Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0036

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

Cybercrime, Social Media, and Student Awareness

Mr. Rajkumar Thaware
Librarian,
Athawale College Of Social Work
Bhandara

Abstract

The rapid growth of the internet and social media has transformed how students live, learn, and connect with others, with platforms like Facebook, Instagram, Twitter (X), Snapchat, TikTok, and WhatsApp becoming central to their daily lives. A 2023 Statista report notes that over 4.9 billion people use social media globally, many of them young people, including students who spend hours online sharing, chatting, and exploring. However, this rise in usage has brought serious risks, particularly cybercrime—illegal activities such as hacking, phishing, and bullying conducted through digital means. Students are prime targets due to their active online presence, trust in social media, and lack of awareness about hidden dangers, such as fake messages or oversharing personal details. This paper explores the nature of cybercrime, its occurrence on social media, and the critical need for student awareness to combat these threats. It highlights practical safety measures, like using strong passwords and avoiding suspicious links, and emphasizes the role of schools, parents, and students working together to build a safer digital environment. Drawing on studies like the one from Majmaah University (Alotaibi et al., 2021), it shows how education can empower students to protect their privacy and security. Ultimately, the paper argues that with awareness and collective effort, students can enjoy social media's benefits while minimizing its risks, making the internet a secure and enjoyable space for all.

keywords:Cybercrime, SocialMedia,Student Awareness, Cybersecurity, Online Safety Phishing, Cyberbullying

Introduction

The internet has transformed the way we live, work, and connect with the world. It has made life easier by letting us shop, learn, and talk to people far away with just a few clicks. Among the most popular parts of the internet are social media platforms like Facebook, Instagram, Twitter (X), Snapchat, TikTok, and WhatsApp. These platforms are a big part of daily life, especially for students. Young people use them to chat with friends, share photos and videos, follow trends, and even do school projects. For example, a student might join a study group on WhatsApp or watch educational videos on TikTok. According to a 2023 report by Statista, more than 4.9 billion people around the world use social media, and a large number of them are teenagers and young adults, including students. This number keeps growing as more people get smartphones and internet access.

While social media brings many benefits, it also comes with serious risks. One of the biggest dangers is cybercrime, which means illegal activities that happen online. Cybercrime can take many forms, such as stealing someone's personal information, bullying people through messages, or tricking them into sending money. For instance, a student might get a fake message promising a prize, only to lose money instead. Students are especially at risk because they spend so much time online—sometimes hours every day—scrolling through posts, liking pictures, or chatting

with friends. They often trust what they see on social media and may not realize when something is dangerous. The excitement of connecting with others can make them forget about the hidden threats waiting online.

Cybercrime is a growing problem as more people join social media. Criminals see students as easy targets because they are young, curious, and sometimes unaware of how to stay safe. A single mistake, like clicking a bad link or sharing too much personal information, can lead to big trouble. This paper aims to explain what cybercrime is and how it happens on social media platforms. It will also show why students need to learn about these dangers and how they can protect themselves. By understanding cybercrime, students can enjoy the fun parts of social media—like staying connected and having fun—without falling into traps set by cybercriminals. Awareness is the key to staying safe in today's digital world, and this paper will explore how students, with help from schools and families, can take control of their online safety.

What is Cybercrime?

Cybercrime is any crime that uses computers, phones, or the internet. Cybercriminals are people who break the law online to harm others or make money illegally. According to the Federal Bureau of Investigation (FBI), cybercrime costs people and businesses billions of dollars every year (FBI, 2023).

Cybercrime is any crime that uses computers, phones, or the internet.

This means cybercrime is not like traditional crimes that happen in person, such as stealing a wallet from someone's pocket. Instead, it happens in the digital world using technology. For example, if someone uses a computer to break into your email account, that's cybercrime. Or if they send you a fake message on your phone to trick you, that's also cybercrime. The tools—computers, smartphones, or the internet—are what make it different from other crimes. It can happen anywhere, anytime, as long as there's a device and an internet connection. This makes cybercrime hard to stop because criminals can attack from far away, even from another country.

Cybercriminals are people who break the law online to harm others or make money illegally.

Cybercriminals are the people who do these crimes. They're not always strangers in dark rooms; sometimes they're people who know how to use technology to take advantage of others. Their goal might be to hurt someone—like posting mean things to embarrass them—or to make money in a wrong way. For example, a cybercriminal might trick you into giving them your bank details by pretending to be your friend. Another might hack into a company's system to steal money. They break laws, but instead of using guns or knives, they use keyboards and codes. This makes them sneaky and hard to catch because they can hide behind fake names or accounts online.

According to the Federal Bureau of Investigation (FBI), cybercrime costs people and businesses billions of dollars every year (FBI, 2023).

The FBI is a big organization in the United States that fights crime, including cybercrime. They keep track of how much damage it causes. When they say "billions of dollars every year," they mean cybercrime is very expensive. For example, if someone steals your credit card details online and spends your money, that's part of the cost. Or if a business gets hacked and loses customer information, they might have to pay to fix it. The FBI's 2023 Internet Crime Report

showed that in 2022 alone, people in the U.S. lost over $10 billion to cybercrime. This money comes from scams, stolen data, and other online crimes. It affects regular people—like students who lose money to fake offers—and big companies that get attacked by hackers. The huge cost shows how serious and widespread cybercrime has become.

So, cybercrime is about using technology—like computers or phones—to do bad things online. The people who do it, called cybercriminals, want to either harm others or get rich by breaking the law. The FBI warns that this problem is so big that it takes away billions of dollars every year, hurting people, families, and businesses. For students, this means cybercrime isn't just a faraway issue—it's something that could affect them too, especially when they're on social media or browsing the internet.

Some common types of cybercrime include:

- **Hacking**: When someone breaks into your account or device without permission. For example, a hacker might guess your password and take over your social media profile.
- **Phishing**: This is when cybercriminals send fake messages or emails pretending to be someone you trust, like a friend or a bank, to trick you into sharing passwords or personal details.
- **Cyberbullying**: Using the internet to harass, threaten, or embarrass someone. This often happens on social media through mean comments or messages.
- **Identity Theft**: Stealing someone's personal information, like their name or photos, to pretend to be them or commit fraud.
- **Scams**: Fake offers or messages that trick people into sending money. For instance, a student might see a "win a free phone" ad that's really a scam.

These crimes can happen to anyone, but students are especially vulnerable because they use social media a lot and may not know how to spot dangers.

Social Media and Cybercrime

Social media makes it easy to connect with people, but it's also a place where cybercriminals look for victims. Students often post personal things online, like their school name, birthday, or where they live. A study by the Pew Research Center found that 81% of teens share personal information on social media, which can be risky (Pew Research Center, 2022). Here's how cybercrime happens on social media:

- **Fake Accounts**: Criminals create fake profiles to trick students into accepting friend requests. Once connected, they might ask for money or private information.
- **Phishing Links**: A message might say, "Click here to see a funny video," but the link could steal your login details or put a virus on your device.
- **Cyberbullying**: Bullies use social media to spread rumors or send hurtful messages. The Cyberbullying Research Center says 37% of students have faced online bullying (Patchin & Hinduja, 2023).
- **Scams**: Ads or messages promising free gifts or jobs can trick students into giving money or bank details.

Students love social media because it's fun and fast, but they don't always see the risks. For example, a student might think a message from a "friend" is safe, not knowing the account was hacked.

Why Student Awareness is Important

Awareness means knowing about cybercrime and how to avoid it. Many students don't realize how dangerous the internet can be. A study at Majmaah University in Saudi Arabia found that most students lacked knowledge about cybersecurity and often shared too much online (Alotaibi et al., 2021).

"Why Student Awareness is Important" based on the statement you provided. I've elaborated on each point with examples, details, and a clear explanation, while keeping it in simple English.

Awareness means knowing about cybercrime and how to avoid it.

Awareness is like having a map to stay safe in a tricky place. It means students understand what cybercrime is—like hacking, scams, or bullying online—and learn ways to protect themselves. For example, if a student knows that a random message asking for their password might be a trick, they won't fall for it. Awareness isn't just about knowing the dangers; it's also about knowing what to do, like using strong passwords or not clicking strange links. Without this knowledge, students are like travelers without a guide, easily lost in the dangerous parts of the internet.

Many students don't realize how dangerous the internet can be.

A lot of students see the internet as a fun place to play games, watch videos, or talk to friends. They don't always think about the risks hiding behind the screen. For instance, a student might post a photo of their school uniform or their house without knowing that a stranger could use it to find them. The internet feels safe because it's familiar, but it's full of hidden threats—like cybercriminals waiting to take advantage of mistakes. Because students use it so much, they might not stop to think about how one wrong move could cause big problems, like losing money or getting harassed.

A study at Majmaah University in Saudi Arabia found that most students lacked knowledge about cybersecurity and often shared too much online (Alotaibi et al., 2021).

This study shows real proof of the problem. Researchers at Majmaah University in Saudi Arabia talked to students and found that many didn't know basic things about staying safe online, like how to spot a fake website or why sharing personal details is risky. For example, some students posted their phone numbers or home addresses on social media, thinking it was no big deal. The study said this happened because they weren't taught enough about cybersecurity—the skills and knowledge to protect themselves online. When students don't know these things, they accidentally make it easy for cybercriminals to target them.

Without awareness, students might:

Here's what could happen if students don't learn about cybercrime:

Lose personal information: If a student shares their password or clicks a phishing link, a criminal could steal their social media account or even their bank details.

Get tricked by scams: A fake message promising free gift cards might trick them into sending money or giving away private info.

Face cyberbullying: Without knowing how to spot or report mean behavior online, they might suffer from hurtful comments or threats.

Put others at risk: Sharing too much, like a friend's photo or location, could accidentally harm someone else.

Lose trust in technology: After a bad experience, like getting hacked, they might feel scared to use the internet at all, even for schoolwork.

Student awareness is important because it's the first step to staying safe online. The internet is a big part of students' lives, but many don't see its dangers—like how a single post or click can lead to trouble. The Majmaah University study proves that without proper knowledge, students make mistakes, like sharing too much, because they don't understand cybersecurity. If they don't learn about cybercrime, they could lose things that matter—like their privacy, money, or peace of mind. Awareness gives them the power to enjoy the internet without fear, turning risks into something they can handle.

Without awareness, students might:

- Lose personal information, like passwords or bank details.
- Get tricked by scams or fake messages.
- Face emotional harm from cyberbullying.

When students learn about cybercrime, they can protect themselves and enjoy social media safely. Schools and parents play a big role in teaching them. For example, a survey in Palestine showed that 52.4% of university students had been victims of cybercrime or knew someone who had, proving how common it is (Hassan et al., 2024). Awareness helps students spot trouble early and stay safe.

How to Stay Safe

Students can follow simple steps to avoid cybercrime on social media. Here are some practical tips based on advice from experts:

1. **Keep Accounts Private**: Use strong passwords with letters, numbers, and symbols. Don't share passwords with anyone, even friends. The National Cyber Security Centre (NCSC) says strong passwords stop 80% of hacking attempts (NCSC, 2023).
2. **Think Before Clicking**: Don't open links or download files from unknown people. Phishing attacks often hide in innocent-looking messages.
3. **Don't Overshare**: Avoid posting things like your home address, phone number, or school schedule. Cybercriminals can use this to target you.
4. **Check Privacy Settings**: Make your social media profiles private so only friends can see your posts. A study showed that private accounts are less likely to be hacked (Alzubaidi, 2021).
5. **Report Problems**: If you see something suspicious, like a fake account or bullying, tell an adult or report it to the platform. Most social media sites have a "report" button.
6. **Update Software**: Keep your phone and apps updated. Updates fix security problems that hackers might use.

These steps are easy but powerful. For example, the FBI suggests that reporting cybercrime quickly can help catch criminals and stop more attacks (FBI, 2023).

Role of Schools and Parents

Schools and parents can help students stay safe online. Schools can teach about cybercrime in classes or workshops. A study in Saudi Arabia found that students who got cybersecurity training were more careful online (Alotaibi et al., 2021). Parents can talk to their kids about what they do online and set rules, like limiting screen time or checking friend lists. Working together, schools and parents can make students smarter about social media risks.

Conclusion

Cybercrime is a serious and growing problem that gets worse as more people join social media every day. With billions of users worldwide, platforms like Facebook, Instagram, and Twitter (X) are busy places where criminals find new ways to attack. Students are especially at risk because they love using these platforms to share their lives—posting pictures, chatting with friends, or following their favorite stars. For example, a student might share a photo of a fun day out without realizing it could help a stranger figure out where they live. They enjoy connecting online, but they don't always see the dangers hiding behind the fun. Cybercriminals know this and target students because they're young, trusting, and often unaware of the tricks used against them.

This paper explained what cybercrime is: illegal acts like hacking, phishing, and bullying that happen through computers and the internet. It showed how these crimes play out on social media—like fake accounts tricking students into sharing passwords or bullies using comments to hurt feelings. It also made clear why awareness is so important. Many students don't know how risky it is to overshare or click unknown links, and studies, like the one from Majmaah University, prove they need more education about staying safe (Alotaibi et al., 2021). Without this knowledge, they can lose their privacy, money, or even their confidence, making the internet feel scary instead of exciting.

The good news is that students can protect themselves with simple steps. Using strong passwords—ones that mix letters, numbers, and symbols—makes it harder for hackers to break in. Not clicking strange links in messages or emails keeps them safe from phishing traps. Other tips, like keeping accounts private and reporting suspicious things, also help. These actions don't take much time but can stop big problems. For instance, a student who avoids a scam by checking a message with an adult saves themselves trouble and stress. Safety online isn't hard—it just needs attention and practice.Fighting cybercrime isn't just up to students, though. Schools, parents, and students must team up to make a difference. Schools can teach lessons or hold workshops about cybersecurity, showing students how to spot dangers and react. Parents can guide their kids by setting rules—like no sharing personal details—and checking in on what they do online. Students themselves can spread the word to friends, helping everyone stay smart about social media. When everyone works together, it's like building a strong wall against cybercriminals. No one has to face the problem alone.

In the end, the internet doesn't have to be a risky place. With awareness and care, it can stay a fun and safe space for everyone. Students can keep enjoying the things they love—sharing moments, learning new things, and connecting with others—without fear. Cybercrime is a challenge, but it's one we can beat. By learning, teaching, and watching out for each other,

students can take charge of their online world. The future of social media depends on today's actions, and with the right steps, it can be a place where creativity and safety go hand in hand.

References

1. Alotaibi, M., et al. (2021). "Assessment of Cybersecurity Awareness among Students of Majmaah University." *MDPI Journal*. Retrieved from www.mdpi.com.
2. Alzubaidi, A. (2021). "Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia." *Heliyon*, 7(1).
3. Federal Bureau of Investigation (FBI). (2023). "Internet Crime Report 2022." Retrieved from www.fbi.gov.
4. Hassan, N., et al. (2024). "Risky Online Behaviors and Cybercrime Awareness among Undergraduate Students at Al Quds University." *Crime Science Journal*.
5. National Cyber Security Centre (NCSC). (2023). "Password Guidance: Simplifying Your Approach." Retrieved from www.ncsc.gov.uk.
6. Patchin, J. W., & Hinduja, S. (2023). "Cyberbullying Research Center: 2023 Statistics." Retrieved from www.cyberbullying.org.
7. Pew Research Center. (2022). "Teens, Social Media and Technology 2022." Retrieved from www.pewresearch.org.
8. Statista. (2023). "Number of Social Media Users Worldwide." Retrieved from www.statista.com.