“Examining bank initiatives to safeguard and promote customer awareness to deter Online Financial Fraud in Ireland”

KRISHNAN SANJEEV NAIR

20003928

Dublin Business School

This dissertation is submitted for the degree of Masters of Science in Financial Technology

August 2024

Declaration

I, Krishnan Sanjeev Nair, hereby affirm that this research is entirely my own original work and has not been submitted to any institution or university for the award of a Degree or Diploma. Furthermore, I have accurately referenced all the literature and sources utilized in this study, ensuring full compliance with Dublin Business School's academic honesty policy.

Signed by: 

(Krishnan Sanjeev Nair)

Acknowledgments

I would like to express my deepest gratitude to Professor Satya Prakash, whose mentorship, guidance and support have been invaluable throughout the course of this dissertation. His expertise and encouragement inspired me to delve deeply into the subject and his constructive feedback was instrumental in shaping the direction of this research.

I am also immensely thankful to my classmates at Dublin Business School, whose collaboration made this academic journey both enriching and enjoyable. The shared experiences and insightful discussions have greatly contributed to the development of my ideas and the successful completion of this study.

Lastly, I would like to extend my heartfelt thanks to my family, whose unwavering support and encouragement provided me with the strength and motivation to pursue this degree. Their understanding and patience during this demanding period were crucial to my success.

Thank you all for your contributions to this achievement.

Table of Contents

“Examining bank initiatives to safeguard and promote customer awareness to deter Online Financial Fraud in Ireland”

ABSTRACT:

In an increasingly digitalized world, the prevalence of online financial fraud poses a significant threat to individuals availing such services. A rapid increase in reliance on online banking is making the sector susceptible to cyber attacks. As per latest CSO data (Central Statistics Office, 2023) – more than 90% on Irish Bank User are active online banking platform. With such growing concern of Online Financial Fraud in Ireland, this study examines the effectiveness of banks' initiatives in safeguarding customers and promoting awareness from falling prey of any malicious attempts. The research aims to assess to what extent such awareness campaigns educate customers from falling prey of any online fraud attempt. It also aims to evaluate the effectiveness of these initiatives and assess the impact of any demographic variables on customer perceptions. A quantitative approach will be employed using a self-administered online survey. The collected data will be analyzed using descriptive statistics and inferential statistics to identify correlations between variables. Through this research it is expected to identify which types of bank awareness campaigns are more effective in educating customers and to determine if customer engagement with such awareness campaigns leads to a secure online banking practices.

CHAPTER ONE: RESEARCH BACKGROUND

1.1. Research Background

"At its heart, the need for consumer protection arises from an imbalance of power, information and resources between consumers and their financial service providers, placing consumers at a disadvantage." (Susan, World Bank, 2016). It can be witnessed, the ongoing turmoil in financial market globally to fight against organized financial fraud. Online financial fraud poses a significant threat to both individuals and financial institutions, with increasingly sophisticated tactics employed by cybercriminals to exploit vulnerabilities in digital transactions. Ireland, is not an exception, where the banking and financial sector is at the forefront of efforts to combat

online financial fraud, implementing various initiatives to safeguard customers and promote awareness to fight against such threats.

According to Michael McGrath, Minister of Finance, Ireland, primary role of any financial service institution is to provide adequate consumer protection by imparting financial literacy and propagating financial awareness campaigns to reach out maximum customer population. Financial institutions should be required to apply fair, non-coercive and reasonable practices to take sufficient action to protect their customer interest and keep customer confidence and brand loyalty intact.

There has been multiple studies conducted in the field of Consumer Protection, Financial Literacy and Awareness by financial institutions, but this study seeks to examine the efforts undertaken by bank in Ireland to promote customer awareness, to educate about online financial fraud and effectiveness of such bank initiatives to safeguard and deter from online fraud. By evaluating the current landscape of bank-led fraud prevention measures and customer perceptions, this research aims to provide valuable insights into the effectiveness and impact of these initiatives on mitigating the risks associated with online fraud. Consumers who are empowered with proper knowledge and information are aware of their responsibilities and can take ownership of own actions to identify any Online Fraud and safeguard themselves from such malicious attempts (Johann Füller et al., 2009).

1.2. Understanding Online Financial Fraud in Ireland

For the purpose of this study, a concise understanding of Online Financial Fraud is crucial. Online financial fraud refers to any criminal activity that uses the internet to steal money or personal information from unsuspecting individuals (Kremling J. et al., 2018). According to Tom Mullen (2020), senior risk manager at AIB, online financial fraud encompasses a range of deceptive practices carried out through digital channels with the aim of unlawfully acquiring financial assets or sensitive information. In today's increasingly interconnected world, the prevalence of online financial fraud poses significant risks to individuals, businesses, and financial institutions alike. Perpetrators of online financial fraud employ various tactics to deceive their prey (Fraudster-tactics, Bank of Ireland, 2024). The Garda Síochána also released

some of the most common type of Fraud Reported in Ireland in their official website. In this respect it is important to have an understanding few of the potential fraud attempts that originate from the Internet and commonly prevalent in Ireland (Common Fraud Threats, AIB, 2024).

1. **Email Scam (Phishing Scam) –** Most common and increasingly trending scam technique used by fraudsters impersonating as known Supplier, Contractor or Solicitor of the bank customer advising them to change the bank details and share new bank account number through fake email and ask to route all future payments in the new bank account, which belongs to the criminals.
2. **Investment Scam Warning–** In this type of scam, the criminals use some banks fake email id along with name of a real staff that apparently resembles with banks original employee details. Banks account holder is then contacted by the perpetrator (commonly referred as Bad Actor) and get a form filled up from fake website to offer investment product of renowned financial services. Simultaneously the Bad Actor convinces the customer to transfer the investment fund into an account which the customer later realizes to be a scam.
3. **Text Message Fraud (Smishing Scam) –** It is very common fraud technique used by fraudster to obtain personal banking and card information for purpose of identity theft or financial gain. The fraudster send text message to customer's registered mobile number that appear to come from legitimate bank source and end up sharing personal or sensitive information or login to fake website and provide bank credentials.
4. **Phone Scam (Vishing Scam)** – In such scam, the fraudster calls the customer impersonating as bank employee for providing any service or request for financial / personal information – like debit or credit card details for financial gains.
5. **Purchase Scam (Online Buying Scam) –** While purchasing online, customers must be aware that they are logging to legitimate website. Fraudster advertises using images of genuine products of big brands at too low price to be true. The scammers use cloned site where goods are never actually available for sale however consumer end up paying money to buy the goods in the fake website.
6. **Payday Loan Scam –** This is one of the trending scam where the fraudster provide fake Payday Loan Application form to the bank customers via online and convince them to fill the personal details and loan application along with IBAN details. Upon a fake loan

approval, the fraudster asks customer to make Advance payment or down payment in a fake account.

7. **Mum and Dad Whatsapp Scam** - In this instance the scammers contact bank customers from unknown number, pretending to be their child/ grandchild and ask for money by creating some dramatic scenario or emergency situation.

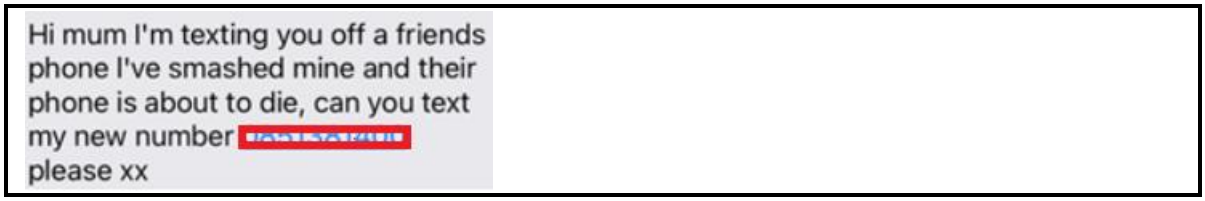


Image source: https://aib.ie/security-centre/common-frauds-and-threats

8. **Holiday Scam –** Some holiday deals are just too good to be true and the criminals set up fake websites and ads offering some dream holiday at a discounted price. And the bank customer falls to such luring trap; end up paying money to book airlines ticket and hotel booking that never existed in the fake website.
9. **Malware (Trojan and Viruses)** – Malware is short form of 'Malicious Software' whose impact can be moderate to dangerous. Banking specific malware can gather specific information about personal and security credentials of bank account as entered in the personal computer while login to Internet Banking. Such malware can gain access to the device once the fraudster tricked the bank customer and install the virus in the personal computer.
10. **SIM Swap Fraud** – Objective of such fraud is to intercept the SMS as delivered in customers registered mobile with bank account. The fraudster approaches the mobile service provider impersonating to be the bank customer and request to assign the existing mobile number with a New / Replacement SIM. Once the SIM swap process is executed, the fraudster gets access to all banking related SMS / Unique Codes and dupe the bank customer.

1.3. Measures by the Financial Agencies to Combat Online Financial Fraud

To address the rising threat of online financial fraud, various measures have been implemented by banks and regulatory bodies in Ireland. The Central Bank of Ireland (2020) has strengthened regulatory requirements for financial institutions, emphasizing the need for robust cybersecurity measures and customer education programs. The banking system is making every attempt to safeguard their customers by educating them and promoting financial awareness and literacy campaigns from falling prey to unscrupulous act (Bele J.L. et al., 2014).

As per the latest fraud awareness initiative led by Banking & Payments Federation Ireland (BPFI), shows "Most of the increase in bank fraud was driven by online card fraud or 'card not present' fraud where a criminal uses the victim's compromised card information to make an online purchase (up by 24% in value year-on-year to €27.1m in 2022)."

The Irish banking system in their endeavor to fight against Online Fraud is making continuous effort to empower their customers and imparting financial education through multi faceted literacy campaigns. Here, the Central Bank of Ireland plays a pivotal role in setting up the Directives, Regulations and fostering a collaborative environment that empowers all the banks in Ireland to combat online financial fraud. For instance, the Bank of Ireland's **Financial Wellbeing Programme** aims to improve financial literacy and awareness among consumers, helping them recognize and avoid potential frauds (Bank of Ireland, 2019).The banks are also making arrangement for financial literacy campaigns like **"Ollie the Owl"** program, which is a youth financial wellbeing programme (Bank of Ireland, 2020) and **"Stop. Think. Check"** another campaign of Bank of Ireland in collaboration with An Garda Síochána (90%, Red C, Feb '24), has been conducted to expand the awareness of fraud and ways to prevent them. Similar campaign launched by AIB, **'FraudSMART** – Play your PART', through which it educated with tips how to Be Informed, Be Alert, Be Secure (Security Centre, AIB). Such financial awareness campaigns help to impart knowledge and ability to customers to identify and detect any attempt of online financial fraud and stay alert.

There have been multiple empirical studies providing insights into various aspects of online financial fraud prevention initiatives in the context of Irish banks. With rapid increase in reliance on online financial services is making the Irish banking sector susceptible to cyber attacks. As per latest CSO (Central Statistics Office, 2023) data – more than 90% on Irish Bank User are

active online banking platform. More usage of Online banking, mobile payments and digital wallets create potential access points for fraudsters. The fraudulent techniques whereby scammers trick bank customers into entering their usernames and password is called 'phishing'. Therefore, phishing scams are used to coerce unsuspecting users to disclose personal and banking information (F Cassim et al., 2014). Another study mentioned that, communications, raising awareness and education as a key way to preventing people from falling victim to financial crimes (Seána Cunningham, 2023). In this respect it is pertinent to refer the study examining the effectiveness of customer education programs in reducing online fraud (Ghosh & Sultan, 2012).

Deloitte (2019) shared report how Machine Learning (ML) and Artificial Intelligence (AI) based technologies can analyze transaction patterns in real-time, identifying suspicious activities more efficiently than traditional methods. Banks in Ireland are more inclined to use these technologies along with ongoing efforts towards customer awareness campaigns. Several findings suggest that financial literacy programs and AI Technology can be successful in improving customer awareness and reducing the likelihood of falling victim to fraud (Chen et al., 2018).

1.4. Customer awareness of Online Financial Fraud in Ireland

Customer awareness campaigns play a vital role in promoting financial literacy, empowering consumers, and enhancing trust in financial institutions. Irish banks, cognizant of the ever-evolving nature of financial products and services, have implemented various initiatives to raise awareness among their customers about key banking concepts, risks, and opportunities. These customer awareness campaigns serve as an essential tool for fostering informed decision-making, mitigating financial risks and promoting responsible financial behavior among individuals and communities across Ireland.

From educating customers about the importance of cybersecurity and fraud prevention to promoting sustainable banking practices and digital literacy, Irish banks have embarked on a diverse range of Financial Wellbeing Programme to engage, inform, and empower their customers. A comprehensive analysis of the various initiatives undertaken by multiple banks in Ireland is studied below.

i) Financial literacy and importance

Without an understanding of basic financial concepts and knowledge, people are not well equipped to make decisions related to financial management (Leora Klapper et al., S&P survey, 2014). Financial literacy is getting more and more critical with increasingly complex financial products flooding the market and reliance on digital mode also deepening among the population. As per World Bank report, Governments in many countries pushing to boost access to financial services, the number of people with bank accounts and access to credit products is rising rapidly. Multiple such factors making the financial sector more susceptible to malicious frauds specially through Online mode.

The Organisation for Economic Cooperation and Development (OECD, 2011) defined the financial literacy, 'A combination of awareness, knowledge, skill, attitude and behavior necessary to make sound financial decisions and ultimately achieve individual financial wellbeing (Kempson E, 2009). Financial literacy is more than just being able to read a statement. It is about having a broader understanding of finances, including where there are risks and how to prevent such risk. (Petra Hielkema, EIOPA, 2022). It has been outlined by Central Bank of Ireland, the Regulatory Banking Authority in Ireland, financial literacy and education is highly relevant for consumer protection in Ireland. It recommended that financial education and awareness should be started as early as possible and can be taught in primary schools.

ii) Financial Awareness among Irish consumers

Terms like Financial Knowledge and Financial Awareness are often used interchangeably as part of Financial Literacy (Gusaptono, 2020). Financial awareness is part of financial literacy and is an important factor influencing knowledge and impacting financial decision-making (Dewi et al., 2020). When someone has financial awareness, they will begin to be aware of their finances from the knowledge they have gained about money and can any avoid financial problems that might arise and protect their money (Pahlevi & Nashrullah, 2021). Thus, we can concluded from various related researches that awareness of the use of financial knowledge, will support good financial decision-making and safe keeping the money from malicious frauds.

As per the latest OECD report, 44% of adults in Ireland do not have the minimum level of digital financial awareness to navigate their finance. As per Michael McGrath, Minister for Finance, Ireland states that development of financial literacy is essential for overall financial wellbeing of Irish citizens. The teaching of financial education and creating a mass awareness should take place through multiple levels in schools and supported through core subjects like mathematics as per Department of Finance, Ireland.

1.5. Financial Awareness campaigns lead by Banks in Ireland:

The Central Bank of Ireland (CBI), the regulatory banking body of Ireland, has a significant role in promoting customer awareness to safeguard against potential frauds. The Central Bank provides a regulatory oversight, guidance, monitoring and fostering collaboration across the banking sector in Ireland. Its actions contribute to building a more resilient and secure banking ecosystem that prioritizes customer protection and financial integrity (Jim Stewart, 2001).

The Central Bank of Ireland serves as the primary regulatory authority overseeing the banking sector in Ireland. As part of its mandate, the CBI establishes and enforces Financial Regulations, guidelines and best practices related to fraud prevention, consumer protection, and financial literacy. By setting clear standards and expectations for banks, the CBI plays a pivotal role in shaping the industry's approach to promoting customer awareness and safeguarding against fraud.

Financial Regulations referred to the Rules and Laws of the country for all firms operating in financial industry including Banks, Insurance companies, Credit Unions, Financial Brokers and Asset Managers. At this point it is important to understand who develops these Rules and Laws and how it is enforced.

The Central Bank of Ireland plays a crucial role towards oversight and enforcement of these rules by ensuring the safety and soundness of the financial system while protecting consumers. Any Regulations or Directives as declared by European Central Bank (ECB) need to be harmonized to its National Law within given timeline by the Central Bank of Ireland (Explainers, Central Bank of Ireland). It regulates and supervises over 10,000 financial service providers operating in Ireland ensuring all financial regulations are abided. Poorly regulated financial institutions have the potential to undermine the stability of the financial system, harm

consumers and can damage the prospects for the economy. That's why strong financial regulations are enforced by CBI - to put rules in place to stop things from going wrong, and to safeguard the wider financial system and protect consumers.

The Central Bank of Ireland has enforced multiple Regulations and Directives over the years for consumer safety and uniform service standard across the country in financial industry.

Derville Rowland, Deputy Governor, Central Bank of Ireland has said. "Unfortunately nobody is immune to the threat posed by financial fraud. Advances in technology have created great opportunities for consumers, but have also given fraudsters increased access to innocent victims." There are multiple consumers' awareness programs and information campaigns are conducted to help Irish consumers avoid personal financial scams.

The Central Bank of Ireland has conducted the **'SAFE'** test, which gives all its consumers four practical steps to take while buying or investing in a financial product or dealing with a firm through a website, social media, an unsolicited phone call, email, text or pop up message. It has been guided to the consumers to follow these below steps while making such decisions-

1. Stop: Think and ask yourself challenging questions about what you are being offered particularly if that seems too good to be true.
2. Assess: Make sure the firm is legitimate and do certain back checks through internet.
3. Fact check: Seek advice to ensure that the product or service is legitimate
4. Expose and report: If you have any concerns, contact the Central Bank.

Central Bank of Ireland has released public advisory stating – 'Always take your time when buying investment products or applying for a loan. Never act on the spot – especially if a provider puts you under pressure for a 'deal' – this is always an indicator you are not dealing with a legitimate service provider. Remember that if something seems too good to be true – it probably is.' The Central Bank is sharing awareness videos with real life customer experiences in multiple social media platforms to make it more accessible and acceptable to reach out to mass.

Image source: https://centralbank.ie/scams

Bank of Ireland, one of the leading commercial Irish banks, plays a leading role towards promoting customer awareness campaigns across Ireland. It has recently invested €2 million towards consumer awareness campaign under name **'Big Move'**. With 2 major banks – Ulster Bank and KBC Bank leaving the Irish market Up to one million current and deposit account customers are looking for new banks ahead (RTE news report). So as to make this transition smooth and free from any fraud, Bank of Ireland launched this campaign to spread mass customer awareness through TV, radio, print, outdoor, digital and social media. Bank of Ireland has committed an investment of €50 million on customer fraud prevention and protection campaigns. As per press release, the bank will invest €15 million on new fraud prevention technology, along with a range of high-profile consumer awareness campaigns to support their customers who are often targeted by fraudsters (Red C, Feb '24). In a recent public survey, Bank of Ireland has been accepted as the financial institution most associated with educating the general public about fraud. As per Myles O'Grady, Group CEO of Bank of Ireland, banks are on the front line in defending their customers, and wider society, from financial frauds and threat. However he acknowledged more action is needed by the bank as well telecoms companies, social media and tech firms, fintechs and State agencies. Nicola Sadlier, Head of Fraud, Bank of Ireland, has said that consumers must Stop, Think, Check, if something sounds too good to be true. Bank of Ireland has held 40 fraud awareness events in 13 counties from Jan – May 2024

and has committed to holding events in every county by the end of 2024, as per latest press release by the bank. In its effort to fight against cyber crime the Bank of Ireland is working with renowned cyber psychologist and Academic Advisor to the European Cyber Crime Centre (EC3), Professor Mary Aiken, to build consumer awareness about fraud and explain the human psychology used by fraudsters (Red C, June '23).

In March 2019, Bank of Ireland initiated a five-year **Financial Wellbeing Programme** aimed to improve consumer's financial literacy, capability and confidence with an initial allocation of €5 million and rolled out of the programme named – '**Ollie the Owl.'** The programme was launched in over 3000 primary schools across Ireland to give children aged seven to twelve a head start in developing good financial habits for life. The initiative was part of the Bank of Ireland Financial Wellbeing Programme that includes a varied age of customers - children, parents and teachers. Through child-focused and accessible characters, the initiative brings together stories, learning activities and interactive games to teach children about the basics of money management in a fun and interactive way (Press Release, Bank of Ireland, 2019). As per Rory Carty, Head of Youth Banking, Bank of Ireland, any good financial habits start at an early age. And through such campaigns Bank of Ireland engages with children from a young age so that as they get older they are more confident and knowledgeable when it comes to managing money effectively.

Bank of Ireland implements one of the most extensive consumer fraud awareness programs in Ireland as a central part of its commitment to safeguard the financial wellbeing of its customers. As per a public survey conducted, majority of members see the Bank of Ireland as the financial institution most associated with educating the general public about fraud. (Red C, Feb '24). Bank of Ireland on regular basis updates various online articles and blogs covering a wide range of topics such as budgeting, saving, investing, and retirement planning. This will help their consumers to make their financial decisions independently rather than relying on some third party sources wherein they fall prey of financial frauds. Their Blogs also discuss the latest financial trends, tips for financial management and insights into economic developments. As per latest press release, Nicola Sadlier, Head of Fraud at the bank said there has been 32% increase in Purchase Scams as reported compared to previous year. He also said through Purchase Scam the fraudster lure consumers to make payments for goods or services which then transpire to be fake. Bank has sensitized their consumers and urged to do only secure payment process by

reputable sites. The bank runs 24/7 emergency calling lines to reach the Fraud Team and immediately register any complain. As per Paul O' Brien, Head of Group Security at Bank of Ireland has advised their consumers to rely more on Debit or Credit Card transfers since they can be tracked easily if there is any fraudulent transactions rather than direct bank transfer. Aine McCleary, Group Chief Customer Officer at Bank of Ireland, in a recent press release, has said that people must be equipped with the skills to make smart financial decisions which are key to the bank's financial literacy investment. She also added it is vital for the young Irish population of age group 18-24 years, being financially literate as they are easily being targeted by fraudsters trying to recruit them for illegal activities like 'money-muling'. She warned these may even result in serious consequence on the future of this age population. Bank of Ireland's latest Financial Wellbeing Index - conducted in October 2023 - showed that the country's financial literacy score for 2023 was 53%. Bank of Ireland will continue its investment to increase Financial Literacy among its customer in Ireland. As per latest press data, Bank of Ireland will invest €2.4m in financial literacy programmes for both primary and secondary schools reaching 60,000 children and young people through its initiatives during 2024- 25. Another funding of over €1m will be invested by the bank to promote a team of Youth Financial Coordinators and Financial Wellbeing Coaches to deliver financial education to support financial literacy and capability among young students and adults. Through another service initiative **'Bank at Work'**, the bank facilitates any organizations to help support their employees' Financial Wellbeing. As a part of Social Responsibility, Bank of Ireland conducts talks, seminars both virtual and in person, to help and support this initiative. The bank through these campaigns are urging its consumers to Always, Bide your time, Contact your Bank whenever they think there is any probable fraud attempt. The bank warned their consumers to be extra vigilant in their interactions with businesses online and when responding to unsolicited or unexpected texts, emails or phone calls. As per press release by Bank of Ireland, customers should Stop, Think and Check and following these 3 simple steps they can become FraudSMART and stay protected from Impersonation Fraud.

Allied Irish Banks (AIB), another formidable bank in Ireland has also been proactive in running various customer awareness campaigns aimed at promoting financial literacy and safeguarding customers against online financial fraud. Through its campaign like **Fraud Awareness Week**, the bank takes initiative for mass awareness campaigns by collaborating with industry partners

and regulatory bodies to raise awareness about financial fraud. As per Carol Lawton, Head of Financial Crime, AIB, 'Scams can be very sophisticated and criminals go to great lengths to defraud by compromising people's emails or computers, sending emails and messages that appear legitimate, and creating high quality online advertisements, brochures and other materials.' With this campaign, AIB urges their customers to be extremely cautious and vigilant at all times, advice to verify any requests for payments from unknown party, trusted contacts by calling them on known phone numbers. They must be careful before clicking unknown links resulting malware that might gain access to their systems. They must check authenticity of any advertisement in website or lucrative investment opportunity that seems too good to be true.

AIB in support with Banking and Payments Federation Ireland (BPFI) runs a campaign **'FraudSMART – Play Your PART.'** Anyone can be the target of financial fraud and scams and the best defense is to stay informed, alert and secure. There is a specific Digital Hub created that serves as a comprehensive resource center for customers seeking information on how to stay safe online. Through this section customer will find information on the most common frauds along with key advice and tips that will enable them to avoid becoming the victim of fraud or scams. As per a press release (BPFI, May 7, 2024) issued fresh warning as fraudsters are targeting people over age 50-55 years. A worrying trend emerged where fraudsters are re-targeting people who have already fall victim to an investment scam earlier and now promising them to recover their money. In a recent press release, Niamh Davenport, Head of Financial Crime, BPFI, raised concerns with recent increase in complex investment scams and emphasized on Customer Awareness and Literacy campaigns to safeguard themselves. There is 25.6% jump year on year from 2022-23, in authorised push payment (APP) fraud, involving online and mobile banking transfers. Victims have suffered overall loss of €8.6m over the same period. Such investment scam amounts can start from around €5k up to many multiples of this, with some cases reaching between €50k and €600k and often people who have worked hard to build up a pension and are looking for a last opportunity to top up their finances ahead of retirement mostly fall prey to such traps. Mr Davenport has raised high alert on most prevalent types of APP fraud are through such investment scams and urged customers to be extra vigilant. They must verify every information with some trusted third party – legal / financial professionals or consultants and even close family friends before taking such financial decisions. **'Future Spark'** by AIB, is a skill based interdisciplinary programme for post primary schools that joins the dots

for young people and their teachers as they navigate major transitions and key life moments by providing rich educational resources across multiple subject areas such as Guidance Related Learning, Wellbeing, Business, Economics, Accounting, Financial Education and Home Economics. Through this initiative, AIB has touch based over 630 schools in Ireland sharing 270 free educational resources of which 93% are digital based. AIB has made every effort to make maximum inclusion in the programme through National AIB Future Sparks School Impact Awards rewarding positive change in the community and conducting AIB Career Skill Competition to enthuse the young crowd (AIB FutureSpark, 2024). The programme is targeted to secondary school students, from 1st to 6th Year and offers workshops and educational materials that cover basic financial concepts, online safety, and fraud prevention. These programs are designed to equip young people with the knowledge and skills they need to manage their finances responsibly and stay safe in the digital world. The programme also helps them to learn future-proof skills such as critical thinking, communication, creativity, teamwork and resilience so that they can take sound decision and instill strong awareness of fraud prevention from a early age.

Permanent Trustee Savings Bank (PTSB), one of the leading banks and third largest in Ireland, is not far behind taking critical initiatives to curb Online Fraud for their banking customers. PTSB has introduced a new technology – '**PTSB Protect'** to its banking application which will protect their customers from falling victim of any online fraud. As per recent press release by PTSB, this feature will alert bank customers when they receive any message containing a fraudulent link and block them from accessing any suspicious website. The feature will compare all such links on customer's phone against a known **Blocklist,** which might pose as legitimate websites however deceptively obtain personal or banking details from their mobile phone. The bank also confirms that the **Blocklist** will be maintained and updated by the bank daily. If any link in customers mobile matches an entry on the **Blocklist**, the website will either be blocked or an alert will be triggered to the customer mobile to stay alert (Irishexaminer, Oct 12, 2023). The Chief Operating Officer of PTSB, Peter Vance said, "Attempts to defraud customers through criminal activity has increased significantly over the last number of years, With scams getting more sophisticated, consumers need to continue to be on their guard at all times". Working in partnership with Expleo, a global technology, engineering and consulting service provider, Permanent TSB, becomes the first bank in the world to integrate such a security

feature - **'PTSB Protect'** into its mobile banking app. The complexity of modern cyber attacks and online frauds make it difficult to trust the technology to tell what's real from what's fake. Such anti-smishing solution puts online safety front and centre and gives banking customers the assurance they need (Phil Codd, Managing Director Expleo Ireland).

PTSB runs another anti fraud campaign – **Protect Your Kids Online** targeting the young generation and kids. It urges parents that even when their kids are shopping or playing games online they need to be protected from online fraud attempts.

CHAPTER TWO: RESEARCH QUESTION

2.1. Research Question

Ireland, being a prominent financial hub of the European Union, the Irish banks has implemented various initiatives aimed at protecting customer's financial safety and promoting awareness towards cyber threats. Focus of this research is to delve into the effectiveness of these initiatives and revolve around the impact of such programs on customer perceptions. Each question of this research will critically examine the nuances of bank-led efforts to combat online financial fraud in Ireland that are essential for devising targeted strategies to enhance customer protection and mitigate fraud risks.

1. How have banking initiatives towards public awareness campaigns against financial frauds evolved in recent years in Ireland? – Through this question we will examine the efforts undertaken by the Irish banks over the recent years to promote awareness and educate their customers to deter any online frauds.

2. Are there any disparities in customer perception towards such initiatives across demographic variables such as age, gender, education and income levels? - This question will focus on the impact of above demographic factors on customer perception towards banks campaigns against financial frauds. Further, it will delve to understand the effectiveness of such efforts and what the customers perceive about such campaigns.

3. How effective are the various campaigns and programmes undertaken by banks in Ireland to curb down Online Financial Fraud – It is imperative to understand whether all such activities

and campaigns with huge budgets allocated by the financial institutions including Govt of Ireland are effective to reduce Online Frauds and protect the customers from loosing hard earned money.

2.2. Research aims and objectives

The primary aim of this research is to evaluate effectiveness of the measures and strategies undertaken by the banks in Ireland to propagate customer awareness campaigns to combat the incidence of online financial frauds. Also to identify key drivers and challenges influencing such public awareness campaigns against financial frauds.

Additionally, this research also aims to examine the disparities in customer perceptions towards such bank initiatives and scope to enhance effectiveness and inclusivity across demography. This will try to analyse the factors such as technological advancements, regulatory changes, consumer behaviors that might shape the development and implementation of these initiatives in more effective manner.

To achieve the laid down aims, the following objectives has been set for the purpose-

1. Examine critically the existing bank initiatives over recent years, as implemented in Ireland to safeguard their customers to fall prey to any incidence.
2. Conduct a survey across demographic variables such as age, income level and digital literacy towards customer perceptions and attitudes towards bank initiatives.

By addressing these research objectives, this study aims to offer insights into how demographic variables influence customer perception towards banking initiatives targeting public awareness campaigns against financial frauds in Ireland. The study will also focus on scope of enhancing the relevance, accessibility, and impact of these initiatives for diverse customer segment from falling prey to any malicious fraud attack.

CHAPTER THREE: LITERATURE REVIEW

3.1. Increasing Risk of Financial Fraud in Online Platform

In a rapid changing global environment, the risk from financial crime and cyber fraud are fast changing and evolving. Online financial fraud is becoming growing concern for both banks and consumers across Ireland. The rise of digital banking and e-commerce in Ireland has been accompanied by a growing risk of financial fraud on online platforms (Consumer Protection Outlook Report, Central Bank of Ireland, 2021). This literature review examines the factors contributing to this increase, the types of fraud prevalent in Ireland and the measures taken to combat these threats. As more and more financial transactions migrating online, fraudsters are developing increasingly sophisticated methods to dupe money and personal information as well (Gandhi V.K. et al., 2012). This widespread adoption of digital banking and e-commerce has created more opportunities for fraudsters to easily dupe the consumers. Symantec Corporation (2019) highlights the increasing sophistication and prevalence of cyber threats, indicating that cybercriminals are continuously developing advanced techniques to exploit vulnerabilities in online financial systems (Internet Security Threat Report, Symantec Corporation, 2019).

Moreover, the COVID-19 pandemic accelerated the shift towards online transactions, further exposing consumers and businesses to fraud risks. According to the Central Bank of Ireland (2021), the surge in digital transactions during the pandemic created additional opportunities for fraudsters to exploit both new and existing vulnerabilities.

3.2. Literature gap and Research rationale

Plethora of research has been conducted about importance of online fraud prevention and various techniques to safeguard from such fraudulent attacks (Internet Security Threat Report, Symantec Corporation, 2019). While these researches mostly touches on customer perception of fraud prevention initiatives however there is limited understanding of how different demographic groups responds to such campaigns. There is a scope to examine such disparities among customer responsiveness to bank initiatives conducted in Ireland. Various challenges are being faced by these banks and financial institutions while delivering the campaigns like age, digital

literacy rate, demography even can be a factor where presence of such banking institutions are low (Lusardi & Mitchell, 2014). So it is worth exploring how various demographic factors can influence the effectiveness of awareness campaigns and banks can accordingly take initiatives to work mitigating such challenges (Financial Conduct Authority, 2019).

Even after so many financial wellbeing campaigns and awareness programmes are organized by the banks but it is critical to measure the effectiveness of such campaigns and strategies deployed by the Irish banks (Irish Payments Services Organisation, 2019). There is a lack of empirical evidence assessing the effectiveness of these specific initiatives. Existing research has highlighted the existence of campaigns without evaluating their impact on reducing fraud incidence (Smith, 2020). There is an urgency to evaluate how effective such campaigns are, on the mass customer population in varied demographic strata of Ireland.

The Central Bank of Ireland and other regulatory entities play a significant role in shaping policies and guidelines for fraud prevention and consumer protection in Ireland (Central Bank of Ireland, 2020). The research seeks to address how the regulatory entities influence and collaborate with the banks and other FinTech firms in Ireland to promote customer awareness and fraud prevention (European Banking Authority, 2021). Understanding their impact and collaboration with banks can provide insights into regulatory effectiveness. Examining how banks comply with regulatory requirements and utilize regulatory guidance that can help identifying areas where additional support or adjustments are needed (Central Bank of Ireland, 2020).

There is a multifaceted rationale of this study encompassing the increasing threat of online financial fraud, the evolving role of banks in customer protection and the need of a empirical guide for effective strategies adopted by the banks in Ireland (Smith, 2020). This study will also examine the role of Central Bank of Ireland and other regulatory entities shaping policies and guidelines for fraud prevention and consumer protection (Central Bank of Ireland, 2020). Through this research we will delve into such under explored areas for better insight on the disparities and challenges of such campaigns along with effectiveness of bank initiatives to deter online fraud.

3.3. Economic and Social Impact of Online Cyber fraud in Ireland

Cyber criminals are rapidly enhancing and escalating their attacks, taking advantage of the fear and uncertainty brought about by the Covid 19 pandemic followed by global social and economic conditions has further given an impetus to this cyber criminals. Simultaneously, the increased reliance on connectivity and digital infrastructure has created more opportunities for cyber intrusions and attacks. Cybercrime poses increasing risks to organizations and individuals across Ireland and the world, with daily incidence of attacks taking place. Such staggering figures clearly suggest that cybercriminals do not distinguish between their victims; they simply exploit whatever they can with the intent to steal funds, information or to cause disruption. (Mike Harris, Head Cyber Security, Grant Thorton Ireland, 2021).

As per latest report published by Banking and Payment Federation, Ireland dated 30th May'24; Fraudsters stole almost €100 million (€98.6m) through frauds and scams in 2023, an increase of over 16% (16.4%) on 2022, according to a new report published by FraudSMART. It further reveals that 'Card Fraud' accounted for 95% of fraudulent transactions and 36% (€35.2 million) of gross fraud losses in 2023. Overall usage of Cards for transaction by consumers and businesses rose significantly, with the Central Bank of Ireland data (CBI, 2023) reporting a 28.8% increase in debit and credit card payments in 2023 vis-à-vis fraudulent card payments increased by 8.2% in the same period. Unauthorised electronic transfers accounted for only 3% of the volume but major hit is on overall volume of such fraud resulting 34% (€33.8 million) of losses. Such fraud occurs when someone makes a payment through mobile or online banking, without the account holder's authorisation or permission, often called 'account takeover'. This type of fraud results when account holder divulges sensitive bank relation information like PIN, Password to third party. As per Niamh Davenport, Head of Financial Crime, BPFI, these figures are a timely reminder to be on alert for credit and debit card fraud (BPFI, May 2024). The BPFI report continues that consumers and businesses were scammed out of €18.1 million through authorised push payment (APP fraud) while sending money directly to an account controlled by the criminal. While APP Fraud makes up just 1% of fraudulent transactions and 18% of losses, it represents a significant increase compared to 2022 in both volume and value terms (42.5% and 82.2% respectively). As per Minister of Justice, Helen McEntee, number of cases registered by Garda National Crime Bureau (GNCB) has increased by 111% over 2022 along with 370%

increase only in fraud related crimes made up of 'Vishing', 'Smishing' and 'Phishing' (The Cost of Cybercrime Report, Grant Thorton, 2022).

The Irish Government announced in February 2021 that it is investing €193 million over six years into research on cybersecurity, artificial intelligence, ethics, and data privacy as they acknowledges that cybercrime is a growing phenomenon and recognise that it must be taken seriously (National Cyber Security Strategy 2019- 2024, Mid Term Review, Govt of Ireland, May 2023).

3.4. Effectiveness of Bank Campaigns to reduce Online Financial Fraud

Public and private banks and fintech companies in Ireland are continuously running several awareness campaigns to combat financial fraud, such as those discussed above. Despite these well intentioned efforts, there is limited empirical evidence on their effectiveness to actually curb down online financial frauds (Gotelaere & Paoli, 2022; Button & Cross, 2017; Cross & Kelly, 2016; Prenzler, 2020). Multiple data and facts as released by CSO and Garda Síochána suggest limited outcome of all such campaigns. Recent data of Top Fraud Type list in Ireland as released by Garda Síochán, 'Card Not Present', 'Phishing' and 'Smishing' are among top crimes in fraud list (Garda, 2023). The behaviors targeted by these campaigns can be heavily influenced by situational and emotional factors, including relationship status and mental health issues (Poppleton et al., 2021). Additionally, criminals may impersonate bank or police officers (Choi et al., 2017). As noted by an anti-fraud expert from renowned bank discussed in his study, "most awareness campaigns include messages like, 'don't trust people who call claiming to be from the police or a bank.' In essence, individuals influenced by an awareness campaign initiated by a public authority or bank tend to ignore the campaign's advice when the actual fraudster claims to be from such an authority or bank, particularly among those vulnerable to fraud.

Despite heightened awareness, cybercrime incidents in Ireland are on the rise, with 61% of Irish organizations reporting that they have fallen victim to cybercrime, including fraud, in the past two years, resulting in an average estimated loss of €3.1 million (National Cyber Security Strategy 2019–2024). Ransomware, one of the most predominant cyber attack tool now a days in corporate, around one-in-six of those attacked was hit with a ransom and more than half (58%) paid up the ransom. Figures say that 65% of such Ransomware are stemmed through 'Phishing' attacks and 75% Irish firms end up paying the ransom (Source: Hiscox Cyber Readiness Report

2021). As per the Hiscox Report, the frequency of online fraud attacks in Ireland increased by 26% year-on-year with financial services being most attractive target. As per the survey conducted during this study, disappointingly Ireland has the largest proportion of firms (36%) ranked as cyber novices with low financial security and awareness knowledge as compared to global average (Hiscox Insurance Cyber Readiness Report, 2021).

Some scholars has conducted studies to identify effective ways to reduce fraud incidence, however, there exists little empirical evidence as to whether awareness campaigns actually work. A study conducted by the AARP Foundation (2003) found that direct peer counseling can help reduce telemarketing fraud. The research focused on individuals considered "at-risk," identified from fraudster call sheets seized by the U.S. Federal Bureau of Investigation (FBI). Another researcher Scheibe et al. (2014) demonstrated that warning previous victims could decrease their susceptibility to future fraud. The study included 895 individuals who had been identified as fraud victims by the U.S. Postal Inspection Service has been sampled and observed the action has actually reduced susceptibility. Burke et al. (2022) conducted a study that online educational interventions with video or text may reduce fraud susceptibility.

CHAPTER FOUR: RESEARCH METHODOLOGY

4.1. Research philosophy

Any research philosophy significantly helps in shaping the selected research approach and methods (Saunders, Lewis & Thornhill, 2019). The research philosophy is often based on distinct research paradigms with different underlying assumptions about the nature of knowledge and the methods of acquiring it (Martin Ganon et al, 2022). The research philosophy underpinning this study is based on a Positivism Approach by observing and describing the present phenomenon of Online Financial Frauds in Ireland. The study seeks to uncover the various actions and initiatives undertaken to create awareness towards Online Financial Crimes by multiple banks in Ireland as well Central Bank of Ireland through empirical observation and logical analysis. In this process we use quantitative methods, such as surveys, to test hypotheses and gather data that can be measured and analyzed statistically. By doing so it will help us to understand the effectiveness of

such campaigns undertaken by the banks and what challenges they face in this endeavor.

4.2. Positivism and its relevance

Central to our study is Positivism Research philosophy that considers reality as objective and independent of human perception. Essence of the approach is that knowledge is obtained through direct observation and experimentation and that it is possible to discover universal truths (Bryman A, 2016). The approach emphasizes the use of scientific methods by utilizing systematic and empirical observation, often in the form of quantitative methods. With the nature of this study, multiple criteria will support the approach undertaken.

Quantifiable Data: Positivism emphasizes the use of empirical data, which is crucial for objectively measuring the effectiveness of bank initiatives to create awareness among mass customers against online fraud. By collecting and analyzing quantitative data on the prevalence of online financial fraud in Ireland and the reach and impact of awareness campaigns, the research can provide evidence of what works has been conducted and areas of improvement.

Consistency and Comparability: The study will be using standardized metrics and methodologies that will allow consistent measurement across different banks and customer demographic groups, facilitating comparison and generalization of findings across banks in Ireland.

Predictive Insights: Positivism aims to uncover causal relationships through empirical observation and statistical analysis. This will help to seek insights of the efforts undertaken by banks in Ireland and cause behind their success or failure of such campaigns.

Generalisability of Findings: According to Saunders et al. (2023), positivism research typically involves larger sample sizes and structured methods that will lead to generalisability of findings. In our study, the findings about fraud prevention techniques and strategies can be generalized among multiple banks in Ireland as well various demography of customers based on multiple factors.

Reduce Bias: The positivism approach minimizes personal biases of the variables by focusing on observable data, statistics that are measurable. This ensures that the research findings are

based on objective data rather than subjective interpretation. This method can also replicate the study to verify results, strengthening the evidence base for effectiveness of fraud prevention strategies adopted by different banks in Ireland.

Data Analysis: And finally the Positivism approach supports the use of statistical tools to analyze large datasets. This is particularly relevant for examining the effectiveness of various bank initiatives and understanding the demographic factors that influence customer awareness and susceptibility to fraud. For our research analysis we have used multiple statistical tools and computer languages to understand and interpret the outcomes.

Applying a Positivism philosophy to this research is warranted by the need for objective, quantifiable evidence to evaluate the effectiveness of bank initiatives against online financial fraud. The ability to identify causal relationships, generalize findings, reduce bias and utilize statistical tools makes positivism a suitable and robust methodology for this study.

4.3. Research Approach

One of the ways of research methodology construction is based on theoretical concept of "Research Onion", proposed by Saunders et al. (2016). Research Onion depicts an exhaustive description of the main layers that should be followed in order to formulate an effective methodology (Raithatha, 2017). For the purpose of this research, we have categorized Research Methodology into two popular paradigms: Deductive and Inductive. Deductive research begins with an existing theory and proceeds to test specific hypotheses through data collection, whereas Inductive research starts by gathering data and then develops a theory based on the findings (Saunders et al., 2023). The key difference between these approaches lies in their reasoning direction—deductive reasoning follows a top-down approach, while inductive reasoning follows a bottom-up approach.

4.3.1. Deductive Approach

The deductive approach is a research methodology that begins with a general theory or hypothesis and then tests it through the collection and analysis of specific data. This approach is often associated with the positivist paradigm, which emphasizes the importance of objective and quantifiable data (Aleksandras Melnikovas, 2018). In a deductive approach, the researcher

formulates a hypothesis based on existing theories and then designs a research strategy to test the validity of the hypothesis. The results either confirm or refute the original hypothesis, contributing to the refinement or development of the underlying theory.

4.3.2. Rationale for selecting the Deductive Approach

For this dissertation, which investigates the evolution and effectiveness of banking initiatives aimed at raising public awareness about financial fraud in Ireland, the deductive approach is particularly appropriate. Primary factors driving to choose the Deductive Approach are:

1. Given that this study aims to assess the effectiveness of existing strategies and campaigns, it is essential to prepare appropriate hypotheses regarding consumer behavior, fraud prevention and the role of banking institutions (Saunders et al., 2023).
2. By employing a deductive approach for this research we will systematically test multiple hypotheses by using the empirical data from surveys, reports and statistical analyses the results to derive the research outcome. Hypothesis's are evaluated by comparing it with empirical observations, ultimately leading to its acceptance or rejection (Sneider & Larner, 2009).
3. Furthermore, a deductive argument can be characterized as a reasoning process that moves from the general to the specific, or a top-down approach (Pelissier, 2008).The deductive approach has a tendency to apply new solutions to old and existing problems (Graham and Carmichael, 2012). This methodology ensures that the study remains focused on objective, measurable outcomes, enabling the identification of causal relationships and grounded with strong empirical observations between banking initiatives and consumer awareness levels across different demographics (Locke, 2007).
4. The approach also allows for generalization of findings, providing robust conclusions that can inform future policy and strategy development within the banking sector in Ireland (Saunders et al., 2023).

4.4. Survey Strategy for the Study

In this research, the survey strategy is employed as the central approach for gathering empirical data from customers. The survey method is particularly well-suited for this study, as it allows for

the collection of a large amount of data from a broad demographic, providing a comprehensive understanding of customer behaviors and attitudes. Surveys are effective for capturing quantifiable data, which aligns with the deductive research approach of this study, where hypotheses derived from existing theories are tested against empirical observations.

The key instrument within this strategy is to prepare a well researched questionnaire. A structured questionnaire has been designed, consisting predominantly of closed-ended questions. Closed-ended questions are suitable to ensure that the responses can be easily quantified and statistically analyzed, making it possible to identify patterns, trends and correlations within the variables. This approach facilitates the generalization of findings across the larger population, which is critical for making conclusions about customer awareness and responses to online financial fraud prevention initiatives.

The questionnaire has been meticulously developed based on a thorough review of existing literature which provides a foundation for understanding factors influencing customer behavior and perceptions in online banking. By grounding the questions in established research, the study ensures that the data collected is relevant and aligned with the key variables being examined, such as the effectiveness of fraud prevention campaigns across different demographic groups.

The survey has been disseminated through online across multiple popular social media platforms on Facebook, LinkedIn and Whatsapp. The online survey not only aligns with the context of safety and security of online banking in Ireland but also tries to get customer sentiment towards security features provided by their banks to protect them from getting victim of online fraud.

4.5. Research participants

4.5.1. Research Population characteristics

The intended survey respondents are bank account holders across Ireland aged between 18 and above, both male and female, who are actively using the internet banking facility to meet their day to day banking requirements. The survey participants are either active in Online Financial Transactions, Online Viewing of Bank Account Status, Online Investments or even Online Shopping. The rationale for selecting such demographic distribution is that they epitomize the

probable customer base for online banking in Ireland. By zeroing in on respondents who are only active in Online Banking platform, the research aims to uncover key actions taken by various banks in Ireland to raise awareness among their customer about online financial fraud. And at the same time the Research Objective tries to establish the effectiveness of all such awareness campaigns to deter Online Fraud.

Estimated sample size for survey: The sample size must have enough data to be representative of entire population, yet to allow efficient data processing and analysis. For this study, a sample size of around 120-150 participants is considered, to get a fair picture of the customer perception towards security of online banking facility. This range provides sufficient statistical power for analysis while also reducing the likelihood of sampling errors.

4.5.2. Inclusion and exclusion criteria

Qualifying conditions for inclusion: To participate in this survey, respondents must be Irish residents aged between 18 years and above, who regularly use online banking services, and have encountered or are aware of fraud prevention initiatives implemented by their bank. These criteria are intended to ensure that participants are sufficiently familiar with online banking and the fraud prevention efforts of financial institutions, enabling them to provide insightful and relevant responses to the survey questions. The selected age range is aimed at capturing perspectives from individuals who are more likely to be digitally literate and engaged with online financial services.

Criteria for Exclusion: Individuals who do not meet the above-mentioned inclusion criteria—such as those who have not used online banking services recently or who fall outside the specified age range—will be excluded from the study.

4.5.3. Survey Participant selection

The study will employ a non-random sampling approach, specifically convenience sampling, due to its practicality and ease of access to the targeted demographic. Participants will be recruited through popular social networking platforms such as Facebook, Whatsapp and LinkedIn as well as other online forums where there is access by Irish online bank account users. To ensure that

only eligible individuals participate the survey, a preliminary screening questionnaire will be administered.

4.6. Quantitative Paradigm

The quantitative paradigm for this research focuses on objectively measuring and analyzing the effectiveness of bank initiatives against online financial fraud in Ireland. This approach emphasizes the collection of numerical data through structured surveys or questionnaires, enabling statistical analysis to identify patterns, correlations, and causal relationships (Holman, 1993). The study will employ a deductive approach, starting with hypotheses derived from existing literature on fraud prevention strategies and testing these hypotheses using empirical data obtained from survey (Johnson & Onwuegbuzie, 2004). The sample size will be carefully selected to ensure optimum representation of entire population and statistical tools will be utilized to quantify the impact of various banking security measures on consumer protection. The quantitative paradigm allows for the generalization of findings across the broader population, providing banks with actionable insights to refine their fraud prevention strategies. The use of objective, quantifiable data minimizes bias and enhances the reliability and validity of the research outcomes.

4.6.1. Data Collection Methodology

The data collection for this research will be conducted through a structured survey questionnaire, targeting consumers having bank account in Ireland who utilize online banking services. The survey will consist primarily of closed-ended questions to ensure data will be quantifiable and analyzed easily. Key areas of inquiry will include participants' experiences with online banking, perceptions of security, awareness of bank-led fraud prevention initiatives and responses to attempted fraud. The questionnaire will be designed based on insights from the literature review, ensuring relevance to the research objectives.

The survey will be distributed electronically via social media platforms, targeting a diverse demographic to achieve a representative sample. A preliminary screening will ensure that only respondents who actively use online banking are included. To enhance the response rate, the survey will be concise, and participants will be assured of confidentiality and anonymity.

Collected data will be subjected to statistical analysis to identify trends and evaluate the effectiveness of existing bank initiatives.

4.6.2. Questionnaire Design

The questionnaire for this research will be carefully designed to gather relevant data on Irish consumers' perceptions of online banking security and the effectiveness of fraud prevention initiatives. It will consist of primarily closed-ended questions, Likert scales, multiple choice formats to ensure ease of analysis. The questions will be structured into sections covering demographic information, online banking usage patterns, awareness of security measures and effectiveness of their bank's initiative. Pilot testing will be conducted to refine the questions for clarity and relevance, ensuring that the final questionnaire effectively captures the data needed for robust analysis.

4.6.3. Deployment of the Survey Questionnaire

The survey for this research will be deployed using Google Forms, a user-friendly and accessible platform for efficient data collection, interpretation and analysis. Google Forms is chosen for its wide accessibility, ease of use and integration with data analysis tools. The survey link will be distributed via social media platforms and online banking forums to reach a broad demographic of Irish consumers. Participants can complete the survey with complete anonymity and at their convenience. The form will be mobile-friendly to accommodate users who primarily access the internet via smart phones as well personal computer/laptops. Responses will be automatically collected and stored securely in a Google Sheet, allowing for real-time data monitoring and easy export for further analysis. Google Forms will enable anonymous responses, encouraging honest and unbiased feedback from participants, which is crucial for obtaining reliable data on sensitive topics like online banking fraud.

4.6.4. Interpretation and Preliminary Discussion

After the analysis, the study enters a critical phase that connects raw data to actionable insights i.e. the Interpretation and Preliminary Discussion. This stage is essential for transforming statistical outcomes into meaningful conclusions that directly address the research objectives and questions. While the Data Analysis section focuses on quantifying relationships and identifying

patterns among variables, this section interprets what these numerical findings reveal about customers perception about online fraud and the banking measures to protect them from such online fraud. This phase is crucial for understanding the implications of the data to realize the customer perception about effectiveness of their banks initiative for further actionable recommendations.

The interpretation and preliminary discussion of the survey questionnaire responses involve a multi-faceted approach using statistical tools like Chi-square tests, Cramér's V score and Natural Language Processing (NLP) techniques including Python Word Cloud.

Statistical Analysis using Chi-Square and Cramer's V: The Chi-square test is employed to assess the relationships between categorical variables, such as demographic factors like age, gender and their responses to specific questions regarding online banking security. By examining these relationships, we have tried to determine whether such Independent Variables have influence on customer response and behavior. If the Chi-square test indicates significant relationships, Cramér's V is calculated to measure the strength of these associations. A higher Cramér's V score suggests a stronger association, providing insights into which demographic factors significantly influence perceptions of online banking security.

NLP and Python Word Cloud Analysis: To analyze the customer suggestions and feedbacks we have used NLP techniques, including sentiment analysis and word cloud generation, for such open-ended responses. Word clouds visually represent the most frequently mentioned words and phrases where we have used most Frequent Key Word, Bigrams and Trigrams used by the survey participants. For instance, the frequent appearance of terms likes "fraud prevention," "banking security," and "multi-factor authentication" suggests these are major areas of concern among respondents. Sentiment analysis further categorizes these responses into positive, neutral, or negative sentiments, offering a deeper understanding of customer attitudes toward their banks' fraud prevention initiatives.

4.6.5. Ethical Consideration

For this study, ethical considerations are paramount. Participants will be informed about the purpose of the research, ensuring transparency. Consent will be obtained before data collection,

with assurances that participation is voluntary and responses are confidential. Data will be kept fully anonymous to protect participants' identities and any sensitive information will be securely stored. The study will comply with relevant data protection laws, including GDPR and will avoid any potential harm to participants by ensuring that the survey content is non-invasive and respectful of respondents' privacy and personal boundaries. Ethical approval will be sought from the relevant institutional review board.

4.6.6. Informed Consent

Before data collection through survey began, the participants will recieve an information page detailing the research's purpose and objectives, the nature of their participation, any potential risks and the expected duration. This will ensure that participants fully understood what about their participation would entail. Participants are also made aware of complete anonymity of their identity while participating in the survey. This process will ensure that consent was informed and voluntary.

CHAPTER FIVE: RESEARCH RESULT AND INTERPRETATION

The Research Results and Interpretation section is pivotal in bridging the gap between raw data and the study's research objectives. This section will present the findings derived from the collected data, offering a detailed analysis and interpretation of key results. By examining patterns, relationships and trends within the data, this section aims to provide insights that answer the research questions and support or refute the hypotheses. Through the use of Statistical Tools, Natural Language Processing (NLP) and data visualization techniques, the study will translate numerical results into meaningful conclusions, shedding light on the effectiveness of banking initiatives in combating online financial fraud in Ireland.

5.1. Descriptive Statistics

The Descriptive Statistics section plays a vital role in setting the context for the data by providing a detailed demographic overview of the sample population. This section analyzes various demographic factors, including gender, age, education level, employment status. Analyzing these demographic aspects is key, as they form the basis for understanding how the study's core variables, particularly those related to consumer perspective and attitudes toward

online financial fraud prevention, are influenced. By categorizing the sample into these demographic segments, the research aims to present a clearer picture of the customer perception and behavior towards online fraud and banking security, setting the stage for more in-depth statistical analyses in the following sections.

5.2. Inferential Statistics

Use of Inferential statistics play is as well crucial for analysis of the results and outcome of this dissertation, particularly in evaluating the effectiveness of bank initiatives aimed at combating online financial fraud. Inferential statistics helps to draw a conclusion and make predictions about a larger population based on the sample data collected. This is particularly relevant for understanding the broader impact of fraud prevention campaigns on various demographic groups across Ireland. Use of tools like **Chi-Square Analysis** enables the examination of relationships between various categorical variables, such as the association between demographic factors (e.g., age, gender) and awareness of fraud prevention initiatives. By doing so, the study can identify patterns or differences in how various groups respond to these initiatives. **Cramér's V** further quantifies the strength of these associations, providing a more nuanced understanding of the effectiveness of the campaigns. **Word Clouds** are used to summarize and visually represent the frequency of words or phrases in a dataset, offering a clear and immediate way to interpret qualitative data. This helps identify key themes or concerns among participants. The most frequent words can highlight dominant issues or areas of satisfaction, while the least frequent words may reveal shadow areas that could require further investigation.

Table: Demographic information of the survey respondents: Total Respondents - 102

Characteristics	Numbers	Percentage
Gender		
Male	68	68.30%
Female	31	30.70%
Prefer Not to Say	1	1.00%
Age groups (in years)		
18-24	12	12.00%
25-34	37	36.60%
35-44	30	29.70%
45-54	16	15.80%
55-64	5	5.00%
65 above	2	2.00%
Education Level		
High School or below	10	9.90%
Gradute	16	15.80%
Post Graduate	67	67.30%
Phd or above	7	6.90%
Others	2	1.10%
Employment Status		
Student	20	19.80%
Employed-Part Time	22	21.80%
Employed-Full Time	42	41.60%
Self Employed	5	4.90%
Professional	8	7.90%
Retired	1	1.00%
Others	4	4.00%

(Source: Self-made)

5.3. Statistical Analysis

Before delving into the detailed results of the survey, it is essential to establish the foundation for the statistical analysis employed in this dissertation. The Chi-Square Test of Independence has been chosen as a key analytical tool to explore the relationships between various categorical variables gathered from the survey data. This test is particularly suited to the study's objective of assessing the effectiveness of banking initiatives against online financial fraud, as it allows for the examination of associations between demographic factors—such as age, gender—and the respondents' awareness and responsiveness to these initiatives.

By applying the Chi-Square analysis, this dissertation aims to identify significant patterns and correlations that could shed light on the factors influencing the success or limitations of fraud prevention strategies among different segments of the population. The insights gained from this analysis will be instrumental in interpreting how demographic variables may impact the effectiveness of these banking initiatives, ultimately guiding recommendations for more targeted and effective fraud prevention measures.

The following sections will present the results of the Chi-Square analysis, offering a comprehensive interpretation of how these statistical findings align with the broader research objectives. This section is prepared basis the Survey Questions numbers as responded by the survey participants, basis which Research Questions will be analysed.

Question 11 -How satisfied you are with security measures of your bank for Online Banking?

Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Gender** and **Satisfaction level of bank customers with security measures of Online Banking facility offered by their banks.**

- **Independent Variable**: Gender
- **Dependent Variable:** Satisfaction level of bank customers with security measures of Online Banking facility offered by their banks
- **Null Hypothesis –** There is no association between Gender and Customer satisfaction on security measures of Online Banking.
- **Alternate Hypothesis** – There is an association between gender and Customer satisfaction on security measures of Online Banking.

Pearson Chi-Square Analysis

Pearson Chi-Square: 229.811, df = 12, $p < .001$

The Pearson Chi-Square value of 229.811 with 12 degrees of freedom is significant at $p < .001$. This indicates that there is a statistically significant association between gender and the satisfaction level with the security measures of the online banking facility. **Hence we can reject Null Hypothesis.**

Statistical Significance: The large chi-square value suggests that the observed frequencies of satisfaction levels differ significantly from the expected frequencies, indicating a strong relationship between the two variables.

Cramer's V value: 0.627

Cramer's V value of 0.627 suggests a strong association between gender and satisfaction with online banking security measures with the p-value (< .001) confirms the statistical significance of this association.

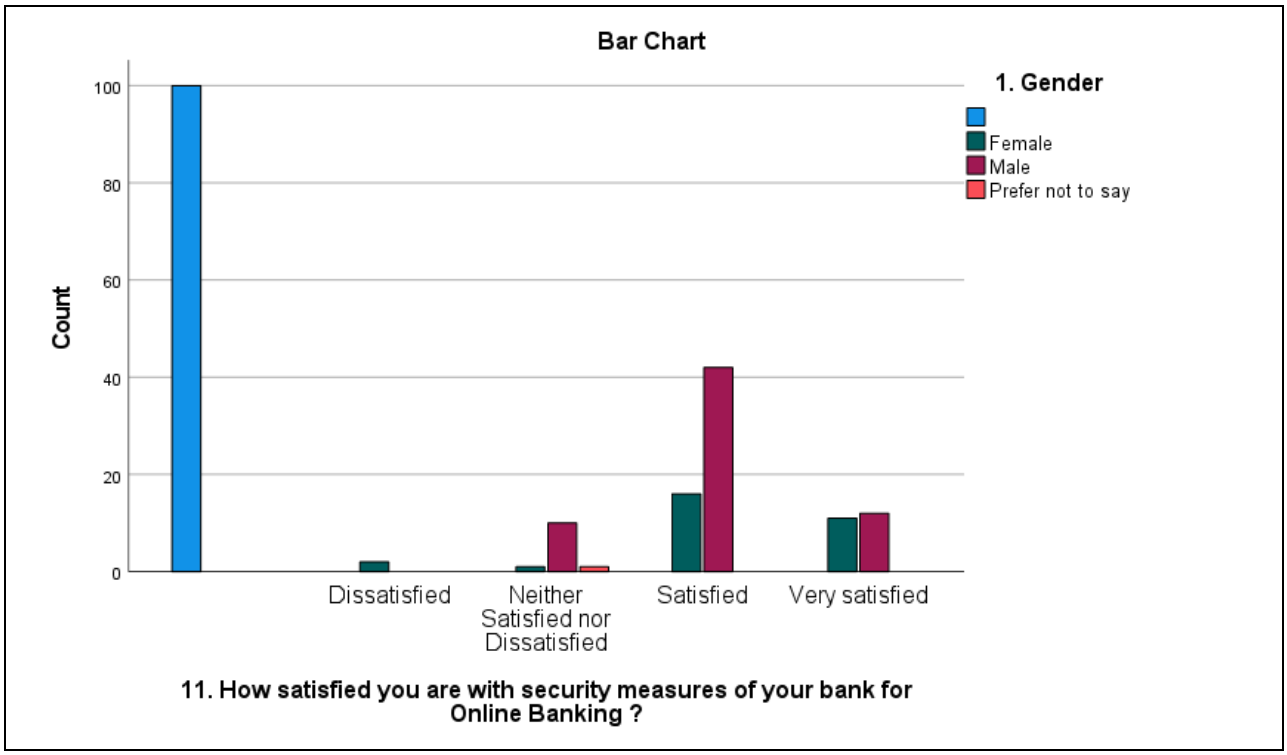
Practical Significance:

The significant association between gender and satisfaction levels indicates that male and female customers might have different perceptions of the security measures implemented by the bank. With traces of Male gender inclined to be more satisfied with bank actions as compared to Female. Banks should analyze these differences in detail to understand specific concerns or preferences of each gender. Banks can use the insights from this analysis to develop targeted initiatives aimed at improving satisfaction levels among the gender that may be less satisfied with current security measures. Providing personalized customer support that takes into account gender-specific preferences and concerns regarding online banking security can enhance overall satisfaction. This might include dedicated support teams or targeted communication campaigns.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	229.811[a]	12	<.001
Likelihood Ratio	285.275	12	<.001
a. 11 cells (55.0%) have expected count less than 5. The minimum expected count is .01.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.086	<.001
	Cramer's V	.627	<.001



Question 11 - Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Age of participants** and **Satisfaction level of bank customers with security measures of Online Banking facility offered by their banks.**

- **Independent Variable**: Age
- **Dependent Variable:** Satisfaction level of bank customers with security measures of Online Banking facility offered by their banks
- **Null Hypothesis –** There is no association between Age and Customer satisfaction on security measures of Online Banking.
- **Alternate Hypothesis** – There is an association between Age of survey participants and Customer satisfaction on security measures of Online Banking.

Pearson Chi-Square Analysis

Pearson Chi-Square: 234.403, df = 24, $p < .001$

The Pearson Chi-Square value of 234.403 with 24 degrees of freedom is highly significant ($p < .001$). This indicates a strong statistical association between the age of the customers and their satisfaction levels with the bank's online banking security measures. **Thus we can reject Null Hypothesis in this case.**

Statistical Significance: The p-value < .001 indicates a statistically significant association between Age and satisfaction levels with the bank's online banking security measures. This suggests that Age influences Customer satisfaction level of online financial security measures set up by their banks.

Cramer's V value: 0.548

Cramer's V value of 0.548 suggests a strength of the association is moderate between Age and Customer Satisfaction level with the p-value (< .001) confirms the statistical significance of this association.

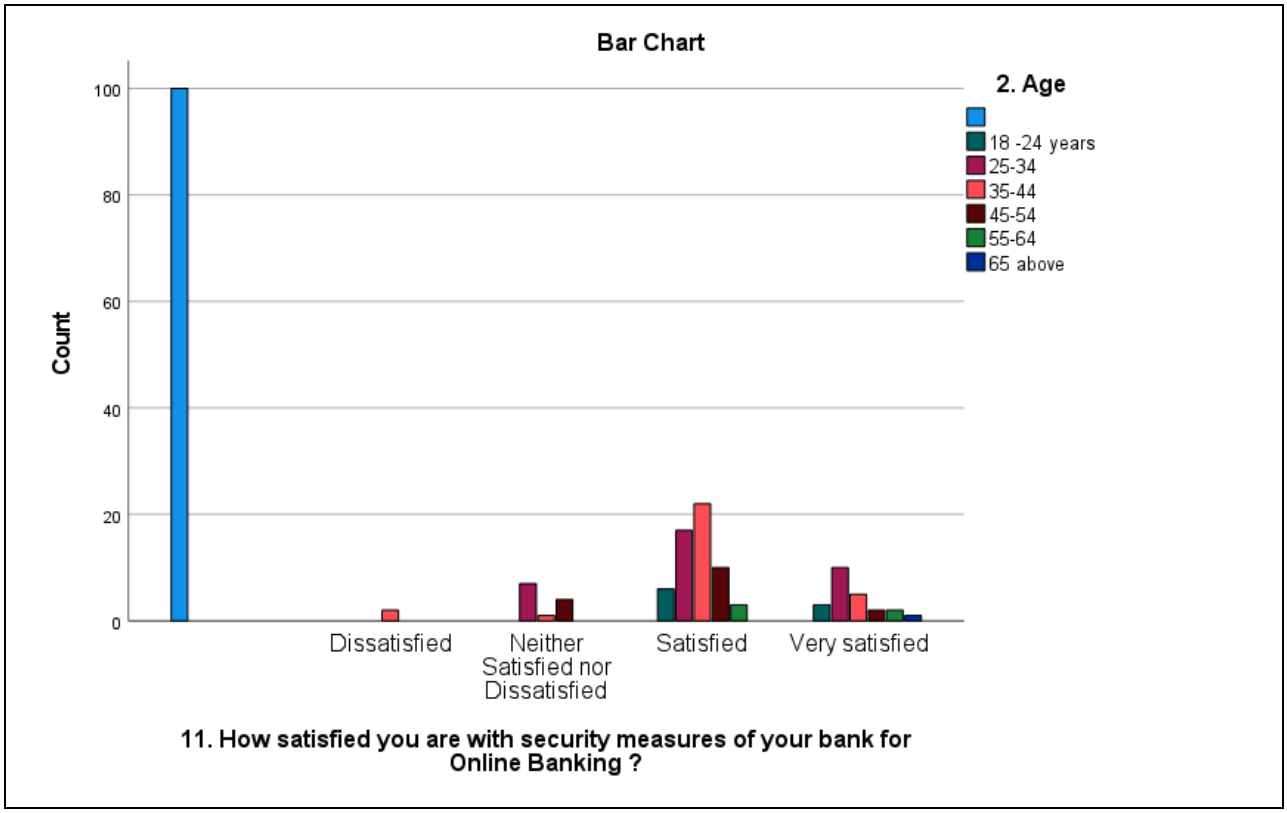
Practical Significance:

Given the statistical association between age and customer satisfaction levels, it is evident from the analysis that Age Group 35-44 years are most Satisfied with their bank safety measures. Keeping this in mind, banks must develop and promote security features basis different age category. While at same time must ensure that security features are user-friendly and easy to understand for older customers. By implementing features that cater to different age groups, will ensure that all age demographics feel secure and satisfied with the online banking facilities. Bank can also conduct age-specific educational campaigns to inform customers about how to use security features effectively and safely.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	234.403[a]	24	<.001
Likelihood Ratio	291.418	24	<.001
a. 26 cells (74.3%) have expected count less than 5. The minimum expected count is .01.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.096	<.001
	Cramer's V	.548	<.001



Question 12 - How familiar are you with different types of Online financial fraud (e.g., phishing, smishing)?

Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Gender** and **Familiarity with different types of online financial fraud.**

- **Independent Variable**: Gender
- **Dependent Variable:** Familiarity with different types of online financial fraud.
- **Null Hypothesis –** There is no association between Gender and familiarity with different types of online financial fraud.
- **Alternate Hypothesis** – There is an association between gender and familiarity with different types of online financial fraud. In other words, gender does influence how familiar individuals are with various types of online financial fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 203.426, df = 9, p < .001

The Pearson Chi-Square value of 203.426 with 9 degrees of freedom is highly significant with p value of < .001. **Therefore, with p value less than 0.001, we reject the null hypothesis** and conclude that there is a statistically significant association between gender and familiarity with different types of online financial fraud.

Statistical Significance: The p-value < .001 indicates a statistically significant association between gender and familiarity with different types of online financial fraud. This suggests that gender influences how familiar individuals are with various types of online financial fraud.

Cramer's V value: 0.590

Cramer's V value of 0.590 indicates a strong association between gender and familiarity with different types of online financial fraud. The value ranges from 0 to 1, with values closer to 1 indicating a stronger association. A value of 0.590 suggests a moderate relationship.

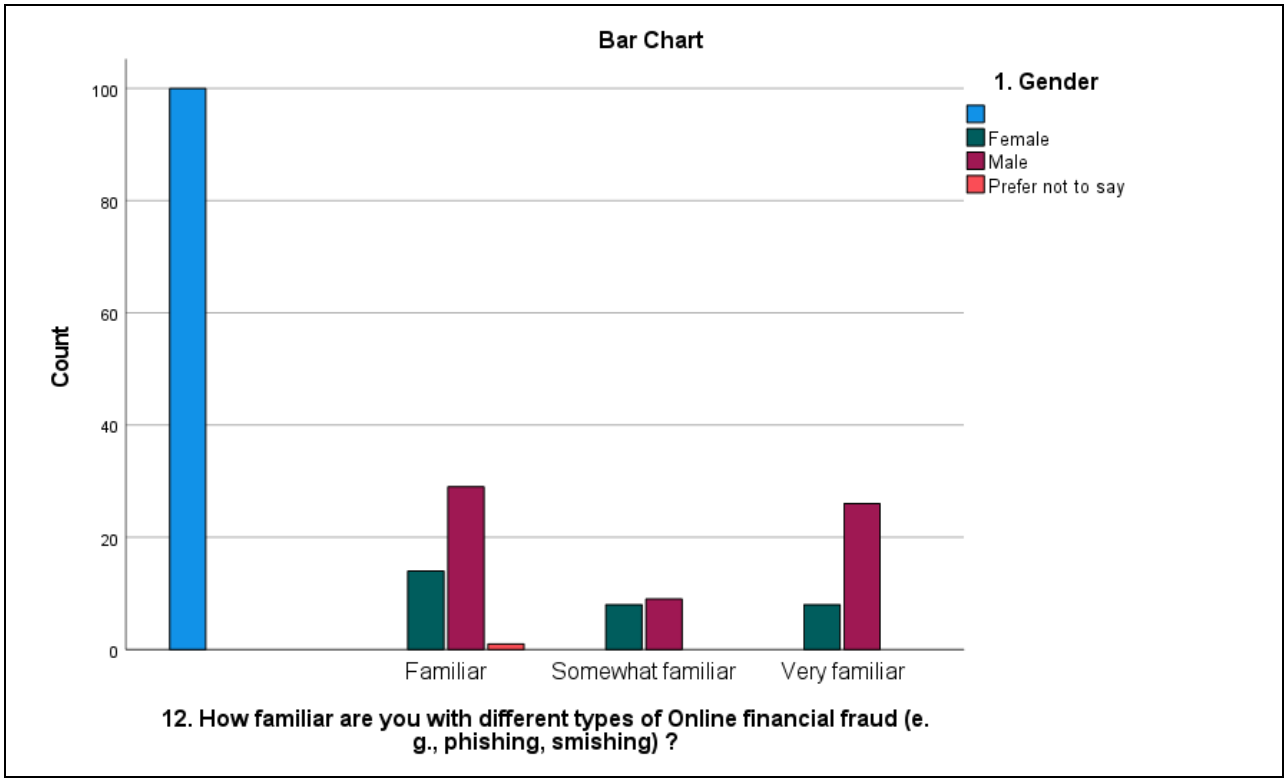
Practical Significance:

Since there is a significant association between gender and familiarity with online financial fraud, banks should consider customizing their educational campaigns based on gender. It is evident from the histogram that Male gender is more familiar as compared to overall participants. Understanding these differences can help the banks in designing more effective fraud prevention messages. Implement digital literacy programs that focus on improving the overall understanding of online security and fraud prevention. The bank should promote the use of advanced security features (like two-factor authentication and fraud alerts) more vigorously among the gender group that is found to be less familiar with online financial fraud. This will provide additional layer of security even if they fail to identify any fraud attempt. Educating customers about these security measures and their importance can help reduce the incidence of fraud.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	203.426[a]	9	<.001
Likelihood Ratio	274.606	9	<.001
a. 5 cells (31.3%) have expected count less than 5. The minimum expected count is .09.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.021	<.001
	Cramer's V	.590	<.001



Question 12 - Through this Chi- Square test we have tried to analyse if there is a statistically significant association between **Age** and **Familiarity with different types of online financial fraud.**

- **Independent Variable**: Age
- **Dependent Variable:** Familiarity with different types of online financial fraud.
- **Null Hypothesis –** There is no association between Age and familiarity with different types of online financial fraud.
- **Alternate Hypothesis** – There is an association between Age and familiarity with different types of online financial fraud. In other words, age does influence how familiar individuals are with various types of online financial fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 216.754, df = 18, p < .001

The Pearson Chi-Square value of 216.754 with 18 degrees of freedom is highly significant with p value < .001. This indicates a statistically significant association between age and familiarity with different types of online financial fraud. T**hus we reject Null Hypothesis in this case**. The low p-value suggests that the likelihood of this association occurring by chance is less than 0.1%.

Statistical Significance: The Chi-Square test of 216.754, df = 18, p < .001, indicates a significant association between age and familiarity with online financial fraud. Cramer's V value of .609 suggests a strong relationship, highlighting the importance of age-specific strategies in enhancing customer awareness and fraud prevention.

Cramer's V value: 0.609

The value of 0.609 indicates a strong association between the age of respondents and their familiarity with different types of online financial fraud. Cramer's V ranges from 0 to 1, where values closer to 1 signify a stronger association. Here, .609 is a substantial value indicating a considerable association.

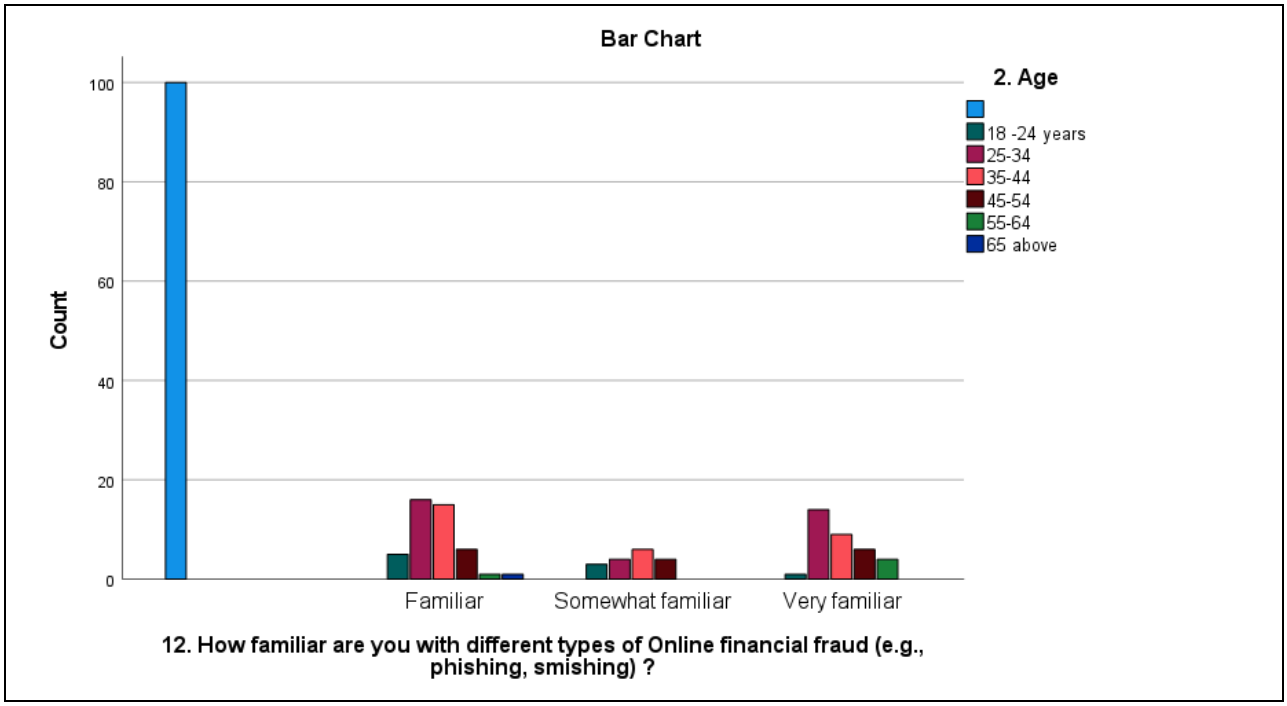
Practical Significance:

As per the statistical outcome establishing significant association with Age of respondents across all category and Familiarity with different types of online financial fraud banks might develop age-specific awareness campaigns like for older customers might need more fundamental information about online fraud, while younger customers, who may already be familiar with basic fraud types, might benefit from more advanced insights. Bank should plan to implement educational resources that are accessible to all age groups for example online tutorials, interactive modules and frequently updated security tips. Continuous feedback will help in fine-tuning the campaigns for better reach and impact. With such actions banks can take a more strategic approach in educating their customers, thereby reducing the risk of fraud across all age demographics.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	216.754[a]	18	<.001
Likelihood Ratio	281.942	18	<.001
a. 17 cells (60.7%) have expected count less than 5. The minimum expected count is .09.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.054	<.001
	Cramer's V	.609	<.001



Question 14- Have you ever seen or participated in any awareness campaigns from your bank about online fraud prevention?

Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Gender** and **Participation in any awareness campaign for fraud prevention from their bank.**

- **Independent Variable**: Gender
- **Dependent Variable:** Participation in awareness campaign for fraud prevention from their bank.
- **Null Hypothesis –** There is no relation between Gender and Participation in any awareness campaign for fraud prevention from their bank.
- **Alternate Hypothesis** – There is a significant relation between Gender and Participation in any awareness campaign for fraud prevention from their bank.

Pearson Chi-Square Analysis

Pearson Chi-Square: 195.033, df = 09, p < .001

The Chi-Square test statistic of 195.033 with 9 degrees of freedom and a p-value less than .001 indicates that there is a statistically significant association between gender and participation in awareness campaigns for fraud prevention from their bank. This significance suggests that the observed differences in campaign participation between genders are not due to random chance. **And we can reject Null Hypothesis in this case as well.**

Statistical Significance: The above statistical results indicate a statistically significant association between gender and participation in fraud prevention awareness campaigns. This is further supported by the high Cramer's V value of 0.577, suggesting a strong relationship. Banks should leverage this insight to design targeted awareness campaigns, potentially increasing engagement and effectiveness by addressing gender-specific preferences and concerns.

Cramer's V value: 0.577

Cramer's V score of 0.577 indicates a moderate association between gender and participation in fraud prevention awareness campaigns. This suggests that there is a statistical relationship where gender plays a notable role in influencing participation rates. Banks should consider gender-specific strategies to enhance the effectiveness of these campaigns.

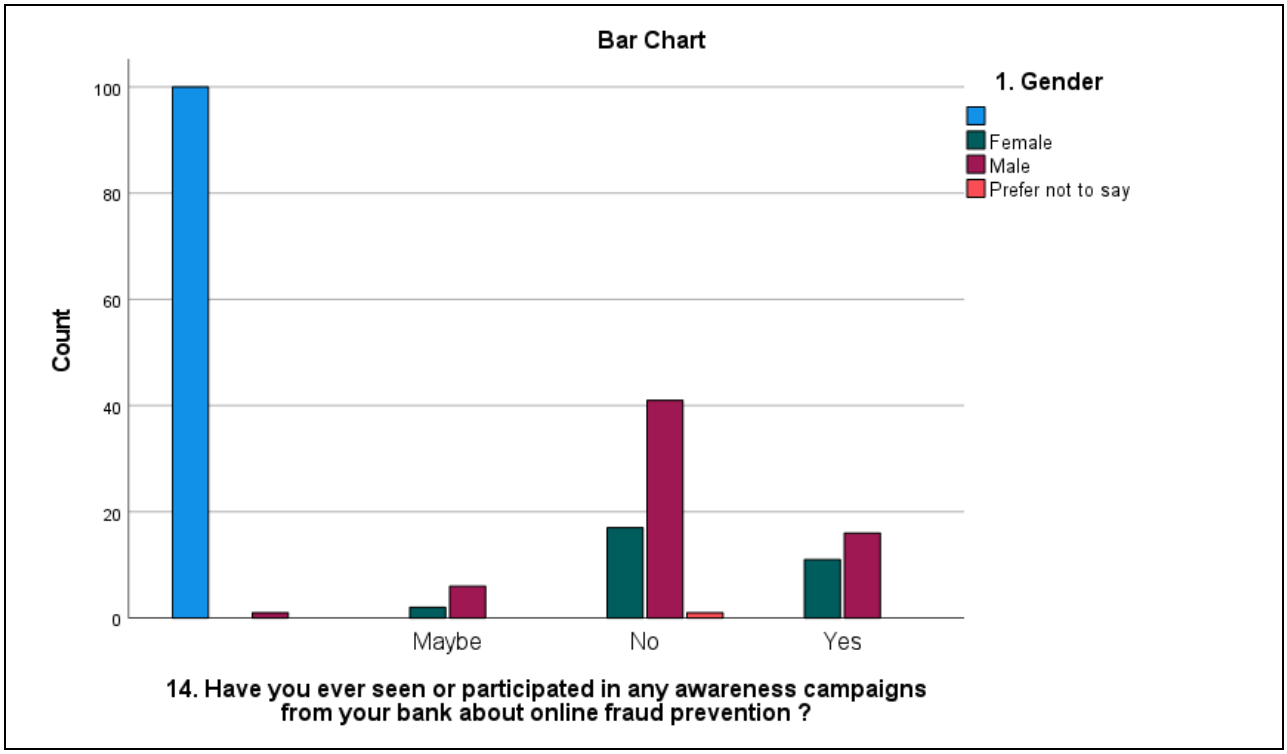
Practical Significance:

The strong association between Gender and Participation in Fraud prevention awareness campaigns implies that banks should consider gender-specific strategies when designing and promoting these campaigns. Tailoring content and outreach methods to address the unique concerns and behaviors of different genders could enhance engagement and effectiveness. By recognizing and addressing these differences, banks can improve the reach and impact of their fraud prevention efforts, ultimately leading to better-informed customers and reduced incidences of online fraud.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	195.033[a]	9	<.001
Likelihood Ratio	262.003	9	<.001
a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .04.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.000	<.001
	Cramer's V	.577	<.001



Question 14 Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Age of Survey participants** and **Participation in any awareness campaign for fraud prevention from their bank.**

- **Independent Variable**: Age
- **Dependent Variable:** Participation in awareness campaign for fraud prevention from their bank.
- **Null Hypothesis –** There is no relation between Age and Participation in any awareness campaign for fraud prevention from their bank.
- **Alternate Hypothesis** – There is a significant relation between Age and Participation in any awareness campaign for fraud prevention from their bank.

Pearson Chi-Square Analysis

Pearson Chi-Square: 216.938, df = 18, $p < .001$

The Pearson Chi-Square value of 216.938 with 18 degrees of freedom is significant at $p < .001$. This large Chi-Square value indicates a greater difference between the observed and expected frequencies, suggesting a stronger association between the variables. And P-value < .001 indicates a statistically significant association between age and participation in bank awareness campaigns about online fraud prevention. **So here as well we can reject Null Hypothesis based on the statistical outcome.**

Statistical Significance: The Chi-Square test result (Chi-Square value of 216.938 with 18 degrees of freedom and a p-value < .001) indicates that there is a statistically significant association between age of participants and individual participation in bank awareness campaigns about online fraud prevention.

Cramer's V value: 0.609

A value of 0.609 indicates a strong association between age and participation in awareness campaigns.

Practical Significance:

We can conclude with the given results there is a significant association between age and participation in fraud prevention campaigns, basis which banks can customize their awareness efforts to better engage different age groups. To make the campaigns more far reaching and effective bank can develop campaign materials that cater specifically to different age groups. For example, younger participants might prefer digital content, Utilize social media, mobile apps, and online videos to engage younger customers. While older participants might benefit from in-person workshops or printed materials. Leverage traditional media such as newspapers, direct mail, and in-branch seminars to reach older customers. By doing so, will enhance customer engagement, increase participation rates and ultimately strengthen their overall fraud prevention efforts making it more effective.

Test Results and Graph Chart:

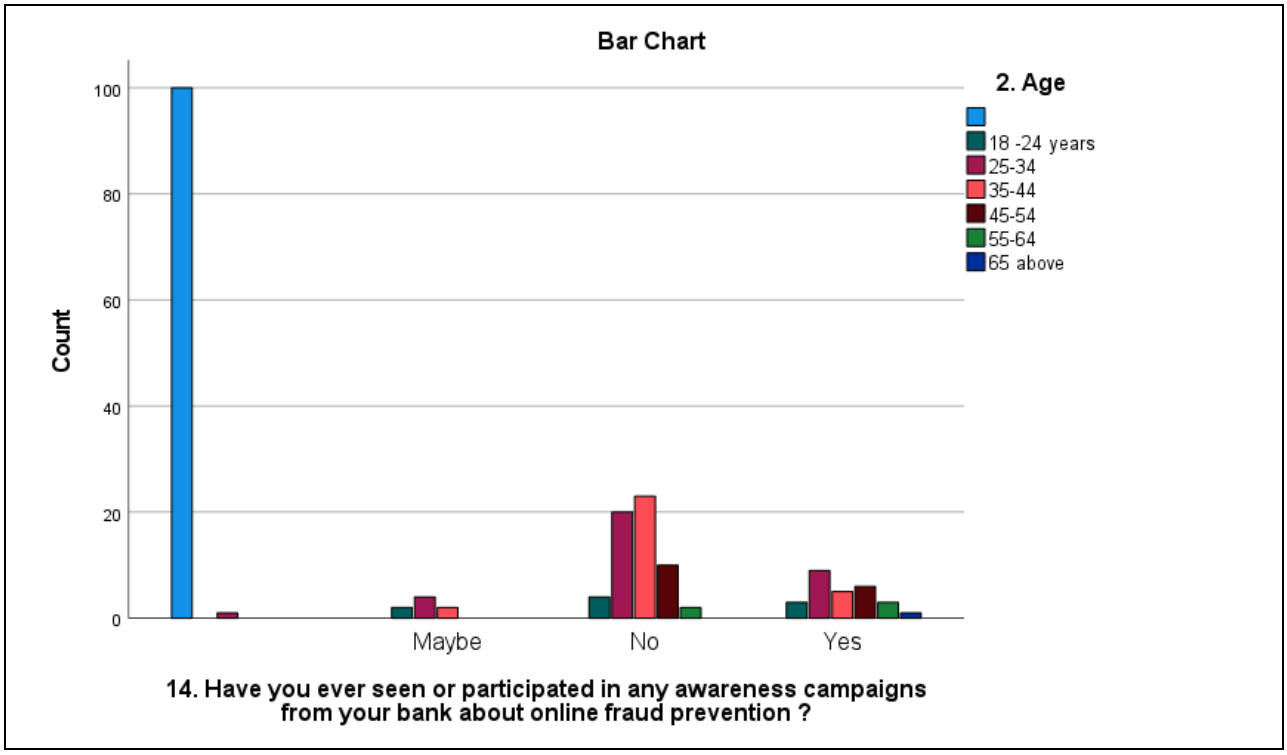
Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	216.938[a]	18	<.001
Likelihood Ratio	274.529	18	<.001

a. 20 cells (71.4%) have expected count less than 5. The minimum expected count is .04.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	1.055	<.001
	Cramer's V	.609	<.001



Question15. Do you believe that your bank adequately emphasizes safety and security of online banking to prevent any fraud?

Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Gender** and **Customer perception whether their bank takes adequate safety and security measures to prevent online fraud.**

- **Independent Variable**: Gender
- **Dependent Variable:** Customer perception whether their bank takes adequate safety and security measures to prevent online fraud
- **Null Hypothesis –** There is no relation between Gender and Customer perception whether bank takes adequate safety and security measures to prevent online fraud**.**
- **Alternate Hypothesis** – There is a significant relation between Gender and Customer perception whether bank takes adequate safety and security measures to prevent online fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 210.628, df = 15, p < .001

The Chi-Square value of 210.628 with degree of freedom of 15 and p-value less than .001 indicates a significant difference between the observed and expected frequencies in the contingency table, suggesting strong association between gender and Customer perception whether bank takes adequate safety and security measures to prevent online fraud. **Hence we can reject Null Hypothesis.**

Statistical Significance: The Pearson Chi-Square value of 210.628 with 15 degrees of freedom is significant at p < .001. This indicates that there is a statistically significant association between gender and the perception of the bank's security measures. The probability that this association is due to chance is less than 0.1%.

Cramer's V value: 0.600

Cramer's V value is a measure of association ranges from 0 to 1, with values closer to 1 indicating a stronger association. A value of 0.600 indicates a strong association between gender and perception of the bank's security measures. The approximate significance value of < .001 confirms that this association is statistically significant.

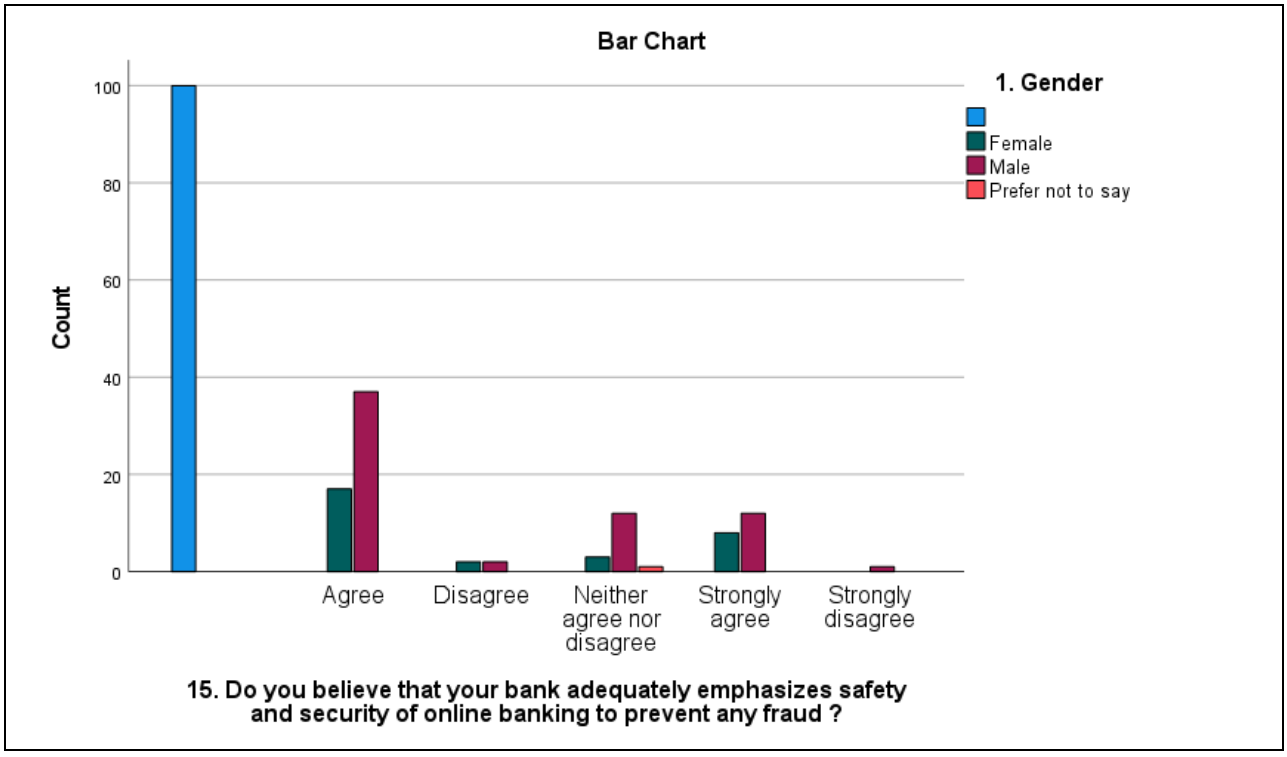
Practical Significance:

Given the significant association between Gender and Customer perception of the bank's security measures, banks can use this information to improve their communication to better address the concerns of different genders. It is also evident Male gender are more Satisfied with banking measures as compared to Female. This apprehension among the Female might be lack of awareness of various Fraud Attempts techniques as well. Banks can take effort to clearly explain the security measures in place through channels preferred by each gender. For example, younger males might prefer detailed explanations via online videos, while older females might appreciate in-branch consultations. Regular updates and notifications about new security measures can help build trust. Sharing customer testimonials and success stories about how the bank has protected customers from online fraud can help to build customer confidence and trust on the bank.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	210.628[a]	15	<.001
Likelihood Ratio	276.795	15	<.001
a. 14 cells (58.3%) have expected count less than 5. The minimum expected count is .01.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.039	<.001
	Cramer's V	.600	<.001



Question 15 - Through this Chi- Square test we have tried to analyze the statistically relation between **Age** and **Customer perception whether their bank takes adequate safety and security measures to prevent online fraud.**

- **Independent Variable**: Age
- **Dependent Variable:** Customer perception whether their bank takes adequate safety and security measures to prevent online fraud

- **Null Hypothesis –** There is no relation between Age of Customer and Customer perception whether bank takes adequate safety and security measures to prevent online fraud**.**
- **Alternate Hypothesis** – There is a significant relation between Age and Customer perception whether bank takes adequate safety and security measures to prevent online fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 225.090, df = 30, $p < .001$

This result indicates there is a statistically significant association between Age and Customer perception of whether their bank takes adequate safety and security measures to prevent online fraud. The p-value being less than 0.001 suggests that the probability of this association occurring by chance is very low, **thus rejecting Null Hypothesis in this case**.

Statistical Significance: The results suggest statistically significant association between age and customer perception of their bank's safety and security measures to prevent online fraud. With low p-value (< .001) suggests that this relationship is not due to chance. These findings suggest that banks should consider age-specific strategies to address varying security concerns among their customers.

Cramer's V value: 0.480:

The outcome indicates a moderate association between age and customer perception of bank safety measures. This means that age is a significant factor influencing how customers perceive the effectiveness of their bank's security measures.

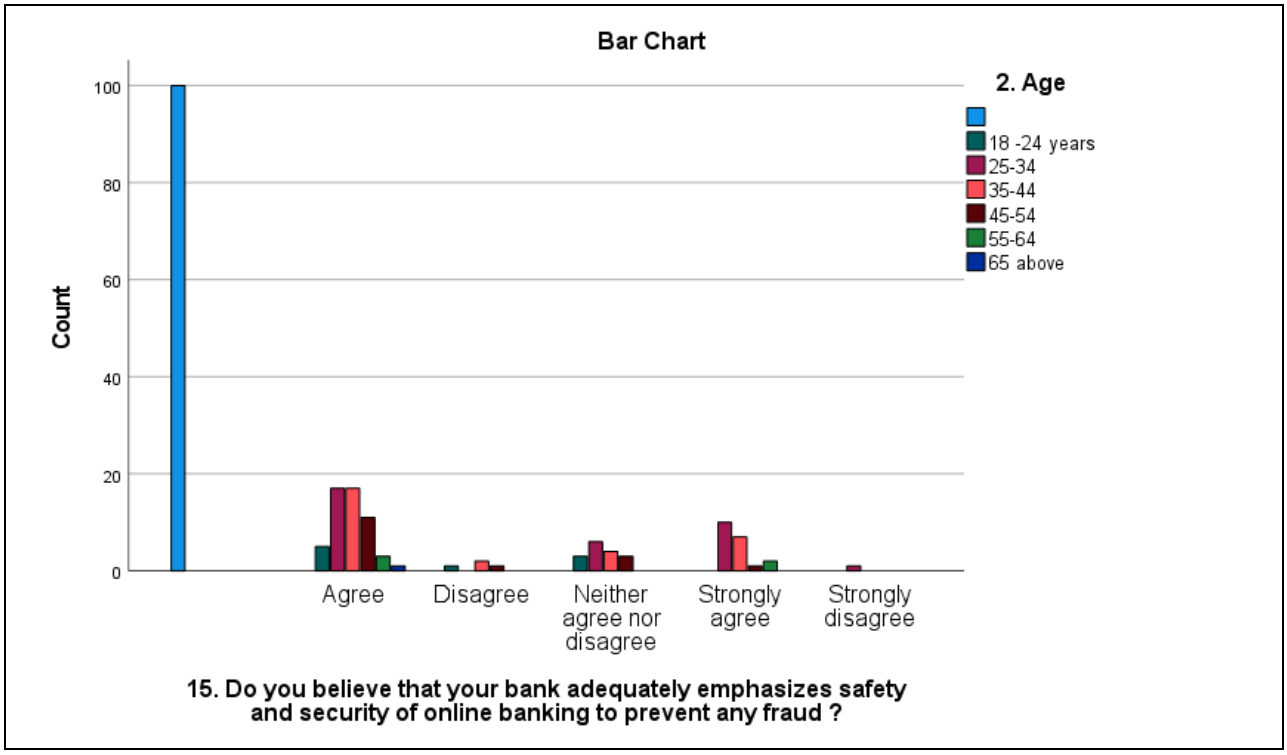
Practical Significance:

Banks should consider age-specific communication strategies to effectively address the safety and security concerns of different age groups. For example, younger customers may respond better to digital and tech-focused messages, while older customers might appreciate more straightforward communications. Understanding that age significantly affects perception can help banks engage more effectively with their customers by addressing their specific concerns and expectations regarding online fraud prevention.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	225.090[a]	30	<.001
Likelihood Ratio	289.464	30	<.001
a. 33 cells (78.6%) have expected count less than 5. The minimum expected count is .01.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.074	<.001
	Cramer's V	.480	<.001



Question16. How helpful do you find the awareness campaigns by your bank preventing online fraud tactics?

Through this Chi-Square test we have assessed whether there is a significant association between the two categorical variables: **Gender** and the **Customer perceiving the Bank Awareness campaigns are helpful in preventing online fraud.**

- **Independent Variable**: Gender

- **Dependent Variable:** Perception of the helpfulness of bank awareness campaigns in preventing online fraud.
- **Null Hypothesis** – There is no relation between Gender and Customer perceiving the bank awareness campaigns are helpful in preventing online fraud.
- **Alternate Hypothesis** – There is a relation between Gender and Customer perceiving the bank awareness campaigns are helpful in preventing online fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 231.815, df = 12, p < .001

In this case, the p-value less than 0.05 with 95% confidence level, suggests that the observed association between the Gender and Customer perception are statistically significant. There is strong relation between gender and the perception of the helpfulness of the bank awareness campaigns. **So we can reject Null Hypothesis in this case.**

Statistical Significance: The very low p-value (< .001) suggests that there is a statistically significant association between gender and the perception of the helpfulness of the bank's awareness campaigns in preventing online fraud. In other words, how individuals perceive the helpfulness of these campaigns for preventing online fraud appears to depend on their gender.

Cramer's V value: 0.629

Cramer's V value of 0.629 indicates a strong association between gender and the perception of the helpfulness of bank awareness campaigns in preventing online fraud. This value, closer to 1, suggests a substantial relationship.

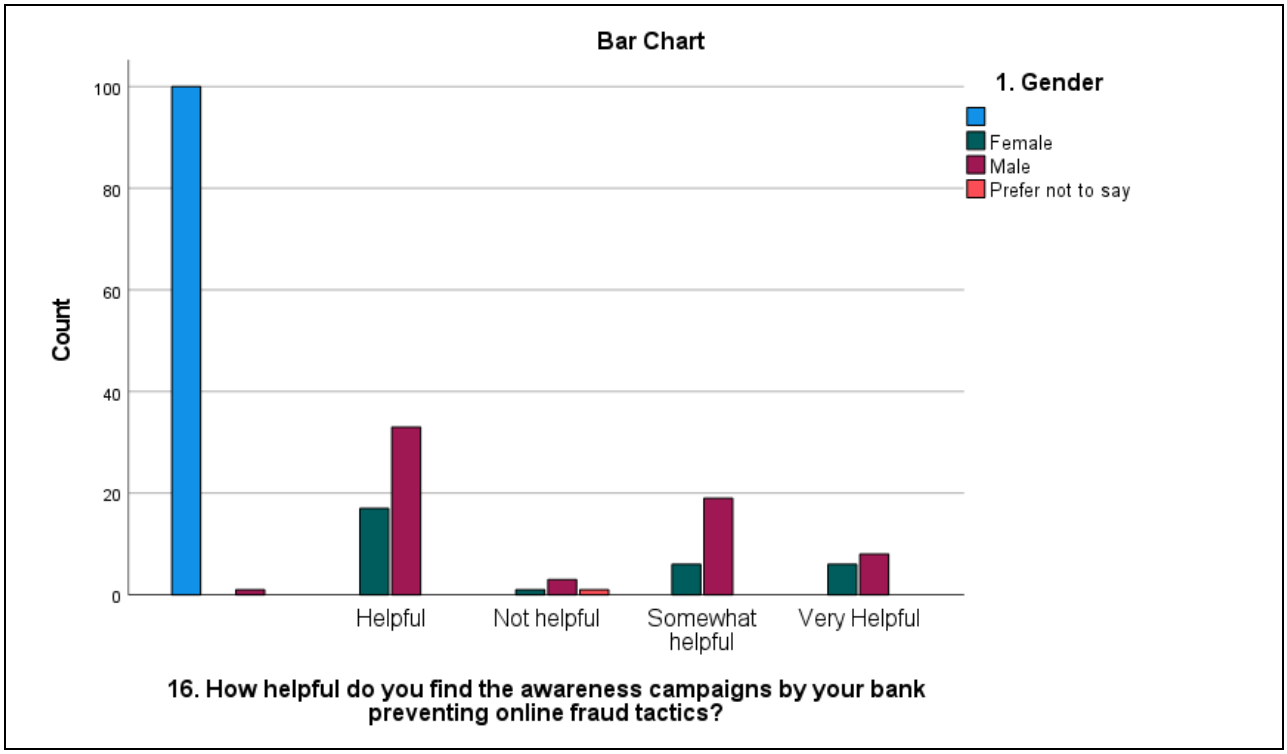
Practical Significance:

The bank can infer that Gender plays a vital role in how their campaigns are perceived in terms of preventing online fraud. This information can be used to tailor awareness campaigns more effectively by considering gender-specific preferences or perceptions. Create customized content that addresses the specific perceptions and needs of each gender. For example, if women find certain types of information more helpful, focus on those areas in the campaigns targeted at female customers. Bank can also focus on the medium of communication as per the digital literacy level of the customers. For instance, one gender may respond better to email campaigns while the other may prefer social media or in-person workshops. Banks can also look for the scope to promote digital literacy programs tailored to the needs of each gender, focusing on areas where there are significant gaps in perception and understanding.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	231.815[a]	12	<.001
Likelihood Ratio	267.525	12	<.001
a. 11 cells (55.0%) have expected count less than 5. The minimum expected count is .03.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.090	<.001
	Cramer's V	.629	<.001



Question 16- Through this Chi-Square test we have assessed whether there is a significant association between the two categorical variables: **Age of survey participant** and the **Perception of the helpfulness of bank awareness campaigns in preventing online fraud.**

- **Independent Variable**: Age

- **Dependent Variable:** Perception of the helpfulness of bank awareness campaigns in preventing online fraud.
- **Null Hypothesis** – There is no relation between Age and Customer perceiving the Bank Awareness campaigns are helpful in preventing online fraud.

- **Alternate Hypothesis** – There is a relation between Age of respondents and Customer perceiving the Bank Awareness campaigns is helpful in preventing online fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 212.059, df = 24, p < .001

The Pearson Chi-Square test result is 212.059 with 24 degrees of freedom and a p-value less than 0.001. This indicates a highly significant association between the independent variable- Age and the dependent variable- Perception of the helpfulness of bank awareness campaigns in preventing online fraud. **Thus we reject null hypothesis, which states that there is no association between these variables, is rejected.**

Statistical Significance: The statistical significance of the results is confirmed by the very low p-values (< .001) for both the Pearson Chi-Square test and the Likelihood Ratio. These results indicate that the observed association is not random and statistically significant.

Cramer's V value: 0.521

The Cramer's V value is 0.521, with a significance level of less than .001. Cramer's V measures the strength of the association on a scale from 0 to 1. A value of 0.521 suggests a moderate to strong relationship between age and the perception of the helpfulness of bank awareness campaigns.

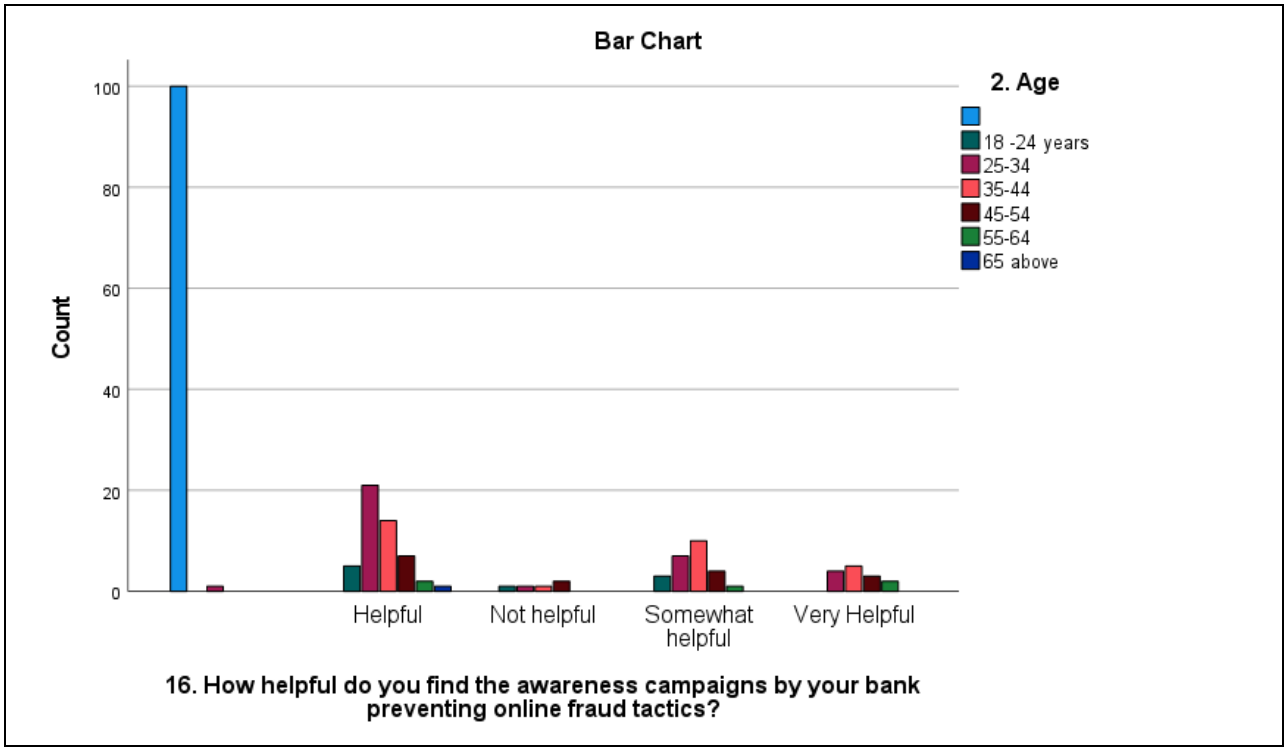
Practical Significance:

The significant p-value and Pearson Chi-Square value supported by moderately strong Cramer's V value suggests that age plays an important role in how customers perceive the helpfulness of bank awareness campaigns in preventing online fraud. Different age groups have their different perception and opinion about the effectiveness of the bank campaigns. Banks should consider tailoring their awareness campaigns to different age groups to enhance their effectiveness. This could involve using different communication channels, messaging styles and educational materials that can reach out each age category and make an impact in their understanding and implementation.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	212.059[a]	24	<.001
Likelihood Ratio	272.021	24	<.001
a. 26 cells (74.3%) have expected count less than 5. The minimum expected count is .03.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	1.043	<.001
	Cramer's V	.521	<.001



Question 17. Have you ever encountered any online fraudulent attempt?

Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Gender** and **Customer encountering online fraud.**

- **Independent Variable**: Gender
- **Dependent Variable:** Likelihood of customer being encountered to online fraud.
- **Null Hypothesis –** There is no relation between Gender and Likelihood of customer encountering online fraud
- **Alternate Hypothesis** – There is a significant relation between Gender and Likelihood of customer encountering online fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 116.571, df = 6, p < .001

A higher Pearson Chi-Square value of 116.571 indicates a larger difference between the observed and expected counts, suggesting a stronger association. A p-value of less than .001 means that there is less than a 0.1% chance that the observed association is due to random variation. **Hence we Reject the Null Hypothesis** to conclude there is statistically significant relation between Gender and Customers encountering online fraud.

Statistical Significance: The Pearson Chi-Square value of 116.571 with 6 degrees of freedom is significant at p < .001. This indicates a statistically significant association between gender and whether customers have encountered online fraud. The probability that this association is due to chance is less than 0.1%.

Cramer's V value: 0.547

Cramer's V value of 0.547 indicates a moderate to strong association between gender and the likelihood of encountering online fraud. Since Cramer's V ranges from 0 to 1, a value closer to 1 indicates a stronger relationship.

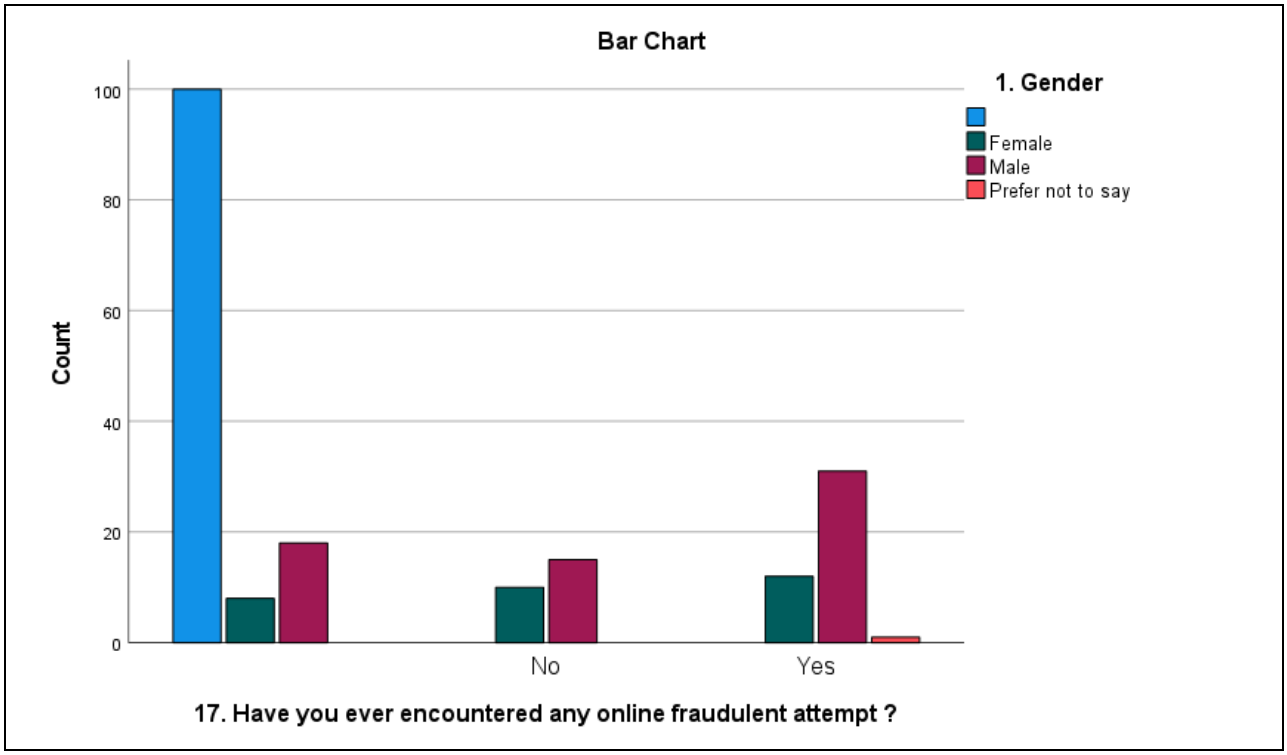
Practical Significance:

Given the above results, we can conclude that there is a statistically significant relationship between gender and the likelihood of encountering online fraud among the customers surveyed. This establishes that gender is a factor that influences whether a customer is likely to experience online fraud. AS per the response obtained it reflects Male gender are more likely to encounter Fraud Attempt unlike the Female. Bank can develop and deploy targeted fraud prevention campaigns that address the specific vulnerabilities and concerns of different genders. Another good way to build customer confidence is to highlight success stories of customer overcoming fraud attempt and provide clear guidance on how to avoid common fraud schemes. Bank can plan to conduct workshops, webinars, and informational sessions on online fraud prevention, ensuring they are inclusive and address gender-specific concerns. By acknowledging the significant association between genders and encountering online fraud, banks can take proactive steps to enhance their security measures and better protect their customers.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	116.571[a]	6	<.001
Likelihood Ratio	144.528	6	<.001
a. 4 cells (33.3%) have expected count less than 5. The minimum expected count is .13.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.773	<.001
	Cramer's V	.547	<.001



Question 17 - Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Age of respondents** and **Customer encountering online fraud.**

- **Independent Variable**: Age
- **Dependent Variable:** Likelihood of customer being encountered to online fraud.

- **Null Hypothesis –** There is no relation between Age and Likelihood of customer encountering online fraud

- **Alternate Hypothesis** – There is a significant relation between Age of customer and Likelihood of customer encountering online fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 130.503, df = 12, $p < .001$

The Pearson Chi-Square value of 130.503 with 12 degrees of freedom and a p-value of less than 0.001 indicate a statistically significant association between Age and the likelihood of encountering online fraud. This suggests that age plays a significant role in determining the likelihood of a customer encountering online fraud. **So we can Reject Null Hypothesis.**

Statistical Significance: The p-values in the Chi-Square test is less than 0.001, demonstrating that the results are highly statistically significant. This significance level implies that the observed association between age and the likelihood of encountering online fraud is not due to random chance.

Cramer's V value: 0.578

The Cramer's V value of 0.578 indicates a strong association between age and the likelihood of encountering online fraud. This value, significant at $p < .001$, suggests that age is an important factor influencing customers' likelihood of facing online fraud, highlighting the need for age-specific fraud prevention measures.

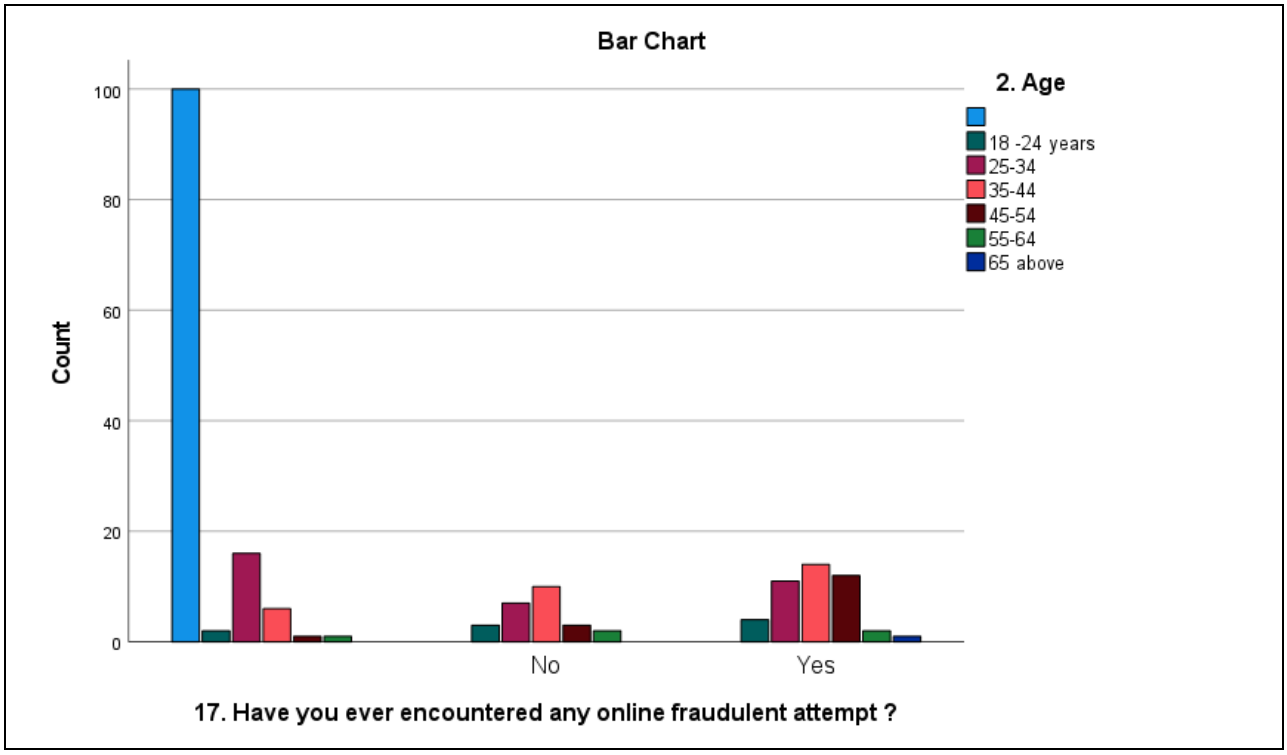
Practical Significance:

The strong Cramer's V value of 0.578 signifies a robust relationship between age and the likelihood of encountering online fraud. Practically, this means that banks should tailor their fraud prevention strategies to different age groups. For instance, younger customers might benefit more from digital literacy programs and advanced security features, while older customers may need simpler, more user-friendly security measures and personal guidance. Recognizing this age-based disparity can help banks develop more effective and targeted interventions, ultimately enhancing overall customer protection and reducing the incidence of online fraud across various age demographics.

Test Results and Graph Chart

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	130.503[a]	12	<.001
Likelihood Ratio	157.938	12	<.001
a. 12 cells (57.1%) have expected count less than 5. The minimum expected count is .13.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.818	<.001
	Cramer's V	.578	<.001



Question 18. Are these preventive measure from your bank has helped you to avoid any fraudulent attempts?

Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Gender** and **Customer perception on the effectiveness of bank lead preventive measures in avoiding online fraud.**

- **Independent Variable**: Gender
- **Dependent Variable:** Customer perception on the effectiveness of bank lead preventive measures in avoiding online fraud.

- **Null Hypothesis –** There is no relation between Gender and Effectiveness of bank lead preventive measures to avoid online fraud.

- **Alternate Hypothesis** – There is a significant relation between Gender and Effectiveness of bank lead preventive measures to avoid online fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 137.192, df = 9, p < .001

A higher value indicates a greater difference between observed and expected frequencies. In our case, a value of 137.192 is relatively high, suggesting a substantial difference between the observed data. A p-value of less than .001 suggests that there is less than a 0.1% probability that the observed association is due to random variation. Since the p-value is significantly less than the conventional threshold of 0.05, **we reject the null hypothesis.**

Statistical Significance: The Pearson Chi-Square test value 137.192, df = 9, p < .001 indicates a statistically significant association between gender and the perception of the effectiveness of the bank's preventive measures against online fraud. The p-value less than .001 suggest that this association is unlikely to be due to chance. Overall we can conclude from statistical outcome, gender influences customer perception of the bank's fraud prevention efforts.

Cramer's V value: 0.484

Cramer's V is a measure of association for nominal variables, providing a value between 0 and 1, where higher values indicate a stronger association. A Cramer's V value of .484 suggests a moderate association between gender and the perception of the effectiveness of preventive measures.

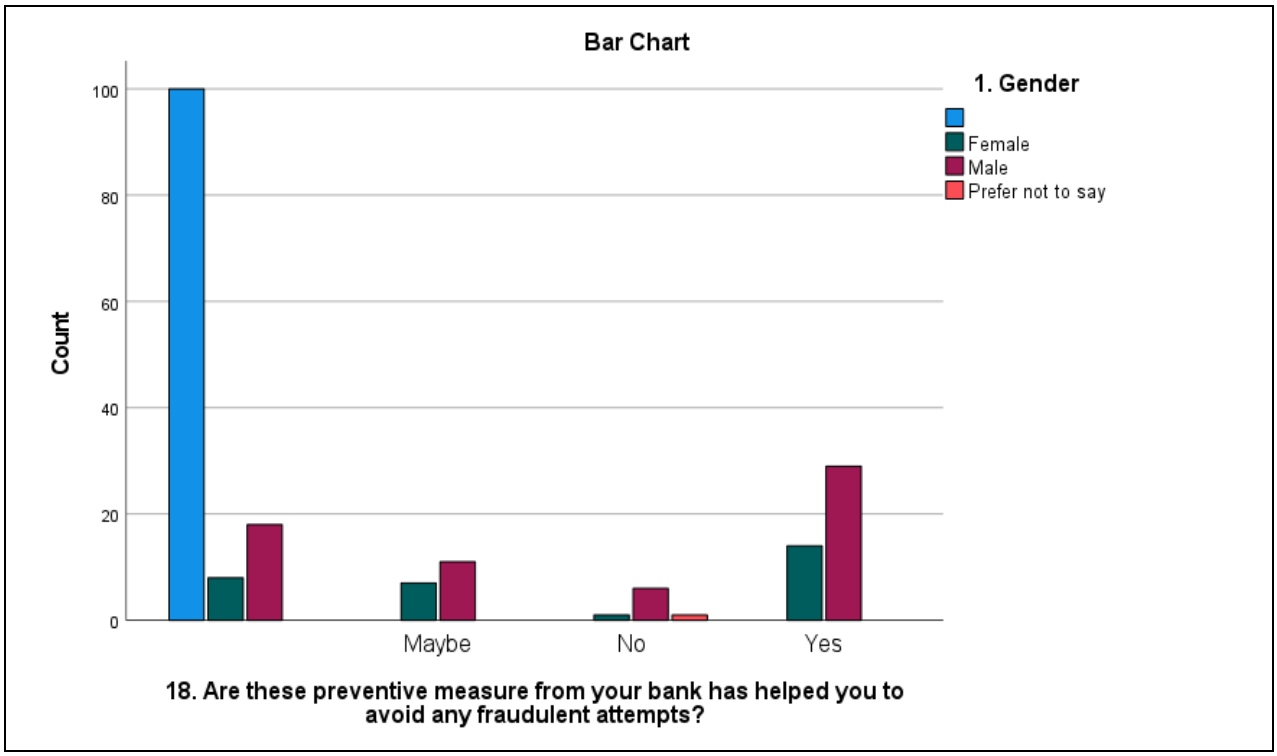
Practical Significance:

With the given outcome there is a significant association between gender and the perception of the effectiveness of the bank's preventive measures in avoiding online fraud. From the responses received Male gender has find the bank awareness campaigns more effective to avoid fraud attempts. Banks must develop gender-specific communication strategies to ensure that the effectiveness of preventive measures is perceived equally across different genders. There must be periodical engagement customers through focus groups and surveys to gather deeper insights into their perceptions and experiences. There must be continuous monitoring of the effectiveness of preventive measures and adjust strategies based on feedback and emerging fraud trends. This can lead to higher customer satisfaction, loyalty, and trust in the bank's security measures.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	137.192[a]	9	<.001
Likelihood Ratio	148.549	9	<.001
a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .04.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.839	<.001
	Cramer's V	.484	<.001



Question 18 - Through this Chi- Square test we have tried to analyze if there is a statistically significant association between **Age of respondents** and **Customer perception on the effectiveness of bank lead preventive measures in avoiding online fraud.**

- **Independent Variable**: Age
- **Dependent Variable:** Customer perception on the effectiveness of bank lead preventive measures in avoiding online fraud.

- **Null Hypothesis –** There is no relation between Age and Effectiveness of bank lead preventive measures to avoid online fraud.

- **Alternate Hypothesis** – There is a significant relation between Age of respondents and Effectiveness of bank lead preventive measures to avoid online fraud.

Pearson Chi-Square Analysis

Pearson Chi-Square: 134.381, df = 18, p < .001

The Pearson Chi-Square value is 134.381 with degrees of freedom (df) of 18 and a p-value less than 0.001. This low p-value indicates that the observed differences between the expected and actual frequencies are statistically significant. Hence we can **reject Null Hypothesis in this case.**

Statistical Significance:

The statistical significance of the Chi-Square test, with a p-value < 0.001, reveals a strong association between the examined variables related to bank initiatives aimed at safeguarding customers and promoting awareness to deter online financial fraud in Ireland. The Cramer's V value of 0.479 indicates a moderate relationship, underscoring the practical relevance of these findings in enhancing the effectiveness of banks' fraud prevention strategies and customer education efforts.

Cramer's V value: 0.479

The Cramer's V value is 0.479, which is a measure of the strength of the association between the variables. A value of 0.479 suggests a moderate association between the referred variables. The significance level of <0.001 further supports this conclusion.

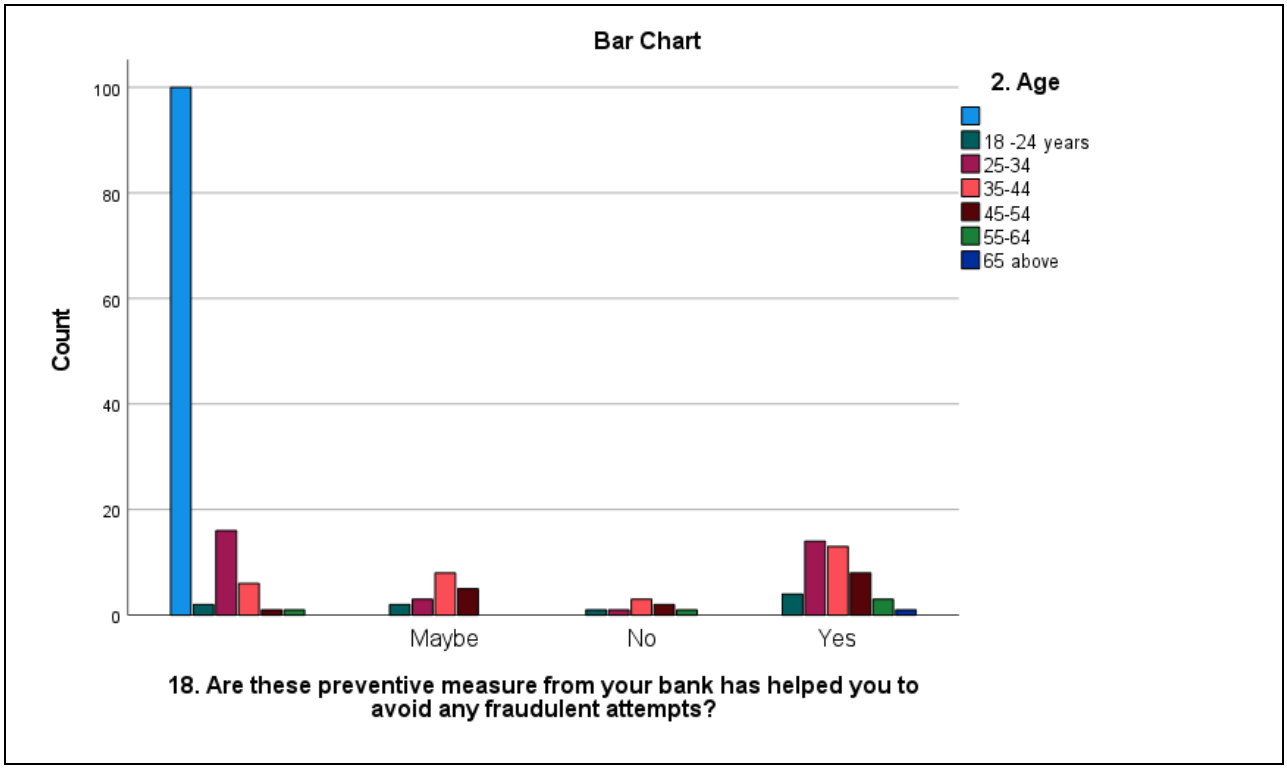
Practical Significance:

From the bank's perspective, the significant Chi-Square results and the moderate-to-strong Cramer's V value underscore the effectiveness of existing fraud prevention measures and customer awareness initiatives. Banks should continue investing in and possibly enhancing these awareness programs, as they are likely playing a crucial role in reducing online financial fraud. Additionally, the results indicate that customer education efforts are well-targeted, but there may still be room to strengthen the impact of these initiatives across different customer segments. This data-driven approach allows banks to optimize their strategies for maximum effectiveness in safeguarding their customers.

Test Results and Graph Chart:

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	134.381[a]	18	<.001
Likelihood Ratio	161.333	18	<.001
a. 19 cells (67.9%) have expected count less than 5. The minimum expected count is .04.			

Symmetric Measures			
		Value	Approximate Significance
Nominal by Nominal	Phi	.830	<.001
	Cramer's V	.479	<.001



20. Please add some comments or suggestions towards your bank regarding online banking security and fraud prevention initiative?

For this question, we have analyzed the feedback and recommendations provided by survey participants concerning the safety measures their banks could implement to enhance fraud prevention in online banking. By using **Natural Language Processing (NLP)** we have done sentiment analysis by using the comments and utilized **Word Cloud** to visualize the data. Word clouds visually represent the frequency of words, with larger words indicating higher usage. The analysis included **Single Words, Bigrams and Trigrams**, highlighting both the **Top Five Most Frequently Used Words** and the **Top Five Least Frequently Used Words**. Analyzing the most and least frequent single words, bigrams and trigrams provides a clear and concise understanding of the research background and concerns expressed by participants. The use of most frequent words helps to identify dominant topics and common sentiments, allowing focusing on areas that are most relevant to the participants.

Conversely, analyzing the least frequent words highlights less-discussed matters but which might turn out to be potentially significant issues that may warrant further investigation. This dual

approach ensures a comprehensive understanding of the participants' perspectives, enhancing the overall analysis by revealing both prevalent trends and overlooked nuances if any.

Sentiment Analysis

Top 5 Most Frequently Used Words

The word cloud provided highlights the Top 5 Most Frequently Used Words in comments from survey participants using online banking in Ireland. These words are "banking," "fraud," "customers," "bank," and "security." The sentiment analysis based on the Word Cloud and word frequencies, we have prepared strategic interpretation:

The frequent mention of **"fraud"** with a likely negative sentiment indicates a strong need for a dynamic fraud prevention measures. Banks should invest in advanced fraud detection systems and increase customer education on identifying and preventing fraud.

The prominence of **"customers"** highlights the importance of customer experience. Bank should look forward to create a customer feedback mechanism to gather customer insights and tailor banking services to meet customer needs better. Enhancing customer support channels to

acknowledge any fraud reporting and address customer concerns promptly, will definitely add more confidence and trust on the bank.

The word **"Security"** being frequently mentioned by customer during feedback and suggestions that indicates a positive sentiment that customers value strong security measures to be adopted by their banks. Customers likely to trust and rely on their banks for their safe keeping. Bank should conduct regular security awareness campaigns to keep them informed about the latest threats and safety practices.

Further the mention of words like **"banking" and "bank"** in frequent interval reflects the overall customer experience. Improve the usability and functionality of online banking platforms. Bank should plan to ensure seamless and intuitive user experiences while proving online banking platform. Along with the ease of accessibility, bank should also ensure safety concerns as well.

Top 5 Most Frequently Used Bigrams

Here, we have analyzed the Top Five Most Frequently Used Bigrams from the survey comments, which provide deeper insights into the participants' perspectives on online banking safety measures. The identified bigrams include "online banking," "security fraud," "bank online," "banking security," and "factor authentication."

Implement Multi-Factor Authentication: Given the emphasis on **"factor authentication,"** banks should prioritize the implementation of multi-factor authentication (MFA) to add an extra layer of security. This can be through use of personalized PIN along with generating One Time Password (OTP) or In-App confirmation etc. This will help in preventing unauthorized access and reducing fraud incidents.

Focus on Awareness Programs: The frequent use of bigram - **"security fraud"**, highlights a significant concern regarding fraud related to online banking security measures. Conducting gender and age specific awareness campaigns about security fraud can educate customers on recognizing and avoiding potential threats. Various fraud techniques such as phishing, social engineering and safe online practices can be shared to the customers. Such sentiment is very essential by providing resources and training on usage of security features to empower customers to protect their accounts effectively.

Regular Updates on Security Practices: The bigram - **"Online Banking" and "Bank Online",** appears prominently in customer suggestions, indicating a high level of engagement and concern among participants about the general concept of online banking. Keeping customers informed about the latest security measures and potential threats can build trust. Transparency about the steps taken to safeguard their information can reassure customers and enhance their confidence in "O**nline Banking."**

Partnerships with Security Experts: The recurrence of the bigram- **"Banking Security",** establishes the importance placed on security measures by the survey participants. Collaboration with cybersecurity experts can help banks stay informed about the latest threats and best practices. This collaboration will also ensure proactive measures taken by bank leading to the development of more effective security solutions.

Top 5 Most Frequently Used Trigrams

Here, we have analyzed the top five most frequently used trigrams as referred in above Word Cloud, derived from the survey comments. These trigrams include "banking security fraud," "online banking security," "security fraud prevention," "multi-factor authentication," and "regular security audits."

As we have seen in our previous Sentiment Analysis of Single Word and Bigram, there is similar alignment in the customer perception in Trigram as well. **"Banking Security Fraud"** reflects a deep concern among participants about the coherence of security and fraud within banking. It indicates that customers view security as a crucial element in preventing fraudulent activities. And customer relies on their bank to adopt stringent measures to protect them from any fraud incidence.

"Online Banking Security": The frequent mention of this trigram lays the importance of security specifically within the context of online banking, suggesting that customers are particularly worried about the safety of digital banking platforms and their dependence on their banks for safety and security.

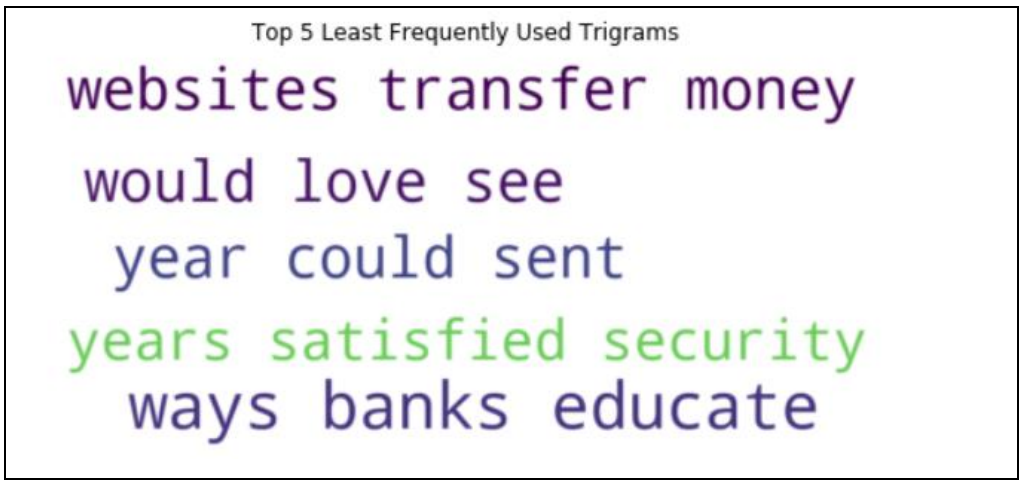
"Security Fraud Prevention": This trigram highlights a proactive stance among participants, emphasizing the need for preventive measures to combat fraud effectively. Banks should not only implement security measures but also engage in proactive fraud prevention initiatives. Bank

should responsibly share regular updates on emerging threats and tips on how their customers can avoid falling victim to fraud.

"Multi-Factor Authentication": The inclusion of this trigram points to a growing awareness and demand for advanced security features such as multi-factor authentication (MFA). Given the strong emphasis on MFA in every analysis it is evident that banks should prioritize the implementation and promotion of MFA across all online banking platforms. Banks must ensure that customers are aware of and utilize MFA can significantly reduce the risk of unauthorized access.

"Regular Security Audits": This trigram suggests that customers expect ongoing vigilance in the form of regular security assessments to ensure that banking systems remain secure over time. The frequent mention of "regular security audits" highlights the importance of maintaining a secure banking environment. Banks should conduct regular audits of their security systems and communicate the results to customers to build trust and reassure them of their commitment to security.

The sentiment analysis of the top five most used trigrams reveals that customers are highly concerned about security, particularly in the context of online banking and fraud prevention. To address these concerns, banks should focus on strengthening security protocols, conducting regular audits, educating customers, and collaborating with cybersecurity experts. By taking these steps, banks can enhance their security measures, prevent fraud, and ultimately build greater trust with their customers.



Top 5 Least Frequently Used Trigrams

In this Word Cloud we have analyzed the five least frequently used Trigrams in the context of the research topic, particularly focusing on NLP sentiment analysis, Analyzing the least frequent trigrams might reveal less-discussed yet potentially important issues that could require further exploration:

"Websites transfer money", suggests concerns or feedback related to the process of transferring money through bank websites. It might be a reflection of user experience based on bank's security and reliability of online transactions with ease. Bank customer always expects seamless online transfer of money at same time security will be taken care by their trusted bank.

Use of trigrams like **"Would love see"** likely to represent a desire for improvements or expectation among the bank customers in addition to online banking features, implying a positive sentiment towards potential enhancements.

Trigram like **"year could sent"** is somewhat ambiguous, but it may refer to expectations or reflections on a time frame, perhaps related to service delivery or communication from the bank.

"Years satisfied security" might indicate customer satisfaction with the security measures in place over a period, possibly showing a positive sentiment towards the bank's efforts in maintaining secure transactions.

"Ways banks educate" This phrase points to methods or strategies banks use to educate their customers, likely emphasizing the importance of awareness campaigns and customer education.

The use of NLP in this research offers significant benefits by enabling the extraction of meaningful insights from large unstructured text survey feedback. Using techniques like word clouds, it is possible to visualize and identify key themes, sentiments and patterns in survey feedback. By focusing using this Word Cloud we can focus on underexplored areas, NLP facilitates a more comprehensive understanding of consumer perceptions with further scope of improvements. Furthermore, NLP can serve as a powerful tool for future research, helping to uncover new trends and areas that merit deeper investigation, thereby continuously enhancing the effectiveness of customer awareness campaigns.

5.4. **Summary of Key Findings**

The statistical analysis of the Survey Response using Chi-Square Test, Cramer's V value and further application of Sentiment Analysis by using Word Cloud data provide several key findings for this research on bank initiatives to safeguard customers against online financial fraud in Ireland.

Chi-Square and Cramer's V Analysis: The Chi-Square test yielded a highly significant result, indicating that there are strong associations between customer awareness and the effectiveness of bank initiatives to prevent online fraud with various Demographic factors like Age, Gender. The moderate-to-strong Cramer's V value suggests that while the relationship is substantial, there is still room for improvement. Banks' current strategies are evidently making an impact, but additional measures could further enhance these efforts.

Word Cloud Analysis: The word cloud analysis, focusing on the most and least frequently used words, bigrams, and trigrams, highlights the area of concern to customers. Terms like "banking security," "fraud prevention," and "multi-factor authentication" were among the most frequently mentioned, underscoring the importance customer’s perception on these aspects factors. More frequent use of such words clearly shows the customer concern about security aspects of their bank while using online banking. The analysis of less frequently mentioned terms revealed

underlying issues that, although not prominent, may still be significant and warrant further investigation.

Overall Findings: Collectively, these findings suggest that banks in Ireland are on the right path with their fraud prevention and customer education initiatives. However, there is a clear need for continuous improvement along with customer feedback process particularly in addressing less visible but potentially impactful areas of concern. The strong statistical relationships identified affirm that customer awareness and bank measures are interconnected and optimizing these can lead to even more effective fraud prevention strategies. This research emphasizes the importance of a data-driven approach in enhancing the security and trustworthiness of online banking services.

CHAPTER SIX: DISCUSSION AND CONCLUSION

6.1. Discussion in Context of Research Questions

Based on the statistical results, findings and hypothesis testing, the key factors influencing the safety and security of online banking of Irish Banks and as well address our Research Questions can be summarized as follows:

1. Evolution of Banking Initiatives towards Public Awareness Campaigns in Ireland:

The word cloud analysis highlighted the frequent use of terms such as **"Security," "Fraud," and "Customers,"** indicating a strong focus on these areas in customer feedback towards Irish Banks. Over recent years, Irish banks have increasingly concentrated their public awareness campaigns on security and fraud prevention. The emphasis on **"Banking Security fraud"** and **"Online banking security"** in bigrams and trigrams further supports this evolution. The surge in online fraud attacks poses a significant threat to the future of online banking. Without effective countermeasures, banks may face escalating costs and a substantial erosion of consumer trust. Consequently, addressing these critical issues requires managing both perceived and actual security concerns (Sarel D. et al., 2006). This suggests that banks have prioritized educating

customers about the risks of online fraud along with imparting knowledge of fraud prevention measures and secure banking practices (Hoffman et al., 2016). The research findings also indicate that banks have significantly ramped up their efforts in recent years, incorporating a mix of traditional and digital channels to reach their customer across varied demography (Dapp T. et al., 2014). Bank initiatives have evolved to include more sophisticated and targeted educational campaigns starting from primary school level, which emphasize not only the identification of fraudulent activities but also proactive measures customers can take to protect themselves. Use of more personalized communication approach adopted by the banks in Ireland has been effective in raising customer awareness and lowering the risk of online fraud.

2. Disparities in customer perception across Demographic Variables:

The Chi-Square test results revealed statistically significant relationships between demographic (Independent) Variables (such as age, gender) and customer perceptions of bank initiatives. Along with moderate strength of such association with each variable, suggests that these demographic factors do influence how customers perceive and engage with fraud prevention campaigns. For example, younger customers or those with higher levels of education may have different expectations and responses to bank initiatives compared to older or less-educated customers. Such results lead to the necessity of tailor made awareness campaigns to be conducted by the banks in Ireland to effectively reach and resonate with diverse customer segments. A critical component of such shift must focus on personalized outreach strategies, allowing banks and financial institutions to connect with customers on a more individual basis, thereby enhancing customer satisfaction and loyalty and trust towards them. (Lucky Benjamin et al., 2024). The research findings indicate the banks should implement a more targeted approach in their campaigns, making sure that their messaging and outreach are specifically designed to connect with various customer segments of all demography.

3. Effectiveness of campaigns and programs to curb Online Financial Fraud:

The effectiveness of the various campaigns is reflected in both the Word Cloud and Chi-Square analysis. The frequent mention of terms like **"Multi-factor authentication"** and **"Security audits"** suggests that customers are aware of and value these specific security measures. The statistical significance of the Chi-Square test also suggests that while some campaigns are

effective, there is room for improvement, particularly in how these initiatives are perceived and understood by different demographic groups. Despite multiple efforts and all the good intentions, there is little empirical evidence as to whether such bank campaigns works to curb online fraud (Gotelaere & Paoli, 2022; Button & Cross, 2017; Cross & Kelly, 2016; Prenzler, 2020). In this context, various studies have pinpointed that lack of effective control to deter fraud, despite all such bank efforts might be due to significant risk factors such as age-related cognitive decline (Gamble et al., 2014), lack of emotional reactions (Kircanski et al., 2018), overconfidence in financial knowledge (Gamble et al., 2014) and the presence of depression coupled with unmet social needs (Lichtenberg et al., 2013). In a study it was demonstrated that short online educational programs using video or text content can potentially lower individuals' susceptibility to fraud (Burke et al.,2022). The study conducted by Smith and Akman (2008) across Australia and New Zealand, running media campaigns through TV, Radio etc concluded that such campaign was effective in raising public awareness about fraud and increased reporting.

In Ireland, the incidence of online financial fraud has shown significant fluctuations over the past few years. After peaking during the pandemic, fraud cases decreased substantially in 2022. According to the Central Statistics Office (CSO), there was a 56% drop in fraud, deception and related offenses in Q4 2022 compared to the same period in 2021(Recorded Crime Report, CSO). The recorded incidents fell from 5,297 to 2,310, largely due to a reduction in unauthorized transactions and phishing attempts. However, despite this recent decline, the number of fraud cases in 2022 remained 46% higher than the levels recorded in 2019, before the pandemic. This indicates that while there has been a significant decrease recently, the overall trend suggests a higher baseline of fraud activity compared to pre-pandemic levels.

These fluctuations highlight the ongoing challenges in combating online financial fraud, as cybercriminals continue to adapt innovative methods. The data underscores the need for continued vigilance and robust security measures to be adopted by all the banks in Ireland to protect consumers in the evolving digital landscape. Banks need to adopt targeted and personalized communication strategies to address the specific needs and vulnerabilities of diverse customer groups. This approach not only strengthens customer trust but also reduces the risk of fraud.

6.2. Future Work

The findings suggest that while banks in Ireland have made substantial progress in promoting awareness and implementing security measures, the effectiveness of these campaigns varies across different customer demographics. To enhance the overall impact, banks should continue to evolve their strategies, focusing on targeted communication and education efforts that address the specific needs and concerns of diverse customer groups. For future research, it is crucial to explore the long-term effectiveness of these initiatives and identify emerging trends in cybercrime that may require new strategies. Additionally, further studies could investigate the role of technology, such as AI and machine learning, in predicting and preventing online financial fraud. Expanding the scope to include comparative studies across different countries could also provide valuable insights into global best practices that could be applied in Ireland. This will ensure that Irish banks remain resilient and adaptive in the face of evolving cyber threats.

APPENDICES

Appendix 1 – Debriefing Form

Dear Participant,

My name is REDACTED I am currently pursuing Master of Science in Financial Technology at Dublin Business School and I am conducting research project titled "Examining bank initiatives to safeguard and promote customer awareness to deter Online Financial Fraud in Ireland". This study is a part of my academic work and will be submitted as my dissertation. I would like to invite you to participate in a research study that will form the basis for my dissertation. Please read the following information before deciding whether to participate.

What are the objectives of the study?

The purpose of this study is to investigate how the banks in Ireland are implementing and enhancing initiatives to safeguard customers against vulnerabilities of online financial fraud. It focuses on assessing the effectiveness of awareness campaigns and exploring customer perceptions across various demographics to better understand the impact of these efforts and further scope of improvement.

Why have you been invited to participate?

I would like to collect information from individuals residing in Ireland having bank account in Ireland meeting all the following criteria:

• Aged 18-50 years.

• Have a bank account in Ireland.

• Use the internet banking regularly.

What does participation involve?

Participation involves completing an online survey that will take approximately 3-4 minutes. The survey will consist of questions related to your demographics and user experiences and perceptions about accessing Online Banking facility

Right to withdraw:

Participants have the right to withdraw from the research at any time for whatever reason. Participants can also request at any time to have their response data removed from record. The identity of all respondents will be kept anonymous and there will be no record of personal information.

Appendix 2 – Survey Questionnaire

Informed Consent- Thank you for your interest to participate in this research study. This survey is being conducted by Krishnan Sanjeev Nair pursuing MSc. in Financial Technology from Dublin Business School, Ireland. This study is conducted to understand Irish bank customers' awareness of online financial fraud and effectiveness of bank-led awareness campaigns in Ireland.

This survey will take approximately 3 minutes to complete. You will be asked questions about your demographic details followed by questions related to your awareness towards online banking and financial fraud along with effectiveness of your bank initiatives within Ireland, in this respect.

All your responses will be kept strictly confidential. Your name or any other identifiable information will not be linked to your answers. The data will be stored securely and used solely for the purposes of this academic research study.

Do you agree to participate in the survey?

- Yes
- No

1. Gender

- Male
- Female
- Prefer not to say

2. Age

- 18 -24 years
- 25-34
- 35-44
- 45-54
- 55-64
- 65 above

3. Education Level

- High School or below
- Graduate
- Post graduate
- PdD or above
- Other

4. Employment Status

- Student
- Employed- Part Time
- Employed- Full Time
- Self Employed
- Professional
- Retired
- Other

5. Do you access Online Banking to manage bank account?

- Yes
- No

6. If you answer Yes for Q5. what device you use to access Online Banking ? (Can select multiple boxes)

- Personal Mobile / Tablet
- Personal Desktop / Laptop
- Public / Shared device
- Other

7. If your answer is Yes for Q5, what type of network you use to access Online Banking? (Can select multiple boxes)

- Own mobile network
- Personal Wi-Fi
- Public Wi-Fi
- Office Wi-Fi / LAN

8. How often you use Online Banking in a month?

- Daily
- Weekly Once
- Monthly Once
- More Frequently
- Rarely

9. What type of Online Banking Service you normally avail ? (Can select multiple boxes)

- Checking Account Balance
- Transfer of Fund
- Paying Utility Bills
- Online Shopping
- Investment

10. How often you change password of your Online Banking?

- Every Month
- Every 3 months
- Every 6 months
- Unless prompted

11. How satisfied you are with security measures of your bank for Online Banking?

- Very satisfied
- Satisfied
- Neither Satisfied nor Dissatisfied
- Dissatisfied
- Very dissatisfied

12. How familiar are you with different types of Online financial fraud (e.g., phishing, smishing)?

- Very familiar
- Familiar
- Somewhat familiar
- Not familiar at all

13. If you are familiar, please select the channels through which you received such awareness information from your bank? (Can select multiple boxes)

- Email
- SMS
- Postal mail
- Social media
- Online Bank portal
- In person

14. Have you ever seen or participated in any awareness campaigns from your bank about online fraud prevention?

- Yes
- No
- Maybe

15. Do you believe that your bank adequately emphasizes safety and security of online banking to prevent any fraud?

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

16. How helpful do you find the awareness campaigns by your bank preventing online fraud tactics?

- Very Helpful
- Helpful
- Somewhat helpful
- Not helpful

17. Have you ever encountered any online fraudulent attempt?

- Yes
- No

18. Are these preventive measures from your bank have helped you to avoid any fraudulent attempts?

- Yes
- No
- Maybe

19. On a scale of 5, how confident you are to identify any financial fraud attempt ? (5 being most confident)

- Least confident
- 1
- 2
- 3
- 4
- 5
- Most confident

20. Please add some comments or suggestions towards your bank regarding online banking security and fraud prevention initiative?

References:

1. Adelmann, F., Elliott, J., Ergen, I., Gaidosch, T., Jenkinson, N., Khiaonarong, T., Morozova, A., Schwarz, N. and Wilson, C. (n.d.). Cyber Risk and Financial Stability: It's a Small World After All. [online] Available at: https://www.imf.org/-/media/Files/Publications/SDN/2020/English/SDNEA2020007.ashx. [Accessed 10 Jun. 2024].
2. AIB Future Sparks. (n.d.). Helping Developing Key Life Skills. [online] Available at: https://aibfuturesparks.ie/ [Accessed 28 May. 2024]
3. AIB. (n.d.). How Do You Prevent Fraud? [online] Available at: https://aib.ie/security-centre/how-do-you-prevent-fraud [Accessed 22 Jun. 2024].
4. Aleksandras Melnikovas (2018). Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies * Journal of Futures Studies. [online] Journal of Futures Studies. Available at: https://jfsdigital.org/articles-and-essays/2018-2/towards-an-explicit-research-methodology-adapting-research-onion-model-for-futures-studies.[Accessed 8 Aug. 2024]
5. Balkin, J.M., Yale, P. and Al, E. (2007). Cybercrime: digital cops in a networked environment. New York: New York University Press.
6. Bank of Ireland expands series of fraud awareness events - Bank of Ireland Group Website. [online] Available at: https://www.bankofireland.com/about-bank-of-ireland/press-releases/2024/bank-of-ireland-expands-series-of-fraud-awareness-events [Accessed 22 Jun. 2024]
7. Bank of Ireland launches nationwide drive to improve the financial literacy of Ireland's primary school children - Bank of Ireland Group Website. [online] Available at: https://www.bankofireland.com/about-bank-of-ireland/press-releases/2019/bank-of-ireland-launches-nationwide-drive-to-improve-the-financial-literacy-of-irelands-primary-school-children/ [Accessed 27 Jun. 2024].
8. Bank of Ireland- Youth Financial Wellbeing - Talking quids with OLLIE Primary School Teacher Pack P2 to P7 Class resource. (n.d.). Available at: https://www.bankofirelanduk.com/app/uploads/2020/02/Approved-OMI028587-Ollie-the-Owl-Teacher-Guide-Oct19-FINAL-DIGITAL-v8.pdf [Accessed 22 Jun. 2024]
9. Bank of Ireland's 'Big Move' to help those moving banks. (2022). www.rte.ie. [online] Available at: https://www.rte.ie/news/business/2022/0509/1296893-bank-of-ireland-big-move-campaign/ [Accessed 27 Jun. 2024].

10. Bank, E.C. (2020). Payments statistics: 2019. www.ecb.europa.eu. [online] Available at: https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2019~71119b94d1.en.html [Accessed 02 Jun. 2024].
11. Benjamin, None Prisca Amajuoyi and None Kudirat Bukola Adeusi (2024). Marketing, communication, banking, and Fintech: personalization in Fintech marketing, enhancing customer communication for financial inclusion. International journal of management & entrepreneurship research, 6(5), pp.1687–1701. doi:https://doi.org/10.51594/ijmer.v6i5.1142. [Accessed 18 Aug. 2024.]
12. Cassim, F. (2014). Addressing the Spectre of Phishing: are Adequate Measures in Place to Protect Victims of Phishing? Comparative and International Law Journal of Southern Africa, [online] 47(3), pp.401–428. Available at: https://unisapressjournals.co.za/index.php/CILSA/article/view/11005/5460 [Accessed 14 Jun. 2024].
13. Central Bank launches campaign to help consumers avoid scam operations. [online] Available at: https://www.centralbank.ie/news/article/press-release-central-bank-launches-campaign-to-help-consumers-avoid-scam-operations-01-november-2023 [Accessed 27 Jun. 2024].
14. Central Bank of Ireland (2014). Explainer - What is financial regulation and why does it matter? [online] Central Bank of Ireland. Available at: https://www.centralbank.ie/consumer-hub/explainers/what-is-financial-regulation-and-why-does-it-matter. [Accessed 25 Jun. 2024].
15. Central Statistics Office (2019). Home - CSO - Central Statistics Office. [online] Www.cso.ie. Available at: https://www.cso.ie/en/ [Accessed 02 Jun. 2024].
16. Central Statistics Office (2024). Main Results Recorded Crime Q4 2023 - Central Statistics Office. [online] Www.cso.ie. Available at: https://www.cso.ie/en/releasesandpublications/ep/p-rc/recordedcrimeq42023/mainresults/ [Accessed 20 Aug. 2024].
17. Chen, B., Chen, Z. and Yao, T. (2018). Financial Literacy Confidence and Retirement Planning: Evidence from China. SSRN Electronic Journal. doi:https://doi.org/10.2139/ssrn.3282478.
18. Consumer Protection Outlook 2020. [online] Available at: https://www.centralbank.ie/news/article/press-release-consumer-protection-outlook-9-march-2020 [Accessed 27 Jun. 2024]
19. Cyber Readiness | Hiscox Ireland. [online] Available at: https://www.hiscox.ie/cyber-readiness#:~:text=Key%20findings%20from%20the%20Cyber [Accessed 2 Jul. 2024]

20. Dapp, T. and Slomka, L. (2014). Current Issues Digital economy and structural change. [online] Available at: https://www.finextra.com/finextra-downloads/featuredocs/prod0000000000345837.pdf. [Accessed 20 Aug. 2024.]
21. Deloitte (2023). How Artificial Intelligence Is Transforming the Financial Services Industry. [online] www.deloitte.com. Available at: https://www.deloitte.com/ng/en/services/risk-advisory/services/how-artificial-intelligence-is-transforming-the-financial-services-industry.html.
22. Europa.eu. (2023). Available at: https://www.eba.europa.eu/guidelines-ict-and-security-risk-management. [Accessed 29 May 2024].
23. fionamurphy (2024). Fraudsters stole almost €100m in 2023 as holiday makers warned to be extra vigilant. [online] FraudSMART. Available at: https://www.fraudsmart.ie/2024/05/30/fraudsters-stole-almost-100m-holiday-makers-warned-to-be-extra-vigilant/ [Accessed 1 Jul. 2024].
24. Fraud And Financial Crime | permanent tsb. [online] Available at: https://www.ptsb.ie/help-and-support/help-with-banking/fraud-and-financial-crime/[Accessed 27 Jun. 2024].
25. FraudSMART. (n.d.). Alerts. [online] Available at: https://www.fraudsmart.ie/alerts/ [Accessed 23 Jun. 2024].
26. Fraudster Tactics - Bank of Ireland Group Website. [online] Available at: https://www.bankofireland.com/security-zone/fraudster-tactics/ [Accessed 22 Jun. 2024].
27. Gannon, M.J., Taheri, B. and Azer, J. (2022), "Contemporary Research Paradigms and Philosophies", Okumus, F., Rasoolimanesh, S.M. and Jahani, S. (Ed.) Contemporary Research Methods in Hospitality and Tourism, Emerald Publishing Limited, Leeds, pp. 5-19.
28. Garda. (n.d.). What are the 6 most common types of fraud in Ireland today and how to avoid becoming a victim? [online] Available at: https://www.garda.ie/en/crime/fraud/what-are-the-6-most-common-types-of-fraud-in-ireland-today-and-how-to-avoid-becoming-a-victim-.html.
29. GFLEC (2015). S&P Global FinLit Survey | Global Financial Literacy Excellence Center (GFLEC). [online] Global Financial Literacy Excellence Center (GFLEC). Available at: https://gflec.org/initiatives/sp-global-finlit-survey/.[Accessed 22 Jun. 2024].
30. gov.ie /finance, P. by the B.D.D. of F. (2023). Financial Literacy in Ireland Evidence Base for a National Strategy.
31. Irish Payments Services Organisation (IPSO), 2019. Annual Report 2019. [online] Available at: https://www.ipso.ie/reports/annual-report-2019.pdf [Accessed 28 May 2024].
32. Karamchand Gandhi, V. (2012). An Overview Study on Cyber crimes in Internet. [online] 2(1). Available at: https://core.ac.uk/download/pdf/234676934.pdf.Ghosh & Sultan, 2012. The impact of customer education programs on online fraud. [Accessed 14 Jun. 2024].

33. Klapper, L., Lusardi, A. and Van Oudheusden, P. (2015). Financial Literacy Around the World: INSIGHTS FROM THE STANDARD & POOR'S RATINGS SERVICES GLOBAL FINANCIAL LITERACY SURVEY. [online] Available at: https://gflec.org/wp-content/uploads/2015/11/3313-Finlit_Report_FINAL-5.11.16.pdf.[Accessed 22 Jun. 2024].
34. Kremling, J. and Sharp, A.M. (2018). Cyberspace, cybersecurity, and cybercrime.
35. Lapuh Bele, J., Dimc, M., Rozman, D. and Sladoje, A. (2014). RAISING AWARENESS OF CYBERCRIME -THE USE OF EDUCATION AS A MEANS OF PREVENTION AND PROTECTION. [online] Available at: https://files.eric.ed.gov/fulltext/ED557216.pdf. [Accessed 02 Jun. 2024].
36. Lusardi, A. & Mitchell, O. S., 2014. The Economic Importance of Financial Literacy: Theory and Evidence. Journal of Economic Literature, 52(1), pp. 5-44. doi:10.1257/jel.52.1.5
37. Maimon D., Louderback E.R (2019). Cyber-dependent crimes: an Interdisciplinary review-Annual Review of Criminology. pp.2:191-21
38. Mid-Term Review. (2019). Available at: https://assets.gov.ie/261971/356d743c-b154-4a5f-b7ae-eb6714c2d011.pdf.
39. Mike Harris and Howard Shortt (2022). The Cost of Cybercrime 2022. [online] www.grantthornton.ie. Available at: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---cost-of-cybercrime-2022.pdf.
40. Nir Kshetri and Springerlink (Online Service (2010). The Global Cybercrime Industry : Economic, Institutional and Strategic Perspectives. Berlin, Heidelberg: Springer Berlin Heidelberg.
41. Onwuegbuzie, Anthony J. "Why can't we all get along? Towards a framework for unifying research paradigms." Education, vol. 122, no. 3, spring 2002, pp. 518+. Gale Academic OneFile. Available at https://gale.com/apps/doc/A87691062/AONE?u=anon~e2da0be0&sid=googleScholar&xid=e507e509. [Accessed 12 Aug. 2024.]
42. Protect Your Kids Online - Help | permanent tsb. [online] Available at: https://www.ptsb.ie/help-and-support/help-with-banking/fraud-and-financial-crime/protect-your-kids-online/ [Accessed 28 Jun. 2024]
43. Rasmus, Gerlings, J. and Ferwerda, J. (2024). Do Awareness Campaigns Reduce Financial Fraud? European Journal on Criminal Policy and Research. doi:https://doi.org/10.1007/s10610-024-09573-1.

44. REFLECTING IRELAND - FINANCIAL FRAUD. [online] Available at: https://www.behaviourwise.ie/reflecting-ireland-financial-fraud [Accessed 27 Jun. 2024].

45. Report finds low financial literacy levels in Ireland. (2024). www.rte.ie. [online] Available at: https://www.rte.ie/news/business/2024/0419/1444587-report-finds-low-financial-literacy-levels-in-ireland/ [Accessed 27 Jun. 2024].

46. Research Reports. [online] Available at: https://www.gov.ie/en/collection/29943-research-reports/?referrer=https://www.justice.ie/en/JELR/Cybercrime_-_Current_Threats_and_Responses.pdf/Files/Cybercrime_-_Current_Threats_and_Responses.pdf [Accessed 2 Jul. 2024]

47. Rutledge, S.L. (2010). Consumer Protection and Financial Literacy: Lessons from Nine Country Studies. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1619168. [Accessed 10 Jun. 2024].

48. Sarel, D. and Marmorstein, H. (2006). Addressing consumers' concerns about online security: A conceptual and empirical analysis of banks' actions. Journal of Financial Services Marketing, 11(2), pp.99–115. doi:https://doi.org/10.1057/palgrave.fsm.4760025. [Accessed 18 Aug. 2024.]

49. Saunders, M., Lewis, P. and Thornhill, A. (2019). Research Methods for Business students. 8th ed. New Delhi: Pearson.

50. Seána Cunningham (2014). 'Preventing Financial Crime in a Rapidly Changing Environment: a Regulator's View' - Remarks by Seána Cunningham, Director of Enforcement and Anti-Money Laundering, at European Anti-Financial Crime Summit. [online] Centralbank.ie. Available at: https://www.centralbank.ie/news/article/preventing-financial-crime-in-a-rapidly-changing-environment-a-regulator-s-view-remarks-by-se%C3%A1na-cunningham-director-of-enforcement-and-anti-money-laundering-at-european-anti-financial-crime-summit-25-may-2023 [Accessed 27 Jun. 2024].

51. Security Zone - Bank of Ireland Group Website. [online] Available at: https://www.bankofireland.com/security-zone/ [Accessed 23 Jun. 2024].

52. Smith, J., 2020. Effectiveness of Online Fraud Prevention Initiatives. International Journal of Cybersecurity, 12(4), pp. 22-35.

53. Stewart, J. (2001). Financial regulation in Ireland: Should the regulator be the Central Bank? Journal of Financial Regulation and Compliance, 9(1), pp.42–55. doi:https://doi.org/10.1108/eb025061.Frauds - https://www.garda.ie/en/crime/fraud/

54. Symantec.com. (2019). Internet Security Threat Report (ISTR) 2019 | Symantec. [online] Available at: https://www.symantec.com/security-center/threat-report.

55. The Economic Cost of Cybercrime. (2021). Available at: https://www.grantthornton.ie/globalassets/1.-member-firms/ireland/insights/publications/grant-thornton---the-economic-cost-of-cybercrime.pdf.
56. Walsh, E. (2023). 'World first' as Permanent TSB introduces new in-app feature targeting fraudsters. [online] Irish Examiner. Available at: https://www.irishexaminer.com/business/technology/arid-41246239.html [Accessed 27 Jun. 2024].
57. Warwick Ashford (2019). Financial services top cyber attack target. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/news/252467639/Financial-services-top-cyber-attack-target [Accessed 2 Jul. 2024]
58. Wenhu Du, Min Chen (2023). Too Much or less? the Effect of Financial Literacy on Resident Fraud Victimization. p.Volume 148.
59. Wilson, J.O.S., Panos, G.A. and Adcock, C. (2021). Financial Literacy and Responsible Finance in the FinTech Era: Capabilities and Challenges. Routledge.
60. Worldbank.org. (2020). Good Practices for Consumer Protection and Financial Literacy in Europe and Central Asia: A Diagnostic Tool. [online] Available at: https://documents1.worldbank.org/curated/en/519401468028499582/text/703420ESW0P1120008Oct080for0release.txt. [Accessed 22 Jun. 2024]