**End of Module Assignment Expert Report**

**Written by Ali Ahmad**

**University of Essex**

**Dr Maria Albanou**

Contents

[1. Introduction: 3](#_Toc120433716)

[2. Cyber Security Challenges 3](#_Toc120433717)

[3. Common Types of Identity Theft 4](#_Toc120433718)

[a. Phishing 4](#_Toc120433719)

[b. Debit card or credit card fraud 4](#_Toc120433720)

[c. Mail identity theft 4](#_Toc120433721)

[d. Phishing scam in Qatar 4](#_Toc120433722)

[4. How is Qatar dealing with cybercrime and other forms of online insecurity? 5](#_Toc120433723)

[5. Rights and Ethics to dealing with these crimes 5](#_Toc120433724)

[6. Limitations with these dealings 6](#_Toc120433725)

[7. Cybercrime laws in Qatar 6](#_Toc120433726)

[8. Tools Used against the Cybercrime Investigation 7](#_Toc120433727)

[a. Forensics Investigation: 8](#_Toc120433728)

[b. Limitations Faced: 8](#_Toc120433729)

[9. Other relevant laws 8](#_Toc120433730)

[10. References 8](#_Toc120433731)

# Introduction:

The Internet has empowered us to communicate with individuals from all around the world on a level we could not have imagined. With these obstacles removed, we are better able to work together in both our personal and professional lives. Cyberspace is now a living, breathing aspect of our culture that drives innovation, improves our standard of living, and helps the economy in ways we could never have imagined. There is a high potential for gain, but also a high potential for loss. Since there are no physical limits to cyberspace, it also presents potential for harm to persons and businesses to those who would do us harm.

The prevalence of cybercrime in the international society is an increasing worry for individual safety, particularly because it is aligned with the theft of cyberidentity. Europeans, just like many other people all throughout the world, can occasionally find themselves the victims of identity theft committed online. According to (Manap et. al., 2015), the term "cyber-identity theft" refers to a theft that is enabled by the Internet and in which the perpetrator targets an individual's personally identifiable information (PII) to perpetrate fraud or theft. PII refers to personally identifiable information, which can include sensitive private data such as names, addresses, national identity numbers, and social security numbers. Because people are continuously conducting business, connecting with one another, and sharing important data through online platforms, they leave behind digital footprints that contain personally identifiable information (PII) that an adversary might use to execute a cybercrime against them.

# Cyber Security Challenges

Qatar's cybercrime laws are unique among Middle Eastern nations.

Especially in light of recent highprofile assaults on its media and government websites and the networks of its energy industry, this shows just how seriously it takes cybercrime and cyber security.Before the blockade against Qatar was imposed in June 2017 by Saudi Arabia, the United Arab Emirates, Bahrain, and Egypt, the website of the Qatar News Agency (QNA) allegedly reported that His Highness the Amir Sheikh Tamim bin Hamad Al Thani had called Iran a "superpower," praised Hams, and assumed that US President Donald Trump could not last long. After this, according to OSAC, the QNA website went down and hasn't returned to service to this day.

Several U.S. residents in Qatar informed the Ministry of Interior and the Regional Security Office about internet fraud in 2018. Scammers used the embassy's name and contact details to convince their victims to wire funds for fictitious services, such as assistance with finding employment, paying for college tuition in the United States, or purchasing costly equipment. Trend Micro has reportedly stopped or uncovered over 15 million cyber attacks in Qatar since 2020, as detailed in the company's annual cybersecurity report.

The organization prevented almost 7 million URL victim assaults, over 1.6 million malware attacks, and over 4 million email threats (Kilani, 2022).

# Common Types of Identity Theft

To conduct identity theft, criminals must gain access to sufficient of a victim's private information to commit fraud on their behalf. These facts can be stolen through a variety of means, including overt theft, social engineering, and cybercrime data harvesting (Huziej, M., 2021).

## Phishing

To gain access to personal information like a person's name, address, SSN, bank account details, or password, phishers will often pose as a legitimate business online. It is then put to use in order to gain entry to protected areas or accounts.

## Debit card or credit card fraud

Credit card and bank statement fraud is a form of identity theft because the victim often does not suspect anything is amiss until they receive their statement and discover unauthorized charges. It's not too late to fix the problem, but the damage has been done. If you tell your credit card company within 60 days of receiving your statement, they should cancel the unauthorized charges and give a refund. However, the true mystery is how this happened.

Numerous methods exist for thieves to get your financial data and exploit it to make unauthorized purchases. Gas station and ATM card readers are common locations for thieves to install card-skimming devices. Skimmers are devices that can be used to steal sensitive information from your debit or credit cards. A pinhole camera is set up nearby to record the digits of the pins. Criminals will either use your account without your knowledge or sell your card to those who will.

## Mail identity theft

Con artists may get a lot of information from your email. Identity thieves may use your personal information to fraudulently access financial accounts, credit cards, loans, mobile phones, and even passports in your name. Identity thieves can obtain your personal information through mail theft, trash and recycling bin rummaging, and, if you've recently moved, either opening mail addressed to your old address or fraudulently setting up mail redirection.

## Phishing scam in Qatar

To mark its silver anniversary, Qatar Airways last year began sending out complimentary plane tickets to two people in each family to a select group of WhatsApp users. In the URL, the "a" has been replaced by “a" for the site: www.qatarairwys.com. To "claim" the "free tickets," visitors to the website were first given the remaining amount of tickets, then requested to take part in a survey and send the link to 15 friends/groups via WhatsApp. No longer accessible, this fraudulent website has been shut down. In response to the "fake anniversary offer," Qatar Airways issued a statement on their Twitter account (Chung, L., 2019).

The Government of Qatar's Ministry of Transportation and Communications has also launched a public education campaign to warn citizens about the dangers of phishing.

**How to avoid Phishing:**

* Do not let just anyone in on your personal details; be careful whom you share them.
* You should never open a link in an email that you are unsure of it.
* Verify the website's address for any spelling mistakes or other red flags that can suggest it is a phishing site.
* Instantly notify the relevant body or trade association.

# How is Qatar dealing with cybercrime and other forms of online insecurity?

1. To combat these dangers and provide a secure online community, Qatar is bolstering its cyber security measures and working with its international peers. In 2005, the Ministry (then known as the Ministry of Information and Communications Technology) partnered with Carnegie Mellon University to develop the Qatar Computer Emergency Response Team (Q-CERT).
2. To monitor and counteract cyber threats, the Cyber Security Division's Q-CERT and Critical Information Infrastructure Protection (CIIP) teams work together with other Qatari government agencies, businesses in the private and public sectors, and ordinary individuals. Protecting personal information and ensuring the safety of Internet users is a top priority for the Division.
3. Given that information security issues are global in scope, the Cyber Security Division is a member of FIRST, an international network of incident response and security teams. Keeping everyone up-to-date on the newest security risks and countermeasures is a top priority, which is why FIRST promotes regional connections between security teams and partners throughout the globe. In addition, the Division participates in the international Meridian Process to safeguard vital information infrastructure.

# Rights and Ethics to dealing with these crimes

The Qatari government passed Cybercrime Prevention Law No. 14 of 2014 on September 16, 2014, so that there are more ways to fight online and cybercrimes. The new law has different fines and punishments for breaking the rules when using computers, the internet, or information technology networks. More crimes that fit together. The goal of the law is to protect the country's electronic infrastructure and improve Qatar's cyber security as a whole. To meet the most important requirements, the law well be published in the Official Gazette as soon as it goes into effect (Alhout, 2014).

When the law was been made, there was a lot of debate because many people thought that some parts of the Act hurt their right to free speech and access to the media. The law has several parts, some of which are list below:

1. The law says that making a fake official electronic document can get you up to 10 years in prison and a fine of up to 200,000 Qatari riyals (QR). However, the law lowers the maximum prison sentence to three years and the maximum fine to 100,000 Qatari riyals (QR). People who use the Internet to steal someone's identity, pose as another person or business, steal things that can be moved, or imitate another person or business face similar punishments.

2. Measures to protect against "content crimes," which are crimes that make it illegal to spread "fake news." Since these terms are not been defined, it is not clear what kind of content could get local journalists and social media users in trouble. Before sharing news with the public, news organizations, people who use social media and journalists should be careful and check where it came from so they do not break the law.

3. A jail sentence of up to three years and a fine of up to 200,000 QR for having or using an ATM or credit card without permission, as well as for stealing numbers or making fake electronic cards.

4. A prison sentence of up to three years and a fine of up to 500,000 Qatari riyals for breaking intellectual property rights on the Internet (article 13). This includes copyrights, patents, trade secrets, trademarks, trade names, geographical indications, industrial designs, and designs of integrated circuits. 5. Up to three years in prison and a fine of up to 500,000 Qatari riyals for using the Internet to break intellectual property rights.

# Limitations with these dealings

Due to the existing situation, intra-GCC collaboration in the fight against cybercrime is dependent on bilateral links and informal channels, such as police-to-police or agency-to-agency communication. These methods are beneficial, but they are insufficient to build an efficient regime since they limit the investigative steps that may performed, lack a coherent approach, and are compelled to operate across many laws enforcement networks. Mutual Legal Assistance Treaties79 (MLATs) are "agreements between governments that permit the exchange of information pertinent to an ongoing inquiry in at least one of those nations." In most cases, informal processes precede official petitions for MLATs. MLATs are "agreements between governments that permit the exchange of information pertinent to an inquiry taking place in at least one of those nations." 80 Due to the nature and frequency of cybercrime, as well as the nature of the evidence, however, informal channels are not appropriate for cybercrime investigations. They do not deliver the requisite responsiveness in a timely manner or interstate alignment of priorities. They do not guarantee these two things (Merdrignac-Conanec, et. al., 2017).

# Cybercrime laws in Qatar

1. The government of Qatar passed Cyber Crime Prevention Law No.14 of 2014 on September 16, 2014, to make it easier for the country to fight cybercrime. Laws have a wide range of penalties for crimes committed through the Internet, IT networks, computers, and other connected devices. The laws meant to protect Qatar's technical infrastructure and improve the country's cyber security as a whole. The law has ways to stop most internet crimes and makes sure that each kind of internet crime punished harshly.
2. Law No. 14 of 2014 on Combating Cyber Crime makes it possible for cybercrime cases to bring to court in Qatar. It also makes it illegal to commit a crime with the help of a computer, the Internet, a database, or any other kind of information technology (Article 45).
3. Some of the rules of the law, according to the website of Al Tamimi and Co. (Alhout, R., 2017), are as follows:
   1. If you fake a formal electronic version, you could get 10 years in prison and a fine of up to 200,000 QR. If you fake an informal piece of information, you could get 3 years in prison and a fine of up to 100,000 QR. People who steal people's identities, break into homes, or steal really goods over the Internet get the same punishments as people who pretend to be someone else or an organization.
   2. Details about "content crimes" that make it illegal to print "fake news." Because these phrases are not clear, it is not clear what could get local reporters and people on social media in trouble. Therefore, news organizations, people who use social media and reporters must be careful when using unconfirmed sources to tell the public about the news.
   3. For illegally having or using an electronic card like an ATM or credit card, stealing card credentials, or making electronic cards, the maximum penalty is three years in prison and a fine of up to QR 200,000.
   4. In Qatar, you can get up to three years in prison and a fine of up to 500,000 Qatari riyals for breaking intellectual property rights online. This includes things like copyrights, patents, trade secrets, trademarks, trade names, geographical indications, industrial designs, and integrated circuit designs (article 13). Qatari law covers blackmail, fraud, and other types of cybercrime. Because these crimes can happen anywhere in the world, the law also covers things like international cooperation (Al-Thani, T. B. H., 2011).

# Tools Used against the Cybercrime Investigation

Cybercrime Technologies, which has its headquarters in Qatar and is an ADF Authorized Partner, specializes in the analysis of digital crimes performed on a wide range of electronic devices. Qatar also has the National Cyber Security Agency, popularly known as the NCSA, was founded because of Amiri Decision No.1 of 2021. In addition to its other functions, the NCSA is responsible for the execution and oversight of matters pertaining to national cyber risks and threats, the improvement of preparedness and resilience against cyber crises, and the protection of critical infrastructure (Entity, 2022). These organizations technical consultants and investigators have extensive expertise in their respective industries and may give help in a variety of specialized areas, including the following:

* Digital Forensics
* Cyber Crime
* Cyberwarfare
* Social exploitation
* Terrorism Protection in Addition to Other Concerns

Throughout its more than two decades of experience, Cycure has collaborated with national and international Government, Law Enforcement, and Military institutions. In addition, the organization has expertise in the field of technological evaluation as it pertains to public safety and security (Solutions, 2020).

## Forensics Investigation:

The forensic investigation laboratory can analyze a broad variety of cases. In addition, the corporation maintains significant and close contacts with law enforcement, which helps to guarantee that its digital investigation tools can satisfy the ever-changing needs of these organizations. The organization's examiners are aware of the need to protect the validity of digital evidence, which includes performing on-site investigations and transporting evidence in a secure manner to preserve the chain of custody.

## Limitations Faced:

Cybercrime investigations might face several challenges. One difficulty is user anonymity in ICTs. Individuals with anonymity may participate in activities without disclosing themselves or their actions (Maras, 2016). Cybercriminals hide their identities in several ways. This method includes proxy servers. An intermediate server, or proxy server, links a client to the server from which the client requests resources (Maras, 2014, p. 294). Anonymizers often called anonymous proxy servers, mask users' IP addresses with those of another user (Chow, 2012).

# Other relevant laws

Legislation No. 13 of 2016 protects the privacy of individuals' personal information in Qatar.

The legislation contains provisions for the privacy of minors, as well as fundamental data protection obligations in the management of data, and preventive measures against loss, injury, modification, disclosure, or unauthorized access, and in certain circumstances authorization from persons.

# References

Manap, N.A., Rahim, A.A. and Taji, H. (2015) ‘Cyberspace Identity Theft: The Conceptual Framework’, Mediterranean Journal of Social Sciences, 6(4), pp. 595–605. Available at: <https://doi.org/10.5901/mjss.2015.v6n4s3p595>.

Kilani, H. (2022, July 26). 15 million cyber threats targeting Qatar blocked this year: report. Retrieved November 24, 2022, from Doha News | Qatar website: <https://dohanews.co/15-million-cyber-threats-targeting-qatar-blocked-this-year-report/>.

Huziej, M. (2021, June 30). The common types of identity theft. Retrieved November 24, 2022, from CPD Online College website: <https://cpdonline.co.uk/knowledge-base/business/common-types-of-identity-theft/#:~:text=The%20National%20Crime%20Agency%20identifies>

Chung, L. (2019, January 25). Watch out for phishing scam in Qatar. Retrieved November 24, 2022, from ILoveQatar.net website: <https://www.iloveqatar.net/news/general/watch-out-of-phishing-scam-in-qatar>.

Alhout, R. (2014, August). Cyber Crime Prevention Law in Qatar. Retrieved November 24, 2022, from Tamimi.com website: <https://www.tamimi.com/pdflawupdate/?pageID=5013>.

Merdrignac-Conanec, O., Durand, G., Walfort, S., Hakmeh, N., & Zhang, X. (2017). Elaboration of CaLa 2 S 4 transparent ceramics from novel precursor powders route. Ceramics International, 43(8), 5984–5989. <https://doi.org/10.1016/j.ceramint.2017.01.132>.

Alhout, R. (2017, August). Cyber Crime Prevention Law in Qatar - Al Tamimi & Company. Retrieved November 24, 2022, from Al Tamimi & Company website: <https://www.tamimi.com/law-update-articles/cyber-crime-prevention-law-in-qatar/>.

Al-Thani, T. B. H. (2011). Qatar National Development Strategy 2011~2016. In un.org. UN.org. Retrieved from UN.org website: <https://www.un.org/development/desa/disabilities/wp-content/uploads/sites/15/2019/10/Qatar_Qatar-National-Development-Strategy.pdf>.

Solutions, A. D. F. (2020). Cycure Technologies (Qatar). Retrieved November 24, 2022, from www.adfsolutions.com website: <https://www.adfsolutions.com/partner/cycure-technologies-digital-forensics-qatar>

Entity, G. (2022, August 5). National Cyber Security Agency. Retrieved November 24, 2022, from https://hukoomi.gov.qa website: <https://hukoomi.gov.qa/en/government-office/national-cyber-security-agency>.

Maras, Marie-Helen. (2016). *[Cybercriminology](https://www.unodc.org/e4j/data/_university_uni_/cybercriminology.html?lng=en&match=Cybercriminology" \t "_blank)* . Oxford University Press.

Maras, Marie-Helen. (2014). [Inside Darknet: The Takedown of Silk Road](https://www.unodc.org/e4j/data/_university_uni_/inside_darknet_the_takedown_of_silk_road.html?lng=en&match=Inside%20Darknet:%20The%20Takedown%20of%20Silk%20Road) . Criminal Justice Matters, Vol. 98(1), 22-23.

Chow, Peter. (2012). [*Surfing the Web Anonymously*- The Good and Evil of the Anonymizer](https://www.unodc.org/e4j/data/_university_uni_/surfing_the_web_anonymously_-_the_good_and_evil_of_the_anonymizer.html?lng=en&match=Surfing%20the%20Web%20Anonymously). SANS Institute InfoSec Reading Room.