

Password managers

Micro exercise

Exercise introduction

This micro exercise is focused on password manager software. It is a short and sharp session that explores this topic using a combination of interactive activities covering what password managers are and what you should consider when deciding whether to use them. You will have the opportunity to evaluate yourselves as a group against various competencies and at the end of the exercise you will be provided with a report summarising your evaluation.

Participants and timing

Allow around 15 to 30 minutes, you may choose to tailor this to the time you and your participants have available.

Required attendees

You can have as many or as few people involved as you like, and no one taking part in this exercise needs to be a cyber security expert. We recommend 3–5 people including a nominated facilitator to run the session and keep the conversation on track.

What is expected of the participants?

You're here to think, talk and learn about this topic. You don't need to be a cyber security expert; it is not a test. Instead, we aim to enable collaborative discussions that further your knowledge and help you identify areas of improvement.

Your nominated facilitator is here to run the session and keep the conversation on track, in whatever way the group is comfortable with.

Context

Remembering lots of long or complex passwords is difficult, often leading people to choose short and simple passwords or to use the same password for multiple systems and accounts. An easy to guess password, or one used for multiple systems, is one of the most common ways hackers can compromise your online accounts.

Password managers are used to securely store and remember the passwords you use for online accounts. They are available as an application, or as a service in your web browser, known as a browser extension. They offer advantages for both users and organisations by helping people use unique, complex passwords for multiple systems and accounts.

Questions

Question 1 of 3

What are some of the benefits and features of password managers?

Answer

- All your passwords will be stored securely and only accessed by you, using a master password.
- You can use them to generate strong complex passwords for you to use.
- You do not have to remember all your passwords.
- You can synchronise your passwords to use across different devices. For example, some password managers can be used across your phone, tablet, laptop, and desktop.
- You can use them to alert you to any passwords that have been seen in breaches.
- You can use them to spot fake websites that try to steal your information.

Question 2 of 3

What are some of the drawbacks of using password managers?

Answer

- If you forget the master password to the password manager then you will no longer be able to get access to your stored passwords.
- As all your passwords will be stored in the same place, if an attacker gets access to your password manager then they will have all your passwords.
- You must remember to keep the password manager installed, and up to date, across all the devices you use.

Question 3 of 3

What are some steps you can take to keep your password manager secure?

Answer

- Install updates when they become available.
- Set a strong master password. If you need to write it down, keep it very safe, then destroy it once your master password is memorised.
- Follow NCSC guidance on using password managers, which includes setting a strong master password. This is available in Related Guidance later in the exercise.
- Do not share your master password with anyone else.
- If you share a computer with others and you save passwords in your browser-based password manager, ensure that everyone has their own account and that you logoff when you are finished.
- Ensure that the master password is a unique password – do not use that password anywhere else.
- Turn on Multi-factor Authentication (MFA) if it is available.

Case study

Brute force attacks

In June 2021, Microsoft revealed that it had identified new activity from an Advanced Persistent Threat (APT) known as NOBELIUM targeting organisations globally with the aim of gaining access to users' accounts. An APT is a cyber attack where a hacker accesses a system and remains undetected for a long time.

NOBELIUM was a sophisticated, large-scale attack attempting to gain access to any number of users' accounts in multiple organisations, by means of as a brute force attack.

Brute force attacks use computing power to automatically enter a huge number of passwords guesses in an attempt to gain unauthorised access. There are some specific variations of brute force attacks which are good to understand how they target users' passwords:

- Dictionary attack - A type of brute force attack where words in a dictionary, phrases or common passwords as used for guesses
- Password spraying - Using a small number of commonly used passwords in an attempt to access a large number of accounts

This type of threat illustrates the need for strong passwords, alongside other measures such as Multi-factor Authentication (MFA) and good Identity and Access Management (IAM), to help defend your organisation from cyber attack.

Source: [NCSC news article "Microsoft update on brute force and password spraying activity"](#)

Scenario

Consider the scenario outlined and run through the remaining points when you are ready:

The scenario

Employees have been giving feedback that they are frustrated with having multiple systems with complex password requirements. Recalling the correct password(s) throughout the day is having an impact on efficiency, password strength being used, and leading to an increase in requests to your IT team/supplier to reset passwords. Some employees have mentioned they have heard of similar organisations rolling out a password manager solution for their employees, which has been well received.

Things to consider

What would you do in this scenario?

- How would you engage your IT security teams to consider using a password manager?
- How would you get buy-in from senior leaders in your organisation?
- How would you disseminate information on password managers to employees?
- What training or guidance would your employees need?
- How would you build a password manager into your daily business activities?

Your response

Answering **Yes** or **No**, would your organisation consider implementing a password manager?

Discuss this as a group and consider what your answer would be.

The potential impacts of answering **Yes** or **No** will be revealed on the next pages.

Responding “Yes”

When deciding to use a password manager, you should be sure to:

- Turn on Multi-factor Authentication (MFA) on the password manager account. This means that even if a cyber criminal knows the master password, they still won't be able to access your password manager account.
- Set a strong master password to control access to your password manager account (for example by using three random words). You cannot store this password in the password manager itself, so if you cannot remember it, write it down on paper and keep it very safe, then destroy it once your master password is memorised.
- Install all updates for your password manager as soon as you're prompted.
- Follow NCSC guidance on where and how the password manager should be used. For example, you should never save your password in a browser on a shared device.

Responding “No”

In the absence of a password manager, does your organisation have:

- Clear policies on passwords, including complexity criteria & usage of passwords?
- Audit or compliance procedures to make sure password policies are followed?
- Single Sign-On, to make it easier for users to access multiple systems and applications in your organisation?
- Additional or other authentication methods to help keep your organisation secure? Such as Multi-factor Authentication (MFA)?
- Efficient procedures for employees to reset their password(s)?

Advice

- Consider the benefits and drawbacks of password managers specific to your organisation.
- Keep up to date with the NCSC's latest news and guidance on password managers.
- If you are considering using a password manager solution, refer to the NCSC buyers guide [here](#).
- Check the password manager is accessible for everyone that will use it, including those who require assistive technology.

Evaluation

Discuss the following statements and rate them on a scale of:

1. Not at all confident
2. Slightly confident
3. Somewhat confident
4. Fairly confident
5. Completely confident

- We understand the benefits of using a password manager.
- We understand the drawbacks of using a password manager.
- Users know how to keep the password manager application secure.
- We understand some of the additional functionality that can be in password managers.

Conclusion

Password managers are a useful tool for generating and storing strong passwords, ensuring that your online accounts are not vulnerable to common attacks. However, passwords are not perfect and there are still opportunities for attackers to compromise even the strongest passwords. Just like other software, password managers must be built and managed securely.

In the future it is hoped that alternative, more secure, methods of authentication will be available, however for now password managers offer lots of advantages for both users and organisations. More top tips on the use of password managers can be found on the NCSC website.

Next steps

Make recommendations that will develop confidence in the areas that have been identified as having scope for improvement. Areas for improvement could be where you have given a lower confidence rating in any of the exercise observations. Discuss with and allocate the recommendations to the people in your organisation who can facilitate change and action improvement. Discuss the risks associated with not addressing the recommendations.

Ensure any recommendations are implemented and when ready, run the exercise again to see how those changes have impacted upon your organisation.

Also refer to the Related Guidance, below, which may help you in those areas you have identified as needing improvement.

To run further exercises please go back to [Exercise in a box](#).

Related guidance from the NCSC

[Small Business Guide](#) - How to improve cyber security within your organisation - quickly, easily and at low cost.

[Small Business Guide: Response and Recovery](#) - Guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident.

[Mitigating Malware](#) - This guidance describes how organisations of all sizes - and home users - can reduce the likelihood of being infected by malware.

[Top tips for staying secure online](#) - Guidance on how to use Password managers, including using browsers and apps to safely store your passwords.

[What does the NCSC think of Password Managers](#) - Read more insight from the NCSC on their view of using password managers.

[Three random words](#) - Guidance that helps understand the benefits of using three random words for passwords, including how to best use this technique.