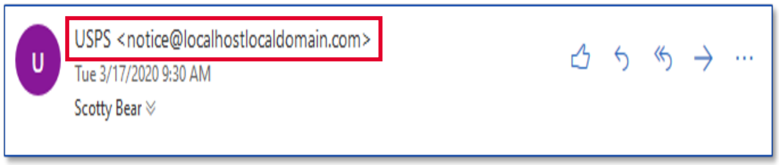
Tips for Spotting Phishing Emails

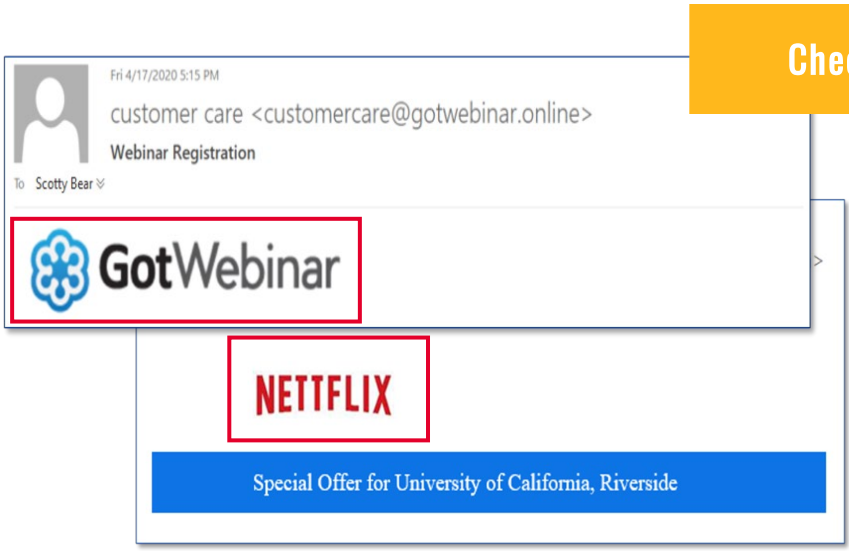
Check the sender

Make sure the sender information and the email address match. You would generally expect the sender email address to have the name of the sending organization in it. In this example you might expect the email to be notice@usps.com.



U USPS <notice@localhostlocaldomain.com>
Tue 3/17/2020 9:30 AM
Scotty Bear

Check the legitimacy of the company

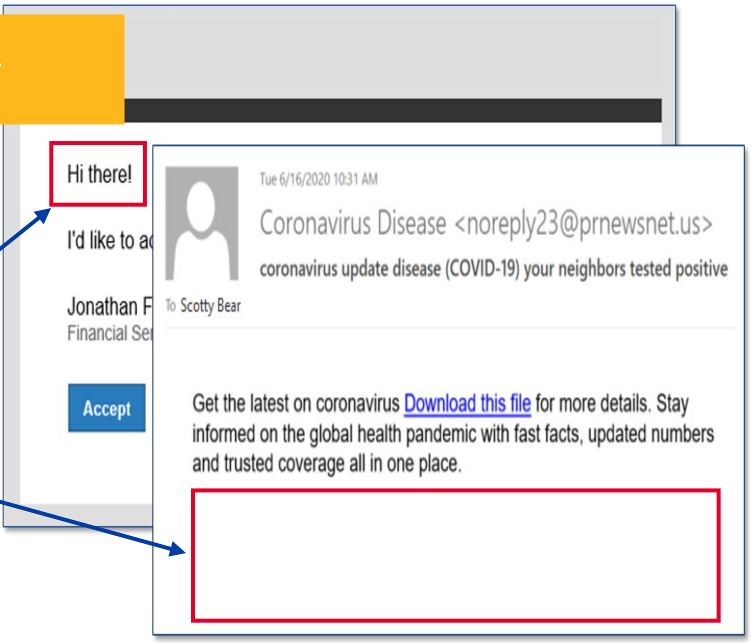


Fri 4/17/2020 5:15 PM
customer care <customercare@gotwebinar.online>
Webinar Registration
To Scotty Bear

Special Offer for University of California, Riverside

It is often the case that phishing emails will be sent from what appears to be a legitimate entity. However, there are often mistakes that reveal this is not the case. In these examples, the name of the company is spelled incorrectly. A quick internet search reveals these types of mistakes.

Check the email salutation and closing



Hi there!

I'd like to a

Jonathan F
Financial Se

Tue 6/16/2020 10:31 AM
Coronavirus Disease <noreply23@prnewsnet.us>
coronavirus update disease (COVID-19) your neighbors tested positive
To Scotty Bear

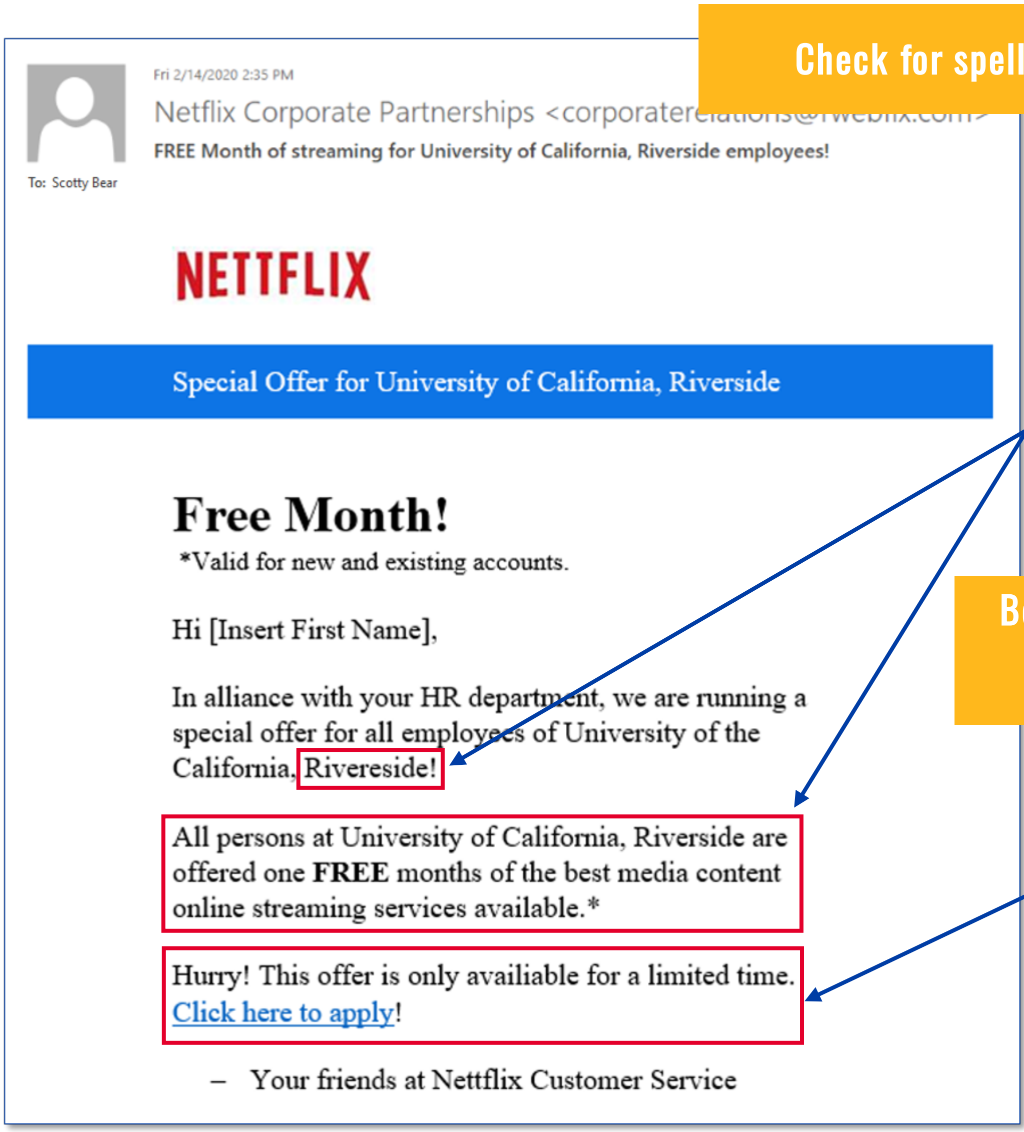
Get the latest on coronavirus Download this file for more details. Stay informed on the global health pandemic with fast facts, updated numbers and trusted coverage all in one place.

In phishing emails, the salutation and closing of emails is often absent or not appropriate.

Generally, directed emails like this example would be addressed to a specific individual rather than a generic greeting like 'Hi there!'

The closing of a legitimate email would generally have information about the sending company, a means to make contact, or to unsubscribe from future emails.

Tips for Spotting Phishing Emails



Fri 2/14/2020 2:35 PM

Netflix Corporate Partnerships <corporaterelations@rwebflix.com>

FREE Month of streaming for University of California, Riverside employees!

To: Scotty Bear

NETTFLIX

Special Offer for University of California, Riverside

Free Month!

*Valid for new and existing accounts.

Hi [Insert First Name],

In alliance with your HR department, we are running a special offer for all employees of University of the California, Rivereside!

All persons at University of California, Riverside are offered one **FREE** months of the best media content online streaming services available.*

Hurry! This offer is only availiable for a limited time. Click here to apply!

– Your friends at Nettflix Customer Service

Check for spelling / grammar errors

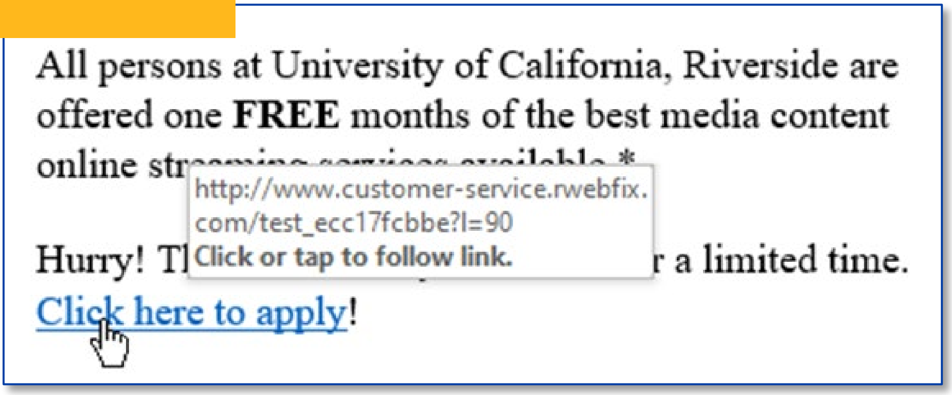
Phishing emails often contain spelling and grammar errors. It would be very unusual to see mistakes in a legitimate email. If you notice these types of errors, you should definitely proceed with caution.

Be aware when there is an urgent call to action

Beware when an email contains an urgent call to action. Phishing email will try to get you to act quickly so that you don't have time to think before acting.

Hover over the links in emails

It is always good practice to hover over the links in emails. Hovering over the link will show you where you will be redirected when you click it. This practice often reveals fraudulent links.



All persons at University of California, Riverside are offered one **FREE** months of the best media content online str

http://www.customer-service.rwebfix.com/test_ecc17fcbbe?l=90

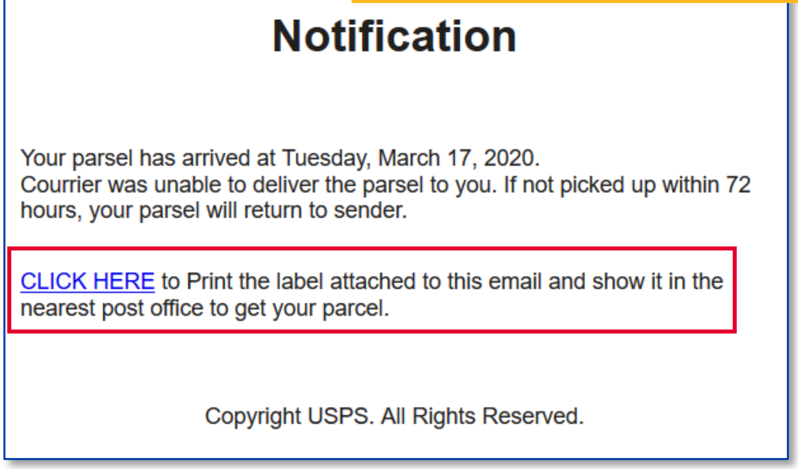
Click or tap to follow link.

Hurry! Tl r a limited time.

Click here to apply!

Tips for Spotting Phishing Emails

Look for information in the email that doesn't make sense



Notification

Your parsel has arrived at Tuesday, March 17, 2020.
Courrier was unable to deliver the parsel to you. If not picked up within 72 hours, your parsel will return to sender.

CLICK HERE to Print the label attached to this email and show it in the nearest post office to get your parcel.

Copyright USPS. All Rights Reserved.

Think about whether the email even makes sense. In this example, you are instructed to go to the nearest post office to get your parcel. If this were genuine, it would specify which post office has your package.

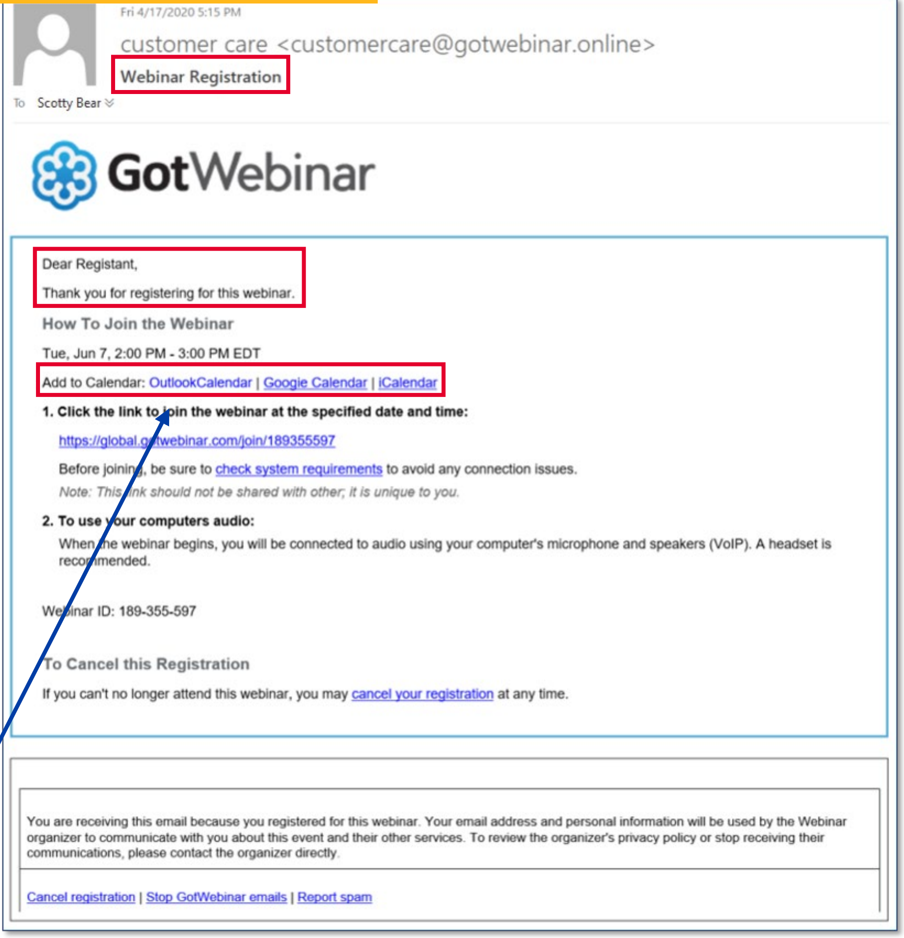
There is a good chance that if something doesn't quite make sense, that the email is a phishing scam.

Is the information in the email body / subject vague?

Using vague information is another sign of a phishing email. In this example, you would expect the subject to contain specific information about the webinar. Again, in the body you might expect more specific information. In addition, the subject and body of the email suggest that you registered for a webinar. If this is the case, you should compare the details of the email to the webinar you did register for.

Look for inconsistencies in the formatting of the email

In addition to the spelling and grammar errors highlighted earlier, phishing emails often have formatting errors in terms of inconsistent use of fonts and font sizes.



Fri 4/17/2020 5:15 PM

customer care <customercare@gotwebinar.online>

Webinar Registration

To Scotty Bear

GotWebinar

Dear Registant,

Thank you for registering for this webinar.

How To Join the Webinar

Tue, Jun 7, 2:00 PM - 3:00 PM EDT

Add to Calendar: OutlookCalendar | Google Calendar | iCalendar

1. Click the link to join the webinar at the specified date and time:

https://global.gotwebinar.com/join/189355597

Before joining, be sure to check system requirements to avoid any connection issues.

Note: This link should not be shared with other; it is unique to you.

2. To use your computers audio:

When the webinar begins, you will be connected to audio using your computer's microphone and speakers (VoIP). A headset is recommended.

Webinar ID: 189-355-597

To Cancel this Registration

If you can't no longer attend this webinar, you may cancel your registration at any time.

You are receiving this email because you registered for this webinar. Your email address and personal information will be used by the Webinar organizer to communicate with you about this event and their other services. To review the organizer's privacy policy or stop receiving their communications, please contact the organizer directly.

Cancel registration | Stop GotWebinar emails | Report spam

Tips for Spotting Phishing Emails

Consider all of the factors

It is unlikely that a phishing email will contain all of the errors outlined above. You may only be looking for one error. This means that to spot phishing emails, you need to be vigilant and consider all of the possible issues outlined in this document.

If you do consider all the factors when looking at an email you might thing is suspicious, it will greatly reduce your risk of getting caught out by a phishing scam.

Remember! If it doesn't look right, it probably isn't!!

Trust your instincts. If you suspect an email is suspicious, you should treat it as such.

It is better to be safe than sorry!