وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Security Guidelines for Critical Users Working From Home

Version: 1.0

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: May 2020

Document History			
Version	Date	Description	Comments
1.0	May 2020	Release of Document Version 1.0	

Table of Contents

Legal Mandate(s)

Cabinet decision No. (26) for the year 2018 of the establishment of Cyber Security Sector within the Ministry of Transport & Communications, and 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 the 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 a knowledge-based society and digital economy.

Article (2) of the Cabinet decision No. 926) of the year 2018 and 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 in consideration of the current applicable laws of the State of Qatar. If 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.

Introduction

The current pandemic has seen an unprecedented use of technology to facilitate the organization's business continuity plans and continuation of work during the crisis to maintain social distancing precautions.

And while organizations are putting in efforts to secure the remote access services, it is also incumbent on the end-users to take adequate steps and precautions to ensure a safe and secure experience while using these remote services.

This document looks at some of the risks posed to the end-users and how to mitigate them to have a safe and secure experience while using these remote services.

Objective

The objective of this guideline is to help end-users understand the cyber risks and the controls to mitigate cyber threats and experience a safe and secure experience.

Scope and Audience

Any individual, including high-profile individuals and the devices and the associated infrastructure they use to connect and remotely access services and audio/video conferencing solutions.

Understand the Risks

As an end-user, you may be connecting remotely to connect to your enterprise systems, namely email, business applications, and/or using audio/video facilities to communicate with your team, customers and/or vendors.

The remote system could be a company owned and managed device or an employee-owned unmanaged home device or worse a public terminal at an internet kiosk, business lounge, or an airport. These devices will connect through a home broadband connection, ISP Data services, public Wi-Fi, or guest wireless networks, in all cases, untrusted networks, so to say.

As such, this increases the threat attack surface for your systems unless these threats are suitably controlled and the risks mitigated.

The principal risks that the organization's faces include:

1. Loss of personal and confidential data.
2. Denial-of-service attacks and preventing the use of operational systems.
3. Corruption of data leading to loss of integrity.
4. Financial frauds
5. Reputational damage caused as the consequence of any of these risks occurring

Evolving Threats

The following are some of the leading threats faced by misconfigured or improperly secured devices (laptops/tablets/home routers) and/or insecure user practices.

Wi-Fi-based attacks: Unless secured adequately, traditional Wi-Fi systems are vulnerable and malicious actors (This could be insiders such as guests using the Wi-Fi facilities or hackers, cybercriminals, etc.) could use them to breach into corporate systems or fellow users.

Ransomware and Data Leakage: These are attacks where malicious actors gain access to your systems and stay there as much as possible and try to identify and exfiltrate critical data outside the organization. The data includes business data as well as guest's information (personal/financial (credit cards), etc.). Alternatively, the malicious actor may encrypt your data and demand a ransom to give you back the access to data.

Social Engineering and Phishing: These are attacks where an attacker poses as a legitimate institution or an individual to lure the target into providing sensitive data such as personally identifiable information, banking, and credit card details and passwords. Such attempts may be over various channels such as phone, email, social media, and even face to face.

Malware Infection: These are attacks where a malicious actor infects the endpoint machine to monitor user activities, such as keystrokes (keylogging), web surfing activity and patterns, passwords, network connections, eavesdropping online meetings/conversation. Such events can be captured and collected on the infected machine and then transmitted back to the malicious actor.

Guidelines

Work from Home is a reality now more than ever. COVID-19 has taught us that we need to be ready and flexible with our work arrangements.

But it is ever more critical that the users are more diligent and take the necessary precautions to ensure a secure work experience.

The guidelines below have been written from an end-user perspective to help the users formulate a strategy and implement controls to secure themselves from any potential cyber-attack.

The document complements the National Information Assurance Policy V2.0 and the Security Guidelines for VPN Services v1.0.

People:

1. Have awareness about current cyber threats such as PHISHING, APTs, etc.
2. Be aware and vigilant against Social Engineering threats.
3. Do not click on suspicious links/URLs. Always remember and practice to LOOK before you CLICK.
4. If you receive an unexpected email, especially with an unusual request, kindly double-check with the sender off-line through a phone or through a new email (do not reply on the same email) to verify the veracity of the email and its content.

5. Do not share your passwords with anybody, including your family. It is not about TRUST; it is about ACCOUNTABILITY.

Process:

1. Make sure your devices (laptops, tablets, mobiles, etc.) and applications are updated with the latest security patches.
2. VVIP/VIP (Corporate Senior Management) & Administrators should use a dedicated corporate-owned, managed, and security hardened machine for conducting virtual VIP meetings, managing official corporate social media accounts, and other critical operations.
3. Any such device should only be used for the designated activity and should not have any other application except for official email.
4. Any suspicious emails or applications behaving suspiciously should be immediately reported to the corporate security team or Q-CERT hotline.

Technology:

1. Users must use corporate laptops/devices for accessing any enterprise applications.
2. The corporate laptop/device should have adequate security policies configured, endpoint protection installed, and updated and all applications and security updates patched.
3. Passwords should comply with the corporate password policy. On a minimum, use passwords that are easy to remember and hard to guess, e.g., passphrases and change passwords at regular intervals.
4. The information on the local portable device should be encrypted.
5. Home Wi-Fi should be secured by using Wi-Fi encryption standards, such as WPA-2 protocol.
6. The Home Router should be hardened, on a minimum, change the default usernames and passwords.
7. VVIP/VIP users should never connect directly over the internet. All connections to the internet should go through the corporate VPN connection
8. The application used for the Video/Audio conference should be selected based on a due security assessment. Make sure the app supports and uses encryption.
9. Users should use End to End encryption for all conference calls.
10. All videoconferences/audio conferences should be:
    a. Closed and controlled in terms of attendees
    b. Password protected to authenticate the attendees.
11. Have a dedicated/isolated room/corner in your house to attend any such virtual meetings. The room should be soundproofed or secured adequately to protect against leakage of voice, overhearing, etc.
12. Lock your device when not in use, configure screen locks to be activated if no activity for more than 30 seconds.