Recent Cybercrimes In Fiji

Shireen Nisha, Mohammed Farik

Abstract: In this age of digital natives, we are immersed in digital information 24/7. Individuals, organizations, and government have their share of information systems to mange and use in the various processes of their digital existence. Being a small island state and still developing amidst various problems, Fiji cannot afford losses due to cybercrime. This paper aims to create awareness in regards to some major cybercrimes in Fiji in the year 2016. We believe that the cases and solutions discussed will assist in enforcing better cyber security measures to prevent being victims of such cybercrimes in the future.

Index Terms: Cybercrimes, Cyber security, Defacement, Harassment, Phishing, Scam

1 Introduction

Fiji, with a population of 915,303 has 419,958 Internet users and 380,000 Facebook users as of June 2016 [1]. Cyber security is a part and parcel of our daily lives in this era where even a child generates and keeps data of some sort. Not just individuals but many companies have fallen victim to cyber crimes worldwide. Fiji hasn't been spared by cybercriminals either, despite it being just "a dot in the ocean". Cybercrimes takes many forms with the major one being cyber deception. According to Razim Buksh, the director Financial Intelligence Unit (FIU) of Fiji, cyber deception is one cybercrime that has caused many Fijian companies losses in thousands of dollars between the years 2013 to 2015 [2]. Fiji, a small island nation, is still recovering from a recent severe category 5 tropical cyclone Winston, that making landfall on the main island of Vitilevu at its peak intensity on 20th February, 2016, has had an estimated initial damage bill of $650 million [3]. It isn't tech-savvy in comparison to the likes of some of its neighboring oceanic countries such as Australia and New Zealand, yet it has such high rate of losses through cybercrimes. If Fijian citizens and businesses continue to incur losses at this rate then it's going to have a major negative impact on Fiji's already staggering economy. This motivates the proposed work to study the existing cases of cybercrimes in Fiji to bring them to light to the general public and to propose ways to mitigate or safeguard from these attacks. The rest of the paper is organized as follows: next section reviews some cases of cybercrimes that has occurred Fiji in recent years, section 3 will look at the analytics of these cases, while section 4 briefly discusses the proposed solutions. Lastly, section 5 concludes the paper and discusses about the future work in this area.

- *Shireen Nisha is currently pursuing masters degree program in Information Technology in the School of Science and Technology at the University of Fij. E-mail: shireenn@unifiji.ac.fj*
- *Mohammed Farik is a Lecturer in Information Technology in the School of Science and Technology at the University of Fiji. E-mail: mohamedf@unifiji.ac.fj*

2 Cases of Cybercrimes in Fiji

2.1 Cyber Deception

The most recent case of cyber deception was highlighted on 19th August 2016, cautioning public about several fake Facebook profiles of the governor of the Reserve Bank of Fiji (RBF), Barry Whiteside. These bogus sites have lured the unsuspecting public into sending funds to secure proceeds of fake lotteries, investments and loans [4]. The scam was identified when one of the victims approached RBF seeking approval to send money in order to have his grant which had been approved by the Governor himself [5]. As of 27th August 2016, FIU in correlation with the Fiji Cybercrimes Unit were still investigating the three reported cases of people falling victim to this fake Facebook account. FUI has managed to shut-down the fake account and has traced the perpetrators to be from overseas, believing that they could be operating out of Africa [5]. In this case, the threat agent can be any individual within the social media population of Africa, especially someone with prior knowledge of social media usage and practices. Both tangible and intangible assets have been affected or had been used in this case. Intangible asset is the goodwill of RBF which could have been tarnished if it hadn't been brought to the attention of FIU. The tangible assets used by the criminal in this case was the RBF letterhead and logo which was used on documents asserting to offer loans and grants to make their communication look authentic [5]. Another asset that was affected is the saving of the victims which they remitted. Various types of cyber deception occurs when social media is involved, especially Facebook, where millions are connected. Another case which came into light in December 2014 was of a fake online shopping Facebook account, *Vakaviti Fashions* which made headlines as numerous complaints were made from western and northern division highlighting failure to deliver goods despite paying by making deposits. A 22 year old local woman was charged with 9 counts of obtaining financial advantage by deception in relation to this case [6]. The exploit was to take advantage of the vulnerabilities. One of the vulnerabilities in this case was the availability of authentic content from the RBF website (http://www.rbf.gov.fj/), particularly extracting the logo and devising a letterhead that followed the same format of the downloadable forms on the website. Another loophole was the ease with which anyone can create an FB account without giving much personal data about themselves. Other vulnerabilities were users' interactions and addiction to FB, users' submissive nature and level of online discourse.

2.2 Email Phishing

Building up from the above case of RBF fake FB account, is email phishing [4], [5]. As an addition to the fake FB account case, email accounts had been created to look like official email account of RBF, however it didn't have the official domain (*@ rbf. gov.fj)* [4]. The threat agent in this case is the same individual as the fake FB account creator who exploited the vulnerability located on the official RBF website to get the tangible assets. In this case it's the contact details of the executive management team, particularly the designation and email address of each member which were used to orchestrate the phishing attack to make victims believe that they actually were communicating with Governor Whiteside [4].

2.3 Website Defacement

Website defacement is probably another prime security concern for most organizations that have a web presence, particularly, religious, government, bank and corporate websites [7].The attacker gets unauthorized access to the web server, replaces the hosted website with their own and then makes changes maybe in the visual appearance of the site or a webpage [8]. In March 2016, the Royal Fiji Military Force (RFMF) website was defaced by a Kurdish hacker, MuhmadEmad, known for his anti-ISIS views, who allegedly has hacked numerous U.S. and Turkey government websites over the past two years. Of the 58 sites that the Fiji government hosts, only five were affected and RFMF website was one of them [9]. It seems that the attacker is a hackivist [10] expressing concern and trying to bring the attention of troop-contributing countries to the growing attacks on soldiers in Sinai [11] where the Kurdish armies of Peshmerga are also situated and are fighting to defend their homeland from ISIS forces based in Iraq [9]. This type of attack exploits vulnerabilities in the codes of the web application and sends malicious scripts to the application to be executed when any user input tasks are performed. The asset used in this case is the RFMF website which couldn't provide the required services to the intended users till the time the website was put back on line.

2.4 ATM/Credit Card Scam

ATM/Credit card scams is yet another attack that is becoming prevalent in Fiji and costing the banking industry million in losses, as stated by the chief executive of ANZ Pacific and Fiji on February 20, 2016. This statement came about after claims by 2 customers that their credit cards have been skimmed abroad, one for the amount of $10,000 in Saudi Arabia and the other for sum of $2000 in Ukraine. In order to protect its customers from fraudsters the instant step taken by ANZ after this revelation was to cancel all customers' cards temporally till the matter was resolved by FIU [12]. It seems that the perpetrators obtained card details either through ATM or EFTPOS skimming devices or via skimming of ecommerce and banking site. In Fiji the first reported case of skimming device usage was in 2003, with the last major one being in December, 2015, which affected over 500 credit and debit card holders [13]. A tip from a taxi driver altered police about a group making numerous suspicious withdrawals in Lautoka area leading to the arrest of 6 Chinese nationals who had in their possession 384 BSP, Westpac and ANZ ATM fake cards plus over FJ$22,807 in cash. The group had orchestrated the entire scheme, which started with the arrival of the group into Fiji from China on December 3, 2015, followed by making fake ATM cards from skimmed card details until 5th December, leading on to massive withdrawal using the fake cards on 6th and ending with flying out of Fiji on 7th December[14]. Other items confiscated from the hotel room that they stayed in was a card making device, a laptop and 104 more fake cards hidden inside a sofa in the room. They have been charged with 10 counts of theft and 10 counts of dishonestly obtaining or dealing with personal financial information [15]. In the case of credit card scams, the threat agent are the scammers who have either set up fake sites or skimming devices on ATMs that captures the assets, which are the user's personal and financial details. There has also been some cases of malware affected android devices which pretends to be adobe flash players but scans the system for banking apps and then reports back to the hackers so they could install the fake login page to capture users bank details [13]. The asset gained by the scammer eventually is money from the victims account.

2.5 Cyber Bullying/Harassment

Cyber bullying/harassment is another case of Internet related crime and it isn't uncommon even in a small island nation such as Fiji. This attack is particularly applied to children who use social media sometimes even without their parents' knowledge. One such case in Fiji was of a year 8 student of a prominent Suva school who got raped by a 17-year-old boy from Nadi when she went to meet him in Nadi as orchestrated through their Facebook communication. Social media is used to bully children and teenagers into doing things that isn't normal for them and they remain quite even after the incident mainly because of fear of being blackmailed [16].

2.6 Cyber Maltreatment of Children

Since the discussion of the above case is based on child social networking, there is yet another area which could be linked to cyber crime, that is cyber maltreatment of children. On June 27, 2016, Fiji Cybercrime Unit started investigating a disturbing FB post showing some adults giving beer to a child to drink. ACP Luke Navela, Chief of Intelligence and Investigations stated that any social media posts showing the maltreatment of children will be thoroughly investigated [17].

3 Case Analysis

Data regarding the six cases of cybercrimes as discussed in this paper has been analyzed and Fig. 1. shows the graph projecting the victims of each of these cases. While most cases show that the general public mostly fall victims, website defacement has a more specific victim which is the organization that is targeted. However, the general public too gets affected indirectly. Suppose if a website goes out of service while the company tried to rectify the defacement issue, then the general public is temporally denied access to some information or service they may need. Therefore we could say that the general public is almost every time affected either directly or indirectly whenever that is a cybercrime. In addition to that a more specific group is being targeted by some perpetrators who prey on the innocent nature of children and teenagers through the use of popular social media sites. Fig. 1 also shows the victims of cyber bullying/harassment and cyber maltreatment to be 50% children and 50% general public.

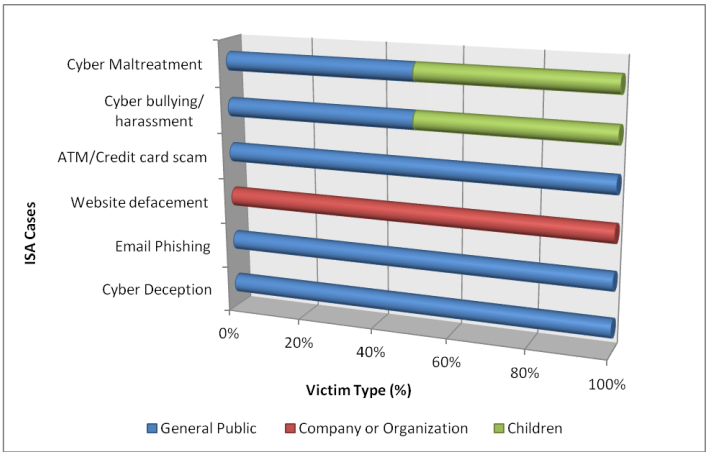

Fig. 1. *Major Cybercrime Cases in Fiji in 2016 and Victims*

TABLE 1
CYBERCRIME TYPE, DATE OF ATTACK, AND VULNERABILITIES EXPLOITED

CYBERCRIME Type	Date	Vulnerabilities
Cyber Deception	Aug 2016	• Ease of access to authentic content. • Ease of FB account creation without giving much personal details • Users interaction and addiction to social media • User's submissive nature and level of online discourse.
Email Phishing	Aug 2016	• Ease of access to authentic contact information • Lacks time to check if email has official domain
Website defacement	Mar 2016	• Loopholes in codes of web application
ATM/ Credit card scam	Feb 2016	• Working class society lacks time to ensure safety measures • No anti-virus or anti-malware enabled. • Online bankers not verifying account activities from ATM or another computer.
Cyber bullying/ harassment	Apr 2015	• Innocence of a child. • Parental negligence • User's interaction and addiction to social media • User's submissive nature and level of online discourse.
Cyber Maltreatment	Jun 2016	• Innocence of a child. • User's interaction and addiction to social media • User's submissive nature and level of online discourse.

4 POSSIBLE SOLUTIONS

Fiji has a set of laws that handles computer crime offences in the form of sections 336 to 351 of the Crimes Decree # 43 of 2009. Even though, this serves as a deterrent to some there are many others who know the limitations and disregard the legal implications of being convicted with a cyber crime in Fiji. Take for instance the ATM card scam [14], as discussed earlier in this paper about outsiders coming into Fiji with plans of conducting cyber crime. The government needs to tough the law. Apart from this, there are several alternatives for each case discussed below.

4.1 Cyber Deception

Several alternative solutions could be implemented which could prevent this type of attack in the future. Major thing is to create awareness to the general public about the methods used by RBF to conduct all transactions. After the incident, RBF has told the media that none of his staff communicates with anyone via Facebook or other social media regarding official business matters [4]. This awareness could have been made before the attack happened. Patching up the loopholes would definitely resolve the issue. This means that the free and easy access to company assets that were used here should be blocked somehow. All forms downloaded from RBF site should have a digital water mark embedded several places that have a logo or on the letterhead. If there could be some kind of algorithm made that scrambles the pixels in the logo any time the logo is saved then the criminal would not be able to use it in their documents.

4.2 Email Phishing

Novelty in this case is also to massively create awareness. RBF doesn't conduct business transactions with the general public and they definitely don't do any transactions via emails therefore a little bit of awareness could prevent people from responding to such unsolicited emails and revealing any personal and financial information on the fake loan documents. In addition, if the executive members details are not freely accessible then maybe criminals couldn't know the user names for the staffs email address and would had not been able to create an authentic looking alternative email.

4.3 Website Defacement

Alternative solutions is to implement basic level security procedure and keep the website and all systems attached to it, even the operating system secure by being updated with the most recent patches. Another solution could be to in the web server make all static content oriented file systems in as read only and store the database that contains the web content within separate demilitarized zones. Using G-Server from Gilian Technologies could also help in preventing such attacks in the sense that it works. It compares the archived digital signatures of original objects with that of each object leaving the Web server. If it matches then the content is sent to the user, else its first restored from backup of the original object and then sent to the user. Moreover, enabling dedicated intrusion detections systems to do auto detection and repair of suspiciously altered content could also be good [18].

4.4 ATM/Credit Card Scam

To detect and prevent future incidents some of the following measures can be taken. One of them is user vigilance when doing financial transactions, be it online sites or ATMs. Online bankers should enable antivirus and anti-malware security checks on the computers or smart phone. They should also check their account activity or balance from another computer if possible or from the ATM and any email or messages stating to be from the bank asking to verify the account should not be replied to [13].

4.5 Cyber Bullying/Harassment

In the above case the threat agent is the 17 year old boy who exploited the immaturity of a child to satisfy his physical desires. One way of preventing this incident in future is if parents enabled a GPS tracking app on their children's mobile

phones which is always connected with their system. When they send their children to school and anytime they go out of range of the normal route then an alert could be created which can help raise the alarm to parents to act quickly.

5 CONCLUSION

Almost half the country's population is active online. It's no wonder that so many are affected by cybercrimes. On one hand technological advancements promises to offer numerous potential benefits to the entire country while on the other hand it is the cause of a vast number of problems, particularly when it comes to information security. Current standards and procedures employed in security mechanism techniques have to be improved. Fiji being a member of the commonwealth could use the legal proceedings of cyber crime cases from other commonwealth countries to serve as precedence when dealing similar cases locally. Public awareness through digital literacy campaigns, not just amongst school students but in villages and communities, also has to be raised to ensure that they do not fall victim of such attacks in future. Together if these areas are strengthened then our society can have better confidence in the benefits offered by the new digital age.

REFERENCES

[1] Internet World Stats.com, " Oceania And South Pacific," Pacific: Internet World Stats.com, 2016. [Online]. Available: http://www.internetworldstats.com/pacific.htm#fj. [Accessed 25 September 2016].

[2] N. Delaibaitiki, "Fijian Firms Lose Thousands Of Dollars Through Cyber Crime," SUNCITY: Fiji Sun Online, 13 December 2015. [Online]. Available: http://fijisun.com.fj/2015/12/13/fijian-firms-lose-thousands-of-dollars-through-cyber-crime/. [Accessed 13 August 2016].

[3] ABC News, "Cyclone Winston: Damage bill reaches $650 million, Fiji Government says," News: ABC.net.au, 26 February 2016. [Online]. Available:http://www.abc.net.au/news/2016-02-26/cyclone-winston-damage-bill-reaches-650-million-dollars/7201846. [Accessed 5 October 2016].

[4] Reserve Bank of Fiji, "RBF Cautions Over Fake Facebook Account Of Governor, Transactions," SUNBIZ: Fiji Sun Online, 19 August 2016. [Online]. Available:http://fijisun.com.fj/2016/08/19/rbf-cautions-over-fake-facebook-account-of-governor-transactions/. [Accessed 22 August 2016].

[5] P. Prakash, "FIU Investigates Fake Facebook Account Cases," Fiji Broadcasting Commission, FBC, 27 August 2016. [Online]. Available: http://www.fbc.com.fj/fiji/43291/fiu-investigates-fake-facebook-account-cases. [Accessed 29 August 2016].

[6] FijiLive, "Woman charged over online scam," Fijilive.com, 25 December 2014. [Online] Available at: http://fijilive.com/fijliive-print-story.Fijilive?60095.Fijilive [Accessed 3 September 2016].

[7] Banff Cyber Technologies, "Best Practices to address the issue of Web Defacement," Articles: Banff Cyber Technologies, 24 March 2016. [Online]. Available: https://www.banffcyber.com/best-practices-to-address-the-issue-of-web-defacement/. [Accessed 18 August 2016].

[8] The OWASP Foundation, "Cross-site Scripting (XSS)", Page: The OWASP Foundation, 4 June 2016. [Online]. Available: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS). [Accessed 18 August 2016].

[9] A. Penjueli, '5 government websites attacked by Kurdish hacker," National: Newswire, 11 March 2016. [Online]. Available: https://www.newswire.com.fj/national/government-websites-attacked-by-kurdish-hacker-restored/. [Accessed August 2016].

[10] M. Rouse, " hacktivism," Definition: Search Security, June 2007. [Online]. Available: http://searchsecurity.techtarget.com/definition/hacktivism. [Accessed 18 August 2016].

[11] E. Dyer, "ISIS seen as growing threat to Canadian peacekeepers in Sinai," Politics: CBC News, 31 March 2016. [Online]. Available: http://www.cbc.ca/news/politics/global-affairs-briefing-peacekeepers-isis-1.3512727. [Accessed 19 August 2016].

[12] R. Valemei, "Scam!," Front page/News: The Fiji Times, 20 February 2016. [Online]. Available: http://www.fijitimes.com/story.aspx?id=342290. [Accessed 18 August 2016].

[13] Consumer Council Of Fiji, "Online bank robbers," Front page/Business: Consumer Council Of Fiji, 26 March 2016. [Online]. Available: http://fijitimes.com/story.aspx?id=347038. [Accessed 18 August 2016].

[14] S. Qalubau, "6 Chinese nationals charged over ATM scam in Fiji," People's Daily Online, 14 December 2015, [Online] Available: http://en.people.cn/n/2015/1214/c90000-8990158.html [Accessed 15 September 2016].

[15] S. Singh, "More charges laid on Chinese nationals in relation to ATM scam," News: FijiVillage.Com, 9 February 2016. [Online]. Available: http://fijivillage.com/news/More-charges-laid-on-Chinese-nationals-in-relation-to-ATM-scam-9sr5k2/. [Accessed 15 Septmber 2016].

[16] N. Swami, " Police caution," Front page/News: The Fiji Times, 2015. [Online]. Available: http://www.fijitimes.com/story.aspx?id=301150. [Accessed 21 August 2016].

[17] Fiji Police Force Media Cell, "Cyber Crime Unit Investigating Facebook Post," News: Fiji Sun online, 27 June 2016. [Online]. Available: http://fijisun.com.fj/2016/06/27/cyber-crime-unit-investigating-facebook-post/. [Accessed 9 August 2016].

[18] R. L. Scheier, "It doesn't take rocket science to prevent Web site defacement," Search Security, October 2003. [Online]. Available: http://searchsecurity.techtarget.com/tip/It-doesnt-take-rocket-science-to-prevent-Web-site-defacement. [Accessed 20 August 2016].