Cyber Literacy & Awareness among Generation Z and Millennial Students

Research Conducted By: Karol Pierre

Advised By: Richard Perry

May 2019

Copyright © 2019 by Karol Pierre

All Rights Reserved

Acknowledgments

This research could not be conducted without a few key players who aided and guided me in developing the outline and method of execution for this research. At this time, I would like to thank . . .

Dr. Richard Perry, my advisor for this project, who served as a mentor and sound board and provided me with advice that would ensure that I obtained favorable results

Crispin May & Jennifer Cunningham, from the Villanova U.N.I.T & Operations & Security Team, who assisted me in making the proper connections and providing me with the approval to proceed with the research

Jeremy Letournel, from InfoSec Institute, who served as a liaison to gain access to a plethora of resources which include but are not limited to InfoSec Institute's phishing campaign service and email templates

Abstract

The primary objective of this research is to shed light on how millennial and generation z students become victims to cyber attacks such as phishing. This research aims to highlight how introduction of educational stimuli can benefit students by providing techniques to accurately analyze and detect certain attacks. While there is no foolproof solution to eliminating cyber attacks, cyber education is a powerful tool in minimizing the likelihood that an individual will be prone to becoming a victim of cyber crimes. The analysis of this research reveals that introduction to educational cybersecurity material aids in improving the analytical, detective, and preventive skills of students.

Table of Contents

Acknowledgments 3
Abstract 4
1. Problem Statement 6
2. Development of Probable Solution 7
2. 1 Educational Material 7
2. 1. 1 Batch Script 7
2.1.2 PowerPoint Slides 8
3. Research 9
3.1 Phase 1: Establishing the Baseline 9
3.2 Phase 2: Education 10
3.3 Phase 3: Progress Assessment 11
4. Analysis 12
5. Recommendations 14
6. Success & Challenges 15
6.1 Successes 15
6.2 Challenges 15
References 16
Appendices 17
Appendix A: *Cyber Reminder Batch Script Code* 17
Appendix B: *Cyber Literacy & Awareness PowerPoint Slides* 18
Appendix C : *Cyber Literacy & Awareness Assessment 1* 24
Appendix D: *Progress Assessment* 28

1. Problem Statement

According to the annual data book of consumer complaints about fraud released by the Federal Trade Commission back in March of the years, 2017 and 2018, 69% of younger people, specifically Generation Z & Millennials, reported fraud and loss of money [1] as depicted in Figure 1.

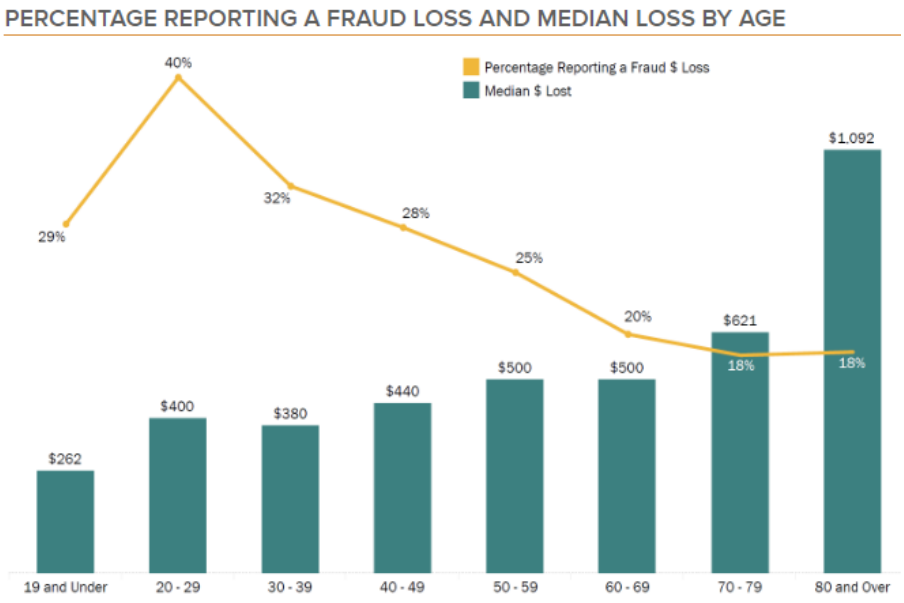


Figure 1: *FTC Fraud Loss by Age*

The top five categories for which reports were submitted are debt collection, identity theft, imposter scams, telephone and mobile services, and banks & lenders. These 5 out of 30 categories serve as 60% of the reports submitted as depicted in Figure 2.

Consumer Sentinel Network Data Book 2017: Report Categories

REPORT CATEGORIES

RANK	CATEGORY	# OF REPORTS	PERCENTAGE
1	Debt Collection	608,535	22.74%
2	Identity Theft	371,061	13.87%
3	Imposter Scams	347,829	13.00%
4	Telephone and Mobile Services	149,578	5.59%
5	Banks and Lenders	149,316	5.58%

Figure 2: *FTC Fraud Report Categories*

The scams are often executed via attack vectors such as social engineering and phishing. Due to lack of education on cyber attacks such as phishing and voice phishing (vishing), people aged up to 29 become victims of these attacks.

2. Development of Probable Solution

While there is no guaranteed solution to end all cyber attacks that lead to identity theft and loss of money, the first step that any individual can take in order to minimize the likelihood of becoming a victim is to educate themselves. By referencing the United States Computer Emergency Readiness Team (US-CERT) and the Federal Bureau of Investigation (FBI)'s Scams & Safety's advice and using templates from Infosec Institute, I have been able to develop a batch script and a set of slides that aims to provide a quick and basic lesson of the varying cyber attacks and methods to detect and prevent the attacks from occurring.

2. 1 Educational Material

2. 1. 1 Batch Script

The cyber reminder batch script runs automatically upon start up of a Windows system and greets the user according to the time of day. It contains 6 tips from US-CERT on how to avoid social engineering attacks, phishing attacks, and identity theft.

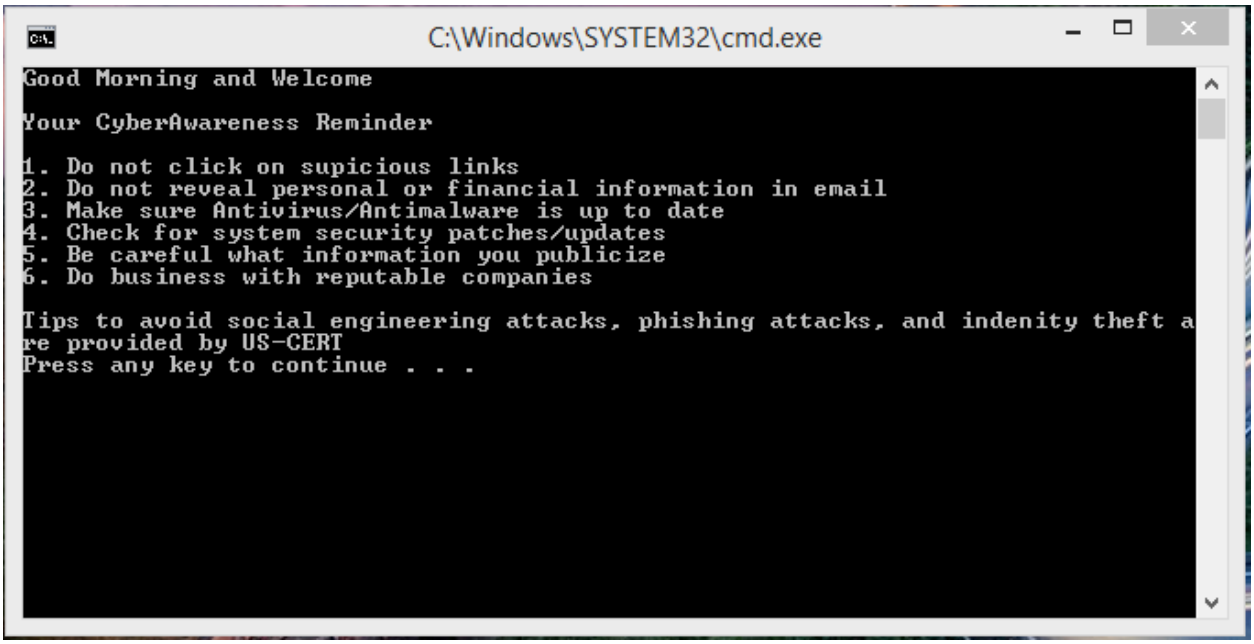


Figure 3: *Cyber Reminder Batch Script Display* (Appendix A)

2.1.2 PowerPoint Slides

The cyber literacy and awareness PowerPoint slides provide definitions on some of the different and most common types of attacks. In addition, they provide key signs to help an individual determine the authenticity of an email and/or advertisement. The final portion of the slides informs the readers of the outcomes of the attacks that can range from identity theft to credit fraud and preventive measures that can be taken to reduce the risk of becoming a victim of those outcomes.



Figure 4: *Cyber Literacy & Awareness Slides Example* (Appendix B)

3. Research

The objective is to determine whether introducing educational material on cyber attacks and prevention methods, with a focus on phishing, would produce a statistical difference in susceptibility to that very attack. Below are the measures taken to generate results with that focus in mind:

- Establish test group
  - participants without Computer Science/Computer Engineering background
  - range of freshmen - seniors (a combination of generation z and millennial students)
  - ensure privacy of collected personal information
- 33 participants signed up
  - 27 participants continued with Phase 1

3.1 Phase 1: Establishing the Baseline

Where does the current test group stand in regards to their knowledge of cyber attacks and prevention methods? The objective here is to assess the current knowledge base of the participants. Refer to Appendix C for all questions that were included in the baseline assessment.

- Knowledge vs. Application

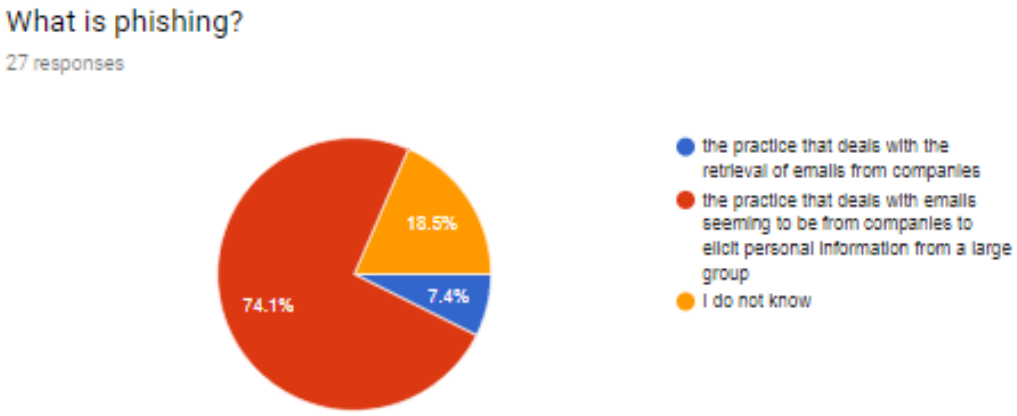


Figure 5: *Phase 1: Establishing Baseline (What is Phishing?)*

74 % of students know the definition of phishing but when asked to apply this knowledge to detect a phishing email this percentage decreases.

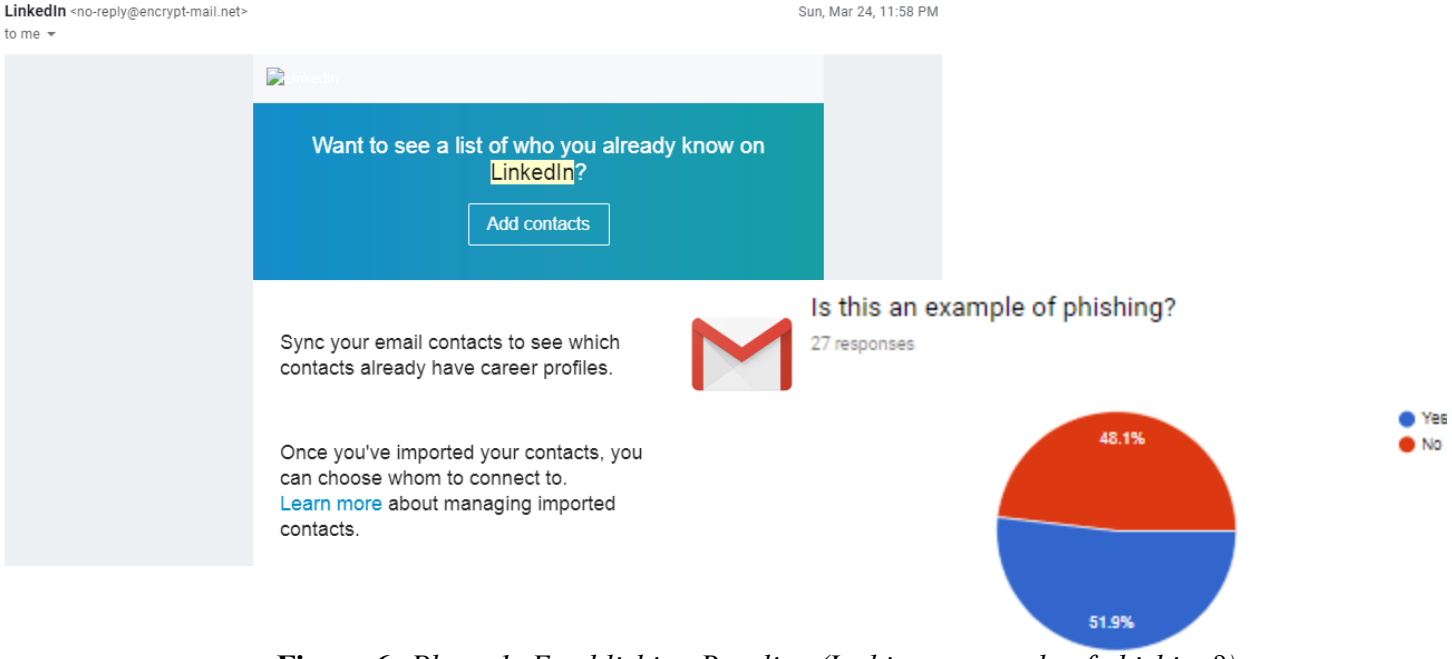


Figure 6: *Phase 1: Establishing Baseline (Is this an example of phishing?)*

74% of the students knew the definition of phishing but now only about 52% of the students were able to accurately detect it. The other questions (Appendix C) reveal roughly the same if not a lower percentage of students being able to accurately detect a phishing attempt.

3.2 Phase 2: Education

Phase 2 of the research focuses on education. Education in cybersecurity is often limited to computer science, electrical engineering, and computer engineering majors. While courses for cyber matters may be available as electives, the lack of enrollment in such courses only fuels the pool of students who may become victims to cyber crimes. Education on preventive measures and detective analysis will better prepare students to identify certain attacks.

Over a course of a week, the participants of the research were provided with the educational material outlined in section 2.1 which was the Cyber Literacy & Awareness PowerPoint. The objectives of the slides are to provide key techniques and methods to remediate the likeliness of being subjected to the consequences of cyber crimes.

3.3 Phase 3: Progress Assessment

After introduction of the educational material, a final assessment was given to determine if there was any improvement. This assessment consisted of similar questions as the primary assessment but included different examples of phishing and other attacks to check the level of improvement and overall comprehension on a few cybersecurity attacks.

The number of participants in the research decreased from 27 to 25; the participation of the missing 2 students represent a small statistical difference and does not greatly impact the results of the assessment which still maintain and showcase improvement in phishing detection when the educational stimuli was introduced.

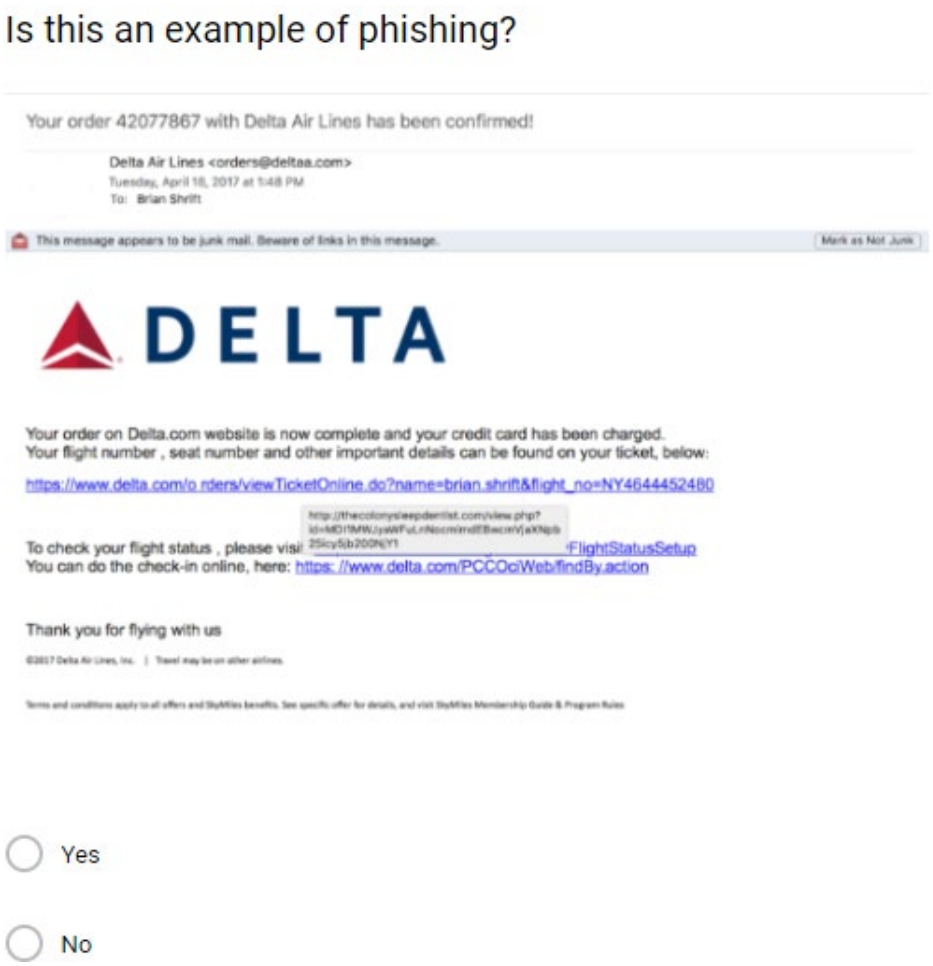


Figure 7: *Progress Assessment Example* (Appendix D)

4. Analysis

Before:

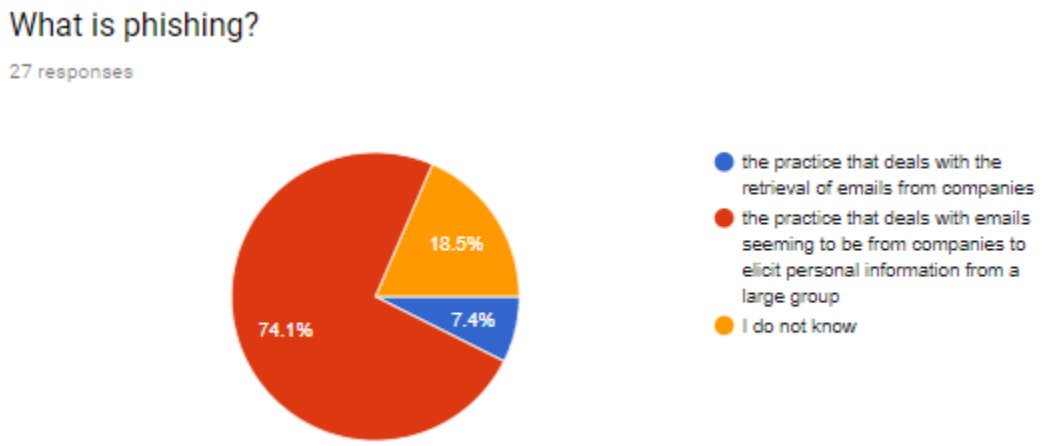


Figure 8: *What is Phishing? Results (Before)*

After:

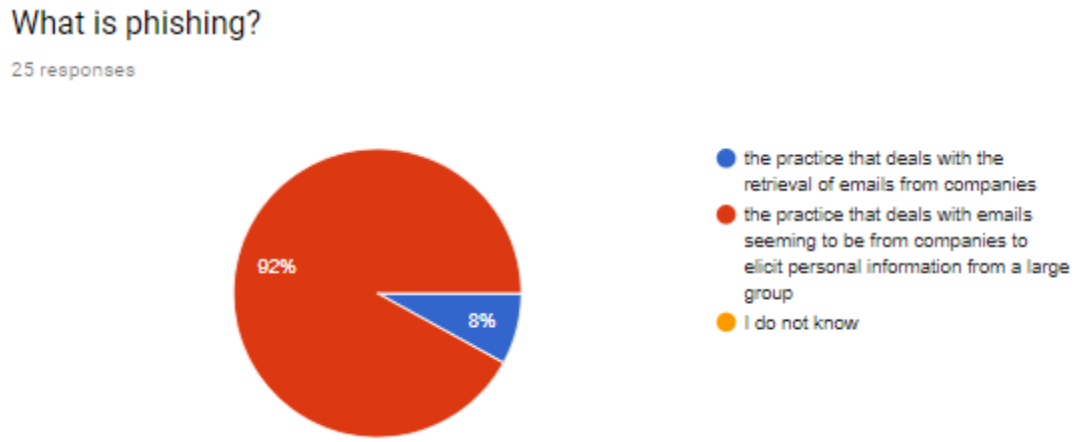


Figure 9: *What is Phishing? Results (After)*

The results from the first question of the initial assessment (Figure 8) compared to the results of the first question of the final assessment (Figure 9) depicts an improvement in the knowledge of what phishing is. If the 2 missing participants would have selected "No", the results would indicate that about 86% of the participants have a clear definition of phishing. This would still represent an 11% increase in the worst case scenario. If the 2 participants would have selected "Yes", the results would indicate that 93% of the participants understand what phishing is and would represent a 12% increase in the best case scenario.

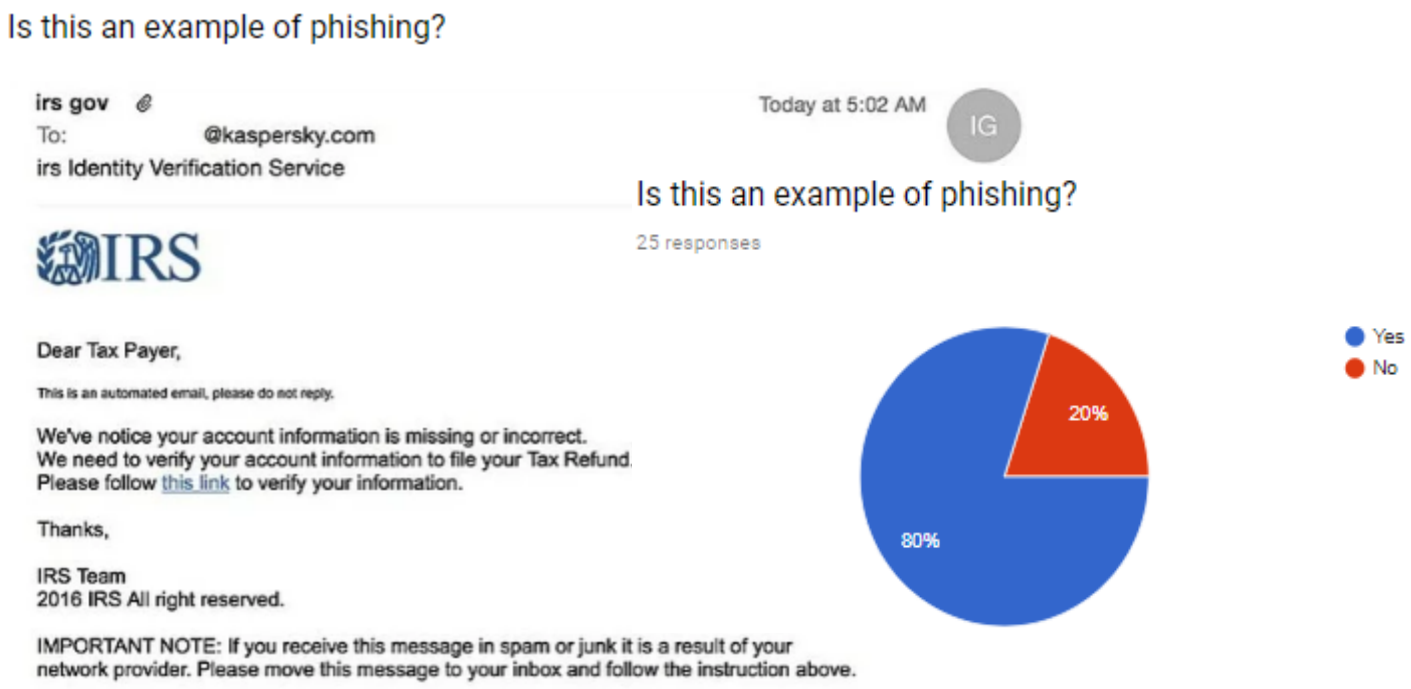


Figure 10: *Phase 3: Progress Assessment (Is this an example of phishing?)*

In discerning whether an example was phishing or not, 80% of the participants were able to accurately depict Figure 10 as a phishing attempt. To be consistent with consideration of missing participants, if the 2 participants would have selected "No", the results would reveal that 75% of the participants are able to accurately depict the phishing attempt. This would still be about a 23% increase in the application of the knowledge of phishing in the worst case scenario. In the best case scenario, if the 2 participants would have selected "Yes", the results would reveal about a 30% increase in the application of the knowledge of phishing via detection.

Before:

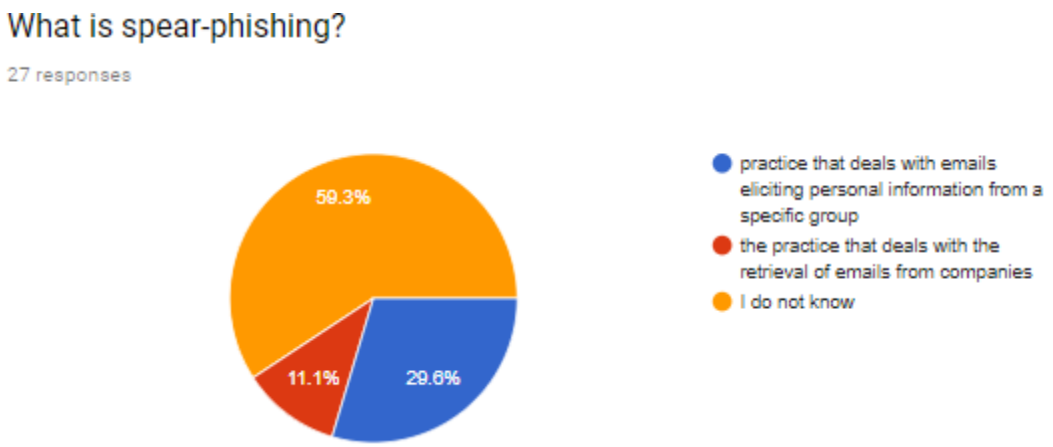


Figure 11: *What is Spear-Phishing? Results (Before)*

After:

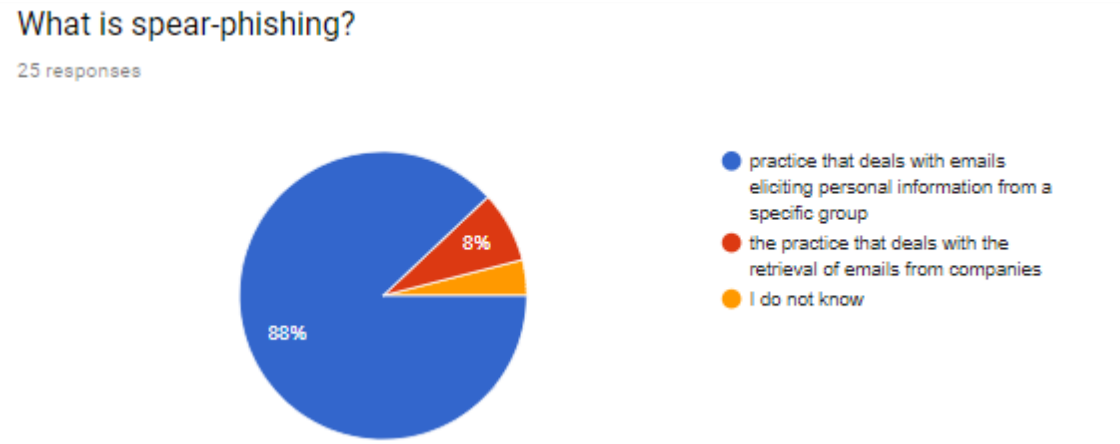


Figure 12: *What is Spear-Phishing? Results (After)*

The results from the first question of the initial assessment (Figure 11) compared to the results of the first question of the final assessment (Figure 12) depicts an improvement in the knowledge of what spear-phishing is. If the 2 missing participants would have selected "No", the results would indicate that about 86% of the participants have a clear definition of spear-phishing. This would still represent an 11% increase in the worst case scenario. If the 2 participants would have selected "Yes", the results would indicate that 93% of the participants understand what spear-phishing is and would represent a 12% increase in the best case scenario.

5. Recommendations

Cybersecurity education is imperative to the future of students because every sector of industry ranging from business to telecommunications and transportation have a need for cybersecurity. As the results suggest, the introduction of cyber educational material increases awareness and analytical capabilities. By introducing a required cybersecurity course to every student, regardless of one's major, the proper tools can be provided so that students may be able to defend themselves from being vulnerable and becoming victims of cyber attacks.

6. Success & Challenges

6.1 Successes

Over the course of this research, I have been able to develop educational tools that produced tangible results from which academic recommendations for cybersecurity related courses can be made. Additionally, the results of this research will be shared with Villanova's U.N.I.T & Technology Services' Cybersecurity Team as additional metrics for their security advancement at the student level across the different colleges.

This research leaves room for improvement and expansion in order to make these recommendations on a national level. This would be a lengthier research that could conducted and executed with the assistance of the accreditation board for the various majors and other universities.

6.2 Challenges

While there have been many challenges when conducting this research, each challenge has served as a lesson for improvement. The primary challenge is that this research project was unfunded. Due to this, the ability to first obtain a greater pool of participants or retain the participants who initially signed up without an incentive became difficult.

The original method of execution for the research, a phishing campaign, was modified as the phishing campaign structure required the whitelisting of the domains & IP addresses of the InfoSec Institute's servers. This step was able to be executed, however when a phishing trial was conducted using both the email address of my advisor and myself, the emails would be directed to spam. This is due in part to the filtering system implemented by Google's email management. As a result the execution of the research was modified to an analysis research which better isolates what is understood or known and how that does not necessarily translate to the application of that knowledge.

References

1. Fedral Trade Commission (FTC). https://www.ftc.gov/policy/reports/policy-reports/commission-staff-reports/consumer-sentinel-network-data-book-2017/top-ten-fraud-categories-id-other. *Accessed: January 23rd, 2019*

2. United States Computer Emergency Readiness Team (US-CERT). https://www.us-cert.gov/ncas/tips. *Accessed: January 23rd, 2019*

3. InfoSec Institute. https://securityiq.infosecinstitute.com/Templates/index. *Accessed: January 23rd, 2019*

Appendices

Appendix A: *Cyber Reminder Batch Script Code*

```
@echo off


REM Simple script that greets user according to time of day and provides user with quick reminders to minimize becoming a victim to cyber crimes and attacks


for /f "delims=:" %%A in ("%time%") do if %%A LSS 12 (echo Good Morning and Welcome) else (echo Good Afternoon and Welcome)

@echo:

@echo Your CyberAwareness Reminder

@echo:

@echo 1. Do not click on supicious links

@echo 2. Do not reveal personal or financial information in email

@echo 3. Make sure Antivirus/Antimalware is up to date

@echo 4. Check for system security patches/updates

@echo 5. Be careful what information you publicize

@echo 6. Do business with reputable companies

@echo:

@echo Tips to avoid social engineering attacks, phishing attacks, and identity theft are provided by US-CERT &pause
```

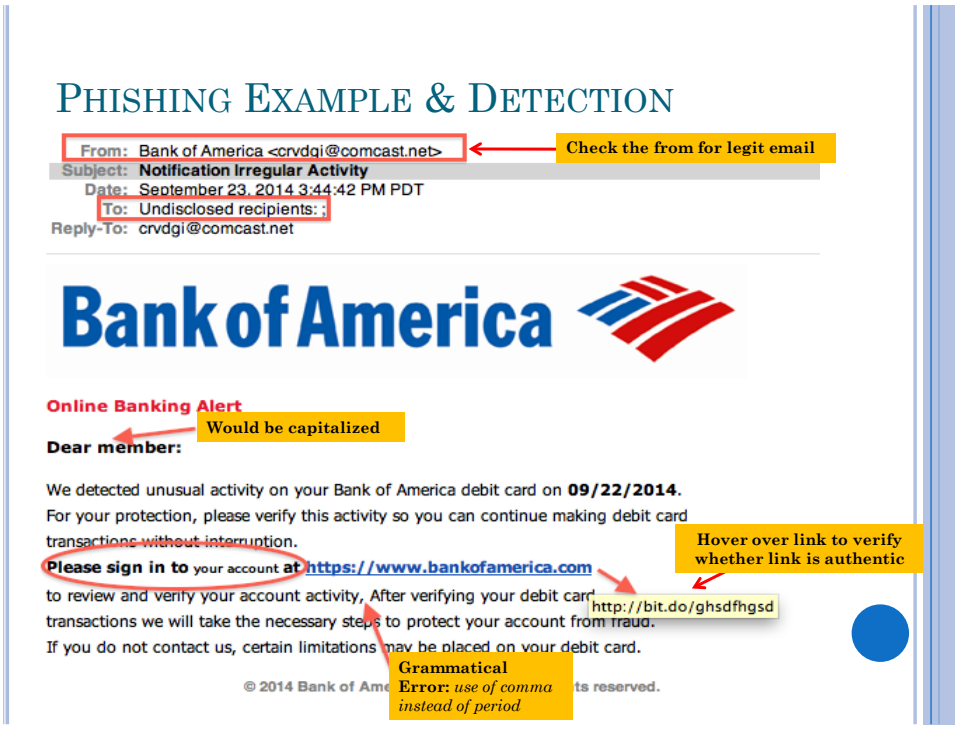
Appendix B: *Cyber Literacy & Awareness PowerPoint Slides*

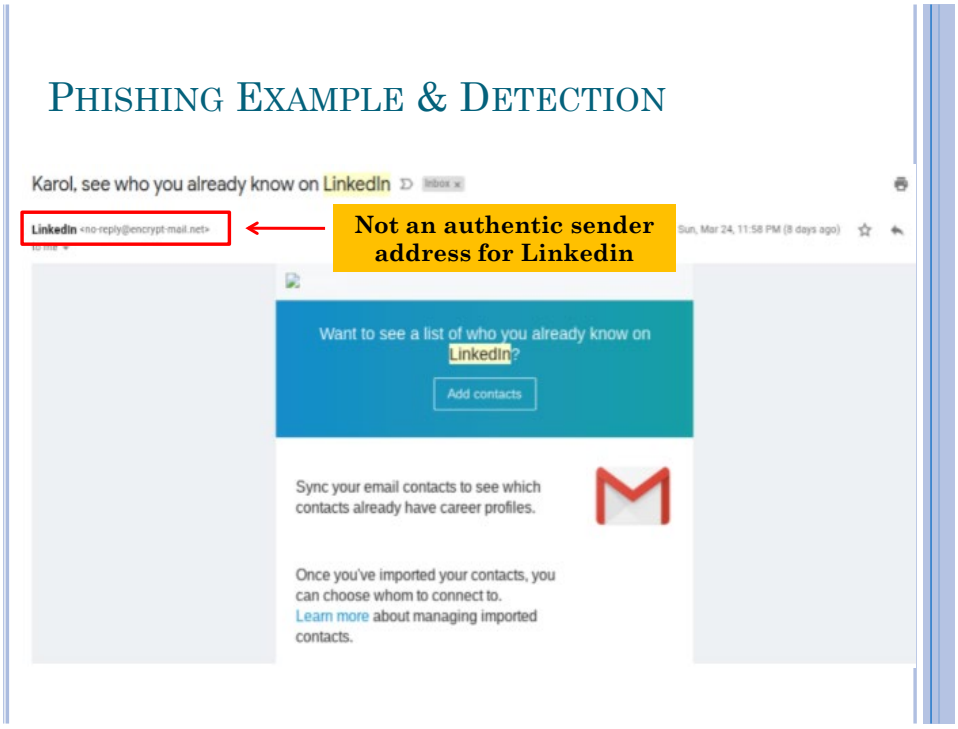


TYPES OF ATTACKS

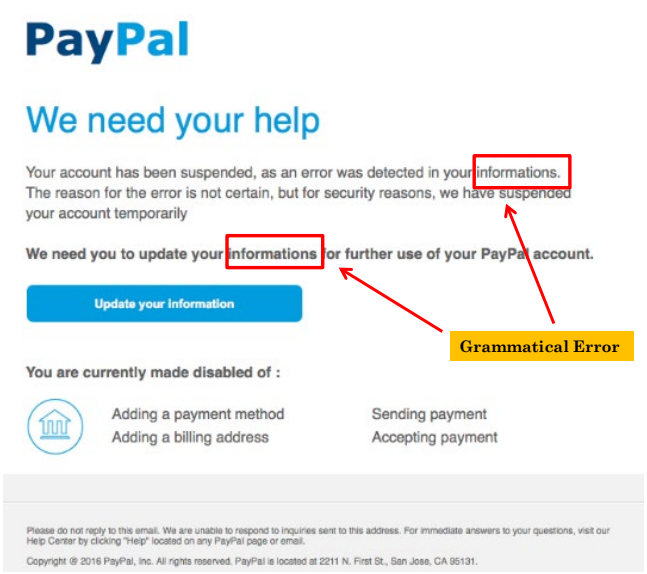


- **Attacker Techniques**
  - **Adware** : digital advertisments that automatically display when a user is online
  - **Scareware** : Victims are bombarded with false alarms and threats, prompting immediate action
  - **Pretexting** : Attacker gains trust by impersonating an official position (bank, tax-officials, police) , ask questions to confirm identity (actually stealing info)
  - **Phishing** : email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims
  - **Spear-phishing** : similar to phishing, but directed at a specific target and requires more time

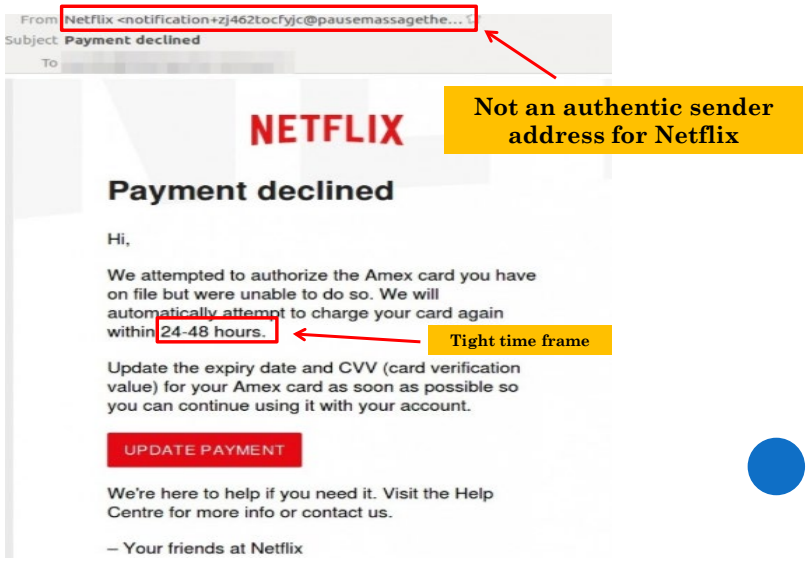

PHISHING EXAMPLE & DETECTION
From: Bank of America <crvdgi@comcast.net>
Check the from for legit email
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net
Bank of America
Online Banking Alert
Would be capitalized
Dear member:
We detected unusual activity on your Bank of America debit card on 09/22/2014.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account at https://www.bankofamerica.com
Hover over link to verify whether link is authentic
to review and verify your account activity. After verifying your debit card
http://bit.do/ghsdfhgsd
transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.
Grammatical Error: use of comma instead of period
© 2014 Bank of Ame
ts reserved.


PHISHING EXAMPLE & DETECTION
Karol, see who you already know on LinkedIn
Inbox x
LinkedIn <no-reply@encrypt-mail.net>
Not an authentic sender address for Linkedin
Sun, Mar 24, 11:58 PM (8 days ago)
Want to see a list of who you already know on LinkedIn?
Add contacts
Sync your email contacts to see which contacts already have career profiles.
Once you've imported your contacts, you can choose whom to connect to.
Learn more about managing imported contacts.

Phishing Example & Detection



Phishing Example & Detection



Scareware Example & Detection



The goal is to alarm and convince you

Adware Example & Detection



Aims to lure user by using word "free"

IMPLICATIONS



- Identity Theft
- Theft of Credit Card Information
- Personal Data Exfiltration:
  - SSN, Insurance, and more
- Human Trafficking
- Blackmail
- Extortion



PREVENTIVE MEASURES

- Don't Open emails and attachments from suspicious sources
- Be wary of tempting offers



- Secure Computing devices
  - Antivirus/Anti-malware, Firewall, email filters, passwords, multifactor authentication
- Slow down
  - Make sure to take your time
  - Read everything through



- Foreign offers are fake
- Beware of any download link

CITED WORKS

- https://securityiq.infosecinstitute.com/Templates/index
- https://www.us-cert.gov/ncas/tips/ST04-014
- https://www.incapsula.com/web-application-security/social-engineering-attack.html
- https://towardsdatascience.com/applied-text-classification-on-email-spam-filtering-part-1-1861e1a83246

Appendix C : *Cyber Literacy & Awareness Assessment 1*

Cyber Literacy & Awareness Assessment 1

Please take this test WITHOUT using any resources.
I need accurate and unbiased responses for the research to be effective.
Please answer all 8 questions

* Required

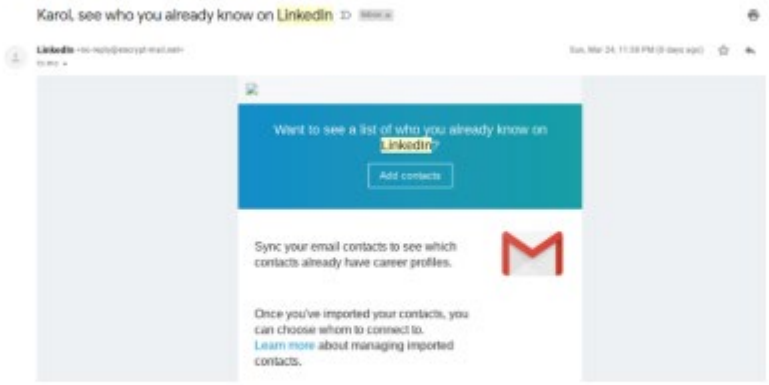
Email address *

Your email

What is phishing? *

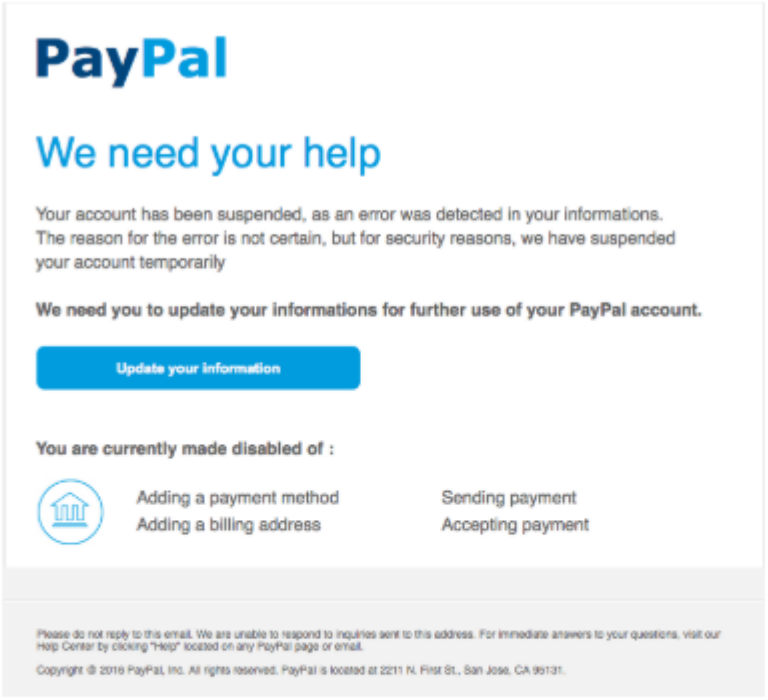
- ◯ the practice that deals with the retrieval of emails from companies
- ◯ the practice that deals with emails seeming to be from companies to elicit personal information from a large group
- ◯ I do not know

Is this an example of phishing? *



- ◯ Yes
- ◯ No

Is this an example of phishing? *



PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

Adding a payment method
Adding a billing address

Sending payment
Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright © 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

- ◯ Yes
- ◯ No

Do you think you would be able to detect a phishing scam? *

- ◯ Yes
- ◯ No

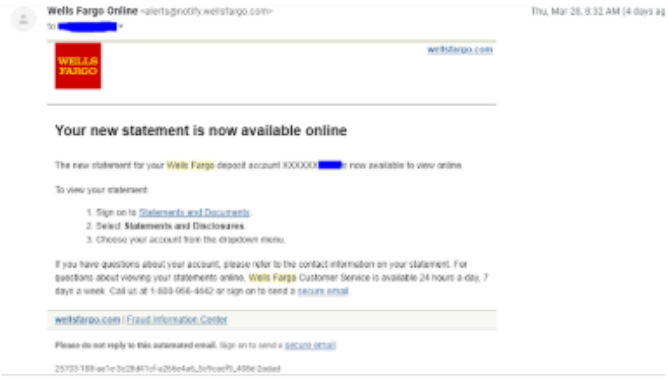
What is spear-phishing? *

- practice that deals with emails eliciting personal information from a specific group
- the practice that deals with the retrieval of emails from companies
- I do not know

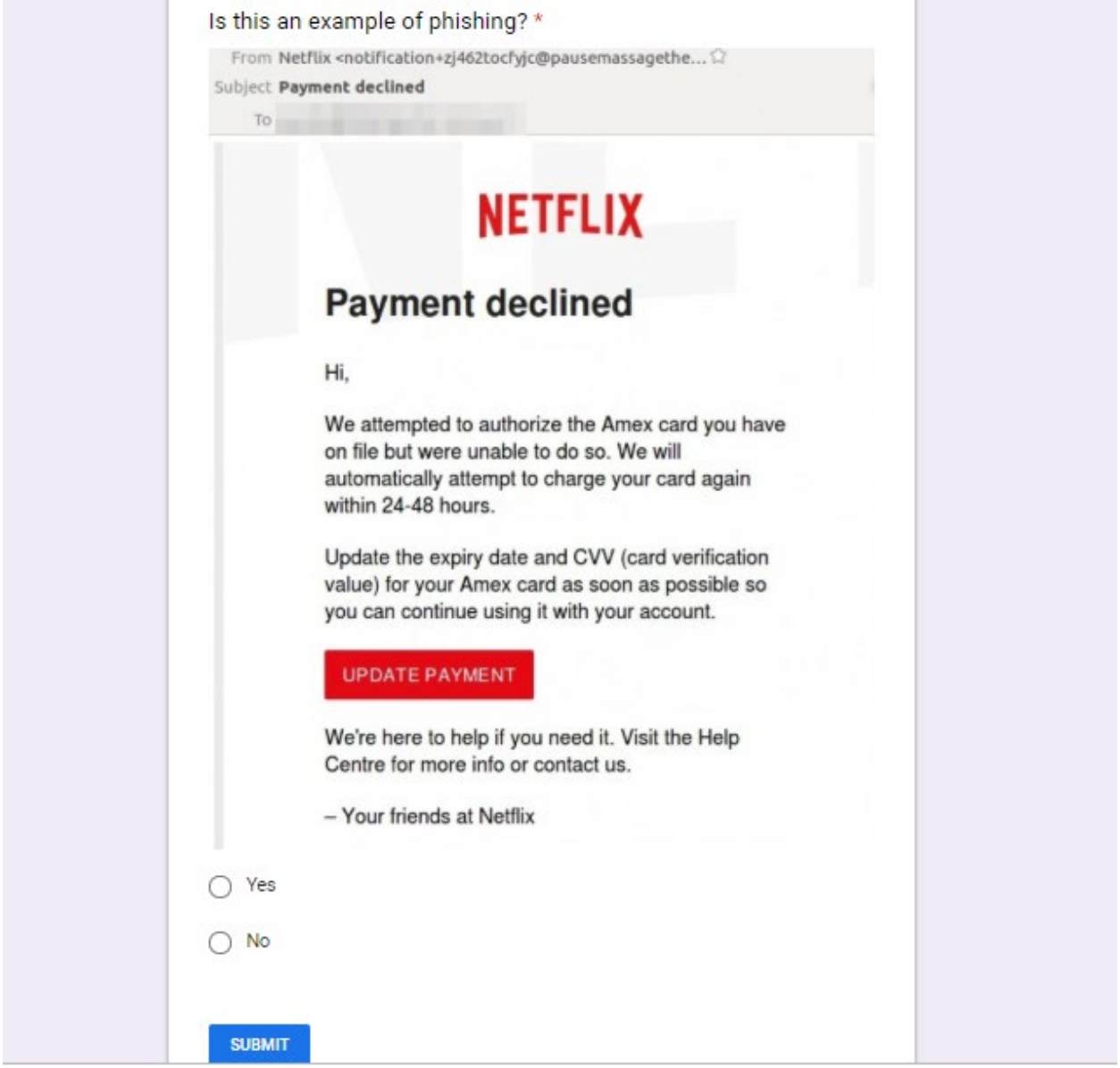
What is a prevention method for phishing? *

- Using a different email address
- Don't click on attachments
- Using a Macbook laptop because they don't get viruses

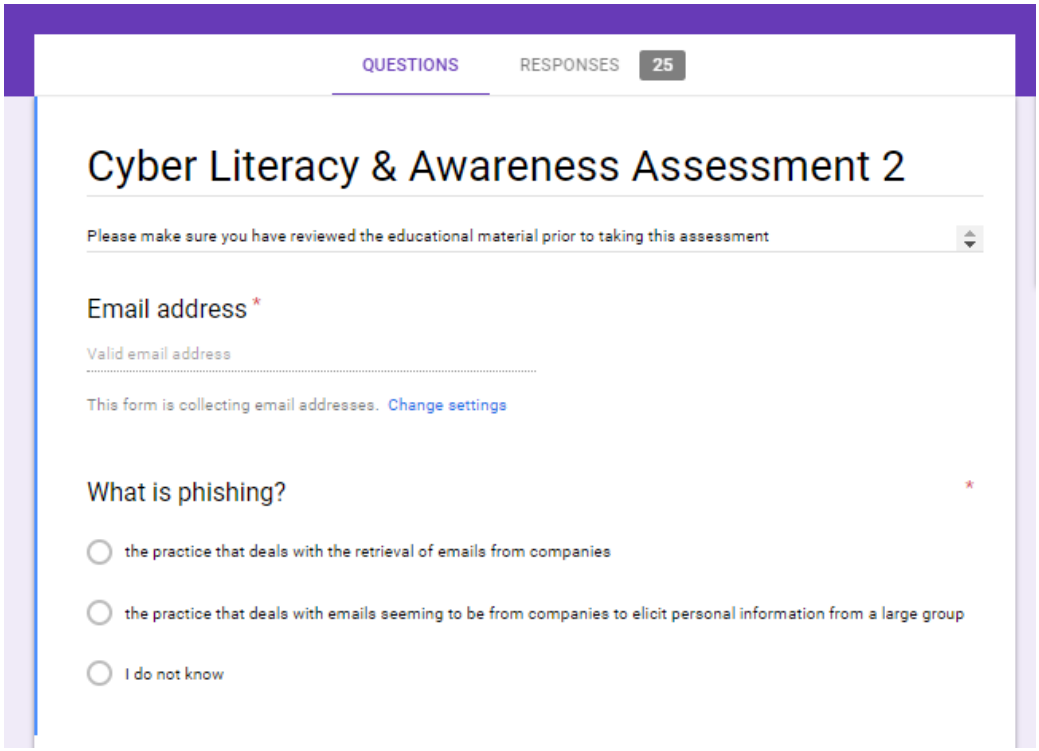
Is this an example of phishing? *

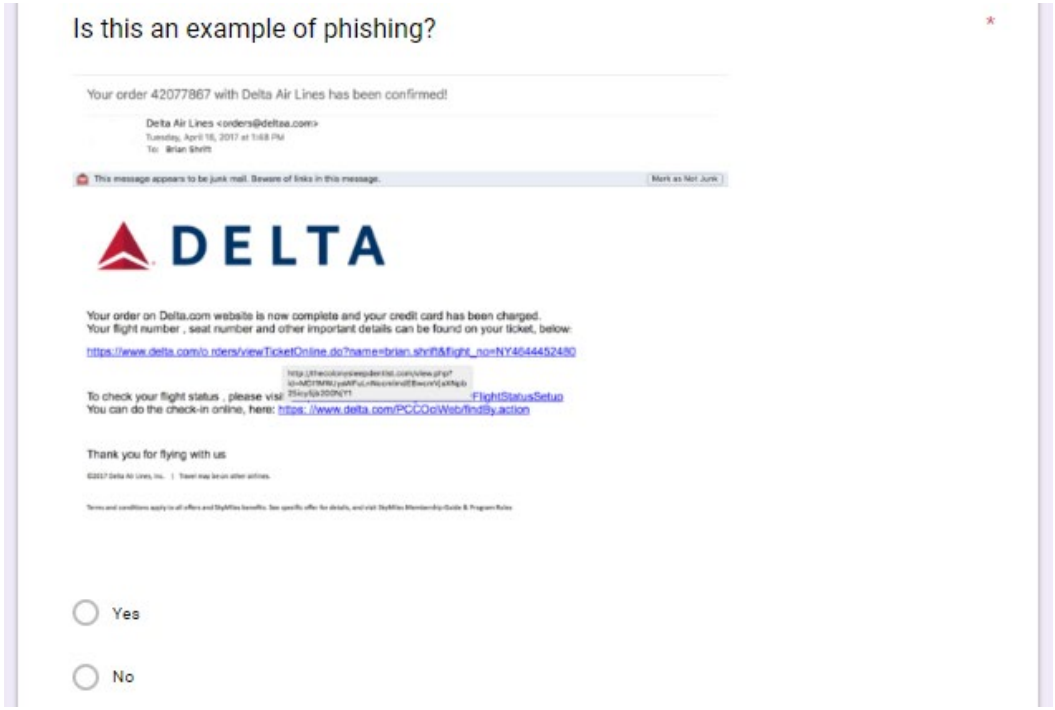


- Yes
- No

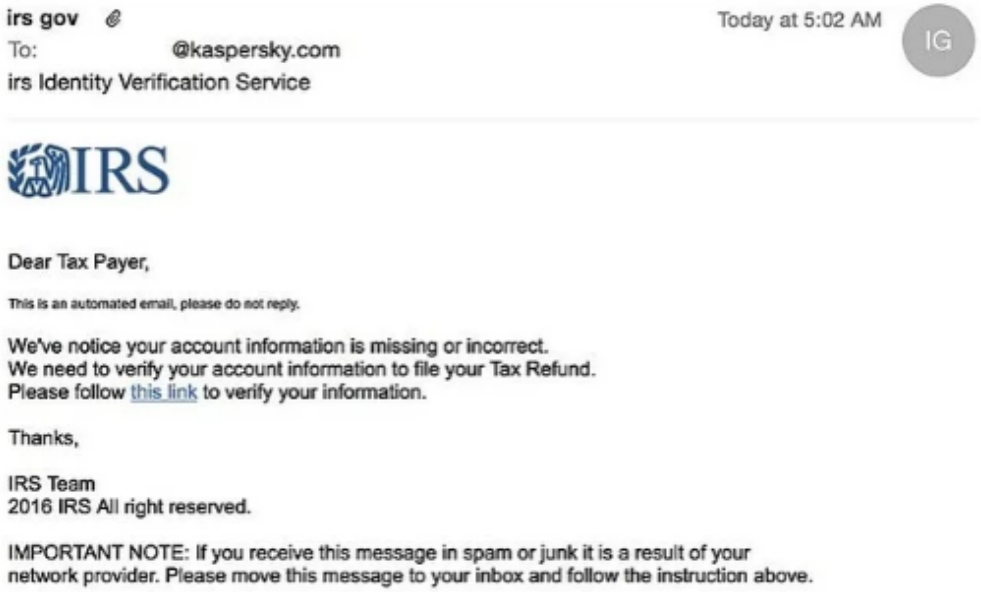

Is this an example of phishing? *
From Netflix <notification+zj462tocfyjc@pausemassagethe...
Subject Payment declined
To
NETFLIX
Payment declined
Hi,
We attempted to authorize the Amex card you have on file but were unable to do so. We will automatically attempt to charge your card again within 24-48 hours.
Update the expiry date and CVV (card verification value) for your Amex card as soon as possible so you can continue using it with your account.
UPDATE PAYMENT
We're here to help if you need it. Visit the Help Centre for more info or contact us.
– Your friends at Netflix
Yes
No
SUBMIT

Appendix D: *Progress Assessment*





Is this an example of phishing? *


irs gov
To: @kaspersky.com
irs Identity Verification Service
Today at 5:02 AM
IG

IRS

Dear Tax Payer,

This is an automated email, please do not reply.

We've notice your account information is missing or incorrect.
We need to verify your account information to file your Tax Refund.
Please follow this link to verify your information.

Thanks,

IRS Team
2016 IRS All right reserved.

IMPORTANT NOTE: If you receive this message in spam or junk it is a result of your network provider. Please move this message to your inbox and follow the instruction above.

- ( ) Yes
- ( ) No

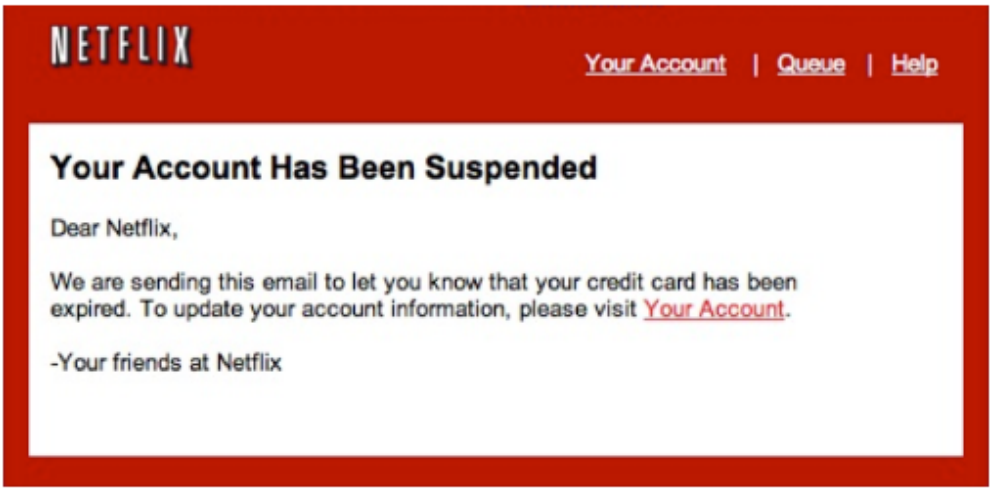
What is spear-phishing? *

- ( ) practice that deals with emails eliciting personal information from a specific group
- ( ) the practice that deals with the retrieval of emails from companies
- ( ) I do not know

What is a prevention method for phishing? *

- ( ) Using email filters
- ( ) Using a Macbook laptop because they don't get viruses
- ( ) I do not know

Is this an example of phishing? *

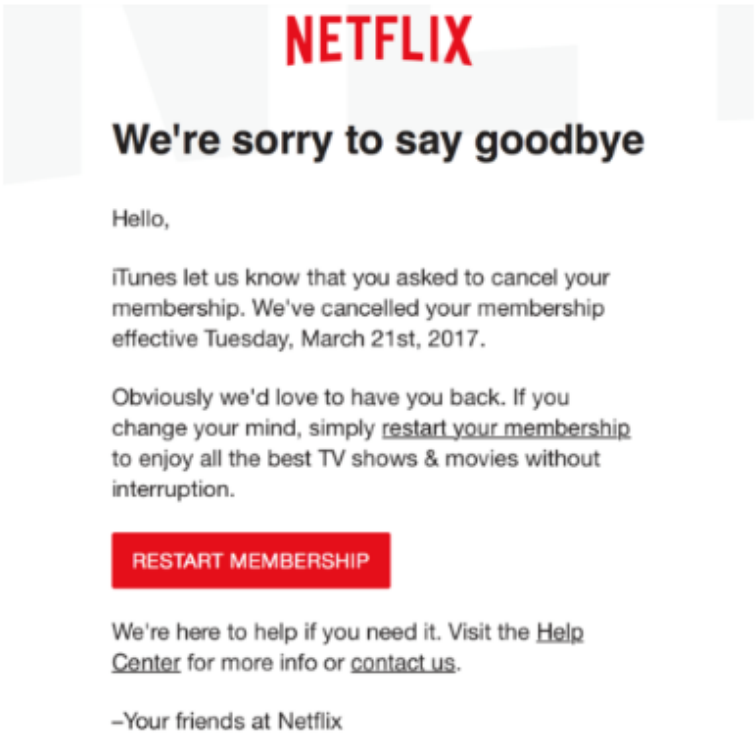


- ○ Yes
- ○ No

When checking the authenticity of an email, a good step to take is to :

- ○ Click on the link provided
- ○ Check the email address of the sender
- ○ I do not know

Is this an example of phishing? *



- ○ Yes
- ○ No