PUBLIC
WI-FI
IMPACT ON
NATIONAL
SECURITY

Public Wi-Fi: Impact on national security

Why this matters

Free Wi-Fi at hotels, cafes and airports can feel like a gift. It is free to use but public Wi-Fi can be a hacker's dream.

While you drink your coffee and scroll through your social media and click on links that interest you, someone could be spying on you and your data.

This information booklet explains the risks and how to protect yourself, your data and our national security.

Why worry about free Wi-Fi

Public Wi-Fi networks are usually open and not secure, which means:

- Anyone can connect to the network, good people and bad people
- Data sent over the network may not be encrypted
- A hacker or cybercriminal can easily intercept your personal information

Using public Wi-Fi is like having a private conversation in a crowded room where strangers can secretly see and hear everything.

What could happen

Identity theft

Hackers can steal your usernames and passwords and possibly your banking information. Once they have this information, they can pretend to be you online and watch what you are doing.

Account hacking

Your social media accounts, like Facebook, your email account or online shopping account could be taken over. A bad person could spend your money.

Malware

Cybercriminals can sneak viruses or spyware onto your device while you are browsing the web.

Fake Wi-Fi hotspots

Any free Wi-Fi network could be real or a trap set by hackers and cybercriminals to lure you into using their Wi-Fi.

How hackers do it

Here are two examples.

Man-in-the-middle attack: Hackers can intercept your connection when you go online using the free airport WiFi to check your bank balance before a flight.

FREE WI-FI

Connect to Wi-Fi

FAKE WI-FI HOTSPOTS

Cybercriminals can set up fake Wi-Fi hotspots with names similar to legitimate public networks.

You could be tricked into connecting to these networks.

You log onto your banking website by sending your username and password to the website, but a cybercriminal sees your username and password before it goes to the bank.

They send your username and password to the bank so that you think everything is normal.

When the bank replies the cybercriminal sees it first and sends the reply to you. You are not aware of what has happened.

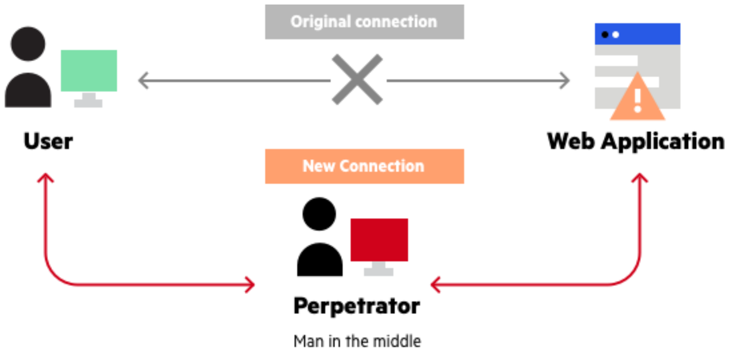


Figure 1: Man in the Middle example from imperva.com

Sniffing tools: After you finish your banking, you visit your favourite online shop, but the website login page does not have the lock icon or https://.

Nearby is a hacker on the same free public airport Wi-Fi network as you. They run a packet sniffer, a program that listens to Wi-Fi traffic.

When you log into an unencrypted page, the sniffer program reads your email and password in plain text.

The hacker now has your shopping account login details.

How to protect yourself

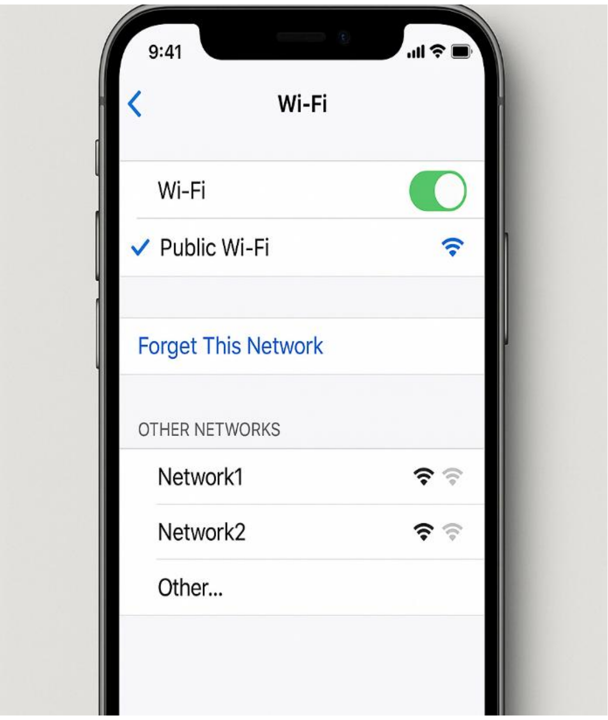
You do not have to give up using public Wi-Fi, just follow these simple tips to keep yourself safe:

- Use a VPN - A Virtual Private Network as it encrypts your data so others cannot see it.

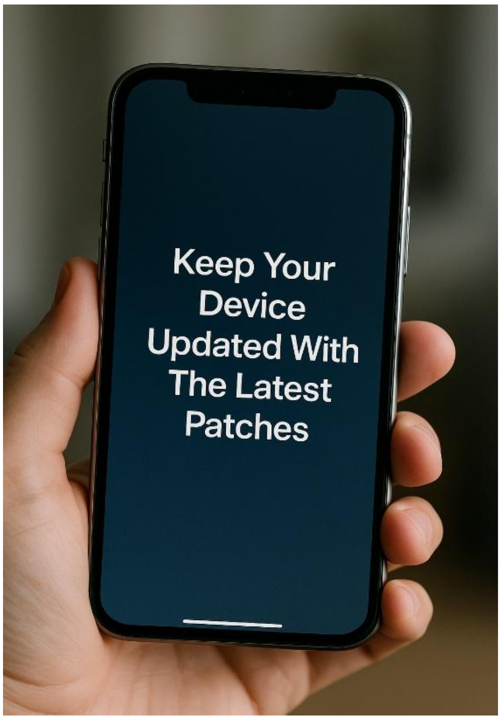
NordVPN® Bitdefender® Surfshark®

- Turn off sharing on your device.

- Visit websites that have https:// or a lock symbol.
- Do not access sensitive accounts (banking, work) while on public Wi-Fi.



Select forget the network in your settings after using the public Wi-Fi.



Keep your devices updated with the latest updates and security patches.

Why it matters for Vanuatu

If the compromised user is a government employee, contractor or service provider, attackers may gain access to sensitive government systems and documents, or operational communications.

Which can escalate beyond personal data theft to sabotage, espionage or disruption of national functions.

Trust and business continuity

Public servants and contractors often use mobile devices and laptops when travelling or working remotely.

Using public Wi-Fi can expose login credentials and sensitive information belonging to the public.

A breach can erode public trust in government operations and services.

Disruption to digital government services can harm citizens.

From one user to many

Cyber attackers can use an infected device as a gateway, risking the entire government network when it reconnects.

Once a malicious actor is on the network this could lead to cyber espionage, foreign interference, data manipulation or sabotage.

Every unprotected connection represents a potential entry point into Vanuatu's national digital framework.

Your connection, our security

By making safer choices online, you are not just protecting yourself, you are protecting the integrity of the services, institutions, and communities we all rely on.