Lab/Hands-on Project 1: Dealing with Phishing E-Mails

**Please do the following:**

1. Read the entire document below and the Module 1 assigned course material.
2. Answer the lab questions (starting on page 15) using this document. To answer each lab question, first select your answer by checking the correct box and provide a brief/one-sentence reason for your answer.
3. Save your document as lab\_hands-on project\_1\_yourfirstName.lastname) and submit it here in this assignment folder

Table of Contents

[Objective 2](#_Toc62829266)

[Estimated Completion Time 2](#_Toc62829267)

[Materials Required 2](#_Toc62829268)

[Introduction 2](#_Toc62829269)

[Common Methods to Identify Phishing Attacks 3](#_Toc62829270)

[Legitimate Messages Don’t Request Sensitive Information 3](#_Toc62829271)

[Legitimate Messages Usually Call You by Your Name 4](#_Toc62829272)

[Legitimate Messages Come from Authentic Domains 5](#_Toc62829273)

[Legitimate Messages Come from People Who Know How to Spell and Write 5](#_Toc62829274)

[Legitimate Messages Don’t Force You to a Web Site 6](#_Toc62829275)

[Legitimate Messages Don’t Include Unsolicited Attachments 7](#_Toc62829276)

[Legitimate Messages Have Links that Match Legitimate URLs 8](#_Toc62829277)

[Legitimate Messages Don’t Create an Artificial Sense of Urgency 9](#_Toc62829278)

[Legitimate Messages Display Reliable Names 10](#_Toc62829279)

[Legitimate Messages Don’t Solicit Money 11](#_Toc62829280)

[How You Should Respond 13](#_Toc62829281)

[Test Your Knowledge 14](#_Toc62829282)

[Example 1 14](#_Toc62829283)

[Example 2 15](#_Toc62829284)

[Example 3 15](#_Toc62829285)

[Example 4 16](#_Toc62829286)

[Example 5 16](#_Toc62829287)

[Example 6 17](#_Toc62829288)

[Example 7 17](#_Toc62829289)

[Example 8 18](#_Toc62829290)

[Example 9 18](#_Toc62829291)

[Example 10 19](#_Toc62829292)

# Objective

Upon completion of this activity, you will be able to identify several types of social engineering attacks that use phishing techniques.

# Estimated Completion Time

If you are prepared, you should be able to complete this lab in 60 to 75 minutes.

# Materials Required

No additional materials are required to complete this lab.

# Introduction

Social engineering is a term to describe malicious actions that exploit human psychology to gain access to sensitive information or money. Attackers manipulate people through dishonest social interactions and exploit the human tendency to trust in an effort to gather valuable information.

Phishing is a popular form of social engineering attack in which an attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information. E-mails with corrupted attachments or poisoned links that redirect users to malicious Web sites are among the common attack vectors used in phishing.

The best defense against e-mail phishing attacks is user awareness. Many organizations now filter employee e-mail using commercial products, but even the best of these products will not stop every phishing e-mail. Having an alert workforce and a trained service support staff are also required.

In this lab, you will first read about the indicators that an e-mail is actually a phishing attack. Next, you will assume the role of a help-desk analyst who is responding to alerts from users that have received suspicious e-mails.[[return to top]](#_top)

## Common Methods to Identify Phishing Attacks

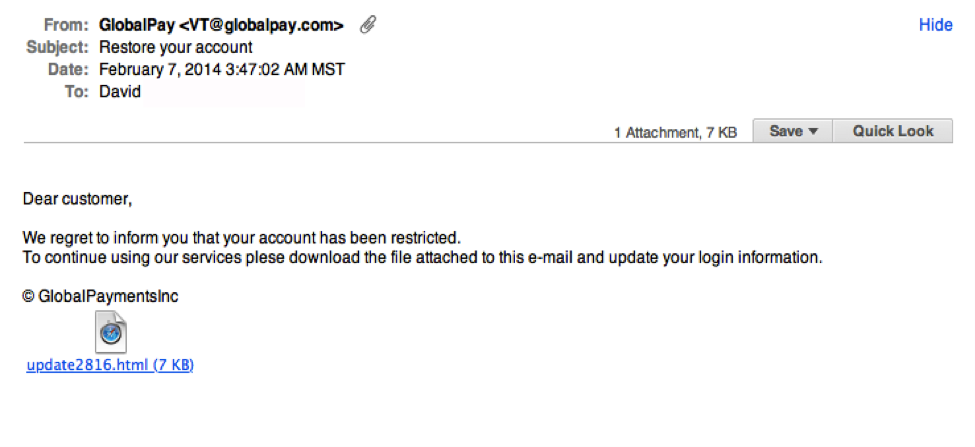
The following questions indicate some of the telltale signs of phishing attacks. In general, you should ask yourself these questions for each e-mail you receive:

* Does the message ask for sensitive information, such as account numbers, passwords, or even your birthday?
* Does the message use your correct name and refer to other details accurately?
* Does the address look authentic?
* Are there misspelled words and improper grammar?
* Does the message force you to a Web site?
* Does the message have an attachment you are not expecting?
* Do links in the message fail to match the visible URL?
* Does the message request that you send money?

Each of these questions is explained with examples in the following sections.

### Legitimate Messages Don’t Request Sensitive Information

If you receive an unsolicited e-mail that appears to be from an official institution and the message includes a functional link or attachment, it’s a scam. Most companies do not send e-mail asking for passwords, credit card information, credit scores, or tax numbers, nor do they send log-in links. If a company needs information, you will usually be asked to visit its Web site or mobile app, but you should not need a special e-mail link—after all, you do business with the company already.



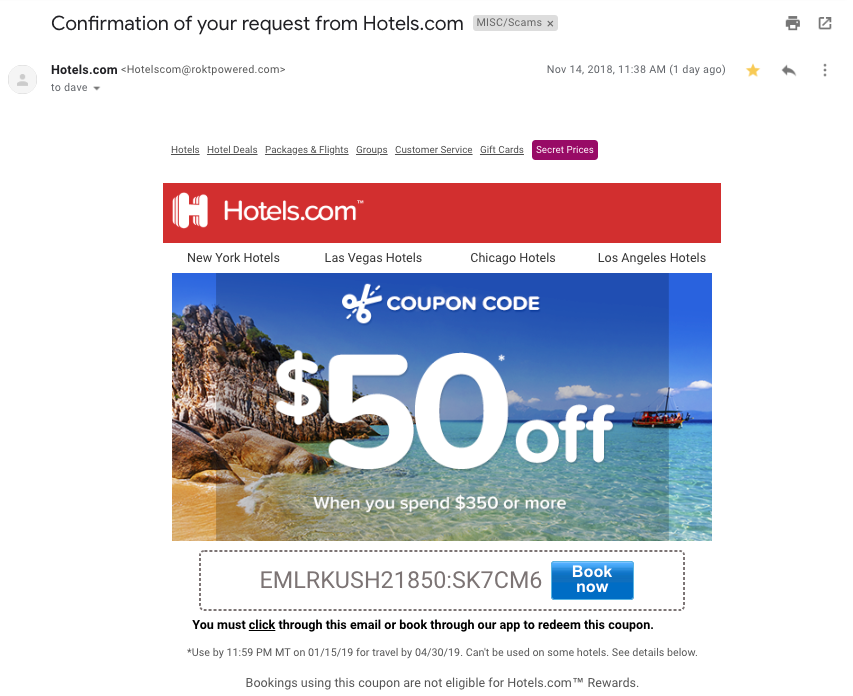
**Figure 3-1**

In Figure 3-1, notice the unsolicited Web link attachment. Also, look at the generic salutation at the beginning (“Dear customer”). Such greetings are discussed next.

### Legitimate Messages Usually Call You by Your Name

Phishing e-mails typically use generic salutations such as “Dear valued member,” “Dear account holder,” or “Dear customer.” If a company you deal with actually required information about your account, the e-mail would refer to you by name and would probably direct you to contact the company via phone, a phone app, or the official company Web site.

However, some hackers simply avoid a salutation altogether. This is especially common with advertisements. In the phishing e-mail shown in Figure 3-2, everything is nearly perfect. So, how would you spot it as suspicious?

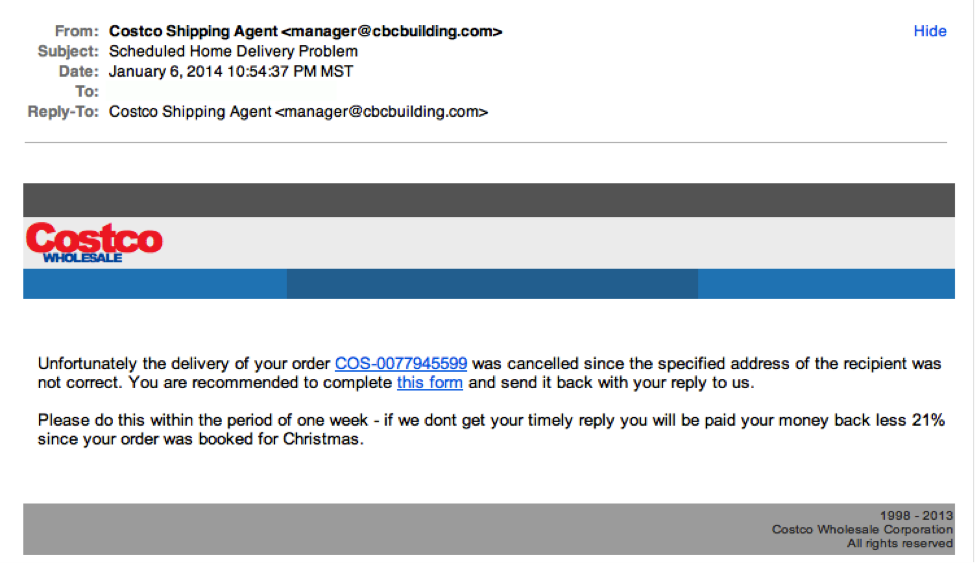


**Figure 3-2**

The example in Figure 3-2 is very convincing, but the fact that the message has the recipient’s name spelled correctly does not make it legitimate. The clue that the message is not legitimate is indicated by the e-mail domain, as you will learn next.

### Legitimate Messages Come from Authentic Domains

Don’t just check the name of the person who sent you the e-mail. Check the e-mail address by hovering your mouse over the contents of the From line. Make sure there have been no alterations, such as additional numbers or letters. For example, be suspicious if the e-mail address appears to be [*michelle@paypal.com*](mailto:michelle@paypal.com) but is [*michelle@paypal23.com*](mailto:michelle@paypal23.com) when you hover the mouse over the From line. This isn’t a foolproof method of demonstrating fraud, however. Some companies make use of varied domains to send e-mails, and some smaller companies use third-party e-mail providers.



**Figure 3-3**

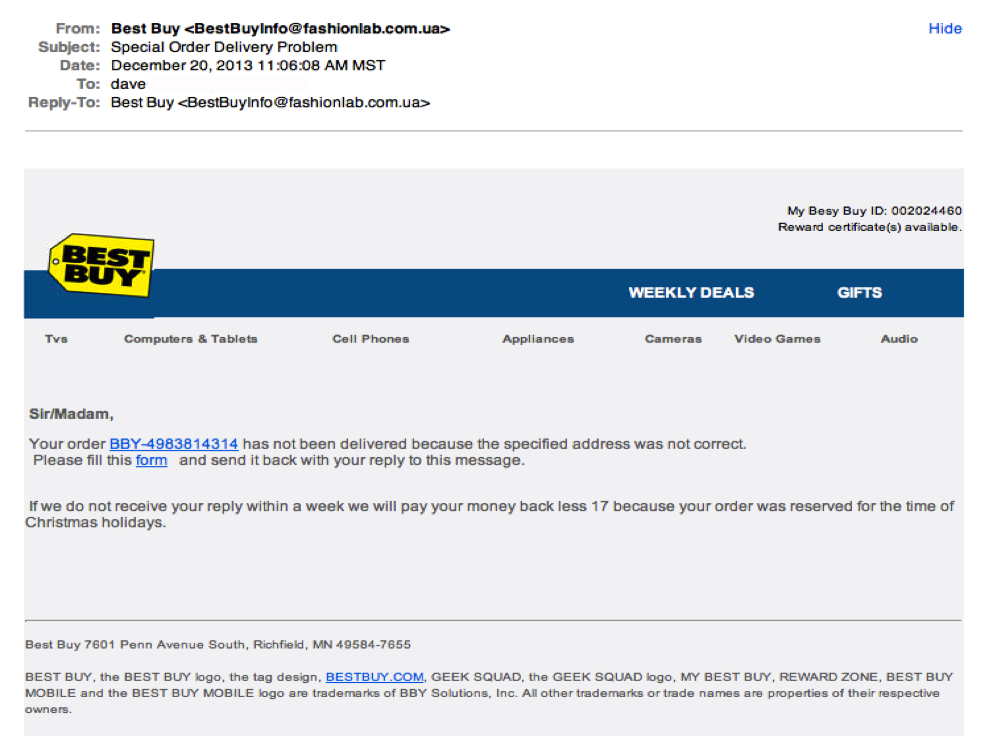
In the example shown in Figure 3-3, the Costco logo is just a bit off. To see the actual logo, you can go to [*https://costco.com*](https://costco.com). Do you see the difference?

Also, note that most companies use the *https://* service in their URLs. If the “s” is missing, dig a little deeper.

### Legitimate Messages Come from People Who Know How to Spell and Write

Possibly the easiest way to recognize a suspicious e-mail is through its use of bad grammar and misspelled words. An e-mail from a legitimate organization is usually well written.

Look at this example below:

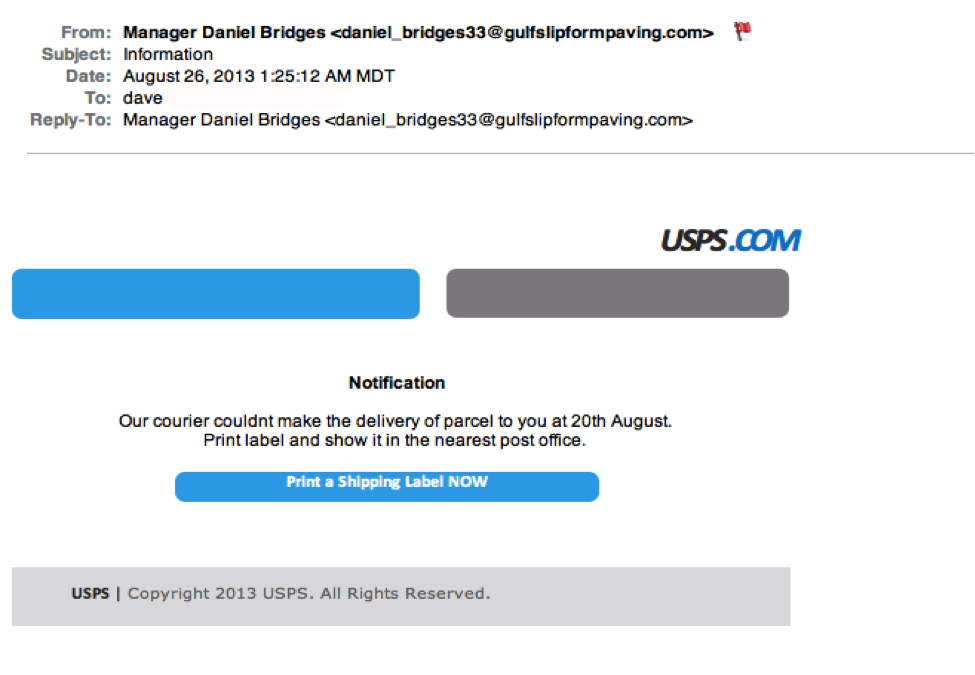


**Figure 3-4**

In addition to the generic salutation in Figure 3-4, the grammar gaffes are a good clue that something is wrong—for example, note the sentence that begins “Please fill this form.” Also, notice the “17” that appears in the middle of the next sentence for no reason.

### Legitimate Messages Don’t Force You to a Web Site

Phishing e-mails are sometimes coded so that the entire message is a graphic image tagged as a hyperlink. Clicking anywhere in the e-mail will open a fake Web page or download malware, ransomware, or spam to your computer. For this reason, you must be careful and deliberate when performing analysis on suspect e-mails. If you click or activate the attachment, it can infect your system. You will need tools to render the attachment or headers harmless without activating the trap. Right-clicking your mouse and using basic tools can be very helpful.



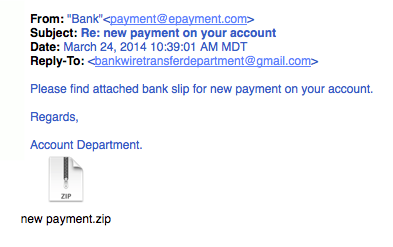
**Figure 3-5**

The entire e-mail shown in Figure 3-5 was sent as an image tagged as a single hyperlink. If a recipient clicked anywhere in the e-mail, a malicious attack would be initiated. You can guard against this by hovering your mouse cursor over the message to see if a link address preview appears.

### Legitimate Messages Don’t Include Unsolicited Attachments

Unsolicited e-mails that contain any type of attachment should make you suspicious. Typically, authentic institutions do not randomly send you e-mail with attachments, but instead direct you to download documents or files from their secured Web site.

Like many of the other tips in this lab, this method isn’t foolproof. Companies that already have your e-mail address sometimes send you information, such as a white paper, that may require a download. In that case, be on the lookout for high-risk attachment file types, such as .exe, .scr, and .zip. Even .pdf and .docx files are suspicious. If you think the e-mail might be legitimate but you have doubts, contact the sender directly using information obtained from a source other than the e-mail.

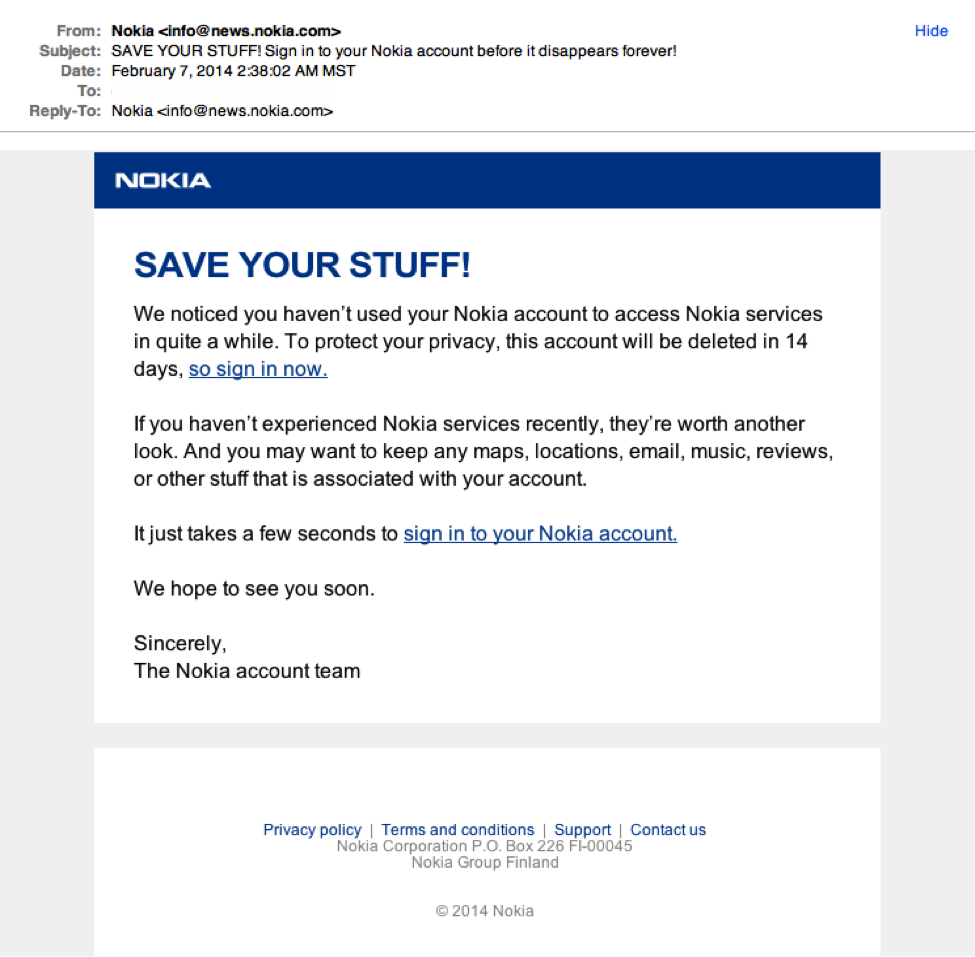


**Figure 3-6**

Before you wonder what’s in the .zip file attached in Figure 3-6, remember that curiosity killed the cat.

### Legitimate Messages Have Links that Match Legitimate URLs

If an e-mail appears to be suspicious, take precautions with any Web links in the message. Make a habit to always double-check URLs. If the link in the text isn't identical to the URL displayed when you hover the mouse cursor over the link, that's a sure sign you will be taken to a site you don’t want to visit. If a hyperlink’s URL doesn’t seem correct or doesn’t match the context of the e-mail, don’t trust it. Instead, use your Web browser to find the company’s authentic Web site. To help ensure security, hover your mouse over an embedded link (without clicking!), confirm that it begins with *https://*, and consider whether the rest of the link looks like what you might expect.



**Figure 3-7**

Although the preceding message looks convincing, Nokia wouldn't actually send a "Save your stuff" e-mail from *info@news.nokia.com*. A mouse flyover of the link would show a domain you should not trust.

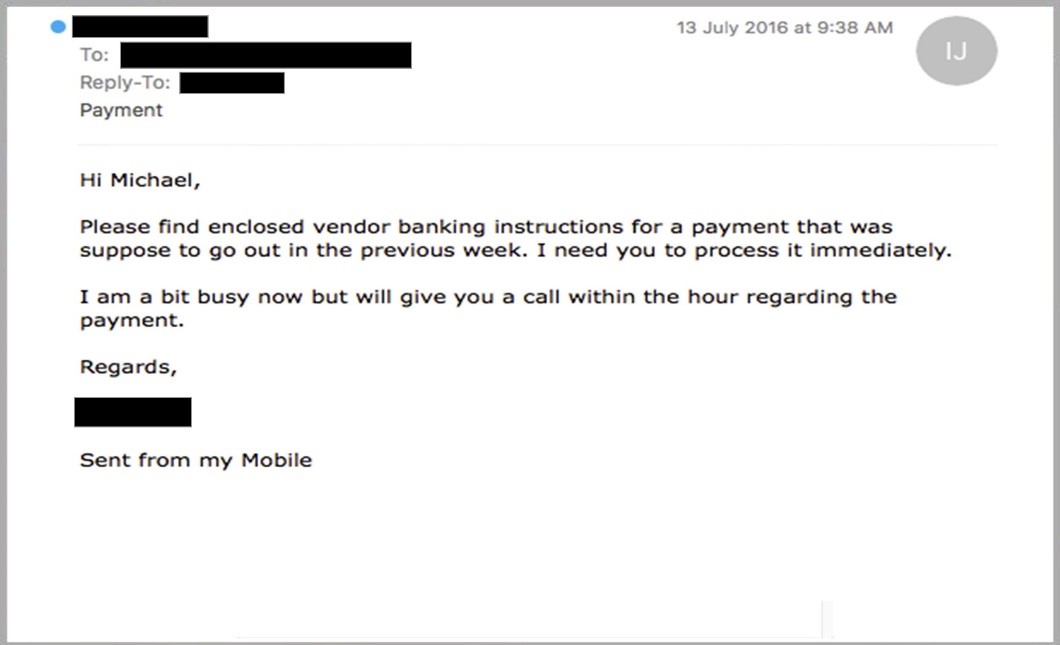
### Legitimate Messages Don’t Create an Artificial Sense of Urgency

Scammers know that most of us procrastinate and then have to get things done in a hurry, so many phishing attempts request that we act now before it’s too late. Scammers also understand that crises in the workplace are common and must be handled quickly. Unfortunately, hurrying creates a greater chance of making mistakes and bad choices.

When you take time to think about something, you are much more likely to notice things that don’t seem quite right. For instance, when you receive an unexpected e-mail from a major company, maybe you’ll think twice and realize that the organization has never contacted you via e-mail. Maybe you’ll receive what appears to be a frantic e-mail from a co-worker and realize that he simply would have called you in case of an actual emergency.

A common workplace scam is to pretend that a problem has arisen with a commonly used service or account, such as that with a bank or credit card company an organization uses. Any actual problems with such accounts would cause an immediate inconvenience. Criminals know we’re likely to drop everything if our boss e-mails us with a vital request, especially when other senior colleagues are supposedly waiting for us to act.

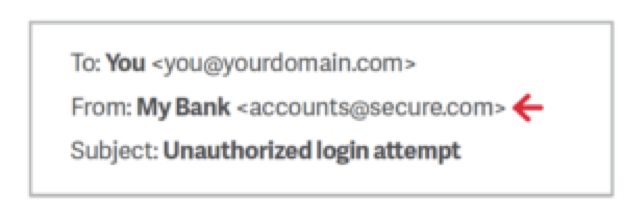
A typical example looks like Figure 3-8.



**Figure 3-8**

### Legitimate Messages Display Reliable Names

A favorite phishing tactic among cybercriminals is to spoof the display name of an e-mail, just like robocalling telemarketers can spoof your phone’s caller ID. For example, if a fraudster wanted to impersonate your bank, the top of the e-mail message might look like Figure 3-9. Check out the domain name (in the example, [*accounts@secure.com*](mailto:accounts@secure.com)) to see if it matches the display name (My Bank).



**Figure 3-9**

### Legitimate Messages Don’t Solicit Money

Many successful phishing attacks create a false sense of urgency or appeal to a person’s greed. One type of scam that attempts to exploit greed is the advance fee fraud, which uses confidence tricks and is much older than e-mail. This approach typically involves promising the victim a significant share of a valuable prize, a desired business objective, or a sum of money in return for a small, up-front payment. This payment is needed to obtain the larger sum—hence the name “advance fee fraud.”

One of the best-known frauds is the Nigerian 419 scam, which has been around for a long time. Originally conducted via phone, fax, and traditional mail, this scam invites victims to send a small amount of money with the promise of receiving a much larger sum in return. The development of e-mail has made it much easier for scammers to reach new victims. The best-known source of these e-mail scams is Nigeria, although they can originate from anywhere. In Nigeria, the e-mails have become a significant source of income for some, although section 419 of the Nigerian legal code prohibits them (hence the name).

A typical Nigerian 419 scam begins with a potential victim opening a letter or e-mail that’s purportedly from a famous person or an exiled politician. The person may claim to be from a place that’s currently in the news, possibly because of a recent civil disturbance. The message explains that, due to political instability or the death of a relative, a significant amount of money is trapped in some form of escrow account. The message goes on to explain that if the reader could send just a small amount of cash, it will pay the fee needed to access the account. In return for their trust and generosity, the reader is promised a large percentage of the money that’s locked away.

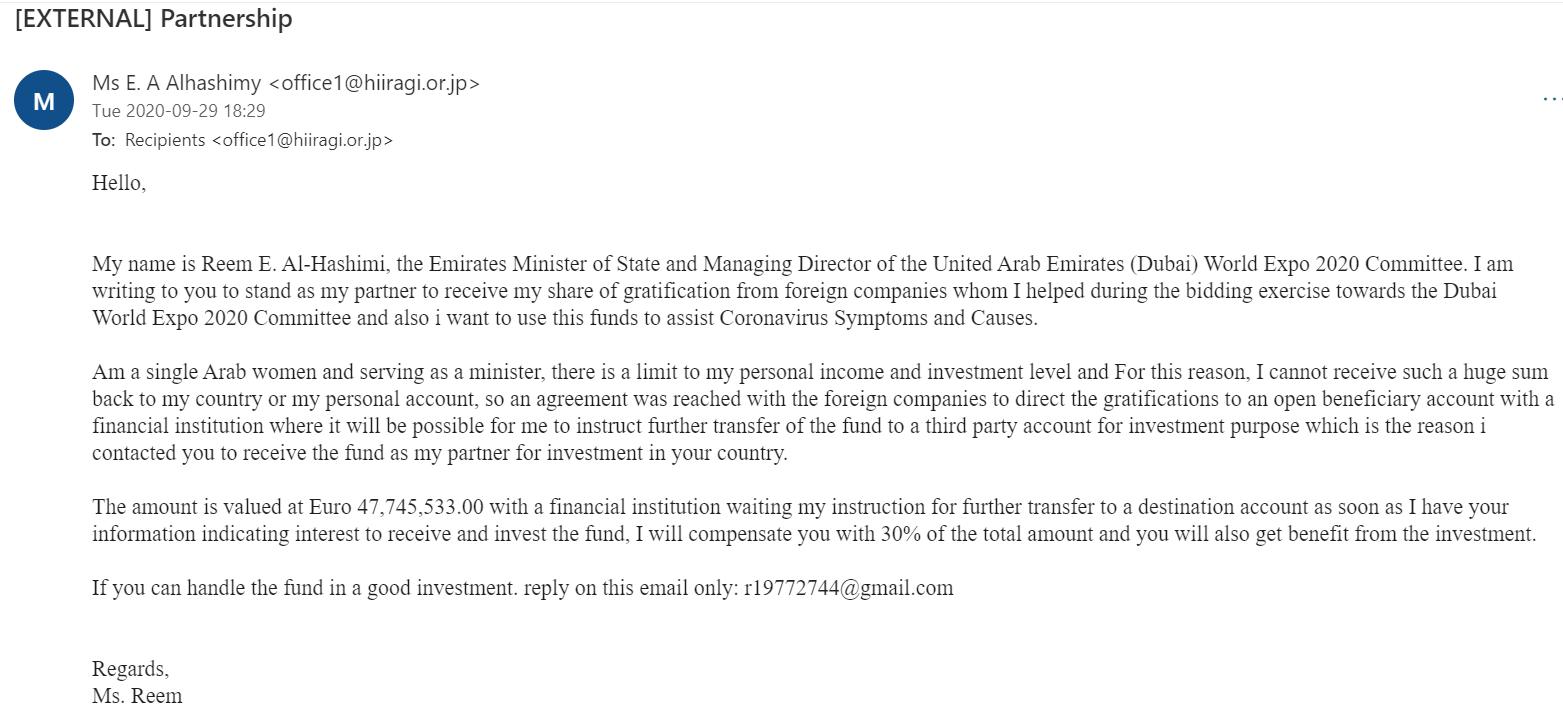
If the reader does decide to send money, more requests will follow. According to subsequent e-mails sent by the scammer, unexpected costs are often discovered, such as increased taxes or bribes to officials. The scammers will continue to ask for money as long as the victim sends it. Needless to say, victims will never receive a payout, regardless of how much money they send.

A variant of the 419 attack involves vendors that supposedly sell products or rent accommodations online. A fraudster first identifies a company from a foreign country that offers to buy a product, rent a property, or contract a service. The fraudster then sends the victim a fake check or international money order for a much greater amount than the item or activity is worth, along with an explanation for why they cannot pay a smaller amount. The fraudster asks the victim to deposit the money in a personal bank account and then transfer the overage back to the fraudster. Later, of course, the victim discovers the swindle and that the original “payment” was fake.

These types of scams have some common traits:

* The message (usually an e-mail) is unexpected.
* You don’t know the sender.
* There is a long, sad story about why the sender needs your help to access money.
* You are asked to help by transferring funds.
* A large payment is offered in exchange for assistance.

The examples of advance fee fraud are many and varied; they include investment proposals, lottery winnings, and online dating scams. The example shown in Figure 3-10 is fairly typical.



**Figure 3-10**

## How You Should Respond

The easiest response to suspected phishing e-mails is to delete them. Most larger organizations have automated filters in place to catch phishing attempts. Most companies also offer staff assistance to deal with such e-mail, and offer an account like [*abuse@yourcompany.com*](mailto:abuse@yourcompany.com) where you can send suspicious messages. Many organizations have a Web resource that explains examples of current phishing messages that are making the rounds; this resource helps users stay abreast of emerging threats in social engineering. At Kennesaw State University in Georgia, the resource is called the phishmarket. You can see it at [*https://uits.kennesaw.edu/ocs/phish-market/index.php*](https://uits.kennesaw.edu/ocs/phish-market/index.php)*.*

When dealing with suspicious e-mail, the best advice is to be skeptical. Phishers are good at what they do. Many malicious e-mails include convincing brand logos, persuasive language, and a seemingly valid e-mail address. However, if an e-mail message looks even remotely suspicious, do not open it. If the message seems too important to ignore and you cannot easily toss it away, try to follow up using resources you can find that are NOT in the e-mail. Go to the sender’s Web site or call the colleague who allegedly sent you the attachment or urgent request. If the original message was valid and urgent, the sender will appreciate your follow-up.

You should report fraudulent e-mail and other types of social engineering attacks. If you work for a company, contact the help desk or the information security team. For suspicious e-mails sent to your personal account, your e-mail provider or ISP may be able to help you. After evaluation, the company’s technical support team should follow up to ensure that the e-mail was deleted and no losses occurred. If you fall victim to a phishing attack, get help as soon as possible because lost time can factor into the ability to recover losses. If the attack involved a bank or a credit card company, or if you have an identity protection service (like LifeLock), get them involved as soon as you can.

When dealing with phishing attacks, it does not matter if your organization has the most secure security system in the world. It takes only one untrained employee to be fooled and give away data your organization has worked hard to protect. Make sure that you and your co-workers understand the examples illustrated in this lab so you can detect the telltale signs of a phishing attempt.

## Lab Assignment Questions & Submission Instructions

Now let’s test your knowledge. Imagine that you are a help-desk analyst reading your organization’s abuse e-mail account as co-workers send in suspicious messages. Take a look at each of the following messages and then determine whether you think they are legitimate or suspicious. For each suspicious message, explain why you think it fails the “smell test.”

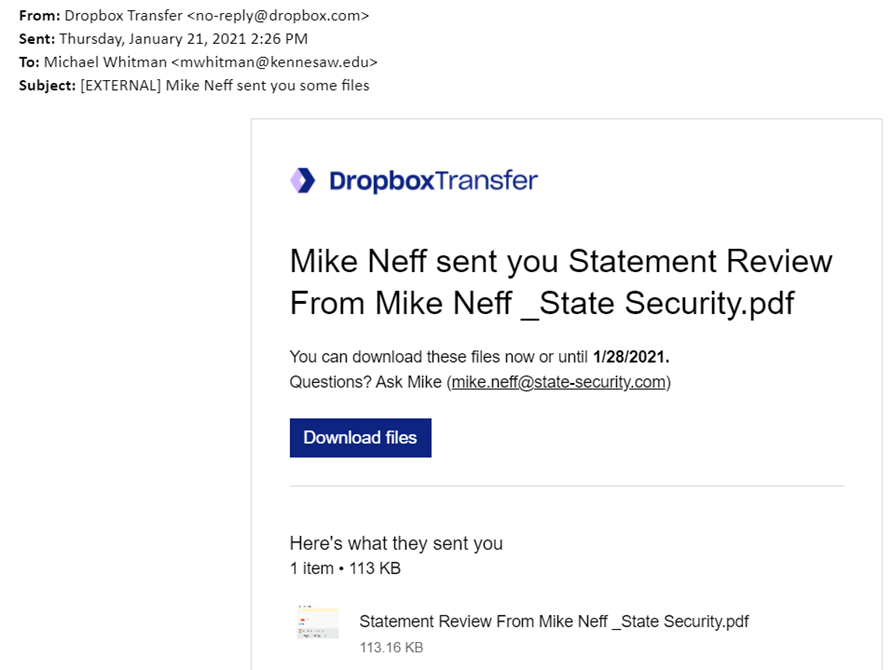
Here is a handy list you can use when evaluating each of the following example e-mails:

* The message asks for sensitive information.
* The message does not contain your correct name; other details are incorrect as well.
* The address does not look authentic.
* There are misspelled words and improper grammar.
* The message forces you to a Web page.
* The message has an attachment that is not expected.
* Links in the message seem suspicious.
* The message requests that you send money.

**Please do the following:**

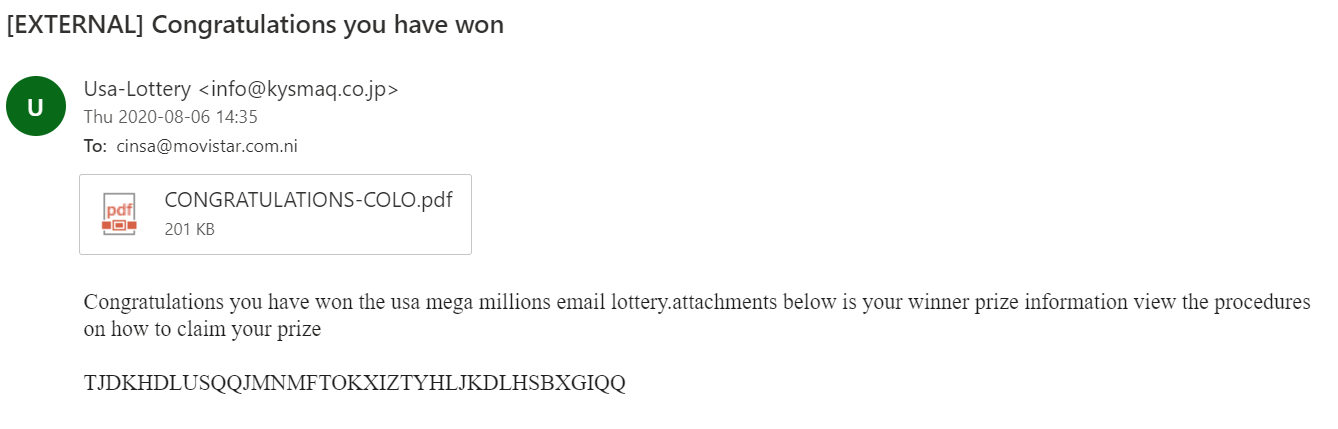
1. Read the entire document and the Module 1 assigned course material.
2. Answer the lab questions starting on the next page. To answer each lab question, first select your answer by checking the correct box and provide a brief/one-sentence reason for your answer. Each question is worth 5 points.
3. Save your document as lab\_hands-on project\_1\_yourfirstName.lastname) and submit it here in this assignment folder

### Example 1



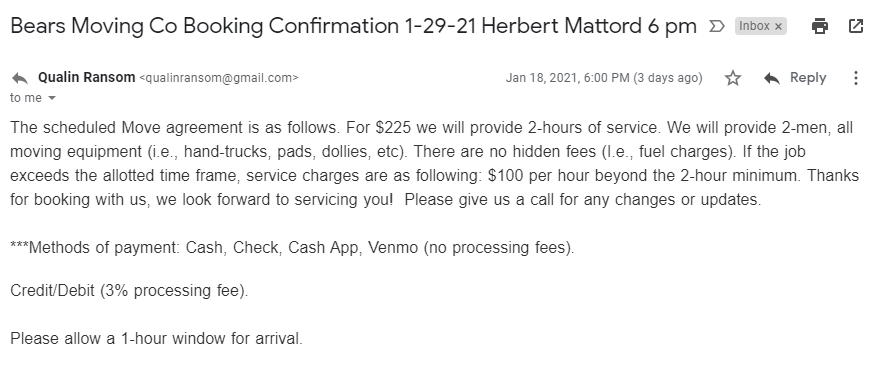
|  |
| --- |
| **Example 1 Response:**  Trustworthy  Suspicious  Reason: The sender’s address does not look authentic. The message forces one to email another person. The email seems to be an image rather than a typed email. |

### Example 2



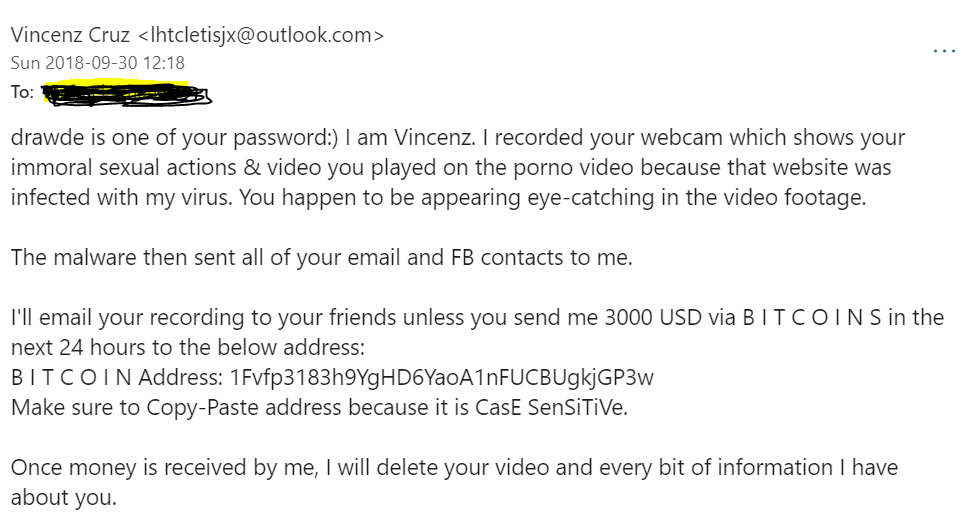
|  |
| --- |
| **Example 2 Response:**  Trustworthy  Suspicious  Reason: There are misspelled words and improper grammar. (“lottery.attachments”). (‘usa’) is in small letters instead of capitalized. Links in the message seem suspicious. The address doesn’t look authentic. |

### Example 3



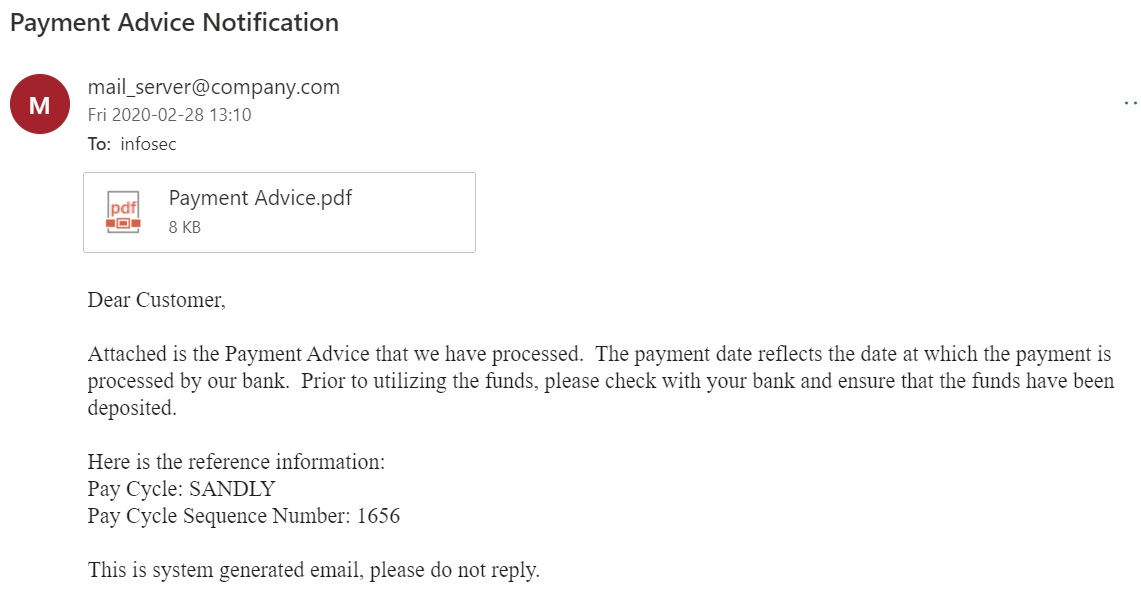
|  |
| --- |
| **Example 3 Response:**  Trustworthy  Suspicious  Reason: The address doesn’t look authentic. (It doesn’t have a company domain). There are misspelled words and improper grammar. No contact information for the company. |

### Example 4



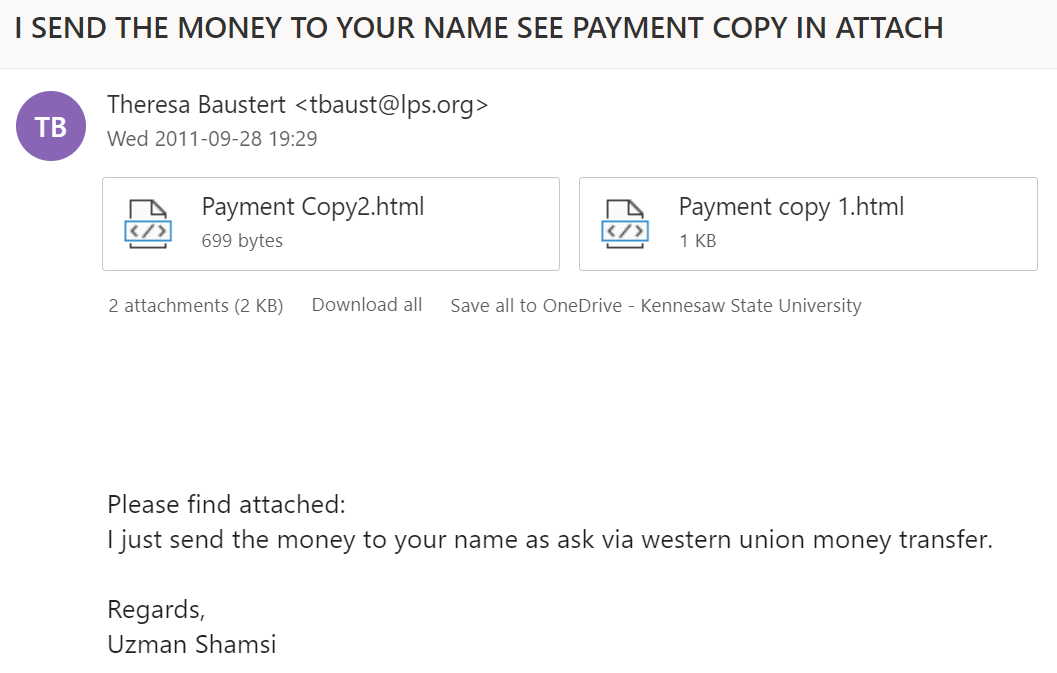
|  |
| --- |
| **Example 4 Response:**  Trustworthy  Suspicious  Reason: There are misspelled words and improper grammar. The message requests that you send money. The message forces you to a Web page. The sender’s email link is not authentic. Links in the message seem suspicious. The message does not contain your correct name; other details are incorrect as well. |

### Example 5



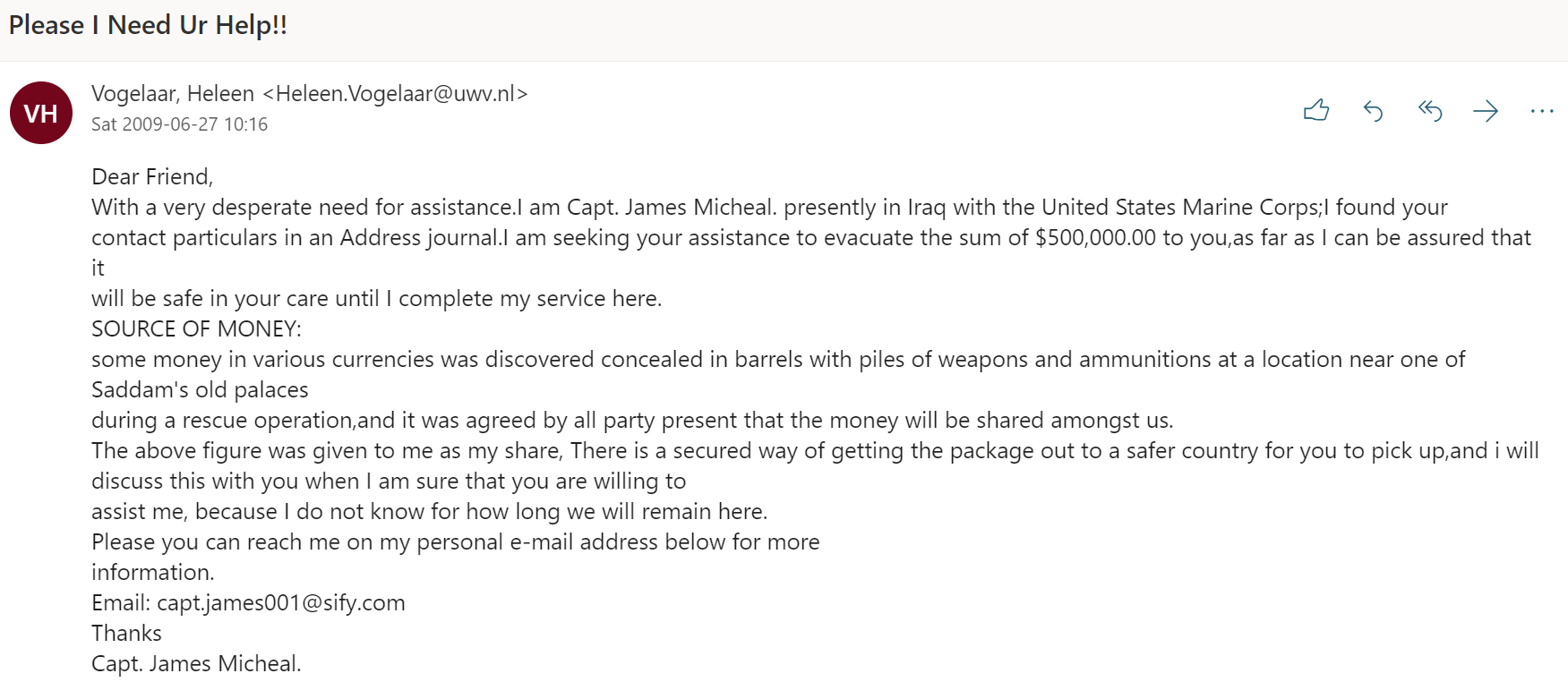
|  |
| --- |
| **Example 5 Response:**  Trustworthy  Suspicious  Reason: The email doesn’t contain the customer’s name. It is a general email rather than a personal one.  The message has an attachment that is not expected. Has reference information that is normally not needed. |

### Example 6



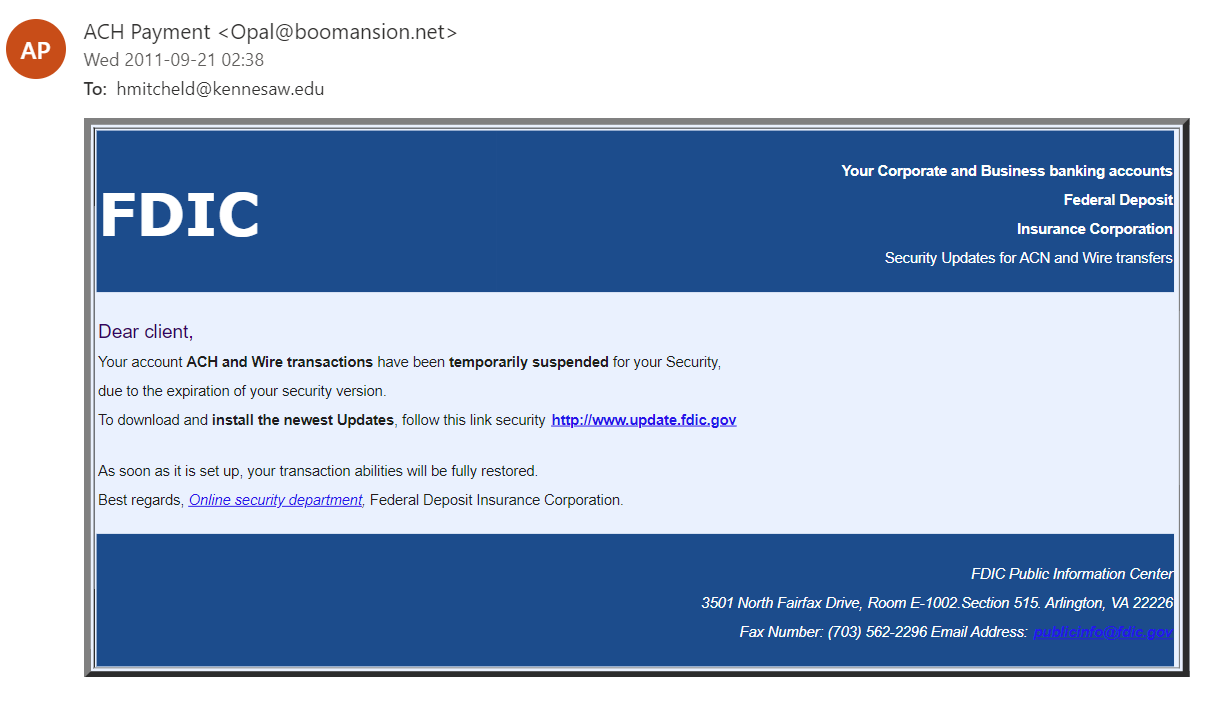
|  |
| --- |
| **Example 6 Response:**  Trustworthy  Suspicious  Reason: There are misspelled words and improper grammar. The message has an attachment that is not expected. Links in the message seem suspicious. The address doesn’t look authentic. |

### Example 7



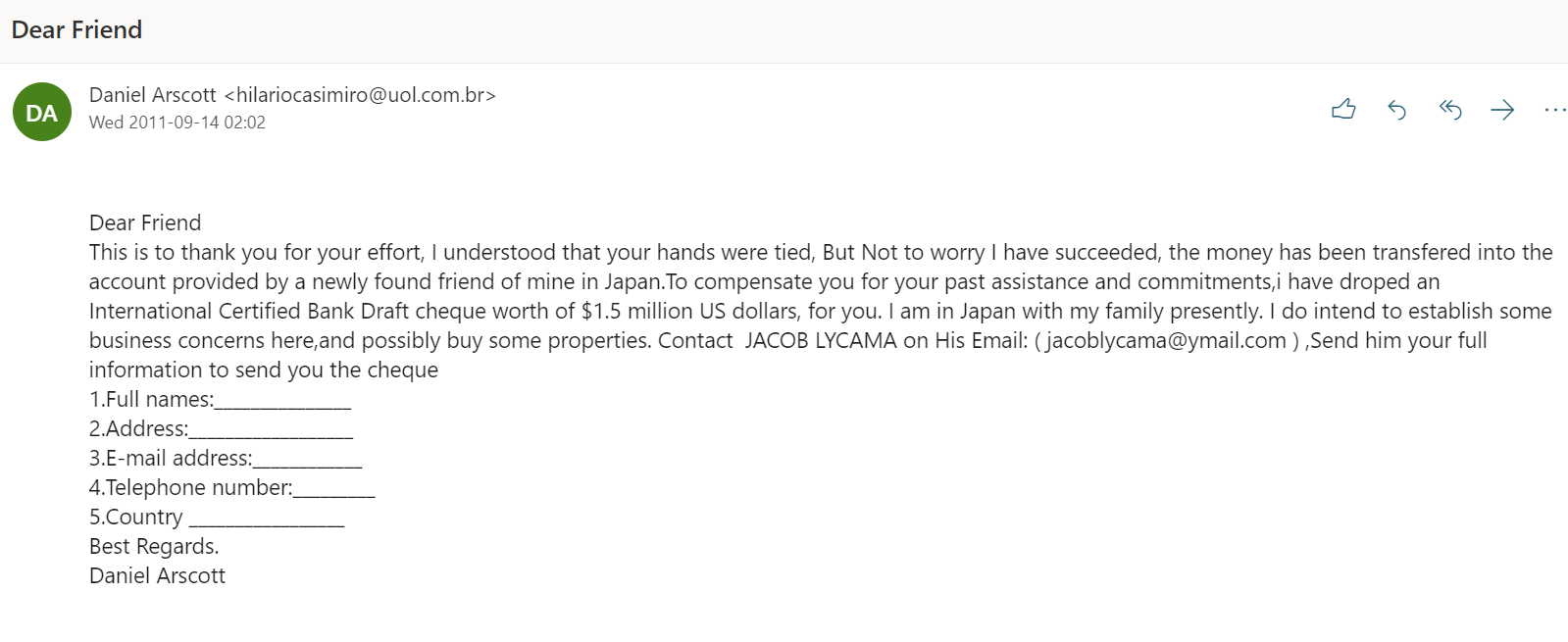
|  |
| --- |
| **Example 7 Response:**  Trustworthy  Suspicious  Reason: The message does not contain your correct name; other details are incorrect as  well. Has an extra email to reach out to that is different from the sender’s email. It requests that one may end up sending money. The email is general and not personal as it refers to the receiver as “friend”. There are misspelled words and improper grammar. |

### Example 8



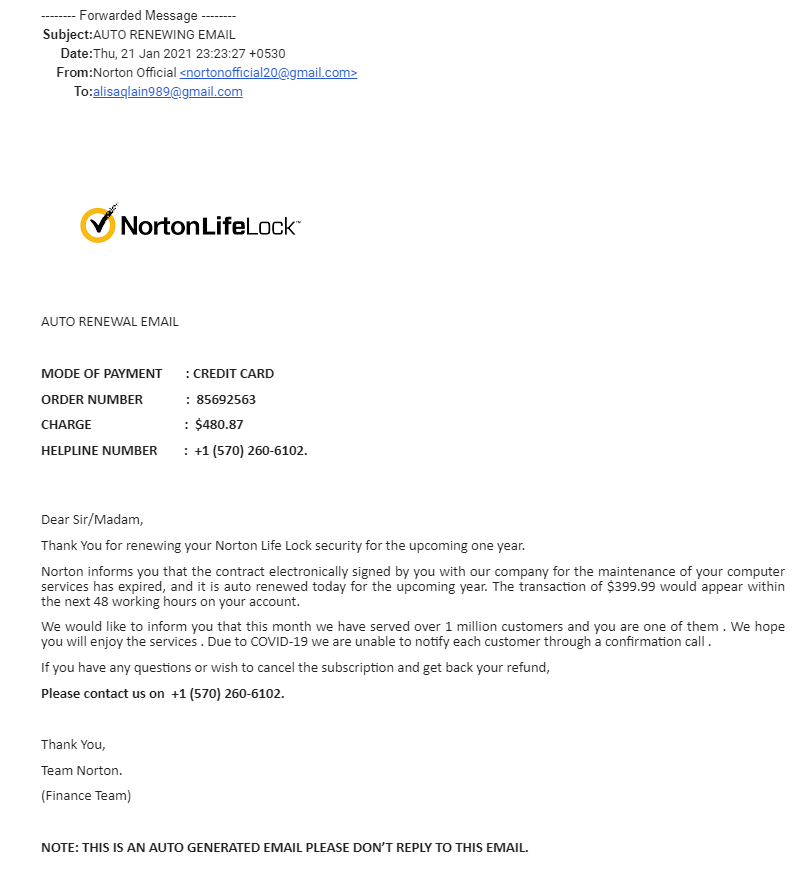
|  |
| --- |
| **Example 8 Response:**  Trustworthy  Suspicious  Reason: The email is a photo and not the actual words. The email address of the sender doesn’t seem legitimate. The email is general as it refers to the receiver as “client”. The senders’ email address and the referred email address are different. |

### Example 9



|  |
| --- |
| **Example 9 Response:**  Trustworthy  Suspicious  Reason: The message does not contain your correct name; other details are incorrect as  well.  There are misspelled words and improper grammar. The message requests that you send your information. The address doesn’t look authentic. |

### Example 10



|  |
| --- |
| **Example 10 Response:**  Trustworthy  Suspicious  Reason: The address doesn’t look authentic. The message does not contain your correct name; other details are incorrect as well. Has phone number that is not the official number on Norton’s Website. The charge amount and the transaction amount is not the same. |