

# Hands-On Lab: Ethical Considerations in IT and Detecting Phishing Attacks

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 978-0-357-50643-1; Ethical Considerations in IT and Detecting Phishing Attacks

## Table of Contents

Objective.....	2
Estimated Completion Time.....	2
Materials Required.....	2
Introduction.....	2
Ethical Considerations in the Use of Information Security Tools.....	3
Are You a White Hat?.....	3
The White Hat Agreement.....	4
(ISC) <sup>2</sup> Code of Ethics.....	5
Self-Reflection and Response.....	7
Instructor's Response.....	7
Detecting and Responding to Phishing Attacks.....	8
Legitimate Messages Don't Request Sensitive Information.....	8
Legitimate Messages Usually Call You by Your Name.....	9
Legitimate Messages Come from Authentic Domains.....	10
Legitimate Messages Come from People Who Know How to Spell and Write.....	11
Legitimate Messages Don't Force You to a Web Site.....	12
Legitimate Messages Don't Include Unsolicited Attachments.....	13
Legitimate Messages Have Links that Match Legitimate URLs.....	13
Legitimate Messages Don't Create an Artificial Sense of Urgency.....	14
Legitimate Messages Display Reliable Names.....	15
Legitimate Messages Don't Solicit Money.....	16
How You Should Respond to Phishing E-Mails.....	18
Test Your Knowledge.....	19
Instructor's Response:.....	26

## Objective

Upon completion of this activity, you will:

- have a better understanding of the ethical expectations of IT professionals; and
- 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:

- The Ethical Considerations lab in 15 to 20 minutes.
- The Phishing E-Mail lab in 60 to 75 minutes.

## Materials Required

Completion of this lab does not require any software to be installed and configured on your computer.

## Introduction

This module does not include a “hands-on” project to develop specific skills. Instead, it discusses two topics that will be useful for the projects you perform in the later modules. You will first learn about the ethical dimension of using information security tools and techniques that many consider to be from the “dark side.”

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 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 to extract personal or confidential information.

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 the second part of this lab, you will begin by reading 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.

[\[return to top\]](#)

## Ethical Considerations in the Use of Information Security Tools

Using some of the “tools of the trade” in information security might lead students (and their instructors) to use software and techniques that are designed to break the rules and allow bad acts to occur. Because each academic community sets certain standards, you need to be aware of how they might apply in your specific circumstances.

Conformance to standards and exhibiting ethical behavior is required to ensure the unhindered pursuit of knowledge and the free exchange of ideas. Academic integrity means that you respect the right of other individuals to express their views and opinions, and that you, as a student or faculty member, do not engage in plagiarism, cheating, illegal access, misuse or destruction of college property, or the falsification of college records or academic work.

As a member of the academic community, and as a future InfoSec or IT professional, you are expected to adhere to standards of ethical behavior. You are expected to read and follow your institution’s code of conduct, which usually is found in your student handbook. You need to be aware that if you violate these standards, you will be subject to penalties outlined in your institution’s student conduct and academic integrity procedures. These penalties likely range from grade penalties to permanent expulsion.

Your instructor may require you to read the white hat agreement and code of ethics that follow. Your instructor might also ask you to sign a form acknowledging that you agree to abide by these ethical standards while you are a student. Your agreement would indicate that you understand the ethical behavior expected of you as part of an academic community, and that you understand the consequences of violating those standards. For those of you in InfoSec or cybersecurity programs, the standard is even higher, given that you will be a guardian of an organization’s data in the future.

### Are You a White Hat?

As part of this course, you may be exposed to systems, tools, and techniques related to information security. With proper use, these components allow a security administrator or technician to better understand vulnerabilities and the security precautions used to defend an organization’s information assets. Misuse of these components, either intentionally or accidentally, can result in breaches of security, damage to data, or other undesirable results.

Because the labs in this book will sometimes be carried out in a public network that is used by people for real work, you must agree to the following before you can participate. If you are unwilling to sign this agreement, your instructor may not allow you to participate in the projects.

## The White Hat Agreement

If you have questions about any of the following guidelines, please contact your instructor. This document may be changed from time to time by your instructor, who will notify you of such changes and may ask you to reaffirm your understanding and agreement.

1. Just because you *can* do something doesn't mean you *should*.
2. As you engage in projects, you will be granted access to tools and training that have the potential to do harm even when they are used to determine or investigate the security of an information system. Use these tools with care and consideration of their impact, and only in the ways specified by your instructor.
3. If any question arises in your mind about whether you can or should perform an activity or use a tool in a particular way, stop and ask your instructor for clarification. In information security, it is most definitely NOT easier to ask for forgiveness than for permission.
4. You are only allowed to use the tools and exercises if you are currently registered for a grade in the course. An instructor always has the right to ask students for appropriate identification if necessary.
5. Any instance of suspected misconduct, any illegal or unauthorized use of tools or exercises, or any action construed as being outside the guidelines of the course syllabus and instruction will be investigated by the instructor and may result in severe academic and/or legal penalties. Being a student does not exempt you from consequences if you commit a crime.
6. All students are expected to follow the (ISC)<sup>2</sup> code of ethics, which is available at [www.isc2.org/ethics](http://www.isc2.org/ethics) and included later in this document.
7. By acknowledging this agreement, you confirm that you *will*:
  - Only perform the actions specified by the course instructor for using security tools on assigned systems.
  - Report any findings to the course instructor or in specified reporting formats without disclosing them to anyone else.
  - Maintain the confidentiality of any private information learned through course exercises.
  - Manage assigned course accounts and resources with the understanding that their contents may be viewed by others.
  - Hold harmless the course instructor and your academic institution for any consequences or actions if you use course content outside the physical or virtual confines of the specified laboratory or classroom.
  - Abide by the computing policies of your academic institution and by all laws governing the use of computer resources on campus.
8. By acknowledging this agreement, you confirm that you *will not*:
  - Attempt to gain access to a system, attempt to increase privileges on any system, or access any data without proper authorization.

- Disclose any information that you discover as a direct or indirect result of this course exercise.
- Take actions that will modify or deny access to any system, data, or service except those to which administrative control has been delegated to you.
- Attempt to perform any actions or use utilities presented in the laboratory outside the confines and structure of the projects or classroom.
- Use any security vulnerabilities beyond the target accounts in the course or beyond the duration of the course exercise.
- Pursue any legal action against the course instructor or the university for any consequences or actions if you use what you learn in the course outside the physical or virtual confines of the laboratory or classroom.

9. You will abide by the following code of ethics:

*Safety of the commonwealth, duty to our principles, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.*

### **(ISC)<sup>2</sup> Code of Ethics**

*Protect society, the common good, necessary public trust and confidence, and the infrastructure.*

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

*Act honorably, honestly, justly, responsibly, and legally.*

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principles, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

*Provide diligent and competent service.*

- Preserve the value of systems, applications, and information.
- Respect the trust and privileges granted to you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.



*Advance and protect the profession.*

- Sponsor for professional advancement those best qualified. All other things being equal, prefer those who are certified and who adhere to these canons.
- Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

The ISC<sup>2</sup> code of ethics is available from [www.isc2.org/ethics](http://www.isc2.org/ethics).

## Self-Reflection and Response

In the space below, write a brief statement indicating your intention to abide by the ethics codes spelled out in this lab.

## Detecting and Responding to Phishing Attacks

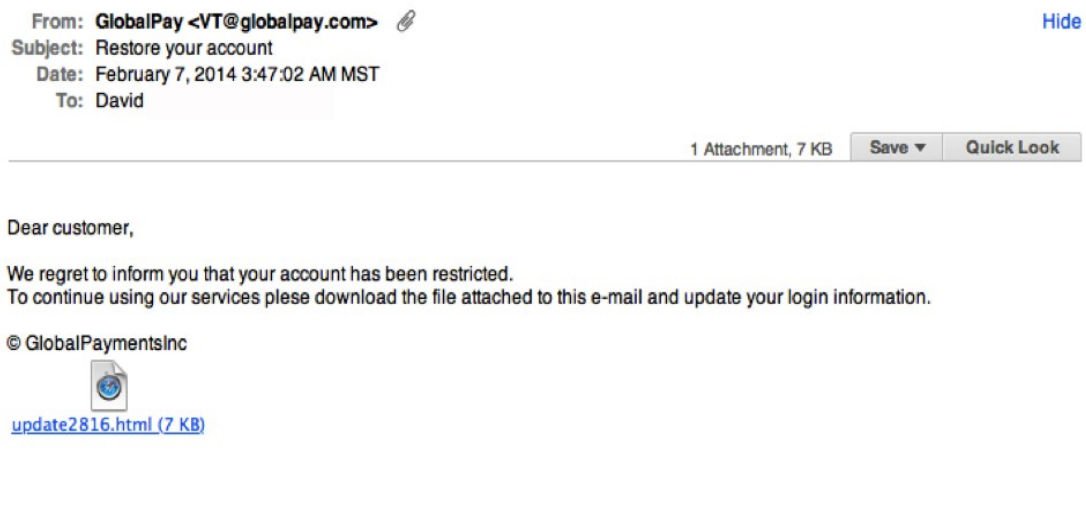
The following questions indicate some of the telltale signs of phishing attacks. In general, you should ask yourself these questions for each e-mail you receive:

- 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 L01-1** Global Pay Phishing E-Mail

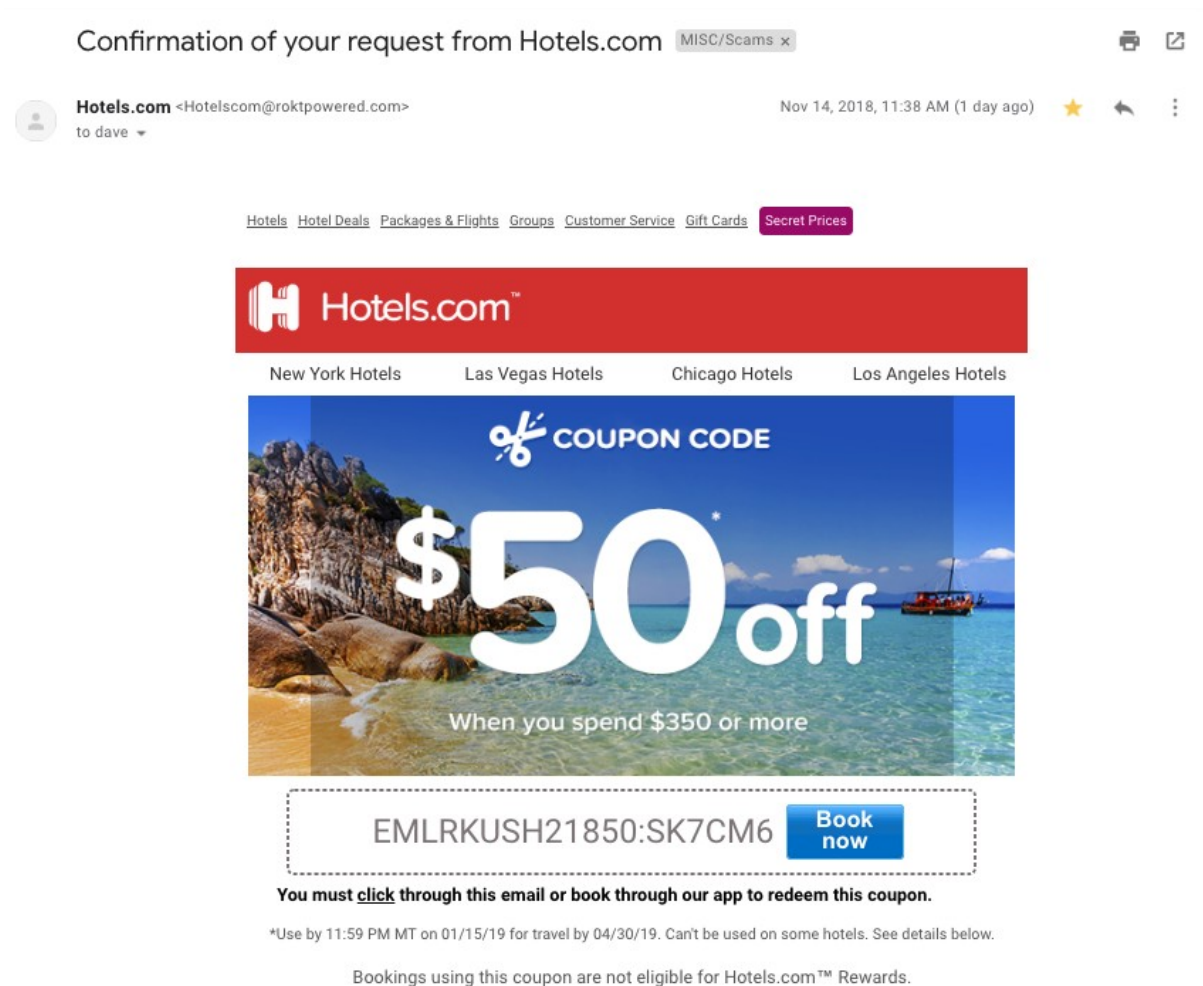
In Figure L01-1, notice the unsolicited web link attachment. Also, look at the generic salutation at the beginning (“Dear customer”). Such greetings are discussed next.

### 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 L01-2, everything is nearly perfect. So, how would you spot it as suspicious?



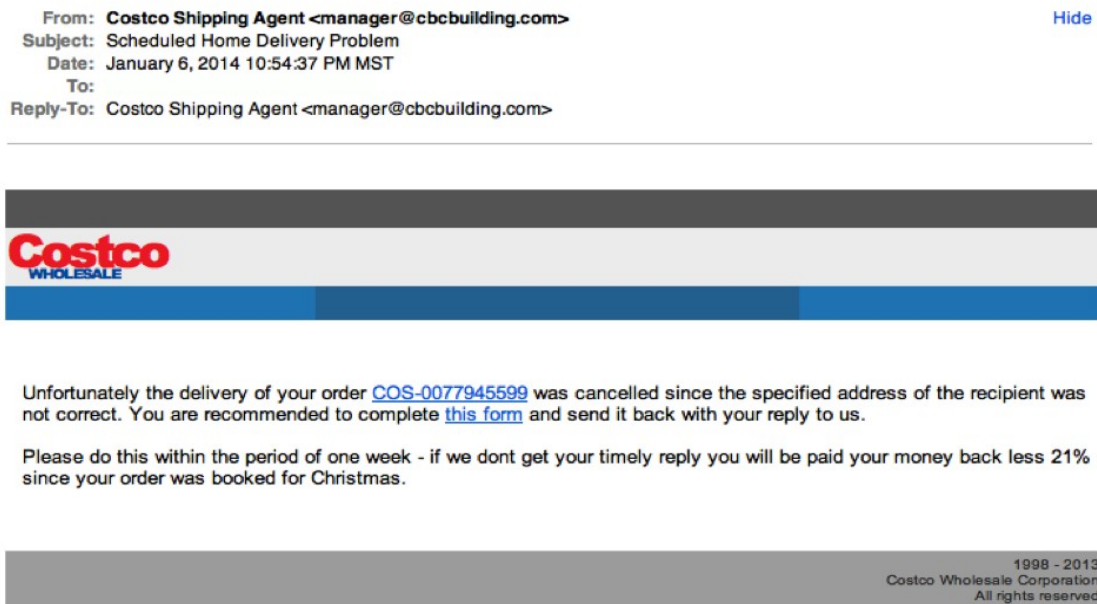
**Figure L01-2** Hotels.com Phishing E-Mail

The example in Figure L01-2 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 L01-3** Costco Phishing E-Mail

In the example shown in Figure L01-3, the Costco logo is just a bit off. To see the actual logo, you can go to <https://costco.com>. Do you see the difference?

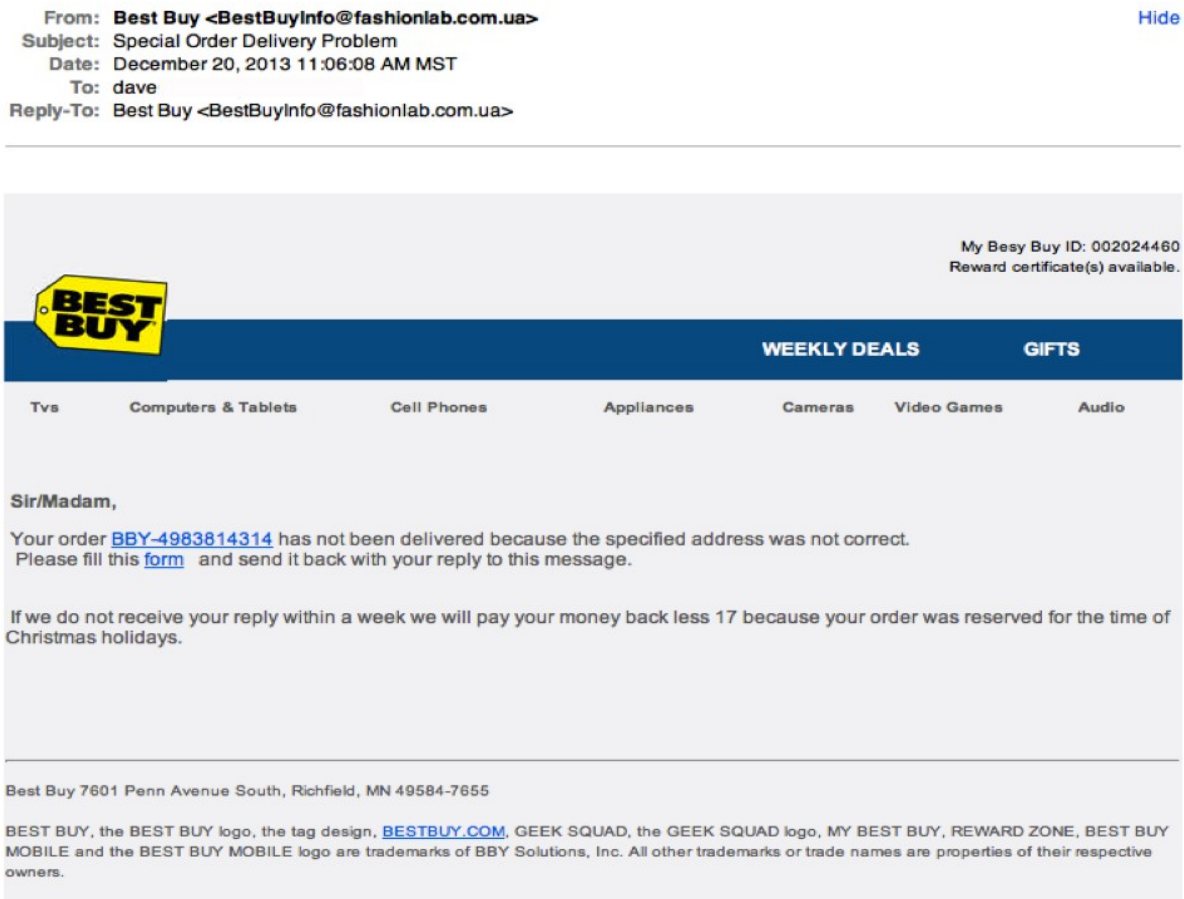
Also, note the “From” field is from a different business: “cbcbuilding.com” rather than “costco.com”

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:




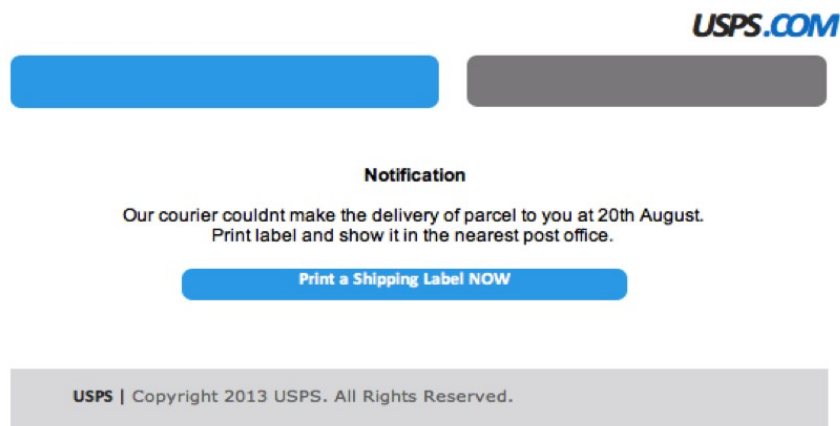
**Figure L01-4** Best Buy Phishing E-Mail

In addition to the generic salutation in Figure L01-4, the grammar gaffes and extra spaces 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.

From: Manager Daniel Bridges <daniel\_bridges33@gulfslipformpaving.com>   
Subject: Information  
Date: August 26, 2013 1:25:12 AM MDT  
To: dave  
Reply-To: Manager Daniel Bridges <daniel\_bridges33@gulfslipformpaving.com>



**Figure L01-5** USPS Phishing E-Mail

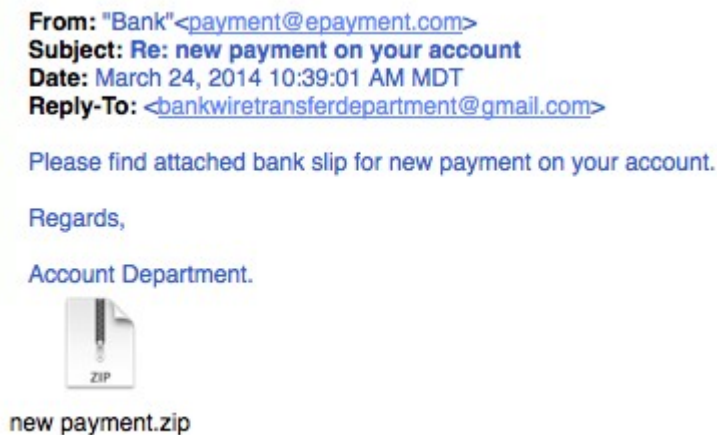
The entire e-mail shown in Figure L01-5 was sent as an image tagged as a single hyperlink. If a recipient clicked anywhere in the e-mail, a malicious attack would be initiated. You can guard against this by hovering your mouse cursor over the message to see if a link address preview appears. You can also see the spelling and grammar errors in the body of the “Notification.”



## 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.

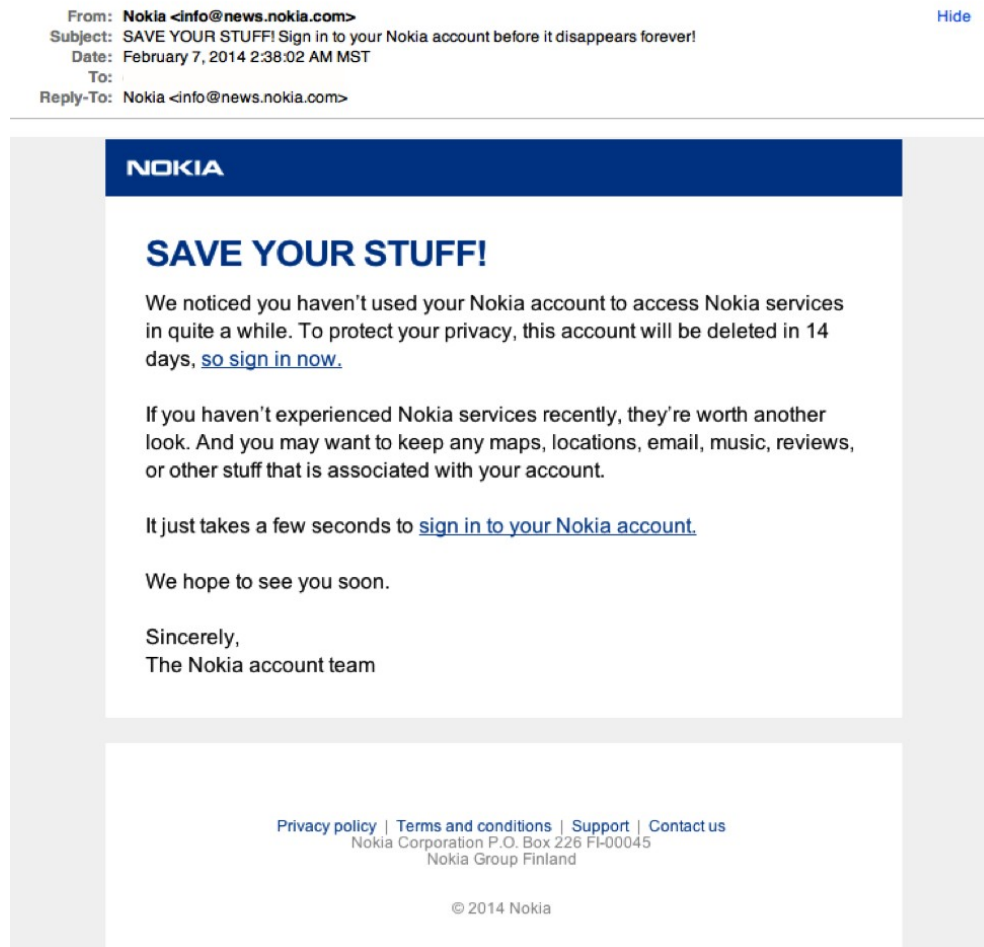


**Figure L01-6** ePayment Phishing E-Mail

Before you wonder what's in the .zip file attached in Figure L01-6, 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 L01-7** Nokia Phishing E-Mail

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.

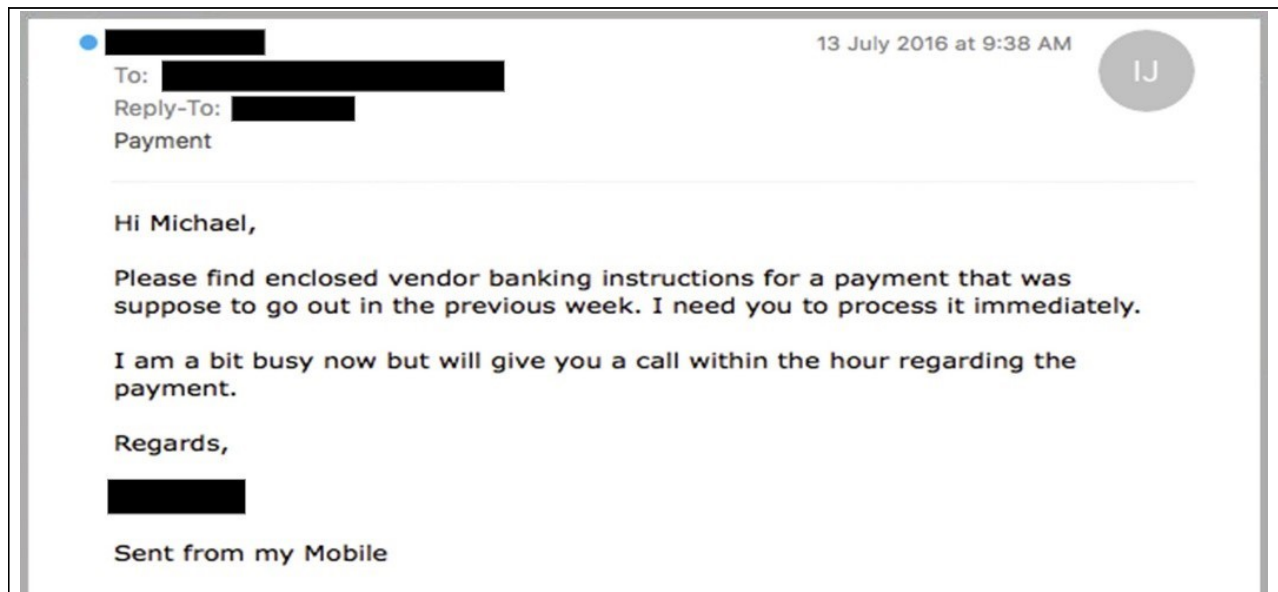
When you take time to think about something, you are much more likely to notice things that don't seem quite right. For instance, when you receive an unexpected e-mail from a major company, maybe you'll think twice and realize that the organization has never contacted you via e-mail. Maybe you'll receive 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.

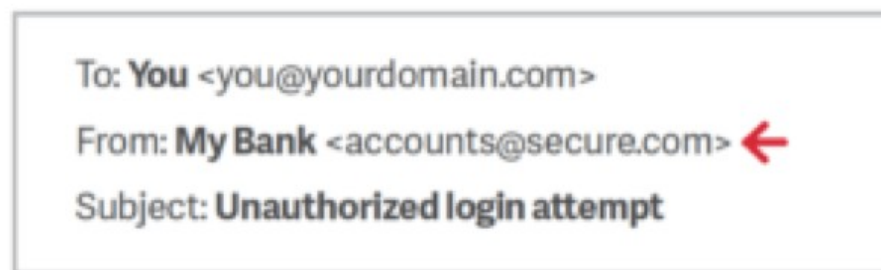
A typical example looks like Figure L01-8.



**Figure L01-8** Mobile Phishing E-Mail

### 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 L01-9. 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 L01-5** Secure.com Phishing E-Mail

## 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 4-1-9 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 4-1-9 of the Nigerian legal code prohibits them (hence the name).

A typical Nigerian 4-1-9 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 4-1-9 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 L01-10 is fairly typical.

[EXTERNAL] Partnership



Ms E. A Alhashimy <office1@hiiragi.or.jp>  
Tue 2020-09-29 18:29  
To: Recipients <office1@hiiragi.or.jp>

Hello,

My name is Reem E. Al-Hashimi, the Emirates Minister of State and Managing Director of the United Arab Emirates (Dubai) World Expo 2020 Committee. I am writing to you to stand as my partner to receive my share of gratification from foreign companies whom I helped during the bidding exercise towards the Dubai World Expo 2020 Committee and also i want to use this funds to assist Coronavirus Symptoms and Causes.

Am a single Arab women and serving as a minister, there is a limit to my personal income and investment level and For this reason, I cannot receive such a huge sum back to my country or my personal account, so an agreement was reached with the foreign companies to direct the gratifications to an open beneficiary account with a financial institution where it will be possible for me to instruct further transfer of the fund to a third party account for investment purpose which is the reason i contacted you to receive the fund as my partner for investment in your country.

The amount is valued at Euro 47,745,533.00 with a financial institution waiting my instruction for further transfer to a destination account as soon as I have your information indicating interest to receive and invest the fund, I will compensate you with 30% of the total amount and you will also get benefit from the investment.

If you can handle the fund in a good investment. reply on this email only: r19772744@gmail.com

Regards,  
Ms. Reem

**Figure L01-10** UAE World Expo Phishing E-Mail

## How You Should Respond to Phishing E-Mails

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>.

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.

## Test Your Knowledge

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. Look at each of the following messages and then determine whether you think they are legitimate or suspicious. Print out the answer page at the end of the lab for recording your answers.

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.



## Example 1

**From:** Dropbox Transfer <no-reply@dropbox.com>  
**Sent:** Thursday, January 21, 2021 2:26 PM  
**To:** Michael Whitman <mwhitman@kennesaw.edu>  
**Subject:** [EXTERNAL] Mike Neff sent you some files




### Mike Neff sent you Statement Review From Mike Neff \_State Security.pdf

You can download these files now or until **1/28/2021**.  
Questions? Ask Mike ([mike.neff@state-security.com](mailto:mike.neff@state-security.com))

[Download files](#)

Here's what they sent you


1 item • 113 KB




Statement Review From Mike Neff \_State Security.pdf  
113.16 KB

## Example 2

[EXTERNAL] Congratulations you have won

 Usa-Lottery <info@kysmaq.co.jp>  
Thu 2020-08-06 14:35  
**To:** cinsa@movistar.com.ni





 CONGRATULATIONS-COLO.pdf  
201 KB


Congratulations you have won the usa mega millions email lottery. attachments below is your winner prize information view the procedures on how to claim your prize


TJDKHDLUSQQJMNMFOTOKXIZTYHLJKDLHSBXGIQQ



### Example 3

Bears Moving Co Booking Confirmation 1-29-21 Herbert Mattord 6 pm    

 **Qualin Ransom** <qualinransom@gmail.com>  
to me ▾

Jan 18, 2021, 6:00 PM (3 days ago) ☆  Reply ⋮

The scheduled Move agreement is as follows. For \$225 we will provide 2-hours of service. We will provide 2-men, all moving equipment (i.e., hand-trucks, pads, dollies, etc). There are no hidden fees (i.e., fuel charges). If the job exceeds the allotted time frame, service charges are as following: \$100 per hour beyond the 2-hour minimum. Thanks for booking with us, we look forward to servicing you! Please give us a call for any changes or updates.

\*\*\*Methods of payment: Cash, Check, Cash App, Venmo (no processing fees).

Credit/Debit (3% processing fee).

Please allow a 1-hour window for arrival.

### Example 4

Vincenz Cruz <lhtcletisjx@outlook.com>

Sun 2018-09-30 12:18

To: 

drawde is one of your password:) I am Vincenz. I recorded your webcam which shows your immoral sexual actions & video you played on the porno video because that website was infected with my virus. You happen to be appearing eye-catching in the video footage.

The malware then sent all of your email and FB contacts to me.

I'll email your recording to your friends unless you send me 3000 USD via B I T C O I N S in the next 24 hours to the below address:

B I T C O I N Address: 1Fvfp3183h9YgHD6YaoA1nFUCBUgkjGP3w

Make sure to Copy-Paste address because it is CasE SenSiTiVe.

Once money is received by me, I will delete your video and every bit of information I have about you.

## Example 5

### Payment Advice Notification



mail\_server@company.com

Fri 2020-02-28 13:10

To: infosec



Payment Advice.pdf

8 KB

Dear Customer,

Attached is the Payment Advice that we have processed. The payment date reflects the date at which the payment is processed by our bank. Prior to utilizing the funds, please check with your bank and ensure that the funds have been deposited.

Here is the reference information:

Pay Cycle: SANDLY

Pay Cycle Sequence Number: 1656

This is system generated email, please do not reply.

## Example 6

### I SEND THE MONEY TO YOUR NAME SEE PAYMENT COPY IN ATTACH



Theresa Baustert <tbaust@lps.org>

Wed 2011-09-28 19:29



Payment Copy2.html

699 bytes



Payment copy 1.html

1 KB

2 attachments (2 KB)   Download all   Save all to OneDrive - Kennesaw State University

Please find attached:

I just send the money to your name as ask via western union money transfer.

Regards,

Uzman Shamsi

## Example 7

Please I Need Ur Help!!



Vogelaar, Heleen <Heleen.Vogelaar@uwv.nl>  
Sat 2009-06-27 10:16



Dear Friend,  
With a very desperate need for assistance.I am Capt. James Micheal. presently in Iraq with the United States Marine Corps;I found your contact particulars in an Address journal.I am seeking your assistance to evacuate the sum of \$500,000.00 to you,as far as I can be assured that it will be safe in your care until I complete my service here.  
SOURCE OF MONEY:  
some money in various currencies was discovered concealed in barrels with piles of weapons and ammunitions at a location near one of Saddam's old palaces during a rescue operation,and it was agreed by all party present that the money will be shared amongst us.  
The above figure was given to me as my share, There is a secured way of getting the package out to a safer country for you to pick up,and i will discuss this with you when I am sure that you are willing to assist me, because I do not know for how long we will remain here.  
Please you can reach me on my personal e-mail address below for more information.  
Email: capt.james001@sify.com  
Thanks  
Capt. James Micheal.

## Example 8



ACH Payment <Opal@boomansion.net>  
Wed 2011-09-21 02:38  
To: hmitcheld@kennesaw.edu

**FDIC**

Your Corporate and Business banking accounts  
Federal Deposit Insurance Corporation  
Security Updates for ACN and Wire transfers

Dear client,

Your account **ACH and Wire transactions** have been **temporarily suspended** for your Security, due to the expiration of your security version.

To download and **install the newest Updates**, follow this link security <http://www.update.fdic.gov>

As soon as it is set up, your transaction abilities will be fully restored.

Best regards, [Online security department](#), Federal Deposit Insurance Corporation.

FDIC Public Information Center  
3501 North Fairfax Drive, Room E-1002, Section 515, Arlington, VA 22226  
Fax Number: (703) 562-2296 Email Address: [publicinfo@fdic.gov](mailto:publicinfo@fdic.gov)

## Example 9

Dear Friend



Daniel Arscott <hilariocasimiro@uol.com.br>  
Wed 2011-09-14 02:02



Dear Friend

This is to thank you for your effort, I understood that your hands were tied, But Not to worry I have succeeded, the money has been transfered into the account provided by a newly found friend of mine in Japan.To compensate you for your past assistance and commitments,i have droped an International Certified Bank Draft cheque worth of \$1.5 million US dollars, for you. I am in Japan with my family presently. I do intend to establish some business concerns here,and possibly buy some properties. Contact JACOB LYCAMA on His Email: ( jacoblycama@gmail.com ),Send him your full information to send you the cheque

1.Full names:\_\_\_\_\_

2.Address:\_\_\_\_\_

3.E-mail address:\_\_\_\_\_

4.Telephone number:\_\_\_\_\_

5.Country \_\_\_\_\_

Best Regards,

Daniel Arscott

## Example 10

----- Forwarded Message -----

**Subject:**AUTO RENEWING EMAIL

**Date:**Thu, 21 Jan 2021 23:23:27 +0530

**From:**Norton Official <[nortonofficial20@gmail.com](mailto:nortonofficial20@gmail.com)>

**To:**[alisaqlain989@gmail.com](mailto:alisaqlain989@gmail.com)



AUTO RENEWAL EMAIL

**MODE OF PAYMENT** : CREDIT CARD  
**ORDER NUMBER** : 85692563  
**CHARGE** : \$480.87  
**HELPLINE NUMBER** : +1 (570) 260-6102.

Dear Sir/Madam,

Thank You for renewing your Norton Life Lock security for the upcoming one year.

Norton informs you that the contract electronically signed by you with our company for the maintenance of your computer services has expired, and it is auto renewed today for the upcoming year. The transaction of \$399.99 would appear within the next 48 working hours on your account.

We would like to inform you that this month we have served over 1 million customers and you are one of them . We hope you will enjoy the services . Due to COVID-19 we are unable to notify each customer through a confirmation call .

If you have any questions or wish to cancel the subscription and get back your refund,

**Please contact us on +1 (570) 260-6102.**

Thank You,

Team Norton.

(Finance Team)

**NOTE: THIS IS AN AUTO GENERATED EMAIL PLEASE DON'T REPLY TO THIS EMAIL.**

## Phishing Email Responses

Email	Trustworthy (T) or Suspicious (S)	Reason
Example 1		
Example 2		
Example 3		
Example 4		
Example 5		
Example 6		
Example 7		
Example 8		
Example 9		
Example 10		