



**safe on social**  
education and consulting

[www.safeonsocial.com](http://www.safeonsocial.com)



# Risks of Connecting Work Devices to Public Wi-Fi

## **Insecure Networks**

Public Wi-Fi networks, including those in hotels, are generally insecure. They often lack robust security measures found in private or home networks, making it easier for cybercriminals to intercept data.

## **Free Wi-Fi Often Comes at a Cost**

While hotel Wi-Fi is often advertised as “free”, it can come at the cost of your personal and professional data. Some networks may track user activity and collect data for marketing purposes, potentially breaching privacy policies.

## **Potential for Data Theft**

Sensitive information such as work emails, business documents, or financial details can be intercepted by cybercriminals on public Wi-Fi. This could result in data breaches or financial loss for the company.

## **Malware Distribution**

Public Wi-Fi networks are common points for hackers to distribute malware. If your device is infected, it can lead to the loss or theft of data, and the malware can potentially spread to other devices in your work network when you reconnect.

## **Man-in-the-Middle Attacks**

These types of attacks allow cybercriminals to intercept the data sent from your device to the network. They can steal sensitive information or inject malicious content into your data streams.

## **Snooping and Sniffing**

Public Wi-Fi makes it easy for cybercriminals to use snooping and sniffing tools. These tools monitor network traffic and capture unencrypted data, revealing sensitive information to the snoop

[www.safeonsocial.com](http://www.safeonsocial.com)

No part of this e-book/cheat sheet or its associated modules may be reproduced or transmitted by any person or entity in any for by any means, electronic or otherwise including photocopying, recording or scanning or by any information storage without prior permission from Safe on Social Media Pty Ltd other than the licensor who is licensed to use this information in newsletters and in print and has been granted permission from the publisher under an annual license. The publisher, authors, licensee, licensor and their respective employees or agents will not accept responsibility for injuries or damage, physical or emotional occasioned to any person as a result of a social media use or any other activities described in this e-book/cheat sheet. very attempt has been made to ensure that the information in this e-book/cheat sheet is accurate, it is the nature of social media to be constantly changing. Therefore, Safe on Social Media Pty Ltd gives no guarantees and accepts no responsibility to the completeness or accuracy of the contents of this guide.

## Exposure to Unregulated Content

Connecting to public Wi-Fi networks can inadvertently expose your device to inappropriate or illegal content, which could lead to serious legal implications for both the individual and the organisation.

## Unauthorised Access

If your device is compromised while connected to a public Wi-Fi network, it may allow an attacker to gain unauthorized access to your device even after you've disconnected from the network, leading to ongoing data security issues.

## Recommendations for Safe Use of Work Devices:

**Use Virtual Private Networks (VPNs)** - These can encrypt your data, preventing it from being intercepted during transmission.

**Limit Activity** - Refrain from accessing sensitive information while connected to a public network.

**Use Secure Wi-Fi Connections** - Whenever possible, connect to secure, password-protected networks, pay for the service.

**Use Mobile Data** - If you must work on sensitive documents, it may be safer to use your mobile data instead like your personal hotspot

**Regular Updates** - Keep your device's software up-to-date, as updates often include security patches.

**Use Multi-Factor Authentication (MFA)** - This provides an additional layer of security, making it more difficult for unauthorized users to gain access to your data.

When in doubt, refrain from using public Wi-Fi for work purposes. The risks often far outweigh the convenience.