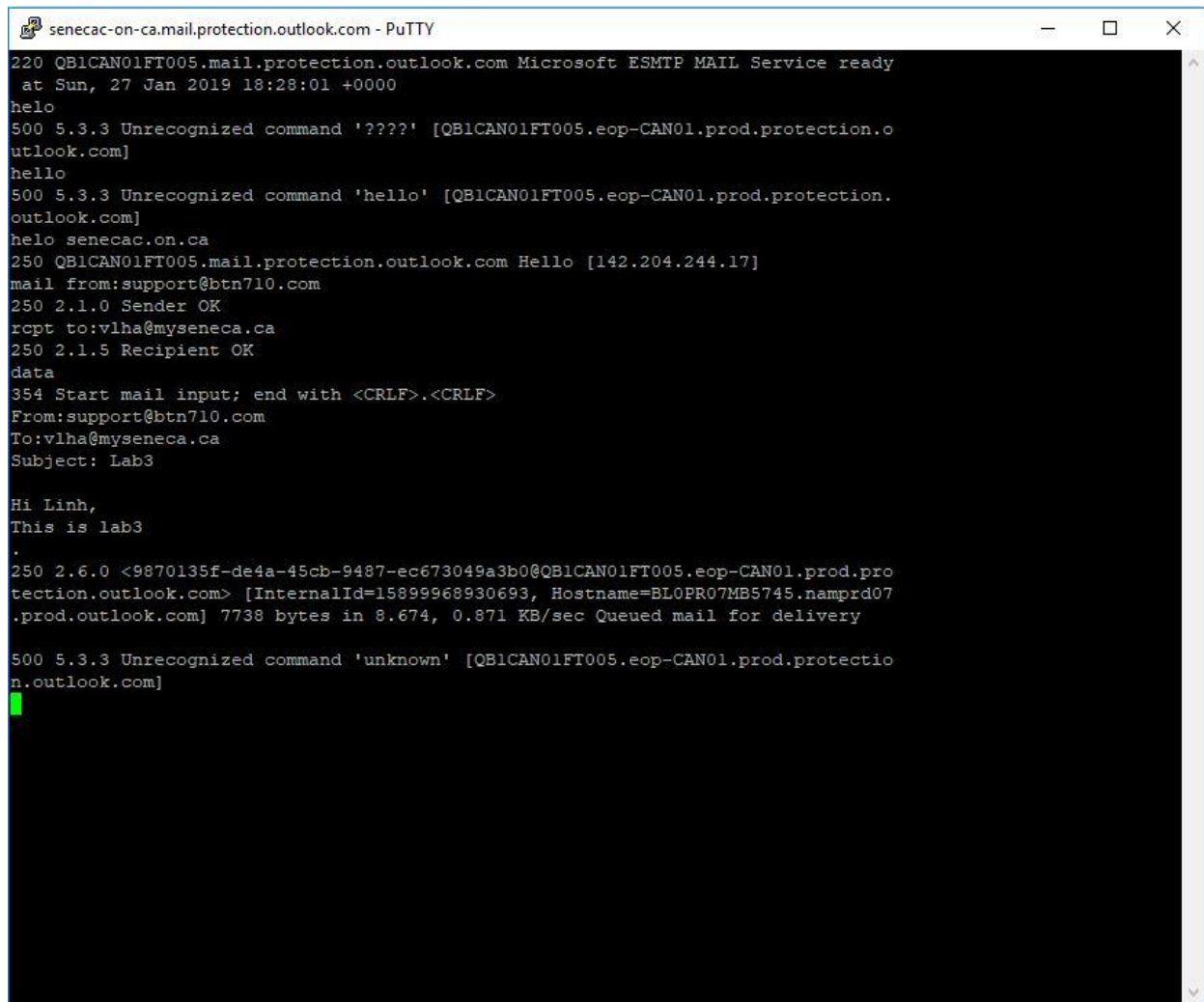


# Lab 3: A Happy Day Phishing

**Name:** Van Linh Ha

**Student Number:** 116592171

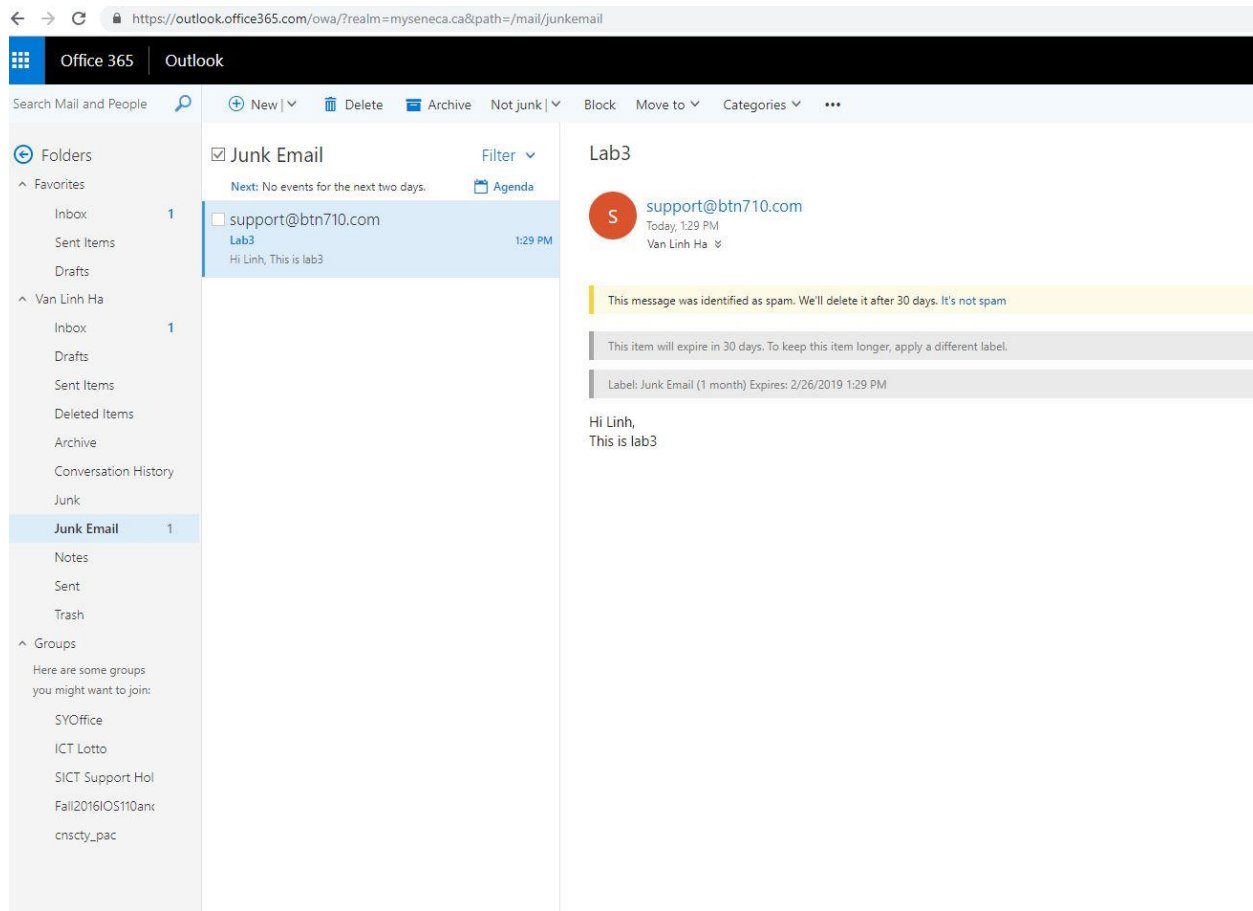
## Part 1: SMTP and Email Headers



```
senecac-on-ca.mail.protection.outlook.com - PuTTY
220 QB1CAN01FT005.mail.protection.outlook.com Microsoft ESMTPL MAIL Service ready
    at Sun, 27 Jan 2019 18:28:01 +0000
helo
500 5.3.3 Unrecognized command '????' [QB1CAN01FT005.eop-CAN01.prod.protection.o
utlook.com]
hello
500 5.3.3 Unrecognized command 'hello' [QB1CAN01FT005.eop-CAN01.prod.protection.
outlook.com]
helo senecac.on.ca
250 QB1CAN01FT005.mail.protection.outlook.com Hello [142.204.244.17]
mail from:support@btn710.com
250 2.1.0 Sender OK
rcpt to:vlha@myseneca.ca
250 2.1.5 Recipient OK
data
354 Start mail input; end with <CRLF>.<CRLF>
From:support@btn710.com
To:vlha@myseneca.ca
Subject: Lab3

Hi Linh,
This is lab3
.
250 2.6.0 <9870135f-de4a-45cb-9487-ec673049a3b0@QB1CAN01FT005.eop-CAN01.prod.pro
tection.outlook.com> [InternalId=15899968930693, Hostname=BL0PR07MB5745.namprd07
.prod.outlook.com] 7738 bytes in 8.674, 0.871 KB/sec Queued mail for delivery

500 5.3.3 Unrecognized command 'unknown' [QB1CAN01FT005.eop-CAN01.prod.protection
.outlook.com]
```



## Part 2: Social Engineering and Phishing

### PHISHING QUIZ

Think you can Outsmart Internet Scammers?

You're a phish-spotting ninja! You correctly identified 14 out of 14 sites in the OpenDNS phishing quiz. You are skilled at spotting even the toughest phishing scams. But beware: cyber criminals are more clever than ever at creating sites that fool even the most experienced phishing detectives. Set up OpenDNS, the world's fastest-growing Internet security and DNS service, and let us take the guesswork out of identifying phishing sites. You can use OpenDNS at [home](#) or at [work](#) and be confident you're always protected, because OpenDNS automatically blocks phishing sites.

Share your results or challenge your friends:

[f](#) [t](#) [✉](#)

**Yahoo! — Phish**

[Find out why](#)

**HSBC — Not a Phish**

**Facebook — Not a Phish**

## **1. Definition**

### **a. Phishing**

- Phishing is the way of cyber attacking where user will be showing a faked email or website, which looks like a legitimate website. When users are using the faked website or email link, it will be redirected all the information that user enters from the keyboard or collected all the cookies or system information. Hacker normally takes user account, bank information, credit card and money.

### **b. Spear phishing**

- Spear phishing is basically email phishing. The point here is email which appear to user will be shown as regular email but from big and popular company or trusted source. According to the trusted or big company email which should have source of the email from the company, but spear phishing is more likely recognizable by using individual email. Hacker can take advantage of less attention of user to easy trick them to click on the link in the email to hack the system and collect information.

### **c. Whaling**

- Whaling is one of another phishing attack which target more on high-position people in the company or people who hold the important position in the group to collect the sensitive data.

## **2. What are the common phishing vectors?**

### **a. Email Phishing**

### **b. Mobile Phishing**

### **c. Cloud Storage Phishing**

**3. What is vishing? Describe how it is carried out. Give examples of successful vishing attacks**

- Vishing is another kind of phishing attack but using voice scams skill. Hacker pretend to be someone who is working at the office or bank or reputed company. Hacker will be using the individual phone call but change Phone ID which will appear on victim screen as official phone number to ask for credit card number, PIN number and all information. In the most successful case, hacker ask victims to provide private credit card number to tell them they need to verify victim's card.

**4. Provide three examples of successful impersonation attacks**

- User in the company receive an email from co-worker with exactly theirs's email address
- User login to company website but after logged in, all the information are gone because of the hacker faked company website to collect user information
- A victim get a call from someone who is pretending to be an officer company to ask them about credit card information.

**5. What is SMiShing? Provide three examples of successful SMiShing attacks**

- User receive an email with the link attached, when user click on to the link, it requires to download a software or package which contains virus or Trojan. The computer will be collecting information automatically and can be controlled by hackers. The computer will become a part of bot network and can be used to attack another Server by using DDOS attack.

**6. How can we protect ourselves against common attacks?**

- Always update software from the provider
- Have a good virus scan software: Windows Defend, Avira, Esec...
- Understand some common scams to avoid being hacked
- Using strong password and never share to anyone
- Encrypt data and using VPN for secure transaction