A Review Of Recent Cyber-Attacks In Fiji

Neeraj A. Sharma, Arjun Pillay, Mohammed Farik

Abstract: Computing technology has evolved in such dramatic ways that a child can use such technology and their features. Internet is one such technology which allows peripheral devices to be connected to each other, creating a network to share information. In the same way information can be attacked. In this paper we will be discussing the different types of cyber-attack that recently took place in Fiji. Common attacks discussed in this review paper are phishing, email scams, website defacement, and skimming. Apart from common preventative methods, some novel recommendations have been made. We believe the Fiji experiences and recommendations will assist technology users prepare better against such attacks.

Index Terms: Cyber-attack, Defacement, Phishing, Scams, Skimming, Spam

1 INTRODUCTION

As the internet and technology evolve it is creating more and more vulnerabilities in today's society. Cyber-attack is any kind of hostile move utilized by an individual or entire organization that aims computer information systems, infrastructures, computer networks, and/or personal computer devices by different method for malicious acts more often than not starting from an anonymous source that either takes, modifies, or crushes a predefined focus by hacking into a vulnerable framework [1]. These can be named as a cyber campaign, cyber-warfare or cyber-terrorism in various connections [2]. Cyber-attack can extend from introducing spyware on a computer to endeavors to annihilate the infrastructure of the whole world. A user mostly depends on the internet and technology where they do online shopping, banking and other source of feeding information to the system over the web. This information's can be hacked using cyber-attacking techniques to view data or gain access to the system. When an attack happens it is called a cyber-attack which is one of the biggest problems that majority of organizations face [1]. In this paper, we will talk about the four cyber-attacks that recently took place in Fiji and these four attacks are in categories of phishing, email scams, website defacement, and skimming. This paper also discusses the prevention aspects but not necessarily limited to these four attacks that happened in Fiji, but how to prevent from the majority of cyber-attacks. One of the biggest problems in the cyber-crime area is awareness. Often companies or organizations spend time and money in protecting assets that they think are more vital to the company and it usually turns out that the smallest types of attacks can lead to catastrophic disaster [3]. So, in section 2, we discuss cyber-attacks that happened in Fiji, in section 3, prevention from cyber-attacks, and conclusion in section 4.

2.1 Phishing

Phishing is a type of attack that allows users to click on a malicious link and allows hackers to break into the system. Phishing attacks are carried out through the emails and around 70 percent of emails are spam [3]. Thankfully there are antivirus companies that made approaches to cater for this vulnerability and prevent users and clients from getting exploited. Nevertheless, there are still many emails sent to users and clients email addresses some of which look legitimate and are replicas of existing websites. The only way to know that it's a false website is through its URL and links from the redirecting pages [3]. Phishing is analogues to "fishing" where attacker plants a bait to lure unsuspecting victims of money related scams. This technique is being preferred by online attackers. Emails proclaiming to be from banks or other popular organizations are sent in large amounts. The email requests the recipients to give sensitive data, for example, their username, password, Client ID or PIN through the means for a fraudulent website which to the user looks legitimate [3]. Fig. 1 shows how a phisher targets a website to lure in the victims. Referring to the figure, we can see that the phisher first researches on how to phish for victim, create and deploy a phishing website, then the phisher creates a phishing website that exactly looks like the legitimate website, followed by that the phisher then sends the victim the link of the phishing website through the use of email and as soon as the victim clicks on the link he/she is redirected to the phishing site. The victim enters his/her credentials and the phisher collects that data and uses it to perpetrate the victim's account.

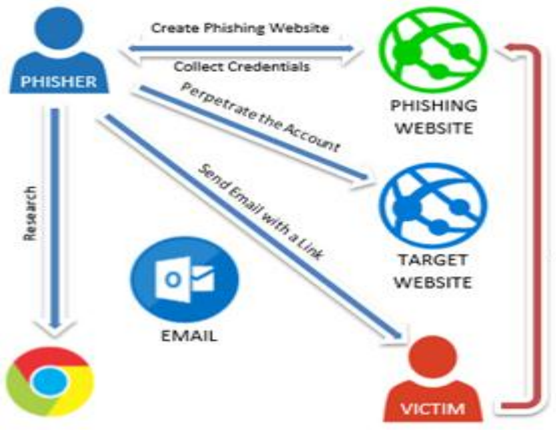
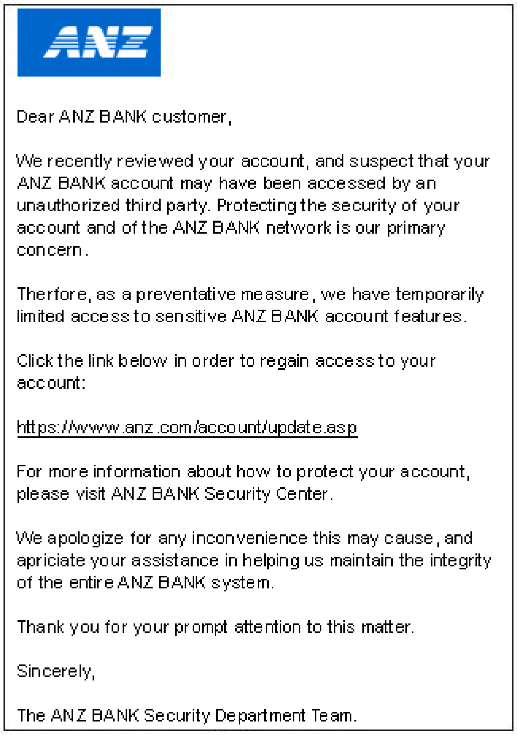


Fig. 1. Phishing Attack

- *Neeraj A. Sharma is currently pursing Master's Degree program in Information Technology at the University of Fiji. Email: neerajs@unifiji.ac.fj*
- *Arjun Pillay is currently pursing Post-Graduate Diploma program in Information Technology at the University of Fiji. Email: arjunp@unifiji.ac.fj*
- *Mohammed Farik is a Lecturer in Information Technology at the University of Fiji. Email: mohammedf@unifiji.ac.fj*

In Fiji, the ANZ bank shows their care for the clients as they demonstrate what sort of email their clients could get and should be cautious and inform the bank regarding these as soon as possible [4]. The bank also informs the clients that in the event that they get these sorts of emails then delete instantly and report to the "ANZ Internet Banking Support Centre". Fig. 2 shows an example of phishing attack that used the credentials of ANZ Bank to attack their banking clients.



Dear ANZ BANK customer,

We recently reviewed your account, and suspect that your ANZ BANK account may have been accessed by an unauthorized third party. Protecting the security of your account and of the ANZ BANK network is our primary concern.

Therfore, as a preventative measure, we have temporarily limited access to sensitive ANZ BANK account features.

Click the link below in order to regain access to your account:

https://www.anz.com/account/update.asp

For more information about how to protect your account, please visit ANZ BANK Security Center.

We apologize for any inconvenience this may cause, and apriciate your assistance in helping us maintain the integrity of the entire ANZ BANK system.

Thank you for your prompt attention to this matter.

Sincerely,

The ANZ BANK Security Department Team.

Fig. 2. *Recipients being attacked using Phishing*

2.2 Email Scams

Email scam occurs when a user enters their personal details into the fake site which looks like an legitimate site for beneficiary use. An email scam is an unsolicited email that claims the prospect of a bargain or something for nothing. Some scam messages ask for business; others invite victims to a website with a detailed likeness to legitimate website. Many individuals have lost their life savings due to this type of fraud. Email scams are also known as email fraud. Various Web clients have gotten messages proclaiming to be from money related establishments or other trustworthy organizations. A few messages advise the recipients that their card number and passwords should be rewritten by signing into a legitimate looking, yet fake website [3]. The motivation behind these sites is to acquire your logon credentials, for example, your own Personal Identification Number (PIN), Client ID, and card number to your internet accounts. Other attackers may convey messages that will request clients or users to download the file(s). Fig. 3 shows how an email scam is carried out. The sender first composes a message using an email client and the senders email client uploads message to SMTP server. SMTP server uses DNS server to locate recipient's domain, the message traverses the internet and probably passing through several routers. A message arrives at receiving server and is placed in recipient's mailbox file or folder. The recipients email client checks mailbox and downloads message for the recipient than finally, the recipient reads the message using the email client.

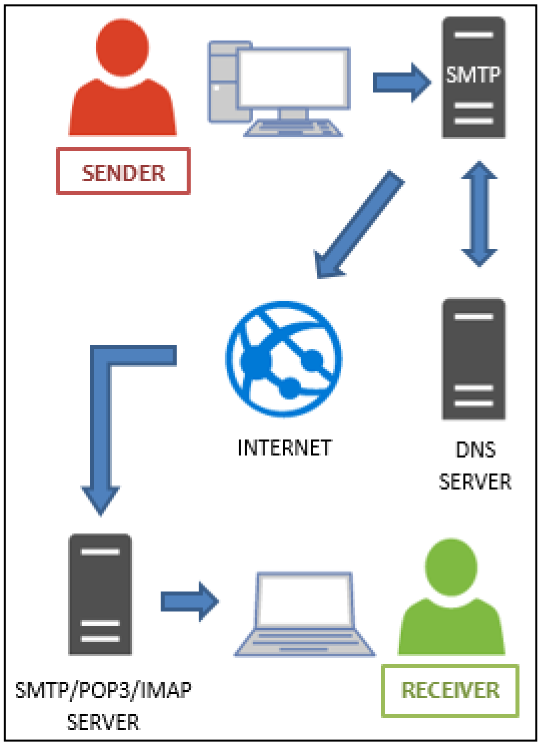
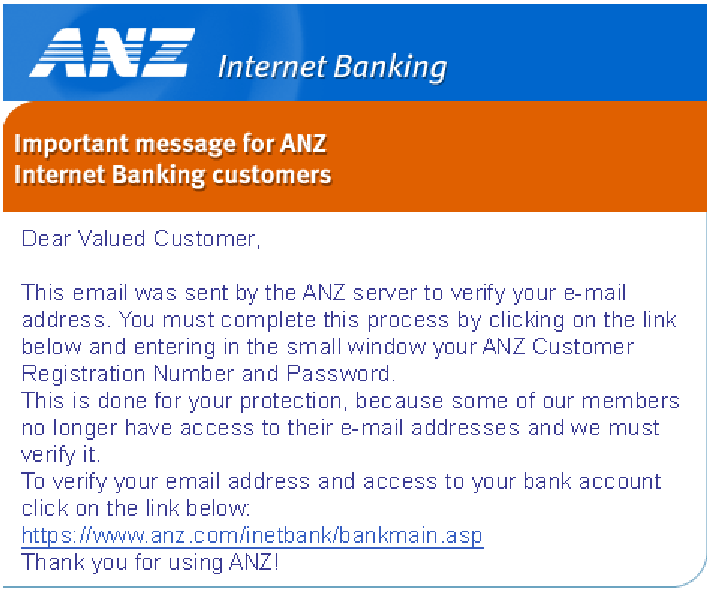


Fig. 3. *Email Scams*

Referring to an attack that happened in Fiji [4], Fig. 4 shows an example of an email scam that used the organization's details such as company logo to email recipients.



Important message for ANZ Internet Banking customers

Dear Valued Customer,

This email was sent by the ANZ server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your ANZ Customer Registration Number and Password.
This is done for your protection, because some of our members no longer have access to their e-mail addresses and we must verify it.
To verify your email address and access to your bank account click on the link below:
https://www.anz.com/inetbank/bankmain.asp
Thank you for using ANZ!

Fig. 4. *Email Scan using ANZ Bank Fiji brand and logo.*

Some common other types of email scams include – Advance-fee fraud, El Gordo de la Primitiva Lottery International Promotions Programmes, FBI email, Hitman, Investment Schemes, Online dating scam, Phishing, Romance scam, Translation/Marriage Agency scam, Secret Shopper, Traffic ticket spam, Word of Mouth, and Job Scams [2].

2.3 Website Defacement

Website defacement is an attack where the hacker replaces the original website with one of his own. Web defacement is one of the biggest security concerns of any organization that hosts a website. Web defacement is often carried out by programmers who break into web servers and replace the original site that either replaces the content of home page or redirects the webpage to another illegal website. Attackers can also plant one of their own pages to exploit threats such as phishing, code infusion, cross web page scripting and so on. These programmers mainly focus defacement on religious websites, government websites, bank websites and corporate websites [3]. Fig. 5 shows how an attacker targets clients through the use of website defacement. In this particular scenario, the perpetrator attacks the web server and replaces the current website with their own website which looks identical to the main website. When the client accesses the fake website then he/she gets vulnerable to phishing, code fusion, cross web page scripting and so on.

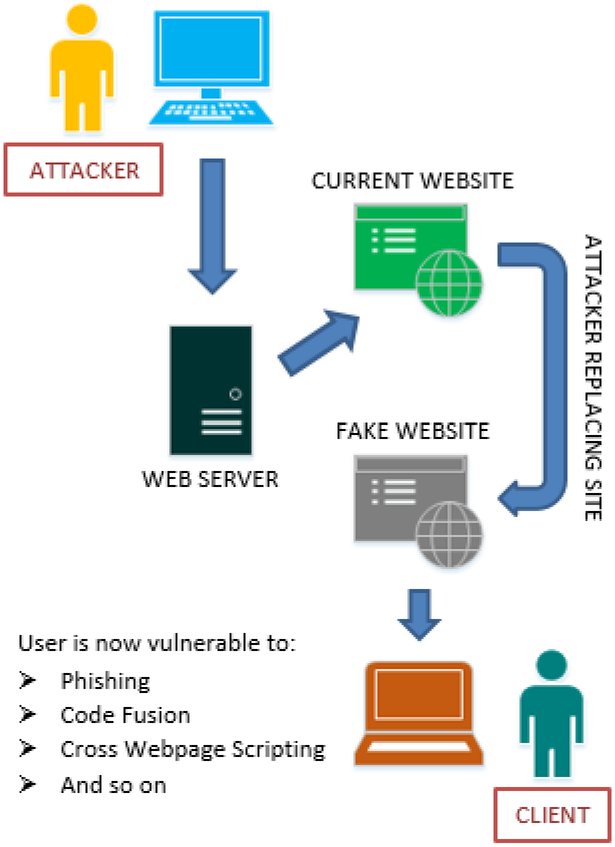
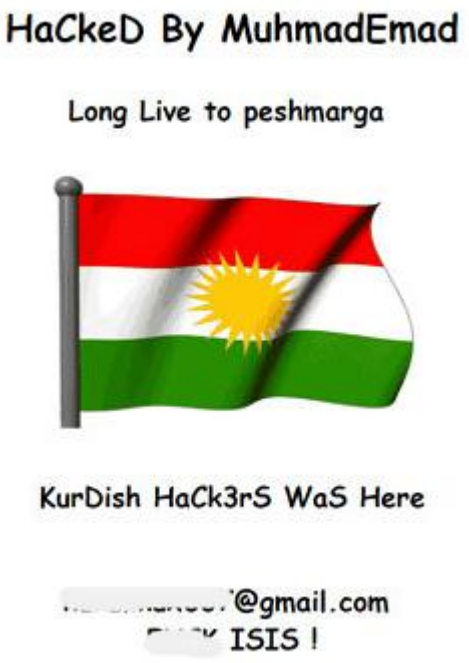


Fig. 5. *Website Defacement*

Recently the Fiji Police, Royal Fiji Military Force, and Immigration Fiji websites were attacked [5]. These attacks were done by "MuhmadEmad" a Kurdish hacker. The hacker uploaded a picture of the Kurdish banner along with the words stating, "KurDish Programmers WaS Here" and "HaCKeD by MuhmadEmad, Long Live to peshmarga" as shown in fig. 6. This was a reference to the Kurdish armed force of Peshmerga, a hostile to Islamic State power situated in Iraq.



HaCkeD By MuhmadEmad

Long Live to peshmarga

KurDish HaCk3rS WaS Here

[redacted]@gmail.com
[redacted] ISIS !

Fig. 6. *Client being attacked through Website Defacement*

The image replaced the homepage of the Royal Fiji Military Force, Fiji Police, and Immigration websites and there was no evidence into suggesting how the websites were hacked. It is said that "MuhmadEmad" has hacked numerous U.S and Turkey Government websites over the past two years.

2.4 Skimming

Skimming attack is where the attacker places a card skimming device which captures the PIN code of the user and also reads the electronic stripes at the back of the card. Skimming is referred to as a crime where the attacker gets hold of private information of a client through the use of their credit cards. The attacker can get hold of the private information in two circumstances, one is by photocopying the client's receipt and getting hold of the private information, this is considered a very basic level of skimming [3], [6]. The second scenario is where the attacker uses a device called the skimmer. These are considered a more advanced level of skimming method where the attackers implement the skimming device over the card slot of an ATM. This will read the cards magnetic strip without the user knowing that the card is going through a skimmer first. These devices usually are connected with a second device that is the camera and it records the users they enter the PIN numbers. If the perpetrators are not using the cameras and there is another method to capture PIN numbers, that is through having a second keypad directly on top of the current keypads. What is does is it will register all the keys pressed by the users and it is in the form where the users won't be able to differentiate whether there is any second keypad or not. All these devices installed in the ATM's are illegal are known as a skimmer. Fig. 7 shows how skimming devices are placed in an ATM machine.

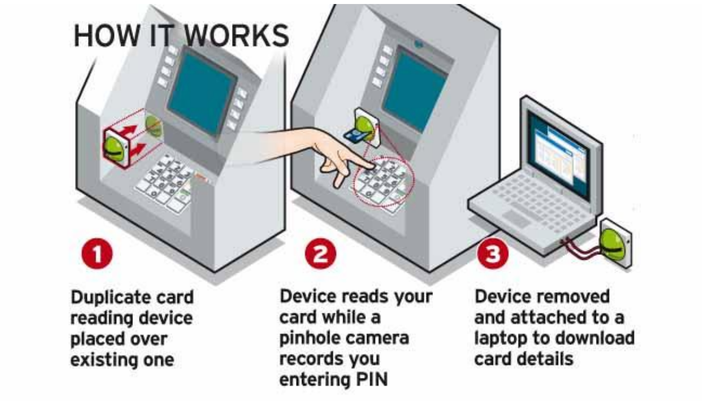

HOW IT WORKS
1
Duplicate card reading device placed over existing one
2
Device reads your card while a pinhole camera records you entering PIN
3
Device removed and attached to a laptop to download card details

Fig. 7. *Skimming Attack*

In Fiji, a card skimming attack has occurred near "Smuggler's Cove BSP ATM" in Wailoaloa, Nadi. The attack has transpired by placing a card skimming device in the original BSP card reader [7]. Fig. 8 shows the images of the original and Skimmer device installed.

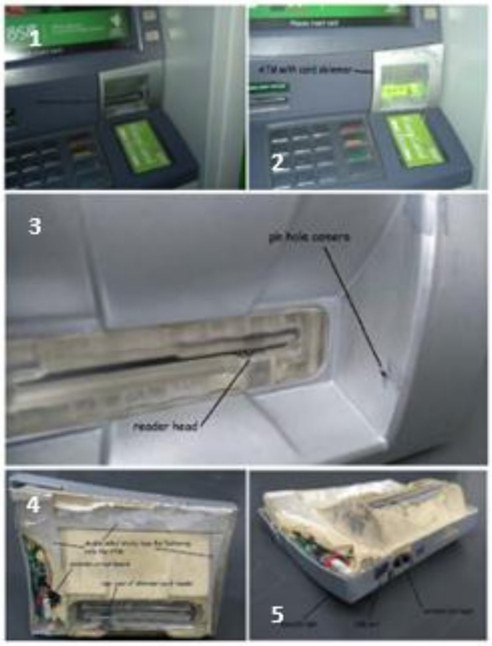


Fig. 8. *Cyber-attack through the use of Skimming device.*

3 Preventative Recommendations

This section discusses some existing and novel approaches to prevent cyber-attacks such as those that occurred in Fiji and also discusses on how these attacks actually take place at the first place. This will surely limit the chances of a user being cyber-attacked in the same way again.

3.1 Phishing

There are two ways of preventing getting attacked through phishing and those are firstly by getting educated involving these types of attacks especially knowing which emails to open and which emails not to open [3]. Secondly, is by having anti-phishing tools installed in your computers that are added to the web browsers so as soon as the users and clients mistakenly open the email link, these anti-phishing tools will block that link [3]. Other solutions for treating this sort of emails are, treating all emails asking for login data, for example, username, password as a threat. Real ANZ Bank emails won't ask for individual subtle elements or log on data, users should directly remove these sorts of email without clicking on any attachment or links, regardless of how innocent or provocative the email subject header sounds.

3.2 Email Scams

On the off chance that the email is from an ambiguous source, or on the other hand you are suspicious of the way the email reads and sounds, delete it straight away. Do not open any links or attachments that came with the email. A good practice is – if you want to access the bank's internet banking page, simply type the address of it on the web browser itself in this instance you could type https://www.anz.com. The following recommendation will prevent users and organizations from threats against email scams, first, filter spams, there are options in the email clients that allow users to turn on the filtering option, having done this it will detect unsolicited, unwanted emails from getting into the user's inbox. Second, don't trust unsolicited email, these emails might look genuine and realistic but at the backend, its main purpose might be something else, for example online banking websites [8]. Third, treat email attachments with caution, while some email client filter or detect emails as spams or virus but others don't, so it is always good to have your system up-to-date with antivirus and download attachments which you think are genuine. Fourth, don't click links in email messages, it is accustoming that nowadays people attempt to target users or clients through this means; it is not a good idea to directly click on a link without knowing who it is from. Usually, these types of links contain threats. Fifth, install antivirus software to keep up to date with all the current threats. Sixth, it is always a good idea to install personal firewalls and keep it up to date to prevent perpetrators from targeting you. Seventh, configure your email client for security in terms of filtering emails and blocking unsolicited emails [8]. Following the above seven methods will keep users safe from email scams.

3.3 Website Defacement

Website defacement is considered one of the biggest security threats to any business or organization that is online. Here are five ways you can protect your business or organization from website defacement [9]. First, security audits and penetration testing, doing a regular audit and penetration testing will help the organization in terms of evaluating all the security aspects of the IT infrastructure. These can be limited to operating systems, service and applications flaws, risky end-user behavior, and improper configurations. Second, defend against SQL injection attacks, SQL injection attacks works in a way that uses SQL statements inserted into data entry fields. An example of an SQL query where the users enter email which can lead to SQL injection attack is:

```
$result = $mysqli->query('SELECT email, userid FROM
members WHERE email = "'.$email.'"')';
```

You can avoid writing this type of queries and use bound variables with prepared statement methods as follows:

```
$stmt = $mysqli->prepare("SELECT email, userid FROM
members WHERE email = ?;");
```

```
$stmt->bind_param("s", $email);
$stmt->execute();
```

This method works because the parameter values are combined with the compiled statement and not an SQL string. Technically, the best methods of preventing SQL injection is to generally avoid the use of dynamically generated SQL in the source codes. It is also a good practice to validate inputs such as: limiting input only to accepted characters, whitelisting, and length checks. Third, defend against cross-site scripting (XSS) attacks, by using web application firewalls (WAF). WAF is able to check for malicious input values, modification of read-only parameters, filter out malicious output and block suspect requests. Fourth, is the use of defacement monitoring and detection software tools. The best website monitoring and detection tools to counter defacing are WebOrion Defacement Monitor, Site24x7, and Nagios. Fifth, prepare to respond to defacement incidents. To be more secure, the web server which had been attacked needs to be taken offline to prevent the attacker from getting more inside of the system. There should also be a technical response team available for when this type of issues arises. If the organization is familiar with all the above five methods, then there is a greater chance that a company can save itself from website defacement attack [9].

3.4 Skimming

Chuck Somers, VP for ATM security and systems outlines some of the important things users can look out for to prevent skimming attacks [10]. These include, first, keeping your eyes open when trying to use the ATM and look out of something that doesn't fit right in the ATM whether it be involving the keypad or the card slot area. Second, cover the keys during typing in the ATM. Third, pay close attention to your accounts for unfamiliar transactions regardless of how small these transactions are. Fourth, it is recommended that you use a credit card rather than your debit card. Credit cards have certain credit limit and the money belongs to the bank and it will be easy to retrieve as well, also your money will be safe. Fifth, don't assume that all ATM's are same, meaning the ATM itself could be a fake if you are a tourist in another country it is recommended that you use the ATM's that are inside the bank. Sixth, trust you're instinctive, if you feel something doesn't feel right, it is recommended that you move away from there and advise the bank regarding that. Seventh, be on the lookout for potential thieves, some skimmers use a combination of high and low tech by having thieves on site as well. When the card gets rejected in the ATM the thief will portray as a customer or user to try and help you in that process gaining the PIN number. Eighth, when in doubt don't use the ATM [10]. If the society is aware of these eight scenarios, then skimming itself will diminish.

3.5 Other ways to Prevent from Cyber-attacks

You may definitely realize that there are no 100% full proof techniques to counter cybercrime and cyber-attacks, yet at the same time, you need to protect your computers. The essential things to do are to utilize or use a good security software, that scans for virus, as well as searches for various sorts of malware, including however not constrained to ransomware, and prevents it from entering the PC [11]. For the most part, these malicious codes are infused into your PCs by going to or downloading things from non-reputed websites, drive-by downloads, the trade-off sites that present malicious advertisings otherwise called Malvertising [11]. Alongside the antivirus, you should use a decent firewall. While the built-in firewall in Windows 8 and Windows 7 is great, you can utilize other firewalls that you feel are robust than the default Windows Firewall [11]. In the event that it is a corporate PC system, ensure there is no Plug and Play support in any of the client PCs. That is, representatives ought not to have the capacity to connect to Flash drives or their own Internet dongles into the USB. The IT department of the organization should keep a watch on all the system usage. Utilizing a decent system activity analyzer encourages in brief participation to unusual practices emerging out of any terminal (representative PC). For security against DDoS attacks, the site is better moderated to various servers, rather than being facilitated essentially on a solitary server. The best strategy would be to have a mirror always up utilizing a cloud administration [11], [12]. That will extraordinarily diminish the odds of a DDoS being fruitful – not for quite a while at any rate. Utilize a decent firewall like Sucuri and find a way to ensure and secure your site. Establish a strong password [13], putting a strong firewall this ensures your system by controlling web activity coming into and streaming out of the business, install antivirus protection (this will protect from virus like Trojan horse and malware attacks) and lastly update the program regularly (means patching and updating the system so that the hackers won't find any loopholes in the system) [12].

4 Conclusion

In this paper, we have looked into the four types of cyber-attacks that took place in Fiji. These were phishing, email scams, website defacement and skimming. The cyber-attacks which we have mentioned can be stopped, by the solutions which we have listed and discussed in this paper. Nevertheless, this paper will instruct users regarding the common attacks that occur and the novel solutions that can keep them safe and also protect them from being hacked.

Reference

[1] Techopedia.com. "What is a Cyberattack? - Definition from Techopedia.," 31 Aug., 2016; https://www.techopedia.com/definition/24748/cyberattack

[2] Wikipedia. "Cyber-attack," 31 Aug., 2016; https://en.wikipedia.org/wiki/Cyber-attack.

[3] R. Grimes. "The 5 cyber-attacks you're most likely to face. ," 11 Aug, 2016; http://www.infoworld.com/article/2616316/security/the-5-cyber-attacks-you-re-most-likely-to-face.html

[4] Anz.com. "Security alerts & reporting fraud | ANZ.," 31 Aug., 2016; http://www.anz.com/personal/ways-bank/security/online-security/alerts-reporting-fraud/

[5] C. Limited. "Fijivillage | Fiji's Latest News and Sports website.," 31 Aug., 2016; http://fijivillage.com/news/Fiji-Police-RFMF-and-Immigration-Fiji-websites-hacked-s9r52k

[6] About-threats.trendmicro.com. "Gateways to Infection: Exploiting Software Vulnerabilities | Trend Micro

Threat Encyclopedia," 11 Aug., 2016; http://about-threats.trendmicro.com/RelatedThreats.aspx?language=tw&name=Gateways+to+Infection%3A+Exploiting+Software+Vulnerabilities.

[7] F. Times, “Skimming in Smuggler's Cove BSP ATM,” *Fiji Times*, 2015.

[8] US-CERT. "Recognizing and Avoiding Email Scams," 26th Oct., 2016; https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf.

[9] BanffCyber.com. "Best Practices to address the issue of Web Defacement," 26 Oct., 2016; https://www.banffcyber.com/best-practices-to-address-the-issue-of-web-defacement/.

[10] L. Heet. "Ways to protect against ATM skimming," 26th Oct., 2016; http://www.creditcards.com/credit-card-news/8-ways-protect-against-atm-skimming-1282.php.

[11] A. Khanse. "Cyber Attacks - Definition, Types, Prevention.," 25 Aug, 2016; http://www.thewindowsclub.com/cyber-attacks-definition-types-prevention.

[12] S. Leach. "Four ways to defend against DDoS attacks. ," 31 Aug., 2016; http://www.networkworld.com/article/2170051/tech-primers/tech-primers-four-ways-to-defend-against-ddos-attacks.html

[13] M. Farik, and S. Ali, “Analysis Of Default Passwords In Routers Against Brute-Force Attack,” *International Journal of Scientific & Technology Research,* vol. 4, no. 09, pp. 341-345, 2015.