وزارة المواصلات والاتصالات
Ministry of Transport & Communications

CYBER SECURITY GUIDELINES

FOR

COMPUTER BASED GAMING APPLICATIONS

Document Control

Version:	1.0
Author:	CS Policies and Standards Section - MOTC
Classification:	Public
Date of Issue:	November 2016

Q-CERT

Contents

Introduction

Online gaming is more popular than ever and every indicator shows that the number of users are only going up with time and the money spent on them is ever increasing.

This has only led to an increase in threats and crimes related to online games. Instances of games and at times fake instances of popular games have been used to spread malicious files. With the popularity of online gaming, cases of privacy breaches have also risen. Online games can also introduce threats such as Spoofing & Phishing, Malicious File Downloads, Social Engineering Scams, Bullying, Character / inventory theft and Computer or smartphone compromise and online and real-world predators

Objective

To provide necessary awareness and guidance to help the online gaming users and developers to avoid, detect, prevent and recover from cyber risks associated with the online games.

Scope

The scope of this document is limited to online gaming (games played over internet / local area network).

Intended Audience

All online gaming users, parents of minor gamers, online gaming providers based in the state of Qatar.

Legal Mandate

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 document 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 later, 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.

Understand the Risks

Games are a leisure activity and developed to entertain, relax and at times educate its users. They were never critical for businesses or individuals. As such, information security was never fundamental while building a game. Games are 150% more likely to include a high-risk vulnerability than an average application available online.

However, times have changed; games have metamorphosed in to a billion dollar industry with huge stakes for organizations that develop them.

The following is a non-exhaustive list of risks that online gaming pose:

1. Spoofing & Phishing, Malicious File Downloads, Social Engineering Scams, Bullying, Character / inventory theft and Computer or smartphone compromise and online and real-world predators
2. **Malicious File Downloads:** Gamers can be a tempted to download a malicious software (potentially decoy games, rooted game applications, Trojan horse apps, viruses etc) to ease their gaming experience or bypass licensing requirements. This could result in their device being exposed and infected by malicious applications including malwares, viruses, key loggers, spy software etc.
3. **Phishing / Spamming:** Since you can never be sure of who your game provider is, there is no assurance that information (such as emails) you provide while downloading or registering may not land in wrong hands. Since quite a number of users opt free games, they in advertently sign up for ad banners, popups, used by the game provider to finance their operations. These pop-ups, private messages or emails may tempt you to websites with malicious content or fraudulent offers pertaining services related to Telecom providers (signing up for premium SMS based services)
4. **Multi-Player Online Games:** Games, particularly MMOG (Massively Multiplayer Online Games) and MMORPG (Massively Multiplayer Online Role-playing Games) allow players to compete with and against each other on a grand scale in real-time. MMOG and MMORPG are increasingly gaining popularity with the digital generation. The virtual worlds in MMOG and MMORPG provide an environment where people communicate with each other using a virtual persona—avatar—and allow strangers who do not necessarily speak the same language to establish relationships (in the virtual worlds). Such interactions could raise the risks of Cyber Bullying, Online Sexual Harassment among others.
5. **Social Engineering Scams:** Online Gaming provides an excellent virtual platform to be-friend perfect strangers. Malicious actors could sweet talk online gamers in to parting with their gaming credentials and potential private / personal data while engaging in conversation or any other communication means the game provide. More often than not, the gaming credentials could reveal a link to the online identity of a gamer, which can then be connected to his physical identity. Further, predators may use online gaming to build a relationship with children and gain their trust.
6. **Cyber Bullying / Online Sexual Harassment:** Some gamers may be aggressive or try to harass other gamers, which may result in psychological consequences or at, least ruin their gaming experience, and such bullies should be reported and blocked or at least avoided. The cyber bullying may also extend itself to online sexual harassments that may include passing comments that may be sexist in definition to virtual manhandling in MMORPG.
7. **Character / Inventory theft:** Malicious actors may hack into or take over identities of gamers to own their achievements and goodies.
8. **Financial:** Games are no longer played for fun alone and are huge money business. Depending on the game itself, you may require to buy a licensed or a full-blown version. Malicious actors may provide rooted gaming applications or hack keys to bypass license requirements. For Online Gaming providers, there is a risk of payment platform being compromised by malicious attackers.
9. **Game Currency:** The rewards earned by players including point and/or game currency is becoming valuable and gaining acceptance with online currency platforms being established to exchange or trade in this game currencies. This makes it a target for malicious actors who might want to benefit from this.
10. **Personal Data:** The game providers collect a lot of personal information including personal details, credit card details (while purchasing licenses / game currencies) etc. and this unless secured adequately is a target for malicious actors.

Recommended Best Practices

1- Online Gamers

Online Identity:

- Maintain as distinct an identity as possible from your normal Online identity.
- Secure your identity where possible with a strong password, use multi-factor authentication if available.

Platform Hygiene:

- Ensure that the platform you play game on (Smart Phones / Tablets / PCs and Laptops) have an effective and updated Anti Malicious software installed and running along with a personal firewall and/or Host Intrusion Detection system (HIDS) running.
- Play only with authorized and licensed versions of games downloaded from authentic sources.
- Verify the authenticity and security of downloaded files and new software.
- Avoid use of cheat programs to skip to higher levels and/or gain specific advantages in a game as this can expose users to unsuitable content and malicious programs affecting your computer.
- Configure your browser with recommended security settings while playing the game through a web interface.
- Make sure you keep the game software up to date. Most multiplayer games automatically update themselves before letting you connect.
- Do not give up on your system's security settings to increase your system's speed.

Phishing / Spamming:

- Do not click on Pop-Ups / Advertisements that appear within the game.
- Do not open attachments or click on links received in emails and/or social media purportedly received from your gaming companions and/or game provider.
- Whilst using the chat facility available within an online game, never give away your username, password or any other personal information, to anyone including your online companions / friends.
- Report any attempts to phish information out from you by your game provider and/or online gamer.
- Choose a user name that does not reveal any personal information. Similarly, if your game includes the ability to create a personal profile, make sure you don't give away any personal information.
- Do not reveal any personal information to other online gamers.
- Be careful how and where you store your credit card information for in-game payments.
- Watch out for frauds when buying or selling 'property / game currency' that exists inside a computer game, in the real world.

Media Disposal

- Prior disposing of your gaming device either by selling, scrapping, giving away or by donating, delete all personal information from the device. The method of doing this varies from device to device. NIA Policy Section C-8 provides guidance on Media sanitization and disposal. Do not forget to delete your account details, and backup or transfer your games to your new device if appropriate.

2- Parents

Oversight

- Set guidelines and ground rules for your children when playing online.
  - Enable parental controls on laptops / Desktops / Smart Phones used by your children to limit cyber exposure of your children.
  - Have a firsthand feel of what the game your child is playing by participating in it with him.
- Check trusted websites for the latest information, share with your children, and encourage them to be web wise.
  - Teach your children cyber security etiquettes.
  - Make them aware about general cyber security threats.
  - Advise your children to use "avatar" rather than an actual picture of themselves on all online gaming / social media platforms.
  - Advise your children against making friends with complete strangers online and against sharing personal / sensitive information with anybody online.
- Keep a close eye on the gaming habits of your children.
  - Make sure your children are aware and know how to report/block a cyberbully.
  - Watch for any changes in your child's emotional / psychological posture to guard against any ill effect / exposure to online games.

3- Games Providers / Developers

Security By Design:

- Ensure that the games developed are secure and adhere to industry best practices and standards during the software development cycle.
- They should comply with security best practices, standards and policies to ensure that security is; imbibed within the design of the product. Qatar has issued the National Information Assurance Policy (NIA Policy V2.0) and games developer should adhere to its control as applicable.
- Any software / hardware deployments should adhere to an established system commissioning procedure that ensures adequate testing (including but not restricted to functional testing, security testing, user experience, acceptance testing etc) prior commissioning of any new software or hardware.

Legal

- Ensure that the games developed adhere to the legislations in target countries.
- As per Qatari Law No. 11 of 2004 gambling[i] is not allowed in Qatar. Further, the country follows a conservative code of conduct and games espousing sex, hate may not be acceptable.

Copy Protection:

- Ensure controls to protect against reverse engineering of code, duplicate copies, key and data protection to secure servers and core logic of the game.
- Define clearly the sources where gamers can buy/download the game.
- Use suitable encryption to ensure the integrity of file available for download.

Protecting the Client:

- Protect your game client against any modifications by malicious actors.
- Ensure that all players use the same modifications.
- Ensure traffic between the client and server is protected against attacks such as packet sniffing or Man in The Middle (MITM) attacks to manipulate the game in their favor.
- Ensure traffic between the client and the server is the minimum required by employing techniques such as Area of Interest Management.
- Ensure the games promote usage of strong passwords and multi factor authentication.

Mitigate against revenue loss:

- Ensure controls to prevent tampering and/or compromise of the in-game purchasing systems, or unauthorized access to assets
- Ensure controls to prevent a "clone" of the back-end server from being created and run independently of the game operator
- Ensure controls to monitor and deter production of free, cracked versions of "for-pay" games.
- Ensure controls to copyright and/or secure Intellectual Property Rights (IPR) of characters / stories / brand.

Virtual Abuse:

- MMOG and MMORPG game providers should provide a channel to gamers to report any form of abuse they encounter during the games.
- Logging gamer's activities to validate any reported abuse by another gamer.
- Providing filtering / censorship options to gamers to filter out unwanted gamers.
- Ensure controls to take action against gamers accused of abuse.

Denial of Service:

- Ensure controls to prevent Denial of Service attacks perpetrated by gamers against each other to gain undue advantage
- Ensure controls to prevent Denial of Service attacks perpetrated by malicious actors against game servers.

Admin Privileges:

- Procedures must be set in place and followed, to ensure misuse by Privilege users / System administrators that manage the game.
- Any changes to the gaming application / server should follow a defined Change Management Procedure.
- Enable logging of all privilege and system actions executed on the game servers.
- Monitor logs to detect and respond to any malicious/suspect action.

Backup and Availability*:*

- Conduct a business impact assessment to assess the availability requirements.
- Design and implement a backup strategy based on the availability requirements.
- Ensure adequate backup copies are available including at off-site locations.

Acceptable Usage

- Define a list of terms and conditions that define acceptable usage for the gamers.
- Prescribe disciplinary actions such as termination for players who break the rules.

[i] Gambling means any game in which the probability of gain and loss depends on uncontrolled chance and each party agree to give an amount of money or any other benefit to be agreed upon, in case of loss, to the winning party.