National College of Ireland

Are micro businesses secure as they move online? An assessment on the suitability of message based Chatbots for tailored content delivery.

MSc Research Project

Cyber Security

Martin Parsons

Student ID:19162031

School of Computing

National College of Ireland

Supervisor: Ross Spelman

National College of Ireland

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Martin Parsons

Student ID: 19162031

Programme: MSc in Cyber Security **Year:** 2022

Module: MSc Research Project

Supervisor: Ross Spelman

Submission Due Date: 15th August 2022

Project Title: Are micro businesses secure as they move online. An assessment on the suitability of message based Chatbots for tailored content delivery

Word Count: 5693 **Page Count:** 14

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Martin Parsons

Date: 5/8/22

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	☑
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☑
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. □	☑

Are micro businesses secure as they move online? An assessment on the suitability of message based Chatbots for tailored content delivery

Martin Parsons

Student ID: **19162031**

Abstract

My research shows that micro-businesses (MB) are not secure as they move online post Covid. It is not a lack of information causing this as there is plenty available online, the problem is how it is being delivered and the way people are accessing it.
Chatbots are gaining popularity across sectors. However, as a content delivery tool, it is still in its infancy. A survey was used to initially assess local micro-businesses vulnerability to cyber-attacks as more of them moved online post-Covid and their general cyber security risk. The research showed they required a solution that provides simple access to easy-to-understand, affordable cyber security information. Next, I focused on a common theme from the survey, a lack of "*easy-to-use information and training*" and proceeded to ascertain if there was a problem with current delivery methods. I selected the most common methods, searching the net, online courseware and then added a third option, a Chatbot for comparison purposes. Chatbots do not appear to have been used in this area even though it is a modern communication channel available on all mobile devices.
In-depth interviews were conducted with 6 of these businesspeople. Users interacted with 3 different content delivery methods for cyber security information relevant to them via a Chatbot, Website and a custom-built Moodle course, in order to ascertain user preferences for a particular delivery method. The research shows that Chatbots may have a future as low-cost, easy-to-use cyber security content delivery systems for micro businesses that lack resources and technical skills. These Chatbots are now affordable, easier to design than in the past and can be scaled quickly. Future research and direction on the full implementation of a Chatbot to serve the needs of micro-businesses for cyber security information and help in particular situations are discussed.

1 Introduction

More businesses are moving online and adopting new technologies every day. Research from the CSO shows this has increased since Covid 19 and the HSE ransomware attack [1] with one in five businesses reporting an increase in online sales [2] and a third of businesses increased their use of social media during the pandemic. More people are buying online now [3] and customers expect businesses to have some kind of online presence. This increases the risk of cyber-attack.
It's not just businesses with Websites that are in danger from cyber attacks. A business without a Website that does not trade online might think that cyber security does not affect them but if they have an email account or surf the web they are at risk. Think of a MB (1 to 10 employees) that has their accounts and or payroll on a computer connected to the internet.

If an employee clicks on a phishing email or visits a compromised Website the company could lose access to their accounts or payroll by way of a ransomware attack. The result of this is a major headache and cost to the business affected if they don't have the correct procedures in place, a data recovery plan and possible legal implications under GDPR (if sensitive customer or staff information is accessed by an attacker with fines of up to 4% of turnover)[4].
Other dangers may come in the form of losing access to social media accounts. If a business uses social media for advertising and for keeping customers up to date, losing access to them could cost them business and customers. Nearly all the research in these areas involves small and medium businesses making this an important area to research. Eurostat's latest security report in 2020 on ICT security excludes businesses with under 10 employees [5].
The latest available research shows that small businesses suffer from a lack of knowledge and awareness of how to protect themselves [6] and that small businesses should equip their employees with the necessary knowledge and tools to protect themselves and their business. While our quantitative survey confirmed these results [7] it also led me to look at the way cyber security content is being delivered to MBs. I started by looking into delivering custom content using Moodle (Appendix 1) but during testing, it became apparent that the delivery method we initially proposed was causing the user problems. I then started looking into Chatbots [8] for content delivery. They are already in use for customer service [9] and marketing but appear to be underutilized for content delivery and during my research, I found limited research examples of this delivery method for micro businesses.

2 Motivations

Having worked in a micro business for years and talking to local business people, I was concerned about the lack of cyber security awareness among these people. After looking at the available research it became clear that small and medium enterprises (SMEs) and their employees were not following best practices, this got me thinking about smaller micro businesses and if they were better or worse off with cyber security and why. My initial research showed that they were not secure and that some of the reasons for this were that they needed a solution that was affordable, available on demand, and simple to use with easy-to-understand content.
The first solution created was using Moodle (Appendix 1). This was hosted on Amazon web services and presented a user cyber security questions and then created custom content based on their answers. Since we were using agile design principles [10], I created a working demo early in the design process. It quickly became clear that my solution was adding to the problem and not solving it. People were not comfortable with Moodle for several reasons, something as simple as having to log in put people off. This led to a change of approach and further research into other methods for content delivery. There is a lot of talk lately about Chatbots and I wondered if they could be used to deliver content to micro businesses. Chatbots are artificial intelligence (AI) programs that can use machine learning (MA) to simulate a conversation with a user using natural languages via a messaging application or Website. Brandtzaeg and Folstad [11] noted that Chatbots could be used to get assistance or information about a task and how easy and convenient they are to use. With businesses finding it harder to source talent or not having funding to employ cyber security people a Chatbot could be used in a similar way, or on a smaller scale than large security operation centres use Chatbots (ChatOps) [12].
Looking at MB owners in Ireland, we find they have on average 3.1 employees and have been in business for 24.7 years [13]. With the average age of all early-stage entrepreneurs in Ireland being between 25 and 44 [14], I can work out from this that the age profile of MB

owners in Ireland is on average between 49 and 68. Studies have shown that older people are less likely to use a computer and know less about the internet than younger people [15].

This paper is going to ask two questions.
(1) Are Micro businesses in Castlebar secure as they move online?
(2) How can we deliver affordable and easy-to-use cyber security content to micro-business people in a form that they are comfortable with?

The layout of this paper starts with an up-to-date literature review followed by the research methodology used. Then the design will be discussed alongside the implementation of our solution. Finally, the results will be discussed in detail and future work looked at.

3 Related work

Since the start of Covid-19 more and more MBs have been moving online and using online services with help and funding from the likes of the local enterprise boards [16]. This brings with it risks as these businesses become targets for cybercriminals. Below we will look at the latest research involving MB and SMEs, where we find a lot of the research has common areas that are affecting businesses regarding cyber security. As mentioned earlier, research is limited on micro businesses, as shown in the ICT Security in Enterprise security report Eurostat (2020a) [17] that excluded businesses of 0-9 employees, highlighting this gap in research data regarding micro businesses. As a result, we will also utilize research on SMEs to augment our data where required.

3.1 Are micro businesses safe online?

Research shows that businesses are not safe online for several different reasons. Sukumar, A.P.C., Xu, Z., Satyanarayana, K & Tomlins, R [18] discuss how Micro/ Small businesses have different characteristics when compared to medium enterprises and are a target of cyber criminals using attacks such as Phishing, Viruses and Hacking. They used a qualitative enquiry for their research to look at the cyber risk management of micro and small businesses in the UK using semi-structured interviews. They found businesses do not understand the risk and even though there is lots of free information available it is not always easily understood or accessed of 19 people interviewed only 4 were aware of cyber security training and education programmes. Businesses believed they had nothing an attacker would want as it was ‘just pure information’. It also noted that policies used by the UK to create cyber threat awareness needed to be improved, while lack of cyber security training was also a concern. This paper didn't look at why these people didn't understand the risk and did not propose a technology solution outside of recommending a framework. Those findings were also backed up by Official Statistics Cyber Security Breaches Survey 2022 Published 30 March 2022 and one of the few other reports to include micro businesses that showed Micro businesses are a target [19]

3.2 We can see that micro businesses are a target but why?

Abdulmajeed Alahmari; Bob Duncan [20] in their paper ‘Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence Discussed using a systematic review method to collect 50 research papers, of which 15 articles were selected. They found as we did, that most of the research is focused on larger firms. It states

that most experts agree cybercrime is the biggest threat to any firm and that SMEs think they are not vulnerable because of their small size. They believe SMEs are more vulnerable because of weaker defences and less expertise. A lack of affordable solutions was also noted as a threat to these businesses and the supply chain, making it a priority for the UK government and the private sector. They concluded that there is a lack of knowledge and awareness about available solutions and that more research is needed in this area which we are researching here and proposing an affordable solution that will not require a high level of computer literacy to use.

A common theme that keeps appearing in the research is that businesses have a lack of knowledge and awareness regarding cyber security. Karen Renaud in 'How smaller businesses struggle with security advice' [21], looked at 110 Scottish SMEs and found they wanted advice and information but struggled with what was available. When SMEs were asked what could be done to help them they said they needed advice and information but that the sheer amount and volume of information is causing confusion and uncertainty. They concluded that what is needed is simple and easy-to-follow instruction and advice and that too many government agencies are offering advice based on their own experience which is confusing businesses but does not recommend what that solution should be.

The inability to gather data from micro businesses is a significant barrier to cyber-security research as found by Tracy Tam, Asha Rao &Joanne Hall in their paper 'The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses [22] and that unlike larger businesses micro ones may not even know they have been attacked. This can be due to a lack of technical skills or unavailability of data that would show an attack happened. Something like ransomware is obvious when it happens but not all attacks are like this such as if data has been stolen or a keylogger running on a machine. Their research showed again that a lack of knowledge and technical skills are stopping micro-businesses from protecting themselves but on the plus side these businesses are agile and can adapt quickly compared to larger ones and an effective method would be to teach them the skills needed to protect themselves. We wish to help in addressing these problems and gather additional data on micro businesses, to better understand the issues they are facing and propose a technology solution to address them.

The literature review has shown that SMEs are not protecting themselves from cyber-attack. There are limitations around the lack of research specifically on Micro businesses and the proposed solutions, I propose to fill this gap. More of these businesses are starting to use online services all the time such as email, online accounts, and banking to name a few. A common theme across all the research papers is a lack of knowledge and technical skill [6,19,20,21,22] as a reason for not having security in place while lots of smaller businesses do not believe they have anything worth attacking or stealing. These micro-businesses can be considered low-hanging fruit for attackers and if and when larger businesses become better protected, attackers will go for the easier target and this needs to be looked at specifically for micro businesses.

3.3 Chatbots

Looking at Chatbots we find research on them for content delivery is limited but a paper by Smutny & P. Schreiberova [23] from 2020 discusses the increased use by educators of instant messaging Chatbots for teaching and learning. They found that Chatbots for learning are still in the early stages but that 72% of users expressed their overall satisfaction with these Chatbots as a virtual tutor but they had a concern about the screen size this is a very high satisfaction and we want to look at this closer and see do micro business people feel the same.

Most papers we found were based on educators and their use in schools. We want to go further and look at Chatbots to deliver content to micro business people and believe this is a unique use for them compared to how big industry is using them on a much larger scale in SOC for example [24]. Bulin Shaqiri [26] built a prototype that allowed end-users to submit their requests for cybersecurity support, with the conversational agent then responding with accurate answers for 3 different types of attack and can gather all the necessary information from the user to possibly identify a potential attack.M. F. Franco et al. [27] discuss a cybersecurity-driven Chatbot for the support of cybersecurity planning and management and identify issues with the limited database for custom answers and how it becomes a lot more complex with the more flows added.
My goal is to create a new Chatbot designed especially for micro business with easy-to-use and understand content delivered in a form the user will be comfortable with.

4 Research Methodology

The research methodology consists of a survey and interviews using both quantitative and qualitative analysis, combining both should deliver significant benefits, enabling me to compare and contrast results and gain much deeper insights and ensuring the limitations of one method is balanced by the strength of the other.
A larger focus group would have been beneficial to gain more in-depth insights. There is scope for getting experimental data, but for this to be useful I would need more users to allow me to collect data through active engagement and run some experiments. The same applies to using something like R-studio which would work better with a bigger data set.
After the data was collected it was cleaned and processed to give us the results discussed below.

4.1 Sample composition

To conduct the initial survey the local chamber of commerce was contacted, and they agreed to help me on the condition I give a talk on cyber security at one of their events (Appendix 2). I demoed the Moodle solution at the event and they agreed to send out the survey to their email list of approximately 500 people. It was also posted on their Instagram and Facebook channels (Appendix 3). The people interviewed were all business people in Castlebar both male and female over the age of 18. This talk allowed me to demo the Moodle solution early in the development process which allowed me to change direction after collecting observational data on its usage. Some of the participants for the Moodle demo also agreed to in-depth interviews to assess the delivery solutions of a Chatbot.

4.2 Interviews and Survey

The study was approved by Ross Spelman of the National College of Ireland, 6 people answered the survey posted by the local Chamber of Commerce, and the rest I got by telephone and in person. All participants signed a consent form before the survey and interview.
The interviews were conducted in person with the same questions asked to each person. During the interview, the participants were presented with a custom-built Chatbot, access to a European agency Website for cyber security [28] and a Moodle course (Appendix 1) that I had also created designed to deliver custom cyber security content based on a user's answers to a specific set of questions. The aim was to gather information about the perception and use

of the Chatbot versus the other delivery methods for cyber security content. After the participants were finished interacting with each platform the interviews started. Some interviewees did not wish to have the audio of the interview recorded, so it was decided to transcribe them as they were being done.

4.3 Survey and interview Development

The survey consisted of 20 questions, based on best practices from around the world. Using cyber security guides from government agencies in Europe [28], the UK [29] and the USA [30] I came up with the commonly recommended best practice. The interviews were performed in person with data transcribed to a google form and then exported to Google sheets for analysis. A total of 54 questions were asked based on the 3 different platforms with 26 questions assigned a numeric rating from 1 to5. The chart below indicates that all 3 agencies concur on backing up data, keeping software updated, using strong passwords and two-factor authentication where possible and having protection against malware.

NIST	Back up Data	Passwords, MFA	Malware protection	Encrypt Devices	Train Staff	Incident response	
ENISA	Back up Data	Passwords, MFA	Malware protection	Incident response	Encryption	Physical security	Use the Cloud
NCSC	Back up Data	Passwords, MFA	Malware protection	Mobile Security	Avoid Phishing		

Table 1: Cyber Security Best Practice

4.4 Data Analysis

The survey was created using Google forms. After the last survey was completed the data was exported to Google sheets formatted and cleaned to filter and remove unwanted data and to check for any errors.
After the last interview was finished the data was cleaned up as some words did not export correctly to Google sheets. Sentiment analysis was performed manually by creating tags for keywords such as easy, simple etc [31]. Next semantic analysis was performed to ascertain a feeling of what the users were saying [32]. This method of analysing data can be slow to do manually and does not scale. As a result the next time we would utilise machine learning software such as [33]. The most relevant results are presented in the tables below along with semantic word clouds [34] to allow us to quickly visualize the results.

5 Design Specifications

After researching several Chatbots it was decided to go with Chatbot.com as it had Facebook messenger integration out of the box. Other Chatbots tested were Manychat [35], Botstar [36]

and Chative [37]. Botstar was originally the preferred platform but is closing down in late 2022.
To build the Chatbot I created an account with Chatbot.com, which allows integration with several popular online services. I set up a Facebook page to link to the Chatbot and then created a dedicated Gmail account to use google sheets to import and export data from the Chatbot using the zapier API. The Chatbot also possesses natural language processing, artificial intelligence (AI) and machine learning to understand users' input better as shown below.

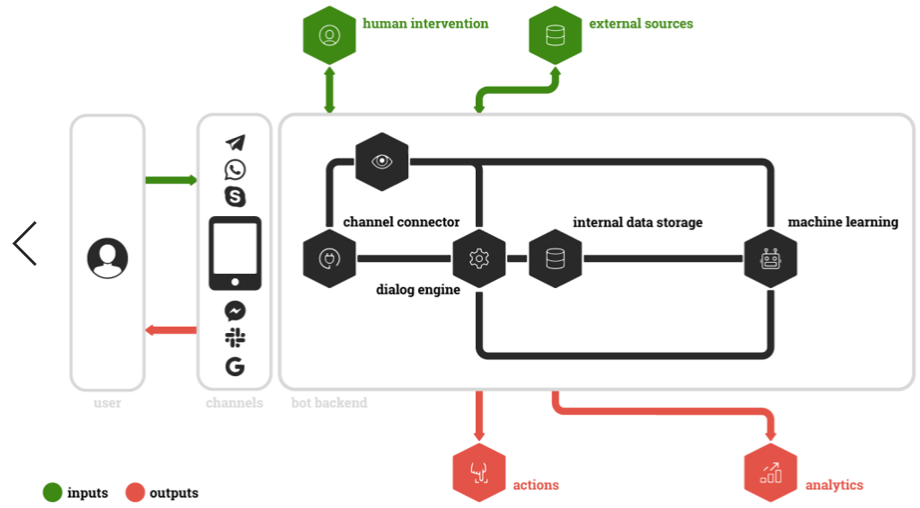


Figure 1: Chatbot Architecture

The Chatbot uses a drag-and-drop visual builder that allows conversation blocks to be used for building stories. A choice of multiple bot response formats and actions are available to design an engaging experience. There is a fallback function in case of miscommunication with the Chatbot to avoid user problems.

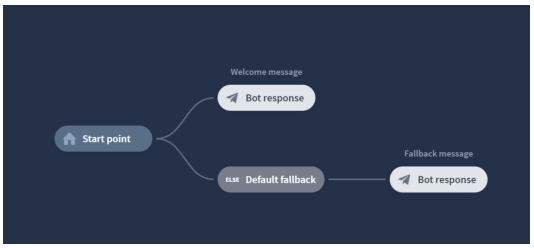


Figure 2: Drag and drop conversation blocks

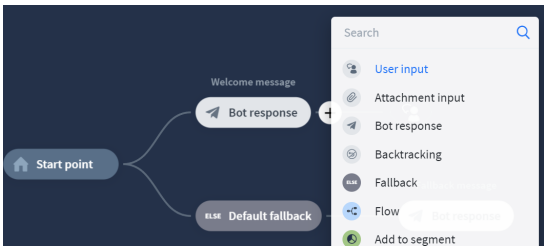


Figure 3: Formats and actions

The Chatbot allows for the gathering of user data via attributes which can be used to customise the Chatbot conversation, these can be created by the developer or default ones used. Buttons can be used so a user doesn't need to type, making for faster navigation and fewer problems with the Chatbot not understanding what a user wants. Images can be added as can links to external content. Filters can be applied to match bot replies within the context

of the conversation. Questions can be used to collect user data or to validate a user. Users can be organised into different segments while allowing the information to be reused in marketing activities. Flows are used to design separate paths or can be set up for AB testing by splitting users into different flows allowing us to test which flows perform best. This testing can be done as the Chatbot is being built from within the Chatbot web app. Redirects are used to keep a conversation moving by redirecting a user to another part of a story by using a go-to step function.

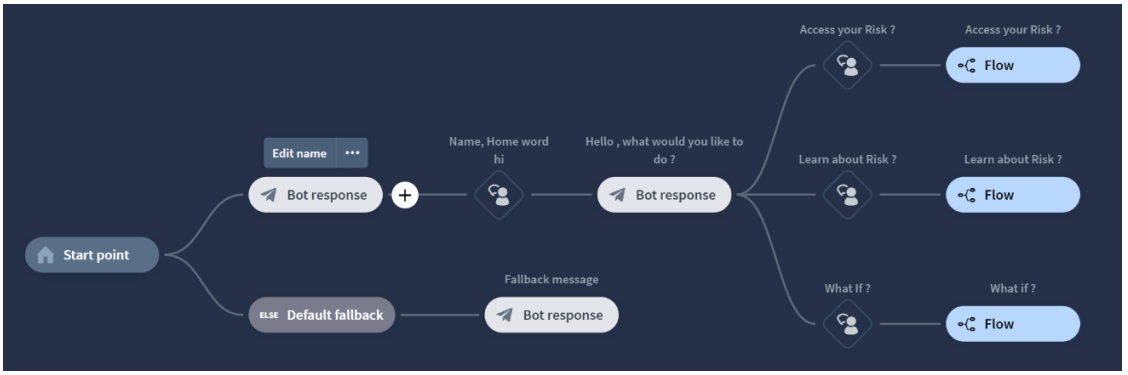


Figure 4: Flows

When the Chatbot is ready to launch there is a selection of customizable widgets for integration with the Website or messaging apps such as messenger or WhatsApp. Webhook are available to allow for communication between the Chatbot and web services using PHP or Node.js and it comes with a selection of tools to analyse data such as heatmaps and track the total number of chats with users and review the most popular interactions.

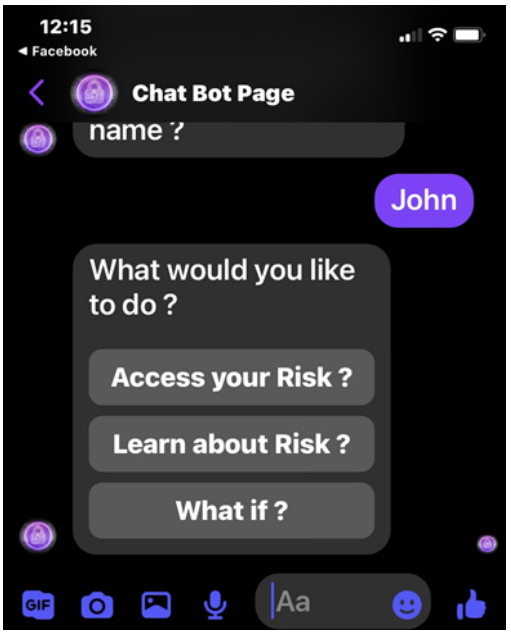


Figure 5: Facebook Messenger

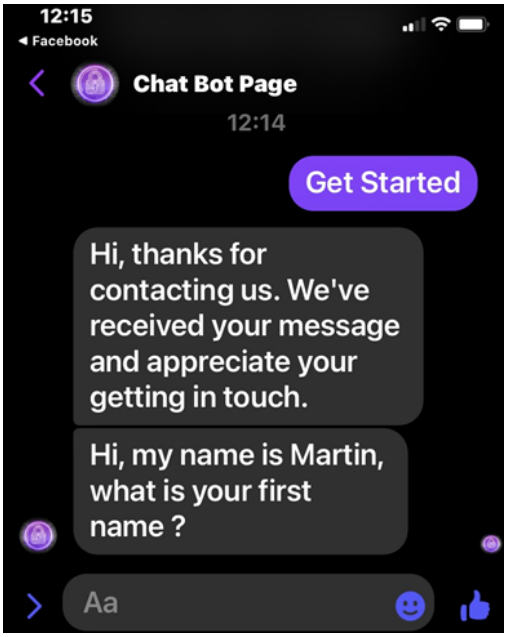


Figure 6: Facebook Messenger

5.1 Implementation

The solution created a cybersecurity delivery method that is affordable to micro-business people that they are comfortable using. This was achieved by creating a Chatbot that can be used with Facebook messenger. The Chatbot allows a user to assess their cyber security risk by asking a series of questions with the risk determined at the end. A user can also learn about cybersecurity risks by following step-by-step instructions or via a video. Finally, they can find out what to do if something happens such as a ransomware attack. These use a decision tree to determine what course of action is required. The goal of the Chatbot is to create a user-friendly and uncomplicated way to deliver cyber security content.

5.2 Software Development Methodology

The methodology used to develop this project was the agile model. This model provides a framework that allows me to adapt to changes and encourages getting working software early in the process. This turned out to be a very important choice as it allowed me to demo the Moodle solution early and then pivot to provide an alternative delivery method via a Chatbot.

5.3 Security

The Chatbot uses AES 256-bit encryption for data and backup storage and HTTPS to securely transmit user data during a chat. Messenger uses end-to-end encryption. Chatbot.com is GDPR compliant and stores its user's data in IBM European data centres.

6 Evaluation

In this section we will answer the two research questions. The findings from the first question are displayed in charts while the findings from the second question are displayed in tables using quotes as a typical answer for each category followed by semantic and semantic analysis. I used a standard rating scheme to analyse certain questions in the interview that had a rating from 1 to 5.

6.1 Research question 1

Are micro businesses secure as they move online?
It appears MB are not secure as they move online and when we compare our results with the tipping point report on SMBs in Ireland from 2022 [40], one of the few studies looking at MBs. We found that 61% were worried about cyber security while the report found that 75% were worried about a cyber attack on their business. The tipping point found only 11% of businesses use 2FA while our research found that 94% know about it and 50% use it.

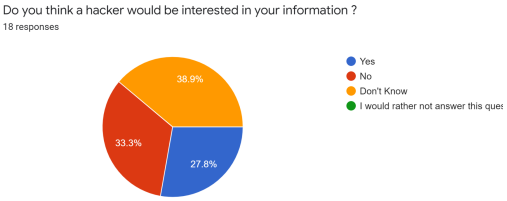


Chart 1: Do you think a hacker would be interested in your information?

"33% said they had no data an attacker would be interested in and 39% did not know if they had any information an attacker would be interested in."

Chart 2: Do you use a computer for your business or payroll?

"Of concern is that 100% of businesses that completed our survey say they use their computer for payroll or accounts while thinking this data would be of no interest to an attacker"

My research also shows that 67% of MBs know how to back up their data and but only 56% actually back it up. It also shows the reason for not being more secure follows a similar theme to what we discovered in our literature review-MB owners do not know how to do the right things due to a lack of technical skill and a lack of easy-to-understand information on how to perform these basic tasks. 35% of users lack information on how to protect themselves while 65% lack technical skills. The reasons given for this were 61% found a lack of easy-to-understand information while 56% also stated a lack of easy-to-understand training was the problem.

These are the same problems we find in the UK which is one of the only other places to report on MB where they say ' smaller organisations took little proactive action on cyber security, driven by a lack of internal knowledge, they often had a fear of the technicalities of cyber security, the huge range of and diversity of material and no agreed information source [19].

The data confirm that there is a problem with current solutions to help secure micro businesses online and are not fit for purpose. This is where a new delivery method may be the answer which Question 2 will take a closer look at.

Next, I focused on the common theme from the survey, a lack of "easy-to-use information and training" and proceeded to ascertain if there was a problem with current delivery methods. I selected the most common methods, searching the net and online courseware and added a third option, a Chatbot for comparison purposes. Chatbots do not appear to have been used in this area even though it is a modern communication channel available on all mobile devices.

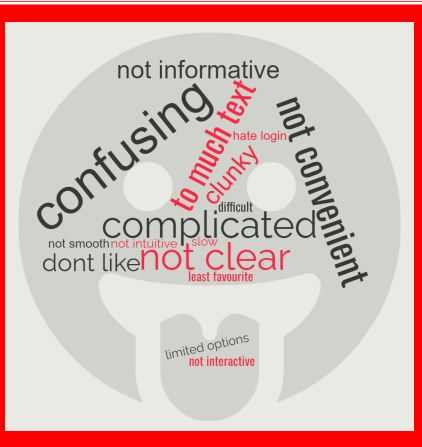
6.2 Research question 2

How can we deliver affordable and easy-to-use cyber security content to micro-business people in a form that they are comfortable with?

In our sample, we conducted 6 in-depth interviews with local micro-business owners.

The interviews asked people 62 questions about their opinions on Moodle (Appendix 1), a Website [28] and a Chatbot for delivering cyber security content. Overall the respondents preferred the Chatbot with statements like ' simple, easy, straight forward, it's like talking to someone, I can check it on my phone which is instant, and these days if I am looking for a quick fix of information it comes from my mobile first'.

Semantic word cloud feedback results

Positive Feedback	Negative Feedback
	
Figure 7: Chatbot positive feedback	**Figure 8: Chatbot negative feedback**
	
Figure 9: Moodle positive feedback	**Figure 10: Moodle negative feedback**
	
Figure 11: Website positive feedback	**Figure 12: Website negative feedback**

We can see in table 2 while everyone was positive about the Chatbot only 2 people were positive about Moodle and the Website. People found the Chabot smoother to use than the other platforms. After analysing all the interviews it is apparent people prefer the Chatbot. In my opinion the reason people prefer the delivery method of the Chatbot is that it is familiar to them and is easier to use than the other options.
Viewing this data by using a word cloud as shown in figures 7-12, highlighting the words used most commonly using word frequency and relevant analysis. This data was collected after doing semantic and sentiment analysis to give us an idea of the general feeling the users have towards each of the options. Finally, we analysed data about each option which was rated from 1 to 5 based on their experience using it. We applied a standard rating scheme to this data. We found the Chatbot was the preferred delivery method by a margin of 2 to 1 as seen in chart 3 below.

	Chatbot	Moodle	Website
Why would you use it for getting cyber security information?	N=6 'I would use it because it is easy to get answers' (Q1, R2) 'Chatbot is easy to use' (Q1, R4)	N=2 'Moodle is fine for content delivery' (Q2, R4) 'Suitable for obtaining full picture in an organised fashion (Q2, R5)	N=2 'Plenty of useful information provided' (Q3, R5)
Why would you not use it for getting cyber security information?	N=0	N=4 'I don't think it is a suitable platform for users. Especially for older person' (Q2, R2)	N=4 'It doesn't tell you how to actually do it, it just provides information about what needs to be done for securing businesses' (Q3, R2)
What made it smooth?	N=5 'it's like asking someone a question and you get the answer' (Q10, R1) 'Speed was good, short answers' (Q10, R5)	N=2 'Easy to use with a quick response' (Q11, R1)	N=2 'Proven tech, familiar layout and process' (Q12, R5) 'It's a straight download. I just then read it' (Q12, R6)
What made it not smooth?	N=1 'You had to follow the a b paths the chatbot suggested, so choice was limited' (Q10, R3)	N=4 'a little sluggish and login etc takes time' (Q11, R5) 'Moodle is a bit clunky' (Q11, R6)	N=4 'I just couldn't find the solutions I was looking for' (Q12, R1) 'Not as smooth as the chatbot' (Q12, R4)

Table 2: Interview Analysis

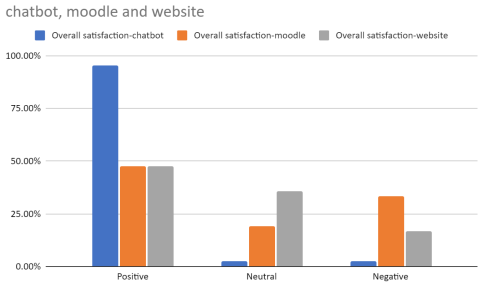


Chart 3: Overall Satisfaction

"When we grouped all the data we found the Chatbot was preferred to the other methods by a margin of 2 to 1 and that almost 100% of users were satisfied with the Chatbot vs only 50% satisfaction with the other platforms"

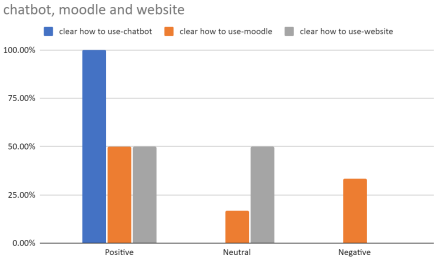


Chart 4: Clear How To Use

"People interviewed found the Chatbot clearer to use than the other platforms. 100% of Chatbot users said it was clear how to use Vs. 50% found the Website and Moodle clear. 30% found Moodle very unclear Vs 50% were neutral on how clear the Website was to use."

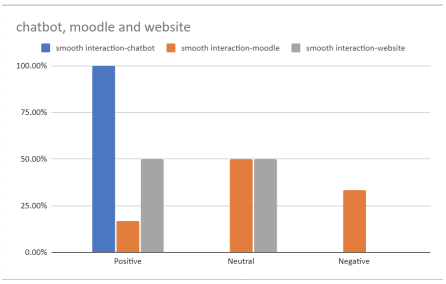


Chart 5: Smooth Interaction

"Users found the Chatbot smoother to interact with than the other platforms with 100% finding the Chatbot a smoother interaction. Only 20% found Moodle smooth with 50% finding the Website smooth."

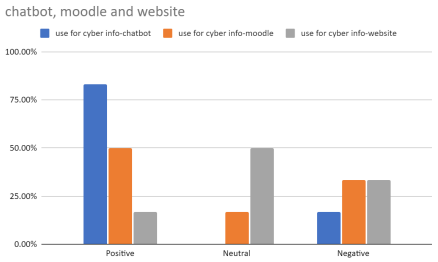


Chart 6: Use For Cyber Security Information

"80% said they would use a Chatbot for getting cyber security information while 50% for Moodle, and 20% would use a Website."

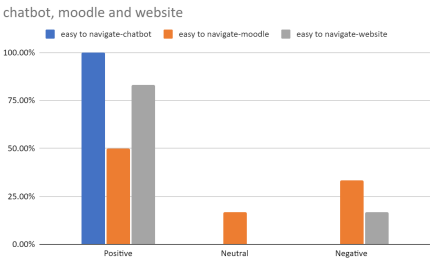


Chart 7: Easy To Navigate

"People found the Chatbot easy to navigate with 100% agreeing it was. As expected, people found the Website easy to navigate with an 80% rating. This falls to 50% of people finding Moodle easy to navigate."

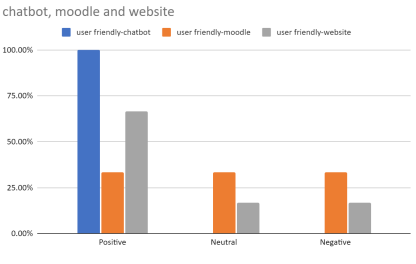


Chart 8: User-Friendly

"Chatbot was the most user-friendly of the platforms. 100% of people found the Chatbot to be user-friendly as opposed to a 70% rating for Website and 30% for Moodle. Only 20% of participants didn't find the Website user-friendly."

7 Conclusion and Future Work

After critically analysing all the data I found that micro businesses are not secure as they move online and they require a solution to give them simple access to easy-to-understand, affordable cyber security information. Looking at the chatbot data, there was an instant liking for it, users found it easy to use, friendly and convenient. They found the Website confusing with too much text, not convenient and clunky, but some people did like how it was familiar and straightforward to use. The users also didn't like Moodle as much as the Chatbot with comments such as not convenient, slow, complicated, and confusing and several users did not like having to log in to use Moodle. Some Moodle users did find it intuitive, fast and familiar but overall we can see from the results that people preferred the Chatbot. I believe the research also shows that Chatbots have a future as low-cost, easy-to-use cyber security content delivery systems for micro businesses that may lack resources and technical skills. These Chatbots are now affordable, easier to design than in the past and can be scaled quickly and can be used to deliver cybersecurity content to micro businesses and the research has shown this.

The local chamber of commerce has shown an interest in testing a more complete Chatbot in the future, further showing me the potential for this. I plan on approaching the local enterprise board about building a Chatbot for use with the micro businesses they support with funding to go online. There is also funding and mentorship available through the ATU new frontiers program [41] that I may look at to help me develop this idea further. I believe this would be of great benefit to everyone involved.

In my opinion, future research should include looking at how this Chatbot could be used for incident response in micro-businesses or SMEs. This was not examined closely while testing but could be an interesting and practical new use for the Chatbot. This could prove effective if a business were the victim of ransomware or any other cyber attack where their computer is unusable by giving them a step-by-step guide to responding to it via their phone. Another area I would like to look closer at is Chatbots and younger people. The Mayo campus of ATU is located in my town (where I conducted the study) and has 1,000 students in attendance, which would be beneficial to future research. Firstly to assess if they like using it and then to see what uses they may have for it. Uses could include, what to do if one thinks they have an STD or have been victims of sexual assault. These are areas students may find it difficult to talk to people about and a Chatbot may be a good starting point for directing them towards the best course of action to take.

The limitations of this research included the difficulty of finding research papers about micro-business and getting people to take part in the survey and interview. I was surprised initially that the survey got so few responses after being sent and seen by so many people. In retrospect, it reinforced that the target group reacted similarly to the online form as they did to similar content delivery methods in the more detailed study.

I have noticed since starting this research that there are now a few more reports being released on micro business showing that it is a growing area of research.

If I was doing this project again I would use machine learning software to analyse the interviews as it took a long time to do this manually. I would also look into using the Chatbot (as it appears to be the prefered content delivery method) for doing the surveys and interviews as this would simplify everything and allow me to test and develop the Chatbot at the same time.

References

1. Corfield, G., n.d. Hospitals cancel outpatient appointments as Irish health service struck by ransomware [WWW Document]. URL https://www.theregister.com/2021/05/14/ireland_hse_ransomware_hospital_conti_wizardspider/
2. Information Society Statistics Enterprises 2021 - CSO - Central Statistics Office [WWW Document], n.d. URL https://www.cso.ie/en/releasesandpublications/ep/p-isse/informationsocietystatisticsenterprises2021/
3. Most consumers expect to keep shopping online after pandemic – The Irish Times [WWW Document], n.d. URL https://www.irishtimes.com/business/retail-and-services/most-consumers-expect-to-keep-shopping-online-after-pandemic-1.4584382
4. Meier, S., n.d. Fines / Penalties. General Data Protection Regulation (GDPR). URL https://gdpr-info.eu/issues/fines-penalties/
5. ICT security in enterprises [WWW Document], n.d. URL https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises
6. Alahmari, A., Duncan, B., 2020. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence, in: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). Presented at the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638
7. Ncubukezi, T., Mwansa, L., Rocaries, F., 2020. A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses, in: 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST). Presented at the 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 1–6. https://doi.org/10.23919/ICITST51030.2020.9351339
8. Araujo, T., 2018. Living up to the Chatbot hype: The influence of anthropomorphic design cues and communicative agency framing on conversational agent and company perceptions. Computers in Human Behavior 85, 183–189. https://doi.org/10.1016/j.chb.2018.03.051
9. Andrade, I.M.D., Tumelero, C., 2022. Increasing customer service efficiency through artificial intelligence Chatbot. Revista de Gestão 29, 238–251. https://doi.org/10.1108/REGE-07-2021-0120
10. 12 Principles Behind the Agile Manifesto | Agile Alliance, 2015. . Agile Alliance |. URL https://www.agilealliance.org/agile101/12-principles-behind-the-agile-manifesto/
11. Brandtzaeg, P., Følstad, A., 2017. Why People Use Chatbots. https://doi.org/10.1007/978-3-319-70284-1_30
12. Perera, V.H., Senarathne, A.N., Rupasinghe, L., 2019. Intelligent SOC Chatbot for Security Operation Center, in: 2019 International Conference on Advancements in Computing (ICAC). Presented at the 2019 International Conference on Advancements in Computing (ICAC), pp. 340–345. https://doi.org/10.1109/ICAC49085.2019.9103388
13. Bourke, D.J., Roper, S., n.d. Micro-Businesses in Ireland: From Ambition to Innovation

39.https://www.ucc.ie/en/media/projectsandcentres/srerc/Micro-BusinessinIrelandReporte-version.pdf
14. Fitzsimons, P., O'Gorman, C., 2018. A SURVEY OF ENTREPRENEURSHIP IN IRELAND https://www.enterprise-ireland.com/en/Publications/Reports-Published-Strategies/GEM-Reports/2018-Global-Entrepreneurship-Monitor-Report.pdf
15. Grimes, G.A., Hough, M.G., Mazur, E., Signorella, M.L., 2010. Older Adults' Knowledge of Internet Hazards. Educational Gerontology 36, 173–192. https://doi.org/10.1080/03601270903183065
16. Carmel, M., n.d. Trading Online Voucher Scheme [WWW Document]. URL https://www.localenterprise.ie/Discover-Business-Supports/Trading-Online-Voucher-Scheme/
17. Database - Digital economy and society - Eurostat [WWW Document], n.d. URL https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database
18. Sukumar, A.P.C., Xu, Z., Satyanarayana, K., Tomlins, R., 2019. An exploration of cyber-security risk management in small businesses: The case UK Micro and Small firms: Institute for Small Business and Entrepreneurship. ISBE 2019 Conference Proceedings.
19. Cyber Security Breaches Survey 2022 [WWW Document], n.d. . GOV.UK. URL https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
20. Alahmari, A., Duncan, B., 2020. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. pp. 1–5. URL https://ieeexplore.ieee.org/document/9139638
21. Renaud, K., 2016. How smaller businesses struggle with security advice. Computer Fraud & Security 2016, 10–18. https://doi.org/10.1016/S1361-3723(16)30062-8
22. Tam, T., Rao, A., Hall, J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. Comput. Secur. 109. https://doi.org/10.1016/j.cose.2021.102385
23. Smutny, P., Schreiberova, P., 2020. Chatbots for learning: A review of educational Chatbots for the Facebook Messenger. Computers & Education 151, 103862. https://doi.org/10.1016/j.compedu.2020.103862
24. Perera, V.H., Senarathne, A.N., Rupasinghe, L., 2019. Intelligent SOC Chatbot for Security Operation Center, in: 2019 International Conference on Advancements in Computing (ICAC). pp. 340–345. https://doi.org/10.1109/ICAC49085.2019.9103388
25. Interacting with educational Chatbots: A systematic review | SpringerLink [WWW Document], n.d. URL https://link.springer.com/article/10.1007/s10639-022-11177-3
26. Bulin Shaqiri, 2021, Development and Refinement of a Chatbot for Cybersecurity Support, University of Zurich, https://files.ifi.uzh.ch/CSG/staff/franco/extern/theses/BA-B-Shaqiri.pdf
27. Franco, M.F., Rodrigues, B., Scheid, E.J., Jacobs, A., Killer, C., Granville, L.Z., Stiller, B., 2020. SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management, in: 2020 16th International Conference on Network and Service Management (CNSM). pp. 1–7. https://doi.org/10.23919/CNSM50824.2020.9269037
28. Cybersecurity guide for SMEs - 12 steps to securing your business [WWW Document], n.d. . ENISA. URL https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

29. Small Business Guide: Cyber Security [WWW Document], n.d. URL https://www.ncsc.gov.uk/collection/small-business-guide All Purpose Guides, 2020. . NIST.
30. All Purpose Guides, small business cybersecurity 2020. NIST. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/all-purpose-guides
31. Sentiment Analysis Guide [WWW Document], n.d. . MonkeyLearn. URL https://monkeylearn.com/sentiment-analysis/
32. Semantic Analysis, Explained [WWW Document], 2020. . MonkeyLearn Blog. URL https://monkeylearn.com/blog/semantic-analysis/
33. Free Online Sentiment Analysis Tool [WWW Document], n.d. . MonkeyLearn. URL https://monkeylearn.com/sentiment-analysis-online/
34. Tag cloud, 2022. Wikipedia. https://en.wikipedia.org/wiki/Tag_cloud
35. ManyChat.Com [WWW Document], n.d. URL https://manychat.com/login?return=%2Ffb105109802201579%2Fdashboard
36. BotStar, n.d. BotStar | Engage Customers Online with Live Chat & Chatbots [WWW Document]. URL https://botstar.com/
37. Chative, n.d. Chative | Engage Customers Online with Live Chat & Chatbots [WWW Document]. URL https://chative.io/
38. Gonda, D.E., Luo, J., Wong, Y.-L., Lei, C.-U., 2018. Evaluation of Developing Educational Chatbots Based on the Seven Principles for Good Teaching, in: 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). pp. 446–453. https://doi.org/10.1109/TALE.2018.8615175
39. Buttons - Menus and actions - Components - Human Interface Guidelines - Design - Apple Developer [WWW Document], n.d. URL https://developer.apple.com/design/human-interface-guidelines/components/menus-and-actions/buttons/
40. .IE Tipping Point Report 2022 [WWW Document], n.d. URL https://www.weare.ie/TippingPoint2022/
41. Atlantic Technological University (ATU) - Galway City + Mayo Campuses, n.d. . New Frontiers programme. URL https://www.newfrontiers.ie/locations/galway-mayo

Appendices

1. Moodle running on AWS

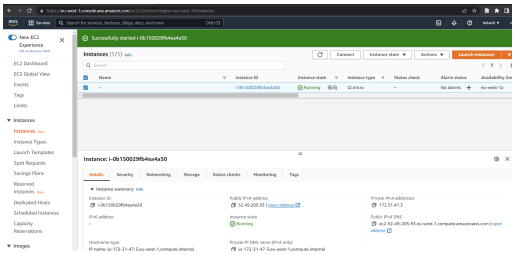


Figure 1: Moodle running on EC2 instance in AWS

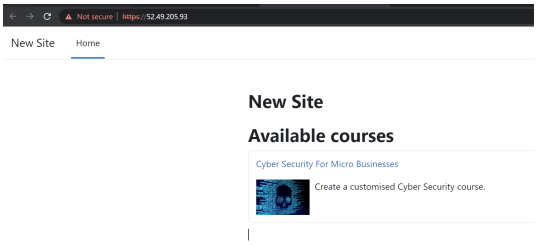


Figure 2: Moodle home page

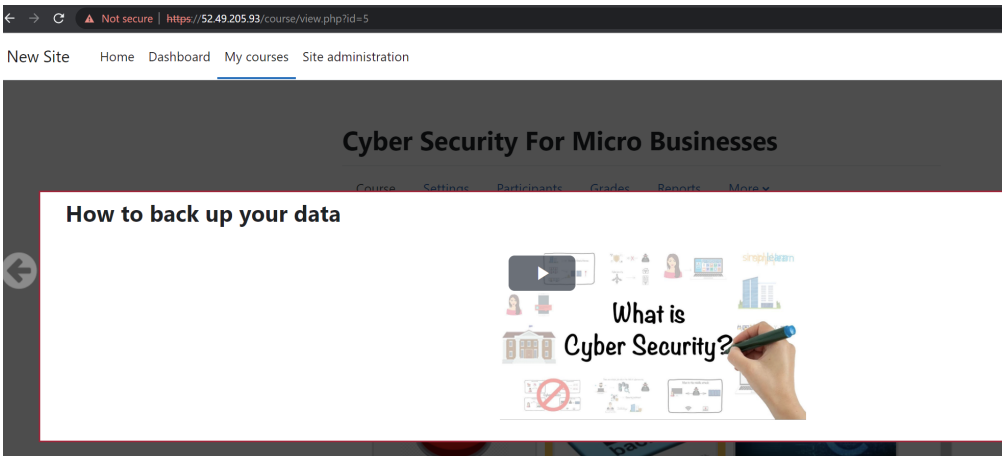


Figure 5: Moodle example of video content

Figure 3: Moodle with each part of the course open

2. **Invite to the cyber security talk with the chamber of commerce in conjunction with Mayo Sligo Leitrim training board (MSLETB)**

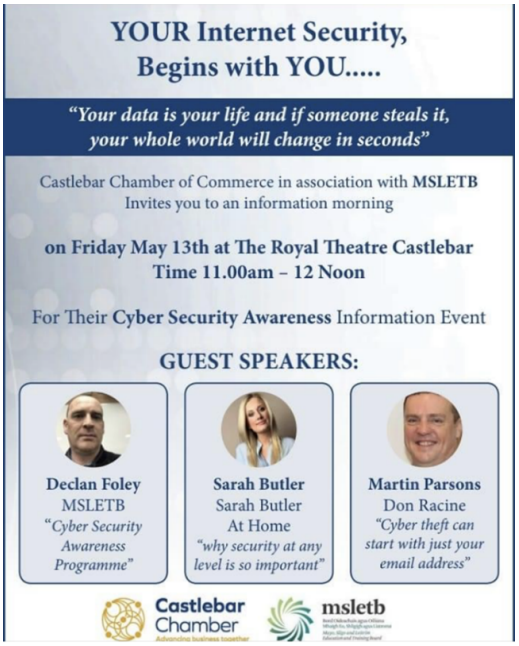


Figure 5: Advertisement from newspaper and online about cyber security talk

3. **Facebook/ Instagram invitation for a survey sent out by the chamber of commerce.**

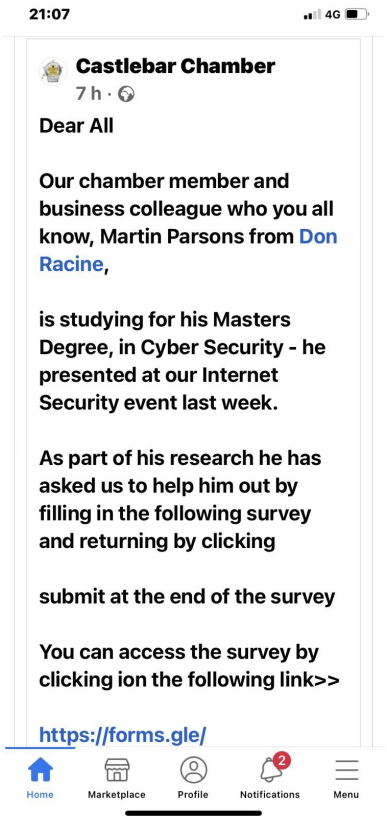


Figure 6: Facebook survey invite

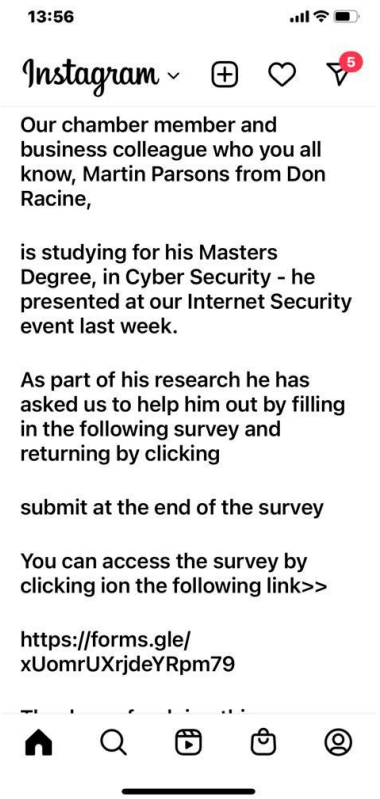


Figure 7: Instagram survey invite