Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

SOCIAL MEDIA AND THE WEB OF SOCIAL ENGINEERING

Kriti Singh, Associate Fellow , CAPS

"Our social tools are not an improvement to modern society, they are a challenge to it."

— Clay Shirky

Communication has kept on evolving itself with the evolution of mankind. In contemporary times, social media has emerged as another revolution within the infinite realms of communication in general and mass media in particular. Social media has altered the very way the human communicates and connects. It has surpassed the boundaries of time, nations, races, and cultures and brought diversities of globe on one platform. Having said so, one cannot deny the flip side of this development of the information society whose information hunger refuses to die down. One of the core vulnerability of the social media is the threat of social engineering or manipulation and the lethality, which it initiates in the digital world that can affect the real world.

Social engineering: The existence of social engineering or social manipulation is as old as the history of communication as it is a skill of influencing an individual mind with the crafty skill of communication. It is combination of science and creativity. The concept seeks to identify the vulnerability of the human element rather than the computer network.[i] Social engineering, as called by hackers, is the 'art' of utilizing human behavior to breach security without the participant (or victims) even realizing that they have been manipulated.[ii] Phishing, spam, baiting, spoofing or hacking, dumpster diving are some of the techniques used by social hackers.

Why Social media breeding ground for social engineers:

With increasing digital penetration and multiple interactive digital platforms booming, the social media has become more and more integrated in our lives. To majority on Internet user the social media is just one another activity, to many 'important activity' of a day. From personal

Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

communication to business communication, social media has acquired an absolute new meaning and multi dimensions. However, this integration of social media has also made it breeding ground for the social engineers to flourish. Following are the few reasons:

- **Fertile ground for intelligence gathering:** Social media provides a fertile ground for a social engineer who is on look out for information. As more and more users circulates their personal information, location information, travel plans, photographs, job details, videos, the more fodder they provide to the social engineers and unknowingly assist him in making them more vulnerable targets.

- **Real human hackers with fake profiles:** Social media is another exposed ground where the social engineers are emerging as major threats. If we see social engineering from the lens of social media, we can redefine it as an activity where a hacker creates convincing fake profiles to connect and interact with a target or group of targets. Hackers create the profiles, build up a network of connections to make them appear trustworthy, and eventually connect with their actual target. Once the request is accepted a hacker can steal information or launch a cyber attack. Instead of a promising HR, marketing, or sales lead, profiles can be serious cyber security threat.[iii]

- **Simplicity increases vulnerability:** The simplicity of the social media platforms in terms of uploading and sharing the content like photos, videos, blogging, messenger services have made it user friendly, thus more popular within the users. However, this simplicity also comes with the flip side, as these users are the prime targets of the social engineers. While elaborating on the abuse of the social media platforms, the Symantec 2014 Internet Security Threat Reports states, "Unfortunately, widespread popularity draws scammers to these social networking platforms, as per the saying, *'If you build it, they will come*.' If a social network attains a certain level of popularity, scammers will find a way to exploit it. In 2012 the shift in spam and phishing towards social media was already underway, although these

threats were harder to recognise than their email counterparts. Symantec identified new scams targeting some of these up-and-coming social networks during 2013."

- **Freebies come with price:** For a social engineer, social media is one of the cheapest way to first infiltrate in the virtual social structures, then create an account, foster relationship with the online users, as majority of the social media platforms comes free of cost for the user. You just need to have an Internet, an email account and can easily access social media platforms like Facebook, LinkedIn, YouTube, and Twitter etc. After winning the confidence of the set target, the social engineer can lure them into the virtual trap or real traps and accomplish the desired aim.

- **New breeding grounds for phishing and spam**: Social media has alternated the trend in phishing and spam. Where previously the social manipulators heavily relied on the emails, today the trend is more towards using social media platforms to locate targets. Now from a crafty email it has transformed into craft social media campaigns designed by the social engineer to trap their targets. Although the style of phishing or spam has evolved but the things or materials to lure the target remain the same. It can be free movie tickets, gift cards, electronic goods, bogus offer etc.

To conclude there is no denial to the fact that the social media is growing and changing every moment, every day. So are the challenges and social engineers or human hackers are one such challenge. Amongst multiple communication platforms, social media has carved for niche for itself. Where it has emerged as a fertile ground for popularity and profit both, sadly it has also provided the breeding grounds for the social manipulators. The answer doesn't lie in shunning of this magnificent dimension of communication but the judicious use of social media and countermeasures to deal with social engineers.

****

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

----------xxxxxxx----------

[i] Rouse, Margaret. "Social Engineering." FROM THE ESSENTIAL GUIDE: How to Hone an Effective Vulnerability Management

[ii] SANS paper "The Threat of Social Engineering and your defence against it." 2003.

[iii] Foster, James. "A CISO's Nightmare: Digital Social Engineering." Securityweek Network: Information Security News. January 12, 2015. http://www.securityweek.com/cisos-nightmare-digital-social-engineering. Accessed February 21, 2015.