



# Cybersecurity

LUSAIL MUSEUM INTERN: TOOBA AZIZ



# Cybersecurity and its importance

It is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.



- Protection from cyberattacks like malware, phishing, and ransomware.
- Preservation of personal data and privacy.
- Smooth business operations and prevention of financial losses.
- National security and defense against cyber threats from other nations.
- Trust and confidence in the digital realm.



# Is public Wi-Fi safe?

- In short, No!
- Using free Wi-Fi hotspots is incredibly convenient, enabling easy access to online accounts, work tasks, and email checking while on the move.
- However, these networks are not flawless and may expose you to potential cyberattacks.
- There are a tremendous number of risks that go along with these networks.



## Public Wi-Fi

### Signs

### Prevention

SSID:	NMOQ-Corporate
Protocol:	Wi-Fi 5 (802.11ac)
Security type:	WPA2-Enterprise
Manufacturer:	Intel Corporation
Description:	Intel(R) Wireless-AC 9560 160MHz
Driver version:	22.60.0.6

SSID:	NMOQ-Guest
Protocol:	Wi-Fi 5 (802.11ac)
Security type:	Open
Manufacturer:	Intel Corporation
Description:	Intel(R) Wireless-AC 9560 160MHz
Driver version:	22.60.0.6



# Signs of a rogue Wi-Fi network



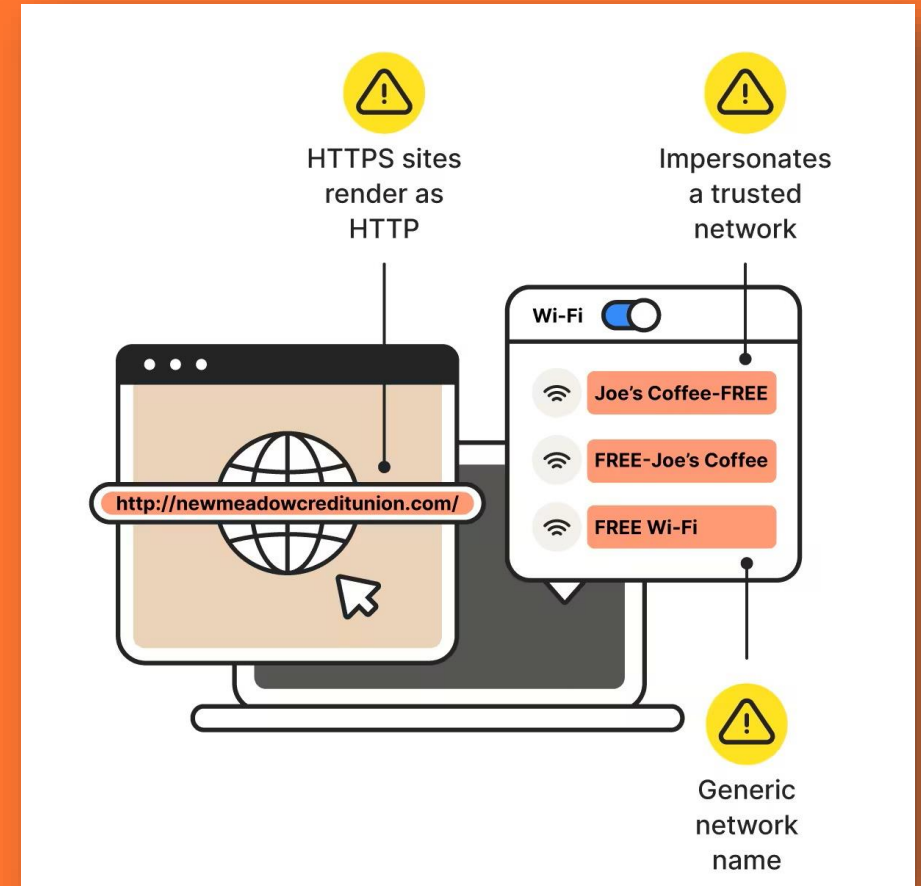
Public Wi-Fi

Signs

Prevention

- While many hackers prefer public Wi-Fi networks, some may take an additional step by setting up a hotspot with malicious intentions.

- Here how you can spot it ->



## Some tips to stay safe on public Wi-Fi:



Public Wi-Fi

Signs

Prevention

1. **Stick to HTTPS websites.**
2. **Avoiding accessing sensitive information.**
3. **Turn off file sharing.**
4. **Use antivirus software.**
5. **Keep your operating system updated.**
6. **Enable Two-Factor Authentication (2FA).**
7. **Disable Auto-Connect to Wi-Fi network.**
8. **Remember to logout.**



# Here is a short research article on cybersecurity in Qatar:



Cybersecurity in Qatar.pdf



## Cybersecurity in Qatar

Tooba Aziz, Asra Marazghi and Hissa Al-Muhammadi  
Department of Computer and Science Engineering  
Qatar University  
Doha, Qatar

**Abstract**—The Internet is one of the most well-known and important invention of the 21 century that affected our lives and changed the way we used to do things. However, it comes with some drawbacks that needs to be considered and addressed because nowadays cybercrimes, cyberattacks and cyberbullying and many harmful acts has increased the risk of using the IT devices and resources, that is why Qatar is trying to improve the cybersecurity field. By creating a ministry of information and communication technology that focuses on protecting the private information and guarantee the safety of the internet. Moreover, this short research article will discuss and review several studies of cybersecurity in Qatar. And evaluate the issues related to cybersecurity in Qatar as well as the preventions and solutions. As cybersecurity is one of the most important IT field these days.

### I. INTRODUCTION (CYBERSECURITY)

Cybersecurity is a method of protecting electronic networks and the data to prevent any unauthorized person from accessing them to ensure that no data or information falls into the hands of an unknown person whose intention is unknown. Moreover, recently a dramatic increase in the number of cyber-attacks in all parts of the world has been witnessed, especially after the Covid-19 pandemic since almost all the internet users went online to continue working. With these attacks, the rate of economic losses has increased dramatically. Therefore, cybersecurity has been a top concern in the United States, Russia, and Europe, but it gained popularity in the Middle East and Africa only a few years ago as the peoples of the region began to observe the importance of such a topic. In previous years, the Middle East region tried to catch up with digitization, expansion, and development in information and communication technologies, especially after increasing the use of the Internet in the region. It has become necessary to obtain cybersecurity precaution measures to protect critical network infrastructure. With the increase of internet users, the rate of crimes and electronic attacks increases, as these actions can lead to economic losses and the dissemination of secret intelligence information, which is an integral part of the national security of any nation. Every user agree that cybersecurity is the main important thing in the internet development. However, it has some drawbacks and issues that while considering them it will be easy to solve.

### II. CYBERSECURITY IN QATAR

#### A. Cybersecurity development in Qatar

On June 5, 2017, the Kingdom of Saudi Arabia, Kingdom of Bahrain, the UAE, and Egypt announced the blockade on Qatar and the complete closure of all borders linking the blockading countries to Qatar, whether land, air, and sea. This

is in addition to prohibiting dealing in Qatari rivals or even dealing with any bank related to Qatar. The UAE hacked the Qatar News Agency (QNA) website in minutes due to the weak protection of the website. After the penetration, many fake and incorrect news attributed to the Emir of Qatar was published, and a blockade was imposed based on this false news. Cyber-attacks targeted social media platforms and state-owned media platforms to spread false news to intimidate the Qatar people and damage their economy. In addition, this attack caused a successive disturbance in trade and transportation in the State of Qatar and associated financial institutions of the government, society, and economy. Such a heinous incident gave us a vivid example of the importance of owning and developing cybersecurity and protecting networks in the country to prevent a recurrence of such an incident. The State of Qatar has strived to develop its cybersecurity in several ways.

The first step is Qatar's National Information Assurance Framework 103 (NIAF), which is the officially recognized national framework responsible for implementing globally authorized cybersecurity standards. The NIAF provides a guide for all policies, standards, and guidelines. Also, the NIAF provides legislation for cybercrime. In addition, Qatar has implemented a national cybersecurity strategy with the development of an action plan. One of the most prominent points of this strategy is the establishment of a team called the Emergency Response Team (Q-CERT), which is a governmental organization that evaluates efforts to improve cybersecurity in the State of Qatar. As Rafael Dean Brown (2018) also mentioned that Qatar is striving to develop its cyber security by adopting many strategies and plans and striving to work according to globally recognized standards (p.15).

### III. LITERATURE REVIEW

This literature produces and discusses many aspects of cybersecurity especially in Qatar, and listed pros and cons as well as many issues related to cybersecurity. Several studies related to cybersecurity in Qatar have main focus on the QNA cyberattacks such as the research by Rafiqel Brown, 2018). As cybersecurity field is increasing rapidly many countries are trying to develop and improve their capability in it as the research on (2021) by Hanan Mohammed, the research evaluated the capability of each country in GCC as well as some other countries in the usage of IT and cybersecurity improvement. The study by Von Fischenstein discussed the issues of cybersecurity in the middle east and north Africa including Qatar (2019). Furthermore, the publication by Fatma

# Thank you!

