

# Mathematical Knowledge and Skills in E-Business Transactions and in Curbing Electronic Fraud

Dr. Frederick-Jonah Toinpere Mercy<sup>1\*</sup>, Dr. Areelu Fisayo<sup>2</sup>

<sup>1</sup>Department of Science Education, Faculty of Education, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

<sup>2</sup>Department of Mathematics Education, College of Science Education, Lagos State University of Education, Otto Ijanikin, Lagos State, Nigeria

DOI: [10.36348/sjhss.2023.v08i06.004](https://doi.org/10.36348/sjhss.2023.v08i06.004)

| Received: 18.04.2023 | Accepted: 29.05.2023 | Published: 08.06.2023

\*Corresponding author: Dr. Frederick-Jonah Toinpere Mercy

Department of Science Education, Faculty of Education, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

## Abstract

The digitalization of commerce and finance has brought us to the era of e-business and e-transactions. E-business transactions refer to the use of electronics in the carrying out of commercial activities (sales and purchases). Unfortunately, the rise of e-business transactions has been plagued by the issue of electronic fraud, which has become prevalent now more than ever. Mathematics as a field is fundamental to life and present in virtually every aspect of man's life and is an essential tool required and used in problem-solving. The business world is not exempt from the influence of mathematics, and considering this, this study explores the relevance of mathematical knowledge and skills in e-business transactions, as well as in solving the problem of electronic fraud. Mathematics was shown to be useful in fraud prevention tools and strategies like cryptography, data management, and optimization, risk assessment, fraud prevention algorithms, etc. We suggest that all the stakeholders in every field should teach the importance and use of mathematical knowledge and skills to all learners in the entire education system and efforts toward encouraging the development of mathematical knowledge and skills for individuals across all fields, especially in science, technology, business world and in form of training among others.

**Keywords:** Mathematics, E-business, E-transactions, electronic fraud.

**Copyright © 2023 The Author(s):** This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

## INTRODUCTION

We live now in a digital world, and the effects of technology can be felt across all aspects of an individual's life. Technology has brought about several innovations, and advancements, and changed the ways several things are being done (Hossain, 2021; Naikoo *et al.*, 2018).

The impacts of technology are especially prominent in the domain of finance (Abad-Segura *et al.*, 2020; Lin, 2016). It has brought about several developments and innovations, and removed the necessity for cash, with the growth of electronic transactions. In simple terms, e-business refers to the utilization of technological and electronic tools in carrying out fundamental business activities (Max, 2022). E-business involves the use of technology and the Internet, across several business activities. E-business transactions thus refer to the sale and purchase of goods and services through electronic means. E-business transactions are associated with a myriad of

benefits including speed, convenience, flexibility and customization, global reach, automation, etc.

With the increase in technological advancements and growing utilization of online transactions, the issue of electronic fraud has become a serious threat, now more than ever (Ibanichuka & Oko, 2019). Various strategies and tools have been developed over time to fight the issue of electronic fraud during e-transactions.

Mathematics deals with the study of numbers, shapes, quantities, and relationships (amongst others), and is the foundation of a wide variety of fields, as well as utilized daily in one form or another by man (Deepika, 2021). Mathematics is often described as the "language of science and technology" due to the impacts it holds and the influence it exhibits in every domain of science and technology. The technology involved in e-business transactions is thus not exempt from the influence of mathematics. This review is thus geared towards exploring the necessity and utilization

of mathematical knowledge and skills in e-business transactions, as well as in curbing electronic fraud.

### Nature of e-business Transactions

Technologies and the internet have revolutionized several major areas of man's life and including the world of commerce and business. Digitalization has led to a new era of e-business. E-business (short for electronic business) refers to one that makes use of technologies and the Internet to conduct various manner of business operations and processes (Max, 2022). In e-businesses, technology is used across all commercial-based processes including sales and purchasing, marketing, customer service, management, etc.

In e-businesses, sales and purchases are typically carried out through electronic transactions. These transactions refer to the transfer of funds/money through electronic channels, over networks like the Internet (Eumer Merchant, 2016; Samayawardena, & Sachindrani, 2018). E-business transactions are those that involve the exchange of goods and services between individuals, through electronic tools or means. E-business transactions have been on a steady rise in popularity over time, and are quite relevant in recent years, with it being the basic framework and structure for several of the major and prominent businesses and commercial activities today.

Transactions in e-businesses are carried out through electronic payment systems, which are crafted to ensure secure and fast transactions over a network (Ali *et al.*, 2019). Fatonah *et al.*, (2018) describe e-payment systems as a type of inter-organizational information system, designed and dedicated to making financial or money-related transactions between different individuals or organizations. These systems enable the e-business to receive payment for goods and services, even from different locations and across different currencies. Electronic payment systems are quite numerous and include the use of digital or mobile wallets (e.g., Palmpay, Paypal), card payment (e.g. debit, credit, smart, stored value card), bank transfers, net banking, biometric payments, QR payments, etc. (Castro, 2022; Lyra, 2022).

E-business transaction models can be categorized into three major types, based on the direction of those transactions. They include; business-to-business transactions, business-to-consumer transactions, and consumer-to-consumer transactions (Mohideen & Manendran, 2017; Naab & Bans-Akutey, 2021). Business-to-business transactions involve the sale of goods and services from one business to another. Business-to-consumer transactions involve the sale of goods and services directly to consumers who are to use/consume them. Consumer-to-consumer transactions refer to one that occurs between two typical consumers,

like the sale of used items in online marketplaces like Jiji, Etsy, eBay, OLx, etc.

E-business transactions are guided and overseen by a variety of legal and regulatory requirements. Businesses running electronic transactions must abide by and obey laws such as those for data privacy, consumer protection, taxes, and general business laws (Fuscaldo, 2023; Sheehan, 2022), in the region where they are based.

The rise in popularity and necessity of e-business transactions can be attributed to several advantages associated with its use. One such advantage is the increased level of convenience as well as speed. Through electronic transactions, payments for goods and services can be completed in just a matter of seconds, without putting much hassle on the customer, as it eliminates the need for getting physical currency (cash) or going to a physical shop location to purchase goods and make payments, etc. (Gundaniya, 2021; Miteva, 2022). The ever-increasing use of mobile devices in everyday activities is a key driver of the use of e-business transactions (Ainavolu, 2022). Mobile devices like smartphones and tablets have made it quite easy for consumers to make e-business transactions at their convenience, anywhere in the world, and at any time. This has led to the growth of mobile commerce, with most e-business tailoring their operations to work on mobile devices.

Another advantage that makes e-business transactions so useful is the greater deal of flexibility and customization/personalization associated with their use (Abimbola, 2023; Smirti, 2018). With digitalization, businesses can tailor their offers to specific customers, personalizing the recommendations and offer they see. This will lead to a boost in sales as well as in meeting the needs of the customers, as they can more easily access what they need from the business. This can be easily observed in online shopping where an individual gets constant recommendations tailored to each unique person based on the trend in their previous purchases, searches, etc. The personalization feature can also be seen in targeted advertisements on online platforms like social media.

Digitalizing businesses through e-business transactions has also proven quite useful for expanding the reach of some businesses, exposing them to a greater customer base (Adil, 2022; Pillemer, 2020). In tandem with this, the customer is also able to get easier access to goods and services that might otherwise be out of their reach, as it eliminates the need for a physical presence in business locations. An example is online stores like Jumia, which uses e-business transactions to be able to reach a wider customer base, all over Nigeria. The customers are also able to get

some goods (even directly from manufacturers) that might not be easy to get locally.

Through e-business transactions, businesses are also able to automate many of their processes (Adil, 2022). E-businesses can automate activities like processing of orders, shipping, management of inventory, data collection, etc. (Almendariz, 2020) leading to a reduction in errors and an enhancement in efficiency. Also, the use of electronic transactions for e-business allows for better and more detailed record keeping as all payments can be tracked and details retrieved, making it easier for businesses to manage their finances.

Though e-business and e-transactions are the clear paths toward the future, it is worth noting that there is a level of challenges associated with their use. One such challenge is the issue of the network. E-business and e-transactions are still burdened with network and connectivity issues, specifically in developing countries like Nigeria, which lacks the needed infrastructure to ensure a reliable network connection (Okonkwo, 2021). As such, it is often to come across issues like customers being debited for unsuccessful transactions, which places an extra burden on the customer as most times these failed transactions are not quickly refunded, forcing the customer to constantly meet (in physical offices) or contact customer care agents of banks or e-payment system used.

The most prominent issue of e-business transactions lies in the domain of security. The steady rise in e-business and e-transactions has unfortunately only led to a boost in the level of fraud and cyber-attacks (ALadan, 2016; James *et al.*, 2018). As such, both business and individuals need to take active steps in protecting their online transactions from the threat of fraud, and this is done in various ways including the use of encryption technology, the use of only secure payment gateways, etc.

### **Electronic Fraud in e-business Transactions**

Electronic fraud is a significant issue and threat facing e-business transactions. Electronic fraud involves the use of deception through the internet and technology to exploit others, usually involving the stealing of sensitive information (such as passwords, personal information, and debit or credit card details) (Ololade *et al.*, 2020). It is otherwise known as cyber fraud or online fraud and is an illegal and criminal act, where the internet and electronic tools are used to steal from or deceive individuals or organizations for personal gains. Due to the rise of the need for technology in man's daily life, and the dependency on electronics, the issue of electronic fraud has become relevant now more than ever, posing a major threat not

just to an individual, but also organizations and businesses, and even governments.

Electronic frauds are of varying types and occur through different means and strategies like phishing, identity theft, malware, online sales or auctions, etc. (Ravichandran, 2023; IamCheated Research Team, 2019). Electronic fraud can also be done through full-blown cyber-attacks like hacking, etc.

Phishing is one of the most popular techniques of electronic fraudsters, whereby fake websites, emails, and text messages, are utilized to trick individuals into revealing sensitive information such as passwords, debit, and credit card details, etc. (Ghazi-Tehrani & Pontell, 2021; Zaharon & Ali, 2021). Websites or other tools used in phishing scams are usually designed in a way that they look legit to the individual, and most times, the fraudsters try to create a sense of urgency and even fear in the victims, to subtly coerce them to act quickly and revealing that sensitive information, without giving it much of a thought.

In identity theft, the personal information of an individual or even an organization is accessed and stolen, and used for activities, without the approval or authorization of the individual (Hussain, 2022). Stolen information can be used in various ways including creating bank accounts, making purchases, taking out loans, stealing victims' money, applying for credit cards, or performing fraudulent activities under the victim's name (Henson, 2017). Through identity theft, fraudsters are also able to contact and dupe friends and families of the identity theft victim, who are under the impression that they are talking to their friends or family. Identity theft results in serious consequences for the victims, especially when the fraudsters become involved in major illegalities under the victim's name, and it is traced back to the victim.

Still, under the issue of identity, some fraudsters also make use of fake identities, where they pretend to be someone that may not even exist, and contact potential victims under that guise. This is often used in catfishing/romance fraud on dating websites and other social media, where they start an online relationship with victims, to get them to send money (MacKay, 2023; Ndyulo, 2021).

The use of malware is also another common tool for fraudsters, where corrupted or malicious software or files are introduced to the computers or gadgets of the victims, which grants the fraudsters access to the victim's sensitive data (Alsayed & Bilgrami, 2017; Jansen & Leukfeldt, 2016). Online sale or auction fraud occurs in online-based marketplaces, where sellers scam buyers, by deceiving them to pay for goods, which are fake or even non-existent

(IamCheated Research Team, 2019; Karo & Sebastian, 2019).

Ponzi schemes and fake investment opportunities have also become quite common, especially in the cryptocurrency domains. Ponzi schemes are fraudulent investment platforms, characterized by the promise of high returns with little risk. Ponzi schemes seem to be legit at the start because early investors in those schemes do see many returns, but the truth behind-the-scene look reveals that these returns are sourced from those that are newly recruited into the scheme, and this continues till the flood of new investors dries out (Chiluwa & Chiluwa, 2022). In Nigeria, the Mavrodi Mondial Moneybox (MMM) scheme, is the most notable case of a widespread Ponzi scheme in recent memory.

Apart from Ponzi schemes, there exist several other types of fake investment frauds that occur through electronics including; pyramid schemes, advanced fee fraud, microcap fraud, pre-IPO investment scams, promissory note scams, etc. (Benny, 2023). In carrying out fraud through fake investment opportunities, it has become popular for fraudsters to lurk online, especially on social media platforms, where they set out to convince potential victims to make investments, with the promise of impressive returns. These individuals often create an online presence or personality that one would attribute to legit and successful business personnel, with them often posting fake reviews of their investments, to deceive gullible individuals and potential victims.

Electronic fraud is quite a global thing on the internet, such that these criminals can operate from anywhere and attack victims from anywhere in the world. This makes it quite difficult for them to be caught and prosecuted (Cross, 2019). Falling victim to fraud can have significant impacts and repercussions including financial losses, emotional trauma, physical and mental health issues, and even damage to one's reputation, and legal liabilities, depending on the type of fraud carried out (Button *et al.*, 2014; International Public Sector Fraud Forum, 2020). Thus, the development of strategies and ways to curb electronic fraud is a major concern, especially for e-businesses and their customers, with many commercial activities being based online, making them more susceptible to being targets of fraudsters. Tools and strategies created to curb electronic fraud range from technical solutions to policy and regulatory frameworks to public awareness campaigns.

### **Mathematics Knowledge and Skills in e-business Transactions**

Mathematics is applied and used in the commercial field of e-business transactions in various ways including for data analytic purposes. E-business

transaction often involves the generation and use of large volumes of numerical or quantifiable based data (Bingwen *et al.*, 2021). Mathematics is needed to analyze, interpret and make sense of those generated data. Data collection, interpretation, and organization tools and strategies such as data mining, machine language learning, and statistical analysis, are all based upon the application of mathematical knowledge and are all required and used to extract and make sense of data, as well as in making an informed decision. Sarkar (2018) highlighted the importance of mathematics in managing and optimizing data describing it as the underpinning structure of most techniques in data science, which is needed for the effective management of data collected through technologies.

Also, the functionality of e-business is dependent on several variables including the optimization of pricing, management of inventory (offline or online), as well as supply chain logistics (etc.). Mathematics is inherently involved in all of these purposes. The functioning of e-businesses and their transactions are all dependent on complex algorithms that directly determine the flow, quality as well as security of transactions (Singh, 2015). Mathematics knowledge and skills are important in this context as it is one of the most essential and indispensable elements in the development of working algorithms no matter the type (Das, 2022). These algorithms and programs that are developed through mathematics are used amongst others for the processing of payments during e-transactions.

E-businesses often make use of forecasting in their provision of goods and services. Forecasting involves the analysis of the wealth of data generated during electronic transactions, to predict and determine future trends as well as demands (Ghosh, 2023; Wu, 2022). Mathematics is the most essential element for forecasting as it is needed for data analysis and accurate predictions. Also, an automated forecasting system can be developed for easier predictions, and mathematics is heavily required in developing such automation.

Artificial intelligence (AI) has grown increasingly popular in recent years and is being generated to serve various purposes, and today is a common feature of a host of e-businesses. AI is typically an intelligent system that can learn, reason, as well as make decisions, in imitation of an actual human (Copeland, 2023; Frankenfield, 2022). Artificial intelligence is used in e-businesses in various ways in the development of chatbots to provide quick and immediate customer support, or tools to personalize recommendations based on the behavior of customers, inventory management, etc. (Johnson, 2022; Utsi, 2022). The development of AI is based on advanced mathematical algorithms, making mathematical knowledge and skills quite the essential variable. Kung

(2021) states that artificial intelligence is mostly mathematics, especially "linear algebra, probability, and calculus". DSouza (2021) states that AI involves and requires good knowledge of mathematics and went further to give a more comprehensive list of mathematics concepts most commonly utilized in AI cutting across mathematical concept areas of algebra (exponents, radicals, factorials, scientific notations, etc.), linear algebra (scalars, vectors, matrices, eigenvectors, and eigenvalues, principal component analysis, etc.), Calculus (derivatives, vector/matrix calculus, gradient algorithms, etc.), Statistics and Probability (basic statistics and probability, Bayes' theorem, common distributions, etc.), information theory (entropy, kullback leibler divergence, cross-entropy), etc. No doubt mathematics is needed in e-business transactions, as it provides the basis and framework for its successful working in terms of accuracy, efficiency, forecasting, data analysis, and even security.

### **Mathematical Knowledge and Skills in Curbing Electronic Fraud in e-business Transactions**

The ever-present threat of electronic fraud has led to the development of several fraud prevention and management techniques as well as research over time. Mathematical knowledge and skills are a common element in the quest to curb electronic fraud and are useful not just to prevent, but also to detect and respond to electronic fraud. A prominent technique/strategy utilized in curbing electronic fraud is risk management.

Risk management refers to the assessment of the chances of an event taking place, as well as considering and evaluating the potential effects of that event, and what steps can be taken to mitigate against it (Rouse, 2023). Mathematical knowledge and skills are needed in this context as they are the basis for risk analysis tools. To carry out a risk assessment, the individual will have to apply the use of some mathematical concepts like probability theory, mathematical modeling, statistics, etc. These mathematical concepts and tools will aid in accurately determining the chances of fraud occurring, how it might occur, as well as how to fight and mitigate against it.

As earlier noted, mathematical knowledge and skills are essential in e-business transactions for the management of large volumes of data generated in e-transactions. The management of data which is dependent on mathematics is also useful for curbing electronic fraud. The use of mathematics to analyze and organize data will allow for easy identification of trends and patterns in e-transactions which will make the detection of fraud easier, and the measures that can be taken against it. Mathematical knowledge and skills are needed to analyze transaction patterns, the behavior of

users, and other data sets, so anomalies and patterns that indicate fraud can be detected.

An example of this is the use of mathematical knowledge in the creation of programs and algorithms that identifies possible fraud indicators like when there is a new login to an e-transaction app on another device, or when there are multiple attempts to log into an e-transaction account, or where there is a sudden peak in the amount of transaction being made that is not typical of the individual, etc. The transaction patterns of customers of e-business can be analyzed so that unusual behaviors like the customer purchasing at an unusual location can be detected. The e-business transaction can be blocked pending verification or additional information from the customer.

Notable in the context of using mathematics for data management for fraud detection is Benford's Law. Benford's Law also known as the "law of first digits" is a mathematical-based law, that gives the expected distribution of digits in datasets that are naturally occurring (Sarkar, 2023; Collins, 2017). Benford's law has major implications in data science and this mathematical law is applied and utilized for fraud detection purposes. Kovach and Ruggiero (2011) (as cited in Amanze & Onukwugha, 2018) developed and tested an electronic fraud detection system for mobile banking, using statistical frameworks of Benford's law and statistical quantiles, with the result showing such applications of mathematics as being effective in detecting instances of electronic fraud.

Also, all manner of fraud detection and prevention tools runs on complex algorithms, and mathematical knowledge is inherently involved in the development of such algorithms. These algorithms vary in their scope and functionalities, as well as the way they protect an e-transaction user from electronic fraud. These tools include statistical analysis tools, detection software, machine learning algorithms, etc. Kanade (2021) and Hyperverge (2022) state that electronic fraud detection techniques generally involve the use of statistical data analysis (statistical parameter calculation, regression analysis, probability distributions, and models, etc.), and Ai-based techniques (data mining, neural networks, machine learning, pattern recognition), both of which requires the use and application of mathematical knowledge. Apart from fraud detection tools, algorithms are also needed in ensuring the security of networks on which e-business transactions are run.

Security tools and protocols like multi-factor authentication, biometric verification (etc.) are recent developments that help mitigate the occurrence of electronic fraud. The development of such tools and protocols is done through complex programming, and this heavily involves the use and application of

mathematical knowledge and skills. Reshma (2022) states that mathematics serves as the foundation of computer programming, and knowledge of mathematics is thus one of the most essential tools needed by programmers, especially in creating complex programs like security tools for online transactions.

One of the major tools used to fight against the occurrence of fraud during e-transactions is cryptography. Cryptography refers to the utilization of algorithms to protect sensitive information to block unauthorized access (Chin, 2022). Cryptography which is achieved through the application of mathematical knowledge and skills is needed in e-business transactions to protect data and information that are of a sensitive nature such as details of credit and debit cards, personal information, login credentials, passwords, etc. Mathematics is relevant in this context since the algorithms necessary for the functionality of cryptography are mathematically based. Singh (2021) highlighted the importance of mathematical knowledge and skills for cryptography, describing mathematics as the basis for it, and that a level of proficiency with a variety of mathematics concepts is needed for cryptography, including algebraic theory, algebraic geometry, discrete mathematics, binary numbers, prime factorization, statistics, complex analysis, etc. Rana (2022) describes applied mathematics as having major connections with cryptology, and that mathematical concepts are needed to create, study and improve cryptology.

Encryption is the principal part and application of cryptography. It involves scrambling data and information, so they are incomprehensible to unauthorized individuals (Ginni, 2021; Khillar, 2020). Encryption technology which is needed for the protection of data during e-business transactions involves the use of complex mathematical algorithms, to encode and decode such sensitive information. Knowledge of mathematics will also be needed not just by e-businesses but also by their customers to fully understand how encryption technology works, so its full capability can be utilized.

After a fruitful or unfruitful fraud attempt, digital forensics might come into play, as it is useful to trace and identify the source of the attack, as well as collect evidence that might be useful in legal actions. Digital forensics is a branch of cybersecurity that is concerned with the search, collection, and investigation of evidence from digital devices (like a computer or mobile phone), usually after a cybercrime like electronic fraud has taken place (Williams, 2023; Tunggal, 2022). Mathematics is needed in digital forensics for this tracking and identification purpose. Sathiyarayanan (2018) states that the successful production and interpretation of pieces of evidence

through digital forensics requires a strong background in mathematics and statistics.

Having good mathematical knowledge will also be useful in preventing an individual from falling victim to electronic fraud attempts like fake investments or Ponzi schemes. Mathematically knowledgeable individuals will be better at discerning investments opportunities that are fraud, as they can make their calculations to see if the offer drafted in the investment offers is even plausible, as most fake investments fraud makes use of big offers and promises to enrich victims, and the lack of authenticity will become obvious when subjected to review through the mathematical lens.

## CONCLUSION

E-business transactions are a prominent feature of modern-day commerce and the path toward the future. Unfortunately, the presence of electronic fraud is a major issue affecting such transactions. Various ways, tools, and techniques have been created to mitigate electronic fraud, and this work shows how and why mathematical knowledge and skills are needed not just for running an e-business, but also for curbing electronic fraud. Mathematical knowledge and skills are shown to be essential to curbing electronic fraud due to their necessity in data management and optimization, risk assessment, cryptography and encryption development of fraud prevention and detection tools and protocols, etc.

## RECOMMENDATIONS

The following recommendations are made based on the review:

1. Teachers and educators in all fields should teach the relevance and use of mathematical knowledge and skills to all learners at primary, secondary, and tertiary levels of education.
2. All stakeholders should make efforts towards encouraging the development of mathematical knowledge and skills for individuals across all fields, especially in science, technology, and the business world.
3. Men and women in offline and online businesses of any form should acquire basic mathematics knowledge and skills to enable them to detect deception and subtle ways of strong-arming them to act without satisfactory information
4. Government should enact strict regulations against electronic fraud and need to train mathematically knowledgeable individuals who can carry out digital forensics to trace these fraudsters.
5. There should be awareness campaigns to educate the general public on common tactics of electronic fraud, and how it can be curbed.

## REFERENCES

- Abad-Segura, E., González-Zamar, M-D., López-Meneses, E., & Vázquez-Cano, E. (2020). Financial technology: review of trends, approaches and management. *Mathematics*, 8(6), 951. <https://www.mdpi.com/2227-7390/8/6/951/pdf>
- Abimbola, A. (2023). The advantages and disadvantages of an e-Business. Mauco. [https://mauonline.net/the-advantages-and-disadvantages-of-an-e-business/#Advantages\\_of\\_E-business\\_for\\_the\\_Merchant](https://mauonline.net/the-advantages-and-disadvantages-of-an-e-business/#Advantages_of_E-business_for_the_Merchant)
- Adil, M. (2022). 10+ Advantages and Disadvantages of E-Commerce Business. Adil Blogger. <https://adilblogger.com/advantages-disadvantages-e-commerce-business/#advantages-of-e-commerce-business>
- Ainavolu, V. B. (2022). Impact of mobile phone usage on growth in e-commerce in India. *International Journal of Creative Research Thoughts*, 10(7), b47—b59. <https://ijcrt.org/papers/IJCRT2207134.pdf>
- ALadan, M. I. (2016). E-commerce security challenges: a taxonomy. *Journal of Economics, Business and Management* 4(10), 589-593. <http://www.joebm.com/vol4/457-MH0011.pdf>
- Ali, M., Hussin, N., & Abed, I. (2019). Electronic payment systems: Architecture, elements, challenges and security concepts: an overview. *Journal of Computational and Theoretical Nanoscience*, 16(11), 4826-4838. <https://www.researchgate.net/profile/Mostafa-A-Ali/publication/338213246>
- Almendariz, M. (2020). Ecommerce automation: 4 reasons why you need It to scale. Extensiv. <https://www.extensiv.com/blog/ecommerce-automation-benefits>
- Alsayed, A., & Bilgrami, A. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and advanced engineering*, 7(1), 109-115. <https://www.researchgate.net/profile/Anwar-Bilgrami/publication/315399380>
- Amanze, B. C., & Onukwugha, C. G. (2018). An enhanced model for bank fraud detection in Nigeria. *International Educational Journal of Science and Engineering*, 1(5), 4-11.
- Benny, A. (2023). Investment fraud: 22 scams to know of (and Avoid) right now. Aura. <https://www.aura.com/learn/investment-fraud>
- Bingwen Y., Chunqiong W., Rongrui Y., Baoqin Y., Nafang S., Xiukao Z., & Yanliang Y. (2021). Big Data-Based E-Commerce Transaction Information Collection Method. *Complexity*, 2021. <https://doi.org/10.1155/2021/8665621>
- Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, 27, 36–54. <https://doi.org/10.1057/sj.2012.11>
- Castro, M. (2022). The best payments systems for ecommerce. Sales Layer. <https://blog.saleslayer.com/best-payment-systems-ecommerce>
- Chiluiwa, I. M., & Chiluiwa, I. (2022). “We are a mutual fund:” how Ponzi scheme operators in Nigeria apply indexical markers to shield deception and fraud on their websites. *Social Semiotics*, 32(3), 355-380. <https://www.researchgate.net/profile/Innocent-Chiluiwa-2/publication/341473533>
- Chin, K. (2022). What is cryptography? And how you can secure your data. UpGuard. <https://www.upguard.com/blog/cryptography>
- Collins, C. (2017). Using excel and Benford’s law to detect fraud. *Journal of Accountancy*. <https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html>
- Copeland, B. (2023). Artificial intelligence. Encyclopedia Britannica. <https://www.britannica.com/technology/artificial-intelligence>
- Cross, C. (2019). Online Fraud. Oxford University Press. <https://doi.org/10.1093/acrefore/9780190264079.013.488>
- Das, S. (2022). Importance of mathematics in computer science. *The Coder World*. <https://www.thecoderworld.com/importance-of-mathematics-in-computer-science/amp/>
- Deepika, K. (2021). Importance of Mathematics—Assessment of Skill of Reasoning. *International journal of multidisciplinary educational research*, 10(7), 84-90. [http://ijmer.s3.amazonaws.com/pdf/volume10/volume10-issue7\(7\)/14.pdf](http://ijmer.s3.amazonaws.com/pdf/volume10/volume10-issue7(7)/14.pdf)
- DSouza, J. (2021). All the Math You Need to Know in Artificial Intelligence. Free Code Camp. <https://www.freecodecamp.org/news/all-the-math-you-need-in-artificial-intelligence/amp/>
- Eumer Merchant. (2016). What is an e-transaction? <http://eumermerchantaccount.com/what-is-an-e-transaction/>
- Fatonah, S., Yulandari, A., & Wibowo, F.W. (2018). A review of e-payment system in e-commerce. *Journal of Physics: Conference Series*, 1140(1), 012033. <https://iopscience.iop.org/article/10.1088/1742-6596/1140/1/012033/pdf>
- Frankenfield, J. (2022). Artificial intelligence: What it is and how It Is used. Investopedia. <https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp>
- Fuscaldo, D. (2023). Online business laws your small business needs to know. Business News Daily. <https://www.businessnewsdaily.com/15904-online-business-laws.html>

- Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & offenders*, 16(3), 316-342. [https://www.utica.edu/academic/institutes/cimip/Phishing\\_Evolves\\_Analyzing-the-Enduring-Cybercrime.pdf](https://www.utica.edu/academic/institutes/cimip/Phishing_Evolves_Analyzing-the-Enduring-Cybercrime.pdf)
- Ghosh, A. (2023). Ecommerce demand forecasting 101: Everything you need to know to grow your business. Seller App. <https://www.sellerapp.com/blog/ecommerce-demand-forecasting/#:~:text=E%2Dcommerce%20demand%20forecasting%20is%20a%20dynamic%20process%20that%20takes,demand%20for%20products%20sold%20online.>
- Ginni. (2021). What is the difference between encryption and cryptography? Tutorial's Point. <https://www.tutorialspoint.com/what-is-the-difference-between-encryption-and-cryptography#>
- Gundaniya, N. (2021). 7 benefits of electronic payments. Customer Think. <https://customerthink.com/7-benefits-of-electronic-payments/>
- Henson, S. (2017). What can identity thieves do with your personal information and how can you protect yourself? Experian. <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>
- Hossain, B. (2021). How technology has changed our day-to-day life. LinkedIn. <https://www.linkedin.com/pulse/how-technology-has-changed-our-day-to-day-life-md-billal-hossain>
- Hussain, A. (2022). What is identity theft? Definition, types, and examples. Investopedia. <https://www.investopedia.com/terms/i/identitytheft.asp>
- Hyperverge. (2022). Fraud detection: types of fraud, detection techniques and systems. <https://www.hyperverge.co/blog/types-of-fraud-detection-techniques-systems>
- IamCheated Research Team (2019). 10 Common types of internet fraud. <https://iamcheated.indianmoney.com/blogs/10-common-types-of-internet-fraud>
- Ibanichuka, E. A. L., & Oko, I. A. (2019). Electronic fraud and financial performance of quoted commercial banks in Nigeria. *International Journal of Advanced Academic Research*, 5(4), 15-35. <https://www.ijaar.org/articles/Volume5-Number4/Management-Practice/ijaar-mp-v5n4-apr19-p2.pdf>
- International Public Sector Fraud Forum (2020). Guide to understanding the total impact of fraud. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/866608/2377\\_The\\_Impact\\_of\\_Fraud\\_AW\\_\\_4\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866608/2377_The_Impact_of_Fraud_AW__4_.pdf)
- James, A., Bulajoul, W., Shehu, Y., Li, Y., & Obande, G. (2018). Security challenges and solutions for e-business. In: Awad, A.I. (eds) and Fairhurst, M. (eds.). *Information security: foundations, technologies and applications*. London: IET. <http://irep.ntu.ac.uk/id/eprint/34738/>
- Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, 10(1), 79-91. <https://www.researchgate.net/profile/Jurjen-Jansen/publication/305618427>
- Johnson, M. (2022). AI in eCommerce: Benefits and examples. Divante <https://www.divante.com/blog/ai-in-ecommerce-benefits-and-examples>
- Kanade, V. (2021). What is fraud detection? Definition, types, applications, and best practices. Spice Works. [https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-fraud-detection/amp/#\\_002](https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-fraud-detection/amp/#_002)
- Karo, R. K., & Sebastian, A. (2019). Juridical analysis on the criminal act of online shop fraud in Indonesia. *Lentera Hukum*, 6, 1-14. <https://core.ac.uk/download/pdf/295409203.pdf>
- Khillar, S. (2020). Difference between encryption and cryptography. Difference Between. <http://www.differencebetween.net/technology/difference-between-encryption-and-cryptography/>
- Kung, I. (2021). How Is Maths Used in Artificial Intelligence? Go Student. <https://insights.gostudent.org/en/how-is-maths-used-in-artificial-intelligence#Mathematics-in--AI-Is-this-the-future>
- Lin, T. C. W. (2016). Compliance, Technology, and modern finance. *Brooklyn Journal of Corporate, Financial & Commercial Law*, 11(1), 159-182. <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1225&context=bjcfcl>
- Lyra. (2021). All about e-payments. <https://www.lyra.com/in/e-payments/>
- MacKay, J. (2023). The Unexpected Dangers of Online Dating [11 Scams To Know]. Aura. [https://www.aura.com/learn/dangers-of-online-dating#1.-Catfishing-\(i.e.,-fake-online-dating-profiles\)](https://www.aura.com/learn/dangers-of-online-dating#1.-Catfishing-(i.e.,-fake-online-dating-profiles))
- Max, D. (2022). What is e-Business: meaning, types, components, model, and features. Temok. <https://www.temok.com/blog/what-is-e-business/>
- Miteva, A. (2022). 12 awesome benefits of online payments for businesses. My Moid. <https://www.mymoid.com/blog/benefits-of-online-payments/>
- Mohideen, B. I., & Mahendran, A. (2017). Secured e-commerce transactions through chaotic map. In *4th International Conference on Advanced Computing and Communication System*. (pp; 1-5).



<https://fardapaper.ir/mohavaha/uploads/2018/11/Fardapaper-Secured-E-commerce-transactions-through-choatic-map.pdf>

- Naab, R., & Bans-Akutey, A. (2021). Assessing the use of e-business strategies by SMEs in Ghana during the COVID-19 pandemic. *Annals of Management and Organization Research*, 2(3), 145-160.  
<https://amor.goodwoodpub.com/media/publications/364213-assessing-the-use-of-e-business-strategy-4694dfa8.pdf>
- Naikoo, A. A., Thakur, S. S., Guroo, T. A., & Lone, A. A. (2018). Development of society under the modern technology-a review. *Scholedge International Journal of Business Policy & Governance*, 5(1), 1-8.  
<https://www.researchgate.net/profile/Aasif-Naikoo/publication/324654099>
- Ndyulo, L. N. L. (2021). Protecting the right to identity against catfishing. [Masters Thesis, Rhodes University]. Commons.  
<https://commons.ru.ac.za/vital/access/services/Download/vital:56782/SOURCE1>
- Okonkwo, M. C. (2021). The growth of e-business in an emerging economy: The case of sma and medium sized enterprises in Nigeria. [Master's Thesis, Tallinn University of Technology].  
<https://digikogu.taltech.ee/et/Download/ea29ef44-6fb0-4c22-87f6-eb0dda881d3c/ErikasvtrkavamajandusegariikidesNigeria.pdf>
- Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020) E-Fraud in Nigerian Banks: Why and How?. *Journal of Financial Risk Management*, 9, 211-228. <https://doi.org/10.4236/jfrm.2020.93012>
- Pillemer, N. (2020). 10 Advantages of E-Commerce for Consumers & Businesses. Become. <https://www.become.co/blog/ecommerce-advantages-consumers-businesses/>
- Rana, K. (2022). Cryptological mathematics. *International Journal for Research in Applied Sciences and Biotechnology*, 9(3). <https://www.ijrasb.com/index.php/ijrasb/article/view/378>
- Ravichandran, H. (2023). Examples of fraud, scams & schemes to avoid right now. Aura. <https://www.aura.com/learn/examples-of-fraud#6.-Employment-scams>
- Reshma, A. (2022). In computer programming, what kinds of math are used? Byju's Future School. <https://www.byjusfutureschool.com/blog/in-computer-programming-what-kinds-of-math-are-used/>
- Rouse, M. (2023). Risk Management. Technopedia. <https://www.techopedia.com/>
- Samayawardena, D. T., & Sachindrani, D. M. T. (2018). Legal issues on electronic transactions: SL VS. EU. In 3rd Interdisciplinary Conference of Management Researchers, 23rd to 25th October. Sabaragamuwa University of Sri Lanka (pp: 355-359).
- Sarkar, T. (2018). Essential math for data science: 'Why' and 'How'. KDNuggets. <https://www.kdnuggets.com/2018/09/essential-math-data-science.html>
- Sarkar, T. (2023). What Is Benford's law and why is it important? Built In. <https://builtin.com/data-science/benfords-law>
- Sathiyarayanan, M. (2018). The role of maths in digital forensic investigations. *LinkedIn*. <https://www.linkedin.com/pulse/role-maths-digital-forensic-investigations-sathiyarayanan>
- Sheehan, A. (2022). Ecommerce laws and regulations to know for selling online. Shopify. <https://www.shopify.com/blog/ecommerce-laws>
- Singh, J. (2021). Cryptography: math or computer science? (must know info). Cyber Security Kings. <https://cybersecuritykings.com/2021/05/18/cryptography-math-or-computer-science-must-know-info/>
- Singh, S. (2015). How algorithms will drive the growth of e-commerce in the future. The Economic Times. <https://m.economictimes.com/tech/internet/how-algorithms-will-drive-the-growth-of-e-commerce-in-the-future/articleshow/45801937.cms>
- Smirti (2018). Benefits of e-business - 10 advantages of e-business. Management Notes. [https://www.managementnote.com/benefits-of-e-business/#The\\_scope\\_of\\_e\\_commerce\\_is\\_%E2%80%A6%E2%80%A6%E2%80%A6%E2%80%A6\\_than\\_digital\\_business](https://www.managementnote.com/benefits-of-e-business/#The_scope_of_e_commerce_is_%E2%80%A6%E2%80%A6%E2%80%A6%E2%80%A6_than_digital_business)
- Tunggal, A.T. (2022). What is Digital Forensics? Up Guard. <https://www.upguard.com/blog/digital-forensics>
- Utsi, P. J. (2022). AI in ecommerce: Use cases and how to get started. Vaimo. <https://www.vaimo.com/ai-in-ecommerce/#:~:text=AI%20enables%20an%20ecommerce%20website,were%20interacting%20with%20a%20person.>
- Williams, L. (2023). What is digital forensics? History, process, types, challenges. Guru 99. <https://www.guru99.com/digital-forensics.html#4>
- Wu, J. (2022). Why the future of e-commerce lies in forecasting? Supply and Demand Chain Executive. <https://www.sdexec.com/sourcing-procurement/erp/article/22030944/oceanwing-why-the-future-of-ecommerce-lies-in-forecasting>
- Zaharon, N. F. M., & Ali, M. M. (2021). Phishing as cyber fraud: The implications and governance. *Hong Kong Journal of Social Sciences*, 57, 119-133. <http://www.hkjoss.com/index.php/journal/article/viewFile/432/428>