CYBER SECURITY ON SOCIAL MEDIA

Online social life is about how ordinary people and citizens take advantage of social media to connect with people for entertainment, socialisation and keeping in touch with the daily lives of friends and family. The networks that support this form of life online are commonly described as social networks.   On a broader perspective it is more a sociological and technological phenomena. Sociologists would define it as a network of people through friendship, work, family, interest and business activities. From a technological perspective these are communication network platforms that enable one to one and group communications for a wide range of purposes. The technology architecture that drive social networking platforms are distributed computer networks. This article outlines common security risks and general rules of thumb that could be adopted by users to secure and protect personal data on social media. The general principle is that we face more security threats due to increase use and interaction with social media platforms and communication networks for entertainment, connecting with friends, family and loved ones. Social media has become one of the ways of enriching our social lives.

Social Media and Network platforms provide unprecedented economic, recreational, social opportunities and freedoms to users. These platforms enable people to interact and communicate seamlessly using a range of data formats such as text, sound and video. This facilitates user access to a wealth of information that could be exploited for good or malicious purposes. These opportunities also come with enormous risks that may compromise data security of users. This could be a breach of privacy, consequently violating confidentiality, integrity and availability of data. This wealth of information also serves as a foundation for building cyber security intelligence essential and critical to securing personal data and devices.

It is important for users to be aware of the inherent reputational value, economic benefits and dangers that come with personal data shared on social media. Whether a user owns, shares or creates data on these platforms, it should be secured from Cyber Attacks such as Ransomware, spoofing, information theft, espionage and blackmailing due to unethical or malicious use of the platform that may result in criminality.

Unethical use of data refers to conduct that may be lawful however inappropriate with social and cultural implications. These may involve using the media to engage in conversation that is likely to breach privacy of individuals or employees carrying out official business for an organization or government without the right level of security clearance or engage in conduct deemed unfit for a person in public office.

Criminal use is breaking any of the laws that govern the use of social media depending on jurisdiction of the law, its enactment or enforcement. Other security breaches may be socially engineered in the form of fake advertisements of products, dating sites, online fundraising schemes, scams designed to extort money, Government tax rebates falsely promoted using web links and direct messaging. This may involve the use of Emails, WhatsApp and Facebook Messenger to obtain private and confidential information from devices consequently enabling the successful launch of a Cyber Attack.

Risks among young adults and children

A profile analysis among young people shows that a vast majority of them are not aware of the extent of the dangers and risks on the Internet. Generally most young people that use online social networks fall within the age group 14 to 19 years old. The main networks comprise Tiktok, Snapchat, Instagram, and Clash Royale a game platform for younger children. A great way to be in contact with people they have lost contact with, as well as expand their current connections. The activities among teenagers and younger adults could comprise, profile viewing, listening to music and sharing contents among close friendship groups. Kids communicate to people they usually know or have known through a friend or a friendship group.

On the contrary adults tend to use WhatsApp, Telegram, facebook and twitter for social or business reasons. Single Mums and Dads also use this as a means of talking to people, dating and building new relationships. It can be an effective way of introducing yourself to people. For instance new undergraduates use this medium as a way of introducing themselves to peers. Parents are less likely to comment on their child's profile. The main concerns online generally include bullying, leaving privacy settings open and sharing photos that could damage people's reputation. There is significant level of lack of awareness and understanding of how profiles could be exploited. This is due to the low level of confidence in the ability to manage the settings on these platforms. This leads to the voluntary display of personal information.
It is however fair to state that although young people in most cases disregard safety and security concerns, they are still aware of some of the risks associated with online activities, however due to the fact that the benefits outweighs the risks less attention is paid to such issues.

Rules of thumb for securing personal data from attacks on social media

These are the rules of thumb to follow in order to protect your personal data and devices; Cyber is an asset that has inherent value as such should be secured. Be threat aware by enabling your data privacy settings on personal devices, follow trust and risk compliance routines by always verifying and assessing social media friendship networks before interacting with new contacts, enforce best practice by changing user identification and passwords routinely, change control settings of computer or mobile devices frequently to determine what information you want to disclose to the public, restart devices frequently to free up the memory of your device in order to prevent DOS (Denial of Service) and to ensure data availability. Limit information you share to unknown contacts, apply multi-factor authentication or multi-step verification at all times for example User ID and Password, Biometric features including finger prints and iris identification are enabled on your devices especially if working remotely.

The above methods when adopted improve and strengthen your device security leading to enhanced data confidentiality, integrity and availability. These are the primary security goals necessary to be met by any user to robustly repel or improve security of private data on a mobile device or computer. The use of the word "improve" denotes there is nothing such as absolute personal data and computer security on social media. Every user should consider adopting best practice highlighted in this article whiles using social media platforms. Due to the expansion of social activities and remote working during COVID-19, there has been sudden surge of security threats on social media and computer networks. It is essential that users operate and adopt a zero security tolerance and compliance approach to security and privacy during this period.

Why secure your device and data?

Cyber is a valuable information asset that requires security by the individual citizen, business or Government. Securing your personal or corporate data for the sole purposes of ensuring confidentiality, integrity and continuous availability of data whether for personal or business purposes although useful is inadequate. Cyber Security should be considered as a strategic asset that pivots the very success of information use. Due to this inherent value and its applications, Hackers would be prepared to explore and exploit vulnerabilities on devices and online to gain superior advantage or monetize data from devices and systems that have been compromised due to unauthorised access.

Computer Network Attacks take place in many forms. These may comprise taking control of a Computer without the Target being aware of the attack using remote Computer code execution. In this part of the series we describe the Victim as the Target. Common Cyber Attacks include but not limited to Disinformation/misinformation, Ransomware, Espionage or Spying and Hacking.

Disclosure versus IP (Intellectual Property) violation. Recently the Social media platform Telegram was compelled to disclose personal data of users due to an Intellectual Property (IP) violation by a court in India. Although Telegram had argued that the court order was likely to compromise the privacy of its users, the court also argued that the interest of the owners of the IP took precedence and prominence over any form of disclosure in that particular instance.

Ransomware is one of the fastest growing Cyber threats that could be used to take control of a Computer in order to exploit the Victim digitally. Digital exploitation compels the Victim of the attack to release confidential information or cause the Integrity of the data to be compromised. Recently BOEING was HACKED by a Ransomware, the "WannaCry" Virus holding a cross section of its Computer Systems hostage that blocked rights of access to critical data as well as preventing availability to critical Data.

Sir Francis Walsingham is known in British Secret Service history as a Spy Master who employed the art of lifting the wax seal of a letter so that it could be opened undetected. William Camden (1551–1623), an English writer described Sir Walsingham as "a most subtle searcher of hidden secrets, "who saw every man, and none saw him." The security a Firewall provides is breached when intelligent tools and techniques are employed to take control, surpass and steal information undetected by evading the security it is designed to provide rendering the Firewall non effective due to the attacker's superior intelligence. It could be argued that the perimeter security a firewall provides to mitigate and respond to the nature of emerging attacks is at best dumb, as it lacks the dynamism and adaptability to respond to the nature of new security threats. This means when Confidentiality is breached, Integrity of a message also becomes compromised.

Hacking is the unauthorised access and subsequent use of other people's Computer Systems, Information resources and assets. The attacks usually take place in several phases, using information gathering and analysis. It involves methods of obtaining information to exploit security vulnerabilities. Social engineering is one of such methods used by an attacker to extract information. The two main categories of social engineering are; Computer based deception: The act of deceiving the Victim into believing that they are interacting with the 'real' computer system by getting the Victim to provide confidential information. Human approach: This is done through deception by taking advantage of the Victim's lack of knowledge and the natural human aspiration to be helpful and liked.

Hacking of passwords can take place using Brute force, a technique that uses exhaustive key search to crack a private or confidential message by automatically making reference to a dictionary. A Malware can also disrupt every day's operations of a system leading to Denial of Service (DOS). Although considered as old fashioned by some experts, it is still effective.

Future use of Social Media and the Internet.

The primary role of the Internet is to reconfigure how we access information and do things such as getting to know people, understand their behaviour and how we can leverage this behaviour as part of developing useful relationships as cyber beings. Many people also use the social networks to kindle new relationships or rekindles past ones according to William Dutton, Professor at the Oxford Internet Institute. People usually meet on online dating sites, chat rooms and instant messaging platforms to facilitate this aspiration. Online dating sites have been prolific in the last decade in many parts of the world. For instance a couple that meet online are likely to have similar interest. A group of university students with similar interests will usually form online associations to further this interest, with the view of building stronger relationships to advance that group's programme. Many commercial opportunities can be created online, with very low capital. The barrier to entry in a business sense is very low for emerging entrepreneurs. There are however issues such as identity theft, bullying, exploitation of innocent people that requires effective response and strategy for mitigating these threats.

Emerging Cybersecurity Trends

Firewalls have not been able to competently withstand the new forms of attacks giving that the new forms of attacks have become more sophisticated. The attacking strategies employed by Hackers have surpassed the Security that traditional Firewalls provide. It can be argued that the cost of implementing or embedding them as part of a Home or Corporate network has become unjustifiable. This has driven the need for emerging technologies and concepts in the field of *Artificial Intelligence also known as nature inspired algorithms* for profiling, pattern analysis, Context Based Reasoning (CBR), predictive intelligence and artificial neural networks using deep learning as an alternative to securing Personal data, Home and Corporate Networks.

.

Author: *Professor Godfried Williams is CEO of Intellas and IBM Partner in the United Kingdom, Fellow of the British Computer Society and Subject Matter Expert in Cybersecurity, Analytics and Artificial Intelligence at the University of Essex (UK) Online Computing & Business Schools.*
Email: g.williams@intellas.biz