Qubahan Techno Journal

Review on Social Media and Digital Security

Rasan Ismail
Department of Computer Science

Duhok, Kurdistan Region of Iraq
Renas.rekany@nawroz.edu.krd

***Abstract*— The emerging social media with inherent capabilities seems to be gaining edge over comprehensiveness, diversity and wisdom, nevertheless its security and trustworthiness issues have also become increasingly serious, which need to be addressed urgently. The available studies mainly aim at both social media content and user security, including model, protocol, mechanism and algorithm. Unfortunately, there is a lack of investigating on effective and efficient evaluations and measurements for security and trustworthiness of various social media tools, platforms and applications, thus has effect on their further improvement and evolution. To address the challenge, this paper firstly made a survey on the state-of-the-art of social media networks security and trustworthiness particularly for the increasingly growing sophistication and variety of attacks as well as related intelligence applications. And then, we highlighted a new direction on evaluating and measuring those fundamental and underlying platforms, meanwhile proposing a hierarchical architecture for crowd evaluations based on signaling theory and crowd computing, which is essential for social media ecosystem. Finally, we conclude our work with several open issues and cutting-edge challenges.**

***Keywords*— Social Media, Digital Security, Digital Growth, Networks.**

I. INTRODUCTION

Digital technology is changing the way in which society is operating and the ways we live our lives. Every day, there is new ways to work and to play, new methods of interacting with one another. As our digital footprint grows exponentially, we are forming our own online identities. Digital security is the protection of this online identity. Criminals are finding new ways to operate and steal information from digital users for their own personal gain. Digital security is an all-encompassing term which includes the tools you can use to secure your identity, assets and technology in the online and mobile world. These tools you can use to protect your identity include anti-virus software, web services, biometrics and secure personal devices you carry with you every day. Devices such as a smart card-based USB token, the SIM card in your cell phone, the secure chip in your contactless payment card or an ePassport are digital security devices because they give you the freedom to communicate, travel, shop and work using your digital identity in a way that is convenient, enjoyable and secure[3]. While digital security systems have been disclosed, present digital security systems do not fully take advantage of the significant intelligence possibilities offered by digital cameras, programmable digital signal processors, and programmable communications processors. Nor do the present systems offer a fully integrated networked digital security system including a centralized web server that allows for authentication and access control to digital security services, remote configuration of intelligent camera units and customer servers, and significant administrative and billing functions via the Internet[1,2].

Fig.1: Social Media Security

II. LITERATURE REVIEW

One of the great things about social media is staying connected wherever you are. However, it's important to think about where and how you log in to your accounts.

- Use bookmarks or favorites to access social media sites, or type the URLs into your browser. Don't access your accounts through links that someone else has sent you, or links on other websites. These could lead you to fake sites, allowing attackers to access your personal details or even install malware on your device.
- Make sure your browser or website doesn't store or remember your login details on shared or public devices, like library computers or shared tablets. If you do, and someone else uses that device, they'll get access to your social media accounts too.
- Be cautious of logging in to your social media accounts using a hotspot or free WiFi — if you're logging on at a cafe, for example. These networks are 'untrusted'. That means it's possible that others could see what you're doing when you use them.

If you access your social media accounts through an app on your phone or your tablet, make sure you lock it when you're not using it.

2.1 Types of digital security on social media

As you can see, there is a lot that can go wrong if your digital data is compromised. Fortunately, security in the digital world comes in many forms, offering a wide choice of defense methods. These include:

2.1.1 Use strong passwords on your accounts

Using strong and unique passwords for each of your social media accounts is one of the easiest ways to keep them secure. Here's what you need to do [4] .

- Use a different password for each of your social media accounts. Don't use the same password for your Facebook account as you do for Instagram, for example. That way, if someone gets access to one of your account passwords, they won't get easy access to your other accounts as well.
- Make your account passwords long and strong. Short sentences make the best passwords as they're easy to remember. For example, a string of four or more random words is just as strong as a 10 character password that uses a mix of numbers, letters and symbols.
- Don't use the information you share on your social media accounts to create your passwords — this information is easy for attackers to find out. For example, if you share pictures of your dog online, make sure you don't use your dog's name as your password too.

Don't share your passwords with anyone — not even your partner, your parents, or your children.

Fig.2: Password Security

2.1.2 Antivirus Software

Viruses delivered through malware and other malicious systems infect your data and bring your system to a screeching halt. A good antivirus program not only detects and cleans out these infections, but also keeps out suspicious programs and isolates likely threats[5].

2.1.3 Current, Updated Firewalls

This tool monitors web traffic, identifies authorized users, blocks unauthorized access, and—if current enough—will even protect against next-generation viruses. Firewalls have been around for years, and many cyber security experts dismiss them as obsolete. However, a state-of-the-art version is a potentially useful tool for keeping out unwanted users[6].

2.1.4 Proxies

Proxies are digital security tools that bridge the gap between users and the internet, using filtering rules in line with an organization's IT policies. Proxies block dangerous websites and leverage an authentication system that can control access and monitor usage[7].

2.1.5 Remote Monitoring Software

Remote monitoring allows the data security team to collect information, diagnose problems, and oversee all the applications and hardware from a remote location. Remote monitoring provides flexibility and convenience, enabling administrators to resolve any issue anytime, anywhere[8].

2.1.6 Vulnerability Scanner

This tool detects, evaluates, and manages any weak spots in your organization's system. Vulnerability scanners not only identify flaws but also prioritizes them to help you organize your countermeasures. IT security teams can use scanners for both web applications and internal systems[9].

III. Types of Information in Digital Security Risk

Not every bit (or byte) of your information is useful to cybercriminals. A total stranger finding out that you prefer the original Star Wars trilogy to the sequels is scarcely an earth-shattering revelation that could compromise your identity or financial security. So, the kinds of data are at risk is:

3.1 Personal Identification Data

This data includes your name, phone number, address, email account name, IP address, and, most damaging, your Social Security number. It also includes information that potentially pinpoints your location. Personal data is often used for identity theft and social engineering. Also, a hacker who has your Social Security number (or equivalent) can open credit card accounts in your name, thereby eventually destroying your credit score[10].

3.2 Personal Payment Data

If it has to do with financial transactions, it's considered personal payment data. This information includes credit and debit card numbers (including expiration dates), online banking numbers (account and routing), and PIN codes. Criminals who gain access to your online banking information can even transfer funds out of the accounts or make purchases[11].

3.3 Personal Health Data

Also known as personal health information (PHI), this data type encompasses information on your health, including medical history, prescription drugs, health insurance subscriptions, and doctor and hospital visits. This information is precious to high-rolling cybercriminals since they can use your health information to file false insurance claims or order and resell prescription drugs[12].

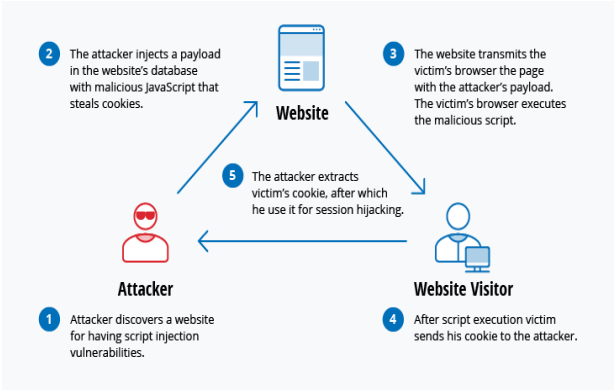

Fig.3: Digital Security Risk and Attack

IV. Analytics and Statistics about Social Media

There was plenty of strong growth across all things digital in the first quarter of 2018. The number of internet users rose by 4.54 billion in 2020, reaching a total of 7.75 billion by the end of the quarter. More than 5 billion people around the world now use a mobile phone, with roughly 6 in 10 of those users owning a smartphone. The numbers show that mobile users grew by roughly 2 percent in the 12 months to March, but GSMA Intelligence recalibrated its dataset in February, so the actual growth figure may be even higher. Meanwhile, mobile continues to grow its share of social media use, with 389 million people accessing social media via mobile for the first time in Q1. This 14 percent increase takes the number of mobile social users well past the 4 billion mark, with the total standing at 3.987 billion at the start of the second quarter.[13]

Fig.4: Global Annual Digital Growth [13]

The average internet user now spends 6 hours and 43 minutes online each day. That's 3 minutes less than this time last year, but still equates to more than 100 days of connected time per internet user, per year. If we allow roughly 8 hours a day for sleep, that means we currently spend more than 40 percent of our waking lives using the internet[13].

The world's internet users will spend a cumulative 1.25 billion years online in 2020, with more than one-third of that time spent using social media. However, the amount of time that people spend online varies from country to country, with internet users in the Philippines spending an average of 9 hours and 45 minutes per day online, compared to just 4 hours and 22 minutes per day in Japan[13].

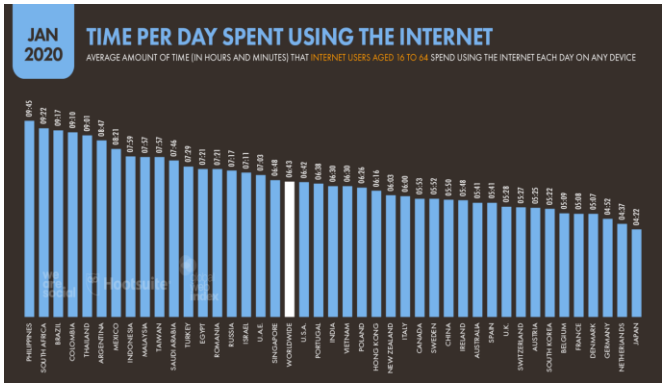

Fig.5: Time Spent using the internet each day January,2020 DataReportal[13]

More than 2 billion people have come online since the first mention of 'The Next Billion', but just over 40 percent of the world's total population – roughly 3.2 billion people – remains unconnected to the internet. More than 1 billion of these 'unconnected' people live in Southern Asia (31 percent of the total). Countries in Africa account for 27 percent of the total, with 870 million people yet to come online across the continent as a whole.[14]

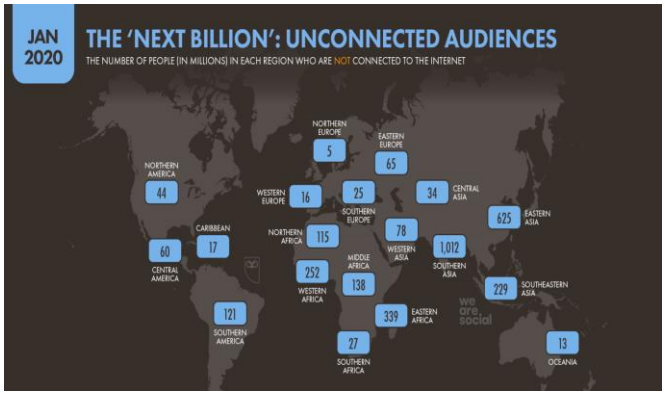

Fig.6: Map of the World's Digitally Unconnected Populations January 2020 DataReportal

V. CONCLUSION

As growing popularity of the Social Networking Sites these have become a prime target for cyber-crimes and attacks. Cyber-crime is becoming a widespread and posing a major threat to the national and economic security. Both public and private institutions in sectors of public health, information and telecommunication, defense, banking and finance are at risk. So the organizations should take proper security measures to be cyber-crime safe and the users should protect their personal information to avoid and identity theft or misuse. The cyberspace is becoming a significant area for cyber-crimes and terrorist to attack on crucial information. So, there is a need of universal collaboration of nations to work together to reduce the constantly growing cyber threat.

References

[1] Zhiyong Zhang, Brij B. Gupta, Social media security and trustworthiness: Overview and new direction, Future Generation Computer Systems, Volume 86, 2018, Pages 914-925, ISSN 0167-739X, https://doi.org/10.1016/j.future.2016.10.007.
[2] Simerly, T. W., Tang, T. S. H., Dutt, A. M., Pledger, P. K., Breton, K. D., & Kay, A. (2011). U.S. Patent No. 7,952,609. Washington, DC: U.S. Patent and Trademark Office.
[3] Redmiles, E. M., Malone, A. R., & Mazurek, M. L. (2016, May). I think they're trying to tell me something: Advice sources and selection for digital security. In 2016 IEEE Symposium on Security and Privacy (SP) (pp. 272-288). IEEE.
[4] Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014). History of information: the case of privacy and security in social media. In Proc. of the History of Information Conference (pp. 283-310).
[5] Rajab Asaad, R., & Masoud Abdulhakim, R. (2021). The Concept of Data Mining and Knowledge Extraction Techniques. Qubahan Academic Journal, 1(2), 17–20. https://doi.org/10.48161/qaj.v1n2a43.
[6] Kim, H. J. (2012). Online social media networking and assessing its security risks. International journal of security and its applications, 6(3), 11-18.
[7] Li, H., Wouhaybi, R. H., & Kohlenberg, T. (2015). "Security challenge assisted password proxy." U.S. Patent No. 9,223,950. Washington, DC: U.S. Patent and Trademark Office.
[8] Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. Academic Journal of Nawroz University, 10(1), 7–12. https://doi.org/10.25007/ajnu.v10n1a998.
[9] Kals, S., Kirda, E., Kruegel, C., & Jovanovic, N. (2006, May). Secubat: a web vulnerability scanner. In Proceedings of the 15th international conference on World Wide Web (pp. 247-256).
[10] Asaad, R. R., Abdurahman, S. M., & Hani, A. A. (2017). Partial Image Encryption using RC4 Stream Cipher Approach and Embedded in an Image. Academic Journal of Nawroz University, 6(3), 40–45. https://doi.org/10.25007/ajnu.v6n3a76.
[11] Oder, I.J.D., Oder, J.D., Cronic, K.J., Sommers, S.M. and Warner, D.W., Shift4 Corp, 2011. Secure payment card transactions. U.S. Patent 7,891,563.
[12] Asaad, R. R., Abdulrahman, S. M., & Hani, A. A. (2017). Advanced Encryption Standard Enhancement with Output Feedback Block Mode Operation. Academic Journal of Nawroz University, 6(3), 1–10. https://doi.org/10.25007/ajnu.v6n3a70.
[13] Data Reportal, (2020) Digital 2020: Global Digital Overview, https://datareportal.com/
[14 Asaad, R. R. (2020). Implementation of a Virus with Treatment and Protection Methods. ICONTECH INTERNATIONAL JOURNAL, 4(2), 28-34. https://doi.org/10.46291/ICONTECHvol4iss2pp28-34