Money and Payment Systems in E-Commerce

Secure E-Commerce Technologies

Faculty of Computer Science and Information Technology

Professor:

Dr.sc.ing. Arnis Lektauers

Team Members:

Ibrahim Can Kilic

Kyaw Min Thant

Edgars Izvestnijs

RIGA, 2022/2023

TABLE OF CONTENTS

1. ELECTRONIC PAYMENTS IN E-COMMERCE

1.1. Electronic payments definition

Nowadays, people prefer to shop online because it is more practical and less time-consuming to purchase. E-commerce enhances sales, buying activities by the people and is backed by electronic payment systems. The public is becoming more obliged to buy online with an increasing demand. Due to the Internet implementation deliveries became faster, broader, more efficient and accurate. E-commerce is one of the results of Internet implementation in the economic field. [1]

In general, e-payment refers to online payments using the Internet. It has various benefits for buyers, sellers, banks, organizations, governments and etc. Any online business needs a fast, secure and reliable system to receive payment from their customers. E-commerce online payment systems are designed to facilitate transactions with maximum efficiency. [1,2]

An online payment works by using a payment gateway to connect digital store to the payment processing system of a choice. This system then works with the bank to distribute funds. It underpins all paperless monetary transactions and has revolutionised the business of processing payments. It has also led to significant reductions in transaction, paperwork and labor costs. [2]

E-commerce sites use electronic payment, being user friendly and less time-consuming than manual processing, it helps business organization to expand its market reach/expansion. [2]

The most common electronic payment method include [2]:

- Credit card;
- Debit card;
- Smart card;
- Electronic money (e-money);
- Electronic funds transfer (EFT);
- Mobile payments.

1.2. Credit card

Credit card payment system is one of the most common electronic payment types. It is small plastic card with a unique number attached to an account. It also has a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which can pay the credit card bill. [3,4,5]

The following key components in the credit card system are [3,4,5]:

- Card holder (customer);
- Merchant − seller of product who can accept credit card payments;
- Card issuer − card holder's bank;
- Acquirer bank − the merchant's bank;
- Card brand − Visa, Mastercard, etc.

1.3. Debit card

Debit card is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between a debit card and a credit card is that in case of payment through debit card, the amount gets deducted from the card's bank account immediately and there should be sufficient balance in the bank account for the transaction to get completed. Debit cards free the customer of carrying cash. [3,4]

1.4. Smart card

Smart card is similar to a credit or a debit card in appearance, but it has a small microprocessor chip embedded in it. It has the capacity to store a customer’s work-

related and/or personal information. Smart cards are also used to store money and the amount gets deducted after every transaction. [3,5]

Smart cards can only be accessed using a PIN that every customer is assigned with. Smart cards are secure, as they store information in encrypted format and are less expensive/provide faster processing. Visa Cash and Octopus cards serve as an example of smart cards. [3,4]

1.5. E-money

Electronic money transactions refer to situation where payment is done over the network and the amount gets transferred from one financial body to another financial body without any involvement of a middleman. E-money transactions are faster, convenient and save a lot of time. [4.5]

Online payments done via credit cards, debit cards, or smart cards are examples of e-money transactions. Another popular example is e-cash. In case of e-cash, both customer and merchant have to sign up with the bank or company issuing e-cash. [4,5]

1.6. Electronic fund transfer

It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in the same bank or different banks. Fund transfer can be done using an ATM (Automated Teller Machine) or using a computer. [4,5]

Nowadays, internet-based EFT is getting popular. In this case, a customer uses the website provided by the bank, logs in to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account. Customer's bank transfers the amount to other account if it is in the same bank, otherwise the transfer request is forwarded to an ACH (Automated Clearing House) to transfer the amount to other account and the amount is deducted from the customer's

account. Once the amount is transferred to other account, the customer is notified of the fund transfer by the bank. [4,5]

1.7. Mobile payments

One of the latest ways of making online payments are through mobile phones. Instead of using a credit card or cash, all the customer has to do is send a payment request to his/her service provider via text message. The customer's mobile account or credit card is charged for the purchase. To set up the mobile payment system, the customer just has to download a software from his/her service provider's website and then link the credit card or mobile billing information to the software. [5]

2. MOBILE PAYMENTS IN E-COMMERCE

2.1. Mobile payments definition

Many banks have adopted technology into their banking apps that allow customers to send money instantly to friends and family members directly from their bank accounts. Mobile payments are also made on site at stores by scanning a barcode from an app on a phone, accepting payments from convenience stores to large, multi-national retailers. [6]

The cost of the purchase may be deducted from a pre-loaded value on the account associated with the particular store, or paid by credit or debit card. Payment information is encrypted during transmission, so it is thought of as being a safer payment method than paying with a debit or credit card. [6]

Mobile payments first became popular in Asia and Europe before becoming more common in the United States and Canada. Early on, mobile payments were sent by a text message. Later, technology allowed for pictures of checks to be taken via cell

phone camera and sent to the payment recipient. This technology eventually morphed into mobile check deposit capabilities for banking apps. [6]

The most obvious benefit of mobile payments is the elimination of a physical wallet. It saves time to not pull out cash and is also safer as as nobody is able to see the contents of your wallet/purse. [6,7]

Payments made through wireless devices like mobile phones and smartphones are thought to provide more convenience, reduce the fee for the transaction, and increase the security of electronic payments. This payment system has also made it easier for businesses to collect useful information about their customers and their purchases. [7]

Mobile payment methods are suitable for offline micropayments as well as for online purchases. This method is a potential attraction for online traders due to an enormous user base of mobile phones. The use of mobile payment service does not only reduce the overall cost of a transaction but also offer a better payment. [7]

However, mobile payment systems have encountered certain challenges in obtaining a significant consumer base for a number of reasons including privacy issues and their inability to organize international payments. [7]

An additional benefit - though a minor one for most people - is that when you are with other people they are not able to tell what card you have. Users with low credit scores and credit cards with low limits might not want, say, an interviewer or date to know these things, and mobile payments offer an additional level of personal privacy.

Mobile transaction volume is growing explosively: Mobile platforms are now a powerful force in shaping the payments industry, particularly credit and debit card payments. A significant portion of card-powered e-commerce transactions take place on tablet or smartphone devices. Tablets and smartphones are also powering transactions at physical stores - on the consumer and merchant side - through apps, scannable QR codes and attachable card readers that transform devices into cash registers. [8,9]

A mobile payment transfer service is shown in Fig. 2.1.1 below [9]:

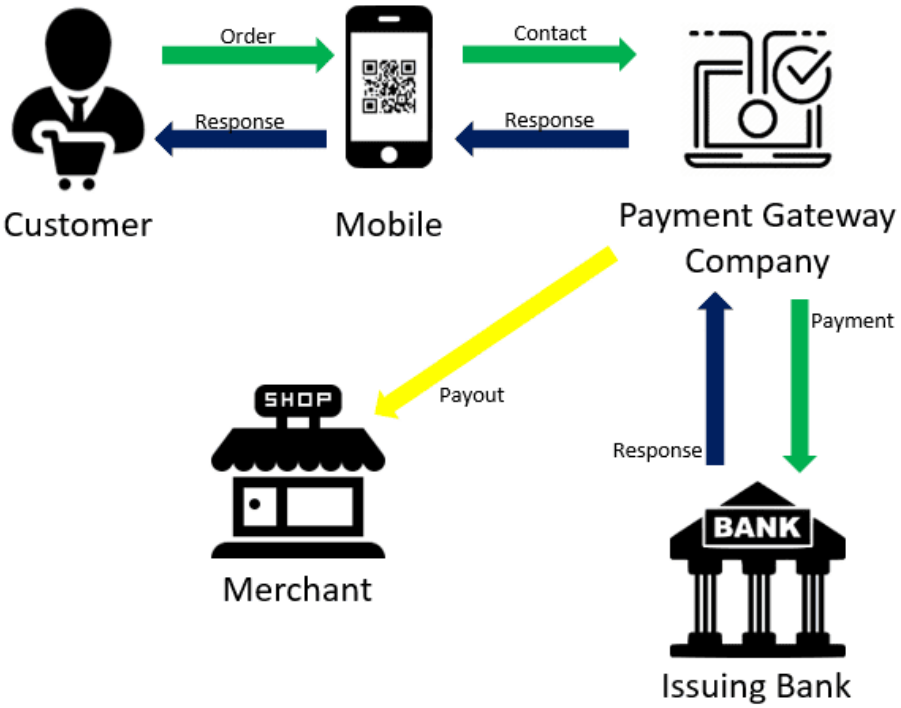

Fig. 2.1.1. Mobile payment process [9]

2.2 Advantages/benefits of mobile payment systems

The following mobile payment advantages are [8,9]:

- One-click payments - online mobile payment offers a quick check-out process that customers can perform by just one click;
- Fast payments - payments via mobile can be done anytime from anywhere and they minimize the time spent while performing a transaction. Mobile payment simplifies the transaction process not only for the customer but also for business owners;
- Better customer experience - provides customers with a better shopping experience by giving a competitive pricing and a variety of products;
- Business utilities – mobile banking, stock market, booking and other features.

2.3. Types of mobile payment systems

- Near-field communication (NFC) payments - a contactless form of payment that uses NFC technology to exchange information between payment devices. NFC-enabled payments need a reader device that can accept contactless payments. These payments are secure as they use dynamic encryption;
- Magnetic secure transmission (MST) payments – a form of payments, in which mobile emits a magnetic signal that is identified and picked up by a card terminal. This method uses a tokenization system making it one of the secure contactless payment acceptance methods;
- Quick response (QR) code payments – it is one of the most popular types of online mobile payment technologies used in e-commerce. Payment is done by scanning the QR code with a QR scanner app or a mobile camera.
- Mobile wallets – mobile wallets are pre-loaded with cash and provide a one-click payment option. Payments via mobile wallets are faster and more convenient;
- Mobile credit card processing - mobile devices are used as a reader for credit cards to accept payments. Payment done via this method is secure fast and beneficial for small or home-based businesses.
- Mobile web-based payments - a customer can access web pages through the mobile or using a mobile payment gateway

2.4. Business impact of mobile payments

Digital wallets like Apple Pay and Google Pay allow customers to purchase goods and services with their digital devices, including smartphones, smartwatches, computers and IoT devices. A mobile-first approach to commerce is the new norm for businesses. Capturing sales from many devices comes with extraordinary benefits, such as better user experience and functionality and increased customer reach. [10]

Since customers are already using their mobile phones, digital wallet use will continue to accelerate. From 2020 to 2025, Statista predicts digital wallet use will double worldwide. [10]

Today, biometric authentication like facial recognition speeds up transactions. Once the digital wallet is activated, customers simply hover their mobile devices over point of sale (POS) terminal to complete a transaction in store in a matter of seconds, saving time and effort for customers and businesses. Digital wallets allow for a safer, no-contact experience for both employees and customers. [11]

Digital wallets are more secure than a card on a traditional POS terminal. When using a digital wallet, the customer's card number is never entered. The information taken from the digital wallet during the transaction is not a card number, but a tokenized version of that data, plus a one-time number tailored to the individual sale. Tokenizing payment information provides an extra layer of protection for business. [11]

In addition to all the benefits of enabling payment by digital wallets mentioned above, providing a mobile app with in-app payment functionality offers additional value to the company brand. This functionality helps to retain customer and benefit from sales, as well as build customer loyalty level.

There are several ways how you can build such loyalty level, such as encouraging to perform specific actions on the platform customers use – the reward that the customer gets is either a personalized offer or a valuable disacount.

Additionally, for those businesses that serve customers on the go a mobile point of sale (mPOS) allows to turn a mobile device into a POS. An mPOS takes chip-enabled cards, contactless payments, and magstripe forms of payment. It also tracks cash and check payments. This technology uses NFC, which efficiently lessens the pay time and attracts more customers who prefer to pay in convenience [11]

3. THE ROLE OF SECURITY FOR E-COMMERCE SYSTEMS

3.1. E-commerce cyber attacks and security

Essentially, e-commerce security refers to a set of guidelines that ensure safe purchasing procedure on the internet. This security includes protocols that protect both the businesses selling their products online, as well as the customers sharing their personal information to purchase these goods. [12]

There are four following e-commerce security protocols [12]:

- Authentication - establishes that both buyer and seller are verifiable identities, that they are who they claim to be;
- Privacy - refers to the protection of customer data, especially from unauthorized third parties;
- Integrity - data remains unedited or altered in any form;
- Non-repudiation - assurance that the validity of something cannot be denied.

E-commerce supply chains face risks from cyber-attacks. Consumers who purchase goods online also risk having their private information stolen. Thus, businesses are investing to improve cyber-security at some cost. Both e-commerce platforms and governments treat cyber-attacks very seriously, as they can compromise users's privacy and may be disastrous for the companies involved. To enjoy the convenience of shopping online, consumers typically need to submit their private information. For example, while mobile payment systems have brought new opportunities for merchants and customers, they have also exposed them to new risks regarding privacy and security issues. The future of mobile payments can be secured by using the latest technology in order to overcome practical and analytical challenges faced by this industry. [13, 14]

Radio barcodes technology is believed to be a revolutionary addition to mobile payment systems. These barcodes send out radio signals that can be used to locate the position of things they are embedded on. By utilizing this technology mobile payment market gets provided an enhanced security and convenience to its consumers. With

enhancing the security protocols and using the latest technology like radio barcodes, mobile payment service providers can create a system that is not only scalable at greater levels but is also most convenient to use for the consumers. [14]

To prevent consumer information from being stolen, e-commerce companies are obligated to implement the right technologies at a nontrivial cost. According to Gartner, worldwide spending on information security products and services exceeded US$114 billion in 2018, representing an increase of 12.4% from US$101.54 billion in 2017. Gartner also predicted that end-user spending for the information security and risk management market will grow at a "compound annual growth rate" of 8.7% from 2018 through 2023 to reach $188.4 billion.3 In addition to e-commerce companies's cyber-security measures, governments all around the world take different measures for cyber-security-related challenges. [13]

The growing popularity of online payment services and payroll systems has opened new pathways for hackers to steal consumers's information and money, a risk, which poses significant threat to the users of e-commerce and banking websites.[13]

3.2. Biometrics

Biometrics are unique, physical, or behavioral characteristics that uniquely identify a person. The right combination of both can help make e-commerce more secure and convenient. Fingerprints and iris scans, for example, can help ensure that a user's identity is protected and that the transaction will be a successful one. The key to selecting the right biometrics for e-commerce is making it easy for consumers to enter their personal information. Biometrics are increasingly being used to protect e-commerce. Facial scanning, for example, is becoming a popular way to make purchases online. It takes an image of a person's face and matches it with a database of similar images. It's a simple process that eliminates the need for complicated passwords. Unlike traditional forms of authentication, biometrics can be used to strengthen the security of e-commerce transactions. [15]

3.3. Malware, privacy and accessibility in e-commerce

The use of malicious software, or malware, is an illegal attempt to breach secure digital ecosystems to access personal information such as names, passwords, and bank account numbers. The e-banking and e-commerce sectors are more concerned with identity fraud than any other industry. [16]

E-commerce has also come to play a crucial role in fulfilling customer demand. With operating system (OS) support, e-commerce applications cannot function on the internet. Online business managers are usually careless and know nothing about possible cyber threats due to a lack of security knowledge [16]

Privacy and accessibility are also essential issues in e-banking. Companies have invested extensively in the security and user interface of their websites, as these websites are frequently targeted by cybercriminals. [16,17]

Prevention from all the activities that result in sharing customer data with unauthorized third parties is called privacy. It must be ensured that customer data and account details stay between the retailer and the customer only, and no third party is included. [17]

Most of the time, the sellers are responsible for the breach of confidentiality when they let others have access to private data. As an online business, it is your job to enable at least a bare minimum of firewall, anti-virus, encryption, or other data protection. It will help to ensure customers that their payment details are safe. [18]

3.4. Types of attacks targeting e-commerce businesses

In addition, it is necessary to know the common vulnerabilities and attacks of the e-commerce security. There are several well-known attacks that target e-commerce services and websites, such as [19,20]:

- Phishing - a social engineering attack used by malicious actors to trick victims into providing personal and confidential information like accounts, passwords, social security numbers, and etc.. It is typically done via email, phone calls, or texts. The process is simple – victim clicks on a malicious link or downloads a file, which compromises personal information or even deploys are ransomware on a device;
- Malware/ransomware - if the website is injected with malware or ransomware, customers might get their devices infected which can lock them out of their system and important data. When customers face an experience like this, the chances of revisiting a website are next to none. Sometimes even commerce servers can get infected, which can result in serious downtime and abnormal cost for the business itself;
- Zero-day exploit/vulnerability - an unknown security flaw that someone can take advantage of. Zero-day exploits are particularly dangerous e-commerce security threats, because they rely on undiscovered vulnerabilities that are difficult to spot and patch immediately;
- E-skimming - the digital version of credit card skimming. While in the physical world, skimmers are installed over credit card readers to skim credit card information, e-skimmers are pieces of malicious code that steal a customer's credit card data during an online transaction on the website. Using secure payment processors such as Sana Pay is a great way to reduce this e-commerce security threat;
- Man in the middle - MITM attack is called an "active eavesdropping attack." A third party intercepts a conversation or transfer of data between two parties. This third party can additionally inject malicious software into the files that are being exchanged, ultimately infecting further systems after the attack has been completed;
- SQL Injection attack - most e-commerce websites maintain databases filled with customer information such as email addresses, physical addresses, phone numbers, etc. This attack allows an unauthorized user to access these databases. By using a nefarious piece of code, a hacker can bypass an authentication page, and gain access to the full back-end database. From there, the user can steal, modify and delete the data;

- Cross Site Scripting (XSS) - in this type of an attack several malicious scripts are injected into benign and trusted websites. When an attacker uses a web application to inject malicious code to different end-users, generally it is in a form of a side script. An attacker can use XSS to send a malicious script to an unsuspecting user. After user enters website and provides information/credential, this side is executed and forwards sensitive information to the attacker. The end-user will never know what the script contains, and when executed, it will do the harm;
- Financial fraud - instead of relying on malicious code, financial fraud relies on stolen credit cards or fake returns in order to benefit at the company's expense. When credit card fraud is discovered, the e-commerce site will have to refund the victim without recouping the goods sold – leaving them on the hook for an expensive bill;
- Insider threats - insider threats are a serious danger for e-commerce businesses. Disgruntled employees (or ex-employees) may attempt to steal company data or proprietary information in hopes of selling it to a rival business.;
- User/human error – user errors happen from the client/employee's side, such as entering incorrect or potentially malicious information that can affect business. There errors happen quite often and need to be addressed by providing guidelines.

Since there are a lot of security threats that target e-commerce, there are also a lot of solutions that ensure your business will be secure. One of the most common security tips is to select a reliable, secure web host for your platform that you run to protect yourself from such threats as malware and SQL injections. If you want to make your network reliable – implement a DMZ (demilitarized zone) network that acts as an exposed point to the Internet and protects your internal LAN network from malicious actors. [20, 21]

In case your budget allows - you need to hire security experts that will conduct penetration tests targeting your website in order to expose vulnerabilities. Do not store customer's data on your webservice or platform - use third-party encrypted tunnels from other services to checkout data and prevent fraud. [21]

Perform regular backups for your business as often as possible, preferrably once per day, monitor what you download and integrate into your website, such as specifical add-ons.

Use a a Website Application Firewall (WAF) that will help to take the security of your eCommerce website to the next level. It will protect your website from XSS, SQL injections, forgery requests, brute force and DDoS attacks. [21]

4. CONCLUSIONS

In this research e-commerce mobile and payments systems were provided and described, as well as the rise of online and security threats that affect e-commerce business. As evidenced, e-commerce has dramatically changed the manner in which regular business is being done. However, the more people become involved in e-commerce, the more issues rise up in e-commerce systems.

This research has emphasized the importance of e-payments to ecommerce and also discussed the various methods of e-payments that are available. Due to the digital nature of e-payments these are open to some issues including fraud and privacy violation. For such cases it is important to comply to the PCI DSS standarts.

Most of the issues associated with electronic payment systems are a result of the fact that these systems are not well mature and they are still evolving. However, progress has been made and most of the issues facing e-payment systems have been addressed through technological advances such as better encryption technology.

However, it is expected that as e-commerce becomes more expansive and e-payment methods mature, most of the issues will be addressed sufficiently. This will bring about customer confidence in the e-payment system and the future growth of e-commerce will be ensured.

Potentially successful enterprises should employ several e-commerce security measures and protocols to keep security threats at bay all the time. Apart from the basic authentication systems like username and passwords, SSL, multi-factor authentication is essential, as well as selecting the right third-party services and web hosts.

Malicious attackers, hackers and fraudsters are constantly looking to take advantage of online shoppers and shopping systems to gain a profitable advantage. Common mistakes that leave people vulnerable include shopping on websites that aren't secure, giving out too much personal information, and falling pray to common social engineering attacks, such as phishing.

5. BIBLIOGRAPHICAL SOURCES

1. Halim, E., Januardin, R., Hebrard, M. 2020, *The impacts of E-payment system and impulsive buying to purchase intention in E-commerce*, Proceedings of 2020 International Conference on Information Management and Technology, ICIMTech 2020, pp. 847.
2. *A guide to e-commerce payment system*s [online]. GoCardless, 2022 [viewed 5 December 2022]. Available from: https://gocardless.com/guides/posts/a-guide-to-e-commerce-payment-systems
3. *E-Commerce - Payment Systems* [online]. Tutorialspoint, 2022 [viewed 7 December 2022]. Available from: https://www.tutorialspoint.com/e_commerce/e_commerce_payment_systems
4. Anindya, R. *What are the different types of e-commerce payment systems?* [online]. Amazon, 2021 [viewed 9 December 2022]. Available from: https://sell.amazon.in/seller-blog/different-types-of-e-commerce-payment-systems
5. *Top 10 online payment methods for e-commerce sites* [online]. Alibaba.com, 2022 [viewed 10 December 2022]. Available from: https://seller.alibaba.com/businessblogs/px001ugaf-top-10-online-payment-methods-for-e-commerce-sites
6. Grant, M., Kvilhaug, S. *Mobile Payment* [online]. Investopedia, 2021 [viewed 11 December 2022]. Available from: https://www.investopedia.com/terms/m/mobile-payment.asp
7. Bezovski, Z. *The impacts of E-payment system and impulsive buying to purchase intention in E-commerce*, European Journal of Business and Management, Vol.8, No.8, 2016, ISSN 2222-1905 (Paper), ISSN 2222-2839 (Online).
8. Danova, T. *There's Virtually No Ceiling To Mobile's Potential In The Larger Payments And E-Commerce Markets* [online]. Business Insider, 2013 [viewed 12 December 2022]. Available from: https://www.businessinsider.com/mobile-payments-and-e-commerce-2013-10

9. *Difference between mobile payment and mobile commerce* [online]. Lyra, 2020 [viewed 10 December 2022]. Available from: https://www.lyra.com/in/mobile-payment-and-mobile-commerce
10. Morales, J. *Mobile First Design Strategy: The When, Why and How* [online]. Adobe, 2021 [viewed 11 December 2022]. Available from: https://xd.adobe.com/ideas/process/ui-design/what-is-mobile-first-design
11. *The benefits of mobile payments as part of your commerce strategy* [online]. Global Payments, 2019 [viewed 13 December 2022]. Available from: https://www.globalpayments.com/insights/2019/06/04/mobile-payments
12. Ham, A. *E-commerce security 101: Essential information for web store owners* [online]. Sana Commerce, 2022 [viewed 14 December 2022]. Available from: https://www.sana-commerce.com/blog/ecommerce-security-101
13. Luo, S., Choi, T.-. 2022, *E-commerce supply chains with considerations of cyber-security: Should governments play a role?*, Production and Operations Management, vol. 31, no. 5, pp. 2107-2126.
14. Wassan, S., Xi, C., Jhanjhi, N., Raza, H. 2021, *A smart comparative analysis for secure electronic websites*, Intelligent Automation and Soft Computing, vol. 30, no. 1, pp. 187-199.
15. *How could the use of biometrics make e commerce more secure?* [online]. EGPA Conference, 2020 [viewed 13 December 2022]. Available from: https://www.egpa-conference2020.org/how-could-the-use-of-biometrics-make-e-commerce-more-secure
16. *Six Reasons Why Digital Security is Vital to eCommerce Success* [online]. Shift4Shop, 2021 [viewed 9 December 2022]. Available from: https://blog.shift4shop.com/digital-security-ecommerce-success
17. *What You Need to Know About Securing Your Ecommerce Site Against Cyber Threats* [online]. BigCommerce, 2022 [viewed 8 December 2022]. Available from: https://www.bigcommerce.com/articles/ecommerce/ecommerce-website-security
18. Varghese, J. *Ecommerce Security: Importance, Issues & Protection Measures* [online]. Astra Security, 2022 [viewed 16 December 2022]. Available from: https://www.getastra.com/blog/knowledge-base/ecommerce-security

19. Rizma, B. *eCommerce Security: Protecting Your Store from Cyberattacks* [online]. Hostinger Tutorials, 2022 [viewed 17 December 2022]. Available from: https://www.hostinger.com/tutorials/ecommerce-security
20. *List of Attacks* [online]. OWASP Foundation, 2022 [viewed 14 December 2022]. Available from: https://owasp.org/www-community/attacks
21. Rukhan, K. *How to Secure Your eCommerce Website: 7 Tips* [online]. Mailmunich, 2022 [viewed 12 December 2022]. Available from: https://www.mailmunch.com/blog/secure-ecommerce-website