Ethical reflection

Since the introduction of social media in the late 1990s, social media has only increased in popularity over the last 12 years, with 3.484 billion users recorded as of early 2019 (Kemp 2019). However, with the ever-growing engagement in social network websites and applications, there leave gaps in data privacy.

Anecdotal evidence has proven that prolonged use of social media has links with multiple mental health issues such as anxiety and depression. As stated in an article by Yubo Hou, Dan Xiong, et. al(2019), with the overdependency and increased usage of technology, namely Social Media, users begin to associate its usage with feelings of euphoria and happiness. The core issue is overdependency, however regardless of overuse, many are unaware of how safe their data really is. Overdependency in social media is one issue, however social media data security is another issue. As stated by Eric Conrad, …Joshua Feldman, in Eleventh Hour(2017), I quote in part one of the Ten Commandments of Computer ethics "Thou shalt not use a computer to harm other people". Though many cyber criminals ignore this part of computing ethics altogether for the interest of their own gain.

One example of cybercriminals disregarding computing ethics is via phishing and social engineering techniques. These techniques, when used on individuals via fake Instagram or Facebook accounts, can illegally obtain users' personal information and data anonymously. Phishing as defined by the web as being a fraudulent social engineering practice where an attacker would send a deceitful message to implant malicious malware or scam an individual of their password and personal information. In the occasional event, a hacker would gain access to an account and in the form of blackmail, will offer the account back in the form of a large sum of money. Often when an account has been stolen, you are able to reset the password using the email address you used to sign up. However recent cases have shown that these malicious attackers would also change the sign-in authentication completely, such as replacing the phone number and email address you would usually do to retrieve an account. However, websites such as Instagram have a feature where you are able to request your account back via ID verification, though because this is automated software, the outcome of getting the account back is never positive.

I do believe there needs to be more control and regulation in regards to verifying someone's identity before signing up for an account. Whether it be verification via passport or photo ID, or more regulations on two-step verifications that many bank websites and applications already use. In addition, there need to be tighter measures that ensure your data is secure. However when it comes to phishing, certain demographics do come into play, and that is susceptibility to phishing attacks. In a study conducted by Algarni, Xu & Chan 2015; Darwish, El Zarka & Aloul 2012; Sheng et al. (2010), internet users between the ages of 18 and 25 were shown to be the most susceptible to phishing attacks. This is due to the generational factor as millennials and generation-z being more engaging in social media and web use. This also stems from social media addiction and overuse of the platforms, resulting in a higher percentage of falling for a phishing scam.

To conclude, I do believe there needs to be big improvements in how social media megacorporation's protect their users information. However some newer platforms are stepping in the right direction at wanting better security for their users, though it is also up to the individual whether they engage knowing the potential risks or not.

References

https://datareportal.com/reports/digital-2019-global-digital-overview

Hou, Y., Xiong, D., Jiang, T., Song, L., & Wang, Q. (2019). Social media addiction: Its impact, mediation, and intervention. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *13*(1), Article 4. https://doi.org/10.5817/CP2019-1-4

Eric Conrad, ... Joshua Feldman, in Eleventh Hour CISSP® (Third Edition), 2017

https://doi.org/10.1016/B978-0-12-811248-9.00001-2

Parker, Heather J., and Stephen V. Flowerday. "Contributing factors to increased susceptibility to social media phishing attacks." *South African Journal of Information Management*, vol. 22, no. 1, 1 Jan. 2020, p. NA. *Gale Academic OneFile*, link.gale.com/apps/doc/A629000138/AONE?u=anon~8aaebac1&sid=googleScholar&xid=d62964ec. Accessed 12 June 2022.