International Journal of Reviews, Surveys and Research (IJRSR)

International Refereed and Indexed Journal for Research Scholars and Practitioners

CYBER SCAMS IN SOCIAL MEDIA AND THEIR PREVENTION TECHNIQUES

Dr. Ram Shukla, Faculty (Operations Area),

Indian Institute of Management – Rohtak (IIM Rohtak), M D University Campus,

Rohtak, Haryana. INDIA.

Abstract **-** The purpose of this paper is to highlight sorts of cyber scams are mostly prevalent on the internet those are affecting the public nowadays and what steps should we take in order to prevent the impact of such scams. The paper proposes a new methodology developed by surveying by which such scams can be avoided and the impostors can be tracked keeping the public safe.

Keywords – Social Media, Cyber Scams, Cyber police

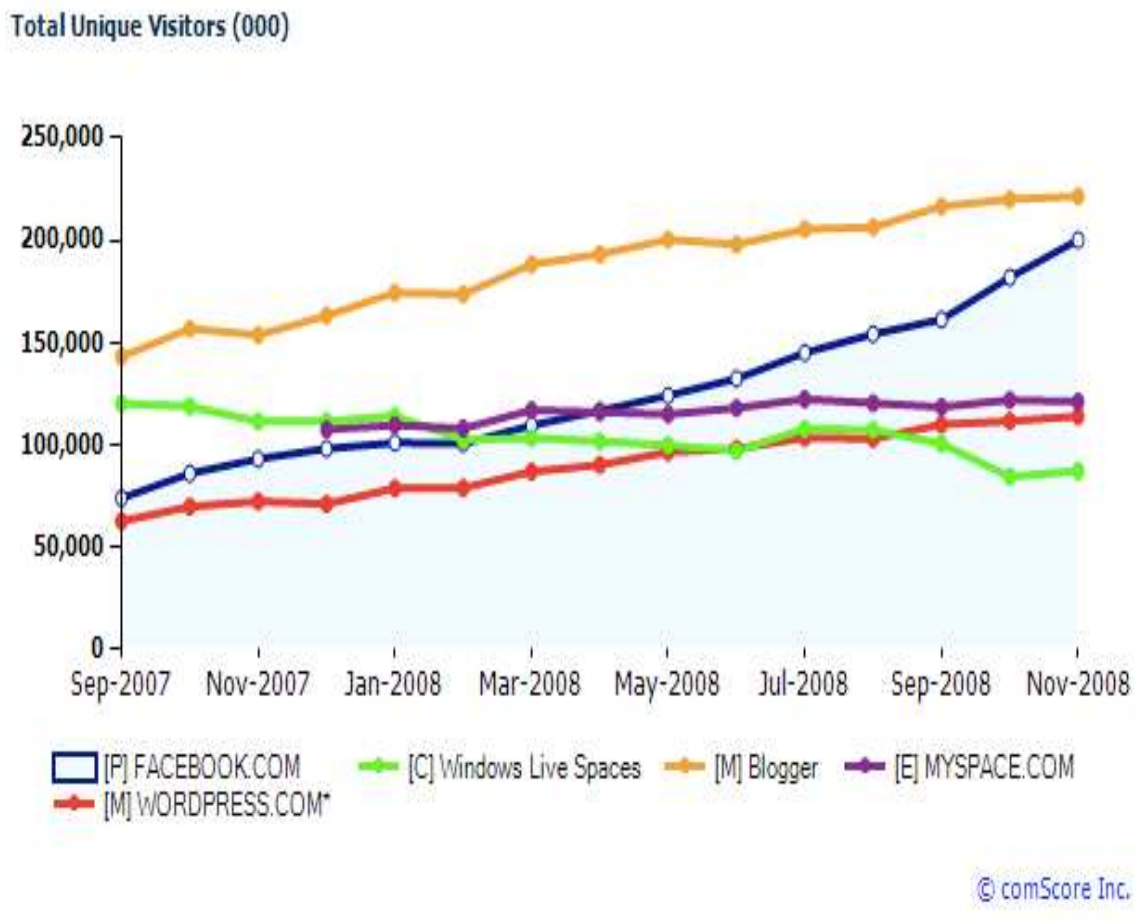
1. INTRODUCTION

The latest way of communication goes against the tide of contemporary marketing strategies, with the emerging new definition of communication, the SOCIAL MEDIA. Many companies have moved on from the traditional marketing fundamentals with the penetration of new bottom-up, democratized system.

The invention of the computers has opened new avenues for the fraudsters. It is an evil having its origin in the growing dependence on computers in modern life. Though there is a great talk about the cyber-crimes there is nothing called cyber-crime. The crimes such as frauds, forgery

are traditional and are covered by the separate statutes such as Indian Penal Code or alike. However the abuse of computer and the related electronic media has given birth to a gamut of new types of crimes which has some peculiar features [4].

A simple yet sturdy definition of these crimes would be “unlawful acts wherein the equipment transforming the information be it a computer or a mobile is either a tool or a target or both”. In India the information Technology Act deals with the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers.



The sudden emergence of social media in the public realm as suggested in the above figure and the realisation of a powerful and coordinated online consumer-force have raised alarms in corporate offices all over. As consumers increasingly influence each other and share opinionated views on brands and products on the internet, businesses are compelled to rethink

and reorganise marketing and communication strategies in order to address this 'threat' to traditional ways of doing business [5]. Social media is currently an evolving 'phenomena' in business marketing. Enlightened marketers are beginning to drive the use of social media as a component in their marketing strategy and campaigns to reach out to customers and fans. Among the sub-disciplines of marketing that may utilize social media include promotions, marketing intelligence, sentiments research, public relations, marketing communications and product and customer management of sub tasks are interlinked [4].

2. MAJOR TYPES OF SOCIAL MEDIA SCAMS

There are many sorts of ways cyber scams trap the public. The increasing demand for internet can be attributed to the growing need to integrate disparate applications, people, processes, and information. In addition to having many uses, it has many disadvantages too. Many scams are prevalent on the internet nowadays but the majority chunk of them can be classified into some categories as below[2].

CELEBRITY SCAMS: While social networking can definitely help you to enhance your online visibility, at the same time it can land you into trouble if your profile is hacked by someone or someone creates a fake profile in your name. In fact this is a trend that is increasingly common. There are many a celebrities whose names have been used to create fake profiles. What is surprising is that in most cases the social media sites are silent in this regard. So what could be the solution for this? Well the answer is simple – one needs to book the social media profile earlier than the scammer. Once the profile is booked in your name you would be safe [2].

DIRECT EMAIL SCAMS: First of all if someone, pretending to represent a company or organization, contact you by e-mail to supply them with usernames, passwords or other critical information by e-mail, then you can be certain it is fraudulent. Today we have something we call SSL (Secure Socket Layer). E-mail is one of the most un-secure methods to send user information and passwords. Most organizations have secure servers, which apply SSL technology to keep your personal information safe. Now that if we receive e-mails with a link to a secure server then it is safe. Well it is wrong. Most banks, financial institutions, or almost any legitimate organization never request updates to personal information via e-mail. You will most certainly never receive e-mail from your bank to update your account details by clicking on a SSL link embedded into the e-mail [1].

FAKE HOAX ABOUT CELEBRITIES: Typically, malicious Facebook and Twitter messages relating to celebrity news contain links that claim to have "secret" information. In the case of Jackson, Cluley said he has heard some of the lures include promises of songs by the King of Pop that have never been heard before or new details and pictures of Jackson's death. However, the link to the information then typically prompts the user to download an update of Adobe Flash. Of course, instead of an update, users end up with a bot Trojan or other piece of malware installed secretly on their computer [2].

DIRECT SCAMS: On Facebook, for example, members might receive a message in their inbox, or a message on their wall, that directs them to another site which looks identical to the Facebook log-in page. Just last week, Twitter users recently began receiving tweets that asked "OMG! Is it true what they said about you in this blog?" The link directed the user to a screen that looked just like the Twitter log-in page, but was instead a phishing site. Of course, once you've entered your user name and password into one of these fake sites, the criminals engineering the con have easy access to your account [2].

APPLICATION ORIENTED SCAMS:

Facebook members who recently decided to use an application that offered an IQ test were unpleasantly surprised to learn they had unwittingly also subscribed to a text messaging service that cost approximately $30 a month. The terms of the service were in fine print that many claimed was nearly impossible to notice [2].

MOST DANGEROUS SCAMS

SOCIAL NETWORK MISSPELLING SCAM

During December 2010, it was discovered that misspellings of a social network site being used as a social engineering ploy. Misspelling the domain name of this site would redirect users to websites coded to look similar to the actual website. The website users were redirected to answer three or four simple survey questions. Upon answering those questions, users were offered a choice of three free gifts. Multiple brands were observed as being offered as gifts, including gift cards to retail stores and various brands of laptops.

After clicking on one of the gifts, users were further redirected to other websites claiming to give free gifts for completing surveys. The surveys typically asked for name, address, phone number, and e-mail address. A user could spend hours filling out multiple surveys and never receive any of the gifts advertised [1].

FAKE ONLINE RECEIPT GENERATOR TARGETS UNSUSPECTING ONLINE MARKETPLACE MERCHANT

A new scam aims to swindle online marketplace sellers by generating fake receipts. This Receipt Generator is an executable file that has been circulating on hacking forums recently. This is a particularly interesting scam - because it does not target regular PC users, it targets the sellers on online marketplace websites. This is what the would-be social engineer sees when running the program:

The social engineer can fill in a variety of information, including item name, price, and the date the order was taken. Additionally, it allows them to choose between the .com, .co.uk, .fr, and .ca marketplace portals. When they hit "Generate," an HTML file is created in the program folder which looks like this:

The program produces what appears to be a genuine marketplace receipt and a copy of the "Printable Order Summary," similar to the documents resulting from legitimate marketplace purchases. Note the small details, such as "Total before tax," "Sales tax," and other particulars that make the receipt convincing.

Many sellers on these markets will ask the buyer to send them a copy of the receipt should the buyer run into trouble, have orders go missing, lose the license key for a piece of software, and so on. The scammer relies on the seller to accept the printout at face value without checking the details. After all, how many sellers would be aware someone went to the trouble of creating a fake receipt generator?

Sellers must remain ever vigilant about this scam, which has been a popular topic in recent hacker forums. The VirusTotal detection rate is currently 1/43 – detected as Hacktool.Win32.Amagen.A [1].

MALICIOUS CODE IN .GOV E-MAIL

A recent malware campaign, disguised as a holiday greeting from the White House, targeted government employees. The recipient received the below e-mail with links to what masqueraded as a greeting card, but when they clicked on the link, it attempted to download a file named "card.exe." The executable program proved to be an information-stealing Trojan, which would disable the recipient's computer security notifications, software updates, and firewall settings. The malware also installed itself into the computer's registry, enabling the code to be executed every time the computer was rebooted. At the time of review, this particular malicious code sample had a low antivirus detection rate of 20%, with only 9 out of 43 antivirus companies reporting detection [1].

3. STATISTICS WITH SOME EXAMPLES ON SUCH SCAMS

Cybercrime statistics are up 33.1% over the previous year. The average person lost $931.00, but some lost thousands and others were wiped out financially. E-mail (74.0%) and web pages (28.9%) were the two primary mechanisms by which the fraudulent contact took place[3].

This is actually in accordance to the increasing use of social media and networking sites in public. Victims included males and females ranging in age from teens to seniors.

Among the top-reported scams were: Check Fraud, Confidence Fraud, E-Mail Fraud, Computer Fraud

Non-delivery, Auction Fraud, Credit/Debit Card Fraud, cyber pornography and Work at Home Scams.

While some scammers work alone, a growing number are part of organized crime rings operating out of Asia, Europe and the former Soviet Union.

4. METHODOLOGY OF PREVENTION

The methodology of prevention mainly involves FBI and the cyber police in the process. Firstly, a major role depends on the CLIENT or the user who is most prone to all such scams. The best method as they say is to always avoid in believing such news. But if the case is more important

there is a simple but an effective methodology that can be implemented to put a check to such traps or rather to prevent users from falling into such traps.

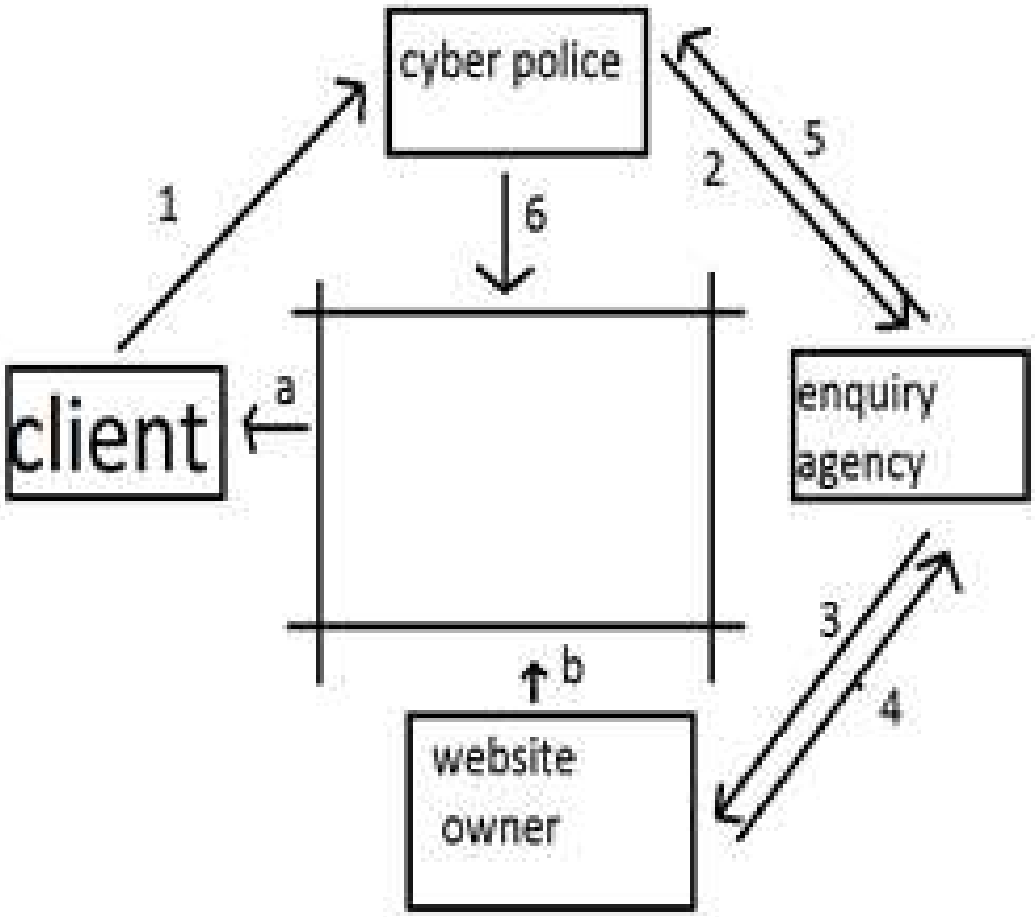
PRIMARY REQUIREMENTS

It is the combined duty of the public and the cyber police in this process. To implement this process there is a requirement of an agency like an ENQUIRY AGENCY that can aid cyber police in running an enquiry that might eventually aid the public in resisting such crimes. In order to put a check to them the public need the following

- An online portal for lodging complaint
- An online database that uploads fraud sites
- A portal to call for identity protection
- A portal to keep a check on identity theft
- An enquiry agency that aids cyber police in enquiring about such fraud sites
- A team with well-equipped knowledge about such crimes
- A team of trackers who can hunt down the source of such websites

IMPLEMENTATION

The implementation involves a simple procedure that is shown in the figure given below. As denoted in the figure below “a” is the process in which the user gets the first look of such website or a suspicion of such scam. Then the CLIENT as suggest in the process “1”, must report the site or the scam to the cyber police who after receiving through the suggested portal. Then the cyber police after receiving such a complaint shall launch an enquiry with the ENQUIRY AGENCY which starts its works through the above suggested intelligence team and tracker team and finally find out through the process “3”the legibility of such a website. Then the agency reports back to the cyber police through process “5” whether the followed up site or blog or any such source is actually trust worthy or not. It investigates in different strategic directions “4” in a controlled way by reducing the risk of implementing projects or change processes.



Then the cyber police finally inform the company or the client whether to trust the suggested site or not and then update on their open database through the process “6”. If the site is not a legitimate one then they launch a case against it and proceed legally and the final decision of the access to their blog or site “b” whether to be continued or not depends on the followed process.

5. CONCLUSION

The above stated is just a list of known frauds in the cyber world where most of them are unknown or untraced yet and they might be yet far ahead as the lawbreakers are always a step ahead of lawmakers.

Even the above suggested solution for the prevention is also just one among many and research is still going on, on this issue regarding the prevention of such activities on the internet. But as already suggested, most of it lies in the hands of public to prevent scams.

REFERENCES

1. Hacktool.Win32.Amagen.A , Internet Crime Complaint Center Reports from the IC3 journals 2009.

2. Dr. R.J.Sabale, Frauds in India – Harmful Matter, Indian Streams Research Journal, Vol.1, Issue 1, Feb 2011 pg. 128-130.

3. Meredith Wadman, Nature 444, 658-659 (7 December 2006) | doi:10.1038/444658a; December 2006.

4. Catherine C. Marshall and Frank M. Shipman, Proceedings of CHI, May 2011