



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 BestBuy™, or a shipment notification from companies like UPS™ or FedEx®.

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 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 find it shows the bestbuy.com URL, not amazon.com! ALWAYS check your links before clicking! Often you will find 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.

Trust your instincts! If it 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 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.

Tips for Spotting Phishing Emails

Example 1

Phishing emails (and links in web pages and documents) contain signs you can look for to see if there is a possibility you are being targeted for a phishing scam. In the example email below—purporting to be from Microsoft® regarding OneDrive™—there are several items that give it away as a phishing email:

- The email says it is from the Microsoft® OneDrive™ service, but the “From” sender address has nothing to do with Microsoft® or any of its products. (fbaofallon.org is clearly not a Microsoft® URL.)
- The “To:” line is not addressed to a human recipient (make sure it is YOUR address, not even another person’s). 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 giveaway that this is a phishing email. If you have an email from Microsoft®, the links should point to a Microsoft® site! Be careful of tricky links as mentioned on Page 1.

Example: <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,” my company’s URL. If you need more clarification, please let us know.

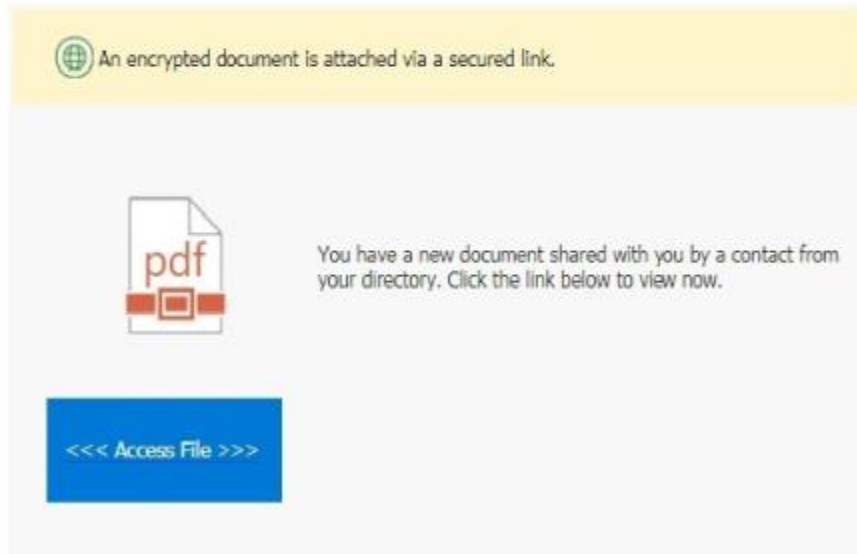
From: OneDrive <1drive-security@fbaofallon.org>

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.



Example 2

This next email (below) seems, at first glance, to be from FedEx®.

- Note the “From” address does not end with “FedEx.com,” but rather “skura.ne.jp.”
- Mousing over the purported FedEx® link reveals a link to “ecolotime.com.”
- Remember that the mouseover link, *not the displayed text*, is where a click will take you.
- Typos and misuse of language is also a giveaway: e.g. “Below is what us needed from you..”

From: FedEx <do-not-reply-global--noussf-xyz@61346.sakura.ne.jp>

Sent: Tuesday, May 29, 2018 4:52 AM

To: Mary Lee <mlee@xyz.com>

Subject: Package Scheduled Delivery Delayed


📧

This shipment was sheduled to be received on 27/05/2018

To mlee@xyz.com

Your parcel has arrived at our terminal and we couldn't find your correct delivery address. Below is what us needed from you.:

- Recent delivery address.
- Your correct name
- Status: Submit

Kindly provide us with  below.

https://fedex.com/tracking_shipment/KlrvWtaIDqSE6SAsiLGgDg

We hope to be able to reach you as soon as possible.

Best Regards

FEDEX Dispatch Personnel

Example 3

This email seems to be from Microsoft® Office™...at first glance! Here are signs it is a phishing email:

- The “From” address is not Microsoft®.
- Typos and misuse of language: e.g. “...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=sevans@newvistas.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 4

This is one that appears to be from DocuSign®. It was designed to hijack a user's Office365™ 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.

NOTE: Modern email applications do not load graphics unless you tell them 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.

Let's analyze this email...

- The "From" address is a person we know in the company, so you might think this is a valid email. Let's always check other things though!
- Mousing over the "View Document" yellow colored box and link, we see the link leads to a site at "ItsInAlabama.com." I don't think that is where DocuSign® hosts its site! Do you?

From: Jay Jeffords Smith <jjsmith@xyx.com>
Date: Thursday, June 28, 2018 at 2:19 PM
Subject: Docu Sign Documents from Jay Jeffords Smith



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 you check EACH link before you click on it! (See graphic on next page...)

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 this document, please contact your account manager by emailing them directly.

<https://support.docusign.com/articles/how-do-i-sign-a-docusign-document-basics-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](#).

We hope these guidelines and examples are helpful to you and your team. Please use this document in your ongoing training.

We also offer an innovative **tool that trains your team members in real time** as they are using their email to help them apply these skills in a real world environment. It takes just seconds a day in each team member's regular course of work, and is remarkably effective in helping keep your people safe from phishing scams while making them more savvy technology users.

For more information on this tool, or any other technology question or need, contact us at **385.312.9030**, or find us online at <https://sanityworx.com>. We look forward to serving you!

(Note: Mouse over the link we just gave you to practice your link-checking skills. *It's really us!*)