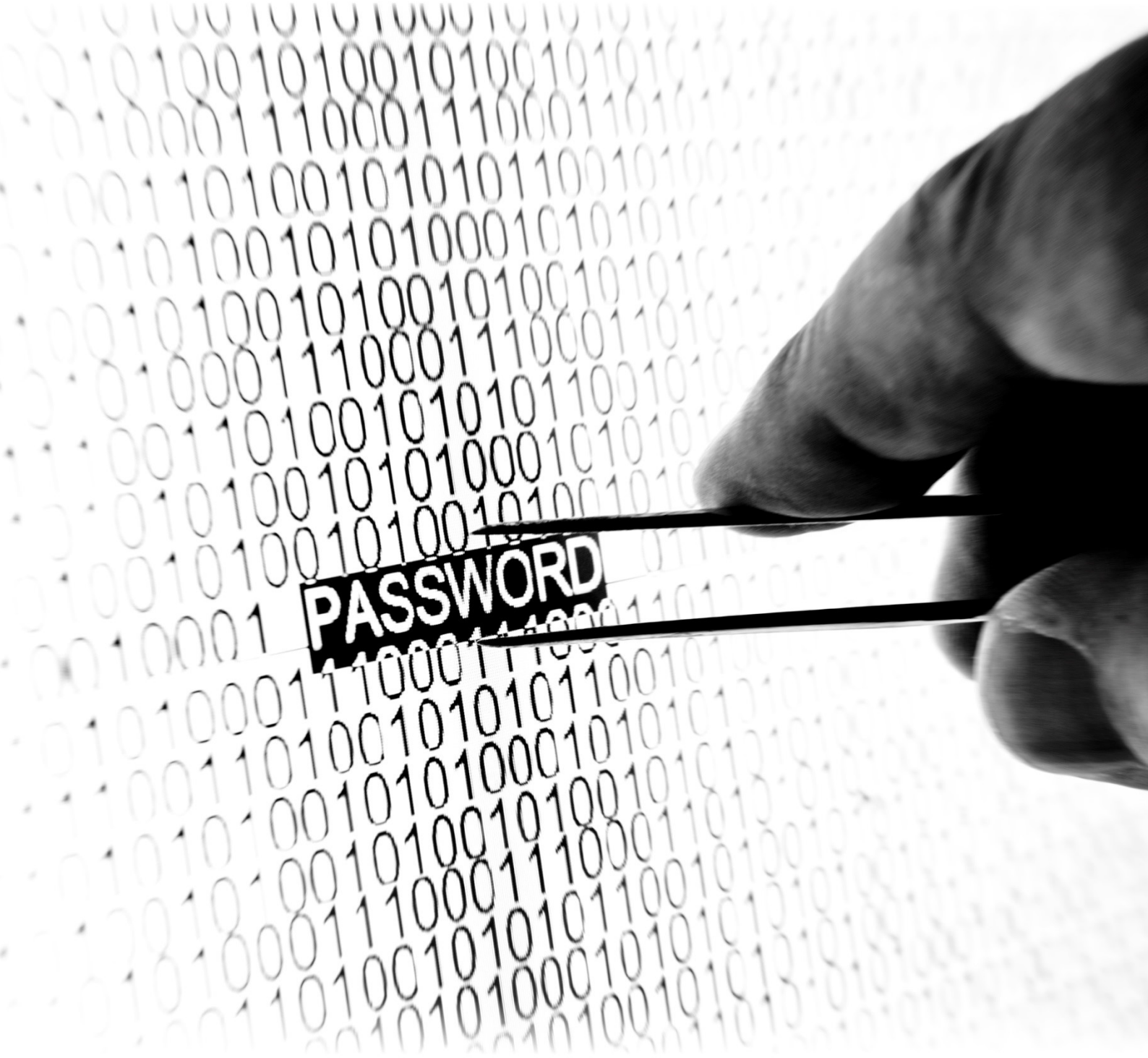
CENTER FOR CYBERSIKKERHED



Guidance

Password security

Password guide for IT users, developers, administrators and senior management.

Table of contents

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Tel: + 45 3332 5580
Email: cfcs@cfcs.dk

4th edition, November 2023.

Front page illustration: LuisPortugal/Getty Images.

Introduction

Strong passwords are essential to protecting key and sensitive information from unauthorized access. Most password guides recommend using different passwords for different accounts and longer and more complex passwords to make them harder to crack.

Many IT users find it frustrating constantly having to think of new, long and complex passwords, making it tempting to store the passwords in places that are easily accessible. However, not all password storage techniques are secure, increasing the risk of passwords falling into the wrong hands. In other words, the numerous requirements for password length and complexity may actually contribute to undermining rather than enhancing security. For instance, from a security point of view, there is a big difference between storing your passwords in a file or in a password manager.

This guide describes some of the attack techniques that hackers use as well as some of the challenges that passwords present. In addition, the guide provides a number of specific password security tips for different levels of an organization.

Below is a description of how this guide can be used by different employee groups in an organization:
IT users can use the guide as inspiration to create strong passwords and protect them from hackers. For further information, please read the chapters *What is a strong password*, *Multifactor authentication* and *How to deal with password overload*. The appendices provide examples of strong passwords.

Senior management can use the guide as inspiration to define specific password policy best practices and ensure their implementation. For further information, please read the chapters *What is a strong password, Multifactor authentication, How to deal with password overload and Awareness and training*.

The IT operations/supplier level can use the guide particularly in connection with the acquisition or operation of systems and services that require authentication. For further information, please read the chapters *Changing all default passwords*, *Focus on administrator accounts, Account lockout and login monitoring* and *Secure handling of passwords in systems*.

IT developers/system administrators can use the guide as inspiration to ensure that user interaction with passwords as well as communication and storage of passwords is performed in a secure manner. For further information, please read the chapters *Focus on administrator accounts*, *Account lockout and login monitoring* and *Secure handling of passwords in systems*.

Senior management can use the guide to familiarize themselves further with the organizational password policy. For further information, please read the chapters *Awareness and training and Organizational password policy*.

Overall recommendations

Below we have compiled a list of the overall password choice and password policy recommendations that are reviewed in this guide. Please note that the list is not exhaustive, as each organization has unique security needs.

Choice of passwords:

- Use multifactor authentication on all Internet-facing systems.
- Use multifactor authentication wherever appropriate.
- Use a password manager for password storage and generation.
- Use passwords that are at least 15 characters long.
- Avoid re-using passwords.

Password policies:

- Avoid unnecessarily complex password creation requirements – pick a good password length. Aim for lower complexity.
- Change passwords on indication or suspicion of compromise.
- Use single sign-on to facilitate user access to the organization's systems.
- Use multifactor authentication on all remote access solutions and privileged accounts.
- Introduce a password black list of commonly used passwords to prevent users from utilizing them.
- Introduce best practices for safe handling of passwords and regular awareness activities.

The challenges of passwords

Strong passwords are complex, typically requiring a mix of upper- and lowercase letters, numbers and special characters. In addition, organizations often impose minimum password length rules, and, in some cases, regular password changes may be a requirement.

Many IT users struggle to meet password requirements, especially when they have to remember numerous complex passwords. This often results in users adopting workarounds and non-secure alternatives, including reusing the same passwords across different systems, using simple and predictable password creation strategies, and storing passwords in insecure places.

When users devise their own password coping mechanisms that pose a risk to cyber security, strong passwords are not enough to defend organizations as hackers know how to exploit these well-known coping strategies to gain unauthorized access. In addition to techniques such as phishing and social engineering, where hackers try to manipulate users into giving up their passwords, tactics such as brute force, rainbow table, dictionary and password spraying attacks are used. These tactics are further described in Appendix 1, *Hacker focus points on p. 25*.

Common undesirable password practices
Most IT users cut corners when creating new passwords, choosing the easiest possible password that fulfils security requirements. For example:

- If the minimum password length is set to 8 characters, users will often create passwords that do not exceed 8 characters.
- If the password must contain uppercase letters, capitalizing the first letter is a common practice.
- If the password requires the use of numbers, users will often put the numbers at the end of the password. Numbers between 0 and 99 or numbers representing a year feature quite frequently. Replacing letters with similar-looking numbers is also common practice, for example replacing the letter ”e” with the number ”3”, or the letter ”o” with the number ”0”, etc.
- If the password must contain special characters, users will often only include one symbol. Some special characters seem more popular than others such as”@” and”!”.
- If regular password changes are required, many users will choose cyclical words such as seasons, quarters, months, etc.
- Some words and numbers are very popular and thus commonly used in passwords. The most frequently used passwords are ”123456”, ”password” and letters typed in succession such as ”qwerty”.
- The password is often the same as the username or part of it.
- The password contains names of family members, friends, pets, etc.

In connection with mandatory periodic password changes, users will often make slight variations of old passwords rather than creating entirely new ones.

Password strength
Even if an organization has multiple password requirements, leading to the assumption that the organization’s passwords are strong, this is not necessarily always the case. If, for instance, the minimum password length requirement is fifteen characters with a mix of upper- and lowercase letters, numbers and special characters, a compliant password could look as follows:

Password123456!

Commonly used passwords
As in the example above, in which the password cannot be considered secure despite meeting formal requirements, many users inadvertently choose a common password that hackers can easily crack. Lists of commonly used passwords are readily available online and may be used against a single username or against numerous usernames in a so-called password spraying attack.

The most commonly used passwords in the English-speaking part of the world.

Use of leaked passwords
When websites become the target of data leaks, for example, usernames and passwords are exposed online and quickly added to the hacker’s list of leaked passwords that are worth trying. The https://haveibeenpwned.com website allows users to check if their login credentials or accounts from their domain have been compromised in a data breach. You should never check active passwords.

What makes up a strong password?

It is difficult to provide specific advice on how to generate passwords that can resist every situation and threat. Consequently, it is important to conduct a risk assessment to determine which mix of protective measures ensures the right balance between security controls and convenience depending on the sensitivity of the asset the password protects.

If single sign-on is used to grant access to multiple systems, the security requirements should be based on the most critical of the systems. Internet-facing systems are often more vulnerable than non-Internet facing internal systems.

Even though password complexity (use of a combination of upper- and lowercase letters, numbers and special characters) reduces the risk of a brute force attack, password length is even more important. As password complexity requirements can cause users to create passwords that follow predictable patterns, stricter password length requirements should be considered instead along with other security measures. For further information on security measures that can help reduce the risk of brute force attacks, please see the section on *Account lockout and login monitoring on p.19*.

Multifactor authentication is emerging as one of the most effective supplementary security solutions that, irrespective of password strength, adds an extra layer of protection beyond passwords. For more information, see the chapter on *Multifactor authentication on p. 10*.

Alternatively, if allowed by the organization's authentication platform, eliminating passwords altogether could be a good solution. For further information, please read the section on *Password-free access on p. 9.*

Keep in mind that no system is 100 per cent secure, regardless of the number of supplementary security controls applied to the system.

Passwords and passphrases

There is a plethora of advice on password choice. Irrespective of the method chosen, it is essential that passwords are kept private. It is also important to choose an adequate password length, ideally a 15-charater minimum, especially if multifactor authentication is not enabled. For more information, see the chapter on *Multifactor* authentication *on p. 10.*

Password examples

Use the first letter of every word in a sentence, for example:
Idmrmbtwii-ros = *I don't mind riding my bike to work if it doesn't rain or snow*
(Here the word "doesn't" has been replaced by the sign "-")

Another method could be to choose a song title and combine it with the name of the artist and signs/numbers:
AbbeyRoad1969TheBeatles

Another approach could be to construct a passphrase that consists of a random string of easy-to-remember words that add length to the password. If a combination of ordinary words is used, it is important to increase the minimum password length to 20 characters.

The examples of passwords and passphrases mentioned here should naturally be avoided as they are publicly available in this guide.

Passphrase examples

A combination of words inspired by a room at home:
PotsRecipeKnifeCupboardFood

A combination of words inspired by most recent travel:
CafeMuseumPoolSunshineHoliday

It is also possible to increase complexity by replacing some of the letters with special characters. For example, changing the double o in the word pool to %, and the l to 1, making the example look like this:

If a password manager is used, making it unnecessary for a user to memorize all their unique passwords, complex and long passwords are still advisable. Such passwords can often be generated by the password manager.

Password-free access
As passwords can be difficult to remember, easy to guess, frequently reused and appear in data leaks, efforts have been made in international forums to find alternatives to passwords.

The passing of the FIDO2[1] standard has facilitated easy and secure access to websites and operating systems by using a public/private key pair instead of passwords. Authentication based on the FIDO2 standard not only solves many of the problems connected with the conventional use of passwords, it is also easy for the user to manage.

Password-free access to, for instance, an online service requires user account registration and generation of a unique public/private key pair. First, the user must choose an authenticator acceptable to the service provider (for example mobile phone or USB hardware key). The user opens the chosen authenticator by means of fingerprints, a hardware key or a PIN code, after which a unique key pair is generated. This key pair is uniquely tied to the authenticator, the user account and the service provider. The public key is sent to the service provider to be stored for subsequent validation.

When the user later accesses the provider's services and enter their usernames, the provider sends a long string of arbitrary numbers (a so-called "nonce") to the user's unit. All the user has to do is open the authenticator, just like they did during the registration phase (for example by means of fingerprints). The unit then locates the relevant private key, encrypts the number with the key, and sends the result back to the provider. The provider validates the number received by using the public key stored for the user, confirming that the user has access to their private key. Provided that the validation is successful, the user is granted access to the services.

During the FIDO2 authentication process, no passwords are sent over the Internet, just as no passwords or other sensitive information are stored at the service provider. The FIDO2 authentication process thus eliminates many of the risks associated with the conventional use of passwords, while still allowing the user to easily access the service.

The CFCS recommends that

- the minimum password length should be set to 15 characters.
- 5-word passphrases with a total minimum length of 20 characters should be used if passphrases are an option.
- passwords should never contain information that can be associated with the user or the organization, such as brands.
- passwords should not be reused.

[1] For more information on FIDO2, please visit: https://fidoalliance.org/fido2/

Multifactor authentication

Today, most systems offer multifactor authentication – one of the most effective security measures to increase login security in connection with access to sensitive information in IT systems. If multifactor authentication is implemented, password strength requirements may be lowered – both in terms of length and complexity.

Multifactor authentication is an authentication method in which the user is granted access after entering their username along with two or three of the following authentication factors:

- Something the user knows (PIN code or password),
- Something the user has (ID card, key card or USB keys)
- Personal features of the user (facial recognition or fingerprints), also known as biometric characteristics.

Most often multifactor authentication requires a combination of verification factors such as a password (something the user knows) and a mobile phone (something the user has) to access a device or service.

Multifactor authentication is already widely used, often in connection with remote access or online banking services. As multifactor authentication offers very strong login security, implementation is advisable wherever possible, and as a minimum on systems that require a high level of security. If, for instance, an account can be used to reset forgotten passwords to other accounts, it should be protected by multifactor authentication.

There are several different methods available for multifactor authentication, including mobile apps generating single-use codes or asking for verification during login attempts, biometric measures such as fingerprints or facial recognition, and USB keys (the latter also being an option in connection with password-free access).

Multifactor authentication based on codes delivered by SMS is considered less secure than other methods and should be avoided. If for some reason it is the only available approach, it is better than relying on passwords alone.

Factors such as security requirements and administration and technology resources determine the method best suited for the individual organization or purpose.

Remote user access
Multifactor authentication should always be employed for remote access. A remote access user will often access organization networks from less secure off-site locations such as the user's own personal network, hotel rooms or cafes. In such locations, organizational security controls cannot be applied, and passwords could thus be more vulnerable to compromise.

The CFCS recommends that

- multifactor authentication should be implemented wherever possible.
- multifactor authentication should always be used for access to privileged accounts.
- multifactor authentication should always be employed for remote access to internal systems.

How to deal with password overload

To alleviate IT users from having to manage numerous and complex passwords, the organization must pinpoint systems where passwords are required and define password length and complexity requirements. It would be relevant to consider keeping systems and services that do not require high levels of security password-free or setting lenient password length and/or complexity requirements.

Single sign-on
Single sign-on helps relieve IT users of the burden of remembering numerous passwords. Single sign-on is standard practice in most organizations, allowing users to use a single set of credentials to gain access to multiple systems. However, if the password is compromised, all of the user's systems are open to hacker attacks, making security a key priority also when using single sign-on systems.

The security and privacy concerns of logging into websites or services using Microsoft, Google, Facebook, or other 3rd party accounts are not covered by this guide.

Password managers
A password manager is a software application that allows users to store their unique and strong passwords in a secure manner. The advantage of password managers is that they enable users to create unique, complex passwords for every account that requires login without having to recall every single password. Password managers are locked by a single master password that obviously has to be strong, as hacker access to the master password would facilitate access to all the stored passwords.

Types of password managers:

- Browser-built-in password managers
- Browser-integrated password managers
- Independent password managers

Browser-built-in password managers are used in the most popular browsers to store passwords for the websites visited by the user, and they enable password synchronization across devices via the manufacturer's associated cloud services. While this solution is easy to use, it most often only supports passwords for websites, offering only limited functionality and encryption options. Even though the stored passwords are encrypted, accessing them in a secure manner depends on the level of security on the device from which they are accessed. This solution is not suitable for critical systems.

Browser-integrated password managers are installed as plug-ins in the most popular browsers. Their functionality is somewhat extended compared to that of the browser-built-in password managers, and they can often help generate secure passwords; they can assist in online searches to determine whether the password has previously been leaked online; and they can be used to check whether passwords are frequently used and thus not recommended. Passwords are stored in encrypted form at the service

provider and are synchronized across devices through their cloud service. This solution is not suitable for critical systems.

Independent password managers are generally not integrated with the browser and thus have a reduced attack surface. Website logins require activation of the password manager by pressing a hotkey or by using the copy/paste function. Independent password managers often have identical or superior functionality to the browser-integrated password managers, and the user can freely choose where to store their encrypted password database. While some password managers have built-in support for all popular cloud services, an alternative option is to store the database locally or with another cloud service provider.

If the encrypted password database is stored at a cloud service provider, synchronization is easy across computers and mobile devices, enabling on-the-spot access to passwords. Still, it is important not to rely exclusively on a single copy of the database stored at a single provider, as this will prove problematic if the service shuts down, experiences a critical outage or suffers an irreparable data loss. Backup support and access to data export are thus features that must factor into the choice of password manager.

Organizations should always opt for tried and tested password manager solutions. Also, regular updating of the chosen password manager solution is important to address any security vulnerabilities.

Regardless of the platform, it is important that the master password that is used to unlock access to all the stored encrypted passwords is very strong. It is advisable to supplement the master password with another factor such as a USB key and/or biometric access control.

Organizations with integrated single sign-on systems and few passwords usually have no need for password managers. Still, due to their tasks and responsibilities, some departments within such organizations may have a special need for storage of multiple passwords, including departments dealing with IT operations or communications and acquisitions. Solutions are available on the market that will provide large organizations that need to handle many privileged account credentials with a secure way to deal with allocation of access privileges, systematic rotation of passwords to critical service accounts, and tracking of accessor identity and time of access to passwords. In addition, password managers used to manage work-related passwords should not be used for private passwords.

Passwords required to restore access after major critical system failure should be stored in physical form in a secure location, ensuring that access to the passwords does not depend on all systems being operational.

Acquisition of password managers
In the acquisition of password managers, care must always be taken to ensure that the chosen solution meets organization security requirements. The CFCS has prepared a list of best practice recommendations for password managers.

In connection with access to the password manager:

- the master password should fulfil the organization's password policy requirements.
- the user should use multifactor authentication.

The password manager should be manufactured and operated by a country that is not considered a high-risk country by the organization.

The password manager should:

- generate random passwords that meet the password requirements of the organization as well as those of the external system or the websites.
- store passwords as hashed and salted values using well-tested password hash functions provide automatic fill-in of user login credentials on previously accessed websites and systems.
- be able to clear the password from the clipboard following a specified period of time when the password has been copied in.
- be able to warn the organization and the user of any compromises of previously accessed websites and/or systems.
- inform the user if a new password created does not conform to the organization's password policy.
- be accessible on all the user's operating systems.
- include regular security patches.
- log all activity.
- If online synchronization is used, end-to-end encryption is a requirement.

Machine-generated passwords

Machine-generated passwords can help improve security as these randomly generated passwords are less predictable than user-generated passwords and thus difficult to break, though their complexity may make it harder for the user to memorize them. If a password manager is not used, the system should offer users a choice of passwords, allowing them to select the one they find most memorable. Machine-generated passwords may comprise five randomly chosen words, or the user can choose from a pool of different passwords, whichever is easier to remember. If a password manager is used, long and complex machine-generated passwords pose no problem, as the user need not remember them by heart.

Password change

Even though mandatory regular password change used to be the standard recommendation, this is no longer necessarily the case. The motivation behind periodic password change, say every three months, was to limit the amount of time that a hacker has access to a compromised account and password. However, a drawback of frequent password change is that many users choose weaker passwords that are easier to remember or follow a predictable pattern, including basing the password on the name or number of the current month, season, etc., which hackers can easily guess.

If an organization has adopted security measures that reduce the risk of password compromise, it may, based on its risk assessment, choose to refrain from demanding regular password changes. Such security measures should include:

- Awareness training of users in how to manage and choose secure passwords
- Policies supported by technical inspections to ensure relevant password length (and possibly complexity)
- Controls to ensure that frequently used or already leaked passwords are not chosen
- Measures to ensure that the user does not recycle the same passwords
- Limitations as to the number of possible login attempts or throttling (see sections on *Account lockout and login monitoring p. 19*)

On suspicion or indication of compromise of one or more passwords, forced password change should always be initiated.

The CFCS recommends that

- password managers should be used when there is a need to store large numbers of unique passwords.
- the choice of solutions should be based on which contents is made accessible through the password and on the organization's risk assessment.
- password changes should only be forced on suspicion of compromise
- a procedure should be implemented for forced password change on suspicion of compromise.
- the organization should consider which technical solutions to implement to best aid the IT user.

Awareness and training

It is key that the organization's IT users understand the in-house password policy and observe password use and password composition rules regardless of the password strength. In addition, IT users must be aware of hacker attack techniques. IT users must know what warning signs to look for and how to respond if they are contacted by individuals posing as, for instance, IT colleagues who ask to test or reset a password, or if they receive unexpected or suspicious-looking emails.

The management is responsible for bringing the organization's IT culture and the IT users' behaviour into focus and, by extension, for informing the latter of any new attack techniques. Security awareness training should be available to guide on strong password and general security best practices, just as follow-ups should be carried out to ensure compliance with IT user behaviour requirements and expectations.

The CFCS recommends that

- management should plan and implement the necessary password policy awareness training for the organization's IT users.

Changing all default passwords

IT equipment and software often comes with default system accounts and passwords set by the manufacturer. Hackers are well aware of this, and vendor-supplied passwords must thus always be changed before deploying the equipment and software.

Default passwords may act as entry points for hackers to access an organization's IT systems and thus its business-critical information. Default passwords and usernames can be found online, and if they have not been changed, hackers will often have little difficulty in gaining access. A key area for attention is preparing a procedure on how to change default passwords – such as passwords to routers, printers, log servers and firewalls – to ensure that they are changed before being activated.

In order to ensure that organizations do not use vendor-supplied defaults upon deployment of hardware or software, it is important that accesses to equipment and software are subject to regular checks.

The CFCS recommends that

- default passwords should be changed as a standard procedure when equipment and software is deployed.

Focus on privileged accounts

Some accounts require more protection than others. Compromises of administrator, service and remote user accounts carry a high risk of unauthorized access to critical information, making extra protection of such accounts a priority. Access to such accounts should thus be safeguarded by multifactor authentication along with longer and more complex passwords.

Administrator rights
Ordinary IT users generally have no need for extended rights to IT systems and infrastructure. IT user rights must always be allocated based on professional requirements.

The system administrator role involves tasks that provide access to system critical infrastructure and to maintenance of internal IT systems, etc. As a result, administrative accounts are prime targets for many hackers, making password protection a key focus area for IT administrators. Access to administrative accounts should be secured through multifactor authentication. If, for some reason, this is not possible, longer and more complex passwords should be used. Administrative accounts should only be used for tasks where extended rights are required.

For the handling of day-to-day tasks, such as email management and Internet access, a non-privileged account without administrator rights should be used.

Administrative accounts should be personal and the password only known to the administrator owning the account. On departure of staff with administrative rights, their privileged accounts should be promptly terminated and passwords on all service accounts known to them changed. In some privileged account management platforms, this process can be automated or avoided entirely by using one-time passwords for administrative tasks.

Privilege management
In order to keep a better overview of the organization's privileged accounts, a Privileged Access Management (PAM) system can be used. PAM solutions are designed to manage, monitor and secure privileged rights and can be used to centralize and optimize the management of privileged accounts.

The CFCS recommends that

- Administrative accounts should be used exclusively for activities that require administrative privileges.
- Privileged accounts should be protected by multifactor authentication.
- a fixed and documented process should be used for shutting down privileged accesses of departing administrators.

Account lockout and login monitoring

All steps should be taken to make it as complicated as possible for hackers to penetrate IT systems containing business-critical information. The below solutions could be adopted to mitigate against several different types of the hacker attacks outlined in Appendix 1 p. 25:

Account lockout
Account lockouts can be a way of preventing hackers from using online attacks to crack passwords and break into internal IT systems. The user account is locked out once the user or hacker has exceeded the pre-defined threshold of login attempts, preventing the hacker from launching dictionary or brute force attacks.

The organization should thus prepare an account lockout policy determining the allowable number of failed login attempts. A sudden high number of attempted logins on an account may indicate malicious activity.

The policy should determine the number of minutes that must pass after a failed login attempt, before the failed logon attempt counter is reset. This approach may help avoid *password spraying attacks*, which are outlined in Appendix 1, *Hacker focus points, p. 25.* The difference is significant between whether the hacker is allowed to carry out the maximum number of unsuccessful login attempts every half hour or only once a day before the account is locked out.

It is also relevant to ensure that the policy addresses how to unlock locked accounts. It is problematic if an IT user can simply call a service desk and request that their account be unlocked and immediately be given a new, temporary password over the phone. In such cases, a hacker may pose as a user and thus gain access to the account. A potential solution to this particular problem could be for the user to be assigned a temporary disposable password via a colleague or for the password to be reset through an existing multifactor authentication method.

The organization should avoid using security questions along the line of ”What is my father’s name?” for the IT user’s own unlocking of the account, as this approach carries the risk that hackers can figure out the answer to such questions without much difficulty using social engineering tactics or open sources such as social media.

Delay of new login attempts
Another method is so-called *throttling* or *delay*. Under this method, the account is not blocked, but for each failed login attempt – or after a specified number of unsuccessful login attempts – a time delay is established before a new login attempt is allowed. This delay can be increased exponentially for each failed login attempt.

Login user notification
If a user logs in from a device that is unknown to the system, a notification of the login sent to the user, for instance through mail or text message, can help increase the chances of detecting account compromises, allowing for prompt action to be taken.

Monitoring and logging of login
In order to counter potential security breaches, the organization is advised to monitor login attempts. The monitoring will often be conducted automatically through software alerting relevant staff if, for instance, the number of attempted logins deviates from the normal rate. The warning threshold of the monitoring tool can be set to reflect the criticality or sensitivity of the system in question. The CFCS often encounters organizations that have been the target of cyber attacks where it can subsequently be ascertained that key log files from the affected IT systems are not available for analysis of the attack. Logging of equipment and systems in the organization's infrastructure is essential to the ability of authorities and organizations to quickly detect and subsequently effectively identify the consequences of cyber attacks.

The CFCS guide *Logging – part of resilient cyber defence (2023)* contains recommendations and measures on how to include logging in the organization's cyber defence regime.

The CFCS recommends that

- account lockout or "throttling" should be used.
- the organization should keep a fixed protocol on how to unlock locked accounts.
- login attempts should be logged and logins monitored.

Secure handling of passwords in systems

Organizations must ensure that confidentiality is maintained during the use, communication and storage of passwords.

Use of passwords
Login pages on systems used by the organization should allow the copying of passwords into the password field, facilitating the use of password managers. Also, there should be no rules limiting the length of the passwords, or the letters or special characters allowed. Also, it is recommended that when choosing their password, users receive a notification if the selected password is frequently used or known from previous leaks. To aid this process, password blacklists are readily available online of frequently used passwords, just as there are databases of leaked passwords that can be integrated via API (see for instance https://haveibeenpwned.com).

Organizations should, to the widest extent possible, employ multifactor authentication on the systems used and consider supporting FIDO2 password-free authentication when implementing new systems.

Communication of passwords
Use of an encrypted communication channel is recommended whenever a password is entered or otherwise exchanged between units/systems over a network.

Password hash
In order to avoid direct storage of passwords, a hash function is used. Hashing involves the conversion of a password to a hash value in the form of a fixed-length byte string. This makes it impossible to figure out the length or complexity of the password based on the hashed value, as the hashed value will always be of the same length. Even a small change to the password will completely change the hashed value.

Salt
Random value that is added to the password prior to hashing, ensuring the uniqueness of the resulting value.

Password storage
Passwords should not be stored in plain text. If the password database is compromised, it is important that data is stored securely to prevent hackers from being able to use the information directly.

Unlike encryption, conversion of passwords into hash values is a one-way mechanism, and extracting a password from hash values is a complete guessing game. Hashing requires standard implementation of a tried-and-tested hash function created exclusively for passwords.

As an extra layer of security, a unique value, a so-called ”salt”, is added to each password prior to hashing. This method ensures that even if the passwords are identical, the resulting stored value is unique, thus protecting against rainbow table attacks (see Appendix 1 p.23).

If a system supports password-free access via the FIDO2 standard, the need for secure storage of passwords is obviously reduced.

The CFCS recommends that

- user interfaces should allow use of password managers.
- user interfaces should be devised to help users choose secure passwords.
- a password blacklist should be created to prevent use of frequently used passwords.
- all communication of passwords should take place over encrypted connections.
- only hashed values based on unique salts should be stored. Hashing should be performed using standard implementations of tried-and-tested password-hashing functions.

Organizational password policy

In the effort to avoid hacking, password length and complexity requirements are often strict. Remembering multiple and complex passwords can be hard, though, making it tempting to recycle passwords or to write them down on paper or on the computer to have them readily at hand.

If the hacker threat is addressed by setting overly strict password requirements, it may unintentionally lead to poor password practice if it is not supported by, for instance, single sign-on or password managers.

The senior management could benefit from rethinking the organization's password policy to increasingly fit the organization's adapted security level, dominant culture and user behaviour. The senior management is responsible for implementing the overall password policy and ensuring that it is supported by relevant technological support solutions. In preparing its password policy, the organization must focus on the differing security requirements in terms of access control to different systems and services. For security reasons, password requirements may thus vary across the organization's internal systems and its Internet- and client-facing systems.

The CFCS has the following password policy recommendations:

- Passwords are required where necessary based on in-house security requirements.
- Unnecessarily complicated password rules are to be avoided – aim for password length and low complexity.
- No recycling of passwords across systems.
- Passwords are personal and not to be shared.
- Multifactor authentication to improve security.
- Implementation and support of password managers.
- Secure technical handling of passwords.

References

Australian Cyber Security Centre. (2021). *Implementing Multi-Factor Authentication* *https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication*

Canadian Centre for Cyber Security. (2019). *Best practices for passphrases and passwords* https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

Center for Cyber Security. (2023). *Logging – part of resilient cyber defence* *https://www.cfcs.dk/*

Grassi, P. A. et al. (2020). Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Rev. 3, Includes updates as of February 3, 2020

Hunt, T. (2022). *Have I been pwned*. *https://haveibeenpwned.com/*

National Cyber Security Centre. (2018). *Password administration for system owners* *https://www.ncsc.gov.uk/collection/passwords*

Appendix 1

Hacker focus points

Usernames and passwords are often required to access IT systems, making them valuable to hackers as tools of entry. In addition, hackers target attacks, for instance by exploiting their knowledge of users and their passwords. This knowledge may be transferred to a number of tools that enable hackers to crack passwords, for instance through installation of a keylogger that registers all keyboard activity. Below are examples of some of the tactics used by hackers to obtain or crack passwords.

Social engineering
Social engineering is a technique where hackers use psychological manipulation to trick unsuspecting users into taking actions they would otherwise not have taken. Such actions may include divulging login credentials or passing on information about the organization, its processes systems or clients.

More sophisticated social engineering often involves hackers trawling websites or a victim's social media accounts ahead of an attack to glean information about the victim or their place of work.

Social engineering can also take place through emails (phishing), text messages (smishing) or via telephone (vishing).

Phishing
Phishing is a tactic that hackers use to lure the recipient of emails into unsuspectingly passing on personal or other sensitive information or providing unauthorized access to, for instance, IT systems.

Using simple social engineering tactics, the attacker will often try to lure their victims into clicking on links to fake websites or to open infected files.

Phishing emails are non-personalized mass emails sent randomly.

Spear phishing
Spear phishing is similar to standard phishing, but differs by sending customized emails to targeted individuals, using techniques transferred from social engineering. Spear phishing emails are typically customized to appear particularly relevant, convincing and credible to the individual recipient, for instance by including names or other types of information specifically related to the recipient that have been harvested in connection with a reconnaissance phase preceding the attack.

Password reuse
Many users often recycle passwords – at work as well as at home. Password reuse carries a high risk of hackers gaining access to not just one but multiple systems when a password is leaked or otherwise compromised.

Dictionary attacks
In dictionary attacks, hackers deploy a list of potential, often commonly used, passwords. Attacks are automated trying out passwords from the list to crack specific passwords. Using a list containing a wide number of common words increases the chances of the hackers finding the right password.

Brute force attacks
In brute force attacks, hackers systematically try all possible combinations of special characters, numbers and letters. Though such attacks can be very time-consuming, they will always be successful provided that the hackers have sufficient time and computational power at their disposal.

Rainbow table attacks
Passwords are hardly ever stored in plain text. Instead, passwords are converted by a mathematical one-way mechanism, a so-called hash function. In order to crack these hashes, hackers can use a rainbow table containing a large number of precomputed hash values of the most commonly used passwords. If they succeed in finding a matching hash value in a rainbow table, the password has been cracked.

Password spraying attacks
Hackers may attack a system by entering popular passwords across all accounts of a particular system. In a large organization with hundreds of users, chances are high that the hackers will eventually guess one or more passwords. This technique is known as password spraying. As most organizations are protected by account lockout policies, hackers are careful to try only a few passwords against each account to avoid account lockout.

Default passwords
New hardware and software often come with vendor-supplied default passwords. If these passwords are not changed by the user, hackers can use their knowledge of the default passwords to obtain administrator access.

Below are examples on how to build strong passwords or passphrases. Please note that the examples provided should not be used in their current form.

Appendix 2

Examples of passwords (at least 15 characters)

Method 1:

- Choose a country and its capital
- Remove the last letter in the name of the country
- Insert at least 2 characters or numerals between the words

Examples:

1. Vilnius#05Lithuani
2. Paris17/&Franc

Method 2:

- First letter of all words in a long sentence
- Specific letters could be replaced by numbers or special characters

Examples:

1. Idmrmbtwii-ros
   (I don't mind riding my bike to work if it doesn't rain or snow)
2. Wig4y,bd2moiin!
   (Water is good for you, but drinking too much of it is not!)

Method 3:

- Title of song and name of artist separated by special characters or numbers

Examples:

1. LovingYou#Elvis
2. 1stWeTakeManhattan&Cohen
3. AbbeyRoad1969TheBeatles
4. BadGuy!BillieEilish

Examples of passphrases (min. 20 characters)

Method 4:

- 5 things/concepts from a room in your house, your latest trip, the shopping basket, etc. – begin all words with capital letters.

Examples:

1. PotsRecipeKnifeCupboardFood
2. CafeMuseumPoolSunshineHoliday
3. FruitYoghurtKiwiCakesCoffee

Please keep in mind that some systems do not allow the use of national characters, in which case they may be replaced by alternative characters.