SPOT THAT PHISH!

A FREE TRAINING ACTIVITY

CSU COMPUTER SERVICES UNLIMITED

WHAT YOU'LL LEARN IN THIS BOOKLET

This booklet is designed to help you and your team recognize phishing attempts before they cause harm.

We've included:

- Tips and signs on how to spot phishing emails, fake websites, and other fraudulent tactics.
- 4 main types of phishing.
- 7 engaging "Spot the Phish" real-world examples.
- "Spot the Phish" answers and explinations.

By the end of this guide, you'll be equipped with the knowledge and tools to defend your business against phishing attacks and ensure that your information stays secure.

WHAT IS PHISHING, AND HOW CAN IT HARM YOUR BUSINESS?

Phishing is a type of cyberattack where attackers attempt to trick individuals into revealing sensitive information, such as passwords, credit card numbers, or personal details, by pretending to be a trustworthy entity. This often happens through deceptive emails, fake websites, or text messages that appear legitimate but are designed to steal your data. If you're not careful, phishing can cause significant harm to your business—leading to financial loss, data breaches, and damage to your company's reputation.

For businesses, the stakes are even higher. A successful phishing attack can compromise customer data, disrupt operations, or provide criminals with access to your internal systems. Phishing is one of the most common methods cybercriminals use to gain access to sensitive information, and if your team isn't properly trained to recognize these threats, it can leave your business vulnerable.

CSU COMPUTER SERVICES UNLIMITED

Here's a list of common features that phishing emails often have. Being aware of these can help you spot a phishing attempt before it causes any harm:

Suspicious Sender Email Address

The sender's email address may look similar to a legitimate one, but with small variations (e.g., "support@amaz0n.com" instead of "support@amazon.com").

Urgent or Threatening Language

Phishing emails often use phrases like "Immediate action required," "Your account has been compromised," or "You've won a prize" to create a sense of urgency or fear.

Generic Greetings

Instead of addressing you by name, phishing emails often start with a generic greeting like "Dear Customer," "Dear User," or "Hello Member."

Suspicious Links

Phishing emails may contain links that appear to go to a legitimate website but actually lead to a fraudulent page. Always hover over the link to see the actual URL before clicking.

Unusual Attachments

Phishing emails may include unexpected attachments, often with unfamiliar file types (e.g., .exe, .zip, or .scr), which could contain malware.

Spelling and Grammar Errors

Many phishing emails contain spelling mistakes, awkward phrasing, or grammatical errors that make the message seem unprofessional or suspicious.

Requests for Sensitive Information

A legitimate organization will never ask you to provide sensitive information, like login credentials or personal data, via email. Be wary of any email requesting this.

Fake Logos and Branding

Phishing emails often mimic the branding, logos, and design elements of legitimate companies, but they may be slightly off, such as distorted logos or low-quality images.

Too Good to Be True Offers

If an email promises something that sounds too good to be true—like an incredible prize, huge discounts, or an unexpected reward—it's likely a phishing attempt.

CSU COMPUTER SERVICES UNLIMITED

Unusual Request or Unexpected Communication

An email that doesn't align with what you typically expect from a company or contact. Phishing emails may pretend to be from a colleague, boss, or vendor.

Inconsistent URLs

The URL in the body of the email may look similar to a legitimate one but often has small differences. Always verify the domain before clicking on any link.

No Personalization or Context

Some phishing emails lack context or personalization that real communication typically has. They may be vague or seem disconnected from your recent activities.

Unusual Requests for Money or Payments

Emails asking you to wire money, transfer funds, or make a payment in an unusual way (especially from someone you don't normally transact with) are red flags.

By keeping an eye out for these common signs, you'll be better equipped to spot phishing attempts and avoid falling victim to them. Sometimes to spot a phish, you have to do research to see if the company email order and such matches. Now, use this information to spot the phish in on these next few pages!

TYPES OF PHISHING

Email Phishing:
Attackers send emails that appear to be from trusted sources, such as banks or online services asking you to click on a link or download an attachment.

Spear Phishing:
This is a targeted attack where the scammer tailors the message to a specific individual by gathering extensive research from data breaches or social media to craft personalized messages or calls that are full of the user's personal details.

Vishing:
Vishing or voice phishing involves attackers calling and pretending to know you or to be from a reputable organization to extract personal information or money.

Smishing:
Attackers send texts to try to trick users into clicking on a malicious link or divulging personal information. These messages range from pretending to be from a business to posing as a random person texting the wrong number.

Quishing:
Quishing tricks people into scanning a fake QR code. The code then directs the user to a fraudulent website that may steal personal information or install malware.

SPOT THAT PHISH #1

From:Michelle Sherman moonsunlight404@gmail.com

Subject:**Adam**

Date:April 9, 2024 at 8:48:24 AM EDT

To:asherman@csuinc.com

Hi, how are you today?
I'm planning to surprise some of the staff with Gifts, Your confidentiality will be appreciated. Let me know when you receive this email. I am going into a meeting shortly with limited communication access. Let me have your personal email address. Thanks.
Regards
Michelle Sherman
President

Here is a phishing email sent to one of our staff that was disguised as an email from CSU's President. Can you spot the phishing signs?

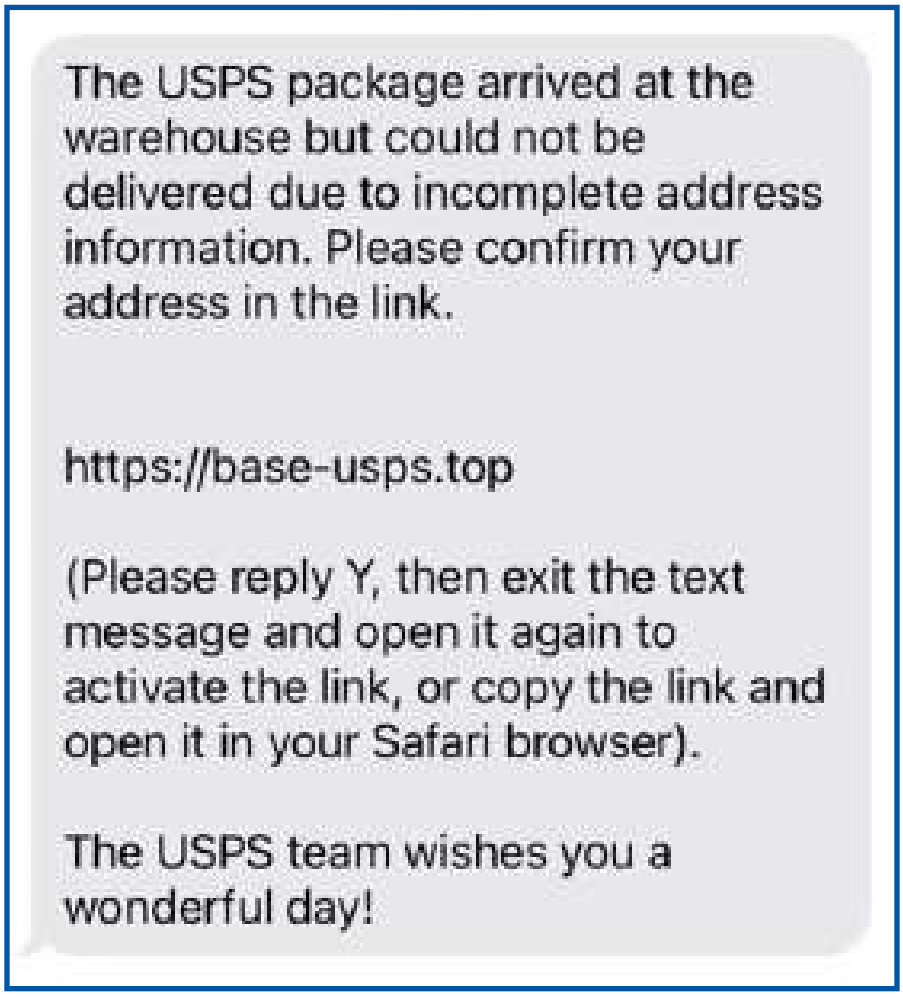
SPOT THAT PHISH #2

Company Name*	Graycor, Inc.
Email*	ryan_schultz@graycorinc.com
Phone*	(630) 800-3509
How many computers do you have? *	100+
How may we help you?	We are interested in placing order for 20 units of HP EliteBook 840 G10 14" Notebook - WUXGA - Intel Core i5 13th Gen i5-1335U - 16 GB - 512 GB SSD - English Keyboard - 89D90UT#ABA. Kindly provide us with a quote, our method of payment is Net 10 days.

Here is a form that was submitted through CSU's website. What's wrong with this one? Is this a phish or not?

CSU COMPUTER SERVICES UNLIMITED

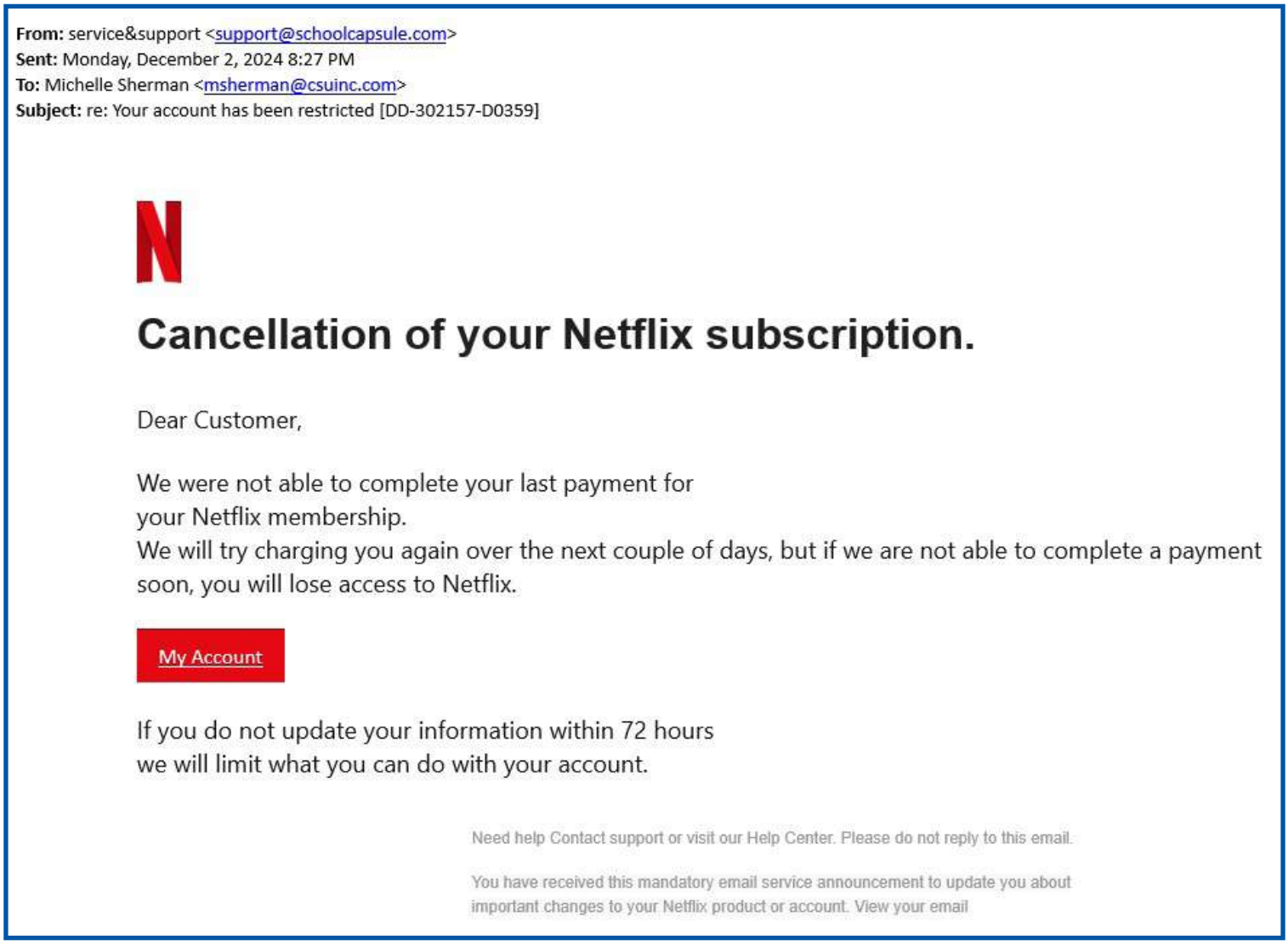
SPOT THAT PHISH #3



Here is a very common phishing text that you may have recieved. Do you know what makes this a phishing text? What do you do when you receive suspicious texts?

Think before you click

SPOT THAT PHISH #4



From: service&support <support@schoolcapsule.com>
Sent: Monday, December 2, 2024 8:27 PM
To: Michelle Sherman <msherman@csuinc.com>
Subject: re: Your account has been restricted [DD-302157-D0359]

Cancellation of your Netflix subscription.

Dear Customer,

We were not able to complete your last payment for
your Netflix membership.
We will try charging you again over the next couple of days, but if we are not able to complete a payment soon, you will lose access to Netflix.

My Account

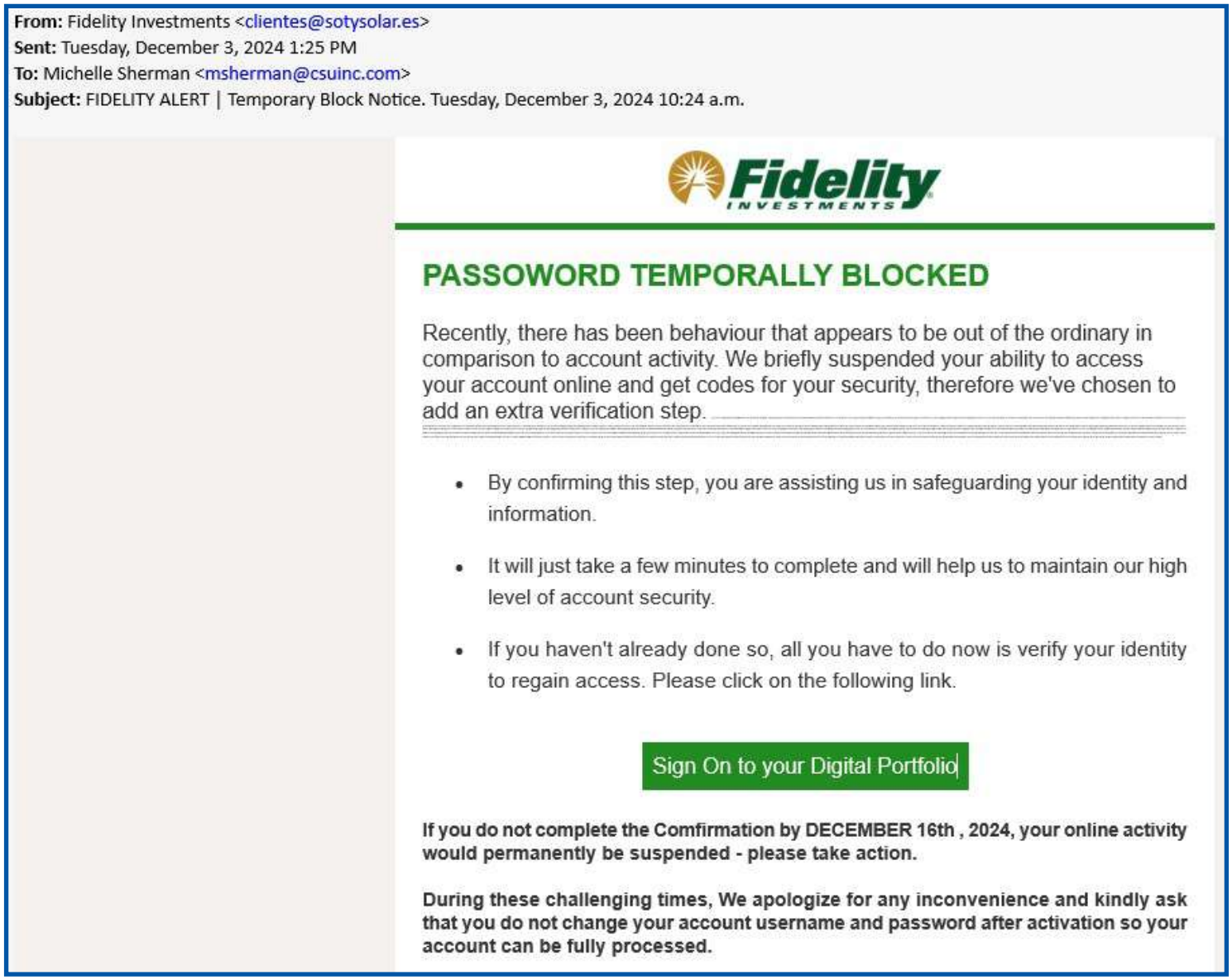
If you do not update your information within 72 hours
we will limit what you can do with your account.

Need help Contact support or visit our Help Center. Please do not reply to this email.

You have received this mandatory email service announcement to update you about important changes to your Netflix product or account. View your email

Here is a well-disguised phishing email sent to a Netflix account holder. How do you know this is a phish?

SPOT THAT PHISH #5



From: Fidelity Investments <clientes@sotysolar.es>
Sent: Tuesday, December 3, 2024 1:25 PM
To: Michelle Sherman <msherman@csuinc.com>
Subject: FIDELITY ALERT | Temporary Block Notice. Tuesday, December 3, 2024 10:24 a.m.

Fidelity INVESTMENTS

PASSOWORD TEMPORALLY BLOCKED

Recently, there has been behaviour that appears to be out of the ordinary in comparison to account activity. We briefly suspended your ability to access your account online and get codes for your security, therefore we've chosen to add an extra verification step.

- By confirming this step, you are assisting us in safeguarding your identity and information.
- It will just take a few minutes to complete and will help us to maintain our high level of account security.
- If you haven't already done so, all you have to do now is verify your identity to regain access. Please click on the following link.

Sign On to your Digital Portfolio

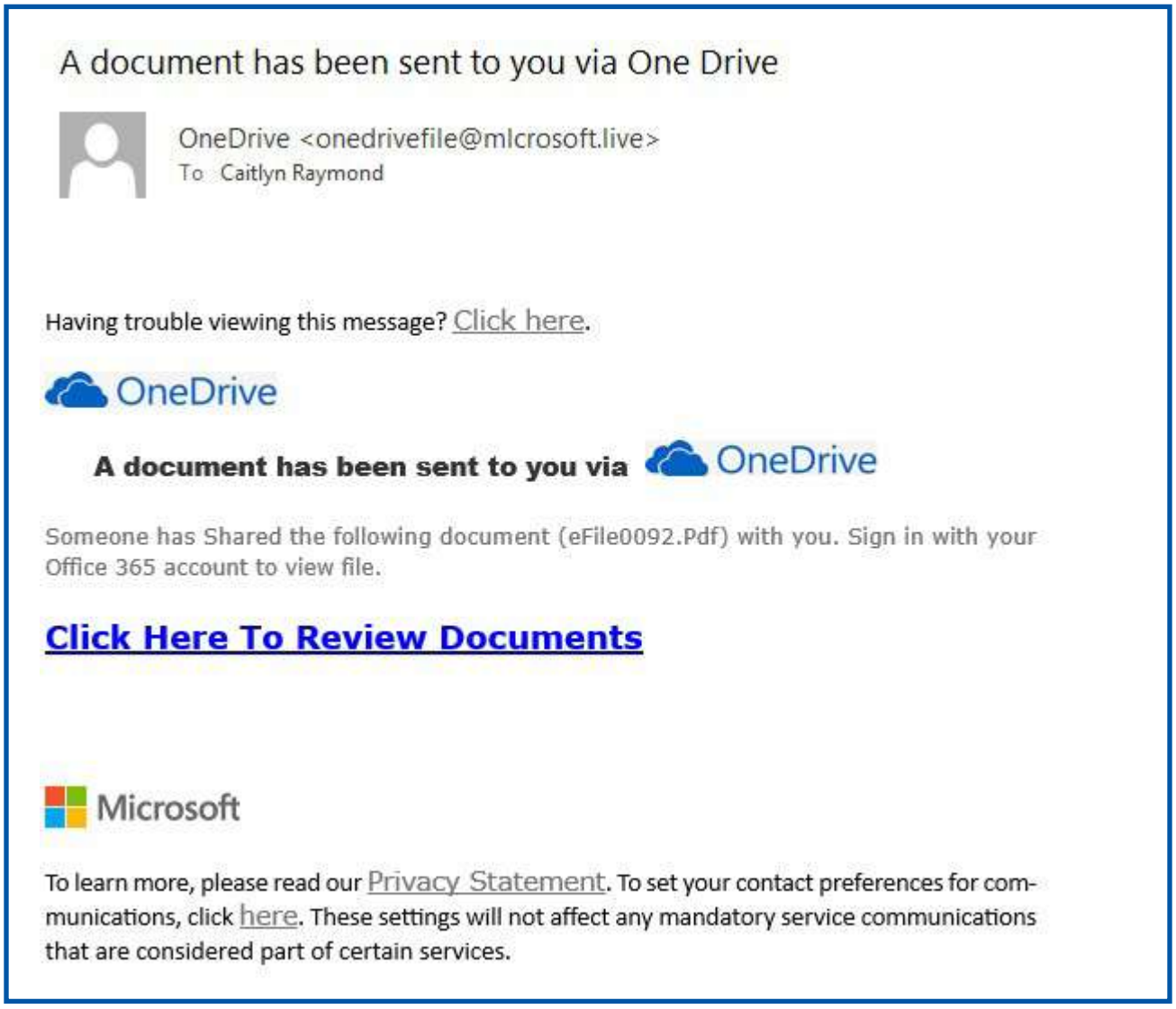
If you do not complete the Comfirmation by DECEMBER 16th , 2024, your online activity would permanently be suspended - please take action.

During these challenging times, We apologize for any inconvenience and kindly ask that you do not change your account username and password after activation so your account can be fully processed.

Here is a nicely formatted phishing email. But how can you tell it's a phish?

Don't unsubscribe unless you're POSITIVE the email is legit

SPOT THAT PHISH #6



A document has been sent to you via One Drive

OneDrive <onedrivefile@mlcrosoft.live>
To Caitlyn Raymond

Having trouble viewing this message? Click here.

OneDrive

A document has been sent to you via OneDrive

Someone has Shared the following document (eFile0092.Pdf) with you. Sign in with your Office 365 account to view file.

Click Here To Review Documents

Microsoft

To learn more, please read our Privacy Statement. To set your contact preferences for communications, click here. These settings will not affect any mandatory service communications that are considered part of certain services.

A document was shared. But it is a phish, why?

Note: You may need to do some research.

SPOT THAT PHISH #7

From: Caitlyn Raymond <frt822249@gmail.com>
Sent: Tuesday, December 17, 2024 11:49 AM
To: Michelle Sherman <msherman@csuinc.com>
Subject: REQUEST FOR DIRECT DEPOSIT MODIFICATION

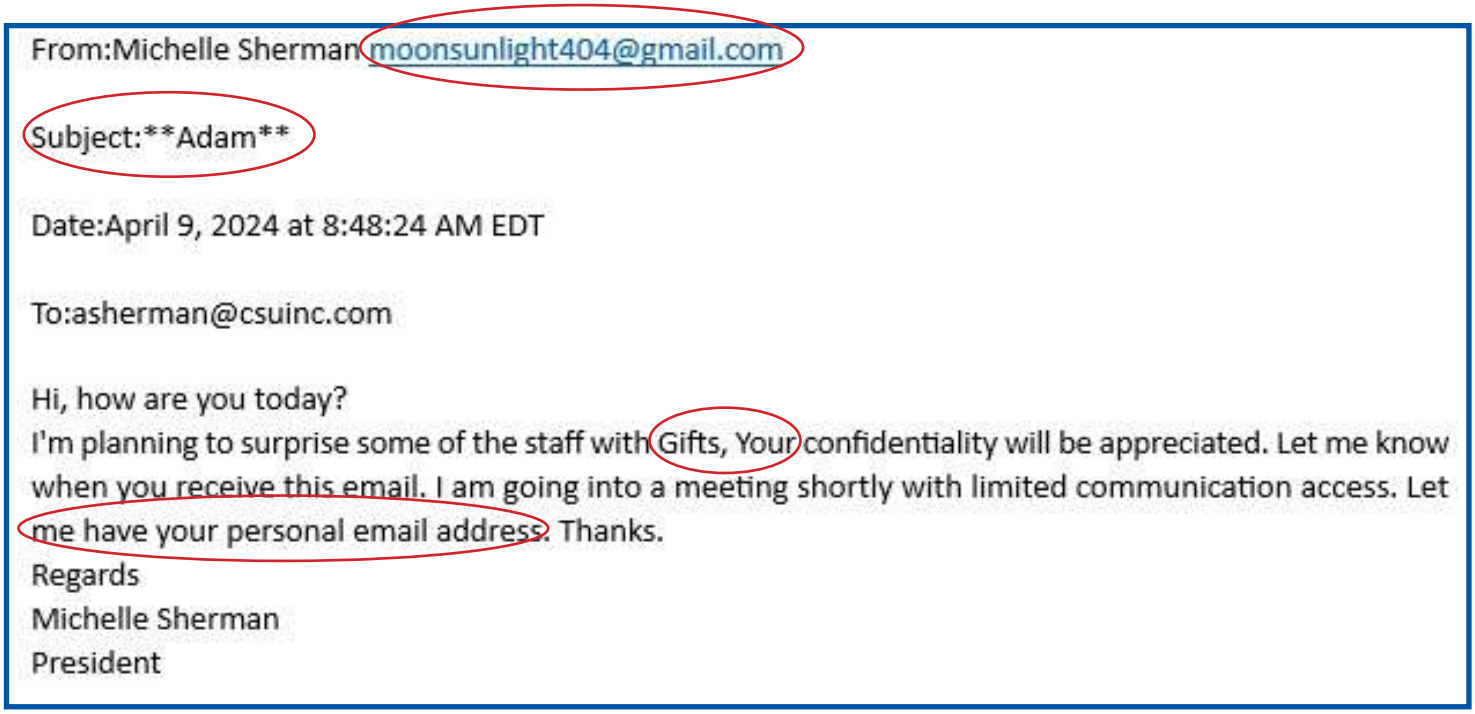
Hi there,

My bank recently emailed me new banking information for the upcoming paycheck.
What specific banking information is needed to put up my new bank account information on file for my upcoming paycheck?

Many Thanks.

Here is an email our President got from an employee. Is this a phishing email?

SPOT THAT PHISH #1 ANSWER



From:Michelle Sherman moonsunlight404@gmail.com

Subject:**Adam**

Date:April 9, 2024 at 8:48:24 AM EDT

To:asherman@csuinc.com

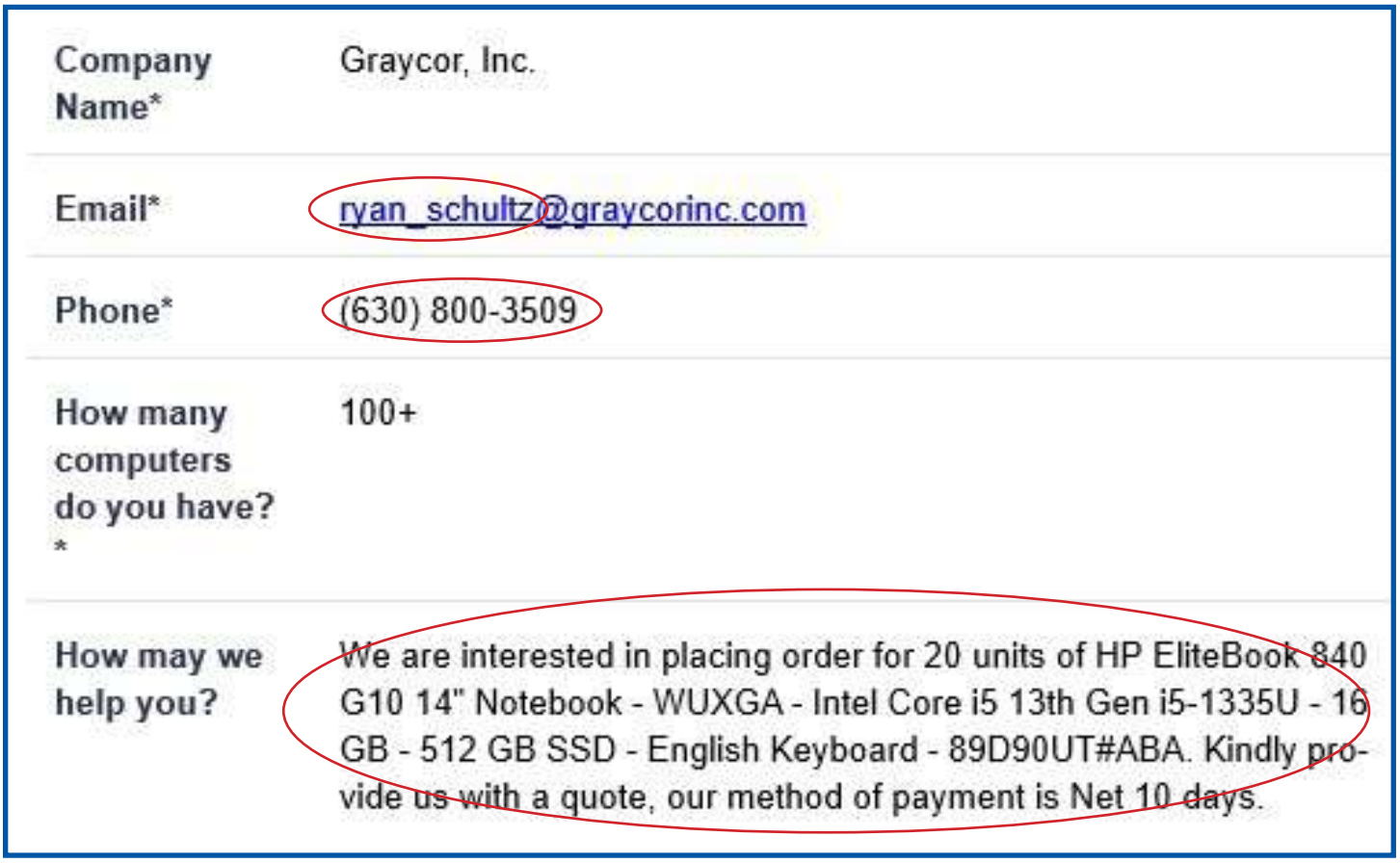
Hi, how are you today?
I'm planning to surprise some of the staff with Gifts, Your confidentiality will be appreciated. Let me know when you receive this email. I am going into a meeting shortly with limited communication access. Let me have your personal email address. Thanks.
Regards
Michelle Sherman
President

1. Email doesn't match with the President's email
2. Odd thing to put as a subject line
3. Grammar errors
4. Asks for personal information

Tip: If you're suspicious and unsure, it's best to reach out to the one who sent it to confirm if it was them or not. To confirm, do not reply to this email. Write a new email asking questions about the legitimacy of the email.

Never reply directly to suspected phishing emails

SPOT THAT PHISH #2 ANSWER



Company Name*	Graycor, Inc.
Email*	ryan_schultz@graycorinc.com
Phone*	(630) 800-3509
How many computers do you have? *	100+
How may we help you?	We are interested in placing order for 20 units of HP EliteBook 840 G10 14" Notebook - WUXGA - Intel Core i5 13th Gen i5-1335U - 16 GB - 512 GB SSD - English Keyboard - 89D90UT#ABA. Kindly provide us with a quote, our method of payment is Net 10 days.

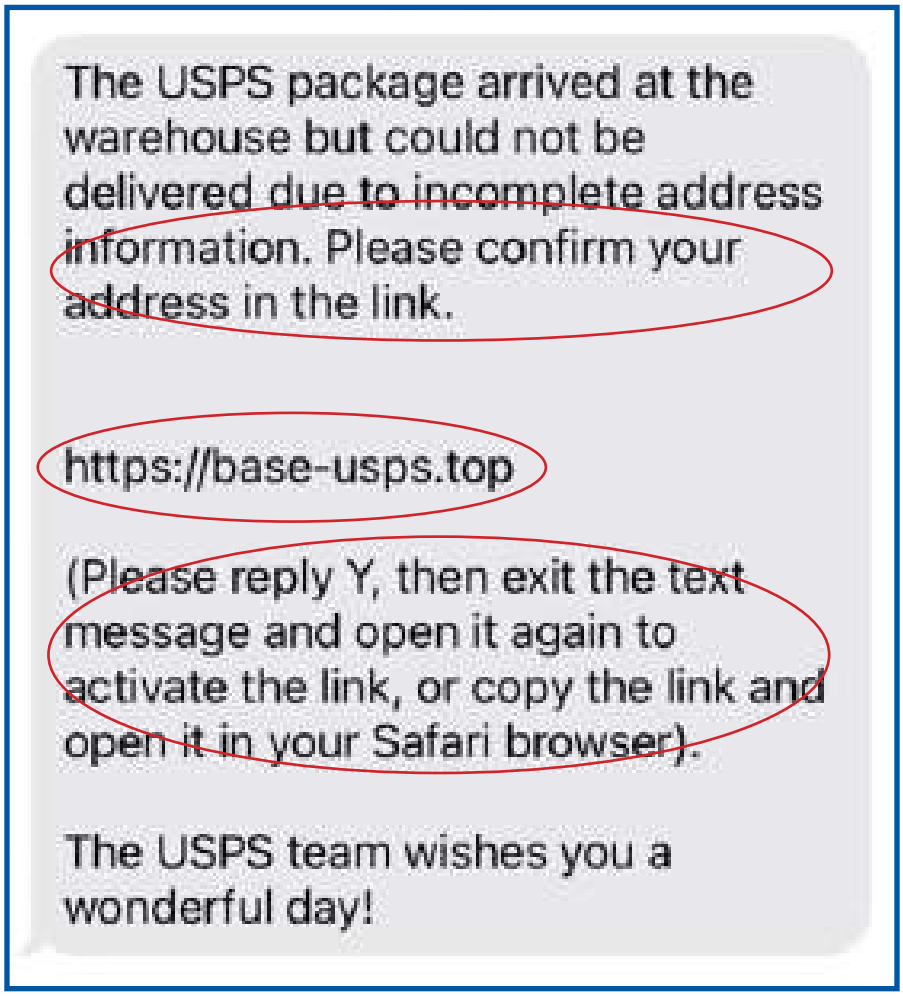
This one takes intuition and some research:

1. Email doesn't match a professional business email standard with the underscore
2. The phone number is out of our state, and doesn't match the number on the website
3. They asked for an item in a form rather than calling us to ask questions
4. This is a big, established company asking us, a small/meduim business IT provider, for technology

Tip: Do your own research to confirm your suspicion.

Too good to be true = too good to be true

SPOT THAT PHISH #3 ANSWER

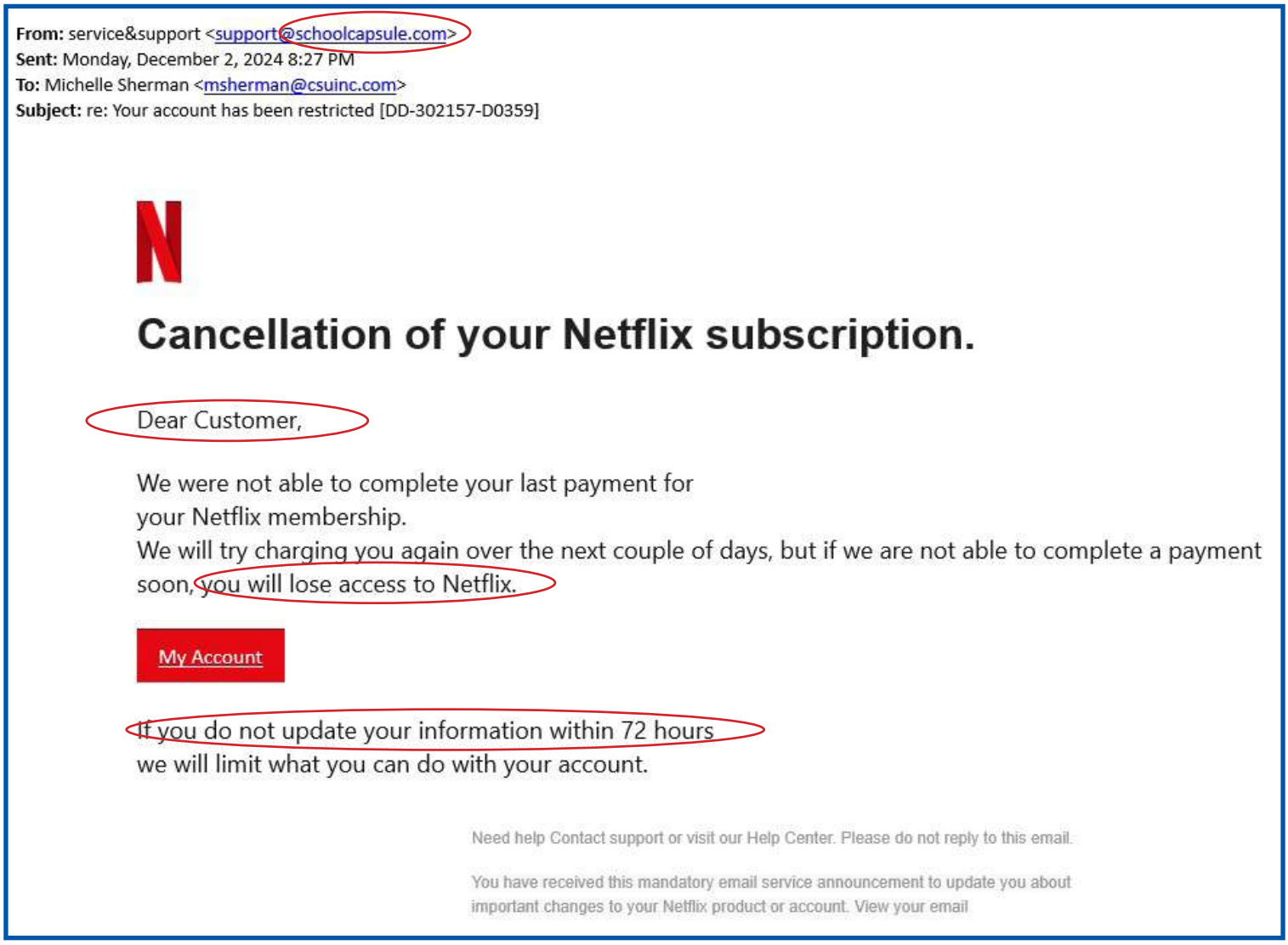


1. Asking for personal information
2. Gives an off-brand/unprofessional link
3. Gives specific and odd instructions
4. It specifies using a “Safari browser” which is specific to Apple products, how do they know what phone you have?

Tip: It’s good to ask yourself questions to verify any suspicion you may have.

USPS has confirmed they do not send texts

SPOT THAT PHISH #4 ANSWER



From: service&support <support@schoolcapsule.com>
Sent: Monday, December 2, 2024 8:27 PM
To: Michelle Sherman <msherman@csuinc.com>
Subject: re: Your account has been restricted [DD-302157-D0359]

Cancellation of your Netflix subscription.

Dear Customer,

We were not able to complete your last payment for
your Netflix membership.
We will try charging you again over the next couple of days, but if we are not able to complete a payment soon, you will lose access to Netflix.

My Account

If you do not update your information within 72 hours
we will limit what you can do with your account.

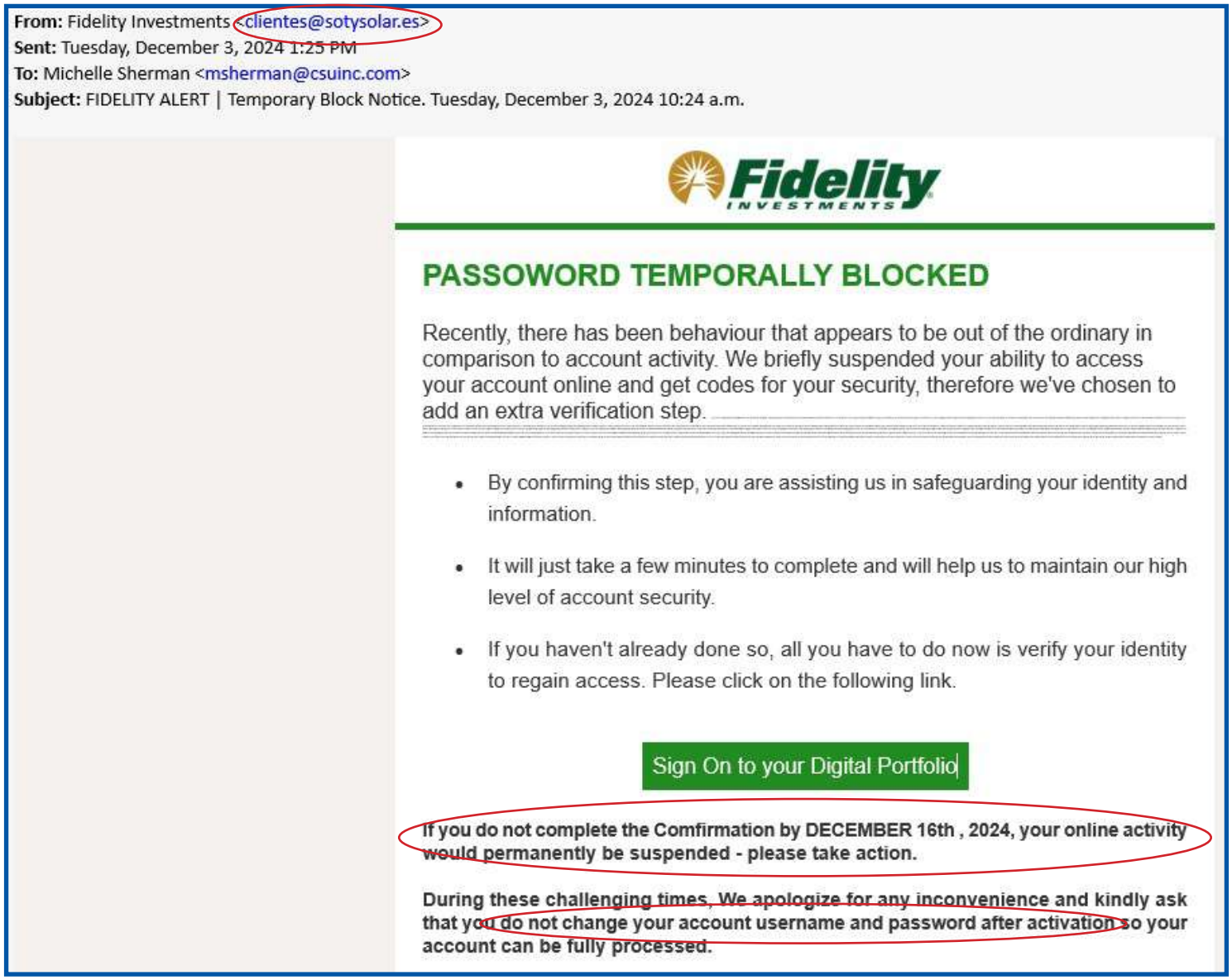
Need help Contact support or visit our Help Center. Please do not reply to this email.

You have received this mandatory email service announcement to update you about important changes to your Netflix product or account. View your email

1. The domain does not match with a typical Netflix domain
2. Greeting it too generic
3. Has a link that you can assume will lead you to a page to fill out payment information
4. It uses very urgent words “lose access” “within 72 hours”

Tip: When it comes to subscriptions, check your bank and credit card statements, and go directly to the company’s website to confirm you have a valid payment method.

SPOT THAT PHISH #5 ANSWER



From: Fidelity Investments <clientes@sotysolar.es>
Sent: Tuesday, December 3, 2024 1:25 PM
To: Michelle Sherman <msherman@csuinc.com>
Subject: FIDELITY ALERT | Temporary Block Notice. Tuesday, December 3, 2024 10:24 a.m.

Fidelity INVESTMENTS

PASSOWORD TEMPORALLY BLOCKED

Recently, there has been behaviour that appears to be out of the ordinary in comparison to account activity. We briefly suspended your ability to access your account online and get codes for your security, therefore we've chosen to add an extra verification step.

- By confirming this step, you are assisting us in safeguarding your identity and information.
- It will just take a few minutes to complete and will help us to maintain our high level of account security.
- If you haven't already done so, all you have to do now is verify your identity to regain access. Please click on the following link.

Sign On to your Digital Portfolio

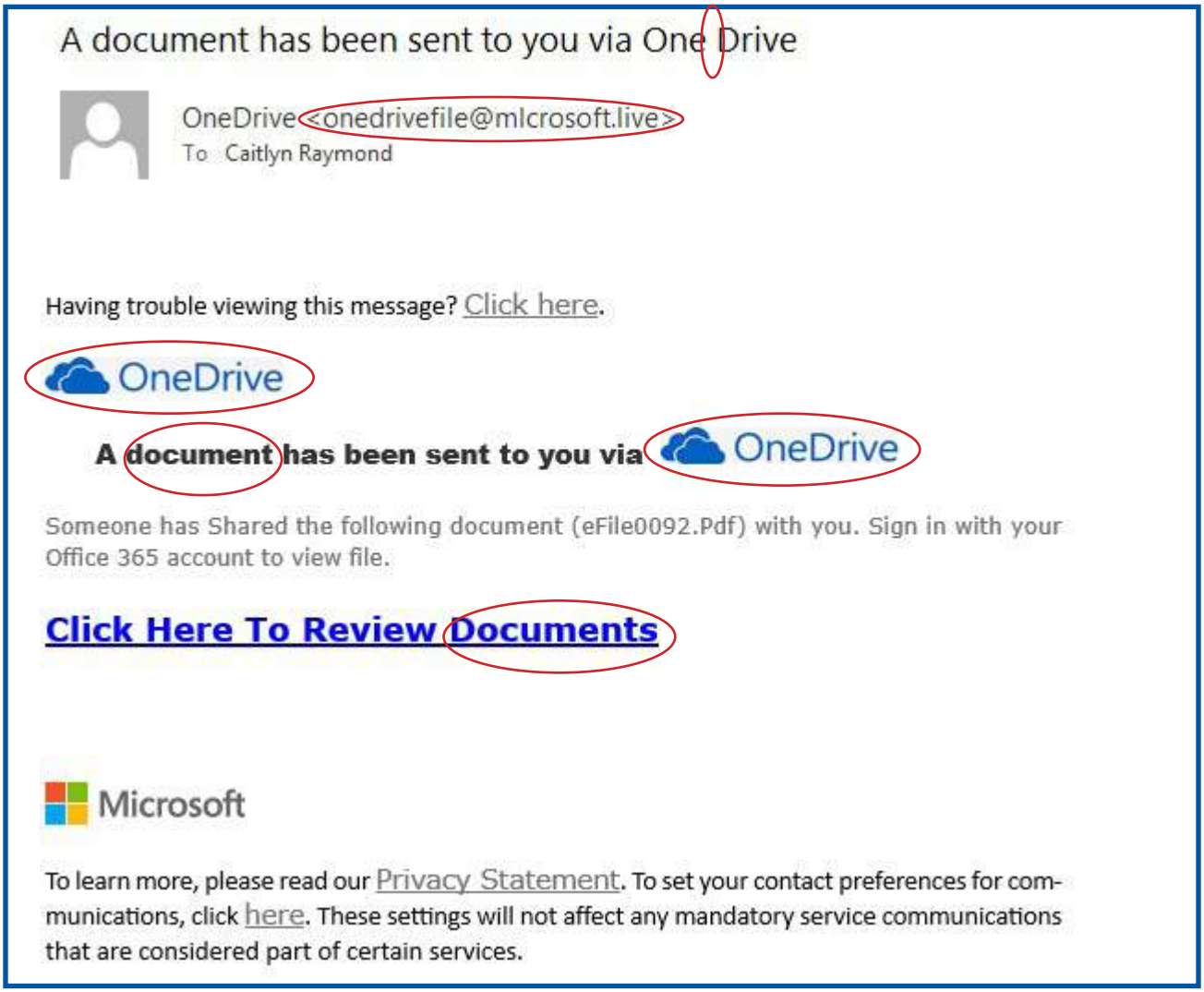
If you do not complete the Comfirmation by DECEMBER 16th , 2024, your online activity would permanently be suspended - please take action.

During these challenging times, We apologize for any inconvenience and kindly ask that you do not change your account username and password after activation so your account can be fully processed.

1. “Clients” is misspelled in the email address and the domain doesn’t match the company
2. Gives a link for you to give personal identifying information
3. Requires urgency with intense words such as “permanently”
4. Gives a suspicious request asking you to NOT change your username and password

Tip: Ask yourself, “is this even a company I do business with?”

SPOT THAT PHISH #6 ANSWER

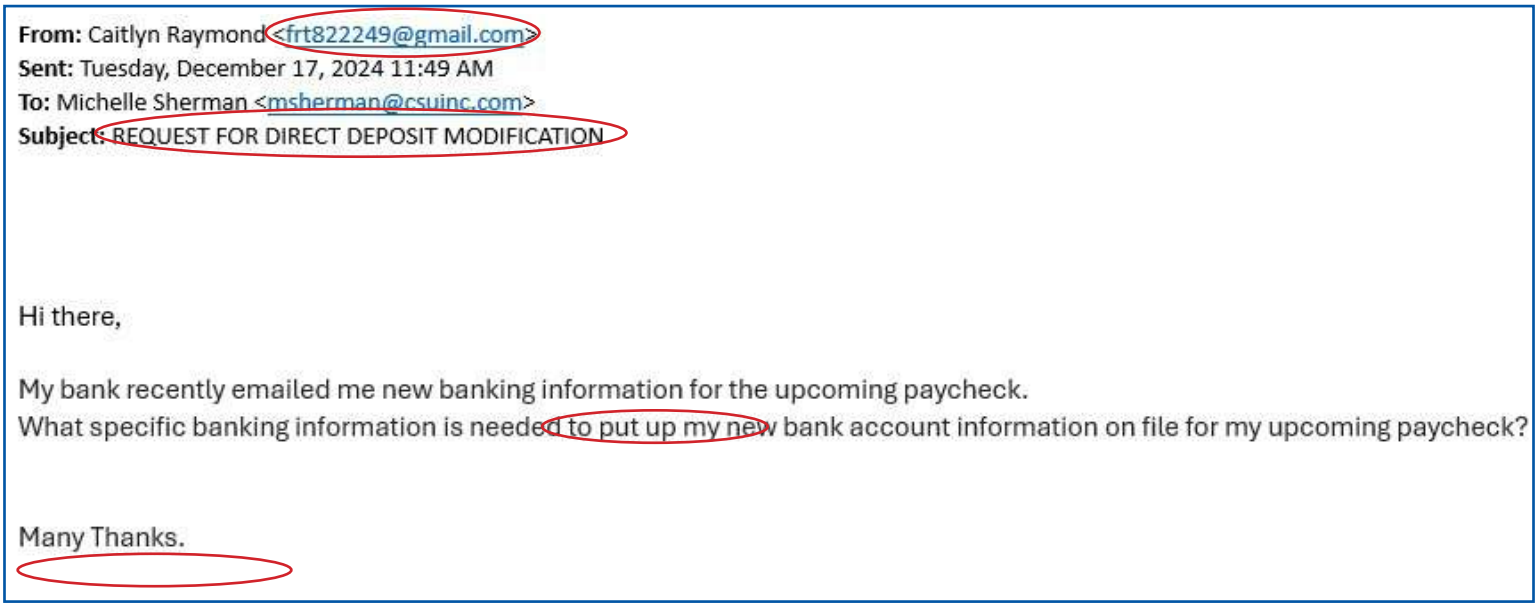


This one also requires some research:

1. This is not a username or domain that OneDrive uses although it looks right. Plus after the "m" in microsoft is an "l" not an "i"
2. The logo has a grey background (not professional) and is oddly placed, twice
3. It doesn't say who shared the file
4. It first says "document" then "documents" which is inconsistent
5. There are a lot of inconsistent fonts

Tip: Look for inconsistancies and unprofessionalism and make sure you know the sender.

SPOT THAT PHISH #7 ANSWER



From: Caitlyn Raymond <frt822249@gmail.com>
Sent: Tuesday, December 17, 2024 11:49 AM
To: Michelle Sherman <msherman@csuinc.com>
Subject: REQUEST FOR DIRECT DEPOSIT MODIFICATION

Hi there,

My bank recently emailed me new banking information for the upcoming paycheck.
What specific banking information is needed to put up my new bank account information on file for my upcoming paycheck?

Many Thanks.

1. A fake email address that doesn't match the employee's real email.
2. All caps subject isn't a good sign
3. Phrased in a way we wouldn't say things
4. No signature

Tip: Even if an email's content isn't necessarily suspicious, be sure to check other parts of an email to identify a phish.

Call the sender to verify an email is from them

BEST PRACTICES TO AVOID PHISHING ATTACKS:

Verify Email Sources

Always verify suspicious emails by contacting the sender through an official channel (such as a phone number from their website) instead of clicking any links or replying directly to the email.

Be Cautious with Links and Attachments

Before clicking any link or downloading an attachment, carefully inspect it. Hover over links to check the URL, and avoid opening files from untrusted sources.

Ask the Supposed Sender Directly

If you receive an email from someone at your company that seems off, don't reply to the email. Instead, reach out to them through another method (like phone or in person) to confirm whether they actually sent it.

Look for Red Flags in the Email

Pay attention to things like poor grammar, strange phrasing, or mismatched branding (e.g., distorted logos, low-quality images) that may indicate the email is not legitimate.

Don't Share Sensitive Information via Email

Never send personal or sensitive information (such as passwords, credit card details, or Social Security numbers) via email. Legitimate companies will never ask for this.

Educate Employees and Team Members

Regularly train your team to recognize phishing emails and ensure they know how to report suspicious activity.

Check for HTTPS in URLs

Always check for "https://" and a padlock symbol in the URL before entering sensitive data on a website. This indicates a secure, encrypted connection.

Report Suspicious Emails

If you receive a suspicious email, report it to your IT department or email provider. This helps protect your organization and prevent others from falling victim.

By following these best practices and being aware of the common signs of phishing, you can significantly reduce the risk of falling victim to a phishing attack and protect both your personal and business information.

CAN WE DO THIS FOR YOU, SO YOU DON'T HAVE TO THINK ABOUT IT?

We've covered a lot of ground, and it might seem a little overwhelming. But it doesn't have to add more stress to your load. Help is always available.

Whether you need to set up a phishing filter for your email or meet cyber insurance requirements, including cybersecurity training, we've got you covered!

CSU COMPUTER SERVICES UNLIMITED

14240-G Sullyfield Circle
Chantilly, VA 20151

Phone: 703-968-2600

Websites: csuinc.com,
vetitservices.com, csugov.com