Asian Social Science; Vol. 14, No. 1; 2018
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

The Dark Side of Social Media: A Reality Becoming More Contemporary by the Day

Ajith Sundaram[1,2]

[1] Research Scholar, Anna University. Chennai, India

[2] Assistant Professor, Rajagiri Centre for Business Studies, India

Correspondence: Ajith Sundaram. E-mail: ajithsundaram@gmail.com

Received: September 16, 2017 Accepted: November 27, 2017 Online Published: December 27, 2017

doi:10.5539/ass.v14n1p23 URL: https://doi.org/10.5539/ass.v14n1p23

Social media was started with the intention of expelling the darkness from the lives of people by way of sharing knowledge, networking and communicating with near and dear. It all started with the purpose of imparting its benefits to all and making it user friendly. But the liberation of the down trodden, intended to voice their opinions, was turned into a hysterical chaos given the liberal mindedness of the people. What started off as a source of knowledge turned people into gadget freaks, attention seeking, financial and societal deficits. Given the nature of social media combined with the need to be social has turned it into a platform to mirror the human's self-image. The world has become a ball of information enabling people to never look or stop anywhere. The world is alive and networked 24/7. The digitalization of media turned out to be a flourishing business, especially through social media, smartphones, tablets and apps. A few billion people are always online and it is expected that heaps of devices and sensors will be available on the web soon.

Social networking sites are an inseparable element of today's Internet driven world and used by innumerable people worldwide. They permit people to part ideas and opinions and help find and communicate with like-minded people, ranging from childhood friends to totally unknown people. This mode of communication exposes more than necessary information, often including intimate data visible and accessible to anyone willing to observe it. Hence privacy is often a key issue to the users. Since huge number of people are online and ready to start conversations, it is also a vulnerable attack-breeding platform for spurious attacks. They spread malware content and spam content by capitalising on the users' innate trust in their relationship network. The Internet is the focal point for data-sharing in today's digital space. A robust part of Web 2.0 is characterised by social networks. They are a great platform for people to interact with friends or discuss ideas with similar-minded people. In short, a social network is an inter-related system of separate units which share a conjoint interest and increase interface or information pooled via the network.

Social networks exist in many different facets. Some are popular in a specific geographic location .Others are popular globally, like Facebook and Twitter. Based on the spread of user base, there are dedicated or specialised groups—some for entrepreneurship, some for professional opportunities while some networks specialize in interacting and keeping in sync with old friends, some even from high school. As one of the predominant uses of social networks is to find people, all important networks provide search feature options, but with different norms. Users can search and find local friends by limiting the probe to a single town or for co-workers by placing a query about company name. Social media has become more recognized with enterprises as well. But on the other hand, IT departments are often wary of social media. Some companies are contemplating on blocking or restricting the access to social networks completely in the organization rather than discussing it with their employees and internalising them of the risks. It is next to impossible for administrators to stop users from accessing social networks from work laptops or smart phones.

Common examples of popular social media sites are

- **Facebook**- Facebook, at present, is on top of the list and is one of the most actively accessed social networks globally. Facebook is an easy networking and interaction tool for everyone. Research shows that Facebook is accessed by more than 1.7 billion people to network, contact and interact with people and also to explore things that are of importance to them. The network enables users to design the profile pages where they can introduce themselves by sharing pictures or anything of interest to them. Facebook also permits different applications to be used within the network
- **My Space**- My Space is a typical social network where people can interchange messages and suggestions. It offers easy incorporation with music and is the reason why it is often used by liberated musicians to display their own work.
- **YouTube**- YouTube is the second largest and popular search engine with more than 2 billion views per day and it is the third most-visited website worldwide, behind Google and Facebook respectively. YouTube can be logged on in 61 different languages and is being used in 75 countries**.** About sixty percent of the views on a video originate from outside the country where it was created. Because of the extent of availability, the exposure a business video gets on YouTube is considered one of the most effective advertising tools available on a 24/7 basis.

- **Twitter**- Twitter is a micro blog service. Twitter is a short-message collaboration and communication medium that permits users to send out messages (tweets) to people who subscribe to followers. Twitter is evolving as one of the most popular social media sites. Currently, the site boasts of 320 million active users and has provisions of using over 35 languages. Each operator can post tiny messages consisting of up to 140 characters. Other users have the option of subscribing or following a particular person's page and receive their update messages.
- **LinkedIn**- LinkedIn is a professional-focused social networking site which was launched in 2003 with the main intention of helping people network and interact professionally. The site helps marketers in finding other business associates, clients, and colleagues who are already in the market. With over 400 million registered users in as many as 200 countries, having more than four million companies with LinkedIn Pages and professionals listing at a rapid rate of two new members every second, LinkedIn holds the label of the world's biggest professional social network.

Alarm bells

Social media is not negative when done safely and diligently. But with the widespread use of it, times change and the behaviour of the people too have changed. The power of social media is such that it has penetrated into deeper strata of the society resulting in open-to-all system. With social media, even fools and pranksters are capable of creating chaos using derogatory posts and ill-made visuals. People are forgetting themselves and are permitting the technology to rule them rather than the other way round. People have become more social online but have become lesser human in the real environment. People have become attention seekers and sensation lovers. Social media and the smart phones are a breakthrough for mankind. But in the quest for knowledge and staying connected, people have lost their love for life and wisdom.

With globalisation, speeds have increased and distances and physical proximities have decreased. But people are more concerned about themselves and hardly care for their fellow beings. Progress in technology has man more independent but lonelier due to lesser social interactions in offline environment. Society has become more individualistic. There is more interaction online but more emptiness and less togetherness. It is high time people find a way that binds more people together. The void in offline lives cannot be compensated through virtual meetings or interactions. Countless people exhibit their opinions and thoughts on the social web, apathetically revealing their personal lives with others in detail.

Physicians have observed a trend of social media related depression in teenagers. Researchers feel that teens who go through such phase are at an increased risk of depression and exhibit solitude resulting in seeking solace in abusive online content and display aggressive behaviour. Parents should always be vigilant in dealing with teenagers and should always monitor their online activities. Not only teenagers, but also adults display outs of anxiety when they find out that their tweets are not retweeted or when their Facebook updates are not liked.

Irrespective of the value, social networking media sites like Facebook, LinkedIn, Twitter, Tumblr, Flickr, YouTube, etc are grabbing and moulding our discernment of our external surroundings. This widespread availability of powerful communication tools have enabled people to reveal their personal as well as professional secrets. This affects the productivity of the self as well as that of the organization. It is high time people stop this kind of culture and convert it into healthier norms for a more responsible behaviour.

Social Media Deficits

We are concerned about the shortcomings that social media has on our lives, those which arise or are stirred by social media. They are

- Social, socio-psychological and rational- forms of Attention -Deficit Malfunction
- Corporate and macro-economic- forms of Monetary Deficit

Addiction in the Attention Deficit Economy

We have allowed many things and behaviours to blow out of proportion. Social media are a pathetic pastime which eats into our time and people have inadvertently enabled it to take control of the personal and professional lives. However, these geeky gadgets with in-built apps and many other features have eaten into the income of a majority of the users. Our penchant for social media is laden with uncertainties. Most of the social media activities are unintentional. Most of the expressions are outbursts in the form of updates or feel-goods or feel-bads. Social media behaviour is gradually shaping itself into an addiction. On a positive note, this addiction can intensify the planned activity or goal. But on the negative front, this addiction distracts from goal and people move away from the intended focus. As a matter of fact, we are not equipped to deal with it. In other way, we are unsure or are ignorant of how to deal with it. Online addiction is omnipresent. We live in attention deficit economy and not in attention economy.

The obsession with social media on mobile devices and coupled with all the hysterias, hazards, etc, that is shared every day, have turned out to be extreme such that there is an indication of irresponsible time-depletion. Consequently, a proper and plain focus, on what is actually vital has become problematic and instinct is taking edge over it. It is high time we do something rather than just dangling with our mobile social media groups via all kinds of useless apps. For reaping the real advantage of social media, we should begin by treating them in a vigilant and focussed way by being less instinctive and more thoughtful. Fortunately, an increased amount of consideration is being diverted to this development. The following negative consequences of social media are looming around everywhere.

1. Social media make us stupid

The question to be asked is if internet has really made mankind smarter. The answer is a pathetic 'no'. We should ask ourselves what the social media is doing to our brains. Violence and multimedia slow our brains and make us blunt, vulnerable lifeless and dull. The reality bites when we devote so much time and attention to it and it gravely disturbs the course of in-depth thought process. Social media simply spread sensations faster than sensibilities. Since, humans assimilate everything and do not remove what is unnecessary, we are reaching a culmination where inspecting our images and interpreting all the comments left behind on the Internet consume away good amount of time. We do not erase things even though they are not worth protecting and we also do not deny ourselves the moments. We are becoming more sceptical of losing our importance if we do not periodically experience special moments and showing that off to others. In the quest to discover such moments and store them, we ourselves are transforming into mute onlookers of our own lives. We are merely observing rather than actually live through such moments. The reminiscence gains prominence rather than the real experience of the moment, while we busily build digital erections around us.

2. Social media are transforming us into anti-social beings

An old saying goes- We shape our tools. But in the modern context, we are shaped by our tools. We are all so pre-occupied with our computers that we have forgotten human interaction in the real world. The computer, a mere machine, has elevated its status to that of human mind and brain. The present day humans are so hooked on to their devices and its content that they have become more social online but pitifully less or nil interaction offline. Chances are that speaking one's mind online will have the same after effects as saying those same things face-to-face and internet users have happily incorporated this element of social media.

3. Ego-tripping, insulating, narrow vision

Being dumb and anti-social can be tracked into the terrains of narcissism and ego- stumbling. This development goes in parallel to many serious problems. On the basis of information disclosed in our profiles, the Internet and social media will inevitably obscure all the true traits of the self, if we do not watch out, and thus eliminates an important source of vision and innovation, leading to increased cocooning and narrow vision.

4. Social media are making us mentally unsound

Humans are actually incapable of analysing and assimilating everything that reaches us via the Internet and social networking media. Our brains freeze after a certain level of assimilating data. It becomes difficult to process too many data. We become agitated, overloaded with facts and figures and we lose control and grip over our brains. In most scenario, it often inclines towards psychotic behaviour, Young people, whose brains are immature and are still in the stages of development, are unprotected and open to round the clock volley of digital content. They are full of activity with texting, messaging, Facebook, Twitter, YouTube, etc. They are glued to their computers, smartphones and gaming gadgets for hours together losing their proximity to the outside world.

5. Social media disintegrate our memory powers

We are always ticking constantly from site to another on the internet. We are always rummaging through the web. Research has proved that we mostly make use our short-term memory for this activity. If there is a barrage of content, this memory shuts down. We barely use our long-term memory anymore despite the fact that this forms the basis of our personality. The over-use of tools and other assets have mainly created a negative impact on the physical parts of human development. But with the advent of computer, the scenario is different. Computers are no longer a frontier of the physical expression of humankind, but an intercessor of our inner self.

6. Social media are extremely manipulative

Many posts on the social media are mere rumours doing the rounds. They lure media fanatics to resort to extreme behaviours. There are propaganda that asks its users to act or react in certain ways to show solidarity with any topic, issue, or a person. Sometimes, there is misrepresentation of facts and figures. The people who spend most of their time online are misled by theses false statistics and visuals. Some videos posted on social media are so extreme in content that the people are ready for indulging in rioting, going on rampage, disrupt public life and damage public property.

7. Social media promote terror

Most of the time, social media plays a pivotal role in the spreading riots. Some messenger media is capable of sending an encrypted message to a big group of people. After any major terror attack or rioting, when probed meticulously, one can see how each attack revealed on the role social media had played. Unrestricted flow of information can be used put into best use. But it can also be used for distribution of evil. And when people resort to social media for violence, we need to stop them with an iron hand.

8. Social media kindles our desire for sensation

On 26 February 2011, a severe seaquake tattered off the coast of Chile leading to the death of many people. The quake impacted not only the land but also the deep seas. A tsunami was born and drifted towards Hawaii. Different social media presented simulated images and the tentative time at which the Hawaiian coast would be flooded. At the specified time, after everyone had plugged into Twitter, nothing happened. People who used Twitter were fuming as they had waited and watched the entire day just to witness zero activity. Another earthquake resulting in tsunami on 11th of March, 2011 directed a nuclear tragedy in the Fukushima I nuclear power plant in Japan. After that, there were live telecast from people who focussed their webcam towards the after maths which was broadcast on U stream. In real time, pictures showed the despair of people in the affected area and how they were impacted by the ever-rising radiation. Some programmes received more than 10,000 views. Social media ensures that there is only a thin line between information and sensation.

9. Social media slams privacy and creativity

People have evolved to be at ease not only with sharing detailed information of different kinds, but also more responsively with more people, some of them even unknown. They are ready to disclose even the most cherished or trivial details of their life- be it personal or work life. They even shamelessly disclose the most intimate moments of life. This social norm has taken shape over time. One possible use of Facebook's data storehouse would be to sell data unearthed from it. Such information could be the foundation stone for any kind of business. And Facebook can do this without hurting users and regulators and lo, it has turned out to be lucrative. All of us possess multiple personalities. And that is absolutely normal, just a part of being human rather. We are like a kaleidoscope. There are many lenses through which others can observe us. All of us are multifaceted people. Social media emphasize that we are a mirror. There is one reflection which we all have. Similarly, we can also view people from any direction and results can be contrasting, yet they seem to be the same.

Irrespective of how restrictive we are and whatever be the privacy measures adopted, social media are ill-equipped to provide complete privacy. It is these gaps that attackers will take advantage of for intrusions. The attacker may capitalise on the weak security aspects of an application or software. So as an intelligent, forward thinking and a responsible user, post and share content carefully and rationally. Social media cannot be isolated from risks. Operate and access as if the material posted is a public property which is openly viewed by known and unknown people alike. Abstain from sharing anything that will put self as well as the members in contacts list and those around at risk.

The most important point to be remembered is that **everything is public on social media.** Be wary of the contents posted on social media as it cannot evade public access. So the ideal way to protect oneself is by restricting the amount of personal details posted on social media. This is applicable not only to the profile of the user, but also applies to the contents, comments or pictures posted. Always be on alert about the replies or responses from fellow users. Be very cautious on the types of contents posted about self, others and children, in particular. Do not reveal details about children as it may attract criminals to the children which may cause irreparable harm to their personalities or even lives.

10. Social media inspires bullying

In the past, children may have been intimidated by bullies at school or in their residing locality. Today, with the rampant spread of the Internet, children are now being tormented in every place and at all times. This has led to an epidemic-like environment which has to be urgently curtailed. When people are not talking to someone directly, they are less prone to the face to face consequences or to feel the implications of their activity. On the internet, it is too easy to say something to someone. There is a thin line between the after effects of cyber bullying and physical bullying. However, if ignored, the repercussions can be fatal. One of the most serious aftermaths is suicide followed by self-esteem issues in a close second spot, followed by depression, self-injury, feelings of loneliness which can seriously damage academic performance in school and general well-being.

Social media- a danger to cyber security

One should be always be careful and have responsiveness regarding the likely threats of sharing information on networking sites.

Threats and over disclosure of information

Attackers may attack social media services and spread infected content or malwares, gain access to personal information like identity, residence, relationship details, etc. Sometimes, the users themselves may disclose too much information than necessary to unauthorised or scrupulous individuals.

1. **Viruses**- social networking sites are the most convenient back ground for spreading of viruses, given their nature of public acceptance and popularity. When a virus is created and implanted in a website, the attacker exposes many unsuspicious users to risk, who in turn share the malicious links with their contacts.

2. Devices- pranksters make use of tools to gain control of a user's account and then gathers all the personal information of the users and the contacts he share. Sometimes, there may also be an attacker pretending as an imposter.

3. Social engineering attacks- the attackers may post a comment or content that looks to have been originated from a genuine networking service or a person in the contact list. If proceeded based on the directions, the user may land up divulging too much of information or pave way for computer attack.

4. Identity theft- when personal details end up into the hands of the attackers, they can assume the identity of the user and post contents in his/her name

5. Third party applications- sometimes social networking sites permit third party applications to be installed. Though it may look inoffensive or harmless, it is capable of peeking into intimate details without the knowledge of the user and post materials, send spams, check friends list, etc.

Professional and personal effects

Professional or personal relationships may be compromised due to unscrupulous access

1. **Business details-** disclosing official incidents on social sites are unethical as well as harmful. It shows the employee or organization in bad light. Sometimes, it causes irreparable damage to professional life. Divulging customer data, internal issues of the company, intellectual property details or other company related matters on social media may bring about a bad reputation both for the employee and the company.
2. **Professional status-** unsuitable images or posts on social networking sites may terminate all future professional prospects. Job recruiters or institutions may check the accounts of their prospective candidates during the application screening process. Contents posted by the candidate that hint his/her political, religious or social inclination may hamper the chances of selection and affect the integrity and or reliability of the candidates. There have been occasions where people were sacked from their jobs for the manner in which they have posted contents or expressed their views.
3. **Personal relationship**- it is impossible to restrict the audience for certain posts. The comments, photos or contents posted thoughtlessly may do much destruction to personal relationships. Being frank and transparent about the personal life on social media does much loss than expected as it is difficult to retract from one's views or comments immediately. As per data, almost 33 percent of the users have expressed their regret for divulging too much information impulsively.
4. **Personal safety**- there have been many incidents of cyber bullying. The information posted may cause pain not only for the user but also many others who are tagged in the posts or photos or are associated with the user. The information posted unconsciously may call for annoying harassment or nuisance. Posting details such as the location, residential address, children's school details are too dangerous and may even cause harm to the child's security. Cyberbullying incidents have impacted many individuals psychologically. So, social media pose as a physical, psychological or even social hazard to the user if is incapable of managing his account meticulously or intelligently.

Social Media and Cyber Security in the work place

Social media is a bizarre tool used by businesses in every sector. It provides the seamless opportunity for advertising, social networking, and increased customer backing and communication. Online platforms are excellent spaces for soliciting customers and handling a brand image. It is next to impossible to keep away from social media propaganda in today's digital culture. But the innumerable positives does not refute the risks involved for businesses. Social media in the work space has been found to be the biggest security issue faced by businesses in the current scenario. Many organisations have become gullible to phishing attacks (fraudulent emails claiming to be from authentic companies). Social media sites help hackers with the podium from which they can launch these attacks. They also open the gates to malware outbreaks, leading to malicious software being installed itself within a device or network. As a matter of fact, Facebook is one of the leading threats with respect to malware infiltration. Use of social media escalates the risk of fraud, spam and intellectual property ambush. In addition to the technical risks involved in social media use, there are also risks triggered by employees who are active social media users during work.

There is only a thin line between what is deemed suitable to an organisation and what can be damaging. People are at liberty to post whatever they want and whenever they want, but this can be of grave risk to privacy and to organisation's goodwill. People should always remember that anything posted on the internet is a public possession and that which cannot be retrieved as and when desired. It can be used fatally against an individual, business or organisation that an individual is linked to. There are chances that an employee can post inappropriate content or share information that ought not to be shared. An employee could gravely cause damage to professional reputation. The guidelines vary depending on sector. Sometimes, employees cannot be held responsible for what is being posted on their very own social media accounts. Hacking social media accounts has become increasingly prevalent, with hackers inventing and evolving fancy tactics all the time.

The following calculations, can be made with a greater amount of belief. They are not trivial and unfortunately, are once again intimately associated to social media.

1. There is a serious word of caution about immature use of social networks and social media. There have been umpteen warnings indicating the dangers of cybercrime, and social media identity may be more amusing to fraudsters than any other online content. Everyone has now become accustomed to Social Security Numbers and credit card data being stolen and sold online to other scrupulous people for carrying out fraudulent movements, but now, the online mafia will sharply focus to shift its attention to our social media IDs.
2. The second warning is closely related to the first. The most important merged cyber-attack will arise from our very own "friends" on social media and networks. We, at present, have crusades against phishing e-mails and an increasing number of advanced threats which are also on their way, based on social systems. The fun element on social media has definitively been crushed.
3. We are most active on social media right on our very own smart gadgets. Year after year, we will dive into an upwelling of more than a thousand cyber-attacks on smartphones and tablets. This has been prevailing for years and we were finally

assaulted by the first real mobile malware in 2011. Criminals and hackers have switched their focus, interest and attention to mobile devices.

4. In the technical territory, mobile platforms and the use of Social media sites indicate that the “safe” tunnels for corporate IT can cause a blind spot. This occurs when security tools are ill-fortified of decrypting in the tunnels. Thus flawed products are clueless of what is going in and out of the business network.
5. As an addition to the previous point, this word of caution conveys a rather simple message- Restraint Is the best deterrent method. It means that there must be continuous observation of whether or not data are seeping or are penetrating through network connections. This can be done by installing a restraint area that is constantly supervised. If unusual circulation is observed, the road in or out can be closed and the data can be analysed. Organizations with the right software will be able to handle the problem and suitable action can be spontaneously taken within seconds.
6. There are also ample external factors that are sources of concern .The happenings can always be used to formulate and implement large-scale cyber-attacks. This occurs not only via search engines, but also increasingly via social media and networks. We have all underestimated this menace. Even now, we are ignorant and do not associate social media with cybercrime, but that is changing.

Dumbing-down anxiety

Our memory is something that has always existed with us and is very dear to us. But with the advent of internet anxiety continues to irk us. We are unsure of what exactly is changing. Our brains are changing and our memory is also changing. Due to structural change, the use of the human memory processing is also changing. Once internet is in front of us, we start browsing. Irony is we have a habit of relying on that Google Effect. Our behaviour is also changing. The Google Effect has created a better understanding of matters. But those who learn tend to become less concerned about facts. People have become interdependent on their computer tools, developing in to interconnected systems that remember less but knows where the information can be found. We must forever be on Google to know information, in other words, believe everything that Google knows. We were always aware that someday digital technology would outshine our own intelligence. We are, forever, amazed at the events happening around us.

Digital technology and functionality are closely intertwined in our lives. The drastic progress of mobile social media is in severe disparity with the pretty gradual growth in large sectors of the economy. Here too the demand for a crucial and daring way of handling social media is directive. We should embrace social media and navigate them in the right direction. This marks the growth process, in which new designs emerge which over a period of time turn out to be the basis of new growth and wealth in the rest of the economy. However, there has to be a sincere and conscious effort to steer social media in the direction of to create a social society and social business and take treatment for dark sides of social media. But we are still unsure of what to do against the assault of social and mobile technology and their content, which creates an imbalance in our tempo on a 24/7 basis, divert and develop us at simultaneously. Mostly, it is hardly an option to train our overworked brain such that we are seldom diverted. Rather the new digital tools should ignore the imminence of real time and give messages in the correct context. This continuous state of distraction can be overpowered by unlearning the culture of multitasking and constant updates.

Technology must be made passive so that we realize that attention replace distraction. There has to be a suitable context or should be created that draws our attention. We are bombarded with more content than at any time in our lives yet the amount of time to assimilate it remains constant. Instant notifications should be reserved only for those few precious individuals and apps that absolutely warrant immediate attention, rather than those trivial ones. Content should never seem like a burden. To turn it into a pleasure, we need to start focusing on ways to regulate the flow. The classification and categorization of information are always subjective. We have to be concerned about consuming content consciously and making information and our information providers beneficial to thus rather than we being subjugated under them. Our gadgets and surprisingly, our human systems are extensions of digital universe. Our gadgets place right amongst emails, tweets, updates and notifications.

Responsible for our own behaviour

With an overdose of enticing technology, taking charge for our own behaviour is tough indeed. We simply starting love our life with our smartphones, tablets and modern apps. Especially, the direct link of social media to our senses and emotions, everything is interactive and is in real time where the digital stimuli is more electrifying than life itself. From time immemorial, man has loved a reckless and adventurous life with scant regard for hard work and lethargies. But now, real life is substituted by digital commotion. It is becoming crystal clear that we can make significant economic and social developments given the abundance of information. But this becomes a reality only when the complexity of the network withers off. The device are undergoing a sea change with respect to technology and functionality. They make use of the underlying technology in a human way. We no longer have struggle to connect all kinds of plugs, sockets, cables and wires; we no longer encounter a frozen software; we are showered with technology that fits impeccably with our inner senses. It is the inception of the humanization of digital technology.

Now we have to evolve consciously from geek into human being. We are pioneers and controllers of technology. This is possible only when we make use of intelligent technology to assists us, to supplement or improves us. Otherwise, we may perish in the ever-increasing deluge of information. And this is where we have to apply our own behaviour and our personal responsibility. Technology and human behaviour are intricately linked, the more powerful and smart our digital achievements, the steadier and safer we should be able to deal with it. In general, we will have to toughen up our stance on such digital temptations and have resistance particularly in handling social media, games and the screen gadgets on which they operate. Though this sounds moralistic, this is harsh reality.

The fact is our memory or our analytical skill is pathetically reduced due to our over dependence on other digital devices of knowledge such as smartphones and apps. Young People suffer from a digital form of Alzheimer's disease. The need to remember things have become a thing of the past as our digital resources do this for us, completely, correctly, automatically and in real time. So, a good idea, for health reasons, would be to distance ourselves a little from this technology as this will do us no harm and in fact, benefit our memory training.

For this, following four golden rules-of-thumb are recommended:

1. Train the memory to avoid it from becoming tangibly poor.

2. Accordingly, try to remember as many telephone numbers, names, poems, quotes and adages as possible, just like memory game winner

3. Try to leave behind as many digital devices as possible and grow with less dependence on them

4. Read books, articles and watch films, documentaries, etc, to successively discuss them with others and generate ideas.

A very important part of our Digital Literacy should be directed towards avoiding drowning into Digital Lethargy or worse- Digital Dementia. It is a question of self-discipline. Behaviour and technology should walk together, oriented to the place where we assign our digital privileges in our life. We would train ourselves to cope with such resources. The issue of how many victims rise up in the meantime, how people could have been properly guided are of scant regard in this fast paced digital era. We are currently living in an obsessive disruptive and distractive environment that is generating serious socio-cultural disorder.

Ironically, entertainment and mental inclinations towards digital devices are causing stress rather than relaxation. . Following are some tips for a happy and fulfilling life as provided by Manfred Spitzer at the end of his *Digitale Demenz* work

•• To start with, eat well and healthily.

•• Keep aside at least 30 minutes' for exercise a day.

•• Do not live in a conceptual world, but live in the present.

•• Pursue tangible and pragmatic goals.

•• Help other people in need, without self-interest, expectations and financial profit.

•• It is good to spend money on experiences than on things.

•• Indulge in music now and again, sing whole-heartedly.

•• A good mood triggers the brain areas for positive thoughts

•• Be active, alert and push away hurdles from path.

•• Make life easier for self wherever and whenever possible.

•• Go out for an outing with family friends instead of always hanging around on social media

•• Spend enough time in natural habitats, especially if there are children

•• Avoid digital media wherever possible and mainly children should be restricted from using digital gadgets.

Computing should be applicable only for computers, it is not the route to living

But it is next to impossible to stay away from digital resources. However, there some responsible digital behaviour.

Accept that digital devices are an elementary component of our society only and nothing beyond it. Understand the sensitivity of Information before digitalising it. Avoid the usage of rude or immoral language while using e-mail, chats, blogs and social networking media. Be empathetic towards the person, who is the reader, on the other side. Refrain from using copy-righted material by way of copying, downloading or sharing with others. Do not use digital devices to cause injury or harm to others. Do not interfere in others' digital uses. Use others' digital gadgets or resources only if authorised to use them. Be digitally responsible when posting, writing or designing online content. Do not steal data from others' digital devices. Do not spy on other people's online behaviour.

Spamming in social networks

Spam can be considered as one of the most typical attacks of all time and it will be wise enough to adapt to latest technologies multiple times ranging from email spam, messaging spam and in-game spam. Obviously, social networks too have become a victim of spam and is gullible to security issues. With the social network usage mounting at an exponential rate, adding millions of users to their existing user base, it leaves itself exposed to astute spammers who take the maximum advantage of the popularity of these networks, to outline spamming procedures, time to time. Almost all of services sanction the users to send messages to each other for free, it offers an easy gateway for spammers. Some networks are meticulously designed such that messages will be sent only if both users are connected online. To evade those type of constraints, bogus versions are created by the fraudsters and multiple friend requests are repeatedly sent so that at least some may accept them. When accepted, the spammer begins sending spam messages. A mere 'friend request' enables short messages to be sent within it, in spite of nil connection between the users.

Obviously, using compromised accounts is a popular spamming technique. Making use of formerly phished account credentials augments the authenticity of the message, as the receiver knows the person who held the compromised account and would be keen to expose the message. It is simple for an automated character to adopt a message that had been posted earlier, from the compromised user account, complement it with spam content and re-send it to all the connected contacts. Other variants like remarking on other people's posts or images and sending notifications to fake events are other ways of messaging to a wide audience. Regrettably, in every space meant for people to write standard information, the spammers will attempt to use them to place advertisements. Spam messages can be regularly seen in direct messages, status updates, comments on videos, contact requests, etc. Some methods can even self-generate multiple messages on different channels. For example, if a user sends event solicitations on Facebook, the user will not only obtain a statement message within Facebook, but also an email notification, unless the user has promptly deactivated notification emails.

Many communities have employed CAPTCHA checks that must be deciphered before sending multiple messages. This is done with the intention of stopping or to at least slow down the programmed spam messaging. Unfortunately, most CAPTCHA regulations can be cracked and there are systems available that use mechanical work to resolve them effectively. Furthermore, pranksters often use multiple accounts simultaneously until each one of them is unnavigable due to day-to-day message limit. Almost all social networks take proactive methods like offering a feature to report spam messages and enable blocking in future. But this feature is helpful or in other words functional only if the attacker does not switch accounts periodically. In addition to the spam embedded in the social networks, the brand statuses of social networks are often tainted to enhance the reliability of bulk mails sent outside of the social network. Since people are always getting friend requests, they are used to it and they often do not fully check the authenticity of the message and may end up clicking the link in the notification email. These links take the user to malicious websites, while others still use the old approach of attaching a spurious attachment with a virus.

Social engineering threats

Luring through baits in social networks

There are multiple procedures of search engine optimization (SEO) attacks. The modus operandi works like this- employ keywords and links such that the sites makes its way into highest ranking ones and pop-up in the first search results. Likewise, related threats can also happen in social networks. Almost all social networks enable users to visualise what is up-to-the-minute and sizzling at that instant. For instance, Twitter grades all the popular titles on its home page. This is easily available to attackers, who can easily seize keywords and incorporate them in their spam texts to get a better ranking. Some attackers began working on benevolent Twitter messages and then forward them. The pranksters then look out for new messages encompassing popular keywords. This could be a message related to a controversial decision taken during a latest sporting event, with a condensed URL connecting to an equivalent news article. The attacker takes this message and substitutes the original, edited URL with his or her own link that directs to a scrupulous site and re-tweets the message. For an ordinary user, it is difficult to distinguish between a genuine and an infected message. Thus the probability that an unsuspicious user stumbles upon an infected link are very high. Not denying the conventional kinds of soliciting messages that promises to link to porn visuals of celebrities or software tools being spammed to trap someone into clicking them.

Follower scams

As the popularity of social networks has shot up, there is a stress on people to have as many friends or followers as possible in their account. The gravity of the issue is such that, in a few social circles, social acceptance is determined on the basis of the number of friends in social networks. Young children are more engrossed on such tactics, the more online friends, the more popular the kid is. This requisite has been observed by scammers and 'friends and follower scams' are rampant on the Internet. The craze has gone to such an extent that some websites offer free services where the account name and password should be given and on return they ensure that the user gains many new followers per day. However, it is ridiculous to part the password with strangers, since there is no regulation over what activities they might indulge in and they do with the available account. In most cases, it violates the rules and conditions of the social network. But, these services will take control of the account and start manipulating it in order to send unrelated junk messages to all the contacts. This was totally uncalled for and this was not what the user wanted. Another system is to auto-follow many users or to send friend requests to random people, in the belief that someone may consent them and follow the user back. Some of these services are even chargeable.

Impersonation of celebrities

All of us would have come across bogus profiles of celebrities existing on various social networks. Unfortunately, there are few systems that can prevent anyone from creating a new account in the name of a celebrity and placing an easily available photo as a profile picture. An ordinary user cannot distinguish or determine if it is a genuine or fake account as long as the posted messages look genuine or until the message rip-off the real identity, people will perceive it as the authorised account. Such fake accounts can be used to blowout bad information about colleagues or fellow celebrities or to entice new followers, who can later be spammed. These fake accounts are vigorously endorsed by subscribing to many arbitrary accounts. These accounts usually contain a few messages which links to promotional offers or events. Some bogus celebrity accounts were used to contact real celebrities, posing as their friends. Some services are offering verified accounts tag. Twitter sanctions the identity of some of their accounts and displays a "checked account" message on those profile sites. But, this method cannot be followed for every noticeable account and they cannot validate that specific celebrity has been sending the messages. Unfortunately past results have shown that the passwords of official accounts are easily guessable. When a successful account is hacked, it results in the messages being posted in the user's account name. This happens frequently especially when celebrity accounts get hacked, weird messages appear on their accounts.

Impersonation of friends

Impersonation is a cause of concern for everyone irrespective of the social network in which they hold their account. There are numerous ways in which a password can be solicited. Phishing spells and Trojans can effectively do this. Once the prankster acquires the password of an account, he can resort to any activity like sending messages or even updating the profile status. These messages or statuses often direct links to different bogus sites to acquire more account passwords. The message looks like it has been originated from a friend's account. Therefore, people may tend to trust it. The pranksters, often capitalise on this trust and curiosity which lead to a greater click rate on those malicious links, resulting in the attack being successful. Users must always be vigilant, as messages propping up from confirmed friends on the list, might have been auto-generated by spyware. So, be judicious while clicking on the links in messages and always be on high alert when asked to download content.

Koobface

The Koobface worm is the pioneer in huge malware attacks which is aimed at social networking sites and is still going strong with its successful mission. It is highly successful as it launches evil social engineering outbreaks and lives on the link-opening behaviour of social media operators. The current options not only communicate from infected users to all their friends in their networks, but also resort to activities like apprising status messages or writing content to profile pages. The link that is posted will be delivered via Facebook's official page which in turn auto-generates a caution message before redirecting the user to the second URL. The attackers are aware that the people are accustomed to latest versions of Koobface which spreads not only on Facebook, but also on other social networks, including MySpace, Hi5, Bebo, Tagged, Netlog, Fubar, LiveJournal, Twitter and Friendster. The bait chart used, usually works on a very simple pattern. A user usually gets a personal message or a text posted on his social media account. The message can be a joke or an interesting video that encompasses a link which directs to a bogus YouTube site. When clicked on the fake YouTube site, the user is directed to download and then install a setup executable to play or view the video. The bogus video sites are operated from infected systems and compromised servers. The attackers are also on the lookout for newer technologies to attack computers. To enable the spoofed video site look more authentic, the link enclosed in the message can permit a unique id which can be used to load the fake friends' name and photo from the social network site. This looks very genuine when encompassed in the video site.

Trojan, after its installation, will download many more elements and start looking for access credentials to other social network sites. Apart from proliferating via social networks, the server also advises the Trojan to download further modules to the client, like including a small Web server to horde the fake video site or an installer for an ambiguous application. CAPTCHA-breaker element too can be downloaded to infected computers, directing the targeted victim to solve a CAPTCHA for the attacker who is camouflaged as a Windows validation check. This enables the Trojan to dodge anti-bot security measure, if any, but still automatically spam out infected messages. There are many modules available that contain a classic data-tracking mechanisms that can decipher passwords and re-direct them back to a drop-server. Manipulating the infected user's accounts enable Koobface fraudsters to accomplish their mission by creating fake accounts whereby they can also get access to online friends with an innate level of conviction at zero cost. This makes the soliciting messages look really genuine and allows the infection to spread like uncontrollably like wildfire via social network. It is not viable for the social network provider to install filters for such purposes.

Phishing

Social networking sites can be accessed by user name and passwords for logging in. So inevitably, they are also vulnerable to phishing attacks. Similar to the phishing attacks on banks, social networking phishing has different variations. Tricky emails claiming to arise from the social network service, offering some update or contest, appear frequently. To view the update status, the user is required to trail a link and log in, thereby disclosing his details to the attacker. The connected page is a bogus copy of the real login page, which is aimed at pilfering user account identifications. There are many other social engineering gimmicks where the user is connected to a link, which kindles the interest of the user and which lures him into a phishing page that steal the passwords. But financial sector is more affected or targeted by phishing activities compared to community sites. The returns from such bank accounts through phishing are much higher. But usage of dummy sites for community networks are huge mainly due to the ease of creation. Some of the scams even impersonate the originals by offering value added services just as the original one does. One such example is that of a service claiming to be given by Twitter. It made the users believe that once the user name and password was given to the fraudsters, they would enable the users to find out who follows their posts. They would display the names of some random fellow users as followers. Meanwhile, they misuse it by sending endorsements and promotional schemes. For this, security software suites can be made use of to reduce the risk as there would be difficulty in spotting the fake one.

Advanced fee scams

Social communities are gullible area for advanced fee scams. This is mainly due to the fact that users reveal too many details regarding their personal self. They also tend to easily fall for fake scams and scammers are shrewd enough to identify such possible victims and alter the motives to lure such victims. These types of scams typically offer huge benefits for nothing in return. After that the fraudster will inform the user about a fake issue which requires a small amount of money to be sorted out. Once the fraudster receives the money, he absconds. Social networking sites are the paradise for fraudsters. They are meticulous planners and cleverly execute their agenda. The social networking site helps identify lot of possible targets along with their personal details. The scammers impersonates another and lures the victims to make an advance fee payment promising a future service. Once they receive the money, the scammers get away. They do it with such impunity and repeat the same scam many times with newer victims.

Misusing information from the social network

The following sections illustrate how information from social networks can be manipulated to undertake attacks.

Resetting passwords

Almost all Web services enable users to reset their password. For this, the user name need to be filled and perfect answers to some security questions need to be given during the time of registering. This is used for verification purposes. There are usual, standard questions, the answers to which can be obtained easily from the profile page of the user itself. This way, the attacker can answer the questions and re-design the account. Once the account is penetrated into, it can be used to carry out future spamming attacks. So to avoid falling prey to such vile ways, users should abstain from using the usual, standard, easy-to-guess security questions. Always create a unique question and use secured passwords.

Make friend with someone to get information

Some intrusion testers use social networks to creep into larger enterprises. Their motive is to search the apt social networks of employees of the target organisation. This is simple, as business networks permit only restricted searches and facilitate the attacker to relate the email addresses and user names to definite companies. Using the information obtained, a believable but fake account can be designed. The attacker can then contact a promising account holder. The scammer, through his regular conversations and soft talks digs into sensitive content that the new contact reveals. Once a high level of rust is built, the scammer probes and finds out sensitive information like sever names, project details or even lure the new friend into opening a backdoor access to his system by way of opening an infected document or website. This shared data is used as a clue to select people from his target group. Though social engineering may not be always successful, it opens up a list of vulnerable people who can be tried on. In most cases, the fake account gets connected to many people from different sectors leading to access even sensitive data, job offers and promotional activities and incentives.

Revealing reconnaissance data

Another common blunder that employees make is by disclosing some seemingly unimportant technical information to the public unintentionally. This could be a comment on his social network account on the kind of job that he is working on currently or how he is stuck with some mundane software or firewall used in his project. This gives enough fodder for the prankster to plan his future course of action. An attacker makes full use of this available product details to decode the safety software that is used by the user or the target company. Therefore, a good idea would be to abstain from revealing too much of job-related data or security-related data on social sites.

Applications and widgets in social networks

A few social networks facilitate frequently used information to be implanted as applications or widgets. These applications can then connect with the user and his set of friends. For instance, it can be a daily humour application that posts a new funny content or a funny joke to the user's profile page daily, for the user and his friends to experience enjoyment. More intricate applications like multi-player games or photo rotation albums are also possible to be embedded.

Each social network uses its unique technique of implanting applications and implanting active content. Some of them permit remote code to be encompassed which is very risky, as it is difficult to monitor and control the content that will be uploaded. Bigger networks have generated their own, unique APIs that enable developers to gather definite information from the user's accounts. Sadly, it permits them to stealthily access some data or can resort to attack users or other applications. The following sections are instances of attacks that has been observed.

Never Text Again Scam

In July 2010, around 300,000 people became victims of a sham application on Facebook. Unexpectedly, more and more personal profiles began displaying a text with the following content: I am shocked! I am NEVER texting AGAIN as I found out this. Video here: http://bit.ly/ worldwide scandal!

Application directing to unrelated malware

There can be loopholes even with legitimate applications. Most of the popular and widely used applications on Facebook are games. Apart from the typical card games and arcade classics, simulation games or in other words, social games, are considered very cool and loved by a number of users. This means that the user can own his virtual fish tank, a virtual island or a realistic farm to take care of. FarmVille is a hugely popular game with current, active user base of over 60 million users per month. The user can multiply his simulated crops and seeds and harvest them to reap experience points and coins. These, in turn can be used to purchase cattle or tools and to reap bigger harvests and so on. Feats can be circulated on the user's profile to display how good a farmer the user is. Just as in real life, the plants in this virtual life takes quite some time to grow and reach the harvesting stage. This is to ensure that the user comes again frequently to view the development. For those impatient uses who hates to wait, there is an option to buy in- game coins with real money using a credit card. For those misers who hate to spend real money either, there are many websites that offer tricky equipment for the game. These "assistant tools" are often typical Trojans that does not help with the game at all, but they clandestinely access passwords and other important information from the user. Hence it is understood that such games can push people to websites that promise helper applications, which in reality are scrupulous programs. It is advisable to keep such offers far away.

Vulnerabilities in applications

Apart from all the activities an application is permitted to undertake including harvesting personal details, it might also bring together a host of new pitfalls to a user's profile. There have been instances of threats in some of the Facebook applications which enabled attacks on user's private data. Most of these were XSS or CSRF attacks that pose grave data violations. But, there have been reports of liabilities that give permissions to legitimate application so as to be transferred on to a malicious application. As a result, any application that has been installed can pose a security risk by being mischievous on its own or due to its weak admittance point.

What applications can ensure

Almost all social networks permit applications to access the user-data via multiple interfaces. Some offer documented APIs that grant definite access to bits of data. This could also include granular access provided on the basis of permission granted, to enable the user to decide on what to surf on the application. Based on its type, the application can be affixed deep into the social network and blended with the user interface. On the other hand, it may just interact on a superficial level, revealing only a limited information on a different website. For instance, Facebook has two rudimentary applications.

Firstly, it has social plug-ins, which permit the assimilation of simple Facebook features on to any website. Canvas applications that communicate with the profile, can send latest messages or open a new page. The "Like" button for a page is to apprise others about the presence of a page and to gain publicity, which is an apt example of a social plug-in. The other applications, to a large degree, get code from remote websites and implement it. In 2010, Facebook altered its basic API and authentication process, enabling it more transparent for the user to decide on what data the application is permitted to practise. The application requires to acquire the extended permissions before trying to access any private information from an account. Once the application receives consent from the user, it can do anything with this available information. The user can annul the liberties and deactivate all the applications any time from the application settings menu. But any information that had been accessed until then could be transferred elsewhere. Since 2010, Facebook necessitates any new developer to authenticate their uniqueness either by an active mobile phone number or a credit card number. This is done to prevent any anonymous developer from registering mock accounts for malicious applications. Unfortunately, this is not an effective prevention measure as any anonymous accounts can be registered with an anonymous phone number, which still prevail in some countries.

An application gets permission for certain activities which are as follows

Access the general data —this comprises the user's name, display picture, list of contacts and all other public elements of the profile.

Access the profile contents —This contains additional information like birthday, favourites, etc.

Send e mail —This is sending straight emails to the listed email address.

Access contents in the news feed —This permits the application to access the posted texts.

Access family and relationships data

Access photos and videos

Access friends' details— These include their personal data, birthdays, etc.

Access the data at any time —The application can read the details even if the user is signed off from the application at that time.

Post to the wall —Post new message on the behalf of the user

These illustrations prove that an application can gain access to almost all the details that a user has included in his profile, given on the condition that the user permits access to those contents. As the applications are permitted to load remote scripts, it is impossible to predict what happens to the user data and how it gets handled. An application very easily accumulates all the available accessible content on an offsite record and store it for a later use. However, there are strict conditions established by Facebook as to what an application can officially access, the rules to which a developer is required to abide by. Still, all users are required to have a glance at the permission-request windows cautiously and verify if the application actually is looking to access those pieces of information. At the end of it, the idea is to protect their intimate information. In addition to this, an application can appeal for offline-access rights from the user. Once granted, the application can get to read the user information at anytime, anywhere irrespective of whether the user is using the application or even signed into Facebook. This access gets cancelled only if the application is plainly removed by the account holder under his application settings. It should be noted that some of the non-public information, might also be accessed through applications. To prevent this action, the user must always alter the access settings of the applications used in his account.

Content threats

Affected profile sites

The founders of popular social networking sites have resorted to and identified steps to monitor the data that users send or upload. But often, some user may find a worm in the execution, or some issue that may have been overlooked. Despite this, it still enables uploading of infected content. One of the most extreme cases happen when it including arbitrary remote content becomes possible. This permits an attacker to embed attacking toolsets within profile sites, leading to an enormous attack on anyone surfing the affected profile. Social media websites may be used as display area or a platform for malware. Some of these do not directly pose a hazard to the user visiting the profile site due to their dormant nature. But, they can easily be distorted by a remote Trojan to update itself. In general, most often we see that infected profiles or status pages contain malicious scripts or links.

Malevolent links

Since users can regulate the content of their own profile, they can add infected content to the pages intentionally. One apparent attack is by readdressing the user to an outward malicious site, which is totally under the control of the attacker. The posts can be crafted intentionally on specific, registered fake accounts or by script attacks. The user redirection can be accomplished by social engineering tricks that redirect the user spontaneously. The social engineering spell is meticulously crafted and is difficult to be blocked by the social media provider as it is hard to differentiate it from harmless, regular posts. Some providers have begun using publicly available URL to block certain URL posts. A few network providers use a transitional re-directing site that cautions the users that they are quitting their page and that the target site is beyond their control. The redirected website may contain anything like advertisements for bogus products, misleading applications, phishing sites or even enable download attacks.

URL limiting services

URL limiting services were existent since a long time. Today, it is usually a short domain name in combination with a function key redirection system. This helps the user to design a short URL from any given link. Since there is no line break, it is easier to share and it gels perfectly into short messages. There are hundreds of limiting services which are freely available. Most services are cheap or sometimes incurs no cost and are available to all. A few of them were designed in combination with applications or browser plug-ins. But, one of the apparent issues with such services is that they confuse the terminal point of the link. This makes it difficult for a user to identify which is genuine and which is malicious, as they do not see its destination. Fortunately, many of the popular services enable viewing of the destination or statistic page with the number of hits made till date.

Script risks

Every social network provides an API that can be used to access the functionality straight from a script. This is extensively used by third-party applications. This technique of access helps an attacker to create automated scripts that can gather any open information or to spread bugs that can reproduce across the network.

Manual script attacks

A simple attack genre that is observed on social media is the manual script attack. The term manual is used because the target is directed to copy and run the script physically. Therefore, a few interaction steps are needed. By following the instructions step-by-step, hidden JavaScript will be copied, which will focus on the users URL bar and will paste the JavaScript, and finally execute it. By following these directions, the script can use the current logged-in session to send messages to all the friends of the user, requesting them to repeat the cycle. The user may be directed to click on a few surveys to reach the application.

Many of the existing services use public blacklists to hinder malicious links from being shortened. Unfortunately, this is not very effective and still allows past, unknown malicious links to be utilised for attacks. The one thing that is common to every attack is that the user voluntarily spreads the information to his friends. Some attackers have also begun adding advertising banners to each of the step, generating further cash flow for them. Users should always be very cautious whenever they are asked to process manual commands, especially if the purpose of the command is unclear. Also exercise caution when disclosing real address or mobile phone number anywhere.

Cross-site scripting (XSS)

Cross site scripting (XSS) attacks are a very common kind of injection attack. There are a range of ways in which an attacker can implant or embed customised scripts in a genuine website. A user who surfs the site or trails a specially-crafted link will reach the specific site. From here, the injected script from the attacker will be sent back as a part of the legitimate site. This enables the script from the attacker to be implanted in the visitor's browser from the susceptible site. This script can exploit the trust the user has in a genuine website and potentially steal session cookies or begin cross-site forgery attacks (CSRF). As people are usually logged into the service when they are surfing other profiles, the script can manipulate the session and infect their own profile with the same infected script. Thus, spreading of malware from one profile to another occurs. Further, the bug will begin posting contents in the victim's name. These messages embed short links that leads to malicious websites. Apart from spreading worms, XSS attacks are often used to take a user's session cookie. Alternatively, the fraudster will use it to include random content. It can help in the designing of phishing sites under the real domain, directing documents back to the attacker. Conventional anti-phishing toolbars cannot discover these phishing sites.

Cross-site request forgery (CSRF)

The CSRF outbreaks capitalise on the trust that a website has in the browser. Whenever a request arises from a user's browser with a valid session, the Web server will accept the request and execute it. The Web server is clueless about the request. It is unaware if it was deliberately made by the user or if a hidden script on a website sent the command clandestinely in the background, without any notice of the user. Since most people are constantly logged into their preferred social sites and seldom log out, this becomes a potential target for CSRF attacks. Such an authenticated session can be distorted by scripts on maliciously-crafted websites or scripts planted by XSS attacks. Those sites can give instructions which will be executed because the current user is logged in. To the social network, it may seem like the user clicked something. This includes potential for disseminating worms. In 2005, My Space became a victim of worm attack. A user guessed the methods to dodge the content filter that was needed for publishing content on profile pages. He also learned that he could use JavaScript in CSS tags without being filtered. By clouding his JavaScript, he was able to execute various actions including reading out the content of the current page and creating new 'http post' quests. This generated a kind of worm which spread rapidly and infected more than one million users within 20 hours. Social networks are still prone to such similar attacks and there is an increasing trend of mass infection. To curtail such risks, users should always log out of any service when they are done with it. Smart security resolutions can always lessen the threat.

5.3.4 Clickjacking

Clickjacking and click-fraud work on the principle where users can be deceived into clicking on things that they do not see or that they are aware of. Usually, an invisible frame is mounted along with some content and spread over an easy game that enable the user to click numerous times at specific places. While a user is under the impression that he has clicked the game, he has, in reality, clicked on the invisible layer and has started some other action. This could be a 'submit key' that gets triggered. This enables the attacker to perform any action that requires a few easy clicks. If the user is signed into a service at the same time, then something like a CSRF attack with manual interaction can ensue. This means, the user can be deceived into clicking on a hidden button to alter his privacy settings or share all the contents in his account.

Sometimes, even CAPTCHAs could be implanted and passed on to the user for resolving.

The messages sometimes contain catchy phrases which lure the users into clicking on the links on the profile sites of infected friends. They will get re-directed to a website where the only visible content may be "click here to continue" written in big letters. Of course, clicking anywhere on the page will activate an invisible 'Like' button, which can update the user's status message with the same text as seen in the earlier accessed profile. This allowed the bug to spread to numerous profile sites with no extra effort. Though there is no direct damage, similar attacks could include malicious URLs or sometimes newer versions include advertisements that generated profits when a user viewed them.

It is not at all cumbersome for users to shield against such clickjacking attacks. In addition to using latest security software, users can also use browser plug-ins, such as NoScript, that will discover some of the hidden frames. As for the owners of websites, there are a few methods which can be practised in order to safeguard their website from being presented in an invisible frame. For instance, Facebook executes some of these approaches to prevent the "Share" button from being used within a hidden frame-tag. This thwarts clickjacking attacks. Despite all these proactive measures some clickjacking attacks still continue. Unfortunately, the like- jacking attack still works. The attacks that took place had tried to use the mobile versions of the social network page, as they are easier to deconstruct and have minimal level of security mechanisms.

Design issues

Privacy

Privacy is a prime cause of concern for all social network users. The user may choose to disclose the amount of private data willing to be shared with the external world. The information that are posted can be restricted to a select set of audience depending on the content or how relevant it is to the group of contacts. Most social networks have a different set of privacy setting for confirmed friends compared to the public audience, which again can be chosen by the account holder. In some cases, a user can decide on what details to share with all his connected friends, but still keep it invisible for someone browsing his public profile. For example, Facebook has three groups of visitors- direct “friends”, the “friends of friends”, “everyone”. Depending on the kind of information, the user can decide on the audience who are permitted to view the contents or who to share the information with. The default sharing setting is “everyone” kind of audience, which is really abundant and share a lot of information. Many users may probably want to alter their privacy settings depending on the kind of content shared or posted.

Likewise, Twitter permits its users to shield their tweets and messages. This means, once they are enabled, all future messages can be viewed solely by those users who have been established as friends. The privacy settings also enable a user to deactivate this option when others can find them by searching for their email address. It is complex to link a Twitter account to a known email address. It is also important to bear in mind that some social networks, indicate in their EULA, that they are entitled to use and even sell the contents that are uploaded. It is understandable that they may need some rights because the content is shared in their network. However, others might be sharing contents with third-parties. The permissions granted, would theoretically include using the texts or images for a commercial ad without asking for consent or without making a payment. Often users are totally in the dark regarding the quantity of information that they are sharing publicly. Irrespective of which social network one uses, it is mandatory to understand the privacy settings and if necessary, alter them to suit to one’s needs. There is only a thin line between participation through sharing information and preserving one’s privacy, especially in matters of social networking.

Erasing data and accounts

Once a message is posted, it is almost impossible to delete it completely from a social network because it would have already been forwarded to others and might have been reposted again. Twitter provides a key to delete messages individually. Undoubtedly, once something is posted on the Internet, it is impossible to delete. Therefore be judicious and cautious before posting something online. As far as Facebook users are concerned, they can go to their profile page and delete any post by means of a Remove button. For those interested in deleting their full account, it is a long and complicated process involving a few steps, compared to deleting individual messages. On Facebook, the user can deactivate a profile from the settings page, which may keep all the data intact, but enable the profile invisible to others. This ensures that it can be re-activated at any time later. Those who genuinely want to delete a Facebook account can log into the account and visit the delete page. The account will then be deactivated for two weeks, during which no further interaction should be made for it to be removed. Unfortunately, this include automated log-ins from affiliate sites that the user might still have in his browser cache. So it is advisable to erase the browser history and cache, to make sure that he or she does not inadvertently log in, which will cancel the deletion process completely.

Information revelation

The prime purpose of a social community is to disseminate information. Therefore, all the information will be unchecked and will be disclosed to others. However, the users are sometimes ignorant of the velocity and impact of the information shared or the implications they carry. The following sections will reveal the effects.

Disclosing location data

People, generally, like to socialize and share their mind. This includes information that might be misused. One of the characteristics, that often goes unheeded, is the location data that is passed along. Many people publicize their exact location, which is not a serious concern per se, but this information can obviously be misused for stalking or for robbery. Some services like FourSquare, emphasise on the geographical location of the people, at a given moment. In FourSquare, users can check-in at different locations. The more frequent they check in, higher the ranking for that place. In this manner, people can see where the fellow users are present, at the same restaurant or attending a concert and so on. Even though FourSquare enables a user to restrict what information to publicly display, it is vulnerable to design flaws.

Sometimes, even if the user disables the option of being shown on location sites, identity of checked in user can be ascertained. Another user group, who should exercise caution on revealing their geographical locations, are the defence personnel. Sending status update messages back home, revealing the troop power and their current camping location, is probably a foolish idea. But, something as simple as uploading some pictures from a specific location, can reveal information, as many cameras are powerful and can automatically embed metadata into pictures. Therefore, unsurprisingly, many military forces have banned the use of social media completely, or have taken precautionary measures by training their users not to reveal too much information. There were already instances of location information being leaked. Apart from showing where the users are located at a given time, it obviously reveals where they are not, for example, at home or in school. So tentatively speaking, a tech- savvy robber could analyse from their profile, when people are not at home, find their residence address and then rob their homes. Sometimes, people could risk their jobs when their superiors track their location when they are found to be absent from work. There have been cases of self-exposure by the employees.

Disclosing identity

In some groups, social networks can be directly connected to fellow internet users, on various platforms. As they provide a real name, it is easy to identify the users behind an anonymous action. In some social networks, a registered user can see the other users who visited his or her profile page, even if that person did not add him or her as a friend or send any message. Mere reading of the profile page, is sufficient for leaving behind the trace of identity. Regrettably, this can be abused with CSRF risks. Any user with evil intention, can add a hidden frame or link to any unrelated website he has control and link it to his own profile site. Whenever someone visits that web page while logged into the social network, they will leave behind their trace in the logs. The site owner can potentially track the true identity of the visitor. Some researchers have advanced a step ahead by tracking another person's social network connections. To illustrate, with the CSS characteristic of links called "visited" and a small bit of JavaScript programme, an attacker can decipher if a user has recently logged on a predefined URL. This process can be used to surf through many sites and to identify all the social networks that are being accessed by the user. Based on the nature of social network, it can also showcase the main profile site of the user or give an evident trace of the user. To guess the identity of the user, determine the intersection of groups to which he is affiliated. To launch such a cross- checking, there should be some background study on the groups available on the network. Also. There should also be some back-tracking work that has to be undertaken to establish the identity of the connection. A social media user can easily be identified if he visits any website by virtue of his identity in the media site. Some social platforms offer this as a feature. Facebook enable a feature called instant personalisation to all its users. This permits third parties to ascertain the identity of the user who visit their website without the user being logged in.

Unprotected frameworks

As social networking platforms are becoming more complicated, undoubtedly, some susceptibilities in their structure can be discovered. The rigorousness varies between snooping personal information of other users and fiddling with other user's accounts.

Sometimes, when there is privacy malfunction, the bug can be tracked in the privacy settings feature itself. It shows a user to check how his reformed privacy setting impacts the way his profile looks to another person by giving a preview. This also gives a read-only rights to someone else's account. Unfortunately, this also includes viewing the private chat interactions or pending friend requests that the other person had. Pranksters can design a crawler that can export the data of millions of users within a few days by means of design bugs, to determine the group affiliation of protected user accounts. This problem may be followed by many data leakages.

Attackers can access information from reserved accounts by using the power-search function even if a user locks his details on his profile site. A mixture of automated queries for every possible combination and permutation enabled reading out all the intended data from protected profiles. Sometimes, after publishing a code update, many private messages can be directed to the wrong person's inbox. Users will not know if the message was acknowledged by the intended person or not.

In SQL intrusions, an attacker can post his specific SQL queries to the linked-database. These assaults can be very catastrophic, as they might disclose user's accounts with passwords, emails address and all other sensitive information. There will also be exterior attacks than can hamper a social network's amenities. Big names like Facebook and Twitter too were smashed by a massive, distributed denial of service (DDoS) threat that rendered the entire web service offline for a few hours. However, one respite is that DDoS damages will not compromise the privacy or security of the account. Just that there will be a restriction on the availability of the network. The issues gets serious when services that are dependent on social media has serious glitches. So any shrewd attacker can pose serious problems to social networks.

Mismanagement as a control structure

The well-designed framework of social networks and their Internet connections make them a potential candidate for botnet control, especially, due to the fact that such commands could merge into the usual social network traffic seen at any major site. The following sections discuss some methods that were misused.

Botnet regulation over status messages

There had been efforts to mistreat social networks as a 'command and control structure' for botnets. However, this is not surprising, especially after several ISPs have blacked out, in order to get rid of botnets. The botnet designers are on the lookout for tougher ways to control their assets. Since social webs are widely distributed, usually having speedy Internet connections, they are a susceptible victim for a command structure. Trojan Whitewell is an example of such a bot that frequently checks the mobile form of existing Facebook account. The attacker can submit a new post to the profile, in order to enable the bot to be downloaded and to run a file from an URL or contact a web server to get new commands. Related concepts have been tried on Twitter, where the bot downloads the up-to-date communications from an existing Twitter account. We have also witnessed a simple Twitter bot-creator tool that can create another bot, which will verify instructions in clear text from designated accounts. This setup need not necessarily deliver extra resistance against black outs, as the social web service provider can merely deactivate the accounts or filter for specific posts. However, the fraudster can always design new accounts. But the already distributed bots will not be able to get notified of these updates.

Some attackers have keenly observed this single-point botch up. KreiosC2 is a good case of a proof-of-concept bot that make use of social networks for governing channels in a more refined way. The bot is likely to command in natural language presented by any user account or it discovers commands implanted as comments in uploaded JPEG files. As a result, there is much complication in blocking and filtering out all the commands for the service provider. It has been observed that almost all of the present efforts aimed at using social networks as a command and control structure are of a very primitive structure. However, it is possible to use the infrastructure for undercover channels in a more refined way.

Information allocation

Apart from making use of social networking profiles as command structures, they can also be used for loading updates or releasing data. Consider the case of a Trojan that downloads a binary data from an established profile. To make matters worse, it is harder to trace, as the updates could be hidden in a media file, such as an image. The new Trojan could then transfer its accumulated data as encrypted text data, such as local passwords to another profile. If the content is complicated enough, it will mix into the normal estimated traffic and can be opened from anywhere.

Best practice tips

On social networking sites, always tread with caution. The user must have awareness regarding the dark side of social media and that it is filled with risks and security threats. With adequate proactive measures, this situation can be confronted and can be transformed into an enjoyable process. Adopting and implementing proper security measures will protect the user as well as the computer from scrupulous and malicious attacks. By protecting oneself, those connected around can also be secured. Social media put forth unique risks. However, the user need not be on panic mode when using social media. The risks can be minimized and social media can be made entertaining and informative by adopting certain precautionary and proactive measures. The following are some of the guidelines that need to be remembered while using social media sites.

Be sceptical

Social networks are a useful resource of business information, as well as, a great channel that gives news-worthy updates from friends. But, they may contain a lot of unimportant and irrelevant information. Generally, anything that is viewed online should be dealt with a great extent of scepticism. Do not ever blindly trust everything that is shared- be it financial assistance, hot topics, trending news or tips on free gifts, especially if it involves clicking on a link or installing an application. Anyone that demands money in advance should be ignored as it is sure to be a scam.

Check privacy policies and settings

Every major social networking service has a unique and specific privacy strategy and rule that are published on their websites, to ensure privacy protection for the users. Ensure that they are thoroughly understood, even though they may be time consuming, boring and tedious to be read. They give tips and explanation on the course of action that need to be taken if the information is shared with other people. Some services extend the ability to control privacy settings for specific clusters, such as permission to share pictures only with a select group of audience like ‘friends only’ and not ‘everyone’. Always make wise use of these settings. By taking advantage of the privacy policies, the user is doing good not only to himself but also others who are associated. There should be no compromise on privacy and choose appropriate action for security. Always keep a tab on safety guidelines and periodically review the settings and options looking for alterations and apply the safest feature. Always undertake a periodic review of services privacy policies and adopt and incorporate all the available security measures.

Good passwords

Use good, strong, complex passwords. Do not set easy and guessable passwords like date of birth, names of family members or pets. If possible, ensure that the password is a combination of letters, numbers, as well as special characters. If remembering complex password is difficult, either use an easy hint or use any of the existing password management functions that can securely safeguard them. Do not ever select a password that can be deduced from the existing information published on the account site. This includes friends’ names, favourite movie stars or author names. Set strong, complicated and difficult to guess passwords for each service.

Protect the password

Never act foolish by sharing the password with others, come what may. These include services that assure to assist to get more friends or such similar gimmicks. Do not lose grip of password.

When entering the password, ensure that user is logged on the authentic website and not a phishing page that appear identical to the original site. On being doubtful to have become prey to a phishing attack and account being compromised, use a clean computer to log into the original site and modify the password.

Be considerate

Always double check before posting or updating something. Any content that is once posted, even if it is to a close group of friends, makes the user loses control over the matter because it will or will not be reposted and the audience cannot be controlled. These issues may be back to haunt the user if he searches for a new position or relationship in the future. Double check before publishing the full information and do it only if it is absolutely necessary. This comprises disclosing too many private details, such as phone numbers, whereabouts, relationships or work-related stuffs. Likewise, abstain from promoting virus hoax or inflated warning messages that will create panic among fellow users, as it does more harm to other users than actually help them. Be diplomatic and respectful to others. Never ever post derogatory messages about others. Be empathetic as one would never want to read derogatory posts about self.

Be cautious

People online are not always who they pretend to be. They may display multiple personalities. The public figure who the user may be following, might turn out to be just be another fan or the co-worker posing as an employee from another office might just be someone conniving against the enterprise. Not everyone who claims to be a friend on social media site can be trusted as a friend.

Stay updated

Make sure that the software installed is up-to-date. It should not only cover the operating system and web browser, but also third-party plug-ins, such as PDF viewers. Install all the cutting-edge versions. Always keep the anti-virus softwares updated. Time bound installation and updating of applications and softwares are pivotal to system safety.

Stay protected

Some of the newer versions of viruses and threats are very complicated and sophisticated. They are sometimes difficult to catch the attention for an unqualified or even experienced user. Use inclusive safety software to shield from these threats.

Share information only with trustworthy contacts

Social media gives the option of choosing an audience for posts. While posting or sharing content, choose the right viewers who should see the posts. Sometimes users try to increase their contact lists, but consider sharing contents only with the appropriate audience. Always segregate the contacts and allocate access features differently for each group. Attackers are manipulative enough to convince users to include them in their close circle. They may even assume fake identities to persuade the user to be added as a contact. Double check the legitimacy of the new contact and confirm the identity who they claim they are before authorising them to access the personal details. However, a proactive measure would be to always add people known to the user than add unknown fraudsters just for the sake of growing the contacts base. Better be cautious than feel remorse later.

Discourage suspicious third party applications

Choose third party application wisely. Do not install scrupulous looking softwares or those conceived by unscrupulous or unreliable vendors. Keep a vigil on the extent of details that third party applications can access. Always check out for applications developed by trust worthy vendors.

All contents online are public

Be aware that anything posted on social media cannot evade public eye. So the intelligent way to protect oneself is by regulating the amount of personal data posted on social media. This relates not only to the profile of the user, but also is pertinent to the contents, comments or photos posted. Always be wary of the responses from fellow users. Be cautious on the kinds of contents posted about self, others and in particular, children. Abstain from divulging details about children as it may attract unwanted attention towards the children which may cause irreparable harm to them.

Conclusion

Social networking communities are an intrinsic element of today’s web world. People use these sites as they want to be in touch with friends, exchange pictures or just kill time when bored. Companies too, have started engaging social media as a marketing tool for targeting their customers with relevant information and give more focus to them. With the availability of user groups capable of covering millions of users, there are always evil ones with malicious motives. Attacks through worms and bugs spread through these social networks. In almost every case, fraudsters have engaged social engineering tricks to send soliciting messages under the pretext of an infected user. Inquisitive people who trail the link will also get corrupted with malware and unintentionally spread the texts further. Unfortunately, many people will click any link in their feeds and add any contact to their personal network, without knowing the real wolf hidden behind the screens. This innate trust, especially from the messages sent by friends, who have an infected account makes the attack-chain to be successful, irrespective of whether it is a phishing attack, a spam or a malicious worm spreading through automated scripts. Past experiences have proved that the safety and privacy of the user can be violated, either by flaws in the underlying structure or by installed applications that have seeped out data. But, many users are still ignorant or rather indifferent towards the security settings provided by the network and expose themselves to the risks that arise out of disclosing too much personal information. Social networks definitely can be definitely be informative and entertaining, but users should exercise caution and behave with the required level of uncertainty.

Copyrights