الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Cyber Security Guidelines

Public Wi-Fi Networks

Public

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled “Cyber Security Guidelines for Public Wi-Fi Networks” - V 2.0 - to help Public Wi-Fi service providers and users to understand and mitigate associated risk.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the “Cyber Security Guidelines for Public Wi-Fi Networks”.

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

Document Control

Document Details	
Document ID	IAG-NGE-GPWN
Version	V 2.0
Classification & Type	Public
Abstract	This document is intended as a guidance to help organizations understand and mitigate the threats to a Public Wi-Fi system.

Review / Approval

Department/Role	Reviewed/Approved	Version	Date
National Cyber Governance and Assurance Affairs		2.0	

Revision History

Version	Author(s)	Revision description	Date
1.0	CSPS	Published	April 2018
2.0	CSPS	Published	January 2023
2.0	CSPS	Published + Minor Corrections	December 2023

LEGAL MANDATE(S)

Emiri decree No. (1) of the year 2021 regarding the establishment of National Cyber Security Agency, sets the mandate for the National Cyber Security Agency (hereinafter referred to as "NCSA"). The NCSA has the authority to supervise, regulate and protect the security of the National Critical Infrastructure via proposing and issuing policies and standards and ensuring compliance.

This document has been prepared taking into consideration current applicable laws of the State of Qatar. In the event a conflict arises between this document (specific provision or clauses) and the laws of Qatar, the latter (law), shall take precedence. Any such term (specific provision or clauses), to that extent shall be deemed omitted from this Document, without affecting the remaining provisions of this document. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Table of Contents

1 Introduction

1.1 Context

Public Wi-Fi Networks in Qatar are widely and readily available in airports, parks, restaurants, coffee shops, libraries, and hotels; these “hotspots” are widespread, and people love to connect to them without thinking twice.

Generally intended as a public service, or a value add for its customers, it does not come without its own share of risks. For starters, we may not always be able to say with a level of assurance who is the wi-fi service provider, or who are the users? Since it is usually a free service, even corporates do not generally put too many controls to secure the service.

And, although it sounds harmless to log on and check your social media account or browse some news articles, everyday activities that require a login — like reading e-mail or checking your bank account could be risky business on public Wi-Fi.

2 Purpose, Scope, and Usage

2.1 Purpose

This document aims to help individuals and organizations to understand the risks associated with using or providing a publicly accessible Wi-Fi network and techniques to mitigate such attacks.

2.2 Scope

Any person or organization that owns, provides, or uses a publicly accessible wireless network in the state of Qatar.

Any organization that maintains a Guest Wi-Fi network and provides internet services to its vendors, temporary staff etc.

2.3 Usage

The guidance provided in this document will help entities to provide secure public wi-fi services to their customers, vendors, and/or public. The document will also help individuals to securely use public wi-fi services.

3 Key Definitions

Organizations / Agencies	Any organization including government / semi-government agencies, commercial organizations etc.
Individual / Individuals	Refers to any person/ group of people connecting to, managing or owning a public Wi-Fi network

4 Guidelines

4.1 Understand the Risks

Features like openness and ease of connection that make free Wi-Fi hotspots desirable for consumers, also make them desirable for hackers. There are a tremendous number of risks, which go along with these public Wi-Fi networks. While business owners may believe they are providing a valuable service to their customers, chances are the security on these networks is very low or nonexistent.

The less security the Wi-Fi hotspot has, the easier it is for an attacker to connect and eavesdrop on users, distribute malware, and steal sensitive information. Techniques such as snooping, sniffing, phishing and MitM (man in the middle attack) are common within such scenarios.

The attacks can lead to consumers being defrauded, for example by stealing credit card data information. They can also lead to leaking consumer private data, photos, and conversations to cybercriminals for them to resell or reuse for malicious actions.

There is a threat of rogue wi-fi hot spots being put up in public places to deceive gullible public into using the services and thereby losing their sensitive information which may be sniffed by the malicious service provider.

Many a times, such services lack access control, i.e., there is no way of knowing who used the services. This may be a huge impediment in case of a cyber incident as there may be no way of pinpointing the action to any person.

4.2 Wi-Fi Owner/ Service Provider

All wireless devices and networks used to operate the Services and to access, store, process, or transmit any Customer information should be implemented in a secure manner and in compliance with the National Information Assurance Standard “NIAS” of the State of Qatar.

These provisions would allow minimizing:

1. Cyber threats from the Internet to the Customers.
2. Cyber threats that might be initiated intentionally or unintentionally by the Customers to other parties over the Internet.
3. Cyber threats that might be initiated intentionally or unintentionally by the Customers to other Customers on the public Wi-Fi network.

4.2.1 Governance

1. Define a service owner for this service. The service owner should be responsible for operating and securing the service to an acceptable level.
2. Conduct a risk assessment and identify the associated risks in operating this service. Implement a plan to mitigate and manage the identified risks to an acceptable level.
3. The Service owner should define the operational, acceptable usage and security procedures for the service.
4. Technical documents regarding the service such as network and functional design documents, network layouts, IP address details etc.; should be documented, secured, and provided access on a need-to-know basis only.

5. Maintain and document an inventory of all devices required to deliver this service.
6. Maintain and manage activity reports, statistics, and usage reports of wireless users.
7. Information security agreement: develop information security user agreement.
8. Information security privacy: define privacy policy for wi-fi users.

4.2.2 Access Control

1. Any wireless services including free or complimentary, should identify, authenticate, and authorize the users before providing any internet access.
2. The service should be able to identify and authenticate the users in an acceptable manner.
   Example: 2 Factor Authentication using a Mobile Device.
3. Display an acceptable usage policy (AUP) to the user upon landing on the captive portal. The user should read and accept the terms of usage prior accessing any website.

4.2.3 Data Collection and Sharing

1. The AUP should also include the legal disclaimers, terms of privacy policy, and consent for use of any personal identifiable information (PII) that may be requested or collected from the user during the process of logging into the system or use of internet services. (Refer to AUP appendix)
2. Any data collected from users should only be used and shared in compliance with the existing legal instruments such as the Personal Data Privacy Protection Law (PDPPL).
3. Personal data should not be shared with any third party except when required and allowed by the PDPPL Article 18.

4.2.4 Security Hardening:

4. When designing your network, segregate your business / corporate network from the public Wi-Fi network. It is better to segregate physically, however logically separated with strong controls could also work if it provides the necessary risk mitigation.
5. Adequate network security measures such as zoning, proper configuration of unified threat management solutions (e.g., firewalls and others), should be put in place in accordance with universal best practices (such as NIAS, NIST 800-41, NIST 800-53, ISO 27001, and others).
6. Use different SSIDs while defining names for the wireless network. Avoid using similar names such as “ABC_Corp” and “ABC_Public” or “ABC_Guest”
7. Use strong wireless security protocols such as WPA2 and EAP-TLS. Do not use WEP and WAP protocols.
8. Remove/Disable default passwords on network switches, routers, wireless access points, and any other hardware. Configure strong passwords in line with the best practices. e.g., A minimum length of 12 characters with no complexity requirements or password length of eighth characters containing at least one of each of a lowercase character (a-z), an uppercase character (A-Z), a digit (0-9), a punctuation/special character.
9. Configure the access points and routers as per universal / vendor best practices. Enable encryption (if available), usually it is disabled by default.
10. Change passwords on a periodic basis.
11. Maintain access logs for users. The access logs should capture attributes such as username (if applicable), associated mobile number (used for authentication), and assigned IP address and date and time etc., which may identify the user.
12. Enable security logging on all devices. Refer to “Guidelines for Incident Management – Prerequisite Measures” for support and guidance.
13. Maintain security logs for a minimum of 120 days.

14. Take adequate measures to ensure the detection, response, and prevention of rogue access points and sniffing technology on the public Wi-Fi network. It is strongly recommended to use Wireless IDS / IPS where public Wi-Fi is available or co-exists with corporate network.
15. Use dynamic exchange mechanisms and secure VPN to transmit PII or payment information to provide sufficient end-to-end encryption and access control.
16. Regularly patch and update your wireless infrastructure.

4.2.5 Physical Security:

1. Adequate measures should be taken to physically secure access points from unauthorized physical access or general physical damage
2. Make sure that wireless router or APs are secured from public / guest wi-fi users; It is recommended that they are not visible or installed in in-accessible areas such as high spots (poles) or under the fake ceiling.
3. If there is Ethernet network ports on the walls, make sure that they are not within the reach of visitors and are secured adequately. If not used, disconnect them from the network.
4. If a device is missing/stolen, consider modifying the SSID (Wi-Fi name) and Passwords.

4.2.6 Incident reporting and handling.

1. Emergency Contact:
    a. Create a Contact list to reach out to personnel (internal teams and support vendors) during an incident. Refer to section 4-8 Incident Management in the NIAS.
    b. Establish contact with NCSA, Law Enforcement Agencies and your ISP.
1. Log any information security incident (breach or a cyber-crime activity) internally as well as with NCSA and law enforcement agencies (MoI).
2. Incidents can be reported to NCSA by calling their hotline 16555 or sending an email to ncsoc@ncsa.gov.qa

4.3 Corporate Guest Wi-Fi

The need for Wi-Fi can extend beyond your employee's needs. People who are just on site for a visit or consultants working from your premises often need internet access, but a guest Wi-Fi come with its risk that could affect the security of your network and data

Below are few recommendations to follow when configuring a guest Wi-Fi within a corporate.

1. Segregation: make sure your guest Wi-Fi is logically and physically separated from your corporate network.
2. Authentication: create a login page for users where credentials are preferably provided offline.
3. AUP: make sure your guests read and understand your restrictions and security measures by agreeing to an AUP before connecting them to internet. (appendix below contains areas AUP is recommended to cover)
4. Placement of equipment: network plan for access points placement should be well thought of, make sure not to cover areas where you won't need guest Wi-Fi in it.
5. Block any risky or illegal use of the internet through your network (such as by gambling online, buying illicit materials, or viewing pornography).
6. Encrypt the guest Wi-Fi network
7. Change the password regularly to prevent people coming back after their visit and be able to connect to Wi-Fi from proximity to your premises.

4.4 Public Wi-Fi Users

4.4.1 General Security Hygiene

1. Do not use old and outdated devices that may be vulnerable and not adequately updated to connect to public Wi-Fi networks.
2. Do not leave your Wi-Fi or Bluetooth connection ON, when you are not using it.
3. Do not allow your Wi-Fi to auto-connect to networks
4. Avoid using an open Wi-Fi network that is not password protected.
5. Do not share your username / password or mobile device for receiving security tokens for accessing public Wi-Fi networks with anybody including friends.
6. Do not access websites that hold your sensitive information, such as financial or health care while connected to a public WI-FI. In case if you have to:
   a. Prefer using your mobile operator's 3G / 4G / 5G service rather than public Wi-Fi hot spots.
   b. Do not log into any account through a mobile app, rather go to the website instead and verify it uses HTTPS before logging in.
   c. Connect through a VPN.
   d. Logout of accounts when done using them.
7. While connecting or connected to a Public Wi-Fi:
   a. Try to verify if it is a legitimate wireless connection. Check the SSID before connecting, as malicious users may set up rogue wireless AP with SSID names deliberately like popular coffee shops, hotel or venue that offers such free Wi-Fi.
   b. Disable file sharing on the local computer.

c. Consider using your personal devices such as mobile phones, tablets while accessing any websites that store or require the input of any sensitive information. It may be worthwhile accessing such sensitive websites via your mobile phone network, instead of the public Wi-Fi connection.

d. Avoid using public / shared terminals for accessing any websites that require input of any sensitive information.

e. While using public / shared terminals make sure to logout from each portal that you have logged into. Clear your browsing history and delete the web cache before you leave the terminal.

5 Compliance and Enforcement

5.1 Compliance and Enforcement

This guideline is published to help organizations better understand the risks to a public wi-fi service and the risks involved in using them.

The guideline complements National Information Assurance Standard and the National Data Classification Policy.

6 Appendix: Acceptable Usage Policy

Below is a list of areas to be covered in the AUP for your Public or Guest Wi-Fi, Wi-Fi users are requested to read and agree in order to connect to internet through your network:

1. Don’t use the Wi-Fi activities that invade another's privacy ex. spamming and invasion of privacy sending of unsolicited or commercial messages.
2. Not to engage in any activity that misappropriates the intellectual property rights of others, including patents, copyrights, trademarks, etc.
3. Accessing accounts, equipment or networks illegally or without authorization belonging to another party or attempting to penetrate security measures of another system (ex. Port scans, stealth scans, etc.).
4. Using the service in violation of laws and regulations of the State of Qatar.
5. Accessing restricted or illegal (e.g. online gambling & pornography sites).
6. Refer from high bandwidth operations such as large files transfers
7. Using the service to transmit, post, upload, or otherwise making available defamatory, harassing, abusive, or threatening material or language that encourages bodily harm or destruction of property.
8. Refer from distributing of malicious files (ex. Internet viruses, Trojan horses).

7 Annexes

7.1 Acronyms

AUP	Acceptable user policy
NCSA	National Cyber Security Agency
NIAS	National Information Assurance Standard
MitM	Man in the middle
PII	Personal Identifiable Information
PDPPL	Personal Data Privacy Protection Law

7.2 References

No references

7.3 List of Figures

No Figures

7.4 Reporting Incidents to NCSA

Organizations may report an incident to NCSA in one of the following ways:

Call NCSA Hotline at 16555 (24 x 7 service)

Email NCSA at ncsoc@ncsa.gov.qa

Agencies may also find the following guidelines useful to prepare themselves to face an attack / incident.

Guidelines for Incident Management – Pre-requisite Measures