SECURITY ASPECTS OF DIGITAL TRANSACTIONS E-COMMERCE AND M-COMMERCE IMPLEMENTATIONS

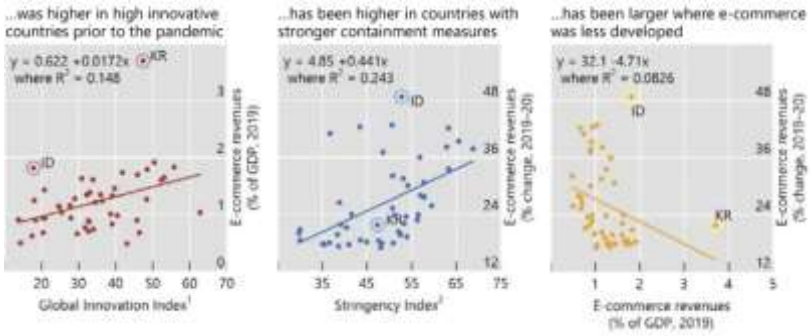
Martin Kiselicki
Faculty of Economics, University Ss. Cyril and Methodius in Skopje, North Macedonia,
Martin.Kiselicki@eccf.ukim.edu.mk
Snezana Ristevska Jovanovska
Faculty of Economics, University Ss. Cyril and Methodius in Skopje, North Macedonia,
Snezana.ristevska@eccf.ukim.edu.mk
Zanina Kirovska
Integrated Business Institute in Skopje, North Macedonia, zanina.kirovska@fbe.edu.mk
Milan Anastasovski
Institute for Transfusion Medicine in Skopje, North Macedonia, milan.atn@gmail.com
Dimitar Jovevski
Faculty of Economics, University Ss. Cyril and Methodius in Skopje, North Macedonia,
Dimitar.jovevski@eccf.ukim.edu.mk

Abstract: Through the accelerated digitization in business, new models of digital transactions are becoming more popular in the last few years. In electronic commerce, in addition to the standard models of B2B (business to business) and B2C (business to customers), m-commerce is becoming increasingly popular, which is defined as conducting e-commerce through wireless communication devices, smartphones and tablets. M-commerce is a new and cutting-edge way of doing business in the world. M-commerce is carried out through mobile devices and appropriate data transfer protocols. This way of doing business is on the rise in the world because the user is not bound to place and time, the service is available anywhere at any time. The paper defines the differences between typical models of e-commerce and m-commerce, in order to make a clear distinction between them. The growth of m-commerce has been investigated in more detail through available statistics and other secondary sources, where trends can also be determined in the next few years, where it is assumed to become one of the dominant patterns of online transactions. The increase in transactions through digital channels also leads to new dangers and security threats, which are amplified because they are new and less tested technologies that could have security flaws. The paper explores the various security threats in e-commerce and m-commerce through analysis and synthesis, where it is shown that there are six different aspects, including integrity, non-repudiation, authenticity, confidentiality, privacy and availability. These aspects are analyzed in more detail through their special elements, as well as the possible strategies for their management. Security, as a very important issue in e-commerce systems, should be taken under the control of companies and government institutions. To this end, a well-managed technology-based strategy should be implemented. A special focus is devoted to the risks and threats in e-commerce, as well as defining the different types of cybercrime that characterize these digital transactions. Through the presentation of the various security aspects of e-commerce and m-commerce, the paper contributes to a better understanding and formation of strategies to deal with the security of transactions with the help of these digital technologies, as well as more frequent changes and synchronization of legal regulations by the institutions in charge of the same ones. Trust in these types of transactions is one of the key elements for their projected growth in the future, making the perception of security vital in the online shopping decision.
Keywords: E-commerce, m-commerce, computer crime, security, m-commerce threats

1. INTRODUCTION

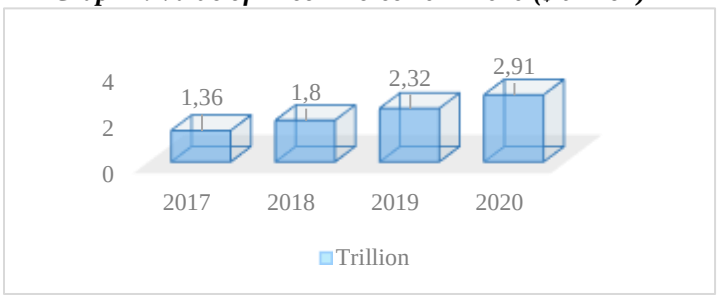
E-commerce transactions have been on the rise in recent years, especially evident during the lockdown periods of the COVID-19 pandemic. E-commerce refers to buying and selling goods and/or services over the Internet (Alfonso et al., 2021). Due to the utilization of Internet technologies, e-commerce transactions were able to be done without a physical presence, from any geographical location. These characteristics were the main driver towards the increased e-commerce adoption between 2020 and 2022. Graph 1 shows that E-commerce adoption is accelerated in each country type – ones with high innovation index, ones with stronger containment measures and less developed countries.

Graph 1. E-commerce adoption during the COVID-19 pandemic



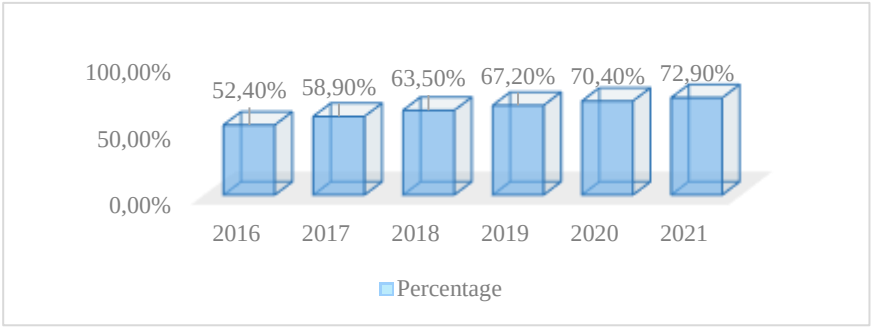
Mobile commerce refers to the conduct of e-commerce through wireless communication devices, smartphones and tablets. M-commerce is carried out through mobile devices and appropriate data transfer protocols. This way of doing business is on the rise in the world because the user is not bound to place and time, the service is available anywhere at any time. As the pandemic restrictions ended, users who adopted e-commerce found purchasing through mobile devices a convenience since it enabled them to be on the move, while still realize their desired online transactions. M-commerce involves purchasing via a mobile device, mobile marketing, mobile banking or using a digital wallet. Mobile shopping in addition to mobile apps can also be done through optimized websites, even through social media platforms (Kourouthanassis & Giaglis, 2012). A prerequisite for the development of m-commerce is the progress and introduction of new technologies in mobile telecommunications, that is, the development of the Wi-Fi network, network services (3G, 4G, 5G), the global system for mobile communication (GSM), etc. Interest in m-commerce is increasing with the availability and mass of mobile technology as well as the possibility of cheap access to mobile internet. The perspective for the growing development of m-commerce comes from the opportunities to develop new business models and the integration of new technologies (Scheepers et al., 2009).

Graph 2. Value of M-commerce 2017-2020 ($ trillion)



Graph 2 and Graph 3 indicate the global growth trend of mobile commerce. Some estimates say that the percentage of m-commerce in the total e-commerce will be up to 75% in the coming years. The reason for the growth so far, on which future estimates are based, is the rapid development of mobile technology and mobile devices, new innovative solutions, accessible mobile internet and the integration of mobile applications in all segments of everyday life. M-commerce will continue to develop and new opportunities and new challenges will appear.

Graph 3. Percentage of M-commerce in E-commerce (%)



One of the main obstacles in e-commerce is consumer distrust in security. This stems from the fear of how their personal data is used as well as the risk of online fraud. With the rapid growth of e-commerce, security risks have also increased in scope. The security of users' computers and mobile devices depends on the security of online transactions and payments (Sangeetha & Suchitra, 2016). It is of great importance to provide security that will meet the needs of users and that will protect them from problems on the Internet. User-friendly e-commerce systems must be secure and reliable to use (Wen & Zhou, 2008). It is important to protect personal data, numbers from payment cards as well as the products that are ordered, otherwise the consumer may suffer financial, social or other damage from unauthorized persons who will have access to them.

2. MATERIALS AND METHODS

For research purposes, secondary data is utilized - scientific papers, studies, books, academic journals, case studies. They will serve to give an overview, current conditions and future aspects in of security and privacy aspects of e-commerce. Several types of research methods were used in the paper:

- Descriptive method, used to describe the basic terms related to the subject of research, through definition and explanation;
- Analytical method, analyze the existing researches;
- The logical method is used for proof when making the final conclusions and recommendations;
- Method of generalization, through which individual observations and observations should lead to general conclusions, which are based on reality.

3. SAFETY ASPECTS OF E-COMMERCE AND M-COMMERCE

Security technologies are largely developed enough for e-commerce and m-commerce in recent years. However, basic security technologies are not yet supported by relevant international law. In an electronic world full of data, messages and transactions, it is important for companies and users to rely on electronic safeguards. In order to be first to market a few years ago, important safety measures were often left out of the planning and have not been taken into account since (Khosrow-pour, 2004). This should not happen despite the turbulence and increasing competition in the e-market. User security should be one of the priorities in e-commerce despite the fact that building secure online transactions is a difficult task as a result of the globalization of business. Computer security is a very complex and widespread topic aimed at protecting data, assets and network from unauthorized access, use, alteration or destruction. Computer attacks and defences can affect individuals, companies, countries, or the entire Internet. The goal of computer security is to prevent or at least minimize attacks. Because of the complexity of computer security, it is divided into two categories: general security related to information systems (for example, encryption) and electronic commerce security, such as consumer protection. Ensuring safe conditions for companies is an important and challenging task. Without absolutely secure e-commerce and m-commerce transactions, it is almost impossible to take advantage of the technology. It is also very difficult to gain the trust of consumers to use e-commerce without secure e-commerce websites and applications.

Reducing risk in electronic commerce is a complex process that includes new technologies, procedures and company strategies, as well as new laws and standards that will enable law enforcement institutions to investigate and prosecute criminals. E-commerce and m-commerce security has six key dimensions (Landon & Traver, 2018):

- **Integrity** - refers to the ability to display secure information through the website or secure data sent and received over the Internet;
- **Non-repudiation** - ensuring that e-commerce participants do not deny (reject) their activities over the Internet. After the transaction is completed, one party can deny that it happened. Although this may be due to a mistake, it still creates a conflict situation that cannot be easily resolved;
- **Authenticity** - the ability to identify the identity of the person or company with whom you communicate on the Internet;
- **Confidentiality** - ensuring that messages and data are available only to those who have the right to see them;
- **Privacy** - the ability to regulate customer information in order to preserve their privacy;
- **Availability** - refers to the ability to guarantee the performance of the website and e-commerce applications as expected.

To produce trust in consumers, e-commerce and m-commerce websites (and subsequently transactions) are preferred to encompass all six aspects. It is difficult to estimate the trust level fall-off ratio without individual aspects, but there is an evident decline which could result in transaction abandonment issues if some security risks are present in regards to the six aspects.

To increase the level of security in e-commerce and m-commerce, vendors usually rely on several technologies:

- **Data encryption technology**. A special algorithm is used here to encrypt and transform information into encrypted text in order to ensure data privacy (Chu, 2019). This helps in protecting user details from various attacks when transferring and storing data;
- **Digital signature technology**. Through special cryptography, a sequence of characters and codes is generated, followed by a password for an electronic signature. These electronic signatures are verified and their accuracy is checked (Shen & Huang, 2011);
- **Digital certificates**. A certification and digital signature body uses various encryption and authentication technologies to ensure security and efficiency in electronic transactions;
- **Security authentication protocol**. There are two widely used security authentication protocols in e-commerce, SSL (Secure Sockets Layer) and SET (Secure Electronic Transaction) protocol. Websites with secure transfers make sure to include an SSL certificate, which is an indicator of trust to consumers. For example, Google ranks websites with SSL certificate higher than others without it (Google, 2022);
- **Other security technologies**. Some common methods are also used, such as network firewall, virtual private network (VPN) and antivirus protection. E-commerce technology alone is not enough and needs to be integrated with other security measures in order to provide a more robust security framework for users.

Risks and threats

Most companies believe that their e-commerce information systems are secure, but in reality, this is not always the case. Specific hardware and software solutions are not sufficient by themselves for system security. The risk in the modern world is high for companies that do not have a precise and decisive strategy for the security of the e-commerce system. Every company has a responsibility to take steps to reduce security risks. The success of providing secure e-commerce depends on the complex connections between the various platforms, database management systems, system software and network infrastructure.

There are many carriers of potential threats and risks in e-commerce and m-commerce, the main ones are:

- **Vulnerable website design**. The Internet and its network protocols were developed to enable computer communication in a trusted community. Therefore, the internet and its protocols are still fundamentally insecure and unable to prevent cybercriminals;
- **Transition to cybercrime for profit**. In the early days of e-commerce, many hackers simply wanted to gain fame or popularity by crashing websites. Today there are many more criminals, who are more sophisticated and technically experts. The most popular is the theft of personal information, credit card numbers, bank accounts, Internet IDs and passwords (Turban et al., 2015);
- **Wireless revolution**. Wireless networks are more difficult to secure than wired networks. Hackers can abuse the functions of smartphones and other devices;
- **Internet black economy**. This black Internet economy refers to e-markets for stolen information and consists of thousands of websites that sell credit card numbers, social security numbers, email addresses, bank account numbers, social network identifiers, passwords and more (Gaspareniene et al., 2016);
- **The sophistication of the attacks**. Cybercriminals are constantly refining their attack tools and skills through technological innovation. They change tactics due to increased security in certain areas and quickly adapt to the situation**.**
- **Operating systems issues.** The final issue present is indirectly connected to m-commerce, which is the underlying platform and architecture. The majority of phones are running either Android with 71.52% in 2022 or iOS with 27.83% in 2022 (Statista, 2022), which are not immune to malware attacks. Recent operating systems have a higher vulnerability score with iOS 15 (8.6) and Android 12 (2.3), while also including a lot of open-source elements which can be exploited (Clario, 2022).

Computer crime

Computer crime is primarily characterized by high dynamics and various types of manifestations. New, much more dangerous forms of criminal behaviour are also appearing, which have not been known before and which know no borders in the world. Hackers are very intelligent perpetrators, and the only real protection against their attacks is strengthening cryptographic protection systems and a tougher criminal policy towards them.

Publicity about various online crimes has led to more concern than is warranted. The fear increases especially when the publicity involves well-known companies (Durkan et al., 2003). Computer crime exists, the public should be made aware of it and preventive measures should be taken.

Fraud

Internet fraud takes many forms, it happens through lying, impersonating users or intercepting data. Fraud with non-delivered products is common, which is connected to non-existent companies that present themselves as such on the Internet. Some unscrupulous companies may charge for services they advertised as free (such as shipping charges).

Theft of personal data and identity theft

More egregious examples of cybercrime are credit card fraud and identity theft; however, it should be noted again that these frauds are not as common as one might think and are usually dealt with promptly and effectively (Regnier & Sahadi, 2006)**.** It should also be added that the use of user data is not always the result of cybercriminals, but of companies that collect data for referral or sale to a third party.

Malicious software

These tools are constantly changing as different forms of protection evolve. One of the most common malicious software used is the "Trojan horse". This software disguised as useful and safe software contains additional hidden code that allows unauthorized collection, exploitation, falsification, or destruction of data (Fuentes et al., 2010). A more frightening example than the Trojan horse is the "HTML injection" technique (Imperva, 2020). This technique modifies the HTML code before the user is taken to the web page. The problem here is that this threat does not break the website's security measures because it manipulates the website's code and not the security. Consequently, the protection of the website is not activated and the user, thinking that he is on the safe side, is in danger of data theft.

Ransomware

Ransomware (ransomware) is a type of malicious software that threatens to release a victim's data, block access to it, and often threaten permanent destruction unless a ransom is paid (Maurya et al., 2018). More advanced ransomware uses a technique called cryptoviral extortion. It encrypts the victim's files, makes them inaccessible and demands payment of a ransom to decrypt them. File recovery can only be performed if the decryption key, which is only available to the attacker, is provided. In these attacks, the ransom is required to be paid in the form of cryptocurrencies because they are very difficult to trace and detect the attacker.

5. CONCLUSIONS

The development and increased use of information technology has led to the emergence of new types of computer crime and security breaches in e-commerce and m-commerce. Technology can be misused in various ways, and cybercrime itself can take the form of any of the traditional types of crime, such as theft, evasion, embezzlement, while unauthorized data obtained through the misuse of information systems can be used in various ways. for obtaining an illegal benefit. Through modern technology, criminal acts have become much easier and even faster. Companies and countries should take appropriate measures in dealing with security risks. These measures should be a combination of technological and legislative measures because only with integrated innovative security programs and a regulated legal framework can security violations be prevented.

M-commerce is specifically concerned because of differentiating factors, such as utilizing wireless networks which are less secure than wired ones, more prone to sniffing and phishing attacks and mobile operating system threats and risks which are always present especially through recent OS updates. To ensure the progress of m-commerce, companies must take into account the security aspects and security risks outlined in the paper and act accordingly, to minimize user doubt in the process. As these types of transactions grow in overall e-commerce, there will be increased interest in implementing malicious software or frauds to capitalize on them. The paper explores different security risks and threats in e-commerce and m-commerce specifically, with a deeper dive into the trends that could follow in the future. Research can be expanded by case studies of m-commerce protection mechanisms, as well as primary research to determine the trust in these types of transactions from the consumers,

REFERENCES

Alfonso V., Boar C., Frost J., Gambacorta L., & Liu J. (2021). E-commerce in the pandemic and beyond. BIS Bulletin, No 36

Durkan, P., Durkin, M., & Gillen, J. (2003). Exploring Efforts to Engender On-line Trust. International Journal of Entrepreneurial Behaviour & Research, Vol. 9. No. 3

Fuentes D., Garcia J., Ortega J., Abril L., & Velasco-Morente F. (2010). Trojan horses in mobile devices. Comput. Sci. Inf. Syst.. 7. 813-822. 10.2298/CSIS090330027F.

Gaspareniene, L., Remeikiene, R., & Navickas, V. (2016). The Concept of Digital Shadow Economy: Consumer's Attitude, Procedia Economics and Finance, volume 39, pp. 502-509

Hale, T., Webster, S., Petherick, A., Phillips, T., & Kira, B. (2020). Oxford COVID-19 Government Response Tracker", Blavatnik School of Government.

Khosrow-pour, M., (2004). *E-Commerce Security: Advice from Experts*. Hershey, PA:Idea Group Publishing

Kourouthanassis, P. E., & Giaglis, G. M. (2012). Introduction to the Special Issue Mobile Commerce: The Past, Present, and Future of Mobile Commerce Research, International Journal of Electronic Commerce, 16(4)

Laudon, K. C., & Traver, C.G. (2018). *E-commerce*: *Business, Technology, Society 13/e*. USA: Pearson

Maurya, A.K., Kumar, N., Agrawa, A., & Khan, R. (2018). Ransomware Evolution, Target and Safety Measures, INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING 6(1):80-85

Regnier, P., & Sahadi, J. (2006). Thwart the ID Thieves. Money, Vol. 35, No. 12: 2006, 124-125

Sangeetha M., & Suchitra R. (2016). The Study of E-commerce Security Issues and Solutions, International Journal of Engineering Research & Technology (IJERT), Special issue 2017, NCRIT – 2016 Conference Proceedings

Scheepers, H., Zeeshan S.A., & Cheung Y. (2009). Influencing Factors for the Adoption of m-Commerce Applications. Monash University, Australia: 11th International Conference on Enterprise Information Systems, 53-60

Shen G., & Huang X. (2011). Advanced Research on Computer Science and Information Engineering. International Conference, Springer:2011, 163-164

Statista (2020). Statista Global Consumer Survey, August.

Turban, E., King, D., Kyu Lee, J., Liang, T., & Turban, D. (2015). *Electronic Commerce: A Managerial and Social Networks Perspective.* Springer Cham Heidelberg New York Dordrecht London: Springer International Publishing Switzerland

World Intellectual Property Organization (2020). "Global innovation index 2020: who will finance innovation?"

Yuanqiao, W., & Chunhui, Z. (2008). Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management

Internet sources:

https://domains.google/tld/security/ (accessed on 10.05.2022)

https://gs.statcounter.com/os-market-share/mobile/worldwide (accessed on 15.06.2022)

https://clario.co/blog/ios-vs-android-security/ (accessed on 11.08.2022)

https://www.imperva.com/learn/application-security/html-injection/ (accessed on 10.08.2022)

https://www.statista.com/statistics/806336/mobile-retail-commerce-share-worldwide/ (accessed on 11.08.2022)