Teenagers: A Social Media Threat Vector

Henry Collier\textsuperscript{1} and Charlotte Morton\textsuperscript{2}

\textsuperscript{1}Norwich University, Northfield, VT, USA
\textsuperscript{2}University of Chester, UK

\texttt{hcollier@norwich.edu}
\texttt{0818685@chester.ac.uk}

Abstract: Social media has grown significantly since the early days. During this time, social media has grown to be a mainstay in most teenagers’ lives. Whether they are on Facebook, Snapchat, X (formerly Twitter), or TikTok, teenagers have fully integrated social media into their lives. Teens tend to post the ins and outs of their lives, sharing sensitive information about themselves to people they know, but also to strangers. Although social media can be used for good, it can also be used by nefarious threat actors to take advantage of teenagers. Social engineers count on their subject’s desire to increase the number of virtual connections, which may increase the endorphin response received when they get “likes”. As such, social engineers create targeting accounts and then try to get as many people to accept them as possible. This increased footprint levitates the chances of a successful social engineering attack. Add to this, when someone shares an abundance of information about themselves, social engineers use this information to target individuals with spear phishing attacks. To further exacerbate the situation, social media uses algorithms to target its users and feed them with a significant amount of information that is not always vetted as being truthful. When someone is influenced by disinformation, it increases their susceptibility by taking away their desire to verify the truth, but rather accept that what they are being told is the truth. This case study examines the dynamics associated with teenagers and their susceptibility to becoming a victim of cybercrime and how social media perpetuates this situation.

Keywords: Social media, Social engineering, Teenagers, Cybercrime, Susceptibility

1. Introduction

The Internet and social media now go hand-in-hand. Social media usage is more common with younger people or teenagers than it is with previous generations. A teenager is someone between the ages of 13 and 19, with adolescence being the transitional stage from childhood to adulthood. However, this can start earlier during the ‘tween’ ages of 9 to 12 or as late as 24 when someone becomes a young adult. For this research, ‘teenagers’ will be individuals between the ages of 13 – 24, as adolescents will be included in this research. This is due to maturity levels changing after the age of 25 (Raymond, 2023).

Digital media is used by many for communication, entertainment, and education. This encompasses social media (Chassiakos and Stager, 2020). Many risks such as data collection of personal information for for-profit companies, cyberbullying and ‘drama’, and inappropriate interactions also occur on social media (Uhls, Ellison and Subrahmanyam, 2017) (Chassiakos and Stager, 2020).

According to a survey of 14-24 year old’s, the negative impacts of social media are increased rates of anxiety and depression, poor body image and sleep, and cyberbullying. Specifically, rates of depression have risen by 70% within the last 25 years (Royal Society for Public Health, 2017). Cross-cutting risks have been highlighted by Livingstone and Stoilova (2021). These risks relate to privacy violations, physical and mental health, and inequalities and discrimination. Research has been highlighting the risks more recently (Goma and Shankar, 2021).

Recommendations to reduce the risks or ‘curse’ of social media include funding and teaching digital literacy in schools starting from Year 1 in the UK, or from the age of 5, and encouraging parents and children to discuss their use of social media to build awareness of the negative aspects of social media (Uhls et al., 2017). However, as teenagers can often pull away from their parents or caregivers, as peer groups become more important, it may not be the easiest of strategies to implement. Teenagers are still developing, and the majority of teenagers have an egocentric perspective. This is a cognitive bias where a teenager assumes that other people share the same perspective as they do. Anxiety can result at this time, along with an importance on peer groups (Psychology Today, 2019). This is where social media can have a major impact on a teenager, and why social media can both be a blessing and a ‘curse’.

2. The Generations

Although there is no defined timeline for each of the 7 generations, as there are slight discrepancies regarding the specific years, we are currently in the Generation of Alpha (Gen A), however, many of Generation Z (Gen Z) fall into this case study’s description of a ‘teenager’. Gen A are usually born after the year 2010 (Cottrell, 2020).
Henry Collier and Charlotte Morton

(Hu, Hu and Hou, 2022). They are considered the children of the Millennial Generation/Generation Y and the siblings of Generation Z (Gen Z). Table 1 provides one timeline of example.

**Table 1: Generation timeline (Cottrell, 2020)**

<table>
<thead>
<tr>
<th>Generation</th>
<th>Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greatest Generation/GI Generation</td>
<td>1901 - 1927</td>
</tr>
<tr>
<td>Silent Generation</td>
<td>1928 - 1945</td>
</tr>
<tr>
<td>Baby Boomers</td>
<td>1946 - 1964</td>
</tr>
<tr>
<td>Generation X</td>
<td>1965 - 1980</td>
</tr>
<tr>
<td>Millennial/Generation Y</td>
<td>1981 - 1996</td>
</tr>
<tr>
<td>Generation Z/iGen</td>
<td>1997 - 2010</td>
</tr>
<tr>
<td>Generation Alpha</td>
<td>2010 - present</td>
</tr>
</tbody>
</table>

Although Gen Z is the first generation to have the ability to be constantly connected via phones, tablets, computers, etc., and are therefore considered ‘digital natives’ (Smith, 2017) and can be described as technological addicts (Adán López Mendoza et al., 2023), Gen A is the first generation to never know of a time without social media (Cottrell, 2020).

### 3. Social Media

According to the Digital 2022 Global Overview report, the number of social media users is 4.62 billion, which represents 58.4% of the world’s total population. This has increased by approximately 10% since 2021 (Kemp, 2022).

Although social media users, or Online Social Network (OSN) users, use social media for self-identity and expression, they also share their political views online (Royal Society for Public Health, 2017) and therefore shape policy. According to briefing notes from the 2022 CASIS Vancouver West Coast Security Conference, Gen Z and A shape policy via social media platforms, such as TikTok. However, their beliefs and views are shaped by app-based algorithms (Kelshall, 2023).

OSN users happily provide personally identifiable factors such as home address, email address, phone number, date of birth, or relationship status, however, it’s not just cyber criminals who will use this information. Social media companies and third parties will harvest and sell this information (Fire et al., 2014).

India’s Gen Z are more likely to share personal information when they suffer from social isolation anxiety or the fear of missing out (FoMO) (Lyngdoh, El-Manstrly and Jeesha, 2022). In the US, Gen Z spends more than 4 hours per day on social media, compared to 18% of adults (Roberts, 2023) (Figure 1). This was a survey of 13–25 year old’s.

![Daily social media usage (Roberts, 2023)](image)

Figure 1: Daily social media usage (Roberts, 2023)
Gen Z’s mostly use YouTube (Busick, 2023) (Figure 2). Gen Alpha also use YouTube, provided to them by their millennial parents (YPulse, 2023).

There are two types of influencers, the most recent due to the digital age is the social media influencer. The classic influencer is a subject matter expert, such as a solicitor, scientist, or reporter (Lajnef, 2023). Companies employ social media influencers to encourage people to buy what they are selling. There are legitimate ways of marketing to Gen Z and Gen A (Anderson, 2022) (Ehlers, 2023) (Feger, 2023), however, these legitimate ways can be used by cybercriminals to get the ‘attention’ of these generations. There are plenty of market research blogs, analysis etc to help organisations market to the new generations, all of which can be used against Gen Z and A in order to gain personal information.

Millennials, and parents of any Gen Z or A, need awareness and a security mindset, as they openly share information about their children online and allow their children to use social media. Therefore, allowing datafication of their children (Livingstone et al., 2020) (Das, 2023). Algorithmic social media practices pose significant harm to adolescents’ mental health (Raffoul et al., 2023) and although paramount, and should be considered further, this case study does not explore algorithms in depth. Teenagers, adolescents, and their parents’ awareness of algorithms can be described as patchy and uneven (Das, 2023), especially if they do not come from a technical background.

4. Motivation

One theoretical framework that can be used when researching social media users is the Uses and Gratifications theory (U&G) (Ma et al., 2019) (Hu, Hu and Hou, 2022) (Ibáñez-Sánchez, Orús and Flavián, 2022) which was originally used for media research purposes. U&G assumes that individuals, and teenagers in this case, actively choose what they want to consume (Ma et al., 2019). U&G was put into 5 categories of needs (cognitive, self-affirmation, affective, social, and escapism) by Blumer and Katz (1974). There have been many other research studies that apply the U&G theory to the use of the internet and social media. Motivations for using the Internet and social media include information seeking, interpersonal utility, entertainment, passing the time, and convenience (Luo and Remus, 2014).

Social media does have a positive side. In one survey, teenagers surveyed advised that they felt able to express themselves freely, which helped with their self-identity. Additionally, they were able to receive emotional support during challenging times and felt that social media interactions helped them with their in-person, real-world relationships (Royal Society for Public Health, 2017). The obvious benefits to social media, such as the ability for teenagers to build social networks that can provide valuable support and friendship (Uhls, Ellison, and Subrahmanyam, 2017) is why so many teenagers continue to use social media apps such as Facebook, TikTok, Instagram or X.
5. Risks and Threats

Teenagers and their social media habits create a unique opportunity for social engineers and other cybercriminals to take advantage of them. They are a prime target for cybercriminals (Tomczyk and Szotkowski, 2023). When we look at the psychology behind the motivation to use social media as extensively as it currently is, we can see that teenagers are putting themselves at a higher risk of becoming a victim than other age groups. The theory of U&G has been used over the last four decades to understand why people seek out and use media in the manner that they do (Al-Menayes, 2015). From an analytical perspective, it is possible to understand why people feel the need to be on social media, especially teenagers. Social media provides a form of instant gratification that is being sought after by individuals, especially teenagers. Teenagers are particularly influenced by instant gratification that provides them with an endorphin release, simply because their minds have not fully matured, giving them the skills needed to distinguish between a need and a want. Teenagers need to obtain “likes” and to demonstrate that they have a large following, both of which feed a person’s ego, which results in a boost of mood-altering (supporting) hormones in the brain. This environment, where someone is pursuing the positive mood-boosting response to stimuli, creates a situation where logic and reasoning are often put aside in favour of the rush, which can lead to poor decision-making. From a security perspective, this loss of logic and reasoning results in many teenagers becoming victims of cybercrime.

A lack of logic and reasoning results in someone being more vulnerable to being a victim of cybercrime. Everyone is susceptible to becoming a victim of cybercrime (Collier, 2021). After all, susceptibility is the state whereby someone has a high likelihood of being influenced and/or harmed by a particular thing. What makes someone susceptible is built around who that person is, their behaviours, their state of mind, their culture, and their emotions. Another factor in someone’s susceptibility is knowledge and life experience. Individuals who have more life experience and have more knowledge of risks tend to be less susceptible. A teenager’s lack of experience and overall knowledge, paired with their immature minds creates the perfect storm for susceptibility.

Some of the risk factors created by social media that increase susceptibility include influence, inference, manipulation, and social engineering. Each of these risk factors plays a pivotal role in adjusting someone’s susceptibility level. This is not to say that these factors do not exist outside of social media, as they do, but rather it is to say that social media is the perfect pipeline for the risk factors to impact the largest number of individuals at one time.

Social media can influence someone and, in many cases, change that person’s mind. One only has to look at the current state of social movements to see how social media influences people, how it moves them into action, and how at times, it muddles their minds. The Black Lives Matter movement is a great example of this, as it put out the very important message of social justice and urged people to step up and change. As a result of this movement, police forces in the United States have begun changing policies to reduce the likelihood that someone of colour in their custody dies an unnecessary death. Positive change is a good thing, however, it can be counterbalanced by the secondary effects of the change. After the Black Lives Matter movement started, there was an increase in anti-police behaviour and defunding of police initiatives. Everyone knows that there are bad police officers, and these individuals need to be weeded out and removed from the force. However, most police officers simply want to serve their community and be a positive force within the community. Like the Black Lives Matter movement, the Defund the Police movement was fed by various social media platforms, and it grew in a cancerous manner and caused much unrest in urban areas.

Whether it is a social movement, a conspiracy theory, or a political movement, social media has the ability to make it grow and fester. Social media does this through the use of its algorithms that are designed to feed people information. If one believes that aliens landed and the governments are keeping them from the population, and they post this on a social media platform, they will start to be inundated with other feeds from other supporters, which will reinforce their opinion. In these cases, much of the information pushed at the user has not been verified or vetted in any way.

Another area of social media that needs to be understood is how easy it is to infer something about someone that otherwise may be something they don’t want to tell everyone. From the perspective of inference, it is possible to reasonably infer someone’s religious belief system, sexual orientation, and political affiliation simply by viewing their posts. If someone wants to keep something private about themselves, they need to be wary about which posts they “like” or support. Certainly, inference is not something that is guaranteed, and individuals can make incorrect inferences, which can be more damaging than an accurate inference.
In addition to influence and inference, it is important to be aware of how social media platforms manipulate teenagers. Once someone makes a post about something or “likes” someone else’s post, the algorithms within social media are designed to feed them more, and in many cases, they are designed to manipulate someone’s thought process, and change behaviour. This manipulation comes in many forms and can impact a teenager's perception of themselves in a negative fashion (Kleemans, et al., 2018). Marketing companies target individuals in many ways, and one of them is through social media. Since teenagers have established their own global market space, they are often in the direct line of fire from these marketing companies (Tripathi, 2016). One area that marketing companies use to target and manipulate teenagers is through the use of celebrity icons. If the marketing company pays one of the Kardashian sisters to do a thirty-second pitch for their product, and that pitch is then pushed out to millions of teenagers, there is a high likelihood that many of these teenagers will then buy that product, simply because their celebrity icon likes it. This is an example of marketing manipulation through social media. Marketing manipulation is only one area where manipulation takes place on social media.

On the political front, there is clear evidence that nation-state threat actors are working to manipulate the population of democratic states in order to sway their election process and circumvent democracy. The threat actors are targeting teenagers who have recently achieved the age to vote. They rely on teenagers being emotional responders and not doing any fact-checking. This type of manipulation is filled with misinformation, which is another big threat of social media.

Social media is a social engineer’s dream. They have access to millions of people and much of the person’s information, so developing a targeted social media attack is easy for them. This is amplified by the fact that many people, especially teenagers, try and grow their network of friends, which leads to social engineers using fake accounts to become friends with people and then target them. Teenagers often don’t implement basic security controls on their social media accounts, so their profiles are open to the public.

6. **Develop a Secure Mindset**

The security mindset can be defined as the intentional consideration of security implications during the decision-making process, and from the perspective of cyber security, the security mindset is the first layer of defence (Collier, et al., 2023). Humans are not born with a security mindset and therefore need to work to actively develop one (Dutton, 2014). Our security mindsets are built around our experiences and apply to each of us a little differently. There are also different forms of a security mindset. For example, someone who walks into a situation and feels as though they are in danger is demonstrating a security mindset. Some might call this a gut feeling, but in truth, this is just an example of the subconscious mind putting things together and then alerting the conscious mind of danger. This process is something that has developed over the millennia as humans have developed. Since the risks within cyber security are not usually physical threats and therefore may not feel as real as the potential for a physical threat, it is possible to understand why people don’t naturally develop a cyber security mindset.

To start building a security mindset, it is first important to understand who the threats are and where they come from. Social media creates an environment where vast amounts of data can be shared with ease (Tayouri, 2015). With the added psychological triggers that promote dopamine release (a desire for more friends and more “likes”), social media has become a goldmine for the social engineer. They use fake accounts to connect with as many people as possible, and then they can scrape that person’s social media, gathering specific data which results in a more devious form of social engineering attack (Ghafir, et al., 2016) (Tayouri, 2015). Stealing a teenager’s identity is one of the most popular forms of cyber activity cybercriminals take as teenagers do not know which information should be kept out of the public domain (Irshad and Soomro, 2018). Teenagers are extremely susceptible to this threat because teenagers embrace the use of social media and openly post massive amounts of information about themselves, and they tend to accept every friend.

After identifying the threats, it is important to look at how one’s actions support the threat. In the case of teenagers and their use of social media, it is clear that the need to have a dominating presence on social media plays a role in increasing their threat. Due to the underdeveloped mind of a teenager and the fact that they are more influenced by emotion, they are more likely to put excessive information about themselves onto social media platforms and to accept connections with people they don’t actually know (Gopnik, 2012). Additionally, most teenagers are not fully aware, nor implement, appropriate security and privacy settings on the social media platforms.

When an individual understands the threats and how their actions support nefarious threats, it is possible for them to develop the skills needed to support a security mindset. For example, knowing that putting too much
information on social media opens you up to a threat should lead to an individual reducing the amount of information posted. Likewise, knowing that accepting every friend request without first determining if you actually know the person, or if you need to have them in your friend’s group, could result in becoming a victim, should make someone more careful about who is accepted.

Developing a security mindset starts with small steps and as each step is taken, defence becomes a stronger component of one’s thinking. Certainly, a security mindset is not going to be the total solution, but it is a start. The true solution is going to be a combination of human-based and technology-based solutions that work together to protect people and their data.

7. Conclusion

The evidence that teenagers are prime targets on social media is pretty evident. More and more are being learned about the risks associated with young people and social media. One of the most significant reasons why teenagers are targeted on social media by threat actors is to steal their identity. The reason why children and teenagers are targeted by cybercriminals is because they don’t check their credit, and don’t have a full understanding of what should be kept private. Whether one is looking at what motivates a teenager to be on social media, how they act while on social media, or what influencing factors exist, it is clear that more needs to be done to help teenagers develop a security mindset. Until teenagers become fully aware of how their actions can put them in harm’s way, and until they actively work to become more secure in their actions, teenagers will continue to be prime targets for social engineers.

References


