# Cybersecurity and Cyberthreats in Social Media

**Agnieszka Orłowska**
University of Technology and Economics in Warsaw, Poland.
Email: agnieszka.orlowska@uth.edu.pl

**Keywords:** Social Media, Cyber Security, Threats, Propaganda, Privacy.

**Article History**
Received on 15th October 2022
Accepted on 30th November 2022
Published on 26th December 2022

**Cite this article**
Orłowska, A. (2022). Cybersecurity and Cyberthreats in Social Media. *Humanities & Social Sciences Reviews*, *10*(6), 45-48. https://doi.org/10.18510/hssr.2022.1067

## Abstract

**Purpose of the study:** This study aimed to explore cyber-security and cyber threats in social media. It includes an analysis of how social media is used as a tool for cyberattacks, the kinds of cyberattacks, and what people are doing to prevent them.

**Methodology:** The paper was prepared using the critical literature review method, mainly in cybersecurity and cyber threats in social media.

**Main findings:** Cybersecurity experts have warned that social media sites like Facebook, Twitter, and Instagram are particularly vulnerable to cyber-attacks because they are used extensively by companies and governments to distribute propaganda, to launch cyberattacks and are full of personal information (like passwords) that can be valuable to criminals.

**Application of the study:** The presented article refers to cybersecurity and cyber threats in social media. It implies reflections in such scientific fields as, among others, security sciences.

**The study's originality:** The study identifies cyber security measures used to handle the identified threats.

## INTRODUCTION

Social media has become an essential part of our lives, and as such, it is constantly targeted by cybercriminals. Cybersecurity concerns around social media have surged in recent years as cybercriminals have taken advantage of the platform's broad reach and ease of use. Social media platforms are a powerful tool for communicating and networking with others, but they also present a few cybersecurity risks. With so many people using social media to share personal information, it is no wonder that cybercriminals are interested in exploiting these vulnerabilities. This article will discuss some of the most common cyber threats and how to protect ourselves. We will also cover some of the best ways to stay ahead of the curve in cybersecurity. Cybersecurity and cyber threats are significant issues, and social media is a primary source of exposure. Social media platforms like Facebook, Twitter, and Instagram are excellent sources of information for businesses and individuals. However, with so much online communication, we must be vigilant about cybersecurity threats and take steps to protect ourselves online.

One way to do that is by using safe browsing practices. Please ensure we always use up-to-date browsers (Chrome, Firefox, Safari), install the latest security patches on our computer, and keep an eye out for suspicious activity or links in messages or posts. Do not share personal financial or login details with anyone we don't know well - expose ourselves to unnecessary risk if something happens to them! Another major step is protecting our data. Always store passwords encrypted on a secure device (like a USB drive), use strong passwords that are difficult to guess (12 + characters), change them regularly, and never reuse the same password at more than one site.

Finally, beware of phishing attacks - phoney emails that look like they come from trusted companies but contain malware attachments disguised as documents or images intended to steal our login credentials. Social media platforms like Facebook, Twitter, and Instagram can be a significant security threat to businesses (Lande, Puchkov & Subach, 2020). A study by the Ponemon Institute found that 56% of small businesses have been victims of cyberattacks in the past two years. Social media platforms are great for sharing information and connecting with customers and clients. However, they also allow criminals and hackers to share malicious content quickly and easily (Herath, Khanna & Ahmed, 2022). This harmful content can spread like wildfire on these platforms, damaging brands and individual users.

Facebook, Twitter, etc., have recently played a key role in user communication. The power of individuals to share information with millions of others is a social media dilemma for corporations. In addition to allowing anybody to publish commercially sensitive information, social media makes it impossible for security staff and cyber specialists to secure enterprises and people. Attacks like denial of service may prohibit or impede legitimate user access to a system. Such assaults are rising at an alarming pace (Khan, Ikram, Murtaza & Asadi, 2021). Cyber thieves steal a person's financial, personal, or confidential information using cyber theft or espionage. Cybercriminals use botnet malware to control computers (Khan, Ikram, Murtaza & Asadi, 2021).

The hackers' tenacity and weakness are cyber defences. New dangers and problems arise with IoT, Big Data, etc. Spear phishing is also on the rise, which involves installing malware on a user's computer and obtaining personal data. The deployed virus may encrypt network drives, databases, and backups, harming the target enterprise (Lande, Puchkov & Subach, 2020). Malware may be spread via website advertising. According to intelligence agencies, state actors are increasingly exploiting digital technologies to achieve strategic goals and resolve or promote conflicts.

Cyber thieves attack people and organizations with phishing emails and install viruses. This may also spread through hacked or exploited websites. This ransomware encrypts crucial data, inflicts software harm, and displays criminal messages. Some hospitals or care institutions are targeted, where continuity is vital (Lee, 2021). The ransom rate also varies. The media may propagate misleading information. Just as harmful is information. Social media fake information propagated by the media is an emerging danger. In Global Risks, the WEF Report 2013 Now, cybercriminals may use armed social media sites and data most significant data breaches a few years ago. Example: LinkedIn was a valuable instrument for surveillance and social engineering, The cybercriminals used (tactics) Daily, and social network security vulnerabilities grew. Misuse of social media involves information leakage and privacy issues (Lee, 2021). It always harms innocent consumers. In addition, internet scammers, Predators prey on weaknesses, utilizing social media and creating harm. Improved technologies and strategies target social media users who cannot confirm or address privacy and trust concerns.

Social media is one of the most popular platforms for exchanging information and ideas, making it a prime location for hackers to launch attacks. Social media platforms are designed to make it easy for users to share information and insights with friends and followers. However, this also makes them vulnerable to cyberattacks. Social media platforms are among the top targets of hackers because they contain a lot of personal and sensitive data. As social media platforms become more popular, they are also becoming more vulnerable to cyberattacks. This is because social media platforms rely on user-generated content (UGC) for their popularity and advertising revenue. UGC often has sensitive information such as passwords, credit card numbers, and other personal data. As a result, social media platforms are constantly at risk of being hacked and data stolen. Given these findings, it's no surprise that many companies are taking measures to increase their security and protect their users' data. Some have developed distinctive features to help users keep track of their security settings and protect their accounts from abuse. Others have launched educational campaigns to educate people about the dangers of online fraud and how to stay safe online.

## SOCIAL MEDIA PLATFORMS AND CYBERSECURITY AND CYBER THREATS IN SOCIAL MEDIA

Social media has revolutionized the way we communicate and connect. However, it also poses several cyber threats to businesses and individuals. Cybersecurity experts warn that social media is one of the most vulnerable points for hackers due to its widespread use by organizations and individuals (Thakur, Hayajneh & Tseng, 2019). Social media platforms are constantly changing their algorithms which can impact search results. Sharing content on Twitter or Facebook can result in an exponential increase in followers or likes. Private messages sent through Messenger or WhatsApp can be accessed by anyone with access to the user's account, etc. As a business proactively protects its online assets from malicious actors, it can mitigate some risks posed by social media usage (Lee, 2021). By implementing proper security measures such as password protection for accounts, firewalls protecting data against attack (both external & internal), encryption of sensitive data before transmission across networks, etc., our organization can ensure that its digital footprint is always secure.

Cyber threats have become a significant issue today. Social media platforms are incredibly versatile tools that can be used for good, but they can also be abused by criminals and terrorists to spread their message or cause damage. Here are some of the most common cyber threats:

- Hacker attacks: Hackers use social media platforms to collect information about company rivals, customers, and other valuable individuals. They then use this data to launch sophisticated hacker attacks (Lindsay, 2015).
- Phishing frauds: Phishers create fake websites that look like legitimate brands (like Facebook or Google). Once someone clicks on the link, phishers install malware on their computer to steal personal information (like bank account numbers) or financial records.
- Fake news: Fake news is any content online that is deliberately false and intended to deceive readers. It may originate from official sources (government propaganda agencies), unofficial sources (Satire sites), or even automated accounts operated by spammers and scammers looking for links back to their websites (Lindsay, 2015).

Cyber threats have raised awareness among businesses and employees about how social media can be used maliciously. To stay safe online, users need to understand cyber-crimes dangers and take simple steps like using strong passwords and not sharing personal details online (Thakur, Hayajneh & Tseng, 2019).

Social engineering attacks are a type of cyberattack that involve exploiting vulnerabilities in social networking sites, email servers, or other systems where users share personal information. Attackers use this information to access user accounts, passwords, and other sensitive data. There are several diverse types of social engineering attacks. Still, some of the more popular ones include phishing attacks (sending unsolicited emails with links that lead to malicious websites), spear phishing (sending fake emails with links that direct victims to spoofed websites), and password theft through sophisticated hacking techniques (Lindsay, 2015). The best way to stay safe from social engineering attacks is to be aware of our surroundings and take precautions against being tricked into sharing personal information. Be sure not to click on unfamiliar links in an email message - instead, go directly to the website. The site's security policy should list specific steps readers should take if they believe they have been victimized by fraud or attack (Park & Kwon, 2021). It is also important to regularly update our antivirus software and firewall protection to protect us against all potential threats.

Social media platforms are an excellent way to stay connected with friends and family, but they also come with risks. Our social media accounts may be accessible from anywhere in the world, which means that our personal information (name, email address, etc.) is vulnerable to theft. In addition, social media can be used for cyberbullying or other malicious activities. To protect ourselves from these mobile security risks, take the following steps:

- Use strong passwords: Make sure our passwords are at least eight characters long and include unique symbols and letter combinations. Do not reuse passwords across different websites or services.
- Protect our phone privacy: Do not disclose personal information such as our Social Security number or bank account numbers on social media platforms. Only post information that we would feel comfortable sharing publicly online.
- Enable two-factor authentication: This step adds an extra layer of protection by requiring users to enter other information (like a code sent via text message) before accessing their account. Two-factor authentication makes it harder for someone else to access our account without first gaining access to both of our devices.

Social networking sites (SNSs) are a prime target for cybercriminals who want to exploit people and businesses. Social media networks ranked the second most fashionable way hackers compromised companies in 2017. That is according to a study by IBM security. One of the main reasons social media networks are so vulnerable is that they allow users to easily share personal information, such as their addresses, phone numbers, and email addresses (Park & Kwon, 2021). Also, since SNSs are built on user-generated content, attackers can find valuable intelligence by scanning public profiles and comment sections.

As long as our social media site is up to date with the latest security patches and we take basic precautions such as using strong passwords and not sharing sensitive data online, you're unlikely to experience any severe financial losses from a cyber-attack. However, if our site is hacked or contains viruses, you may risk identity theft or fraud perpetrated via online platforms like Facebook or Twitter.

There has been an increase in social media cyberattacks, and spam accounts are one of the latest targets. What is a spam account? A spam account is a Twitter or Facebook user created solely to send unsolicited messages (spam) to other users. These messages often contain links to malicious websites, coupons for fake products, or other frauds. Spammers use social media platforms to reach a large audience quickly - typically within minutes of creating their profile. Once they have our email address and other personal information, they can send you unwanted emails directly from that account at any time! This attack wastes our time and can cost you money if you fall victim to fraudulent schemes.

How can we prevent ourselves from becoming a target for spammers on social media? The best way to avoid becoming a target for them is to be aware of the warning signs and act immediately when you see them. Here are some tips: Check the legitimacy of all profiles we're considering following - make sure that the person exists and isn't simply using another person's name or picture without permission. Also, verify their timeline - look for recent posts that mention specific brands or commercial products, etc., and do not blindly follow any strangers into scam territory (van der Walt, Eloff & Grobler, 2018). It's worth underlining - don't share personal information such as our login credentials or bank details online.

## CONCLUSIONS

Amidst growing cyber threats, it is no surprise that cybersecurity companies see a surge in demand for their services. These experts help businesses mitigate some of the risks of social media usage. For example, keeping important passwords and tokens such as logins or passwords safely secured can go a long way in ensuring the security of our business's digital assets. Cyberattacks are not just a part of the past. They continue to haunt social media users and companies alike. The great way is to harden our cybersecurity defences and follow some basic rules, such as changing our passwords regularly and using strong passwords that aren't easy to guess.

Cybersecurity should be taken seriously because it can directly impact a company's business performance. Cybersecurity experts warn that social media is one of the most vulnerable points for hackers. Social networks are frequented by employees, customers, partners, suppliers, and others who may have access to sensitive information. Businesses can mitigate some of the risks posed by social media usage by protecting their online assets. Social media platforms are an excellent way to stay connected with friends and family, but they also come with risks.

To stay safe online, users need to understand the diverse types of cyber crimes and take simple steps such as using strong passwords. Social networking sites (SNSs) are a prime target for cybercriminals who want to exploit people and businesses (Herath, Khanna & Ahmed, 2022). Two-factor authentication makes it harder for someone else to access our account without first gaining access to both of our devices. SNSs ranked as the second most fashionable way hackers compromised businesses in 2017.

There's been an increase in social media cyberattacks, and spam accounts are one of the latest targets. Spammers use social media platforms to reach a large audience quickly. The best way to avoid becoming a target for spammers on social media is to be aware of the warning signs.

## REFERENCES

1. Herath, T., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal Of Cybersecurity and Privacy*, *2*(1), 1-18. https://doi.org/10.3390/jcp2010001
2. Khan, N., Ikram, N., Murtaza, H., & Asadi, M. (2021). Social media users and cybersecurity awareness: predicting self-disclosure using a hybrid artificial intelligence approach. *Kybernetes*. https://doi.org/10.1108/k-05-2021-0377.
3. Lande, D., Puchkov, O., & Subach, I. (2020). System for analyzing big data on cybersecurity issues from social media. *Information Technology and Security*, *8*(1), 4-18. https://doi.org/10.20535/2411-1031.2020.8.1.217993.
4. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671. https://doi.org/10.1016/j.bushor.2021.02.022.
5. Lindsay, J. (2015). Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal Of Cybersecurity*. https://doi.org/10.1093/cyber/tyv003
6. Park, J., & Kwon, H. (2021). Cyberattack detection model using community detection and text analysis on social media. *ICT Express*. https://doi.org/10.1016/j.icte.2021.12.003.
7. Snider, K., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal Of Cybersecurity*, *7*(1). https://doi.org/10.1093/cyber/tyab019.
8. Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber Security in social media: Challenges and the Way Forward. *IT Professional*, *21*(2), 41-49. https://doi.org/10.1109/mitp.2018.2881373.
9. van der Walt, E., Eloff, J., & Grobler, J. (2018). Cyber-security: Identity deception detection on social media platforms. *Computers &Amp; Security*, *78*, 76-89. https://doi.org/10.1016/j.cose.2018.05.015.