وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Cyber Security Guidelines for Public Wi-Fi Networks

Version: 1.0

Author: Cyber Security Policy and Standards

Document Classification: PUBLIC

Published Date: April 2018

Document History:

Version	Description	Date
1.0	Published V1.0 document	April 2018

Table of Contents

1 Legal Mandate(s)

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (22) of Emiri Decision No. 8 of 2016 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

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

2 Introduction

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

3 Audience

Any person/entity 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.

4 Understand the Risk

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 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.

5 Guidelines

5.1 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 Policy ("NIAP") 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 national public Wi-Fi network.

5.1.1 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. The Service owner should define the operational, acceptable usage and security procedures for the service.
3. 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.
4. Maintain and document an inventory of all devices required to deliver this service.
5. Maintain and manage activity reports, statistics and usage reports of wireless users.
6. Information Security Agreement: Develop information security User Agreement.
7. Information Security Privacy: Define Privacy Policy for Wi-Fi users.

5.1.2 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. Present / 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.

5.1.3 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.
2. Any data collected from users should only be used and shared in compliance with the existing legal instruments such as the Privacy Law.

3. Personally Identifiable Information (PII) should not be shared with any third party except when required and allowed by the Information Privacy Protection Law (Article 18).

5.1.4 Security Hardening:

1. 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.
2. 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 to universal best practices (such as NIA Policy, NIST 800-41, NIST 800-53, ISO 27001, and others).
3. Use different SSIDs while defining names for the wireless network. Avoid using similar names such as “ABC_Corp” and “ABC_Public” or “ABC_Guest”
4. Use strong wireless security protocols such as WPA2 and EAP-TLS. Do not use WEP and WAP protocols.
5. Disable default passwords on network switches, routers and wireless access points. Configure strong passwords in line with the best practices. E.g. A minimum length of 12 characters and 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.
6. Configure the Access Points and Routers as per universal / vendor best practices. Enable encryption (if available), usually it is disabled by default.
7. Remove/disable all default accounts from the used hardware e.g. root, administrator, etc.
8. Change passwords on a periodic basis.
9. 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.
10. Enable security logging on all devices. Refer to “Guidelines for Incident Management – Prerequisite Measures” for support and guidance.
11. Maintain Security Logs for a minimum of 120 days.
12. 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.
13. Use Dynamic exchange mechanisms and secure VPN to transmit PII or payment information to provide sufficient end-to-end encryption and access control.
14. Regularly patch and update your wireless infrastructure.

5.1.5 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.

5.1.6 Incident reporting and handling.

1. Log any information security incident (breach or a cyber-crime activity) internally as well as with Q-CERT and Law enforcement agencies (MoI).
2. Incidents can be reported to Q-CERT through the website or calling hotline +974 4493 3408
3. Once a device is missing, consider modifying the SSID (Wi-Fi name) and Passwords.

5.2 Public Wi-Fi Users

5.2.1 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 similar to 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 you logout from each portal that you have logged into. Clear your browsing history and delete the web cache before you leave the terminal.