National Cyber Security Centre

Connecting securely

Micro exercise

Exercise introduction

This micro exercise is focussed on connecting securely to a network when working remotely. It is a short and sharp session that explores this topic using a combination of interactive activities to cover establishing a secure network connection and connecting to a public Wi-Fi network. 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

Organisations have been increasing their ability to enable home and remote working for their employees. This often means the adoption of new working practices, systems, and software, to enable employees to connect and carry out their work.

However, this increase in remote working has provided more opportunities for attackers to compromise users' personal and company data. For example, connecting to public Wi-Fi or insecure networks with mobile devices can allow attackers on the same network to intercept or modify your data.

This micro exercise explores some of the ways users can ensure they are connecting to their home and work environment securely, protecting both their data and their organisation's data.

Questions

Question 1 of 3

What is encryption?

Answer

Encryption uses an algorithm to scramble data, ensuring that it is unreadable to unauthorised parties. Encryption is often implemented without you even knowing it or having to do anything, for example when you are logging on to online banking.

Question 2 of 3

Is your home Wi-Fi encrypted by default?

Answer

Most modern Wi-Fi routers provided by Internet Service Providers (ISPs) will provide encryption of your Wi-Fi network traffic by default. However, you should also ensure that you change the default password on the router to a strong but memorable password, such as Three Random Words in line with NCSC guidance. This helps guard against others gaining access to your Wi-Fi network and intercepting your data.

Question 3 of 3

Some websites display a padlock in the address bar on the browser, what does this mean?

Answer

This indicates that the website is using encryption to protect your data. This ensures that data between yourself and the website, such as passwords, banking details etc., is not viewable by others who may be intercepting your traffic.

Case study

Man in the middle

Remote working has provided us with greater flexibility in where and when we work, however this way of working also increases our personal and organisation's attack surface. If you connect to your organisation or web services and the connection is not encrypted, attackers could eavesdrop on the connection to compromise your personal or company data. This is known as a Man in the Middle (MitM) attack. With access to an unencrypted network the attacker can carry out several actions such as:

- Intercept traffic – The attacker can monitor the websites you visit, messages you send, usernames, passwords, credit card numbers etc.
- Replay and manipulate traffic – Attackers can redirect you to malicious sites.
- Session hijacking – Session hijacking allows an attacker to hijack a connection you may have with a website and pretend to be you.

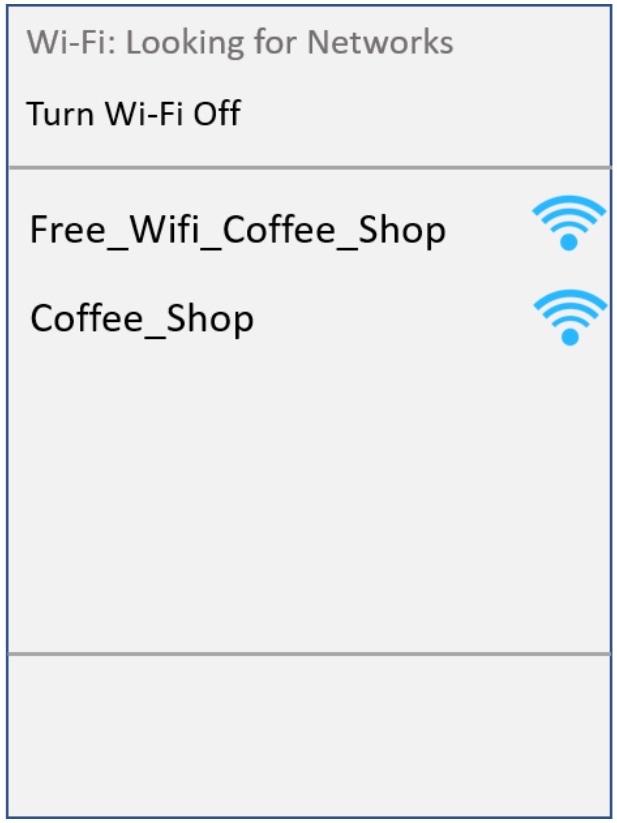
This type of attack has been used by cyber criminals to target commercial companies and their customers for the purpose of carrying out financial fraud.

Scenario

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

The scenario

You have decided to work from the local coffee shop and want to connect your laptop to the Wi-Fi to work or log into social media. When you look at available access points to find the coffee shop Wi-Fi, you see two that are named similarly.



Things to consider

What would you do in this scenario?

- Does your organisation permit you to connect to public Wi-Fi for work purposes?
- Have you ever experienced confusing or similar public Wi-Fi access point names before?
- Which one do you connect to?
- Does it matter if you attempt to connect to the wrong one?

Your response

Answering **Yes** or **No**, would you attempt to determine which is the correct access point before connecting?

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”

- It is important to determine you are connecting to the legitimate and correct access point where you are unsure.
- Use of a VPN will help protect your data.
- If you inadvertently connect to the wrong and potentially malicious Wi-Fi access point, report this to your organisation.

Responding “No”

- This potentially could be an evil twin attack. The only way to know for sure is to ask the shop owner or a member of staff to identify the correct one.
- If you think you have connected to a potentially malicious Wi-Fi access point, report this to your organisation's IT team so that they can provide help and guidance.
- **Evil Twin:** An evil twin is an attacker owned access point that pretends to be the legitimate one by using the same or similar name. For example, an attacker would set up their access point in a coffee shop to attempt to get customers to connect to their Wi-Fi instead of the coffee shop Wi-Fi, potentially allowing the attacker to intercept and manipulate the traffic. Use of a VPN can prevent this type of attack.

Advice

- You should ensure that VPN software and hardware (if applicable) are kept updated.
- Only use public Wi-Fi networks for browsing, if you need to log on to web services or log on to work systems, ensure you use a VPN.
- Ensure your home Wi-Fi router is using WPA2 or greater and has a strong password.
- If you write Wi-Fi passwords down, ensure they are stored securely.

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 are confident that users have access to guidance regarding how to connect securely to our organisation's resources.
- Our organisation makes it easy to get the IT support we need if we are having issues connecting.
- Our organisation ensures that our infrastructure that enables home and remote working is kept up to date and patched.
- Users would feel confident reporting without repercussion if they believed they were victim of an 'Evil Twin' attack.

Conclusion

With the increase in home / remote working, attackers have been making concerted efforts to target those users. Secure connectivity is fundamental to enabling effective home and remote working.

When the technology has been implemented and users are provided with the correct guidance and process, connections to the work environment can be as secure as physically being in the office.

More top tips on secure connectivity and home working 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.
Virtual Private Networks (VPN) Guidance - Guidance for organisations on how to choose, configure and use devices securely.
Home working: preparing your organisation and staff - How to make sure your organisation is prepared for home working.
Setting 2-Step Verification (2SV) - How setting up 2SV can help protect your online accounts, even if your password is stolen.
Three random words - Guidance that helps understand the benefits of using three random words for passwords, including how to best use this technique.