AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

ANALYSIS OF ROLE OF CYBER CELL IN THE E-BANKING FRAUDS

Mr. AJAY D. PATEL,
Research Scholar
Adhyapak Sahayak from V.T.Choksi Sarvajanik Law College Surat
Dr. Vikaram Desai
Guide
Veer Narmad South Gujarat University, Surat, Gujarat.
Email–ajay.patel873@gmail.com

DECLARATION: I AS AN AUTHOR OF THIS PAPER /ARTICLE, HERE BYDECLARE THAT THE PAPER SUBMITTED BY ME FOR PUBLICATIONIN THIS JOURNAL IS COMPLETELY MY OWNPREPARED PAPER.IHAVE CHECKED MY PAPER THROUGH MY GUIDE /SUPERVISOR /EXPERT AND IF ANY ISSUE REGARDING COPYRIGHT /PATENT/ PLAGIARISM/ OTHER REAL AUTHOR ARISE, THE PUBLISHER WILL NOT BE LEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MY CONTENT FROM THE JOURNAL

Abstract

The components of the financial system will alter as a result of technological advancements. They would be able to enhance their internal operations and deliver better client service as a result of it. Technology will dismantle all barriers and promote international banking. As computers are capable of storing, segmenting, combining, finding, and displaying information according to user needs with some speed and precision, e-banking aids us in overcoming the drawbacks of manual systems. Banks would have to do a significant business process redesign. Technology advancement brought about the emergence of fraudulent technology use as well. The growth of banking services and client trust should be prioritised by the RBI, the government, and the banks through the creation of misrepresentation controlling systems. The electronic commerce (Ecommerce) and Internet banking sectors faced a significant challenge due to the potential of cyber security attacks. In this context, the article identifies the many cyberthreats that e-banking customers encounter, analyses how these risks affect customers' behaviour when using e-banking services, and suggests countermeasures. The analysis comes to the conclusion that users of online banking should be aware of basic security precautions in order to avoid cyberattacks and protect their financial data.

Keywords: *E-Banking, Frauds, Cyber Cell*

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

1. Introduction

The ongoing digitization has increased the number of cyber dangers. A growing number of associations base their commercial operations on cutting-edge networks. As a result, there is a greater chance that organisations and their clients will survive cybercrime. There have been a number of cyberattacks against the banking industry and other online banking components during the past few years. These attacks ranged from money theft to the disruption of online payment systems, such as online banking through websites, mobile applications, and iDeal. Due to the financial gain, misrepresentation-related cyberattacks are prevalent in the banking industry and feature a variety of architectures. The impact of cybercrime has led to a serious risk exposure for individuals and associations (personal mischief) (reputational hurt). It includes the potential for financial losses, regulatory concerns, information breach liability, harm to the brand's reputation, and a decline in customer and public trust (Verma, Hussain and Kushwah, 2012). Banks and other (monetary) organisations' cash and reputations are at risk from cybercriminals. Additionally, it has an impact on how consumers and other stakeholders view the association and how much faith they place in it.

The components of the financial system will alter as a result of technological advancements. They would not only be able to enhance internal operations, but they would also be able to offer better customer service. Technology will dismantle all barriers and promote international banking. In order to fully realise the advantages of technology and business process improvements made, banks would need to engage in substantial Business Process Re-Engineering and address issues like the best way to supply goods and services to consumers. How to utilise technology to achieve economies of scale, how to reduce costs, how to develop a customer-centric business strategy. Banks in India have transitioned to core banking stages and transferred exchanges to electronic channels including ATMs, Internet Banking, and Mobile Banking as well as payment cards (debit and credit cards). Additionally, scammers have followed clients into this area. However, in order to avoid placing the full burden on the consumer, the majority of banks need to improve how they respond to scams in these areas. Additionally, there is a lack of clarity among banks about the reporting of these incidents as frauds.

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

The Reserve Bank of India (RBI) recently established a working group on cyber fraud, electronic banking, risk management, and data protection. The functional group recently presented its report, and public data sources were then sought. The final draught was just made public and announced by the RBI after looking into the public data sources. Additionally, the RBI has mandated that all banks immediately establish a position for chief information officers (CIOs) and security at the board level. Data (IT Vision 2011–17) and a recent notification of the draught report's release supplied this guidance. This paper makes various technical and legislative reform recommendations for the Indian banking industry.

2. Review of Literature

According to Jha et alresearch .'s from 2014, phone phishing is one kind of identity theft. Identity theft involves obtaining someone's personal information in order to get access to their private financial information, which is then utilised by fraudsters to conduct fraud. The fraudster obtains the private information over the phone by pretending to be from XYZ Organization and requesting your financial balance information since you won the prize. The fraudster then uses the information to make use of the customer's account information. Since the entire idea of e-banking services is dependent on the information that is the specifics of the person, identity theft is one of the simplest ways to conduct misrepresentation in this field.

According to a 2014 article in Jokhi, Mr. Milind Deora, the former minister of state for correspondence and data technology, said that the total loss incurred by Indians as a result of e-banking scams was around Rs. 54 crores in the first half of 2013–14. E-banking fraud instances are on the rise each year, but because there is little understanding of cyber legislation in India, some incidents are reported and others are not.

According to a 2012 article by Karimzadeh and Alam, the main barriers to the development of electronic banking are legal, security, and technical issues because of which e-banking frauds are committed. In order to prevent the same, it is necessary to implement laws properly, adapt security policies so that customers feel confident that using e-banking services is safe and secure, and raise

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

awareness of these issues. Making consumers aware of these precautions will work best to solve the issue and establish a secure atmosphere for using e-banking services.

According to Khanna and Arora's 2009 study, the main causes of e-banking frauds include a lack of planning and a poor degree of compliance with Reserve Bank of India requirements. They have suggested that one of the preventive measures for which quality preparation is required to be given to the bank staff, the people who are dealing with and have internal command over the electronic banking system, is a regular internal control on the system because typically fraudsters try to find loopholes in the control procedures. The number of instances involving e-banking misrepresentation claims is growing daily because the RBI's standards are not being implemented to the maximum degree possible.

According to Komal and Rani's 2012 study, there are essentially four channels for electronic banking: ATMs, credit cards, the internet, and mobile banking. 24% of respondents believe using credit cards is unsafe, while 29% believe mobile banking is unreliable. Mobile banking is extremely risky because people have a tendency to download applications that are free, and through these free applications, fraudsters steal the person's detailed information that is stored on their mobile device. In addition, they continuously monitor the messages that the person receives, which would give them the information necessary to commit e-banking frauds.

The review by Muthukumaran (2008) outlines the many e-banking fraud schemes, including Unauthorized access to data on a computer system is known as hacking. Phishing is the practise of customers receiving emails from fictitious websites that closely resemble the official websites of financial institutions and asking them to click on the connection and enter their user name, secret key, or other personal information in order to gain access to their records for a specific purpose. He will utilise the information given to the con artists to pull off the scams. The websites made by scammers are so similar to one another that it is quite difficult for someone to discern between them and what an average guy with common sense would be able to identify.

According to a 2013 article by Parameshwara, the G. Gopalkirshna committee, which was established by the RBI in 2011, made a number of recommendations, one of which was the

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

formation of a misrepresentation review chamber in each bank by the extortion risk management group. However, the recommendation has not yet been carried out by all banks that offer their customers electronic banking services.

3. Materials and methods

Information gathering techniques: The review is based on both primary and secondary sources of data.

3.1. Primary data:

A survey was carried out using students from various educational institutions as the target population in the three Odisha areas of Puri, Khurda, and Cuttack. For the survey, convenience testing was performed. 220 consumers of internet banking in Odisha were directly polled for the most recent questionnaire. The survey was carried out in January 2020.

3.2. Secondary data:

In addition to primary data, secondary data is often used into research projects. The secondary data was gathered from various publications, working documents, and websites of several banks.

3.3. Questionnaire Design:

To find out how consumers felt about cyber-assault, a questionnaire with 50 questions was given to them. The questionnaire was evaluated in the P.G. department of commerce at the U. N. College in Cuttack, and revisions were made as necessary based on the input to make it better and more user-friendly. Customers of internet banking who were 18 years of age or older provided the data. A sample size of 220 (n=220) is used to reflect the study's objectives.

3.4. Types of Cyber Threat

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

Users of internet banking need to be informed of the crimes that are possible in order to raise awareness of the cyber risks that are out there. The next sections of this study describe these cybercrimes.

Identity Theft: One of the typical tactics used by cyber criminals when dealing with electronic companies, notably online banking services, is to use someone else's identity—such as their name, date of birth, and address—for fraudulent transactions. Cyber criminals can use the information they have gotten via identity theft to create new accounts, apply for credit cards or cash advances, and apply for government benefits, among other things. The Realm of Bahrain is one of the victims of identity theft crimes, which is one of the crimes with the fastest growing global trend.

Phishing: Phishing is a tactic used by online criminals and fraudsters to trick victims into disclosing their private information and money. Cybercriminals employ a variety of phishing tactics, but the most common one is sending phishing emails to online banking users while posing as a genuine company or association that provides digital services. A "mocking site," a website created by computer fraudsters to seem like the official websites of financial institutions, can also be used for phishing attacks and to steal the financial information of users of online banking. In the current era of mobile applications, protecting online banking data is becoming problematic as researchers at Web sense Security Labs have discovered a stealth Trojan that steals passwords and employs sophisticated DNS redirection techniques to evade server closures and seize online banking data. Computer fraudsters typically utilise phishing through mobile devices, computer apps, and web-based entertainment sites. According to AFCC, the Against Extortion War Room, the total cost of phishing attacks in 2014 was $4.5 billion in lost revenue.

Vishing: Vishing, also known as voice phishing, is a technique used by computer fraudsters to impersonate a contact centre in order to get the financial and personal information of online banking customers. Fraudsters employ an email system to accomplish their goal, asking online banking users to confirm their banking information and other data as part of a normal security check at the phone number supplied in the phishing email.

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

Malware: The biggest danger from online criminals to get unauthorised access to users' records and steal their financial information and other sensitive data is malware (viruses, worms, Trojan horses, and other threats). The rapid development of mobile devices, such as Smartphones and Tablet PCs, encourages the growth of malicious software. In the last several years, computer fraudsters have committed hundreds of thousands of frauds on online customers in commercial sectors, particularly in online banking, to syphon off enormous sums of money. There is a growing need to develop effective defences against these sophisticated malware applications targeting online banking services and other monetary foundations, so mobile phone malware is an important factor to take into consideration in this situation. Some of the developing mobile platforms, such as Android, are the most targeted by malware creators.

Through hacking and breaking, cybercriminals can get access to computers and computer networks and acquire financial information that can then be utilised for illicit purposes. Trojan infections are only one example of the malicious software that cybercriminals prefer to exploit to infiltrate computers.

Robotizing Online Banking Misrepresentation: With the use of Programmed Transfer Systems, cybercriminals and computer fraudsters have now advanced the situation (ATSs). A new technique for automating online banking misrepresentation has been launched, incorporating Spy Eye and ZeuS malware variants as a component of Web Inject files, which are text files with a portion of JavaScript and HTML codes.

Social engineering is the art of persuading individuals to engage in certain behaviours or reveal private information. Cybercriminals and computer fraudsters frequently exploit the sociology field of social engineering to get financial information in order to gain unauthorised access to sensitive data.

Interpersonal organisations: Informal communities are often the entry points used by cybercriminals to get the information supplied by record holders. Cyber criminals may subsequently utilise the data they have gained unauthorizedly. These unofficial platforms, like

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

Facebook and Twitter, allow users to exchange texts, and during that process, users may be routed to another website by being provided with a link by scammers.

Denial of Service (DoS) Assault: Cybercriminals that engage in denial of service (DoS) assaults try to prevent users from accessing network resources. Because of the severity of these attacks, a single distributed denial-of-service (DDoS) attack may soon bring down a single website as well as any intermediary service providers. The costs of DoS attacks on organisations with rudimentary infrastructure might be quite high. An $8 million single-incident deficit resulting from a DoS attack was reported by a survey participant in the 2005 Australian Computer Crime and Security Survey. Online banking services should take into account the significance of these cyberattacks and dangers to their business development, and substantial action should be done to increase security and maintain consistent company growth. The security measures for using online banking services must always be improved in order to reduce potential dangers from cyberspace.

Mobile phones and other electronic devices In the current electronic age, using PDAs and other electronic devices like Computer Tabs has become standard practise. On the foundation of PDAs and computer tablets, security experts foresee significant dangers from online criminals and computer fraudsters. Financial associations and online banking services should take the rise in mobile device use by customers accessing online banking services and applications seriously, along with the threats that exist, to ensure that they are prepared to operate their services on as many of these new platforms as is reasonably anticipated.

Electronic media platforms: People increasingly use more advanced browser-enabled platforms in their homes. These include internet-connected or smart televisions made by various manufacturers as well as media streaming devices. There is also a Google television example there. These platforms also make users concerned about their security when accessing the internet. Through controlled apps, the stages make it simple for cybercriminals and fraudsters to manipulate a range of real devices. Consumer education and understanding of the most effective way to use and access these electronic media platforms is becoming increasingly important.

4. Results

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

We have conducted the following analysis of the data based on data gathered from online banking customers.

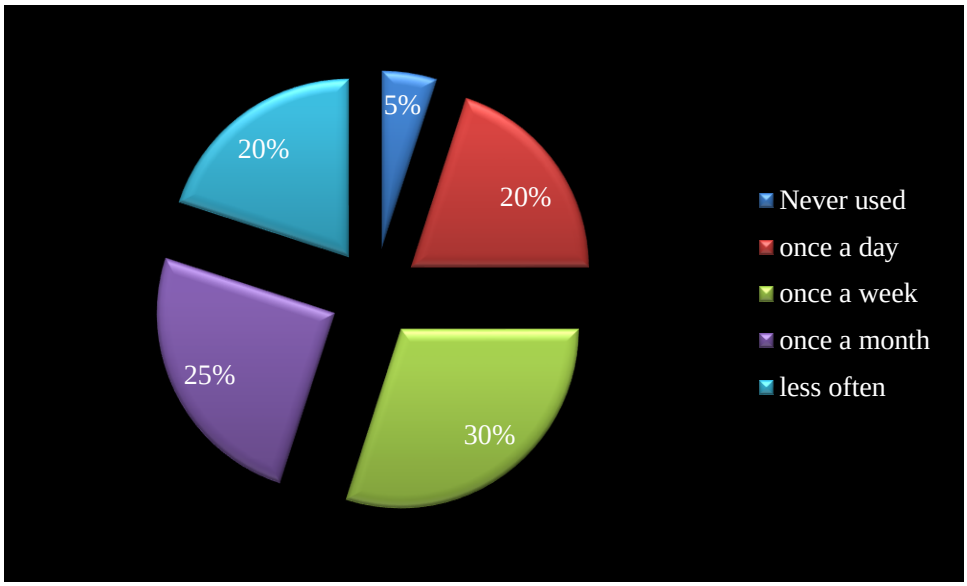

Figure: 1. Measurements of Frequency

Only 20% of the members utilise online banking services daily, and only 30% use them once a week, according to the analysis of the aforementioned Fig. 1. Investigation results show that 95% of members use internet banking. Twenty-five percent of respondents said they use internet banking once a month, while twenty-five percent said they use it less frequently.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

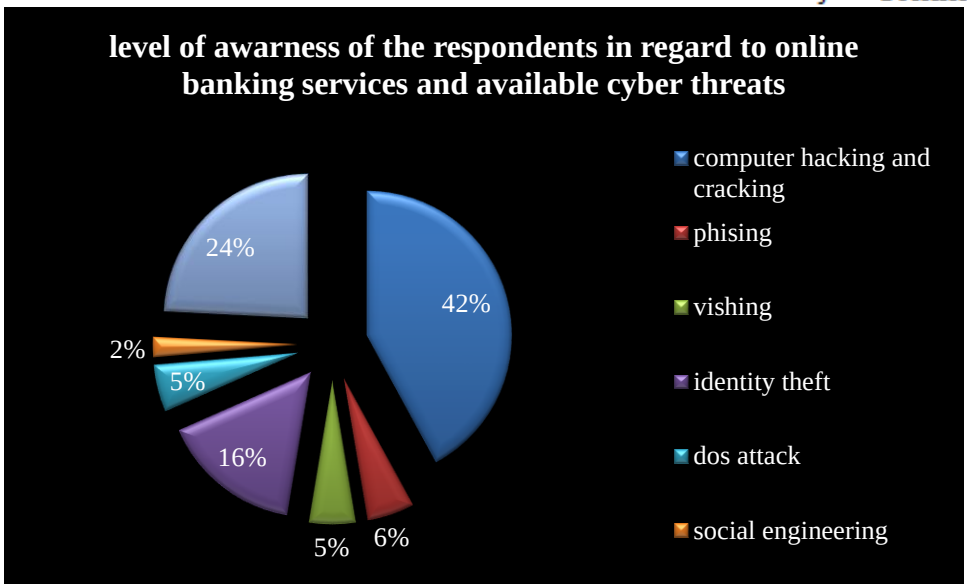

Figure: 2. Measurement of Awareness

Examining Fig. 2 (below) demonstrates the respondents' degree of knowledge on online banking services and current cyberthreats. As shown, 40% of respondents are aware of computer hacking, 5% are aware of phishing, and the other 5% acknowledged they are aware of vishing (phishing over VOIP). Out of 220 respondents, 15% said they were aware of identity theft, while 5% said they were aware of DoS attacks. 2% of respondents said they have heard of friendly engineering. It is important to remember that 23% of respondents are quite familiar with all of the crimes and cyberthreats identified in the poll. On the other hand, it demonstrates that only roughly 77% of online banking consumers are aware of the hazards and accessible cybercrimes.

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

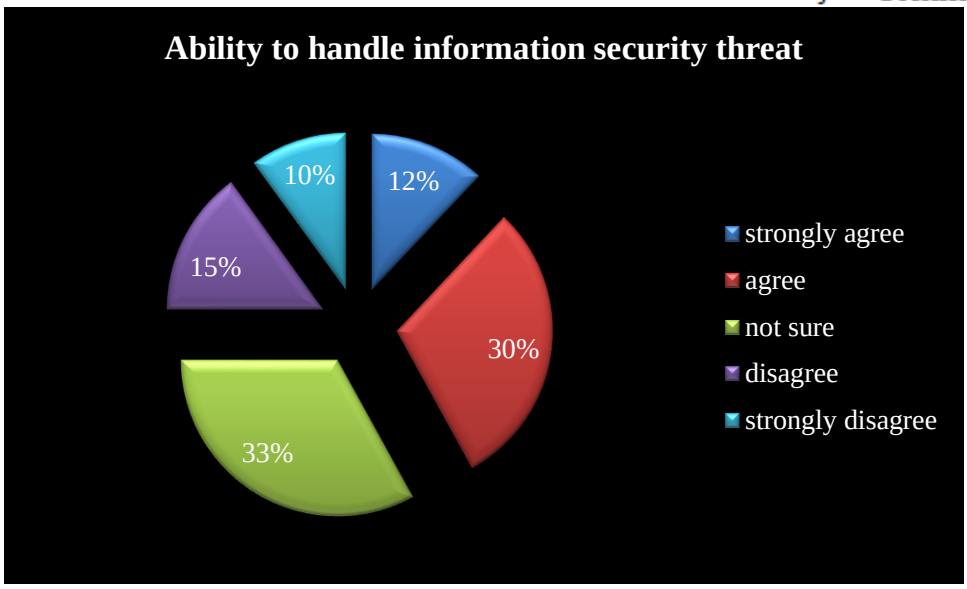

Figure: 3. Understanding of Threat Assessment

According to the analysis of Fig. 3 above, 42% of respondents are able to recognise risks to data security and are further equipped to deal with them. However, 33% of poll participants are unsure of their ability to handle the threats at hand. According to the aforementioned research, 25% of respondents are unable to recognise and respond to such threats.

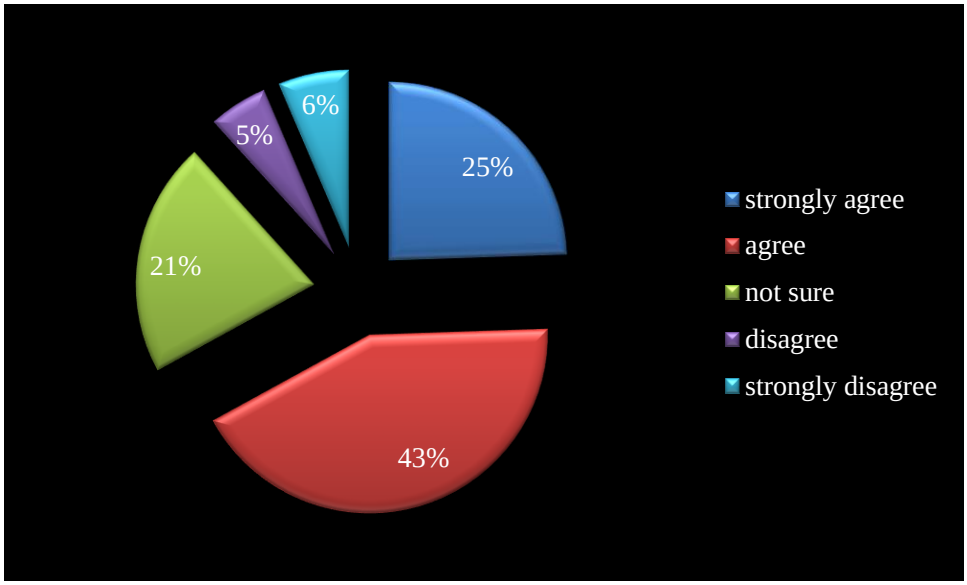

Figure: 4. Person-specific Information Security Risk

AIRO JOURNALS
Free / Unpaid
Peer Reviewed
Multidisciplinary
International
ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

According to the analysis of Fig. 4 above, 63% of survey participants agreed or strongly agreed that every individual has a role to play in lowering data security risks. 11% of respondents disagree with this, while 26% are unsure.

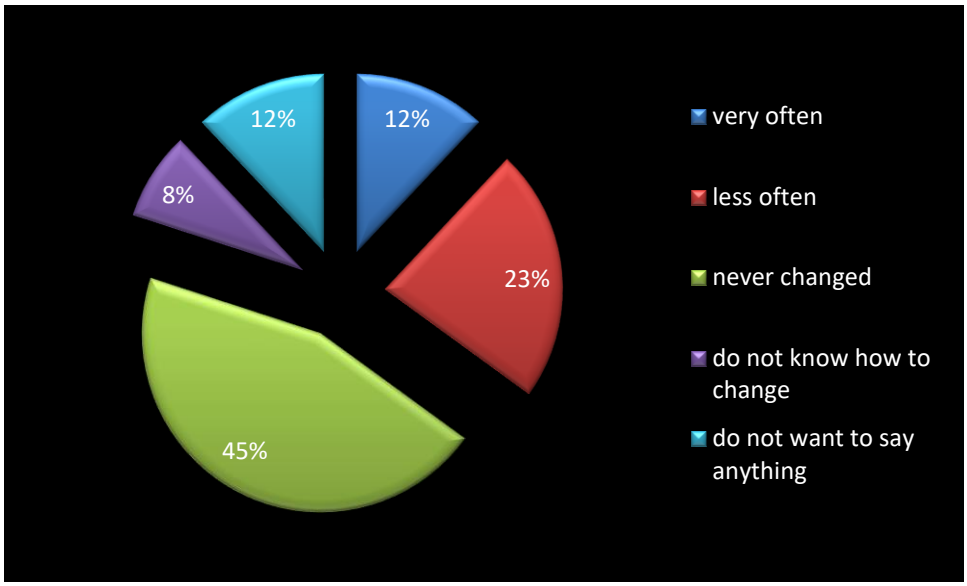

Figure: 5. The frequency of password changes

The analysis of Fig. 5 above demonstrates that 12% of respondents, on average, routinely modify their secret phrase to protect their online banking from online attacks. While 45% of respondents haven't updated their passwords since using internet banking, 23% seldom ever do so. The remaining 8 percent of consumers aren't even aware of how to update their online banking passwords.

5. Discussion

The inference of this research was made possible thanks to the survey that was performed and based on 220 replies. When using online banking services, it is crucial to comprehend and recognise security concerns. Users of internet banking are assessed for confidence. Users of internet banking and other services should be aware of the risks posed by computer fraudsters and criminals when using these services. To steal the financial information of end users, computer fraudsters employ a variety of strategies and methods, including computer hacking, phishing,

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

vishing, identity theft, denial of services, social engineering, and much more. Customers of online banking need actually be aware of these strategies and tactics employed by cybercriminals. However, just 23% of survey participants said that they were aware of essentially all of the hazards highlighted in this research's survey. This demonstrates that around 77% of web users have little to no knowledge of the issues facing the financial sector and the general public. This further provides access points for cybercriminals and fraudsters to unlawfully get client data and use it for their illicit purposes. Users of internet banking must exercise particular caution when using these services. However, more than 63% of users are unable to recognise and respond to the dangers to current data security. Additionally, almost 65% of customers don't exercise any additional caution when using online banking services.

6. Conclusion

The creation of new and more effective distribution and processing channels as well as more cutting-edge products and services in the banking sector has been made possible by the monetary liberalisation and technological revolution. Banking institutions are up against competition from other institutions, non-bank financial intermediaries, and alternative funding sources. By discussing a variety of serious cybercrimes that have been especially linked to the banking industry, the study has given a general overview of the idea of electronic banking. The backbone and lifeblood of the economy is the banking system. The financial system is now based on data technology. The ever-increasing obstacles and financial needs are greatly aided by it. Banks today find it impossible to show money without the use of data technology. However, data technology has also had a negative impact on our financial industry, where fraud, phishing, hacking, forgeries, and other crimes are conducted. When a person engages in any kind of banking exchange through an electronic medium, it is essential to use authentication, identity, and verification measures to prevent cybercrime. The evolution of cybercrime and the difficulty of its detection process need the adoption of appropriate safeguards. In order to combat cybercrime, increased stakeholder cooperation is essential.

According to the Public Crime Records Bureau, there has been a significant increase in the number of cybercrimes in India over the past three years. The issue of electronic crime is really significant.

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

Not only do banks suffer financial losses as a result of cybercrime, but the customer's trust in the institutions is also damaged. The assessment indicates that there has been a growth in the amount of payments made through e-banking, therefore the Indian banking industry cannot strive to avoid banking operations conducted through electronic media. The banking industry should evolve, but in a way that is appropriate for the Indian market.

References

1. *Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.*
2. *DeCuir-Gunby, J.T., Marshall, P.L. & McCulloch, A. (2011). Developing and using a codebook for the analysis of interview data: an example from a professional development research project. Field Methods, 23(2), 136 – 155.*
3. *Dr. Roshan Lal & Dr. Rajni Saluja, E-Banking: The Indian Scenario,December (2012), Vol (1)(4),*
4. *Harun R Khan, Digital India: Emerging Challenges and Opportunities for the Banking Sector, Federation of Indian Banks Association (2014)*
5. *Hunton, P. (2009). The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. Computer Law & Security Review, 25(6), 528 - 535.*
6. *Jang, Y.J. & Lim, B.Y. (2012). Harmonization among National Cyber Security and Cybercrime Response Organizations: New Challenges of Cybercrime.*
7. *Lagazio, M., Sherif, N. & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 1 - 32.*
8. *Liang, H. & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. MIS Quarterly, 33(1), 71 – 90.*
9. *Manzoor, A. (2014). Protecting Customers Online: Response from Pakistani Banks. International Journal of Science and Applied Information Technology, 3(1), 1 – 7*
10. *Martin, N. & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. Computers & Security, 30, 803 – 814.*

ISSN:2320-3714
Volume1 Issue 2
February 2023
Impact Factor:11.7
Subject: Commerce

11. *Minakshi bhosale and dr. k.m. Nalawade (2012) e-banking services: comparative analysis of nationalized banks, ABHINAV National monthly refereed journal of research in commerce & management volume no.1, issue no.11 pp 212-219 |*

12. *RBI Guidelines on Information Security, Electronic Banking, Technology Risk management and Cyber Frauds, 2012.*

13. *Saini, H., Rao, Y.S. & Panda, T.C. (2012). Cyber-Crimes and their impacts: a review. International Journal of Engineering Research, 2(2), 202 – 209.*

14. *Soni RR and Soni Neena, An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks, Vol. 2(7), 22-27, July (2013), Research Journal of Management Sciences, Available online at: www.isca.in*

15. *Verma, M., Hussain, S.A. & Kuswah, S.S. (2012). Cyber Law: Approach To Prevent Cyber Crime. IJRREST: International Journal of Research Review in Engineering Science and Technology, 1(3), 123 – 129.*

******