

How to Check if an Email is Real or Not (Phishing)

I just received this email and noticed it's a phishing email, so I thought I'd explain **a few ways to easily check for scam emails**.

This one says it's from "Onedrive" and the subject line was "New File Received."

Onedrive ▾

New File Received.

To: Recipients



This document requires your signature urgently. It has been securely upload for your safety on OneDrive Cloud. To sign your document online please follow the command below :

Sign Here

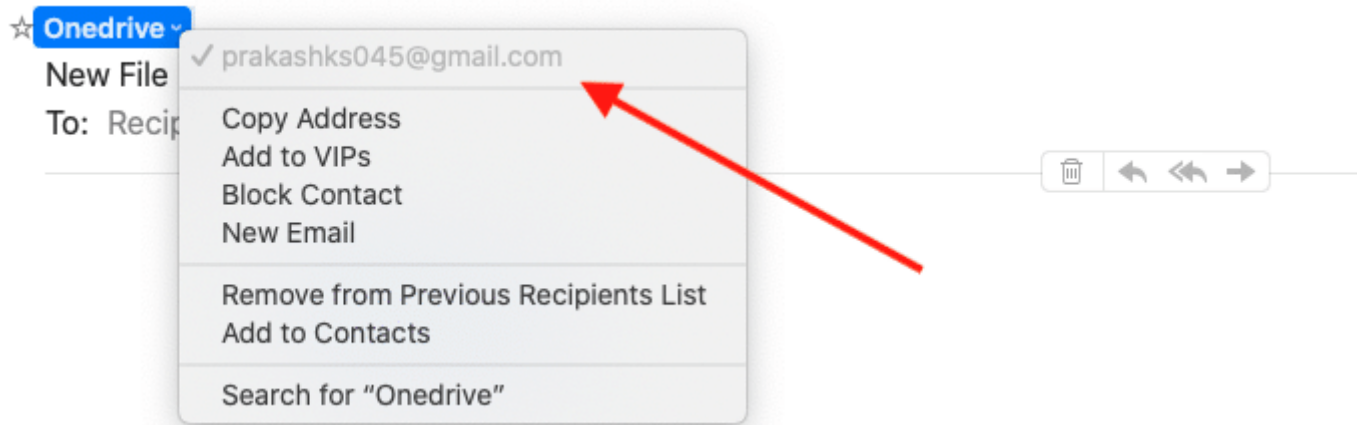
This document does not required to be downloaded. Sign your document online and it will be automatically forwarded to your contact.

[Contact Microsoft](#) [Privacy & Cookies](#) [Terms of Use](#) [Trademarks](#) [About our ads](#) © Microsoft 2020

First, check for misspellings, bad grammar, and bad punctuation.

- "Onedrive" should have been "OneDrive" – so that's wrong
- I see a space before a colon – that's a common way of using a colon in India.
- "It has been securely upload for your safety" – that's bad English.
- The "Sign Here" button's spacing looks off.
- "This document does not required to be downloaded" – more bad English.

Second, mouse over or click on who it's from to reveal the real name:



This document requires your signature urgently. It has been securely upload for your safety on OneDrive Cloud. To sign your document online please follow the command below :

Sign Here

This document does not required to be downloaded. Sign your document online and it will be automatically forwarded to your contact.

[Contact Microsoft](#) [Privacy & Cookies](#) [Terms of Use](#) [Trademarks](#) [About our ads](#) © Microsoft 2020

OK, Mr. Prakash from India... I suspect you're not Microsoft but a scammer.

Third, mouse over the link without clicking on it to see where it goes:

☆ Onedrive

New File Received.

To: Recipients



This document requires your signature urgently. It has been securely upload for your safety on OneDrive Cloud. To sign your document online please follow the command below :

Sign Here 

This docu
online and

led. Sign your document
your contact.

Contact Microsc

bout our ads

© Microsoft 2020

https://u14379061.ct.sendgrid.net/ls/click?
upn=dy820qOi-2Bdog2yM5NXCCChWaHFT7j8jyeW
MrNZgOn9u9KJwXvbAnimjgXIQg8-2BPJpBnNnSA
ppVdTsdj4SSWzaxw-3D-3DO1nm_MpfCaMHPVe-
2B5W2aHcCz1UoaghPhpUtpKTRsDCcgkzhnLqTT
Vhi-2FKfKZR52rCkWzvgs35m0bSaKBGk0ZRdzgn
khanZ029cLj0M8SpcnYapyQwcequsYdKQ-2FB1uH
eQZbLgXmHmu0TzsD7oKFZHaG1sg9YXa-2B-2Bjt
mbu-2FTjpP8JEA762oy26lnLP7QipfwmeMc1yf4FA
l0xphlOrfU02wTw42Ui4btWJVnsm0tQ0ze8cNIYCi
8vTyCenEj2wrU8iJluW

And sendgrid.net doesn't match anything to do with Microsoft, I don't think. Sure, some emails might have this not matching but in light of everything else going on with this email, I'm calling shenanigans on this. It's a scam.

What if I Clicked on the Link?

Well, I did – but just to show you what happens.

Here's how it looks in Firefox (still a great browser in my opinion):



Deceptive site ahead

Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

Advisory provided by [Google Safe Browsing](#).

Go back

pxi.ferter.net has been reported as a deceptive site. You can report a detection problem, ignore the risk and go to this unsafe site.

Learn more about deceptive sites and phishing at www.antiphishing.org. Learn more about Firefox's Phishing and Malware Protection at support.mozilla.org.

And in Chrome (a little rougher on the eyes):



Deceptive site ahead

Attackers on **onees.s3-website.us-east-2.amazonaws.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). [Learn more](#)

☐ Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Hide details

Back to safety

Google Safe Browsing recently [detected phishing](#) on onees.s3-website.us-east-2.amazonaws.com. Phishing sites pretend to be other websites to trick you.

You can [report a detection problem](#) or, if you understand the risks to your security, [visit this unsafe site](#).



Crazy, Right?

I figured it out right away this time and my browser also caught it but to help make sure you don't get fooled, you want as many safety checks in place as possible.

That's why **I wrote a book** about a very easy way to get another layer of protection in place – for both phishing sites and for adult websites (to help make sure they don't pop up).

Go read more about it here – CLICK

Original article: <https://tonyherman.com/check-for-phishing-emails/>

PDF version: https://tonyherman.com/check-for-phishing-emails/?apa_pdf=1

Special Offer for Readers

1,000+ Channels • On-Demand Movies • **5 Devices**

\$69.99/mo (~\$2.33/day)

Try it for a month and see if you like it, then switch.

Start Your Trial

Click to learn more about CUE Broadcast

Tip: Get 3 friends or family to sign up and you get it for free.