Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-5 | May-2025 | Page 161-168

Internet Fraud in Cybercrime

[1]Koiwood Kelvin Forkpa Morris, [2]Prof. (Dr) Parveen Kumar Janjua
[1]B. Sc Forensic Science, [2]Professor & HOD
[1,2]Department of Forensic Science
[1,2]Kalinga University, New Raipur, Chhattisgarh, India

Abstract

Internet fraud is a growing online crime in which scammers trick people using websites, emails, or social media to steal money, businesses, or governments for money or personal gain. As more people use the internet for communication, shopping, and socializing, fraudsters find more ways to take advantage of weak spots in online systems. This can lead to online scams, identity theft, and other harmful activities. As internet use increases, internet fraud is becoming more common and complex. Fraudsters use methods like social engineering, where they manipulate people into trusting them, malware that infects computers to steal information, and fake websites that look real to trick people. These tactics lead victims to give away personal details, such as passwords or credit card numbers, or to make payments without realizing they've been scammed. With access to the internet, criminals can easily hide their identity and carry out illegal activities without being in a specific place. This makes it challenging for local authorities to trace and stop them. As a result, it becomes harder to hold these criminals accountable for their actions. Internet fraud can have serious effects, causing people to lose a lot of money, damage their reputation, and suffer emotional stress that can last a long time. Cyber-criminals are always finding new ways to use technology and take advantage of how people use the internet. Because of this, it's more important than ever for strong security systems to be in place to protect people online. This research aims to help people better understand internet fraud and suggest practical ways to reduce its impact on our local communities and society as a whole. As more people use the internet for activities like shopping and banking, the risks of fraud have increased. Cyber-criminals take advantage of new opportunities to exploit weaknesses in online systems. To address this, we need to improve cybersecurity to protect personal and financial information.

Introduction

Internet fraud is an online scam where criminals trick people through websites, emails, or messages to steal their money or personal information. As the internet becomes more important for communication, shopping, and socializing, these online scams are becoming more common and harder to detect. The internet is easily accessible to many, giving cybercriminals numerous chances to exploit it for illegal activities like scams and identity theft. Internet fraud is a serious problem because it causes large financial losses for people and companies, harms reputations, reduces trust in online platforms, and creates a worldwide threat to digital security.

There are various types of internet fraud:

Internet fraud is a serious issue, involving various dishonest activities, from small tricks to large global crimes. Some common types of internet fraud that affect people include:

Identity Theft: Cybercriminals steal personal information like Social Security numbers, bank account details, or credit card information to impersonate victims and commit fraud. This can cause the victim to lose money, hurt their credit score, and face legal problems.

Phishing: In this type of fraud, cyber-criminals pretend to be trusted organizations like banks or government agencies to trick people into giving up important details, such as usernames, passwords, and credit card numbers. Phishing is often done through fake emails or websites that look real.

Online Scams: Online scams involve different types of fraud, like fake surveys, dating scams, lottery scams, and prize frauds. In these scams, victims are fooled into giving personal information or sending money, hoping for rewards that never actually happen.

Credit Card Fraud: Cybercriminals steal credit card information from unsafe online transactions or when data is leaked in a system. They use this stolen information to make purchases without permission, causing major financial losses for both the cardholder and the banks.

Auction Fraud: On online auction sites like eBay, scammers fool buyers by posting items they don't plan to send or by selling things that don’t exist. After the buyer pays, the scammer disappears, and the buyer receives nothing.

Investment Fraud: Scammers may offer fake investment deals online, claiming huge profits from things like stocks, real estate, or cryptocurrency. Victims are tricked into investing, but they lose their money when the scammer disappears with it.

Literature Review

2.1 Internet Fraud in Cybercrime: As more people use the internet for personal, work, and financial reasons, internet fraud has become a bigger problem. It’s when criminals trick people, businesses, or governments online to steal money or personal information. Experts in areas like technology, law, and psychology are studying how these crimes are getting more complicated and how to stop them. This review looks at their findings, including how internet fraud has changed, the most common types of fraud, how criminals work, the damage it causes, and how to prevent it.

2.1 **Evolution and Growth of Internet Fraud:**

- The internet has helped internet fraud grow quickly. Anderson (2019) says that because the internet is easy to access and allows people to remain anonymous, cyber-crime, including fraud, has become more common. At first, internet fraud was simple, like email scams and fake auctions. But over time, fraud has gotten more complicated. Now, criminals use tricks like phishing, social manipulation, and harmful software to fool people, making it harder to catch them.

- The research by M. S. Gupta, S. Sharma, and A. Jain, published in July 2021, provides a clear plan for detecting fraud in online shopping. It highlights important areas that need more research and the challenges businesses face when creating fraud detection systems. The authors emphasize that using machine learning is important because it can make fraud detection systems more accurate and faster.

- The paper titled 'Recent Trends in Social Engineering Scams and Case Study of Gift Card Scam,' published in October 2021 by Rajasekhar Chaganti, Bharat Bhushan, and others, discusses how social engineering scams have evolved, particularly with the rise of new technology. Scammers are always finding new ways to trick people and businesses.

The authors give useful tips to help people avoid falling for these scams. They also suggest ways that businesses can protect themselves, like using strong security measures and teaching their employees how to recognize scams.

2.2 **Forms of Internet Fraud**

The literature discusses various types of fraud that primarily occur online and affect people. Some examples include:

Phishing: Phishing is an online scam where criminals try to steal personal information, like passwords or credit card numbers, and it often affects local individuals. They pretend to be a trusted organization, like your bank, or even someone you know, to make you believe their request is real. This makes you more likely to share your sensitive information.

Identity Theft: "Identity theft happens when someone takes your details, like your name, address, or bank information, and uses them to impersonate you. They can use this stolen information to make purchases, open accounts, or even borrow money in your name.

Online Auction and Shopping Fraud: This type of fraud happens when scammers trick people into paying for products they never receive, or bad-quality items instead. It usually occurs on websites where people buy and sell things, like eBay or Amazon.

Investment Fraud: Investment fraud happens when scammers trick people into putting money into fake or dishonest investments. They often promise high profits with little or no risk, but these claims are usually false and misleading.

2.3 Tactics and Techniques Used by Cyber-criminals

Cyber-criminals have developed more advanced techniques to carry out internet fraud, taking advantage of technological progress to trick and deceive victims:

Social Engineering: Social engineering is a frequent trick used by cybercriminals to deceive people into sharing personal details, allowing access to their accounts, or doing something harmful, often without them realizing it's a scam, and affecting local individuals. Social engineering takes advantage of human emotions and trust. The goal is to make the victim trust the scammer or feel pressured to act quickly, making them do things they wouldn't usually do.

Outcome and Significance

Internet fraud is growing fast and becoming more complicated, making it a serious problem that needs attention from everyone, governments, companies, and everyday internet users. This study is important because it helps people understand how online scams work, who they affect, and what can be done to stop them. As more people use the internet for things like work, shopping, and banking, the risk of being scammed increases.

Advanced fraud detection systems are designed to monitor and analyze online activities, spotting unusual patterns or suspicious behaviors like irregular financial transactions, fake profiles, or phishing attempts. Using machine learning and artificial intelligence, these systems can track large amounts of online transactions and quickly identify potential fraud. Financial institutions, online stores, and other platforms can use these tools to block fraudulent transactions before any damage is done.

Education is an important way to fight internet fraud. Many people don't know about the dangers of online fraud and the tricks used by cybercriminals, like phishing, fake websites, and social engineering. **Regular awareness campaigns** and **training** can help people recognize these dangers and learn how to stay safe. By teaching individuals how to spot suspicious emails, check if websites are real, create strong and unique passwords, and avoid sharing personal information online, the chances of falling for fraud can be greatly reduced.

To improve security, online platforms should adopt stronger protocols to protect users' personal and financial information. This includes encrypting data to prevent unauthorized access. Additionally, enabling **multi-factor authentication (MFA)** adds an extra layer of protection. Even if cybercriminals manage and obtain a user's login details, they won't be able to access the account without completing another form of verification, like a code sent to the user's phone or a biometric check, such as a fingerprint scan. This makes it significantly harder for fraudsters to break into. This research will teach individuals, businesses, and organizations how to protect themselves from falling victim to fraud and cybercrime. It will focus on methods like using multi-factor authentication and raising awareness through education in schools and communities.

By learning these techniques, people can better recognize and avoid online scams, making it harder for cybercriminals to trick them.

To catch cybercriminals, experts use digital forensics, which involves collecting online evidence like emails, IP addresses, and transaction records. Investigators also analyze malware and phishing scams to understand how fraud happens. In some cases, they recover deleted files or track cryptocurrency transactions to follow the money trail. These methods help law enforcement identify and stop online criminals.

Preventing internet fraud requires awareness and strong security measures. People should avoid clicking on unknown links and sharing personal information on untrusted websites. Businesses must invest in cybersecurity to protect their data. Governments and experts continue to develop better ways to fight cybercrime, but individuals also play a role in staying alert and protecting themselves online.

The forensic significance of internet fraud in cybercrime is important because it helps investigators collect and analyze evidence of online fraud. Forensic experts use tools like data recovery, digital fingerprinting, and tracking IP addresses to trace the actions of cybercriminals and identify victims. They can examine logs, emails, and other digital traces to understand how the fraud took place. This evidence is vital for law enforcement to prosecute criminals, recover stolen money, and prevent future fraud. Digital forensics is crucial in uncovering how internet fraud is carried out and helps in the fight against cybercrime.

Methodology:

This research uses a combination of different methods to study internet fraud in cybercrime. **Primary data** is gathered through surveys and interviews with cybersecurity professionals, law enforcement personnel, and individuals who have experienced online fraud. Surveys help collect information on common fraud cases, public awareness, and the effectiveness of security measures. Interviews provide a deeper understanding of the tactics used by cybercriminals and the difficulties faced by experts in preventing fraud.

Additionally, **secondary data** is obtained from research papers, government publications, and cybersecurity reports. This information helps analyze fraud trends, case studies, and statistical data. Advanced tools, including artificial intelligence, are also used to identify fraud patterns and predict new threats. The study further examines laws and policies from different countries to understand how they address cyber fraud. This study combines both qualitative and quantitative research to better understand internet fraud and offer practical ways to reduce its impact on people in our area

Internet fraud in cybercrime uses various tricks to deceive people, steal personal information, or make money. One of the most common methods is social engineering, where criminals manipulate victims into giving up confidential details like passwords or credit card numbers. They take advantage of human emotions like trust, fear, or urgency. For example, they may pretend to be from a bank or a government agency, sending fake messages that create a sense of panic or urgency, which makes victims more likely to fall for the scam. Install anti-phishing and anti-malware software that can identify and block fraudulent emails or suspicious links. These tools protect users by warning them of potential threats and preventing them from accessing harmful links or opening dangerous attachments.

Phishing is when Cybercriminals often use a trick to send fake emails that look like they come from local banks, stores, or social media sites. These emails usually include dangerous links or attachments that can steal personal details or infect your device with harmful software. Once the malware is on the device, it can gather data, track online activity, or even give the attacker remote access. Phishing scams are becoming more effective with methods like spear-phishing, where attackers customize their messages to make them seem more believable and target specific individuals. Train employees and individuals on how to recognize common social engineering tactics, such as phishing emails, phone scams, and fake requests. Teach people to identify suspicious signs, such as unexpected requests for personal information, urgent messages asking for quick action, or communications from unfamiliar sources.

Online auction scams and investment frauds are common types of internet fraud. In online auction scams, criminals post fake product listings on auction sites, tricking people into paying for items that don’t exist. After the payment is made, the scammer disappears, leaving the victim without the product and unable to get their money back. Investment scams work similarly. Fraudsters often offer fake investment opportunities, promising high returns. They create fake websites or use false reviews to make these opportunities appear legitimate. Both scams focus on gaining trust and creating a sense of urgency, pushing victims to act quickly without verifying if the offer is genuine, which can affect people in our community. To fight investment fraud, it's important to use fraud detection systems that track online activity and spot signs of scams, like fake reviews or unusual transactions. These systems help catch fraud early. People should also check their financial accounts regularly for unauthorized transactions. If they notice anything suspicious, they should report it right away to their bank or financial institution to stop further harm and protect their money.

Preventing internet fraud requires a mix of technology, education, and rules. One key solution is fraud detection software, which uses machine learning to spot suspicious behavior or transactions. Banks and online stores use this software to block fraud in real time. Another important step is educating users, as many people are unaware of online fraud risks. Teaching people to spot phishing emails, recognize fake websites, and use strong, unique passwords can reduce the chances of falling for scams. Regulations like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) help protect personal and financial information by providing guidelines for companies to secure their systems, benefiting both businesses and individuals.

Researchers use various methods to understand internet fraud and develop better ways to prevent it. They analyze data, examine past fraud cases, and apply advanced technologies like artificial intelligence (AI) to detect cybercrime patterns. AI helps identify suspicious activities, while data analysis reveals common fraud techniques used by criminals. Additionally, educating the public through awareness programs is crucial in helping people recognize and avoid online scams.

Preventing internet fraud requires cooperation between governments, businesses, and cybersecurity professionals. Since cybercriminals constantly create new strategies, continuous research is essential to stay ahead of emerging threats. Security measures like multi-factor authentication and encryption provide stronger protection for individuals and organizations.

Result:

1.1 **How familiar are you with the concept of Internet fraud**

In my research, 64% of participants stated that they are familiar with internet fraud, indicating that most people know the risks of online criminal activities. This high level of awareness can be attributed to various factors such as news coverage, online campaigns, and educational programs that teach people about the dangers of online scams. As a result, many in this group are likely to recognize common fraud types like phishing, identity theft, or fake online stores, even if they haven’t personally experienced them.

On the other hand, 30.4% of respondents say they are somewhat familiar with internet fraud. This group may know a little about the issue, but their understanding might not be very deep. They may have heard the terms scam or fraud, but lack knowledge of the different techniques fraudsters use to trick people online. This could be due to less exposure to educational campaigns or limited personal experience with online fraud. While they understand the problem in a general sense, they might not know how to spot or deal with specific threats.

The remaining portion of the respondents, though not directly mentioned, are likely either unaware of internet fraud or have little knowledge of it. These individuals could benefit from targeted education programs to help them better understand the dangers of online fraud. Since internet scams are becoming more complex, especially with new threats like social media scams and phishing emails, increasing awareness among this group is important. Raising awareness about different types of fraud empowers individuals to protect themselves and helps reduce the overall risk of cybercrime in the local area.

1.2 **Have you ever been a victim of Internet Fraud**

In my research, 55% of participants said they have not been victims of internet fraud. This means that more than half of the people in your survey have either avoided scams or simply haven't fallen victim to them. It shows they are likely more careful and aware when using the internet.

On the other hand, 30% of respondents reported being victims of internet fraud. This indicates that a considerable number of individuals in our community have either had their personal information stolen or have been tricked into losing money. It highlights that internet fraud remains a common problem.

The chart in my research shows the difference between those who have been affected by fraud and those who haven't. This helps to highlight the ongoing risks of online scams and the need for people to be more aware and cautious.

Conclusion:

As technology advances, internet fraud is becoming more clever and harder to spot. Because the internet is so easy to access, scammers use tricks like fake emails (known as phishing), stealing identities, and financial scams to get personal information or money. These crimes don't just cause people to lose money—they also hurt the trust we have in online platforms and can damage reputations.

To stay safe, it's important to be alert and take steps to protect ourselves. That means using strong security tools like two-factor authentication, encrypted data, and smart systems that can detect suspicious activity. But stopping online fraud isn't something one person can do alone—it takes teamwork. Businesses, individuals, and governments all need to work together.

Education plays a big role, too. When people understand how scams work, they're less likely to fall for them. Strong laws and strict enforcement also help keep criminals in check. Since online fraud often crosses borders, countries must cooperate to track down and punish those responsible. By combining better security, public awareness, and global efforts, we can create a safer internet for everyone.

References

1. Federal Bureau of Investigation (FBI) - Internet Crime Complaint Center (IC3)
2. Europol - Internet Crime Website: https://www.europol.europa.eu
3. Internet Fraud in Cybercrime:
4. The Psychology of Internet Fraud Victimisation: a Systematic Review" (2019)
5. Cybercrime: Victimization, Perpetration, and Techniques" (2021)
6. A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting" (2024)
7. The Threat of Online Scams: Examining Tactics, Impacts, and Effective Countermeasures" (2024)
8. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy" (2021)

9. Brief Study of Cybercrime on an Internet" *Authors:* Prof. Dhaval Chudasama, Raj Singh Deora *Year:* 2021
10. Digital Fraud: Analyzing the Latest Trends and Tactics in Cybercrime.
11. Cyber Fraud And Consumer"
12. *Author:* Ritesh Kumar Rai *Year:* 2025 https://www.ijllr.com/post/cyber-fraud-andconsumer
13. A Review on Cyber Crimes on the Internet of Things" *Authors:* Soma Navyasree, Febin Prakash *Year:* 2024
14. https://www.researchgate.net/publication/359708894_A_Review_on_Cyber_Crimes_on_the_Int ernet_of_Things
15. Understanding Cybercrime from a Criminal's Perspective: Why and How Youths Engage in Cybercrime" (2022)
16. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy" (2021)
17. Hacker Types, Motivations, and Strategies: A Comprehensive Framework" (2022)
18. The Psychology of Internet Fraud Victimisation: A Systematic Review" (2019).