International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST52411253

Cybersecurity Risk Discussion with Relevant Laws

Pham Anh Dung[1], Dinh Tran Ngoc Huy[2*], Dinh Tran Ngoc Hien[3], Sylwia Gwoździewicz[4]

[1]PhD, Apollos University, Montana, US.

[*2]MBA, Banking University HCMC Ho Chi Minh city, Vietnam - International University of Japan, Niigata, Japan

[3]BSc Ho Chi Minh Technical University Vietnam

[4]PhD, Jacob of Paradies University in Gorzow Wielkopolski, Poland

*Corresponding Author : dtnhuy2010@gmail.com

ARTICLEINFO

Article History:

Accepted: 10 March 2024

Published: 27 March 2024

Publication Issue :

Volume 11, Issue 2

March-April-2024

Page Number :

352-360

ABSTRACT

In the context of post Covid 19 pandemic, This paper outlines What are Cybersecurity risks? For online transactions? And What are suggestions for Protecting consumer interests in online transactions?

By using analysis, experiences, observations, practical situation with cases studies of our country-Vietnam, and also use qualitative, analysis, synthesis research methods, this study suggest that When detecting that the account has an abnormality or mistakenly transferred or received, consumers need to contact the bank directly to solve it, do not bring it online to inquire, and do not send the OTP password to any individual request. Currently, most banks use Smart OTP, biometric authentication..., customers should also switch to this method, limit the use of receiving OTP passwords via SMS to avoid being cheated. Second, to prevent online risks clients need Not to provide personal information, bank account, OTP password, Internet banking and mobile banking username and password for strangers.

Keywords : Cybersecurity Risks, Threats, Online Consumers, Protection, Suggestions

I. INTRODUCTION

Current situation of information security in Vietnam

Of the 48,646 cyberattacks on critical IT systems in the first half of 2022, exploit attacks still accounted for the majority with nearly 53% of total attacks; followed by network scanning attacks (15.65%), APT attacks (14.36%); authentication attacks (9.39%); malicious code attack (7.58%)

According to Senior Colonel Do Minh Kim, Deputy Head of Division 3 - Department of Cybersecurity and High-Tech Crime Prevention (Ministry of Public

Security), many targeted cyber attacks (APTs) have been conducted against computer systems. important information systems of countries, enterprises, and economic groups, causing serious consequences on economic security and business operations.

Challenges to network security, privacy, and information safety are always in a state of high alarm. Information from the Ministry also said: that Vietnam is in the top 10 countries suffering from cyber-attacks and dangerous malware infections, ranked 7th in the number of victims of cyberattacks, and ranked 2nd among countries. most infected with crypto-mining malware.

(source: vnetwork.vn)

In the Draft Law on the identification of organizations and individuals doing business in cyberspace, they include:

- Organizations and individuals doing business by themselves or through online platforms having transactions in cyberspace with consumers, which we are now accustomed to calling e-commerce (online sales platforms) .
- Business organizations and individuals set up, operate and provide online intermediary platform services to consumers.

We also summarize related studies:

Table 1- Previous studies

Authors	Year	Content, results
Williams et al	2020	Companies must implement well-defined software upgrade procedures, should use secure networks like virtual local area networks, and conduct regular penetration tests of their systems. By understanding factors that make individuals, health care organizations, and employers more susceptible to cyberattacks, we can better prepare for the next pandemic.
Maleks Smith et al.	2020	Globalisation, digitalisation and smart technologies have escalated the propensity and severity of cybercrime. Whilst it is an emerging field of research and industry, the importance of robust cybersecurity defence systems has been highlighted at the corporate, national and supranational levels. The impacts of inadequate cybersecurity are estimated to have cost the global economy USD 945 billion in 2020
Gomesh & Deshmukh	2022	The internet brought a new revolution to the financial sector and it has changed the way of operations in the last two decades. Now, people have the option to carry out banking transactions from a place of their choice without having to go to a nearby bank office. E-banking has become an integral part of the banking system and has become a popular method of transaction for the majority of people. A user has a wide range of options for managing his money through numerous internet banking methods. While internet banking is an aid for customers, they still have to be vigilant to keep their accounts safe from cybercriminals and hackers, as everything on the internet is prone to security threats. Internet security measures followed by the majority of the bank sites to protect their information are not up-to-date as compared to the dynamic cyber threats. Such problems have made it easy for confidential financial information to fall into the hands of third parties and cybercriminals. Although there are several security measures to stop data breaches, there are still flaws in these systems. The goal of this study article is to look at the number of cyber security issues in internet banking in India and the consumer's

		awareness of these issues and preventive measures used by them. Our research is particularly based on primary data
Aseri	2021	Online shopping, and e-commerce in general, have gained popularity and provide more convenient and less stressful options transacting online. Consumers can now enjoy accessing products from distant stores according to their preference, a factor that gives consumers the ability to choose without considering distance and long queues. While online shopping promises to be a better option to the consumer, the channel is susceptible to threats, referring to elements that have the potential to inflict serious harm on a user's privacy leading to data breaches and a compromise of data security. As a consequence consumers are uncertain on whether to trust online shopping. This paper includes information on the threats of online shopping and highlights consumer perceptions, including negative consumer perceptions. The paper provides awareness on cyber security issues, including ways online shoppers and merchants can protect themselves from data breaches and attacks through methods such as phishing and adware.

(source: author synthesis and analysis)

II. METHODOLOGY

In this study, the authors choose analysis, experiences, observations, practical situation with cases studies of our country-Vietnam, but it also uses will use qualitative, analysis, synthesis research methods. Relevant regulations and experiences from European countries also researched.

III. MAIN FINDINGS

3.1. Online transactions risks

First risk is identity risk. Verifying the identity of a partner is not easy and can lead to illegal activities such as money laundering, forging documents. Online transactions made when buyers and sellers do not know each other so there are risks.

Second, risks in differences in culture, language, payment habits, international law...

Third, risks from hackers. For instance, hackers can use email or mobile to send sms messages to consumers in which they played roles of banks and ask for consumer personal information such as bank account, username and password of clients account, OTP password in internet banking or mobile banking, etc…then they steal money of clients easily. Or they can send link for consumers to click then they steal money.

Fourth, so called cyber security risks.

Fifth, Using online payment, also known as electronic payment, customers will receive many promotions, discount codes of stores, buy cheaply so they can save costs.

In case you go on a business trip away from home, travel and need to spend a lot of money. At this time, carrying cash in large quantities will not be safe due to the situation of pickpockets and robberies that are difficult to control. With electronic payment, you only need a smartphone connected to the internet to be able to pay easily 24/7. In particular, personal information is highly confidential, so customers are not afraid of being exposed.

In addition to e-wallets, users can pay online via domestic and international bank transfers, etc.

Electronic payment systems can be hacked at any time if users do not have good security or follow security regulations.

The situation of writing the wrong amount of money transferred via bank accounts or e-wallets is not uncommon nowadays. There have been many cases of overpayment or transfer to the wrong object.

Anti-DDoS solution and Web/App protection for businesses DDoS attacks with hundreds of Gbps (Gigabits per second) traffic are capable of bringing down many Web Server systems of targeted businesses. However, VNETWORK's customers will still be assured of safety. We have the security platform of VNIS (VNETWORK Internet Security) that helps to comprehensively protect the enterprise's Web Server against all forms of DDoS attacks as large as thousands of Tbps (Terabit Per Second).

VNIS has been recognized by the world's leading security organization, Gartner, as the platform representing the world's leading Content Delivery Networks (CDNs). Learn more about VNIS's smart web application and website security features below.

(source: vnetwork.vn)

3.2. Cybersecurity risks and Protecting consumer interests in online transactions

Aseri (2021) mentioned risks for online shoppers:

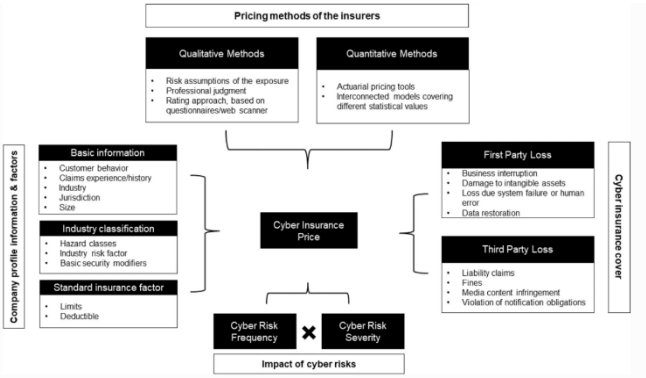
Firs is Phishing: One of the most prevalent security breaches affecting online shoppers are executed through phishing. As the name purports, a user is lured into giving his or her important passwords and credit card details using a click bait. Phishing is a situation where fraudsters transmit emails which they falsely claim to be affiliated to highly reputed firms so as to extract an individual's personal data. Phishing uses disguised emails as its main weapon, the goal being to trick a user with an urgent message such as a request from the user's bank requiring the user to download a form. The malpractice can be categorized according to the user's intentions. It can be done to extract important information from the client, by tailoring a message to resemble a bank. Phishing can also lure a user into downloading malware, the files usually come with .zip extensions or Office documents embedded with malicious code, ransom ware is one of the most common malicious codes and has been detected in 93% of phishing emails.

Second is Fake Online Stores.

Third is Theft of data : Data theft has become an issue as online merchants accumulate important client information on their databases. System administrators and other workers who are authorized to access servers can access data without the owner's knowledge. A survey conducted by the British Retail Consortium (BRC) saw 62% of the respondents acknowledge data theft by system administrators and other workers as a threat.

We also look at:

Figure 1 – An overview of the current cyber information/risk landscape



(source: from EIOPA (2018) and Romanosky et al. (2019)).

Then we can refer to European experiences in dealing with cybersecurity crime:

Launching funding programs for companies and other entities to support their transition to a secure Industry 4.0 ecosystem, including financial support for joint cyber security activities.

Small and medium-sized enterprises are an important driver of innovation and economic growth of the European Union member states. Therefore, in developed countries, enterprises are encouraged to introduce innovations and R&D to secure

environments for new Industry 4.0 ICT, including their components and systems. One of the instruments of financial support is Commission Decision (C (2016) 4400) of 5 July 2016 on the signing of a contractual arrangement on a public-private partnership for cyber security industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organization and Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125 / JHA. From January 1, 2014, to December 31, 2020, the following were allocated and awarded as part of the Facility:

- measures to prevent and combat cyber crime, raising the level of security of citizens and businesses in cyberspace, in particular projects building the capacity of law enforcement and justice authorities, projects ensuring cooperation with the industry sector to empower and protect citizens, and projects improving the ability to deal with cyber-attacks ;
- measures to increase the administrative and operational capacity of the Member States in the field of critical infrastructure protection in all sectors of the economy, in particular projects promoting public-private partnerships to gain trust and facilitate cooperation, coordination, emergency planning and exchange and dissemination of information and best practices between public and private entities.

The instrument should complement and strengthen actions taken to develop cooperation between the relevant European Union bodies and the Member States to achieve the objectives of the Instrument in the field of police cooperation, prevent and combating crime, and crisis management.

The instrument supports actions taken in the Member States, in particular actions to improve police cooperation and coordination between law enforcement authorities, including between relevant Union bodies, in particular Europol and Eurojust, joint investigation teams and any other form of joint cross-border operations, access to information, their exchange and interoperable technologies; networking, identification, exchange and dissemination of know-how, experience, and best practices, information sharing, knowledge of situations and perspectives, emergency planning and interoperability; exchange, training and education of staff and experts of relevant authorities.

The presented recommendations concern broad possibilities to encourage undertaking and strengthening cross-border cooperation when applying for EU funds. On the one hand, companies wanting to implement innovative solutions regarding new ICT technologies in Industry 4.0 and how to secure them. On the other hand, state institutions and bodies wishing to implement appropriate technological constructions, in proportion to the actions taken and the legal and formal scope of their obligations in counteracting cyber crime, also to improve international jurisdiction when it comes to developing countries or countries which are not members of the European Union.

IV. DISCUSSION

In our country we discuss relevant laws to protect consumers:

Vietnam's digital economy is projected to exceed US$43 billion by 2025 as the country continues to pursue projects in e-government, internet of things, smart cities, financial technology, artificial intelligence etc. With cyberspace blurring regional and national boundaries, Vietnam will likely face an increase in cyber threats, and sophisticated attacks.

In recent years, the Vietnam government had issued numerous regulations in its effort to strengthen the local cybersecurity landscape, including:

• Directive No. 22/CT-BTTTT issued in May 2021 by the Ministry of Information and Communications

focused on strengthening the prevention and combat of law violations and crimes on the Internet.

• Decision 1907/QD-TTg issued in 2020 which approves the Ministry of Information and Communications raise awareness and disseminate knowledge about information security for 2021-2025.

• Prime Minister's Directive No.14/CT-TTg in June 2019 enhanced safety measures on cybersecurity of the public sector whereby at least cybersecurity spend must account for 10% of an organisation's total annual IT expenditure in 2020-2025.

• Personal Data Protection Draft Decree, once enacted is set to be the first comprehensive legislation on personal data.

These efforts have yielded positive results given in 2020, Vietnam ranked 25th out of 194 countries in Global Cybersecurity Index (GCI). This ranking is a significant improvement from 2018 and 2017 when Vietnam was placed in the 50th and 100th positions respectively. In addition, this result exceeded Vietnam's target to enter the GCI's top 30 countries in 2030 as per the Prime Minister's Decision No. 749/QD-TTg dated 3 June 2020.

(source: pwc.com).

V. CONCLUSION

First, Clients/consumers are advised to be vigilant when conducting online transactions. When detecting that the account has an abnormality or mistakenly transferred or received, please contact the bank directly to solve it, do not bring it online to inquire, and do not send the OTP password to any individual request. Currently, most banks use Smart OTP, biometric authentication..., customers should also switch to this method, limit the use of receiving OTP passwords via SMS to avoid being cheated.

Second, to prevent online risks clients need:

- Not to provide personal information, bank account, OTP password, Internet banking and mobile banking username and password for strangers
- Not to click on strange links.

VI. REFERENCES

[1]. DT Tinh et al. (2021). Doing Business Research and Teaching Methodology for Undergraduate, Postgraduate and Doctoral Students-Case in Various Markets Including Vietnam, Elementary education Online 20 (1)

[2]. Aseri, A.M. (2021). Security Issues For Online Shoppers, International Journal of Scientific & Technology Research 10(3):112 - 116

[3]. DVT Thuy, DTN Huy, VTK Anh, NN Thach, HT Hanh. (2021). Quality of education of ethnic minority communities in vietnam-problems and recommendations, Elementary Education Online, 20 (4)

[4]. D Thi Ngu, DT Huong, DTN Huy, PT Thanh, ES Dongul. (2021). Language teaching application to English students at master's grade levels on history and macroeconomic-banking management courses in universities and colleges, Journal of Language and Linguistic Studies 17 (3), [1457]-1468

[5]. DTN Huy. (2012). Estimating Beta of Viet Nam listed construction companies groups during the crisis, Journal of Integration and Development 15 (1), 57-71

[6]. Do Thu Huong, Dinh Tran Ngoc Huy, Nguyen Thi Hang ,Pham Thi Huyen Trang ,Duong Thi Ngu. (2021). Discussion on Case Teaching Method in a Risk Management Case Study with Econometric Model at Vietnam Listed Banks – Issues Of Economic Education for Students, Review of International Geographical Education, 11(5).

[7]. DTN Huy. (2015). The critical analysis of limited south asian corporate governance standards after financial crisis, International Journal for Quality Research 9 (4),

[8]. DTN Huy, DTN Hien. (2010). The backbone of European corporate governance standards after financial crisis, corporate scandals and

manipulation, Economic and business review 12 (4)

[9]. D Thi Ngu, DT Huong, DTN Huy, PT Thanh, ES Dongul. (2021). Language teaching application to English students at master's grade levels on history and macroeconomic-banking management courses in universities and colleges, Journal of Language and Linguistic Studies 17 (3)

[10]. DT Tinh, NT Thuy, DT Ngoc Huy. (2021). Doing Business Research and Teaching Methodology for Undergraduate, Postgraduate and Doctoral Students-Case in Various Markets Including Vietnam, Elementary education Online 20 (1)

[11]. DT Hien, DTN Huy, NT Hoa. (2021). Ho Chi Minh Viewpoints about Marxism Moral Human Resource for State Management Level in Vietnam, Psychology and education 58 (5), 2908-2914

[12]. DTN Huy, NN Thach, NT Hoa, NT Dung. (2021). Using Internet Data for Evaluating Market Risk During Period 2011-2020-A Case of Eximbank in Vietnam in the Concept of Sustainable Development, Webology, 18

[13]. Gomes, L et al. (2022). Cyber Security and Internet Banking: Issues and Preventive Measures, Journal of Information technology and science, 8(2)

[14]. Maleks Smith, Z., E. Lostri, and J.A. Lewis. (2020). The hidden costs of cybercrime. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

[15]. NN Thach, HT Hanh, DTN Huy, QN Vu. (2021). Technology Quality Management of the industry 4.0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets-the Case in Vietnam, International Journal for Quality Research 15 (3)

[16]. NT Hoang, DTN Huy. (2021). Determining factors for educating students for choosing to work for foreign units: Absence of self-efficacy , JETT 12 (2), 11-19

[17]. NT Hang, DTN Huy, DT Tinh, DT Huyen. (2021). Educating Students in History and Geography Subjects through Visiting Historical Sites to Develop Local Economy and Community Tourism Services in Thai Nguyen and Ha Giang, Revista geintec-gestao Inovacao E Tecnologias 11 (3), 1-12

[18]. NT Hoa, DTN Huy, T Van Trung. (2021). Implementation of students's scientific research policy at universal education institutions in Vietnam in today situation and solutions , Review of International Geographical Education Online 11 (10), 73-80

[19]. Nguyen Dinh Trung , Le Huong Hoa , Bui Thi Thu, Dinh Tran Ngoc Huy, Le Ngoc Nuong (2021). Using English To Teach Students With Social Sciences Major - Via A Case Of Some Vietnam Newspapers With The Uk, Italian And French Approaches And Regulations On Publishing Fake News And Internet Crime, Journal Of Language And Linguistic Studies, 17(3), 1711-1725

[20]. Nt Hai, Dtn Huy, Nt Hoa, Td Thang. (2021). Educational Perspectives On Differences Between Management Case Study And Economic & Finance Case Study Teaching In Universities , Design Engineering, 12022-12034

[21]. ND Trung, DTN Huy, TH Le, DT Huong, NT Hoa. (2021). ICT, AI, IOTs and technology applications in education-A case with accelerometer and internet learner gender prediction , Advances in Mechanics 9 (3), 1288-1296

[22]. PTH Trang, DTN Huy, NT Hoa, DT Huong, DT Ngu. (2021). Analysis of VI Lenin and Ho Chi Minh Views on the Youth Education Process , Review of International Geographical Education Online 11 (5), 4552-4559

[23]. PN Tram, DT Ngoc Huy. (2021). Educational, Political and Socio-Economic Development of Vietnam Based on Ho Chi Minh's Ideology, Elementary Education Online 20 (1)

[24]. P Anh, DTN Huy, DM Phuc. (2021). Enhancing Database Strategies for Management Information System (Mis) and Bank Sustainability Under Macro Effects-A Case Study in Vietnam Listed Banks, Academy of Strategic Management Journal 20, 1-15

[25]. PM Dat, ND Mau, BTT Loan, DTN Huy. (2020). COMPARATIVE CHINA CORPORATE GOVERNANCE STANDARDS AFTER FINANCIAL CRISIS, CORPORATE SCANDALS AND MANIPULATION, Journal of security & sustainability issues 9 (3)

[26]. Romanosky, S., L. Ablon, A. Kuehn, and T. Jones. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? Journal of Cybersecurity (oxford) 5 (1): tyz002

[27]. S Lin et al. (2022). Exploring the Relationship between Abusive Management, Self-Efficacy and Organizational Performance in the Context of Human–Machine Interaction Technology and Artificial Intelligence with the Effect of Ergonomics, Sustainability 14 (4)

[28]. Thao, N., Anh, N., & An, P. (2019). Impact of corporate social responsibility on reputation, trust, loyalty of the customers in the banking sector – Evidence in Dalat city. Science & Technology Development Journal -Economics-Law and Management, 3(3), 220-235. https://doi.org/https://doi.org/10.32508/stdjelm.v3i3.562

[29]. TTB Hang, DTH Nhung, DTN Huy, NM Hung, MD Pham. (2020). Where Beta is going–case of Viet Nam hotel, airlines and tourism company groups after the low inflation period, Entrepreneurship and Sustainability Issues 7 (3),

[30]. TTH Ha, NB Khoa, DTN Huy, VK Nhan, DH Nhung, PT Anh, PK Duy. (2019). Modern corporate governance standards and role of auditing-cases in some Western european countries after financial crisis, corporate scandals and manipulation, International Journal of Entrepreneurship 23 (1S)

[31]. Torres et al. (2020). Visualizing Research on Industrial Clusters and Global Value Chains: A Bibliometric Analysis, Front. Psychol., 2020 issue. https://doi.org/10.3389/fpsyg.2020.01754

[32]. Van Tuan, P., Huy, D. T. N., & Duy, P. K. (2021). Impacts of Competitor Selection Strategy on Firm Risk-Case in Vietnam Investment and Finance Industry. Revista Geintec-Gestao Inovacao E Tecnologias, 11(3), 127-135.

[33]. VQ Nam, DTN Huy, NT Hang, TH Le, NTP Thanh. (2021). Internet of Things (IoTs) Effects and Building Effective Management Information System (MIS) in Vietnam Enterprises and Human-Computer Interaction Issues in Industry 4.0, Webology, 18

[34]. VQ Nam, DTN Huy, NT Dung. (2021). Suggested Risk Policies from Comparison of 2 Groups of Vietnam Banks-Previous SOE Banks and Private Banks During Post-Low Inflation Period 2015-2020, REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS 11 (2), 531-546

[35]. VQ Nam, DTN Huy, NT Thuy, NT Hang, NT Hoa. (2021). Historical Sites and Architectures in Thai Nguyen City and Ha Giang Province in Vietnam-Sources for Tourism Development, NEW ARCH-INTERNATIONAL JOURNAL OF CONTEMPORARY ARCHITECTURE 8 (2), 342-352

[36]. VQ Nam, DT Tinh, DTN Huy, TH Le, LTT Huong. (2021). Internet of Things (IoT), Artificial Intelligence (AI) Applications for Various Sectors in Emerging Markets-and Risk

Management Information System (RMIS) Issues, Design Engineering, 609-618

[37]. Williams, C.M et al. (2020). Cybersecurity Risks in a Pandemic, J Med Internet Res 2020;22(9):e23692 doi:10.2196/23692

Cite this article as :

Pham Anh Dung, Dinh Tran Ngoc Huy, Dinh Tran Ngoc Hien, Sylwia Gwozdziewicz, "Cybersecurity Risk Discussion with Relevant Laws", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 11 Issue 2, pp. 352-360, March-April 2024. Available at doi : https://doi.org/10.32628/IJSRST52411253
Journal URL : https://ijsrst.com/IJSRST52411253