International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Profile Impostoring: A Use Case on the Rising Social Engineering Attack on Facebook Users

Cephas Mawere[1], Thabiso Peter Mpofu[2]

[1]M.Tech. Student, Department of Bioinformatics, School of IT, Jawaharlal Nehru Technological University Hyderabad, India

[2]M.Tech. Student, Department of Computer Science, School of IT, Jawaharlal Nehru Technological University Hyderabad, India

Abstract: ***Social engineering attacks have taken a new twist as a growing number of people use online social networking sites to foster social relationships among each other and market products. Of interest is Facebook whose users have exponentially increased; some of these users are prominent individuals with high influence in various communities like celebrities, philanthropists, religious ministers and non- profit organizations. Data retrieval from Facebook profiles is thus becoming a major tool for business which has led to most unsuspecting users being victims of deception. Profile impostoring, also known as identity theft, is increasingly on the rise and becoming an underlying threat to information security. The cyber perpetrators are creating fake Facebook profiles of prominent individuals who have a large following. Ordinary individuals are also not at their mercy. With such high pending risk of identity theft there is need to develop methods that help Facebook fans to automatically detect deception, identify imposters and get them arrested.***

Keywords: Social engineering, social networking, profile impostoring, identity theft, information security, cyber perpetrators

1. Introduction

Social engineering (as used by the military or law-enforcement) is the emerging technique for obtaining classified information by interacting and deceiving people who can access that information [3]. Rather than using traditional techniques of attacking the technical shields such as firewalls, many sophisticated computer hackers find that social engineering is more effective and difficult to detect by humans. In the domain of information security, social engineering can get into information system by using people's weakness, just not using the computer's leak [4]. The weakest link in an information-security chain is often the user because people can be manipulated. Social engineering attacks can be complex with multiple ploys and targets [2]. For example, the use of real/fake organization's uniform is frequent everywhere in the world. If anyone can verify the uniformed person in front of him/her quickly, they can escape the damage from above fraud [5].

Social engineering attacks have taken a new twist as a growing number of people use online social networking sites to foster social relationships among each other [1]. Of interest is the ever widening network Facebook, whose following is attributed to the strong growth from emerging markets such as India and Brazil. For example, In India its user base rose by 50 percent to 78 million as of March 31, 2013 compared to the same period in 2012 [8]. Data retrieval from Facebook profiles has thus become a major tool for business which has led to most unsuspecting users being victims of deception [6]. Profile impostoring, also known as identity theft, is increasingly on the rise and becoming an underlying threat to information security. The cyber perpetrators are now creating copy facebook profiles of individuals ranking from ordinary users to brands and prominent accounts who have a large following like philanthropists and religious ministers.

2. Trends in Facebook Impostoring

As of September 30, 2013, it is estimated that 143.3 million accounts (which doubled in less than six months of the same year) on the popular social networking site Facebook may be false or duplicate, with a major chunk of them coming from developing markets like India and Turkey [7], [15]. Facebook revealed that such accounts were duplicates, misclassified or undesirable [10]. A user-misclassified account is one where users create personal profiles for a business, organization or non-human entity such as a pet. As per Facebook guidelines such entities are permitted using a page rather than a personal profile.

Undesirable accounts, which represent user profiles that Facebook determines, are intended to be used for purposes that violate its terms of service like spamming. It is unfortunate that people have not only been creating accounts for their pet rabbits, but also for imaginary friends and other fictional characters for years.

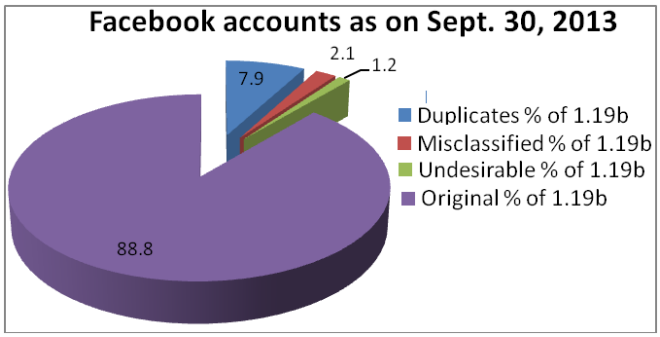

Figure 1: Statistics of Facebook accounts as at Sept. 30, 2013

Facebook, which globally witnessed 1.19 billion monthly active users (MAUs) , an 18% increase on year-over-year (YOY), in a US Securities and Exchange Commission (SEC) filing the SEC filing for the quarter which ended on September 30, 2013 said it estimates up to 7.9 per cent accounts being duplicate, and up to 2.1 per cent and up to

1.2 per cent accounts being user-misclassified and un-desirable, respectively (Figure 1) [7], [23].

Now, MAUs are registered Facebook users who log in and visit the site through the website or a mobile device or take an action to share content or activity with Facebook friends or connections via a third-party website that is integrated with Facebook in the last 30 days as of the date of measurement.

According to the economic times dated 1 November 2013, the filing said Facebook estimated that duplicate accounts (an account that a user maintains in addition to his or her principal account) may have represented between approximately 4.3-7.9 per cent of its worldwide MAUs during the nine months ended September 30, 2013. Accordingly, user-misclassified accounts represented between approximately 0.8-2.1 per cent while undesirable accounts represented between approximately 0.4-1.2 per cent of its worldwide MAUs [7]. This is a significant increase when respectively compared to 5.0 percent, 1.3 percent and 0.9 percent approximations as of December 31, 2012 [15].

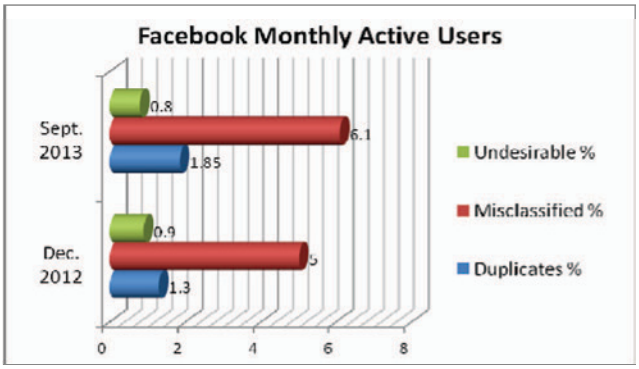

Figure 2 Average MAUs for fake accounts represented between Dec. 31, 2012 and Sept. 30, 2013respectively

Though Facebook had 728 million Daily Active Users (DAUs) for the quarter which is a 25% increase on year-over-year (YOY), fake or duplicates accounts has been a known issue [23]. Fake profiles are generally created by automated programs that then go and 'like' pages at random. It is quite unbelievable that one can now buy fake Facebook accounts that come pre-populated with "fake" friends and photos.

According to one study the average cost for a fake Facebook account is just fifteen (15) dollars. Compared to fake email accounts, this cost is extremely high. Notwithstanding, to a determined fraudster who stands to make thousands or even millions of dollars from fraud, this is a very small cost [12]. These paid services are rampant and India is no exception. With such cases on the rise a new law in California was set in place in July 2011 as a means to prohibit impersonating another individual online for the purposes of harming, intimidating, threatening, or defrauding a person [11]. However, for the first time Facebook has accepted that the growth of fake accounts are more in developing countries like India and Turkey, as compared to developed markets UK and US [7], [23]. For instance, in March 2013 a certain girl found out that a fake Facebook profile of her created by someone was circulating on Facebook. The creator has used all possible ways to make the girl's life hell by sharing provocative pictures, phone numbers, address, and posts. This situation prevailed before and during Orkut days [13]. These incidents are not only common for girls; school kids are not being pardoned too. Obviously this is not a first case and won't be the last case on social media especially Facebook in India.

Highly sought Facebook users in music, acting, fashion, government, politics, religion, journalism, media, sports, business, and other key interest areas have not been spared too from the harsh attacks of impersonation. We have stories like Mayank Sharma or Sufia Khatoon where they used Facebook for good. At the same time we have thousands of incidents where people are being harassed by their fake profiles created on Facebook [10]. Interestingly, at one end, we see Taliban using fake profiles of girls to lure soldiers and gather secrets while at the other end, we have police officials creating fake Facebook profiles to nab culprits [20].

3. Deceptive Strategies of Impostors

3.1 Impersonification at individual level

Fake Facebook accounts are those accounts that do not represent the real, offline identity of the account creator. Facebook imposters usually use the same profile picture and attributes the original users have and keeping their Facebook accounts updated with the latest information posted on the original user's page.

The only difference between the two is usually a spelling in the title or name of the organization or individual such that both new and old fans who don't pay attention to detail like the Facebook page and fall prey to the impostor. Figure 3 and 4 below respectively show a genuine and a fake Facebook account of a public figure called Prophet Uebert Angel.

Figure 3 Example of the real Facebook profile. This is the official page for Prophet Uebert Angel and Spirit Embassy

Unfortunately, in most cases, the impostor is a Facebook friend to the highly sought after Facebook user who like the rest of the fans follows up updates and important information reserved only for the circle of Facebook friends.

Figure 4 Example of an impostor. This fake Facebook page is impersonating Prophet Uebert Angel and Spirit Embassy account disguised as Prophet-Uebert Angel

Once the imposter is successful to lure fans of the popular user to his/her Facebook page, he/she can privately begin to inbox the fans to ask money for his services or in disguise use an excuse of say a pending philanthropic work that needs money to be done. With the trust gained to the original user by the fans, the imposter can easily sequester classified personal information of his victims such as bank details and passwords to secret information. Most of these imposters use secondary accounts that people use for gaming or online dating, joke or spoof accounts that people create for celebrities or their pets. Like the rest of fraudsters and spammers, Facebook impostors attempt to appear like a normal user [22].

A professional imposter manipulates you into believing that someone really cares about you when all they want is to play mind games for his/her own satisfaction or to get money, goods, property, or something else from you.

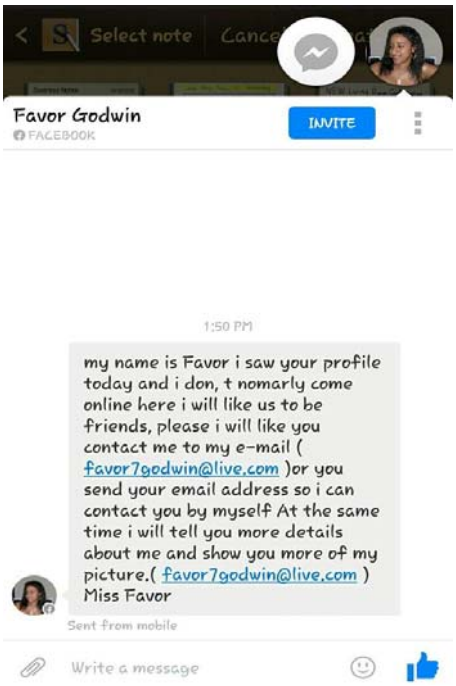

Figure 5 Snapshot example of an impostor inboxing a male Facebook user via Facebook Messenger

One example of such a professional impostor is Natalia Burgess who deceitfully duped a number of young men into relationships using false identities online, all because she felt inadequately loved [9]. Moreover, the imposter might also set you up to steal your identity or valuable information from you that he/she can use to manipulate someone else [22]. One of such tactics is to befriend others in your circle of friends to try and make friendship seem more real. Victims of this deception are more likely to be those Facebook users who have a habit of accepting friend requests from friends of friends' friends. This is usually influenced by similar tastes to yours in music, cooking, dancing, and other hobbies which leave you open to the occasional fake.

There are increasing cases of one person running numerous fake Facebook accounts, pretending to be an array of different people, all vouching for one another and all trying to be friends with someone real! Natalia Burgess, for instance, created many different personalities and put on different voices to prey on her unsuspecting victims. Sadly, impostors of this sort go to incredible lengths to create an array of fake accounts including other social media accounts and websites to give the impression that their fake personas are "real" [9], [22].

3.2 Impostoring at group/ brand/ organization level

Fake Facebook accounts can not only harm individuals (via spam, bullying, blackmail, financial fraud, etc.), but they're also bad for businesses. Many websites and mobile apps use Facebook Login to register new users and by welcoming fake Facebook accounts on to their platform, businesses expose themselves to at least three specific harms: spam, fraud and misspent market budget [12]. For example, personalization and targeting are on the rage these days for online marketing and many websites and apps increasingly rely on social networking sites to provide them with relevant targeting data. It is highly likely that 10% of the people these businesses spent marketing dollars on were fake or had inaccurate data [12]. That's some serious money wasted.

Imposters also use many fake Facebook accounts for affiliate marketing schemes or other shady marketing behavior. These accounts can clog up commenting systems and message boards with their spam and inundate users with annoying messages, not to mention send them links to malware that can compromise their devices and personal information. A recent visit to some Facebook Groups has revealed that those annoying ads for sunglasses, shoes and other apparel pop up every so often. Most of these ads come from those fake accounts which were created on purpose and their mission is to perform different spamming and advertising operations on Facebook; especially on Facebook Groups [10].

Fake Facebook accounts are often used by scammers to defraud other individuals on a company's platform. Peer-to-peer marketplaces, like collaborative consumption services or online dating sites and apps or even gaming platforms, are especially vulnerable. These fraudsters can also use fake accounts to conduct money laundering schemes or use them as "burner" accounts to accompany stolen credit cards when making fraudulent purchases [12]. Recently there were reports of fake accounts being created by computer

programs, which are used for inflating the number of "likes" on Facebook page for a brand [19].

4. Recent Solutions

Now according to the interview made to Mr Pavan Varma, the Business manager at Facebook India by NDTV dated September 11, 2012, the networking giant is making huge efforts to weed out fake profiles from its system to prevent misuse of such identities. Mr Pavan said that if Facebook doubts the ownership of an account, the user would be asked to identify themselves. Pavan further added that these doubts could arise if the account has a generic name rather than the proper name, uses images of celebrities or cartoon characters as display pictures or does not have enough friends [19]. In such cases, Facebook can request the account user to identify him/herself.

The social networking giant introduced the Facebook Help Center which contains the relevant information on how to report the fake account to Facebook admin. Apart from this, Facebook has created other avenues of reaching out to it via mail on appeals@facebook.com and login@facebook.com to explain the problem [13], [20]. However, it usually takes a long time for a report to be resolved by Facebook. In fact, Facebook doesn't mention how long will it take to close the fake account and you won't be the only one complaining about it. There would be whole bunch of people having the same problem. Meanwhile, the impersonated user can send a message to all his or her friends expressing the concern and not to accept any kind of requests from the fake profile. This can at least curtail the problem to some extent [13].

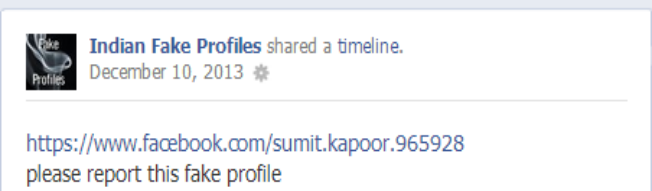

Figure 6 Example of fake profile being reported to fellow Indians by the impersonated user. Image taken from Facebook.com

The social network site has also started self-policing, saying it identifies "false" accounts, by way of dividing into two categories - user-misclassified accounts and undesirable user accounts. On 16 February 2012 Facebook announced that it will begin to allow a small number of public figures to verify their accounts [14]. It announced that users with verified accounts will appear more often in "People To Subscribe To" recommendations on the site, but unlike on Twitter and Google+, there will be no visual indication that a profile is official. Not everyone who allows subscribers will see this option, and for now, users cannot request to be verified.

For Facebook, verifying accounts seems to be about improving its recommendations systems. Recommendation modules around the site have been key to the growth of the social network's new subscribe feature. This will ensure that Facebook is presenting users with the real profiles of people they're in which interested [14]. Serving quality recommendations and being flexible about names helps Facebook compete with Twitter as a platform for asymmetrical relationships. A verified user's birth name will still be shown in the "About" section of timeline.

Currently, there isn't a way for users to definitively tell whether an account is the official profile of someone to whom they want to subscribe. There are already plenty of fake celebrity profiles on the site, and as more public figures begin to use Facebook, the number of impostors will likely increase. Facebook didn't offer details on how verification might affect search. Subscriber numbers do not currently seem to influence how a user is ranked in search [14]. This is frustrating for users and could lead some people to connect with fake pages.

Facebook has also increased its security to group users by providing a service which allows group admins to remove fake accounts from their Facebook group. Now, one can go to his/her Group's wall and click on the hotlink that shows the number of members in the Group.

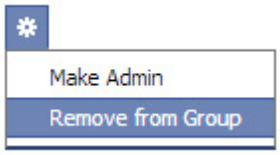

Figure 7 Removing fake accounts. Courtesy of Facebook.com

Once all members appear in a grid like fashion the Group admin can locate the person in question from the grid and click on the star icon below their details. A pop-up menu with two options will appear: "Make Admin" and "Remove from Group" so that the Group Admin can remove the fake account [10].

To ensure that the fake account doesn't access the Group again, Facebook allows the Group Admin to change the Membership settings, such that of the two appearing options he would chose "Any member can add members but the Admin must approve them". With this setting enabled the Group Admin can now see requests from people wanting to join the Group and he/she decides who gets in and who stays out. Factors to be considered will thus include account creation date, wall posts, about, photos and friends as well as Facebook profile url of the requesting person [10]. This keeps the unwanted spammers and pesky marketers unwanted.

However, according to one Facebook user, professional imposters are now known to block the page Admins so that they (imposters) can't be seen and removed. So Group members have to appoint a temporary admin to come in and get rid of the imposters before the regular group admin is reinstated [10]. Nevertheless, Facebook on May 29, 2013 unveiled a 'verified pages' feature meant to help users "find the authentic accounts of celebrities and other high-profile people and businesses on Facebook."A verified page will have "a small, blue check mark beside their name on timelines, in search results, and elsewhere on Facebook," according to a company blog post.

Figure 8 Verified page example of a celebrity-Selena Gomez. Image taken from newsroom.facebook.com.

Facebook is however not the first social media company to try to put an end to users setting up fake celebrity accounts. Twitter began rolling out its own system for verifying the authenticity of Twitter account identities in 2009 [16]-[18]. Following Twitter's lead, Facebook has added verified pages and profiles for celebrities (Figure 8 and 9), other "high-profile" people such as politicians, and businesses. This update makes it even easier for subscribers to find and keep up with journalists, celebrities and other public figures they want to connect to.

It should also make it harder for scammers to create fake Facebook accounts for celebrities and charities in order to solicit illegitimate donations. Verified Pages belong to a small group of prominent public figures (celebrities, journalists, government officials, popular brands and businesses) with large audiences [16], [18].

Verified pages and profiles will be shown with a little blue checkmark, indicating that Facebook has investigated and determined that the account is genuine, not a parody, and legitimately created by the person or brand it claims to represent. Verified Pages and profiles have a small, blue check mark beside their name on timelines, in search results, and elsewhere on Facebook [21].

Figure 9 Verified profile example of Mark Zuckerberg, founder of Facebook. Image taken from foraywhile.com

To verify accounts, Facebook said you'll need to submit government-issued photo ID, which Facebook promises to delete immediately after verification [18]. Interestingly, Facebook says it will proactively reach out to verify accounts, but there is no mechanism to request verification [18].

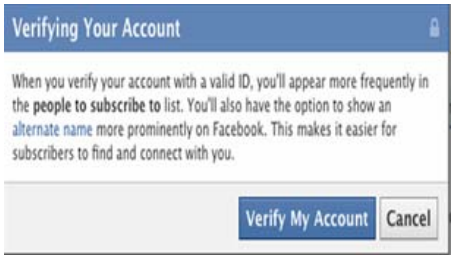

Figure 10 Snapshot for account verification. Image taken from venturebeat.com

Instead, Facebook recommends that celebrities or public figures who believe that they are being impersonated should report a fake account.

5. Conclusion and Recommendations

The number of fake Facebook accounts is increasing daily in form of duplicates, misclassified and undesirable profiles or pages. This is increasing the number of impostors who disguise themselves in one or two of these categories. A lot of unsuspecting Facebook users have therefore become prey to these impostors (social engineers) who impersonate the original profile or page user to solicit funds or blackmail the real Facebook user. Meanwhile Facebook is making fronting efforts to get rid of fake accounts, but currently only validating accounts of brands and celebrities. Thus, it is always better to go to the nearest local Police or Cyber Cell division to report any suspected impostor preying on ordinary individuals. There, the IP of the fake profile creator is easily traced and some respite can be brought to the life of the victimized individual. Apart from this the Indian government of is setting up a National Cyber Coordination Centre to screen content to help its citizens [13]. It is high time when Facebook should not only validate accounts for celebrities but also for common people.

References

[1] Huber, M. ; Kowalski, S. ; Nohlberg, M. ; Tjoa, S, "Towards Automating Social Engineering Using Social Networking Sites", IEEE International Conference on Computational Science and Engineering, vol. 3, pp. 117 - 124, 2009.
[2] Laribee, L. ; Barnes, D.S. ; Rowe, N.C. ; Martell, C.H., "Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems", IEEE Information Assurance Workshop (IAW), pp. 388 - 389, 2006.
[3] Tiantian Qi, "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering", IEEE Intelligence and Security Informatics (ISI), pp. 152- 159, 2007.
[4] Shenchun S. ; Yan C. ; Jianchuan F., "Analysis of Influence for Social Engineering in Information Security Grade Test", IEEE International Conference on Computer Science and Electronics Engineering (ICCSEE), pp. 282- 284, 2012.
[5] Fujikawa, M. ; Nishigaki, M., "A Study of Prevention for Social Engineering Attacks Using Real/Fake Organization's Uniforms: Application of Radio and Intra-Body Communication Technologies", IEEE Sixth International Conference on Availability, Reliability and Security (ARES), pp. 597- 602, 2011.
[6] Alim, S. ; Abdul-Rahman, R. ; Neagu, D. ; Ridley, M., "Data retrieval from online social network profiles forsocial engineering applications", IEEE International

Conference on Internet Technology and Secured Transactions (ITST), pp. 1- 5, 2009.
[7] Press Trust of India, "India, Turkey lead in 143.3 million false & duplicate Facebook account", Economic Times News, indiatimes.com, 1 Nov. 2013. [Online]. Available: http://articles.economictimes.indiatimes.com/2013-11-01/news/43592743_1_worldwide-maus-user-misclassified-accounts-undesirable-accounts. [Accessed: May 28, 2014].
[8] Prasant Naidu, "Users From India, Brazil Fuel Facebook's Growth On Web And Mobile For Q2 2013", Indian Social Media News, lighthouseinsights.in, 27 July 2013. [Online]. Available: http://lighthouseinsights.in/users-from-india-brazil-fuel-facebooks-growth-on-web-and-mobile-for-q2-2013.html. [Accessed: May 24, 2014].
[9] 3News, "Police yet to charge Natalia Burgess", 3news Discussion, 3news.co.nz, 30 May 2011. [Online]. Available: http://www.3news.co.nz/police-yet-to-charge-natalia-burgess/tabid/423/articleid/213142/default.aspx. [Accessed: May 26, 2014].
[10] Kris Olin, "EXPOSED! Fake Facebook Accounts Attacking Facebook Groups", socialmediarevolver.com, 26 June 2013. [Online]. Available: http://socialmediarevolver.com/fake-facebook-accounts-attacking-facebook-groups. [Accessed: May 26, 2014].
[11] Adam Markovitz, "New Law Targets Fake Celebrity Twitter and Facebook Pages. Phony Nick Noltes Beware!" Entertainment Weekly, popwatch.ew.com, 6 Jan 2011. [Online]. Available: http://popwatch.ew.com/2011/01/06/fake-celebrity-twitter-law. [Accessed: May 26, 2014].
[12] Virtrue, "What You Should Know about Fake Facebook Accounts", Verified Identity News, virtrue.us, 19 July 2013, http://www.virtrue.us/what-you-should-know-about-fake-facebook-accounts. [Accessed: May 28, 2014].
[13] Prasant Naidu, "How to Report Fake Facebook Profile or Impersonation", Indian Social Media News, lighthouseinsights.in, 6 March 2012. [Online]. Available: http://lighthouseinsights.in/how-to-report-fake-facebook-profile-or- impersonation.html. [Accessed: May 24, 2014].
[14] Brittany Darwell, "Facebook starts verifying popular accounts", Facebook News, insidefacebook.com, 16 Feb. 2012. [Online]. Available: http://www.insidefacebook.com/2012/02/16/facebook-starts-verifying-popular-accounts. [Accessed: May 26, 2014].
[15] Press Trust of India, "Facebook has about 72 million duplicate, misclassified or undesirable user accounts", IBN News, ibnlive.in.com, 8 Feb. 2013. [Online]. Available: http://ibnlive.in.com/news/facebook-has-about-72-million-duplicate-misclassified-or-undesirable-user-accounts/371600-11.html. [Accessed: May 28, 2014].
[16] Dave Capra, Andy Chung, and Allison Swope, "Verified Pages and Profiles", Facebook News, newsroom.fb.com, 29 May 2013. [Online]. Available: http://newsroom.fb.com/News/619/Verified-Pages-and-Profiles. [Accessed: May 29, 2014].
[17] Benjamin Pimentel, "Facebook rolls out 'verified pages' of celebrities", The Wall Street Journal, marketwatch.com, 29 May 2013. [Online]. Available: http://blogs.marketwatch.com/thetell/2013/05/29/facebook-rolls-out-verified-pages-of-celebrities. [Accessed: May 29, 2014].
[18] John Koetsier, "Facebook launches verified pages and profiles for celebs and brands", Venture Beat News, venturebeat.com, 29 May 2013. [Online]. Available: http://venturebeat.com/2013/05/29/facebook-launches-verified-pages-and-profiles-for-celebs-and-businesses. [Accessed: May 29, 2014].
[19] Press Trust Of India, "Facebook may give you a call if your profile looks suspicious", NDTV news, ndtv.com, 9 Sept. 2012. [Online]. Available: http://www.ndtv.com/article/world/facebook-may-give-you-a-call-if-your-profile-looks-suspicious-264919?curl=1389639218. [Accessed: May 28, 2014].
[20] Prasant Naidu, "Facebook serious about cracking fake profiles", Indian Social Media News, lighthouseinsights.in, 11 Sept. 2012. [Online]. Available: http://lighthouseinsights.in/facebook-serious-about-cracking-fake-profiles.html. [Accessed: May 24, 2014].
[21] Sneha S, "How to identify fake Facebook account and official page of celebrities", foraywhile.com, 11 June 2013. [Online]. Available: http://www.foraywhile.com/how-to-identify-fake-facebook-account-and-official-page-of-celebrities. [Accessed: May 26, 2014].
[22] Victoria Sauder, "How to spot a fake Facebook account", Social Networking- Facebook, wikihow.com. [Online]. Available: http://www.wikihow.com/Spot-a-Fake-Facebook-Account. [Accessed: May 26, 2014].
[23] Prasant Naidu, "India and Turkey lead in fake and duplicate Facebook accounts", Indian Social Media News, lighthouseinsights.in, 4 Nov. 2013. [Online]. Available: http://lighthouseinsights.in/india-and-turkey-lead-in-fake-and-duplicate-facebook-accounts.html. [Accessed: May 24, 2014].

Author Profile

Cephas Mawere received B. Tech degree in Biotechnology from Chinhoyi University of Technology, Zimbabwe in 2010. He is currently pursuing M. Tech Bioinformatics degree at JNTUH, India. He is also a Harare Institute of Technology staff development research fellow. His research interests are in the area of Information Security, High Performance Computing and Computer- Aided Drug Design.

Thabiso Peter Mpofu received B. Tech degree in Computer Science at Harare Institute of Technology (HIT), Zimbabwe in 2010. He is currently pursuing M. Tech Computer Science at JNTUH, India. He is a HIT staff development research fellow. His research interests are in the area of Data Mining, Network Security and Mobile Computing.