

CAT 4 RESOURCE DEVELOPMENT

Group 4-043

Let's Catch the Phish!

Puay Keane Yu 3A2 (18)

Kang Kenzu 3A2 (09)

Evan Lye Wen Kai 3A1 (07)

Abstract

Our project seeks to raise awareness on the threats of online phishing and the methods that can be used to properly identify and avoid phishing scams.

In 2020, the number of banking-related phishing scams increased by 1262 cases, from 80 cases in 2019 to 1342 cases in 2020. Victims also lost more than \$201 million to scams. This shows that there is still a large proportion of the public who are unfamiliar on how to identify and avoid phishing scams. In order to educate the digital immigrants on the ways to avoid scams, we have created a resource package which consists of (1) a set of teaching slides, (2) info posters and (3) a self-produced video. These materials are available in both English and Chinese to target a wider group of elderly.

In order to reach out to more seniors, we shared our materials with an organisation that educates and interacts with the elderly, U 3rd Age.

1 Introduction

1.1 Rationale

As the world slowly migrates into the digital era, users must also become more aware of the risk and threats they might encounter. Digital immigrants who did not grow up during the age of the internet are more susceptible to the risks of phishing. Consequently, this group of users should take extra precaution to combat the plethora of threats they may encounter online.

Online scams are one of the biggest threats in the digital era. This is the act of tricking people to gain material profit. The main target of these scams is the less tech-savvy senior generation.

In order to help these digital immigrants, we have developed a resource package to educate and inform them on how to identify and protect themselves from phishing scams. The elderly will then be more equipped and confident when using their devices.

Concurrently, this will encourage the elderly to pick up modern technology and help accelerate the local population's shift towards a Smart Nation.

1.2 Objectives

Our objectives are to:

1. Raise awareness on online phishing among the elderly
2. Educate the elderly on
 - the techniques used to identify phishing scams
 - the ways to avoid phishing scams

1.3 Target Audience

The target audience were elderly aged 50 and above, whom we felt were prime digital immigrant candidates.

1.4 Resources

Our resources are available in both English and Chinese, comprising of:

1. Teaching Slides
2. Illustrative Poster
3. Self-produced video targeted at the elderly

2 Review

To find out more about the current situation of online phishing, we gathered information from articles from **Today News**, **Straits Times** and **CNA** etc.

The common message we gathered was that the elderly remained an optimal target for the scammers. This is because most of them were unfamiliar with online phishing and had a substantial amount of savings.

We also found government campaigns and initiatives that were previously introduced in an effort to spread awareness regarding online phishing. One example is the Echo Against Scams Initiative which is a police roadshow launched by SPF. The EAS

ambassadors distributed brochures and fridge magnets to participants as reminders to be careful online.

However, we found such physical reminders to be ineffective as they were too mundane and incompatible with the online nature of phishing. Furthermore, this initiative did not specifically target digital immigrants. Hence, we wanted to work on a project that educates the digital immigrants on how to protect themselves against scams.

Research

What is the current situation of online phishing?

Centre recovers \$3.7m from scammers' accounts with banks' help

A specialised nerve centre to deal with reported scam cases has managed to recover 35 per cent or about \$3.7 million in victims' losses since it was set up last June.

Following the reports, the centre managed to freeze 2,600 bank accounts suspected to be involved in scammers' operations to recover some of the losses.

The centre has been working closely with the three major local banks - DBS Bank, United Overseas Bank and OCBC Bank - since its formation, to freeze suspicious bank accounts within a few days.

Previously, the process would have taken about two weeks, leading to a 4 per cent to 8 per cent recovery rate, said the officer-in-charge of the centre, Assistant Superintendent Teng Chin Lock.

Last November, it roped in seven more banks to join the initiative. They are: ANZ, CMB Bank, Citibank, Standard Chartered Bank, Bank of China, HSBC and Maybank.

The centre has also worked with the Association of Banks in Singapore to shorten the time for banks to provide PayNow transaction details to the police, from weeks to a few days.

This increases the chances of recovery of money scammed from victims, said the police.

The setting up of the centre has allowed banks to work closely with the police to disrupt scammers' operations more quickly, said ASP Teng.

The case "recovered" an elderly woman was prevented from transferring a total of \$440,000 to a scammer who claimed to be her husband's business associate.

Bank staff were suspicious and alerted the centre when the woman attempted to make the transfer to an account in Dubai.

Police officers were then dispatched to the scene to prevent the transfer.

However, for most victims of transnational scams, there is often little to no chance of recovering their losses after the transfer has been made, said ASP Teng.

Charmaine Ng

HOW MUCH MONEY HAVE PEOPLE IN SINGAPORE LOST TO SCAMS?

Types of scams	Amount Cheated		
	2020	Change from 2019	Largest sum cheated
Investment	\$569.5m	+\$533.5m	\$56.4m
China officials impersonation	\$539.6m	+\$518.5m	\$54.2m
Internet love	\$533.1m	-\$51.6m	\$51.1m
Tech support	\$522.3m	+\$54.3m	\$51.1m
Loan	\$514.5m	+\$52.7m	\$5735,000
E-commerce	\$56.9m	+\$54.6m	\$51.9m
Banking-related phishing	\$55.8m	+\$55.3m	\$506,000
Social media impersonation	\$55.5m	+\$52.4m	\$5367,000

CNA 9 Feb 2021

Seniors are attractive targets of online scams as they are more likely to have accumulated savings and tend to be more trusting of others. To help seniors avoid becoming a victim of online scams, dedicate some time to teach them about common types of online scams and what to do when they

Gosafeonline 6 Aug 2018

One demographic that is most vulnerable to cyber crime is the elderly. One obvious reason is that they are generally not as technically savvy and may not be as comfortable in the online environment. They are also attractive targets to cyber criminals as most tend to have more wealth or a larger "nest egg". Senior citizens, especially those in Singapore, also

Today 4 Jan 2017

Seniors are prone to fall prey to phishing, especially in banking related activities.

Research

What are the shortcomings of current measures implemented to educate the elderly about online phishing?



Ms Josephine Teo, Minister for Transport and Second Minister for Home Affairs, announced the launch of the police roadshow and Echo against Scams in her speech on Nov 24, 11 mins 05:45:24.

The Straits Times 24 Nov 2018

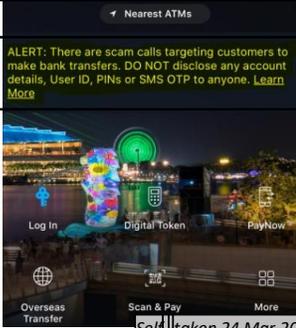
Echo against Scams ambassadors will be distributing anti-scam tool kits to fellow seniors, which include items like brochures on various scams, as well as fridge magnets with images of the staff passes of agencies that commonly visit households, such as the National Environment Agency and various town councils.

The Straits Times 24 Nov 2018

Current measures are mundane and incompatible with the online nature of phishing.

Nearest ATMs

ALERT: There are scam calls targeting customers to make bank transfers. DO NOT disclose any account details, User ID, PINs or SMS OTP to anyone. [Learn More](#)



Self-taken 24 Mar 2021

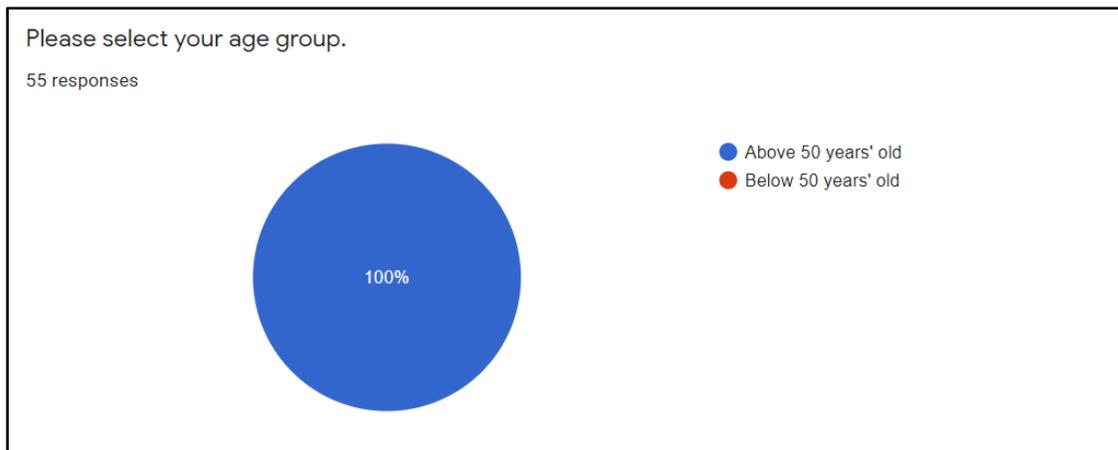
3 Methodology

3.1 Needs Analysis

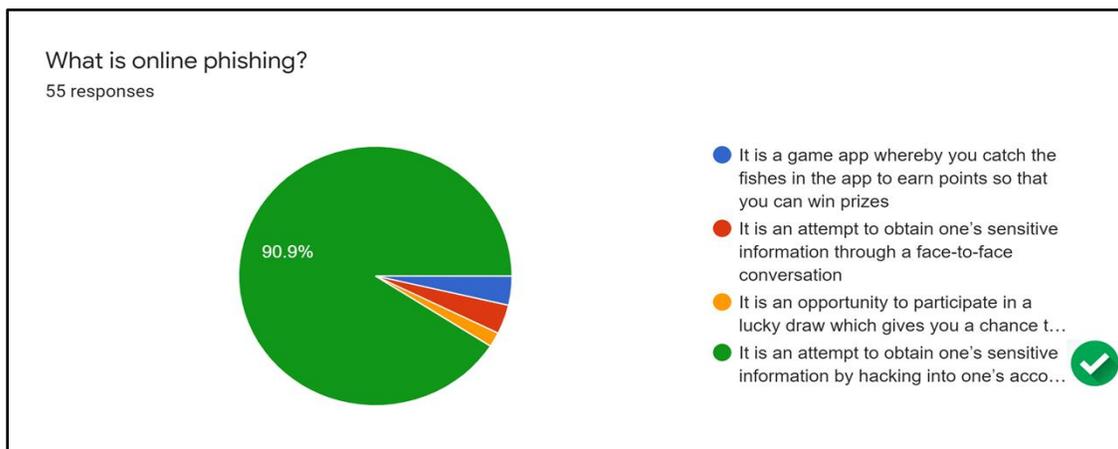
To determine the relevance of our project and the its key aspects, we conducted a quiz to help with our needs analysis. The quiz sought to find out the amount of information digital immigrants know about phishing scams and if they were aware of the methods to properly identify and avoid them.

We interviewed a total of 55 elderly aged 50 and above. From our survey results, we concluded that most elderly understood what online phishing scams were with close to 90.9% of the respondents choosing the correct answer for question 1.

Participant Age Group:

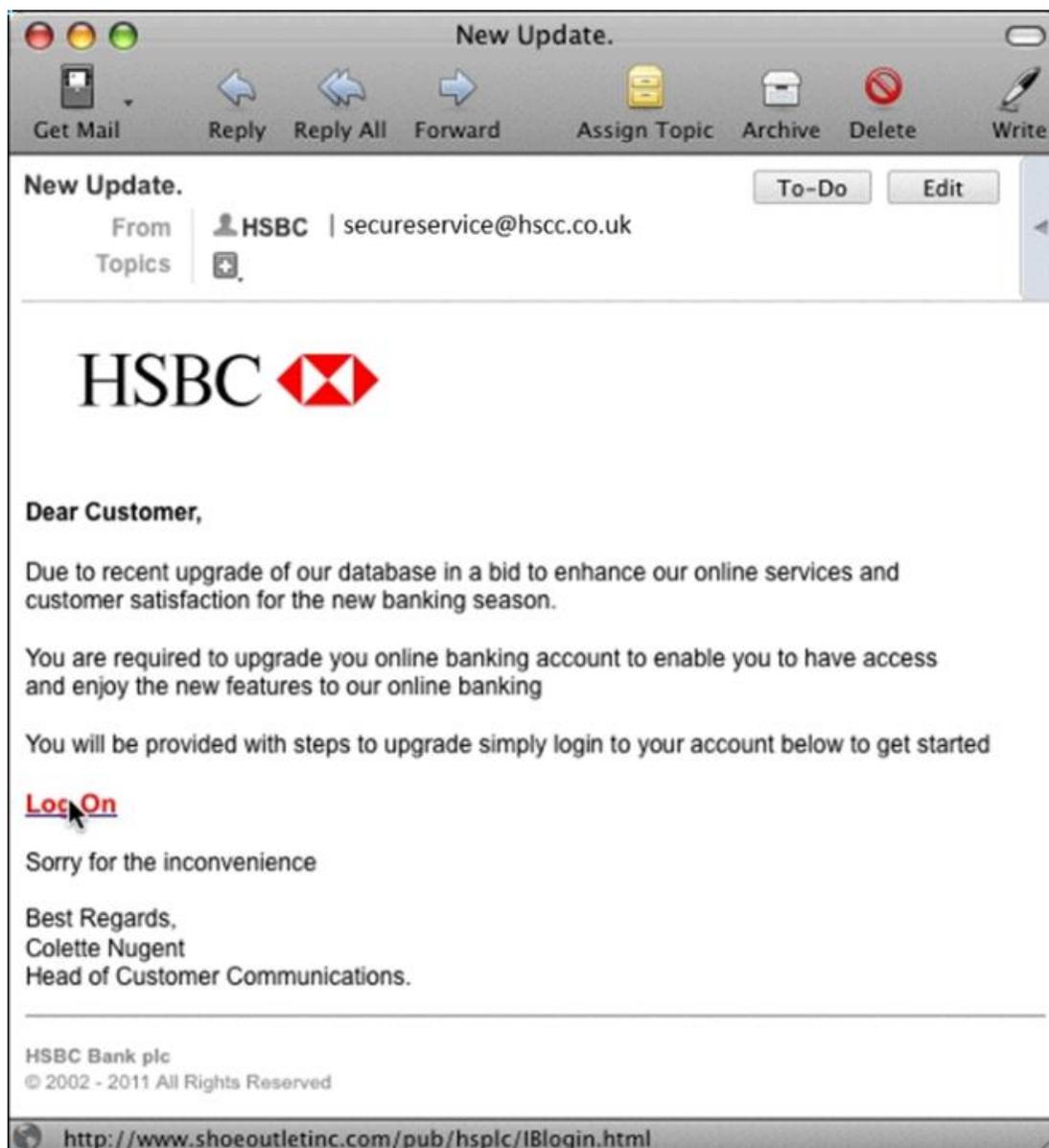


Question 1:



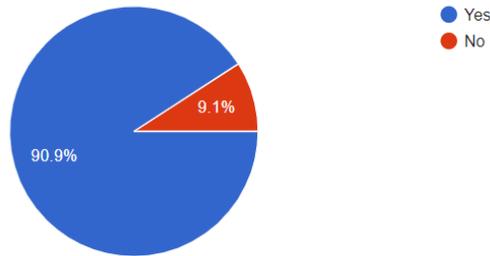
However, they did not know how to identify and avoid scams properly. This can be seen from the responses in question 2. Many of the respondents identified the email given as a scam but they gave the wrong reasons like “no bank logo”, “seems weird” to support their choices. They are unaware of the common tell-tale signs of a phishing scam. Hence, we believe that should more advanced phishing techniques be used in the future, these group of individuals will fall prey easily.

Question 2:



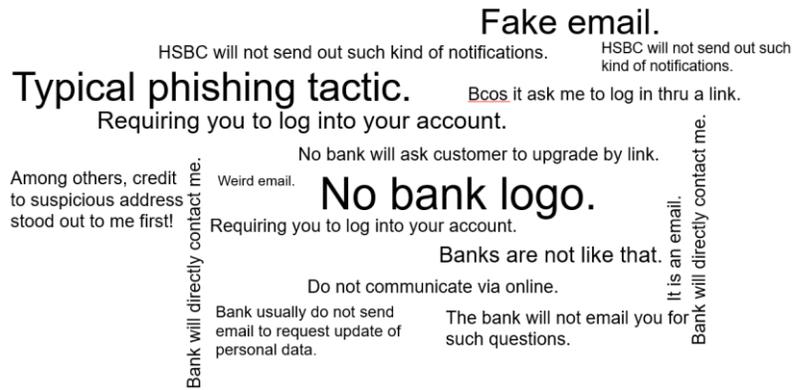
(a) Imagine that you received and read this email. After that, you clicked onto the given link which directed you a HSBC login page. Do you think that this is a scam? (Please select 'Yes' or 'No')

55 responses



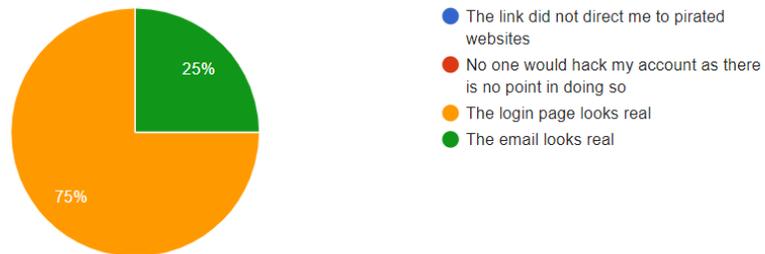
(b) If you have chosen 'yes' in Q2, why did you think that this was a scam? [Only answer this question if you chose 'yes' in (a)]

49 responses



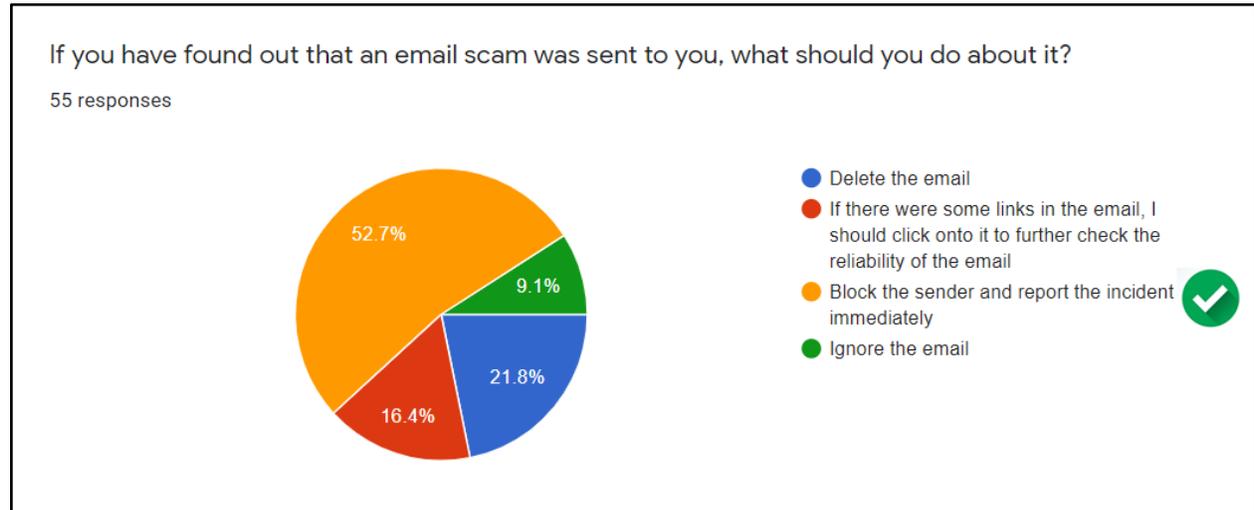
(c) If you have chosen 'no' in Q2, why did you think that this was not a scam? [Only answer this question if you chose 'no' in (a)]

4 responses

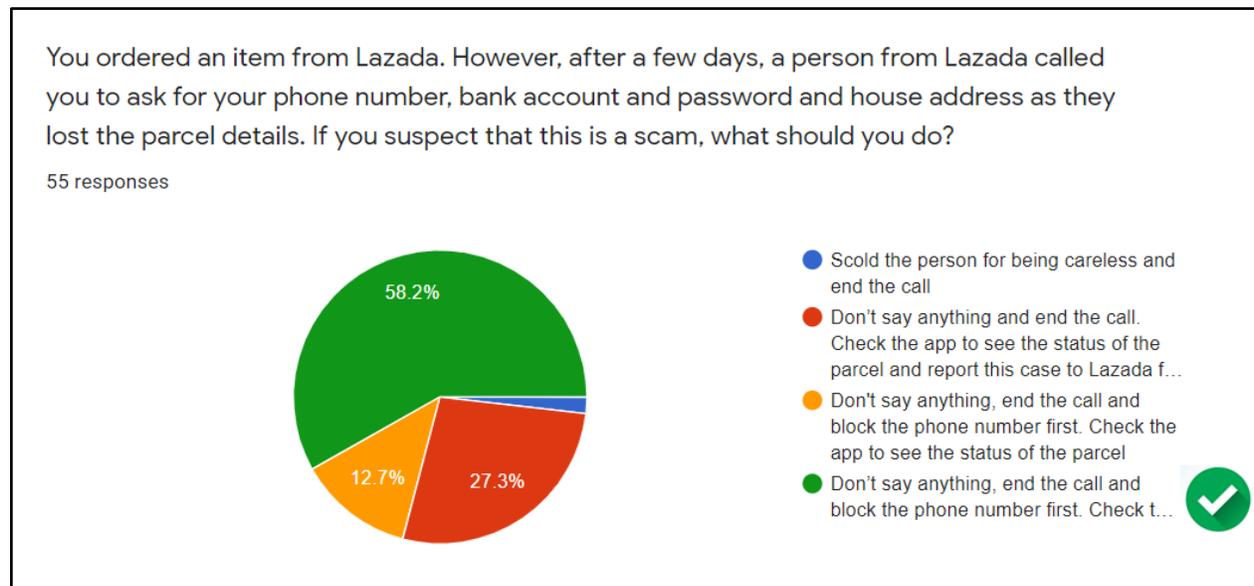


Furthermore, the elderly lack knowledge on the methods to avoid scams. This could be seen from the responses from question 4 and 5. 47.3% of the respondents chose the wrong answer for question 4 and 41.8% of the respondents chose the wrong answer for question 5.

Question 4:



Question 5:



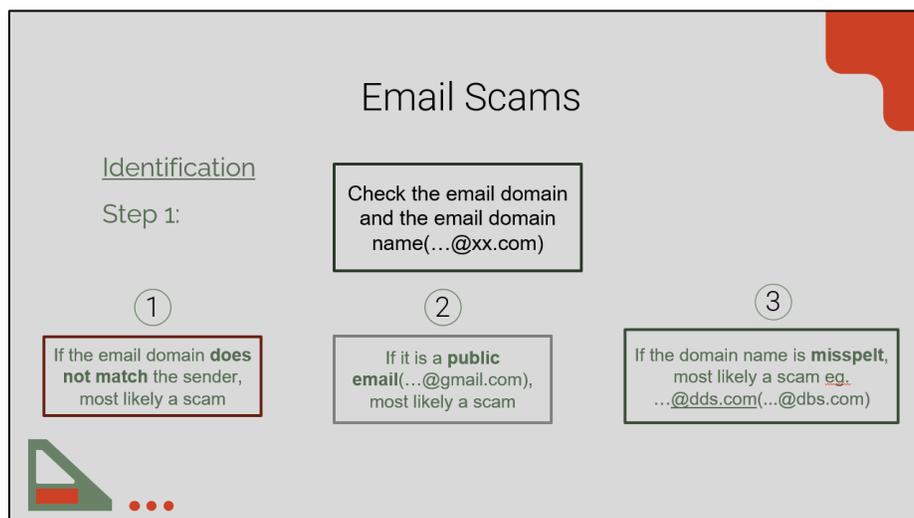
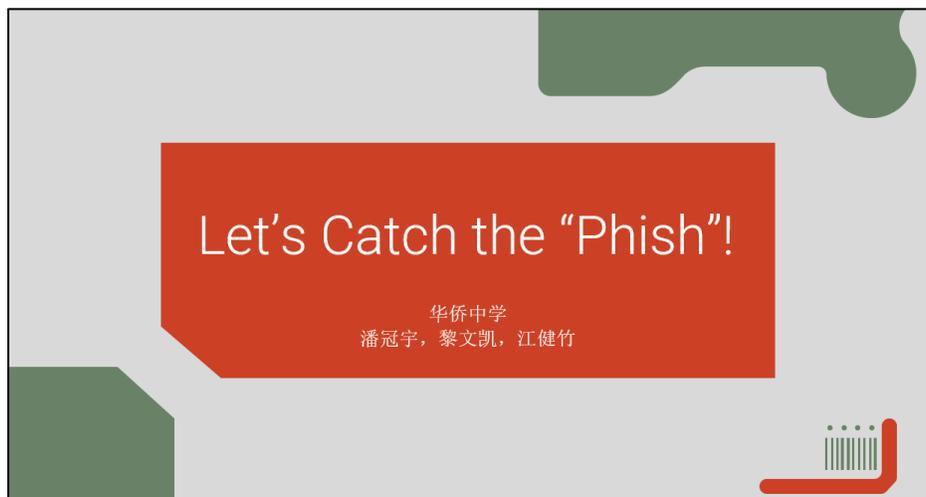
In response to this knowledge gap, we created a resource package to raise awareness on phishing scams among digital immigrants. This package taught them how to identify and avoid possible scams.

Though the majority of respondents gave the correct answers for the quiz, a **significant number** of respondents chose the wrong answers. This shows that a large population of digital immigrants do not know how to identify and avoid scams, which further proves that our project is relevant and necessary.

3.3 Development of Resources

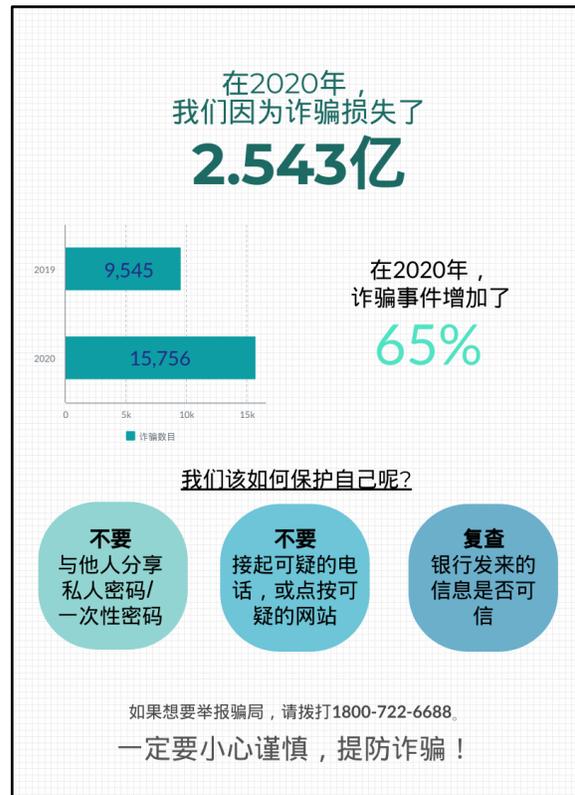
(i) Teaching Slides

We created a set of English and Chinese teaching slides which covers what to look out for on the internet and how to avoid phishing scams. There is also a quiz at the end to test their knowledge regarding online phishing and ensure that they react to these scams with the appropriate response.



(ii) Poster

We created posters to promote awareness on the various steps that should be taken to avoid scams. These posters could also be used as reminders in bank apps to warn and protect users against these scams.



(iii) Video

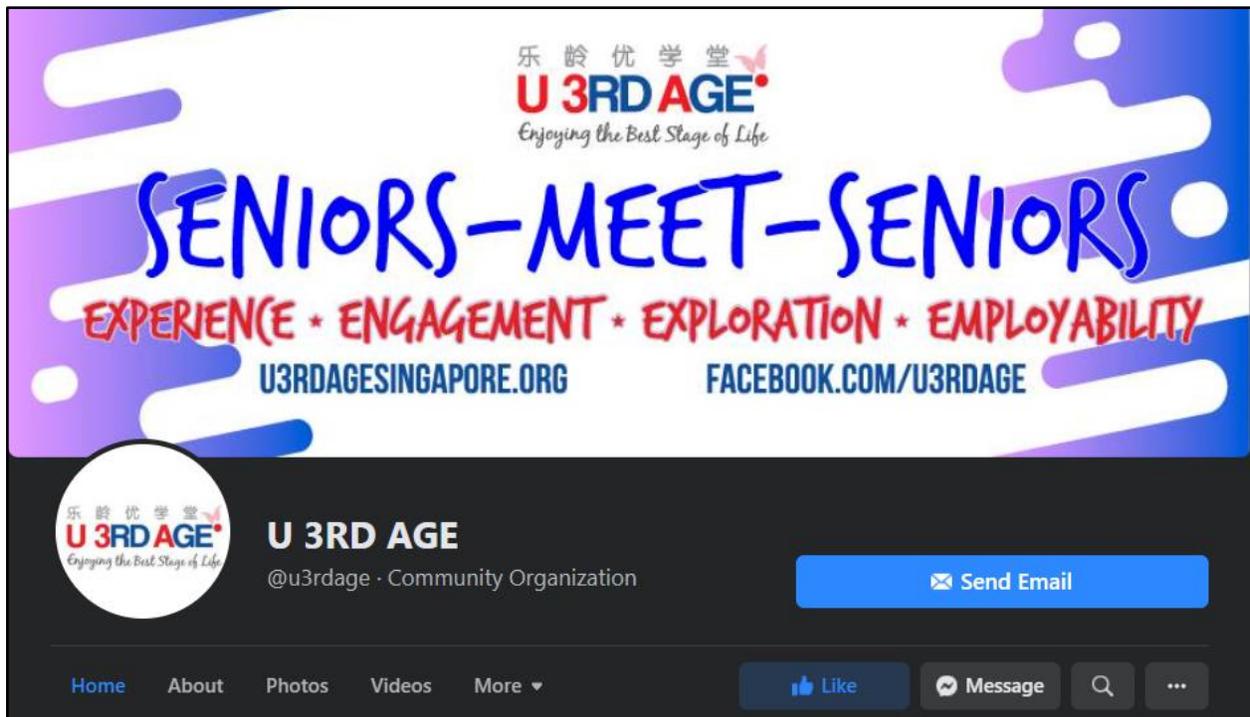
Apart from the previous measures, we produced a skit and added informational slides in it to engage our audience while effectively conveying our message.

This video was acted, filmed and edited by all of our project members. We have included an English voice over with Chinese subtitles and created catchy acronyms and taglines that are easy to remember such as “E.S.S” and “3 Don’ts” to help our audience remember the information covered.



(iv) Pilot test

Due to the Covid-19 restrictions, we were unable to conduct a physical lesson with our target audience. However, we contacted the administrator of an elderly-friendly organisation, U 3rd Age to share our materials. The administrator of U 3rd Age accepted our partnership and would be sharing our materials on their Facebook page.



4 Outcome & Discussion

Based on the responses and feedback given, we concluded that our resource package was effective as it has proven to be easy to understand and remember. Most individuals who viewed our materials were able to remember the 2 taglines after seeing them for the first time.

Throughout the journey, we faced many problems due to the Covid-19 pandemic. We identified 3 main limitations:

- 1)** We could not conduct a physical pilot test due to many restrictions caused by the Covid-19 heightened alerts from June to July. We were unable to physically access and gather feedback. Although we were able to gain some feedback online, we felt that in-person comments would have been more constructive.

- 2)** Our materials were only circulated among U 3rd Age members. With all our audience coming from the same organisation, we lack variety among the elderly population. As a result, we feel that our pilot test is not representative of all digital immigrants. Since the members of U 3rd Age are already part of a Facebook group, it is reasonable to assume that most of them are already more digitally advanced than their peers.

- 3)** Due to the rapid evolution of phishing methods, the effectiveness of our resource package is limited by our ability to ensure that its updated. Therefore, it is difficult for us to constantly update our materials against the most recent phishing “trends”.

5 Conclusion

Despite the Covid-19 restrictions, we managed to overcome several difficulties. Some memorable challenges were:

- 1) Planning around Covid-19 restrictions that only allowed for groups of 2 to gather.

- 2) Being creative in finding an audience to pilot test our resources through an online medium.

From the challenges faced, we learnt to adapt our measures to cater to any unforeseen challenges. We also had to be creative and think out of the box when it came to educating the digital immigrants on an online platform, one that they were less familiar with. For our audience to retain as much knowledge as possible, we challenged ourselves and honed our video-editing skills to produce a succinct and impactful video. Despite facing much adversities, we persevered through the difficulties and produced a final resource package that we are proud of today.

6 References

- Gosafeonline. How to help seniors stay safe online. Retrieved from <https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/how-to-help-seniors-stay-safe-online>
- Joelle H. Fong. Protecting the elderly from cyber attacks. Retrieved from <https://www.todayonline.com/singapore/protecting-elderly-cyber-attacks>
- Venessa Lee. Amid rise in loan scams among the elderly, anti-scam drive launched to educate seniors. Retrieved from <https://www.straitstimes.com/singapore/amid-rise-in-loan-scams-among-the-elderly-anti-scam-drive-launched-to-educate-seniors>
- Jalelah Abu Baker. 10 types of scams which Singaporeans fall for. Retrieved from <https://www.channelnewsasia.com/singapore/more-than-201-million-cheated-top-10-scam-types-2020-police-339081>
- Charmaine Ng. Centre recovers \$3.7m from scammer's account with bank's help. Retrieved from https://www.police.gov.sg/-/media/Lets_Fight_Scams_4.PNG