How to Diagnose A Phishing Email

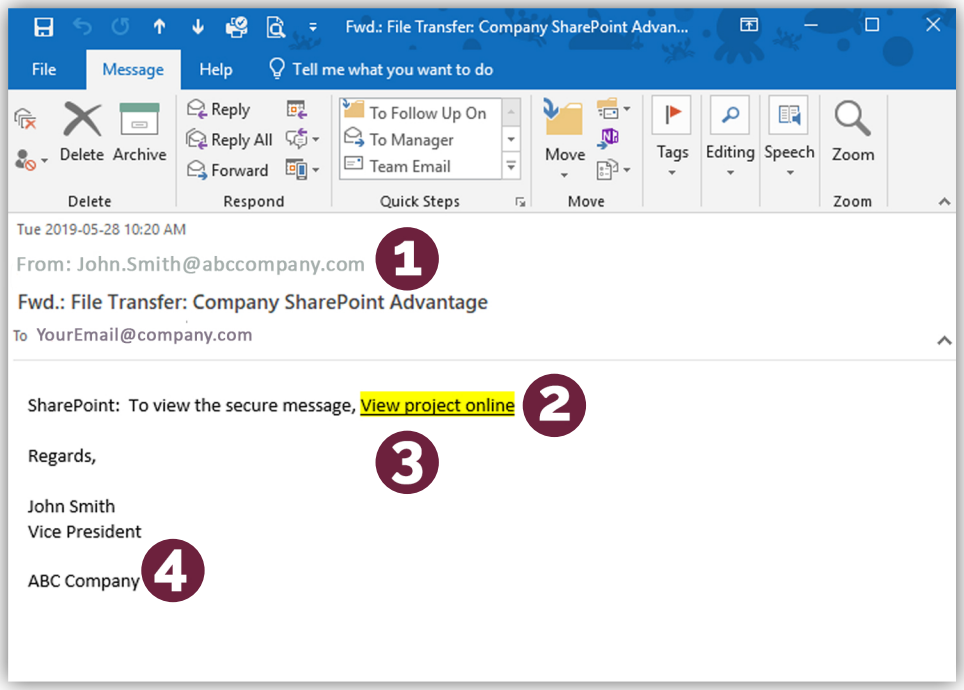
All of us have received suspicious emails in our inbox. Some of these messages can even fool our firewalls and anti-virus software. It is very important that we know how to decipher these messages as a second line of defense from these security attackers. Here is an example of a message that you might receive and some things to look out for!

1. Hover over the "from" email address.

You can see what initially appears as an email address can be altered. You need to hover over it to see the exact source. Ask yourself: is this email coming from a real sender?

2. Hover over the link: "View project link" to see what the true URL link location is.

Ask yourself is this is a trusted site? Would the sender send me this email to direct me to another site?



3. Be wary of outside links.

Be wary of links: "click here", "your message is waiting", "view project online", these links are usually sending us to the outside world. These links can be altered to read something other than the real link.

4. Does the request match the person?

Use common sense defensive questions: is this sender asking for money, passwords, or access, or viewing? Would a real sender ask me this kind of message? (for example, if a phishing email is tailored well to have the Manager's email address, would my Manager ask me to send him Bitcoins)?

How To Defend Against Phishing

1. Spam filtering is the first line of defense. It will determine if the majority of the messages coming in are legitimate or not. If the email is well crafted it can fool spam filtering.

2. If the email gets delivered to your inbox, then YOU are the second line of defense.

3. If you mistakenly click an email or get sent to a site with malware, firewalls, anti-virus programs and a good IT team is your final defense.

If you do click on a link, a good firewall should be able to block the virus. The content would be blocked from being opened to your local machine.

Web filtering should also be enabled on your network. For example, if the link tries to take you to a website that is located in a suspicous country it should automatically be blocked.

A good Unified Threat Management (UTM) strategy will determine if the source of the link is good or one that should be blocked.

It doesn't matter if you have a very secure system in place. It only takes one untrained staff member to be fooled by a phishing attack. Make sure that both you and your staff understand the telltale signs of a phishing attempt.

For Help With Phishing Protection, Contact Us!

ARC MANAGED SERVICES

Need Help Getting Your IT Systems In Order? We're Here To Help
Call 1.866.702.5022, Email: sales@arcbus.com
arcmanagedservices.com