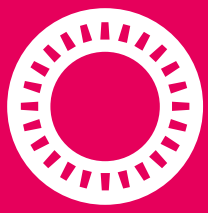


MATESO
PASSWORD SAFE

Password Guidelines

Time for a Paradigm Shift?

Contents

Introduction

More and more security experts are of the opinion that prescribed password guidelines are more likely to harm than benefit the IT security of companies. The German Federal Ministry for Information Security (BSI) now advises against fixed minimum requirements for the complexity and length of passwords, as well as against changing them regularly.[1] The National Institute of Standards and Technology (NIST) has also withdrawn its former recommendation to change passwords every 90 days and has scaled down its complexity requirements.[2]

This whitepaper discusses the risk and security potential of enterprise password policies and the evolution toward loosening them to provide recommendations for action.

> **Passwords should only be changed within a valid reason.**
>
> Federal Office for Information Security

Risik Analysis

In order to create transparency about the type and extent of potential risks posed by password policies in practice, the first step is to define the requirements for a secure password and how to deal with them. Subsequently, possible causes for a paradigm shift are identified and evaluated.

Password Security Requirements

When passwords are created, complexity and length are two decisive characteristics for security. According to the BSI, an independent password of at least eight characters in length must be defined for each application and this password must be kept secret and securely stored. It must only be known to the user.[1]

7 golden Password Rules

(UN?v*UG7p!9?aaQ/	**The more complex and longer, the better**
*****	**Use a unique password per access**
ABC 123 !?$	**Don‘t be stingy with: Upper and lower case letters, numbers and special characters**
	Introduce regular change intervals
PASSWORD1234	**Do not use words or sequences (123, abc, qwerty)**
	No-Go: Information like date of birth, pet name & Co.
PASSWORD SAFE	**Support is strongly recommended: Use Password Generators and Password Manager!**

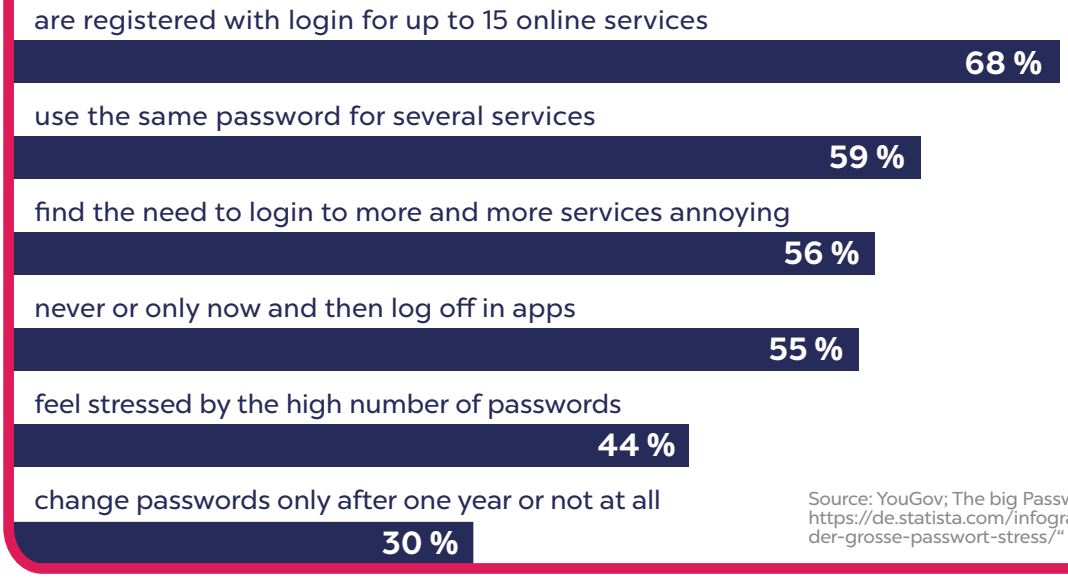
The password should contain special characters, numbers and alternating have upper and lower case letters and does not contain words from the dictionary. No-Go`s are rows of numbers and letters and keyboard patterns. So far, it was also suggested to change the password after a certain time.[3]

Confusion & Overload as a Result

If we now compare these requirements with the fact that each user has to manage at least 15 online accesses, it becomes clear that compliance with various rules can quickly overwhelm the individual employee in reality.[4] As a result, the so-called „password fatigue“ spreads among employees - the feeling of being overwhelmed when creating and remembering too many, too complex passwords.

The big Password Stress

Surveyed Internet users on their handling of passwords



Source: YouGov; The big Password Stress
https://de.statista.com/infografik/7705/
der-grosse-passwort-stress/“

This burden is further increased by automatic log-outs requiring re-typing of passwords and the challenge of providing access to colleagues without violating policies. The more rules are added, the more likely employees will capitulate and resort to insecure workarounds.

Insecure Workarounds in Practice

When employees are overwhelmed, password policies grasp at nothing. Instead, they resort to insecure means that are often not even known to internal IT. According to the market research company Ipsos, one in two people memorize their own passwords. So in the first case, no secure password is created in the first place.[5]

In the second case, the employee creates a complex password. However, since they are difficult to remember, 1 in 5 simply write it down and use it for several services at the same time.[5] Equally popular as dangerous are also homemade solutions such as storing in the browser or in insecure documents like Excel lists. Only 1 in 3 changes his password regularly. If the password does change, tricks are used by replacing or appending only one character.

Lower Specifications as a Solution?

As a result, the German Federal Office for Information Security (BSI) this year abandoned precise minimum specifications for password creation and now recommends a length of 8 to 25 characters in combination with two to four character types.[1] The following applies: The shorter, the more complex and vice versa. NIST also refers in its amendment to the fact that research has shown that users would make very predictable changes to their passwords by giving precise specifications such as simply appending a special character.[2]

It makes sense not to introduce a universal minimum standard for every company, as this would make them known to hackers and be used by them as exclusion criteria to crack passwords. However, companies themselves are under the obligation to define precise minimum requirements for internal company passwords to ensure their implementation.

The BSI also distances itself from regular password changes:
„IT systems or applications SHOULD ONLY request a password change with a valid reason. Purely time-controlled changes SHOULD be avoided. Measures MUST be taken to detect the compromise of passwords. If this is not possible, then it SHOULD be checked whether the disadvantages of a time-controlled password change can be accepted and whether passwords are changed at certain intervals“.[6] It is not discussed in detail when such a valid reason exists and which disadvantages are exactly meant by a time-controlled change. This change is celebrated by experts, as employees would no longer be tormented by password changes.[7]

Since companies often do not learn at all or only too late if their access data falls into the wrong hands, the recommendation to change passwords only in the event of loss or data theft is no longer valid. A regular exchange of passwords is still necessary because the risk of compromise increases with the duration of use.

Since the causes for the improper handling of passwords result from too high requirements, the paradigm shift of the BSI is rather to be classified as out of necessity. Even if the purpose of relieving users was well-intentioned, not changing passwords does not solve the security problem. The security risk is more likely to be aggravated if clear instructions are not communicated to employees.

Risk Assessment without Password Policies

How good do you know your employees?

If you can‘t immediately answer these questions wit a clear „yes“, password policies can actually worsen IT security in your organization:

Are you sure that your employees don‘t use insecure workarounds such as saving passwords in the browser or sharing them via chat and e-mail?

Can you prevent your employees from (re)setting insecure passwords on their own?

Do you still have an overview of all login services and passwords in the company?

Do you know when which employee had access to which password?

Do you know if your employees really stick to your password specifications?

From the analysis it follows that it is not password policies that are responsible for employees resorting to insecure workarounds, but the lack of tools and processes. Properly applied, password policies in combination with a password management solution provide essential protection for companies.

Not having to change passwords on a regular basis does not get to the heart of the problem, nor does it provide greater security. Rather, it can lead to even worse passwords being used over a longer period of time, giving attackers more time to guess them.

> **Even with highly complex passwords, a constant exchange is essential to keep attackers out and close security gaps.**
>
> Sascha Martens, CTO MATESO

However, if employees are forced to change their passwords regularly without providing them with the necessary know-how and systems, the risk that this will be done at the expense of password quality as well as that of compromise will increase. Setting passwords in companies according to self-defined rules and replacing them after a certain period of time therefore still makes sense, since even with strong password protection there is always a residual risk.

Password Manager as essential Component in the entire Company

Experience as well as the paradigm shift in password policies has shown that all these rules often fail in their practicability. In the best case, companies therefore use password generators to decouple people from this security-critical process and ensure that the guidelines are adhered to.

Passwords are like toothbrushes: For a noticeable effect you should use them daily, change them regularly, do not share them with anyone and not leave them lying around openly accessible.

This way, highly complex passwords are created in seconds and, ideally, automatically stored in the corresponding Password Manager and managed for login. This means that the employee does not even know the password, but can still log in securely via single sign-on. The role-based assignment of rights allows employees to use passwords only for login, edit them or share them securely with colleagues.

In addition, certain triggers can be defined according to which new secure passwords are automatically set - for example, after temporary approvals for external service providers, which leads to an extreme reduction in password administration.

Security policies regarding minimum length and complexity can also be predefined for automatic password generation using a password manager. The assignment of individual security levels and the restriction of authorizations also ensures that particularly sensitive accounts and accesses are protected according to their requirements.

Password Managers can also help to increase the security awareness of employees: Notifications in the software alert them if their assigned password is not strong enough to automatically prompt them to set a new, better password, for example. This means that users are not left alone when creating passwords and do not even get the idea of resorting to even less secure means out of necessity.

Implementation of Protection Measures:

We recommend combining the introduction of password policies with the following protection measures:

- **Analyze, if available, the previous implementation of password policies in your company.**
- **Evaluate the security level of existing password creation and management mechanisms.**
- **Conduct regular security awareness trainings.**
- **Define at least one specific contact person for security issues.**
- **Ensure that every employee understands the necessity and correct implementation of password policies.**
- **Verify compliance by implementing password management tools and processes.**

Conclusion

What is clear is that even the strongest password policies are useless if employees are left alone to create and manage passwords. However, the fact that government agencies and security experts have now defused the guidelines is a false signal that does not tackle the cause - the overburdening of individual users - and can even play into the hands of hackers. Instead, the need for a password manager should be emphasized even more, in order to relieve the burden on users and keep up with the fight against cyber threats.

The perfect Password should ...

be stored in a digital safe.

be long, complex and difficult to remember.

be entered automatically.

best not be known by anybody!

So you'd better give your employees valuable tips and provide them with a password manager for implementation. In addition, a concrete security expert is essential in order to always involve the employees in the password management process, to educate them and thus prevent the emergence of insecure solutions such as „Password1" and Excel lists.

Sources:

[1] Bundesamt für Sicherheit in der Informationstechnik 2020; Empfehlungen: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

[2] National Institute of Standards and Technology 2020; Digital Identity Guidelines: https://www.nist.gov/itl/tig/projects/special-publication-800-63

[3] Bundesamt für Sicherheit in der Informationstechnik; Pressebereicht 2011: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit_27012011.html

[4] Der große Passwort-Stress, YouGov: https://de.statista.com/infografik/7705/der-grosse-passwort-stress/

[5] Deutschland; Ipsos; 1.000 Befragte; ab 18 Jahre; Internetnutzer, die in den letzten drei Monaten etwas online gekauft haben; Online-Umfrage: https://de.statista.com/statistik/daten/studie/3609/umfrage/uebersicht-ueber-eigene-online-passwoerter/

[6] Bundesamt für Sicherheit in der Informationstechnik 2020: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identitäts-_und_Berechtigungsmanagement.html

[7] Süddeutsche Zeitung 2020; Die Qual des ständigen Passwort-Wechsels endet: https://www.sueddeutsche.de/digital/passwort-wechseln-bsi-1.4784293

MATESO

MATESO is a leading German IT company, which has successfully established in the DACH region since the company was founded in 2006. The developed password security solution Password Safe is distributed internationally by its worldwide partner network. Well-known references testify to the technological and know-how advantage of the IT software.

Today the constantly growing enterprise registers over 10,000 corporate customers with several million users worldwide - including 20 Dax 30 companies.

PASSWORD SAFE

Pioneer in Enterprise Password Management

Password Safe serves companies as a central digital safe for securing, managing and monitoring sensitive data such as passwords, documents and secrets.

> **In dealing with passwords, humans are still indispensable.**
>
> **Companies are therefore obliged to make this process as secure as possible.**

Sascha Martens
Author und CTO of MATESO

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß, GERMANY
Web: www.passwordsafe.com
Email: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE