

Cybersecurity for children: an investigation into the application of social media

Victor Chang, Lewis Golightly, Qianwen Ariel Xu, Thanaporn Boonmee & Ben S. Liu

To cite this article: Victor Chang, Lewis Golightly, Qianwen Ariel Xu, Thanaporn Boonmee & Ben S. Liu (2023): Cybersecurity for children: an investigation into the application of social media, Enterprise Information Systems, DOI: [10.1080/17517575.2023.2188122](https://doi.org/10.1080/17517575.2023.2188122)

To link to this article: <https://doi.org/10.1080/17517575.2023.2188122>



© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.



Published online: 15 Mar 2023.



Submit your article to this journal [↗](#)



Article views: 177





View related articles [↗](#)



View Crossmark data [↗](#)

Cybersecurity for children: an investigation into the application of social media

Victor Chang ^a, Lewis Golightly^b, Qianwen Ariel Xu^a, Thanaporn Boonmee^c
and Ben S. Liu ^d

^aDepartment of Operations and Information Management, Aston Business School, Aston University, Birmingham, UK; ^bSchool of Computing and Digital Technologies, Teesside University, Middlesbrough, UK; ^cIBSS, Xi'an Jiaotong-Liverpool University, Suzhou, China; ^dSchool of Business, Quinnipiac University, Hamden, CT, USA

ABSTRACT

The paper discusses cybersecurity for children (particularly teenagers) and focuses on Social Media's impact using a theoretical approach. Many social media users are unaware of their Cybersecurity in Social Media and all-round digital privacy and do not understand the importance of developing privacy through taking both digital and physical measures. We identify seven categories of hacking motivations through multimedia platforms: Emotions, Financial gains, Entertainment, Proficiency for jobs, Hacktivism, Espionage, and Cyber-warfare, particularly for children. As vulnerable people, they can be the principal victims. We explore various methods used for hacking, such as Sexting, Facebook depression, and Influence on buying advertisements. In our findings, we demonstrate that the most critical protection method is to fully understand the digital footprint left behind and its possible consequences. The users should know this as a self-protection mechanism to mitigate security issues before problems occur. It means adopting the same mindset and attitude of protecting oneself in the online world as in the real world.

ARTICLE HISTORY

Received 9 January 2022
Accepted 2 March 2023

KEYWORDS

Social Media; Cyber attacks;
Privacy; Multimedia;
Cybersecurity for children;
Consumer behavior

1. Introduction

1.1. Background

The revolution of communication networks and information technology contributes to the development of various fields, industries, and consumer behaviours worldwide. The critical turning point of this technology is Web 2.0, which is the second stage of development of the World Wide Web. This new version of the web emphasises information sharing and interconnectedness between users (Oztemel and Gursev 2020). In the beginning, social media platforms such as Facebook and MySpace were created as communication tools mainly for young people. However, these social networking sites have become the mainstream communication tools for young people of all age groups over the years of

CONTACT Victor Chang  victorchang.research@gmail.com; v.chang1@aston.ac.uk  Department of Operations and Information Management, Aston Business School, Aston University, Birmingham, UK

© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

development. According to the 2021 Children and parents: media use and attitudes report published by OfCom (UK), 44% of 8–11-year-olds and 87% of 12–15-year-olds use social media apps/websites (OfCom 2021). This demonstrates that social networking sites have overtaken email as a primary communication method among young people (Cardon and Marshall 2015). Like many things in the cyber world, social media does come with many privacy concerns. In a journal entitled 'Big data privacy issues in public social media, Smith et al. (2012) show how the growing capabilities of mobile devices have a correlation with the issues in privacy for users. They examine this in the field of big data and reveal that due to the significant amount of data uploaded daily, it is hard for the users to realise the immediate consequences and the future effects it can have.

As long as internet networking continues to evolve, the foremost essential thing developers have to deal with is the security of using social media (Hiatt and Choi 2016). With a vast amount of information stored and shared online, social media security is becoming more critical than ever. Since all connections on social networks can create unexpected access to personal or business information, it primes third-party to take advantage of the social network by having unauthorised access or launching a phishing attack to steal personal information or other forms of hacking (Das, Karmarkar, and Kamruzzaman 2019). For example, LinkedIn leaked the users' email addresses in 2012, and Facebook was hacked in 2016 and 2018, exposing the personal information of its 50 million users.

This study assesses the security and privacy aspects of social media from a Cybersecurity point of view while focusing on hackers. The paper analyzes various unique motivations of hackers and demonstrates the mindset of why hackers want to attack social media platforms. The paper evaluates social media as a platform and then discusses its risks for attacks and mitigations. This study aims to further understand the causes behind the hackers' behaviours and provide guidance to develop effective countermeasures. This paper aims to study the causes and consequences of security, privacy, and hacking in social media. In order to realise these purposes, this paper uses the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) framework to report on the literature review focused on cybersecurity for children using social media. The paper also highlights research challenges that need to be addressed in the future.

1.2. Research contributions

The research focus discussed in this paper is around safety and cybersecurity for children as the specific age group (focusing on teenagers). An in-depth discussion is conducted on the most typical and significant factors of harm resulting in the inappropriate use of social media. This study can lead to the future development of the following research contributions:

- (1) The paper discusses contemporary issues described in social media around cybersecurity and modern attacks and motivations linked to children and young people. In addition, it analyzes and highlights the dangers of the digital footprint.
- (2) The paper summarises recent statistics around Cyber attacks directed at social media.

- (3) The paper provides original recommendations on Cyber protection applied to younger users to help raise awareness and provide a guide to online safety in social media.

1.3. Research motivations

- (1) The paper is designed to help younger audiences have an awareness of the cyber threat landscape of social media.
- (2) The paper will help children defend themselves against the threat landscape and take precautionary steps in the beginning stages of multimedia use.

The remainder of this paper is organised as follows: [Section 2](#) introduces the systematic literature review protocol followed by this paper. [Section 3](#) provides an overview of social media, including the definition of social media and a brief history of the development of social media platforms. [Section 4](#) provides a discussion on basic security in social media and the risk of privacy issues. [Section 5](#) introduces the hacking and explains the attacks and motivations of hackers. We discuss the implications of our research findings between [Sections 6 and 8](#), including methods and recommendations for privacy on social media. Finally, we conclude our paper in [Section 9](#).

2. Systematic review protocol

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) is a well-known framework for conducting systematic literature reviews that includes four main phases: Identification, Screening, and Inclusion (Moher et al. 2009). We followed the PRISMA protocol to ensure an objective and comprehensive literature search.

We first identified relevant databases, including Scopus, Web of Science, and Google Scholar, which provided a complete literature portfolio. Next, a set of key terms was selected: 'cybersecurity', 'social media', and 'children'. Using these specific terms helped to narrow down the search results and identify relevant articles. In the identification phase, 367 papers were identified using key terms by searching the selected databases for keywords, titles, or article abstracts. After removing duplicates and irrelevant studies, 348 articles were left for the next step.

Throughout the screening step, the following criteria were clearly defined:

- (1) Only English-language articles are included;
- (2) Conference reviews and editorials are excluded.
- (3) Papers that do not discuss the intersection of cybersecurity and social media are excluded.

As a result, 272 articles were excluded for non-compliance with criteria 1 and 2, leaving 76 articles for additional assessment in the screening phase. Three or more researchers assessed each article individually to determine whether the papers actually focused on cybersecurity for children and social media and to evaluate their face validity. The review team evaluated each manuscript based on its relevance to the subject matter, assigning a score from three options: 3 for highly relevant, 2 for partially relevant, and 1 for not

relevant. We retained articles in the dataset that were considered relevant or somewhat relevant by at least three researchers. As a result, 54 were included in the Inclusion phase.

3. An overview of social media usage

Social media is growing to increase privacy and security concerns in the modern world. This is due to the ever-growing factors such as accessibility, usability and how mainstream the activity has been incorporated into our daily habits and lives (Irfan 2018; Mao et al. 2020). Social media knows no discrimination – people of all age groups and ethnic and socio-economic backgrounds can all participate. The question that arises with something we give so much of our time and information to is how much we trust these social media sites.

In recent years, social media has become the main channel for people to communicate with others in their social networks. The users spent a lot of time creating their profiles, updating information, and interacting with other users, such as commenting and sharing. Examples of social media are Facebook, WhatsApp, Messenger, Instagram, and Twitter, among many others used in other parts of the world, such as WeChat, LINE, QQ and Sina Weibo in Asia. There are many kinds of social media platforms for different purposes of use. For example, in a social community like Facebook or WeChat, the main purpose of these social media is to connect with friends. Another platform has different main features, such as YouTube and Tik Tok, for social publishing.

Based on a statistics report on Statista.com (Statista 2020), there are 53 million active social media accounts in the UK alone. The total number of social media users worldwide was 3.6 billion in 2020. In 2021, it increased to 4.66 billion. Figure 1 shows that Facebook has the highest number of active users, with 2.895 million accounts, followed by YouTube at 2.291 million active users, and follows direct message platforms, including WhatsApp, Messenger, WeChat, etc., in this order.

Zhang and Gupta (2018) address these concepts by describing possible attacks and their definitions, including identity theft, spam attacks, malware attacks and many others. They also list the array of reasons that cyber attackers might perform these attacks on the sites and end-users, including Revenge/emotions, financial gains, and even Entertainment. The study concludes by discussing the significance of internet site users being aware of the risks and threats to their financial and personal information and should behave securely online.

Their results are backed by the work of Mendhurwar and Mishra (2021), who argue that one of the most critical challenges preventing further innovation and adoption of emerging technology technologies is the issue of security, trust, and privacy. Additionally, Zhang and Gupta (2018) contribute to the existing knowledge on the subject by discussing the human element of security and privacy and explaining how the end-user traits can significantly impact security alongside the specific traits. The study could explore future work and development opportunities in this area, such as generational challenges for social media users and how security and privacy impact them.

Many professionals believe that the privacy of social media relies on users rather than the site. Alzubaidi (2021) investigated the cybersecurity awareness of people in Saudi Arabia and found that only about 70.8% of participants who had been attacked by

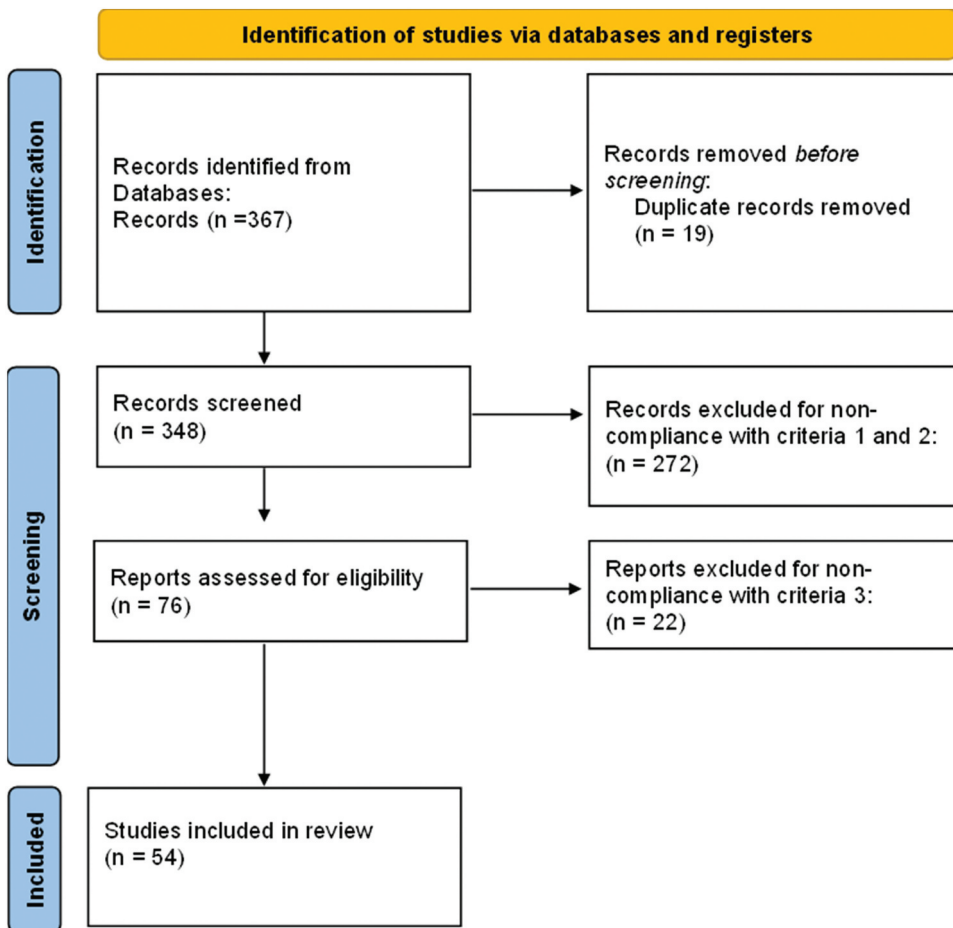


Figure 1. Systematic review protocol.

cybercrimes reported crimes. This number implies a lack of awareness of self-protection against cybercrime.

Vishwanath, Xu, and Ngoh (2018) discuss theoretical methods of protection and motivation theory on Facebook privacy showing how people are responsible for privacy on their profiles and when people have risks associated with privacy concerns. They show that people are more likely to protect themselves from this personal ownership and believe this will prove better privacy standards than conventional social media account privacy settings. The study conveys in detail the Facebook privacy protections in place for the user to use for their security measures. It demonstrates how the users can protect themselves on their own accord. The literature concludes by discussing that users should consider privacy as a cost-benefit evaluation before making important privacy decisions. The authors challenge existing literature by emphasising privacy and security for the user rather than the social networking site. This implies that privacy dangers result from human negligence and omission rather than the result of Facebook's privacy and security standards. The study demonstrates an unconventional method of social media privacy

protection in a step-by-step methodological approach. Thus, the paper can help any Facebook user take action to secure their account.

Lankton, McKnight, and Tripp (2017) discuss methods that social media users breach their privacy and then offer methods to contain their personal information. The research addresses concepts of protection. They mention how limiting the number of self-disclosures that the users perform naturally contains the amount and significance of personal data entering the site. This can be demonstrated by omitting information, such as birth date, gender, and educational information. This works because it cannot be viewed, stolen, or used if the information is not there. The authors convey how the users can decide the variables associated with who can see their social networking site and how the social media site does put that on to the user.

The paper also addresses the challenges associated with the privacy settings use as it does take little effort to become 'friends' with a user on social media, which can grant them access to the information. The study concludes by discussing the findings that older users with the deepest privacy concerns and the lowest trust and technology usage perceptions are most private by having more restrictive privacy settings use, fewer self-disclosures, and smaller network size. The study relates to other studies by exploring the factors that often contribute to a breach of social media privacy.

According to the current literature, several potential reasons why individuals are attracted to cyber attacks can be summarised, including frequent use of public Wi-Fi, using personal information to create passwords, never or rarely changing passwords, lack of education about cyber attack methods, distrust of institutions and failure to report (Alzubaidi, 2021).

3.1. Social media history and development

For the last decade, social media technology has been quickly evolving, making people closer and having more connections. Recently, social media has become the most important channel for communication among people across the world and it also has mobile applications that help users conveniently access it. In this subsection, we will define social media and provide a brief history of social media development.

3.1.1. Social media definition

Social media is a computer-based online social network technology that facilitates information sharing and creates a community. Social media users can generate information and control their privacy within a defined boundary system (Frederic and Woodrow 2012) and examples of popular social media include Facebook, Twitter, MySpace, and Snapchat, to name a few.

3.1.2. Social media development

Social media has become a deep-rooted part of our daily lives. Many people might think it is a relatively new invention, but it started in the late 1990s and began to take shape in the early 2000s. Figure 2 briefly introduces the development timeline of social media. As it shows, the first well-known social media platform 'Six Degrees' was established in 1997.

Since then, the social media platforms or applications we use today have been developing. The remainder of this section introduces the main social media platforms in the history of social media.

The first widely recognised social media site, Six Degree, was launched in 1997, a little over two decades ago. This site allows users to create their own profiles, invite friends, lost family members, create groups, and send messages to other users. At that time, Six Degree attracted about 1 million members who could create profiles and be friends with one another (Heidemann, Klier, and Probst 2012).

Before long, LiveJournal was founded in 1999 as a blog platform allowing users to keep friends by updating their lives, followed by Friendster in 2002 as the first real social media model because it allows users to find their friends in the real world and expand their connection by being friends with their friends' friends (Davis 2010). The website is also used for dating purposes to offer a safe place to meet new people because knowing other people is faster than in the real world. In the real world.

LinkedIn (2022) was introduced in 2003 as the first website that lines up with a business with success in the consumer markets. This social media is still popular among people interested in professional connections and job searches. The main purpose of LinkedIn is

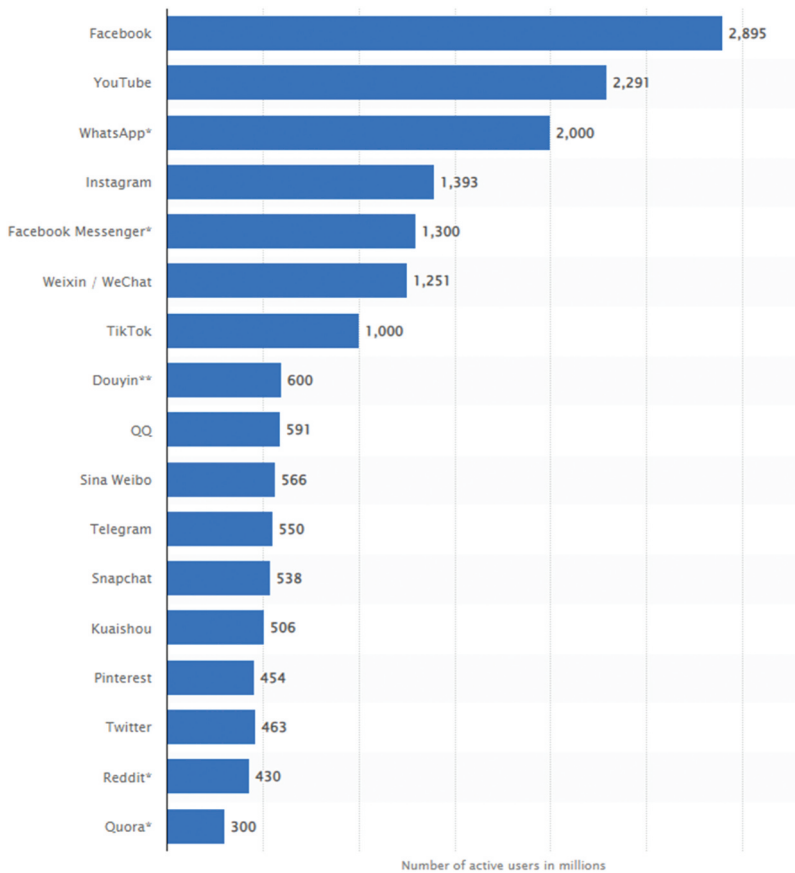


Figure 2. Number of social media active users in 2021 (millions).

to create professional connections between users. The users can post their resumes and private messages for people with a business-orientated mind. It also adds some features for users to have more convenience, such as real-time updates, creating groups, as well as forums for questions and answers.

In the same year, MySpace was also founded in 2003 and became the most popular social network in the US in 2006. It began as a private messenger, but it developed into an instant messenger as time passed. The basic features of MySpace are the same as Friendster with some new features. Users can create their profiles by embedding music, video, or music and sending messages to friends (Mjos 2013).

Most notably, Facebook was launched in 2004, targeting the close community, a college student community at Harvard. When it became an open and free platform, it grew rapidly and became the most popular social network since 2008 (Franz et al. 2019). The user can manage their profile by posting texts, videos, and pictures. Nowadays, it also includes live video in real-time on its platform.

After yet quite different from Facebook, YouTube was made public in 2005. The users can upload and share videos to the public or private. These social media have become popular because users can easily discover new things, greatly impacting the entertainment industry (Stokel-Walker 2019).

Soon after that, Twitter was introduced to the market in 2006 to transmit short messages and make users catch the uptrend quickly. The users can post and interact with limited words, like/dislike opinions, share their thoughts and agree on the agenda with retweets. As of May 2020, the total number of tweets sent per day was around 500 million, although this number has been stabilised since 2014 (Sayce 2020).

While many other platforms have been added to the market since then, Snapchat, launched in 2011, stood out by its design that attracts users to focus on sharing pictures and short videos quickly before the pictures and videos are obsoleted from the platform (Wilken and Humphreys 2021). This social media was focused on person-sharing because users can select which users want to share their messages. After that, it includes stories that allow all of the users' friends to access the users' messages.

4. Cybersecurity issues in social media

While social media platforms evolve rapidly, security and privacy issues continue to be the main challenges for platform developers (Rathore et al. 2017; Laleh, Carminati, and Ferrari 2018). Since this research focuses on the security issues for the personal information of users, we will first explain the basic concept of privacy and security on social media and its risk.

4.1. Basic concepts of security and privacy

In practice, social media platforms have security systems to ensure users' privacy of their information from unauthorised access. Personal data has to be protected appropriately and available only when a legitimate user requires it, referred to as data security. The devout social media platforms apply data security technologies in their products to ensure that digital data on their social media, hardware, software, and hard drives cannot be read by an unauthorised person (Stergiou et al. 2018). Generally, social network

security includes three purposes: integrity, availability, and privacy of information, as shown in [Table 1](#).

Information integrity means that the user data cannot be modified and will remain the same as the original when it was created by the user. The typical attack for information integrity is called man-in-the-middle when the hackers change the data during data transmission.

Data availability refers to that users are ensured to access their data anytime if they have authorised it. It has an attack for this security to harm its services called the denial of service. This attack will disable authorised users' ability to access their data.

Data privacy refers to the purpose of using data on social networks. It could be a proper or legal reason to use this kind of data to include merchants and sell to third parties. Data privacy can also be called information privacy and it applies technologies to determine which data may or may not be shared with third parties (van der Schyff, Flowerday, and Furnell 2020a).

4.2. Risks and issues in social media

As a social media platform is constructed by the relationship between users and the foundation of internet technology and carriers, this can cause problems with the completeness, availability, and confidentiality of internet platforms. Since social media platforms are relatively new yet widely used as new mobile applications, users have reported serious problems with individual privacy and security control.

As the number of social media continues to grow due to the different purposes of these platforms, users keep generating and transmitting content willingly with little awareness of the risk of security and privacy being compromised, making these problems worse. Additionally, the main risk for privacy is that the information is mostly processed in a centralised architecture called the Central Server. As is shown in [Figure 3](#), when freely creating information on social media with a lot of personal identification information, in addition to the internal use of the social media platforms, the users become concerned about the possible identity theft and selling data to third parties (Senthil Kumar, Saravanakumar, and Deepa 2016).

When users' data is sold to third parties or hacked by identity thieves, it causes the users to lose trust in social media because social media fails to protect their information. For example, Facebook has a privacy setting feature that the users can use to control their privacy, but the default is set to the public mode when the new users create their new accounts (van der Schyff, Flowerday, and Furnell 2020a). If the users do not change their security settings, their posts can be

Table 1. Cybersecurity objectives of social media.

Types	Descriptions
1. Integrity	Identities and users' data have to be protected from unauthorized intervention and modification
2. Availability	The users' data have to be available for the owner all the time
3. Confidentiality	Third parties cannot have authorized to access all the users' information and actions via social media

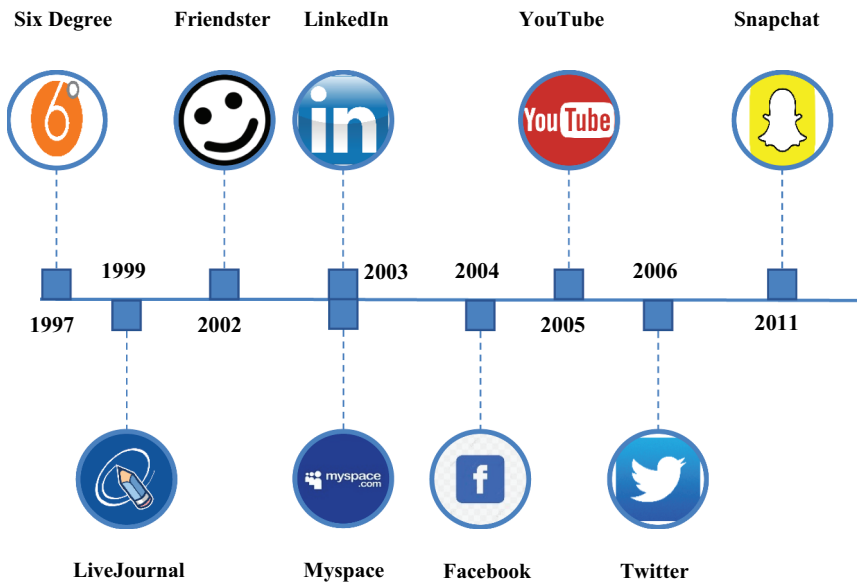


Figure 3. Social media development.

accessed by the public, friends or not, on social media. When enough trusting information such as pictures and identity information has been gathered in a user profile, the hacker can create a fake account to trick your friends and make them believe that account is the actual user. To deal with the risk of security on social media, users have to control the amount of their personal information and how they set the privacy setting.

The biggest problem is that most social media users are unaware of their privacy settings and do not know how to set them. Moreover, most of users do not realise the risk of posting sensitive information on their profiles. Since social media platforms are designed to bring many users together into the same place and interact with one another, the values of the social network lie in its ability to connect and share in openness. However, achieving these values can open up doors for hackers to conduct a variety of cybercrime. Therefore, similar to using other kinds of technology, a security policy is also required for using a social media platform. Despite such, it still has a huge gap that allows hackers to harm users on social media.

Another significant problem with social media is the contradicting nature between Privacy, Security and Accessibility, such that the users can only benefit from two of these three aspects simultaneously. For example, a private and secure account lacks accessibility because the privacy settings will be so high that few others can find the account. However, if an account is private and accessible, it will not be secure, as others can still find information about the account. Finally, if the account is secure and accessible, it will not be private.

According to the National Cybersecurity Centre (NCSC), the best way to keep secure on social media is to understand the user's digital footprint and take measures to protect the user online. For example, this could avoid adding the user's home address and telephone number on the social media page even though the option is available (Ncsc 2020).

5. Hacking attacks on social media

From Figure 3, we can see that one of the security issues that social media users are most concerned about is hacking. It is one that both the users themselves and social media platforms cannot control when attacked by hackers. Actually, there is both unethical and ethical unauthorised access (Figure 4). Ethical hacking is the activity performed by hackers hired by the company to develop a security system and be authorised to hack the network ethically and legally. On the other hand, unethical hacking refers to unauthorised access to the network and seeking benefits from the data. In general, the word hacking causes readers to feel insecure and think it is unethical behaviour. However, social media companies do hire skilful personnel to perform hacking to identify and fix potential security loopholes to improve their security system. Therefore, it should have reliable and applicable regulations for unethical and illegal hacking to protect the vast social media data set. In the following two sections, we will introduce the hacking methods and explore the reasons they do hacking, as shown in Figure 4.

5.1. List of hacking attacks on social media

Operating online and creating a social network with plenty of information, social media attracts numerous hackers who have the intention to benefit from data created in social media by hacking it through various methods (Pybus, Coté, and Blanke 2015; Media Genesis 2018). Our purpose in introducing these hacking methods is to help users understand how hackers operate, so users can pay attention to and take effective measures when suspicious situations occur. In this section, we will describe eleven hacking attacks over social media, including Identity theft, Spam attack, Malware attack, Sybil attack, social phishing, Impersonation, Hijacking, Fake request, Image modification and analysis, Ransomware attacks and Botnet attacks (Figure 4).

5.1.1. Identity theft

Identity theft refers to the stranger or hacker pretending to be the real user (Jain and Gupta 2022). The hacker tries to control the profile of the targeted victim for further accessing the profiles of the victim's contacts. By doing so, the hacker uses the hacked profile in destructive ways to affect the actual users when they activate their accounts.

5.1.2. Spam attacks

Spam attacks occur when hackers know about the victim's communication details and send spam or junk data via emails. Spam emails can increase the victim's cost of using

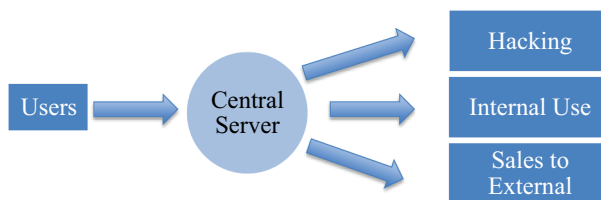


Figure 4. Data Interaction through Central Server.

email and may cause network congestion (Truong, Diep, and Zelinka 2020). Social network administrators use filters to check and mark which emails are spam to mitigate such problems. Thus, the spam report can also help users avoid the messages inside spam emails received in their email inboxes.

5.1.3. Malware attack

Malware attack is the most common type of attack on social media platforms. It begins with the hacker injecting malware scripts into the actual user's account (Stankov and Tsochev 2020). When the actual user clicks on a malicious URL, malware will be installed on the hacker's device, leading the real user to a fake website that tries to steal personal data. Besides, the hacker can access the computer system and disrupt its operation.

5.1.4. Sybil attack

Sybil attack is a type of attack based on fake profiles to damage some functions on social media (Lobo et al. 2020). It can be used for distributing junk information or malware on the network. The solution to prevent this kind of attack is to have a strong authentication mechanism when the users register their accounts.

5.1.5. Social phishing

Social phishing occurs when the hacker tries to steal sensitive information from the actual user through a fake website that looks real or pretends to be an acquaintance of the real user (Jain and Gupta 2022). Typically, a hacker makes a phishing attack by sending spam emails to users. After the users click on the link attached to the spam email, it will link the users to the fake interface of a social media platform. When the users submit their personal information to this fake platform, they become victims because the hackers obtain their data without authorisation and would conduct malicious activities such as financial transfers, etc. Such kind of attack can be mitigated if the user is sensitive to the possible attack and hence carefully examines the incoming data. Details of the four steps in the phishing attack process, namely: Initiation, Execution, User action, and Completion, can be found in relevant literature by those who are interested in these details. In the following, we outline a brief summary of each step (Razaque et al. 2020).

Step 1: In the Initiation step, hackers create fake accounts, mostly on famous social media platforms such as Facebook or Twitter and present them like real websites. After that, the hackers would use malware to hack and create zombie computers for sending large amounts of malicious emails to a lot of real users.

Step 2: In the Execution step, hackers may use a variety of strategies to trap users by attracting the victims to visit their fake social media accounts. For example, hackers may send messages saying, 'We found some insecurity issues in your Facebook account. You should change your password immediately' to lure the victims. Click the attached link that brings the victims to the fake social media (for example, Facebook/Twitter) websites.

Step 3: In the User action step, when the victims are trapped by clicking on the link and accessing the fake website, they would be asked to submit their identity information or other sensitive data. It will be recorded and transmitted to the hackers.

Step 4: The phishing process is completed when hackers obtain personal/sensitive information and then use the data to conduct malicious activities such as financial transfer, which are illegal, unethical and damaging.

5.1.6. Impersonation

In this kind of attack, the hacker tries to create a fake profile pretending to be someone connected to the targeted victim on social media (Sun, Yu, and Zhang 2021). In other words, the hacker tries to impersonate a real-world person. The effectiveness of this kind of attack depends on the authentication techniques that the platform uses for the new register.

5.1.7. Hijacking

Hijacking means the hacker has full control of the actual profile by cracking the login password. Therefore, weak passwords can increase the chance of being cracked and hence attacked by Hijacking. The users should create a strong password for personal security and change it frequently (Moudud-Ul-Huq, Asaduzzaman, and Biswas 2020).

5.1.8. A fake request

A fake request means the hacker would create a fake profile to send a fake friend request to the target user (Jain and Gupta 2022). If the user clicks to accept the request, it will allow the hacker to have more rights and the ability to access target users' information.

5.1.9. Image modification and analysis

The hackers would use facial and image recognition technology to trick their target and the image provided will be linked to the target's profile. This attack can also affect target users' friends and family through the connections between them and the target user (Hassani and Malik 2021).

5.1.10. Ransomware attacks

Ransomware attacks focus on and create a threat to the target user's data files. The hackers would gather data about the victims by encrypting files on an infected computer and then holding the key to decrypt the files until the victim pays a ransom. Additionally, such an attack is blackmail in the cyber world that often links to social media since an attacker generally has complete information about the target. If the files are private and socially undesirable, they could threaten to send them to their friends and family (Richardson and North 2017).

5.1.11. A Botnet attack

A Botnet attack is an automated social media account that automatically creates posts and follows new accounts and new people whenever a specific term is mentioned. These accounts can produce many attacks, such as stealing data, sending spam, and performing a Distributed Denial of Service attack (Orabi et al. 2020).

Information gathering can also be a risk for social media because many users' private information stored on social media can be used by hackers searching for potential victims. This information includes where we live and work, our contact information, and even personal identity information. More details about this issue can be found in Hannay and Baatard (Hannay and Baatard 2011).

A popular method of hacking is a session hijacking attack, which enables the hacker to take over the victim's network session(s). Such a network session is typically on the victim's social media account, giving the hacker access to the victim's social media

account without even needing to know the login credentials. However, there are prevention techniques to mitigate this kind of attack, which can be found in Cashion and Bassiouni (Cashion and Bassiouni 2011).

5.2. Hacking motivations

Seven types of motivation have been identified that motivate hackers to commit cyberattacks on regular users. These are Emotions, Financial gains, Entertainment, Proficiency for jobs, Hacktivism, Espionage, and Cyber-warfare. Each is introduced as follows:

5.2.1. Emotions

Infuriated users of social media may attempt to attack that social media to vent their anger, disappointment, or sense of revenge (Isa 2022). These hackers try to decrease the reputation on social media by blocking their services and making the actual users dissatisfied. If this hacking happened at the organisational level, it could cause a huge impact, such as a huge financial loss.

5.2.2. Financial gains

This is the most common and important reason why hackers attack other social media. The hackers try to obtain others' sensitive personal information, such as bank accounts, then maliciously access their accounts to exploit the financial resources in that account, including stealing and spending money. If applied at the organisational level, this type of practice could include stealing business information of the rivals for unfair competitive advantages in the market.

5.2.3. Entertainment

Some hackers like to gain exciting experiences by hacking social media. They hack other users to build their reputation and make others recognise their hacking skills in hacker society. They did it without expectation of financial or political gain, rather simply enjoying hacking experiences as Entertainment.

5.2.4. Proficiency in jobs

While keeping their platforms secure is the most crucial requirement, many social media firms hire hackers and cyber specialists to improve their security and tackle cyber hackers who want to harm the security of their platforms. It is more efficient to identify the security loopholes in their platforms by asking some experts who have similar skills and logic to hack their platforms and then find solutions to plug the loopholes into preventive action. That makes people with such skills popular due to the high demand in the job market, motivating people to practice their hacking skills by actually hacking.

5.2.5. Hacktivism

Hacktivism in computer networks refers to attacking target victims for political objectives such as promoting free speech, human rights, information ethics, etc. This type of motivation also includes religious reasons, for example, online attacks by religious fundamentalists to protest activities in other countries (ISECOM 2020).

5.2.6. Cyber espionage

This is one of the most important motivations leading hackers to commit cybercrimes. The main purpose is to steal confidential information, including personal information, without the owner's permission at the level of the individual, organisational (e.g. competitors), or national (e.g. other countries). This kind of hacking requires various techniques and software (Buchan and Navarrete 2021).

5.2.7. Cyber-warfare

Lastly, Cyber-warfare hacking is driven by political motivation and the targets are other countries' government websites. The hackers attempt to destroy government communication, financial stability and other things so that the government of another country would not function properly. It actually is a war that happens in cyberspace rather than traditional physical wars fighting on the battleground.

5.3. Scenarios of child cybercrime activities and victims

5.3.1. Identity theft

Children receive and own essential documents. These can include passports and provisional and qualified driving licences. They also receive their national insurance number at the age of sixteen, which, whilst many people, class this age as an adult in the UK system – a person is a minor in law and, therefore, a child until eighteen. Therefore, placing these documents or sharing personal information, such as a national insurance number, with friends and peers can result in identity theft (Manap, Rahim, and Taji 2015).

5.3.2. Spam attacks

Due to children's large social media presence, they can become a victim of a spam attack. Moreover, with website marketing strategies, children do not often read through the terms and conditions of service, meaning they can sign up for marketing ads to be emailed to them. When signing up and agreeing to an illegitimate website, this can cause a spam attack to the child's email address account and cause network congestion (Alazab and Broadhurst 2016).

5.3.3. Malware attack

Children can be particularly susceptible and vulnerable to this method of cyber-attack. This is especially true using a 'baiting' method, as children can be more likely to take the bait than adults, who might give it a more holistic view. An example of this can be when the attacker writes on a USB pen drive 'Class A Final Grades' and leaves it in the corridor. Then a student with any intention, either good or bad, will attempt to view the grades for their purpose, and at that point, a malware attack is executed on the systems (Quayyum, Cruzes, and Jaccheri 2021).

5.3.4. Sybil attack

This attack poses a significant threat to children by hiding behind fake identities on the network. This can be an issue due to the trusting nature of children where they believe that if they are in a system in a legitimate place such as a school or a business, they believe

someone else they have never met will look after the system and stop anything from happening (Shareh et al. 2019).

5.3.5. Social phishing

This attack can be one of the most common that children are susceptible to. This is because of the significant number of social media platforms that children instal on day-to-day devices and networks. One of the reasons children are at greater risk of opening phishing attacks through social media is external factors. For example, when a child is lonely, they are likely to accept friends and message requests from people they do not know and then open messages. Another contributing factor can be financial difficulties, as this can make children open phishing messages that contain a financial reward, for example, portraying they have won money (Fire, Goldschmidt, and Elovici 2014).

5.3.6. Impersonation

Children can fall victim to this attack quickly due to being easily influenced by other people, especially people in places of authority. The method of this attack can come under social engineering, where the attacker will impose on someone different from who they really are and often their intentions. This can be done in a variety of ways with a variety of props. What makes this attack specifically dangerous is that it can be executed in person as well as with technology such as Phishing, Spear-Phishing, Vishing, and Smishing (Guo and Zhang 2020).

5.3.7. Hijacking

Session Hijacking can be highly likely to happen to children due to their typical lack of perspicacity. A Man-In-The-Middle attack can be executed quickly with the right tools and software. This can be especially common in establishments with free customer Wi-Fi, such as a coffee shop or a bus where children will typically look for a 'FREE Wi-Fi' SSID and connect to the first one, which can be the rogue access point where the attack is executed by the malicious actor (Alhayani et al. 2021).

5.3.8. Fake requests

In the modern world and society, fake requests are happening all the time, particularly to children who can have a more relaxed view of people who they socialise with and allow access to information. This attack is typically executed as a 'friend' request through platforms such as Facebook and is so popular is known as 'catfishing' where a person does not appear as they did on the social media platforms in person. For children, this attack can have serious physical consequences but is executed in the medium of cyber (Prabhu Kavın et al. 2022).

5.3.9. Image modification and analysis

This cyber-attack can cause physical harm to children. The attack could work as someone using an image of their family or relations and then tricking them into meeting them at a certain point where physical harm could occur through the medium of computer systems. This has happened many times in the past and can present a danger for children who are active on social media (Hamid et al. 2020).

5.3.10. Ransomware attacks

Ransomware attacks can affect children by being in email attachments or through infected files that are downloaded. This can happen by children attempting to download things at a lower price or where they think they will get a good deal and then when the file is downloaded, it will execute and encrypt the systems, which could be at home or at school, ending up with a ransom for someone in control to pay to get back access to the systems and information (Iovan and Iovan 2016).

5.3.11. Botnet attack

5.3.11.1. Motivations Associated with Children and Cybercrime.

5.3.11.1.1. Emotions. As children are very young and sometimes can lack maturity, they go through some very emotional times with their development and hormonal chemicals in the body. Also, the environmental conditions around children, such as attending school, can cause many emotions and emotional responses, such as experiencing bullying and peer pressure from other children. Both negative and positive emotions can be a driving factor for performing or falling victim to hacking attacks. Often, children do not know how to control their emotions well, and this can cause them to take reckless actions, which can have serious ramifications (Harfath et al. 2021).

5.3.12. Financial gains

With children being young and most of the time being in full-time education, they often lack the ability to earn their own money, which often means that they do not have any or very little. It is also essential to address the society we live in, which is materialistic and competitive, which at times, it can be worse for children than adults (Gandhi et al. 2011).

5.3.13. Entertainment

With government financial shortages and cuts to towns and communities, many children, especially those from low socio-economic backgrounds, often find entertainment in negative actions involving crime and anti-social social behaviour. This is something that can be adapted into cybercrime as time goes on, with computer science education developing in formal curriculum and access to devices becoming more commonplace for young people, including the rise in open-source hacking applications (Rane, Devi, and Wagh 2023).

5.3.14. Proficiency in jobs

Many children are susceptible to misinterpreting positive opportunities as an outcome of hostile actions. This is where young people will see a cybercriminal in the media employed by a reputable company such as GCHQ and be under the illusion that hacking illegally will result in a positive and legitimate outcome. Whilst this may be true for a very select few positive links between criminal behaviour and legitimate elite employment. This can also be an issue as children often look for an easy option for success rather than hard work and dedication, so often, this philosophy is abused as an excuse for discipline (Lim and Thing 2022).

5.3.15. Hacktivism

It is usual for people to act in their own methods of moral and ethical ideologies of what they think is 'right' and 'wrong'. This can be particularly emphasised for young people as they tend to act with more haste than more mature adults. It is likely for children to participate in hacktivism as they will act out of justice and believe that if hacking is done for the right reasons, other people (adults) will agree with them and it will defend them against criminal repercussions (Goswami and Gautam 2022).

5.3.16. Cyber espionage and Cyber-warfare

Whilst these motivations do not apply to children in the same way they apply to adults due to factors such as not being old enough to be employed or go to war, it is important that the previous motivations can lead up to these motivations in later years developing from a child to a young adult (Jha et al. 2021).

6. Motivation for the research

The greatest motivation for the research is to produce and publicly provide an educational paper that has a focus on helping children achieve greater cybersecurity measures whilst online, as it is such a large and essential part of all our lives. With a focus on cybersecurity for a younger age group in society, we aim to contribute to the field from a different angle in this paper by exploring the challenges and solutions to the modern world we will get in with a reliance on technology.

6.1. The negative consequences of using social media

In a medical report at the American Academy of Paediatrics, O'keeffe et al. (2011) discussed how children are an extremely vulnerable audience to social media and what can be a lack of privacy and security in it. As is shown in Figure 5, they identified the following phenomena, including Sexting, Facebook depression and Influence on advertisements on buying:

6.2. Sexting

This is the action of sending or receiving sexually explicit messages, photographs and images through any digital device. In a survey by O'keeffe et al. (2011), they concluded that 20% of teens have engaged in posting nude or semi-nude photographs or videos of themselves. In a study by Low and Khader (2021), there were two key social factors identified in relation to sexting – the first factor is 'Perceived Subjective Norms', where have been highlighted as a key determinant of behaviours – they discuss how the frequency of sexting activity around young people makes the behaviour more 'normal' with how common the action is with their peers. In addition, a common social factor is 'Family Support'. It was found that young people who had more supportive families were less likely to participate in the action of sexting.

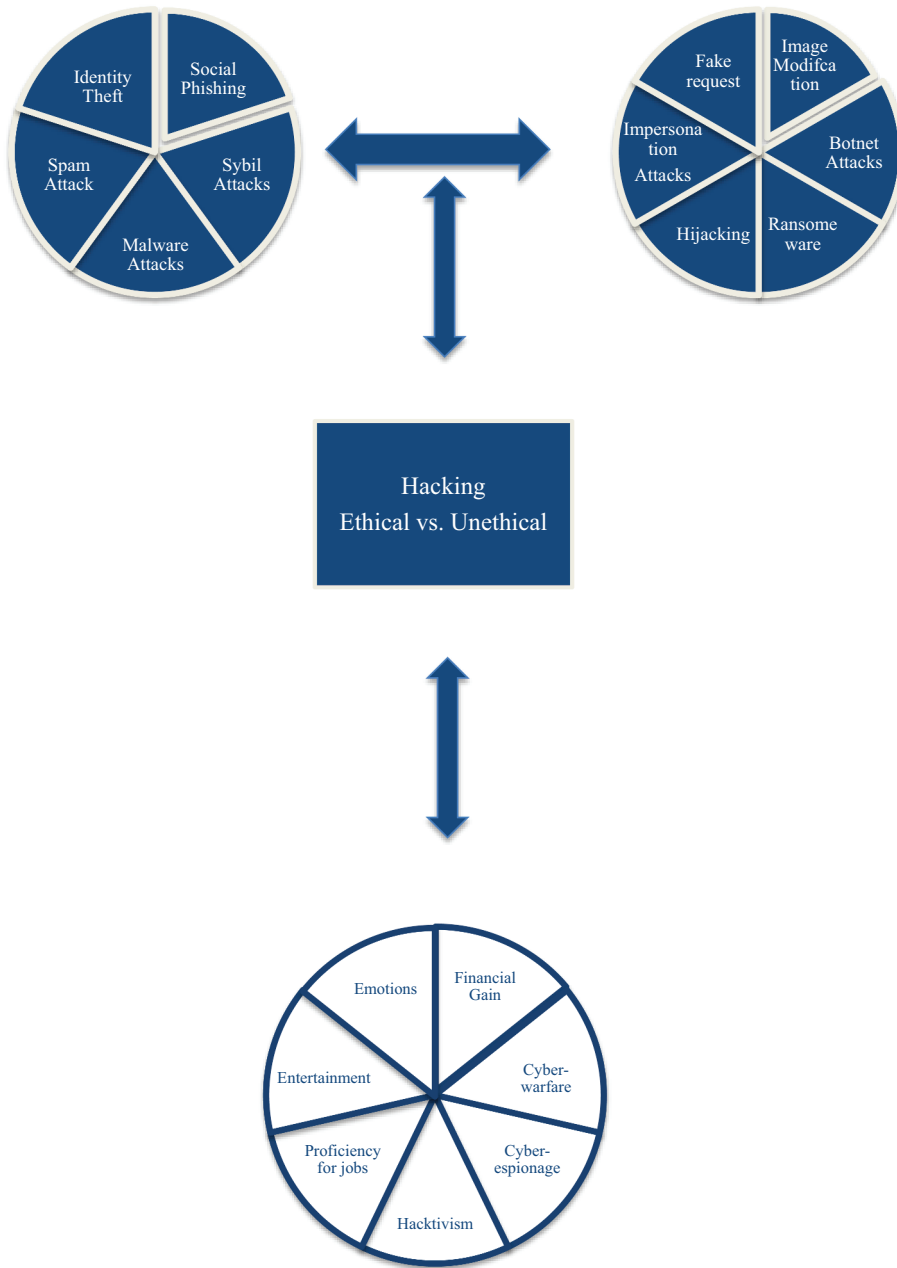


Figure 5. Concept of hacking.

6.3. Facebook depression

This is a mental health condition developed when a teen or young person spends too much time on Facebook or other social media and then shows symptoms of depression. It is thought to be due to the need for acceptance at such a young age and the intensity of the online world might have triggered the need yet unmet by their experience (Madden

et al. 2013). Moreover, in the work of Błachnio and Przepiorka (2016), it has been observed that Facebook addiction can occur without appropriate self-control over the quantity and quality of screen time. They also highlighted the problem with the regulation of emotions, thoughts and behaviours through being met with negative situations that can occur when using the platform – one of the most significant being Facebook intrusion, where someone's account is hacked.

6.3.1. Influence of advertisements on buying

This is the process of how social media sites display related advertisements based on the users' browsing history. These advertisements often are demographic-based, such as on a specific age group. While this strategy affects the buying tendencies of preadolescents and adolescents, it also impacts their perception of what normal buying behaviour should be. When using social media platforms, one of the most common negative aspects that can happen is cyberbullying, which is often reported among young people using the site. In an effort to combat cyberbullying, Kumari et al. (2020) proposed a novel framework that can identify cyberbullying instances by using a new integrated representation of images and text. This works by using a Convolutional Neural Network (CNN)-based multi-model system which can learn the integrated representation of posts (containing image and text), which can classify an individual post as a cyber-bullying or not cyber-bullying.

These three phenomena show that social media risks also apply to a large proportion of its audience ranging from the dangers of child sexual abuse to mental health disorders and behavioural manipulation affecting the users' lives. Fortunately, they can be mitigated by privacy restrictions and parental monitoring.

7. Recommendations for cybersecurity in social media

As discussed in Section 3, most social media users are unaware of the risk of posting sensitive information on their profiles. Even if some recognise the risk, they do not know how to protect privacy and security issues from their own perspective. As shown in Figure 6, we suggest three main methods for users: understanding the risk of leaving a digital footprint behind, using appropriate privacy settings, and avoiding adding home addresses and telephone numbers.

7.1. Children and teenagers

In the United Kingdom, a person who is under 18 years old is classed as a minor in the law. Children as an age group are seen as vulnerable in the United Kingdom. There are laws to protect children as a vulnerable group. This vulnerable factor is increased with the online facilities given to children, as mentioned earlier in the paper. There can be many environmental factors that can trigger danger in cyberspace, as seen from CEOP's website, 'What can make young people vulnerable online' (2022), which includes the following:

- Low self-esteem.
- Questioning sexual orientation.
- Risk-taking behaviour online.

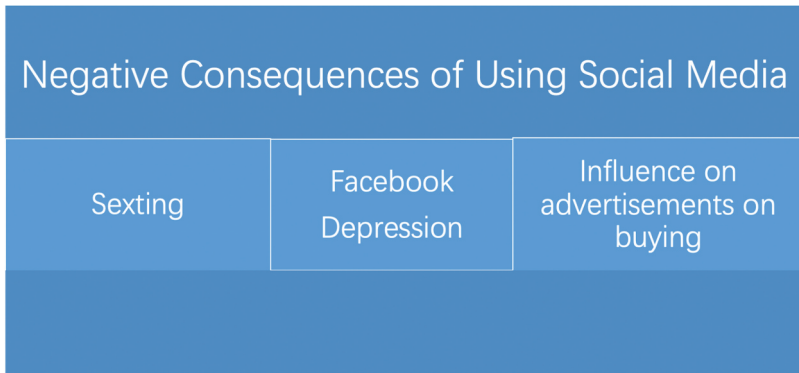


Figure 6. Negative Consequences of Using Social Media for Children.



Figure 7. Methods of protecting privacy and security online.

- Previous victimisation.
- Problems within the family.
- Lack of parental involvement in online life.
- Social isolation.
- Difficulties with friends.
- Problems at school.

7.2. *The digital footprint*

The digital footprint is the content of information produced and observed under the profile of a user, typically on a social media platform, but this can also be on the wider internet. This content can be anything that makes it so dangerous because it can be open to interpretation by different users. Once it is under the profile (typically through posting or sharing), it can be very difficult to remediate the viewing of content attached to a user's profile. An example of this could be if the user had an old profile and now does not have access to it or if the user shared it and people have been able to see it and link the content to the user before they had the chance to unattached themselves from the content.

As shown in [Figure 7](#), the most important protection method for the users' privacy on social media is fully understanding the digital footprint left behind. The users should know this or be educated to know this as a self-protection mechanism that can mitigate security issues before problems occur. It means adopting the same mindset and attitude of protecting oneself in the online world as in the real world. This problem is particularly severe with children while they understand how to use social media and the consequences of the footprint left behind. One of the main reasons for such a phenomenon is the significant time children spend on social media.

In the recent work of Buchanan et al. (2018), we can observe a study on young people's ability to be aware and stay away from the digital footprint and create and develop a positive digital footprint to deal with negative cybersecurity issues. The study highlighted the 'immediacy' and 'longevity' of digital engagement should become assets to the user rather than threats. With this in mind, there is a clear opportunity for young people (teenagers) to create a positive online presence that can benefit them in the future rather than create a bad impression – this can also be noticed with the choice of platform. For example, using LinkedIn instead of Facebook can encourage users to showcase professional and meaningful information about themselves.

According to a recent survey by Heike and Durner (2020), the findings of children's internet access and usage were perplexing from the viewpoint of cybersecurity and risk management. The data that we extracted between the years of 2011 and 2018 show that in Switzerland, 97% of females and 95% of males aged between 12 and 19 years old go online weekly. In European countries, 95% of adolescents aged 16 to 19 years old go online daily. In Brazil, 88% of children aged between 13 and 17 years old go online daily. In America, 42% of children aged between 13 and 17 years old update their location settings and 45% of children update their profile photos on social media. The statistics are given to highlight a significant volume of time, access and usage among children (in the teenage category) worldwide and showcase a serious problem for children who are not aware and do not understand the digital footprint they leave behind (Buchanan et al. 2017).

7.3. *Privacy settings*

Privacy settings can be found on every social media application and are designed to give the users the ability to govern who can see their profile, what content they can see on their profile and if they have the ability to contact them (for example, call them or instant message). Privacy settings differ depending on what social media platform users are on, although they are typically unified with the same focus and intent in recent times. In

addition to the effects on children, the digital footprint can also have a long-lasting and potentially damaging effect on adults once they start looking for career opportunities.

McPeak (2013) believes that 'using social media can be a hazard to those who overlook the privacy settings'. Using appropriate privacy settings can mitigate most of the potentially harmful data as the people from whom the user wants to hide the digital footprint will not easily view the user's profile. Additionally, this can also be beneficial when the users forget their passwords or lock their accounts and cannot physically change their digital footprint. Because it should not matter as anyone outside the users' settings could not view their accounts over time and the accounts will fade as their friend lists do not expand.

Many researchers have looked into the main concerns users have with privacy options, which points to the main concern being how users have to keep up with the constant demand of changing privacy settings and self-presentation. In the research of Fiesler et al. (2017), the authors investigate privacy settings and social media content sharing. They begin by discussing the privacy strategies in place in one of the most reputable and mainstream social media sites (Facebook). A method they have established is targeted disclosure, where the user uses different privacy policies for different posts (subjective to what the post is about).

7.4. Personal information

Personal information can be disclosed through social media. This is encouraged by particular social media platforms – for example, Facebook, which prompts users to add their full name, personal profile picture, mobile number, telephone number, and even their home address. Adding this personal information creates a stronger social media profile as we are adding the most information into our profile, making us more social; however, this is the opposite from a cybersecurity standpoint. The last method we suggest is omitting the most private information on the social media page, such as home address and telephone number. Since when hackers get this kind of information, they can identify a person and commit other crimes. Users can efficiently protect themselves online by understanding and recognising the potential privacy and security issues if ignoring their digital footprint. Users should take responsibility and ownership of what they post online and recognise that even privacy policies by social media sites do not fully protect them; therefore, the accountability lies with themselves.

7.5. Recommendations to protect yourself on social media

In this section, the authors provide recommendations for young people to be aware of and protect themselves whilst using social media for the present and future. In the modern world, there is an array of social media sites being used by all age groups to provide connectivity and enhance methods of communication between us as a race, both nationally and internationally. The recommendations we give can be used transcendentally throughout all and any platforms that are used. The first recommendation focuses on being continuous with the digital footprint you will leave when deciding what you present online under your name and image – this can seem like an obvious focus. However, what can seem valid and innocent to yourself can be interpreted differently

by other people (an example of this could be humour). This can also be around discussing workplace activities and/or businesses (an example of this could be discussing elements of your work you are unhappy about) - this can be seen as valid due to it being your profile. However, a future employer can view this negatively as they will not have their business discussed in this way. Finally, be mindful of the factor that when you delete content under your profile, it means it is deleted but not captured – this means that someone can take an image of this and keep the content under your name (an example of this is screenshotting). You should be aware of what content you are sharing and understand that the content reflects you as an individual in all aspects of your life.

We also recommend that when joining a new social media platform, the first thing performed is the exploration of the privacy settings available to users. There are no exact privacy settings to use, but you should be aware of what your options are and what you are happy with other users being able to see and interact with your profile (An example of this is a teacher may not want their students to see their personal profile). Finally, we recommend being cautious of what personal information you give out to the world from your profile. This can be done by understanding what other users need to know about you and what presumptions can be made about you when disclosing personal data (an example of this is deciding to add a workplace or place of education to the profile).

7.6. Privacy issues in data mining

The data mining issue is closely related to the digital footprint left behind by the users. It is how social media companies use the digital footprint to obtain specific user behaviours, such as when and where users interact with their platform from it. Social media companies use this information to insert correct advertisements at more accurate timing for better advertising effects on the viewers. But the methods adopted by the companies are not always transparent. Some companies can share this data with a third party without any knowledge and consent from the users. Barbier and Liu (2011) describe how data mining works with machine learning, information retrieval, statistics, databases, and visualisation. They discuss the significant influence companies can have over the users and the opportunities for data mining that collects in-depth data to understand the users' opinions and understand them on a personal level.

Data mining is a controversial topic because it has effects like a double-edged sword. On the one hand, it helps users suggest specific goods or services advertised based on their personal consumer needs. Besides, it also gives the users a personal shopping experience without taking their time away via automated shopping. On the other hand, some users see it as an intense breach of their privacy when social media companies are dishonest about their data. This was typically compromised when the users agreed to the terms and conditions of the sites or accounts that are too long to read carefully, even just read through. Thus, many users consider it as a method of entrapment.

In the work of Ranjan (2009), data mining is highlighted as a positive technique, particularly noticed in the healthcare sector. They discuss how data collection is a simple process in hospitals and extended care facilities. The information collected is usually of high quality and patients can easily volunteer their information and submit their details due to the streamlined services provided. There are two main advantages to data mining in the healthcare sector: the discovery of new drugs and the prediction of drugs –

two main contributions to the physical and mental well-being of the population, helping us advance medical knowledge as a society.

8. Challenges and limitations

In this section, we will discuss the challenges and limitations associated with the nature of the research and the scientific impact of the application of children to research. Furthermore, we will also discuss the omitted information that, if released to the scientific community, could have benefited this study by extending and providing more clarity on important issues.

8.1. Challenges and limitations of the research

When conducting research in this area, one of the main challenges is the information and data readily available to the scientific community. This study focuses on the dangers and risks to children as the vulnerable application of Social Media. Therefore, examples and data in this area are very limited because of the lack of information released as case studies for children. The most prudent limitation of this research is that some social networking sites are significantly more established than others, and the sites that are more contemporary than others have not been around long enough to fully understand and appreciate the risks to young people despite the fundamental principles in all technology of this kind. Thus, continued investigations into this area are required when more and new data become available.

8.2. Challenges and limitations of the study

The research demonstrates limitations around being able to explore the cyber-attacks and motivations of children in greater detail. Whilst there will be many ethical considerations around children's research and cybersecurity, the research could have been expanded to explore specific children who had committed the cybercrimes mentioned and their individual motivations behind the activity. Cybersecurity has been one of the major concerns among technology users and even non-users concerned about their loved ones using technology. However, hacking has been prevalently occurring, visibly and invisibly. Technology continues to evolve at an ever-faster pace and human beings become insensitive to what is considered wrong at first. The cybersecurity issue deserves frequent and timely revisits.

9. Conclusion

Social media has become a significant tool in our everyday lives as people use it to communicate with friends, family, and colleagues anywhere on earth. The communication is extended from sending messages and photos to Wi-Fi calling. However, with social media providing ease of communication and working as an important tool for users, it has also suffered from concerning attacks from hackers who exploit the precious tool of social media. Digital footprint has been identified as a significant factor that causes harm to both young and elderly people because they do not have a good understanding of what they

have posted that can become publicly available and its significant consequences in the future. In particular, young children are subjected to a higher risk of these attacks because they spend extensive time using social media. Therefore, the consequences can be severe if they do not understand the risk and simply follow the trends to pursue what others do without thinking twice on social media such as Facebook. In this paper, we summarised various types of recent attacks, the motivations behind hackers, the likely targeted victims, and how the targeted victims may mitigate such a risk hence the negative impacts on them in the early years of their life and social development. Based on the descriptive analysis of security and hacking in social media in this paper, future work can be directed to the methods that can improve the security system for reducing security threats. These may be achieved by designing and assessing innovative social network security and teaching young people the risks of using social media. As a result, younger people are less likely to be typical users of sensitive crime. Rather, they become the users who care about the information disclosure and its consequences in their lives.

Acknowledgments

This work is partly supported by VC Research (VCR 0000098).

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The work was supported by the VC Research [VCR 0000098].

ORCID

Victor Chang  <http://orcid.org/0000-0002-8012-5852>

Ben S. Liu  <http://orcid.org/0000-0002-2950-9607>

References

- Alazab, M., and R. Broadhurst. 2016. "Spam and Criminal Activity." *Trends and Issues in Crime and Criminal Justice* 526: 1–20.
- Alhayani, B., S. T. Abbas, D. Z. Khutar, and H. J. Mohammed, 2021. "Best Ways Computation Intelligent of Face Cyber Attacks." *Materials Today*, 26–31.
- Alzubaidi, A. 2021. "Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia." *Heliyon* 7 (1): e06016.
- Barbier, G., and H. Liu. 2011. "Data Mining in Social Media." In *Social Network Data Analytics*, 327–352. Springer US. doi:10.1007/978-1-4419-8462-3_12.
- Błachnio, A., and A. Przepiorka. 2016. "Dysfunction of Self-Regulation and Self-Control in Facebook Addiction." *The Psychiatric Quarterly* 87 (3): 493–500. doi:10.1007/s11126-015-9403-1.
- Buchanan, R., E. Southgate, J. Scevak, and S. P. Smith. 2018. "Expert Insights into Education for Positive Digital Footprint Development." *Scan: The Journal for Educators* 37: 49–64.

- Buchanan, R., E. Southgate, S. P. Smith, T. Murray, and B. Noble. 2017. "Post No Photos, Leave No Trace: Children's Digital Footprint Management Strategies." *E-Learning and Digital Media* 14 (5): 275–290. doi:10.1177/2042753017751711.
- Buchan, R., and I. Navarrete. 2021. "Cyber espionage and international law." In *Research Handbook on International Law and Cyberspace*, 231–252. Edward Elgar Publishing.
- Cardon, P. W., and B. Marshall. 2015. "The Hype and Reality of Social Media Use for Work Collaboration and Team Communication." *International Journal of Business Communication* 52 (3): 273–293. doi:10.1177/2329488414525446.
- Cashion, J., and M. Bassiouni. 2011. Protocol for Mitigating the Risk of Hijacking Social Networking Sites. In *CollaborateCom 2011 - Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing*. IEEE, pp. 324–331. doi:10.4108/icst.collaboratecom.2011.247167
- CEOP. 2022. What Can Make Young People Vulnerable Online?. Accessed Jan 6 2022. <https://parentzone.org.uk/article/what-can-make-young-people-vulnerable-online>
- Das, R., G. Karmarkar, and J. Kamruzzaman. 2019. How Much I Can Rely on You: Measuring Trustworthiness of a Twitter User. *IEEE Trans. Dependable and Secure Comput.* 1. 10.1109/TDSC.2019.2929782
- Davis, K. 2010. "Coming of Age Online: The Developmental Underpinnings of girls' Blogs." *Journal of Adolescent Research* 25 (1): 145–171. doi:10.1177/0743558409350503.
- Fiesler, C., M. Dye, J. L. Feuston, C. Hiruncharoenvate, C. J. Hutto, S. Morrison, P. Khanipour Roshan, et al., 2017. What (Or Who) is Public? Privacy Settings and Social Media Content Sharing. In *Proceedings of the 2017 ACM conference on computer supported cooperative work and social computing*, Portland Oregon, USA. (pp. 567–580).
- Fire, M., R. Goldschmidt, and Y. Elovici. 2014. "Online Social Networks: Threats and Solutions." *IEEE Communications Surveys & Tutorials* 16 (4): 2019–2036. doi:10.1109/COMST.2014.2321628.
- Franz, D., H. E. Marsh, J. I. Chen, and A. R. Teo. 2019. "Using Facebook for Qualitative Research: A Brief Primer." *Journal of Medical Internet Research* 21 (8): e13544. doi:10.2196/13544.
- Frederic, S., and H. Woodrow. 2012. Boundary Regulation in Social Media. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*. ACM Press, New York, USA, pp. 769–778. 10.1145/2145204.2145320
- Gandhi, R., A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante. 2011. "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political." *IEEE Technology and Society Magazine* 30 (1): 28–38. doi:10.1109/MTS.2011.940293.
- Goswami, A. K., and R. Gautam. 2022. "India's Cybercrime, Cybersecurity and Cyber Regulation. In Proceedings of the National Conference On "Cyber Crime, Security and Regulation" (CCSR)- 2022 Greater Noida, India." pp.47–55. doi:10.55662/CCRSbook.2022.
- Guo, L., and H. Zhang. 2020. A White-Box Impersonation Attack on the Faceld System in the Real World. In *Journal of Physics: Conference Series*, Dalian, China. (Vol. 1651, No. 1, p. 012037). IOP Publishing.
- Hamid, A., M. Alam, H. Sheherin, and A. S. K. Pathan. 2020. "Cyber Security Concerns in Social Networking Service." *International Journal of Communication Networks and Information Security* 12 (2): 198–212. doi:10.17762/ijcnis.v12i2.4634.
- Hannay, P., and G. Baatard. 2011. GeolIntelligence: Data Mining Locational Social Media Content for Profiling and Information Gathering. ECU Publications. Accessed Jan 28 2021. <https://ro.ecu.edu.au/ecuworks2011/329>
- Harfath, M., R. Amrith, N. Dulanaka, P. Perera, L. Rupersinga, and C. Liyanapathirana. 2021. Intelligent Cyber Safe Framework for Children. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, USA (pp. 0023–0029). IEEE.
- Hassani, A., and H. Malik. 2021. "Securing Facial Recognition: The New Spoofs and Solutions." *Biometric Technology Today* 2021 (5): 5–9. doi:10.1016/S0969-4765(21)00059-X.
- Heidemann, J., M. Klier, and F. Probst. 2012. "Online Social Networks: A Survey of a Global Phenomenon." *Computer Networks* 56 (18): 3866–3878. doi:10.1016/j.comnet.2012.08.009.

- Heike, V. O., and A. Durner, 2020. International Data on Youth and Media 2020. Accessed Jan 28 2021. <https://www.bronline.de/jugend/izi/english/International%20Data%20on%20Youth%20and%20Media.pdf>
- Hiatt, D., and Y. B. Choi. 2016. "Role of Security in Social Networking." *International Journal of Advanced Computer Science and Applications* 7 (2): 12–15. doi:10.14569/ijacsa.2016.070202.
- Iovan, S., and A. A. Iovan. 2016. "From Cyber Threats to Cyber-Crime." *Journal of Information Systems & Operations Management* 10: 425–434.
- Irfan, A., 2018. The History of Social Media. <https://www.socialmediatoday.com/news/the-history-of-social-media-infographic-1/522285/>
- İsa, A. V. C. I. 2022. "ANALYSIS of DATA SECURITY and CYBER-ATTACK METHODS in DIGITAL CURRENCY." *Mühendislik Bilimleri ve Tasarım Dergisi* 10 (3): 1000–1013.
- ISECOM, 2020. Hacktivism. Accessed Jan 28 2021. https://www.hackerhighschool.org/lessons/HHS_en20_Hacktivism.v2.pdf
- Jain, A. K., and B. B. Gupta. 2022. "A Survey of Phishing Attack Techniques, Defence Mechanisms and Open Research Challenges." *Enterprise Information Systems* 16 (4): 527–565. doi:10.1080/17517575.2021.1896786.
- Jha, M., C. S. Anand, Y. Mahawar, U. Kalyan, and V. Verma, 2021. Cyber Security: Terms, Laws, Threats and Protection. In *2021 International Conference on Computing Sciences (ICCS)*, Phagwara, India (pp. 148–151). IEEE.
- Kumari, K., J. P. Singh, Y. K. Dwivedi, and N. P. Rana. 2020. "Towards Cyberbullying-Free Social Media in Smart Cities: A Unified Multi-Modal Approach." *Soft Computing* 24 (15): 11059–11070. doi:10.1007/s00500-019-04550-x.
- Laleh, N., B. Carminati, and E. Ferrari. 2018. "Risk Assessment in Social Networks Based on User Anomalous Behaviors." *IEEE Transactions on Dependable and Secure Computing* 15 (2): 295–308. doi:10.1109/TDSC.2016.2540637.
- Lankton, N. K., D. H. McKnight, and J. F. Tripp. 2017. "Facebook Privacy Management Strategies: A Cluster Analysis of User Privacy Behaviors." *Computers in Human Behavior* 76: 149–163. doi:10.1016/j.chb.2017.07.015.
- Lim, J. W., and V. L. Thing. 2022. "Towards Effective Cybercrime Intervention." *arXiv preprint arXiv:2211.09524*. 10.1016/j.scitotenv.2022.156975.
- LinkedIn, O. 2022 About LinkedIn. Available at: <https://www.umd.edu/experiential-learning-career-success/students/students/resource-handout-files/elcs-linkedin-handout.pdf>
- Lobo, A., Y. Mandekar, S. Pundpal, and B. Roy 2020. Detection of Sybil Attacks in Social Networks. In *International Conference on Computational Data and Social Networks* (pp. 366–377). Springer, Cham.
- Low, J., and M. Khader. 2021. "Sexting in Singapore: An Empirical Study." *Introduction to Cyber Forensic Psychology: Understanding the Mind of the Cyber Deviant Perpetrators*. 2021: 353–373.
- Madden, M., A. Lenhart, S. Cortesi, U. Gasser, M. D. Research, A. S. Senior, and M. Beaton, 2013. Teens, Social Media, and Privacy. Pew Research Center. Available at: <http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx> (accessed 1.28.21).
- Manap, N. A., A. A. Rahim, and H. Taji. 2015. "Cyberspace Identity Theft: The Conceptual Framework." *Mediterranean Journal of Social Sciences* 6 (4): 595.
- Mao, Y., Y. Zhu, Y. Liu, Q. Lin, H. Lu, and F. Zhang. 2020. "Classifying User Connections Through Social Media Avatars and Users Social Activities: A Case Study in Identifying Sellers on Social Media." *Enterprise Information Systems* 16 (8–9): 1–20. doi:10.1080/17517575.2020.1856420.
- McPeak, A. A. 2013. "The Facebook Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery of Social Media Data." *Wake Forest Law Review* 48: 887.
- Media Genesis. 2018. Social Media Hacking in 2018. Accessed Jan 28 2021. <https://mediag.com/blog/social-media-hacking-in-2018/>
- Mendhurwar, S., and R. Mishra. 2021. "Integration of Social and IoT Technologies: Architectural Framework for Digital Transformation and Cyber Security Challenges." *Enterprise Information Systems* 15 (4): 565–584. doi:10.1080/17517575.2019.1600041.
- Mjos, O. J. 2013. *Music, Social Media and Global Mobility: MySpace, Facebook, YouTube*. New York, USA: Routledge.

- Moher, D., A. Liberati, J. Tetzlaff, D. G. Altman, and P. R. I. S. M. A. Group T. 2009. "Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement." *Annals of Internal Medicine* 151 (4): 264–269. *. doi:10.7326/0003-4819-151-4-200908180-00135.
- Moudud-Ul-Huq, S., M. Asaduzzaman, and T. Biswas. 2020. "Role of Cloud Computing in Global Accounting Information Systems." *The Bottom Line* 33 (3): 231–250. doi:10.1108/BL-01-2020-0010.
- Ncsc, G. U., 2020. Social Media: How to Use It Safely. Accessed Jan 28 2021. <https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>
- OfCom, 2021. Children and Parents: Media Use and Attitudes Report 2020/2021. Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf (accessed 29 November 2022).
- O'keeffe, G. S., K. Clarke-Pearson, D. A. Mulligan, T. R. Altmann, A. Brown, D. A. Christakis, H. L. Falik, et al. 2011. "Clinical Report - the Impact of Social Media on Children, Adolescents, and Families." *Pediatrics*. doi:10.1542/peds.2011-0054.
- Orabi, M., D. Mouheb, Z. Al Aghbari, and I. Kamel. 2020. "Detection of Bots in Social Media: A Systematic Review." *Information Processing & Management* 57 (4): 102250. doi:10.1016/j.ipm.2020.102250.
- Oztemel, E., and S. Gursev. 2020. "Literature Review of Industry 4.0 and Related Technologies." *Journal of Intelligent Manufacturing* 31 (1): 127–182. doi:<https://doi.org/10.1007/s10845-018-1433-8>.
- Prabhu Kavin, B., S. Karki, S. Hemalatha, D. Singh, R. Vijayalakshmi, M. Thangamani, S. L. A. Haleem, et al. 2022. "Machine Learning-Based Secure Data Acquisition for Fake Accounts Detection in Future Mobile Communication Networks." *Wireless Communications and Mobile Computing* 2022: 1–10. doi:10.1155/2022/6356152.
- Pybus, J., M. Coté, and T. Blanke. 2015. "Hacking the Social Life of Big Data." *Big Data & Society* 2 (2). doi:10.1177/2053951715616649.
- Quayyum, F., D. S. Cruzes, and L. Jaccheri. 2021. "Cybersecurity Awareness for Children: A Systematic Literature Review." *International Journal of Child-Computer Interaction* 30: 100343. doi:10.1016/j.ijcci.2021.100343.
- Rane, S., G. Devi, and S. Wagh. 2023. "Cyber Threats: Fears for Industry." In *Cyber Security Threats and Challenges Facing Human Life*, 43–54. Chapman and Hall/CRC.
- Ranjan, J. 2009. "Data Mining in Pharma Sector: Benefits." *International Journal of Health Care Quality Assurance* 22 (1): 82–92. doi:10.1108/09526860910927970.
- Rathore, S., P. K. Sharma, V. Loia, Y. S. Jeong, and J. H. Park. 2017. "Social Network Security: Issues, Challenges, Threats, and Solutions." *Information Sciences* 421: 43–69. doi:10.1016/j.ins.2017.08.063.
- Razaque, A., M. B. H. Frej, D. Sabyrov, A. Shaikhyn, F. Amsaad, and A. Oun 2020. Detection of Phishing Websites Using Machine Learning. In *2020 IEEE Cloud Summit*, Harrisburg, PA, USA. (pp. 103–107). IEEE.
- Richardson, R., and M. M. North. 2017. "Ransomware: Evolution, Mitigation and Prevention." *International Management Review* 13 (1): 10.
- Sayce, D., 2020. The Number of Tweets per Day in 2020. Accessed Jan 28 2021. <https://www.dsayce.com/social-media/tweets-day/>
- Senthil Kumar, N., K. Saravanakumar, and K. Deepa. 2016. "On Privacy and Security in Social Media – a Comprehensive Study." *Procedia Computer Science* 78: 114–119. doi:<https://doi.org/10.1016/j.procs.2016.02.019>.
- Shareh, M. B., H. Navidi, H. H. S. Javadi, and M. HosseinZadeh. 2019. "Preventing Sybil Attacks in P2P File Sharing Networks Based on the Evolutionary Game Model." *Information Sciences* 470: 94–108. doi:10.1016/j.ins.2018.08.054.
- Smith, M., C. Szongott, B. Henne, and G. Von Voigt, 2012. Big Data Privacy Issues in Public Social Media. In *IEEE International Conference on Digital Ecosystems and Technologies. Presented at the IEEE International Conference on Digital Ecosystems and Technologies*, IEEE, Italy. 10.1109/DEST.2012.6227909

- Stankov, I., and G. Tsochev. 2020. "Vulnerability and Protection of Business Management Systems: Threats and Challenges." *Problems of Engineering Cybernetics and Robotics* 72: 29–40. doi:10.7546/PECR.72.20.04.
- Statista, 2020. Social Media & Users-Generated Content. Accessed Jan 28 2021. <https://www.statista.com/topics/1164/social-networks/>
- Stergiou, C., K. E. Psannis, T. Xifilidis, A. P. Plageras, and B. B. Gupta, 2018. Security and Privacy of Big Data for Social Networking Services in Cloud, *Presented at the IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, Honolulu, HI, pp. 438–443. 10.1109/INFOCOMW.2018.8406831
- Stokel-Walker, C. 2019. *YouTubers: How YouTube Shook Up TV and Created a New Generation of Stars*. Kingston upon Thames, Surrey, United Kingdom: Canbury Press.
- Sun, X., F. R. Yu, and P. Zhang. 2021. "A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs)." *IEEE Transactions on Intelligent Transportation Systems* 23 (7): 6240–6259.
- Truong, T. C., Q. B. Diep, and I. Zelinka. 2020. "Artificial Intelligence in the Cyber Domain: Offense and Defense." *Symmetry* 12 (3): 410. doi:10.3390/sym12030410.
- van der Schyff, K., S. Flowerday, and S. Furnell. 2020a. "Duplicitous Social Media and Data Surveillance: An Evaluation of Privacy Risk." *Computers & Security* 94: 101822. doi:10.1016/j.cose.2020.101822.
- Vishwanath, A., W. Xu, and Z. Ngoh. 2018. "How People Protect Their Privacy on Facebook: A Cost-Benefit View." *Journal of the Association for Information Science and Technology* 69 (5): 700–709. doi:10.1002/asi.23894.
- Wilken, R., and L. Humphreys. 2021. "Placemaking Through Mobile Social Media Platform Snapchat." *Convergence* 27 (3): 579–593. doi:10.1177/1354856521989518.
- Zhang, Z., and B. B. Gupta. 2018. "Social Media Security and Trustworthiness: Overview and New Direction." *Future Generation Computer Systems* 86: 914–925. doi:10.1016/j.future.2016.10.007.