SanityWORX

How to Avoid Being the Victim of a Phishing Scam

Phishing (pronounced "fishing") is a technique used by hackers in the attempt to steal information from you or to take control of your PC. Usually an email is used that looks like an email you may expect to get from your bank, from an online service like OneDrive or NetFlix, as an advertisement for a popular store like Best Buy, or a shipment notification from companies like UPS or FexEx.

Currently, scammers are using the COVID-19 threat as a subject for their scams. Any emails from WHO and the CDC, offers of a "little known cure", special access to vaccines, "new information" or claims to be a charitable organization looking for donations are VERY SUSPECT!!! The WHO and CDC emails especially well done and look just like that organization's real emails.

We have also seen a significant increase in "spear phishing" activities. This is where the sender pretends to be the person's supervisor, company president, HR department or perhaps your bank representative. The emails are usually friendly, but urgent and may ask for a cell phone number to initiate a text conversation or gives explicit and urgent instructions to write a check, wire money, send product etc. These people have done research on your company and act in a way that is designed to gain your confidence and trust.

Here's how you can detect and avoid being the victim of these types of malicious emails:

1. **Look at email suspiciously!** Did I order something from this company? Would my bank really send this to me? Why would "Joe" send me an attachment? If there is *any* question in your mind about whether a message is legitimate, call or email the sender, or go directly to their website to verify. Never click on a link in an email to go someplace important like your bank as the link may lead to a fake website that is designed to look like the real one.
2. **Use some cool tools to check links.** Did you know if you pass your mouse cursor over a link that you find in an email, in your browser or a document, it will display the REAL address to which the link leads, either in a small pop-up window or at the top or bottom of your browser window? Let's practice! Hover your cursor—DON'T CLICK—over this link to a website you know and likely trust: www.amazon.com. You will see a box that shows the bestbuy.com URL, not amazon.com! ALWAYS check your links before clicking! Often you will find that phishing scams use similar, but not correct, names such as "WellsFargoUSA.com" instead of "WellsFargo.com," or a fake domain like "wellsfargo.wewir.com," etc.
3. **Never, EVER give out personal information to people contacting you by email, text message, or phone!** When someone calls you and tells you they are from your bank, ask for an extension and then call the published number (not the one they give you) of the bank and ask for that extension. If you receive a text or email requesting that you click on a link and log in, DO NOT DO IT! Simply go to the site directly and verify you get the correct site before entering any information.
4. **"All your bases are belong to us!"** If you notice poor spelling or grammar, or generic greetings or titles like "Dear Customer" or "Office Manager," you can be quite certain the email is junk and most likely dangerous, as anyone who knows you will most likely use your correct name.
5. **Many messages imply urgency to get you to click on something.** Subject lines like "Today ONLY!" or "Urgent Attention Required!" are designed to get people to feel anticipation or worry and act

without caution in opening links or attachments. Take your time. Think. If you feel anxiety, that should act as a trigger to tell you to step back and analyze the situation before taking action.

6. **You are asked to do something that is not normal or with great urgency.** Emails, text messages, voice calls etc. that urge you to do something that does not follow normal procedures or that goes around a supervisor or process is ALWAYS bad! Simply use a different method of communication to contact your team and verify that the action is correct and approved before doing anything!

Trust your instincts! It if seems too good to be true, it likely is. If links or attachments don't seem right, DO NOT OPEN THEM! Don't trust any links or attachments without verifying them first. Never give username, password, or other personal information to people who contact you—only when you contact them.

A little forethought can save you hours (days, weeks) of headaches—not to mention financial loss—by avoiding being the successful target of a phishing scam. Remember, ***you*** are in control. Use that fact to your advantage in protecting yourself and your company against scammers who prey on those who don't know how to protect themselves.

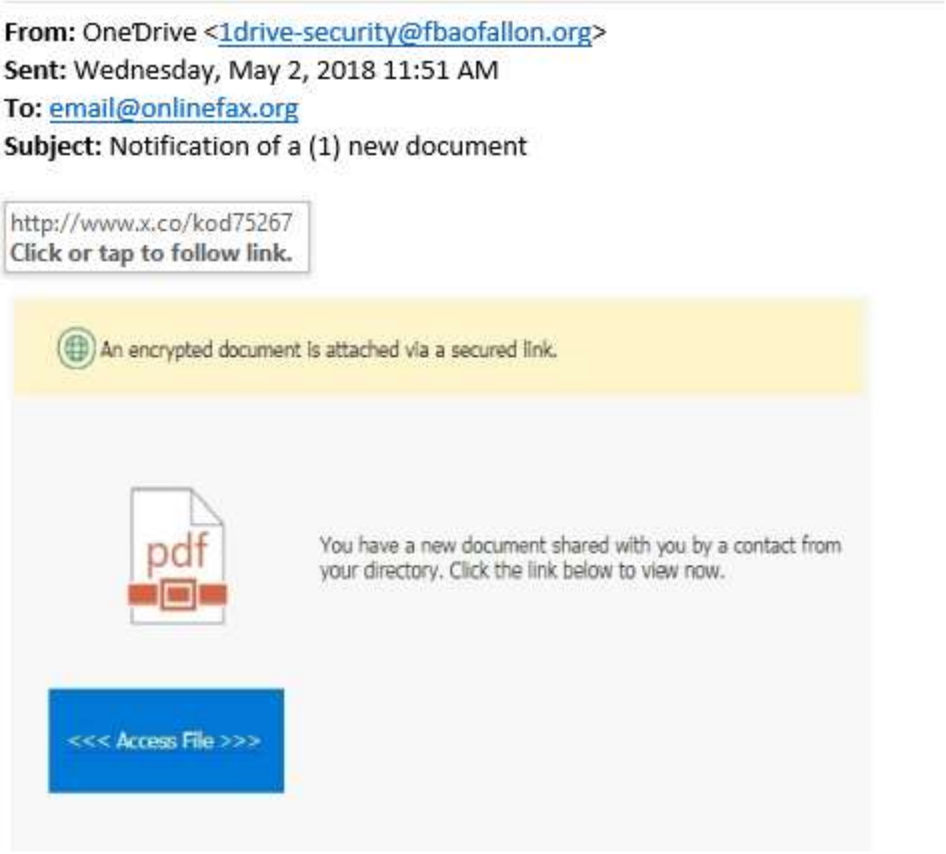
Since the elderly are special targets of scammers, please share this knowledge and teach them how to avoid phone, text and email scams.

See Examples and Tips for spotting these emails below.

Tips for Spotting Phishing Emails

Example 1: Phishing emails (And links in web pages and documents) contain signs that you can look at to see if there is an issue. In the OneDrive email below, there are several items that give it away.

- The email says that it is from the Microsoft OneDrive service, but the "From:" sender address is from a completely different email address
- The "To:" line is not addressed to me, but to a different address. Suspicious!
- When we move our mouse pointer over the blue "Access File" box, we get the white pop-over box (tool tip) that has a completely different address: http://www.x.co/kob75267. This is a dead give away that this is wrong. If you have an email from Microsoft, the links should point to a Microsoft link! Be careful of tricky links as mentioned on Page 1. For instance, http://microsoft.com.sanityworx.com/?/23423 is NOT a link to Microsoft! Please follow the link till you get to the first "/" after the domain. Just to the left of it will be the domain, in this case it is "sanityworx.com". If you need more clarification, please let us know.



From: OneDrive <1drive-security@fbaofallon.org>
Sent: Wednesday, May 2, 2018 11:51 AM
To: email@onlinefax.org
Subject: Notification of a (1) new document

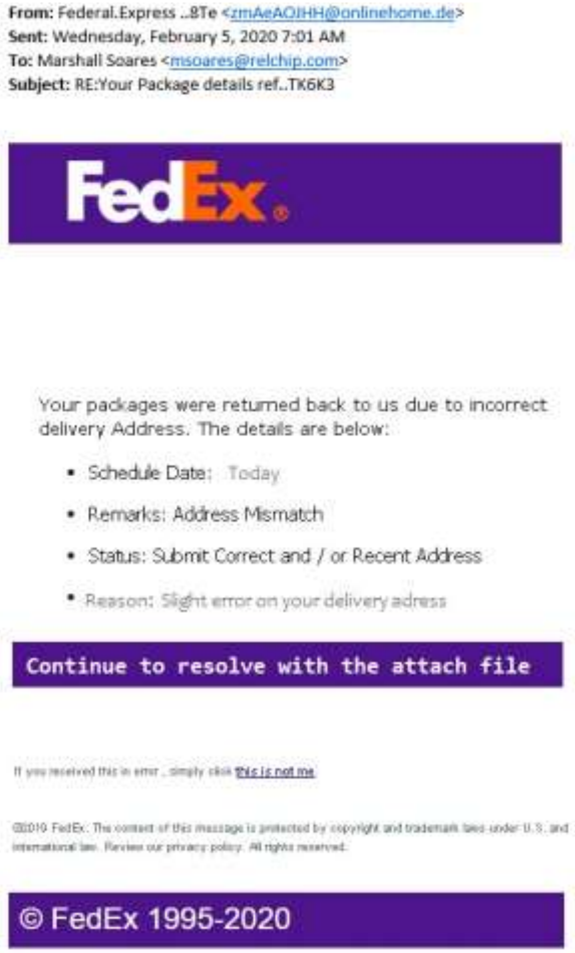
http://www.x.co/kod75267
Click or tap to follow link.

An encrypted document is attached via a secured link.

You have a new document shared with you by a contact from your directory. Click the link below to view now.

Example 2: This email seems at first glance to be from FedEx.

- From address is not FedEx.com, but zmAeAOJHH@onlinehome.de.
- Mousing over the FedEx link gives a link to “ecolotime.com” in the actual email.
- Remember that the “mouse over link”, not the displayed text, is where a click will take you.
- Typos and missuse of language. “Continue to resolve with the attach file”



From: Federal.Express ..8Te <zmAeAOJHH@onlinehome.de>
Sent: Wednesday, February 5, 2020 7:01 AM
To: Marshall Soares <msoares@relchip.com>
Subject: RE:Your Package details ref..TK6K3

Your packages were returned back to us due to incorrect delivery Address. The details are below:

- Schedule Date: Today
- Remarks: Address Mismatch
- Status: Submit Correct and / or Recent Address
- Reason: Slight error on your delivery adress

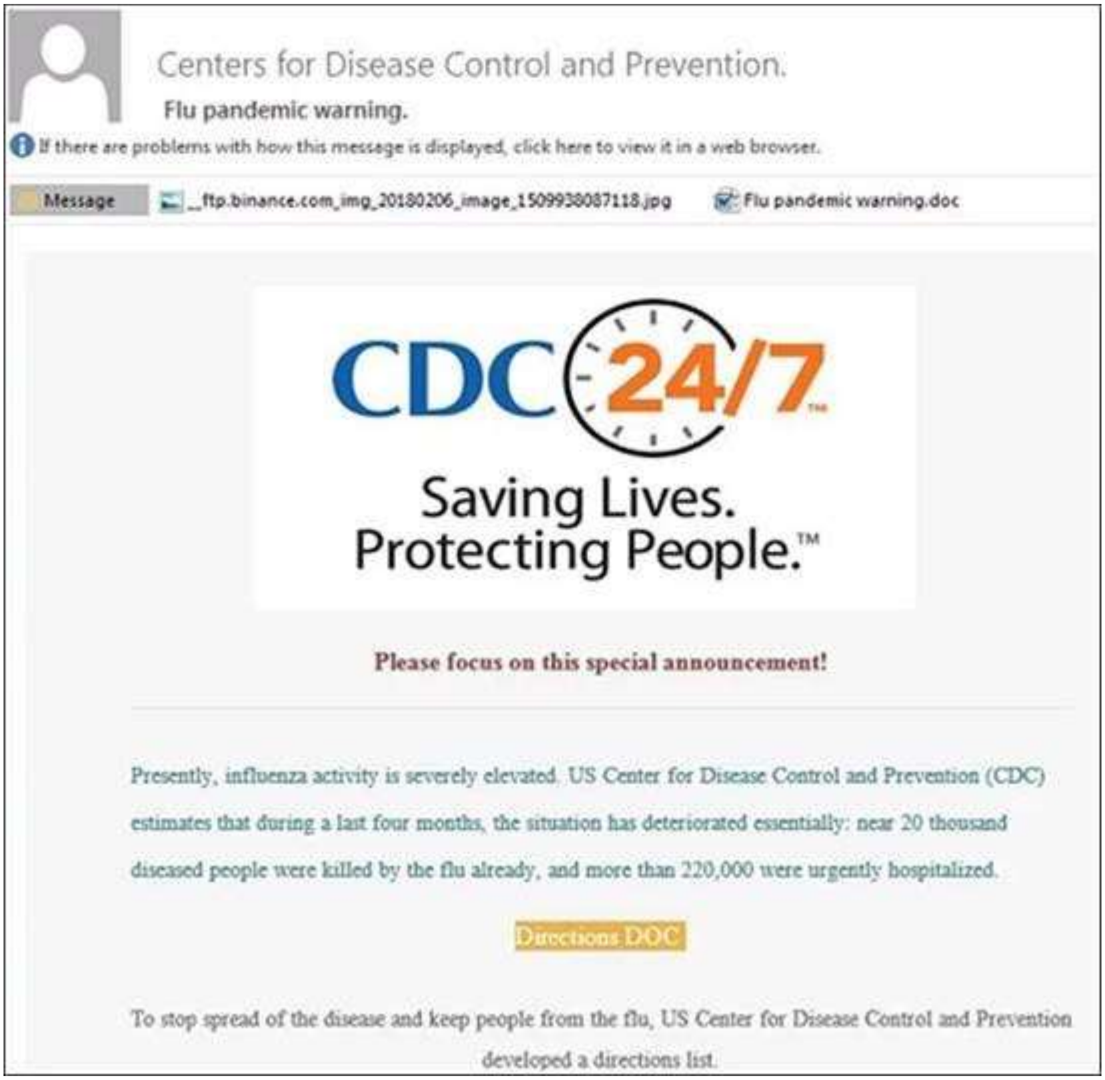
If you received this in error ...simply click this is not me.

©2019 FedEx. The content of this message is protected by copyright and trademark laws under U.S. and international law. Review our privacy policy. All rights reserved.

© FedEx 1995-2020

Example 3: This email appears to be from the Center for Disease Control (CDC)

- The email contains a Word document that was really a malicious program that will damage your computer and steal information. NEVER open a Word, Excel or other document from an unknown sender and be very suspicious of these types of files that are sent to you. You should call or email the sender to make sure that they really sent the file to you before opening.



Centers for Disease Control and Prevention.

Flu pandemic warning.

If there are problems with how this message is displayed, click here to view it in a web browser.

Message | _ftp.binance.com_img_20180206_image_1509938087118.jpg | Flu pandemic warning.doc

Please focus on this special announcement!

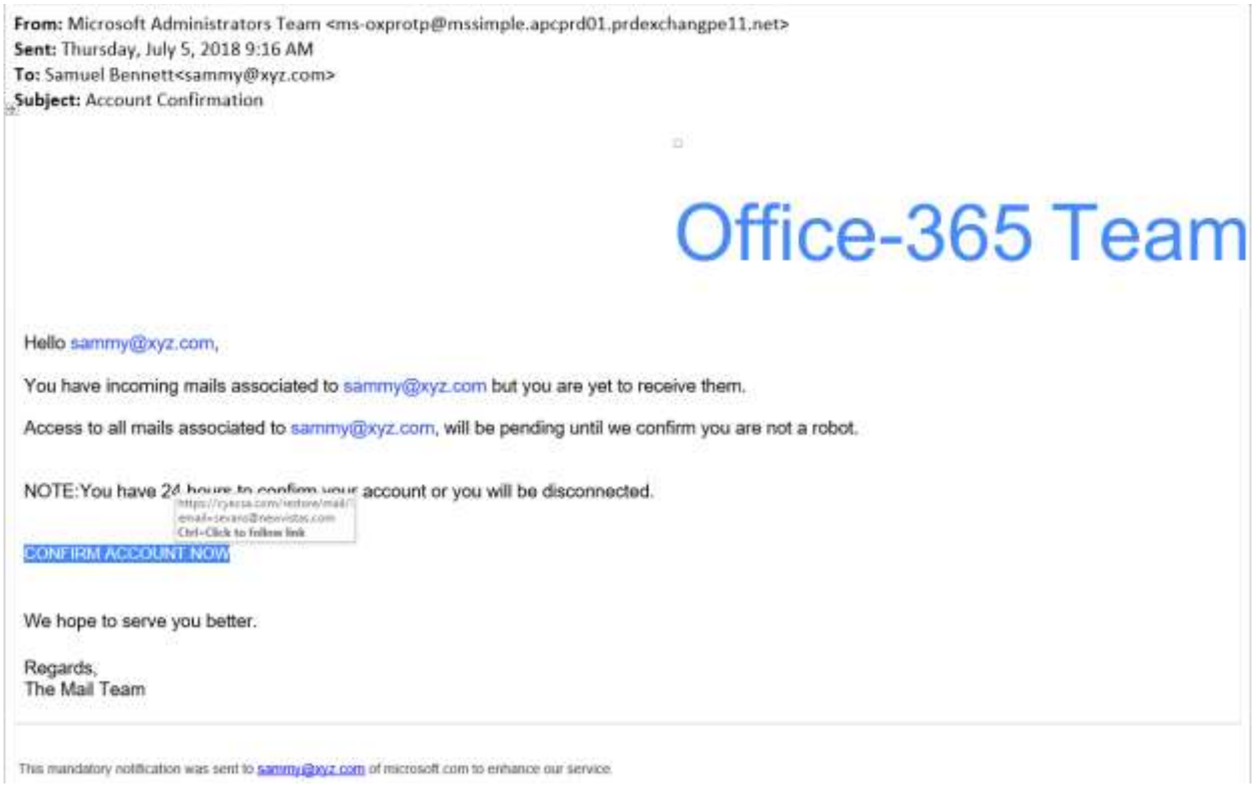
Presently, influenza activity is severely elevated. US Center for Disease Control and Prevention (CDC) estimates that during a last four months, the situation has deteriorated essentially: near 20 thousand diseased people were killed by the flu already, and more than 220,000 were urgently hospitalized.

Directions DOC

To stop spread of the disease and keep people from the flu, US Center for Disease Control and Prevention developed a directions list.

Example 4: This email seems to be from Microsoft Office…at first glance!

- From address is not Microsoft.
- Typos and missuse of language. “…but you are yet to receive them.”
- Mousing over the “Confirm Account Now” blue box shows a link to “cyecsa.com”. Definitely not a Microsoft domain!



From: Microsoft Administrators Team <ms-oxprotp@mssimple.apcprd01.prdexchangpe11.net>
Sent: Thursday, July 5, 2018 9:16 AM
To: Samuel Bennett<sammy@xyz.com>
Subject: Account Confirmation

Office-365 Team

Hello sammy@xyz.com,

You have incoming mails associated to sammy@xyz.com but you are yet to receive them.

Access to all mails associated to sammy@xyz.com, will be pending until we confirm you are not a robot.

NOTE:You have 24 hours to confirm your account or you will be disconnected.

https://cyecsa.com/restore/mail/?
email=sevaro@neevistas.com
Ctrl+Click to follow link

CONFIRM ACCOUNT NOW

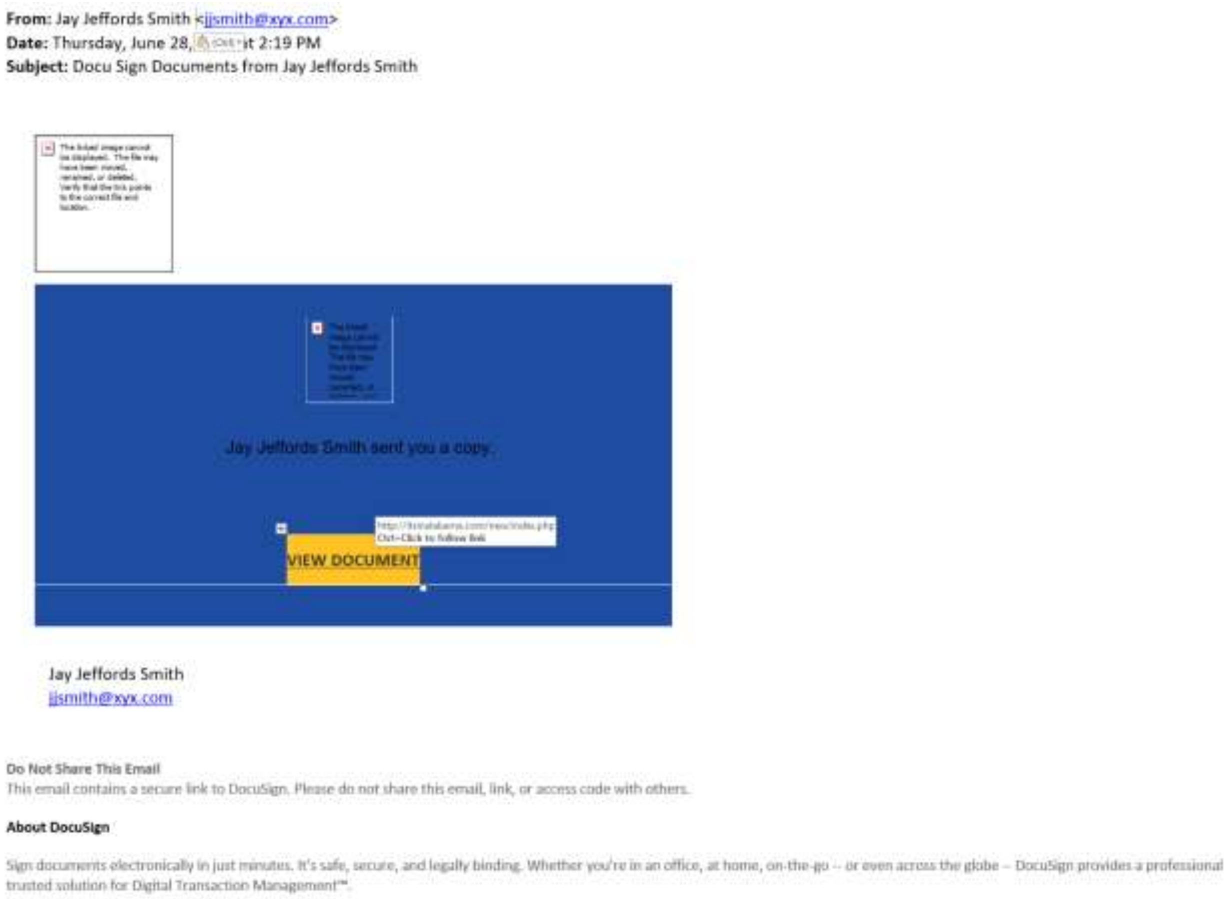
We hope to serve you better.

Regards,
The Mail Team

This mandatory notification was sent to sammy@xyz.com of microsoft.com to enhance our service.

Example 5: This is one that appears to be from Docusign. It was designed to hijack a user's Office 365 account. Once that happens, the hacker can send an even more convincing phishing email to all of that person's contacts within and outside the company. (Modern email applications do not load graphics unless you tell it to download pictures so there are boxes with missing graphics. This email looks very authentic when the photos are showing. I just don't like to download photos unless absolutely necessary.)

- The From: address is from a person that we know in the company, so you might think that this is trustworthy… Lets always check other things though!!!!
- Mousing over the "View Document", yellow colored box and link, we see that link is to a site, "ItsInAlabama.com"! I don't think that is what DocuSign would want us to visit!



From: Jay Jeffords Smith <jjsmith@xyx.com>
Date: Thursday, June 28, [illegible] at 2:19 PM
Subject: Docu Sign Documents from Jay Jeffords Smith

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Jay Jeffords Smith sent you a copy.

http://itsinalabama.com/new/index.php
Ctrl+Click to follow link

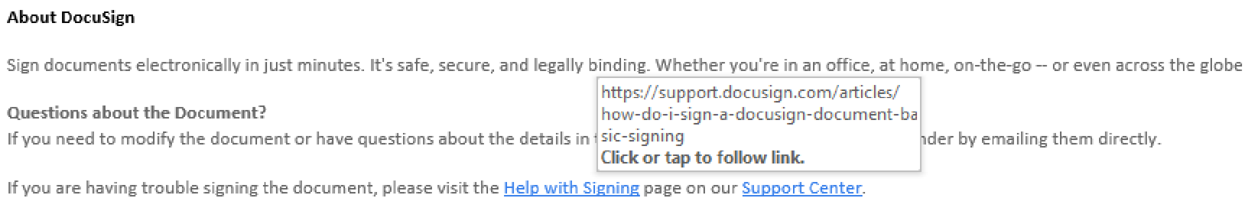
Jay Jeffords Smith
jjsmith@xyx.com

Do Not Share This Email
This email contains a secure link to DocuSign. Please do not share this email, link, or access code with others.

About DocuSign

Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe – DocuSign provides a professional trusted solution for Digital Transaction Management™.

NOTE: Often, only the "call-to-action" part of the email will have bad links, the others, like the support link on the DocuSign email below are real links to DocuSign. Make sure that you are checking EACH link before you click on it!



About DocuSign

Sign documents electronically in just minutes. It's safe, secure, and legally binding. Whether you're in an office, at home, on-the-go -- or even across the globe

Questions about the Document?
If you need to modify the document or have questions about the details in t…nder by emailing them directly.

https://support.docusign.com/articles/how-do-i-sign-a-docusign-document-basic-signing
Click or tap to follow link.

If you are having trouble signing the document, please visit the Help with Signing page on our Support Center.