SWTJC

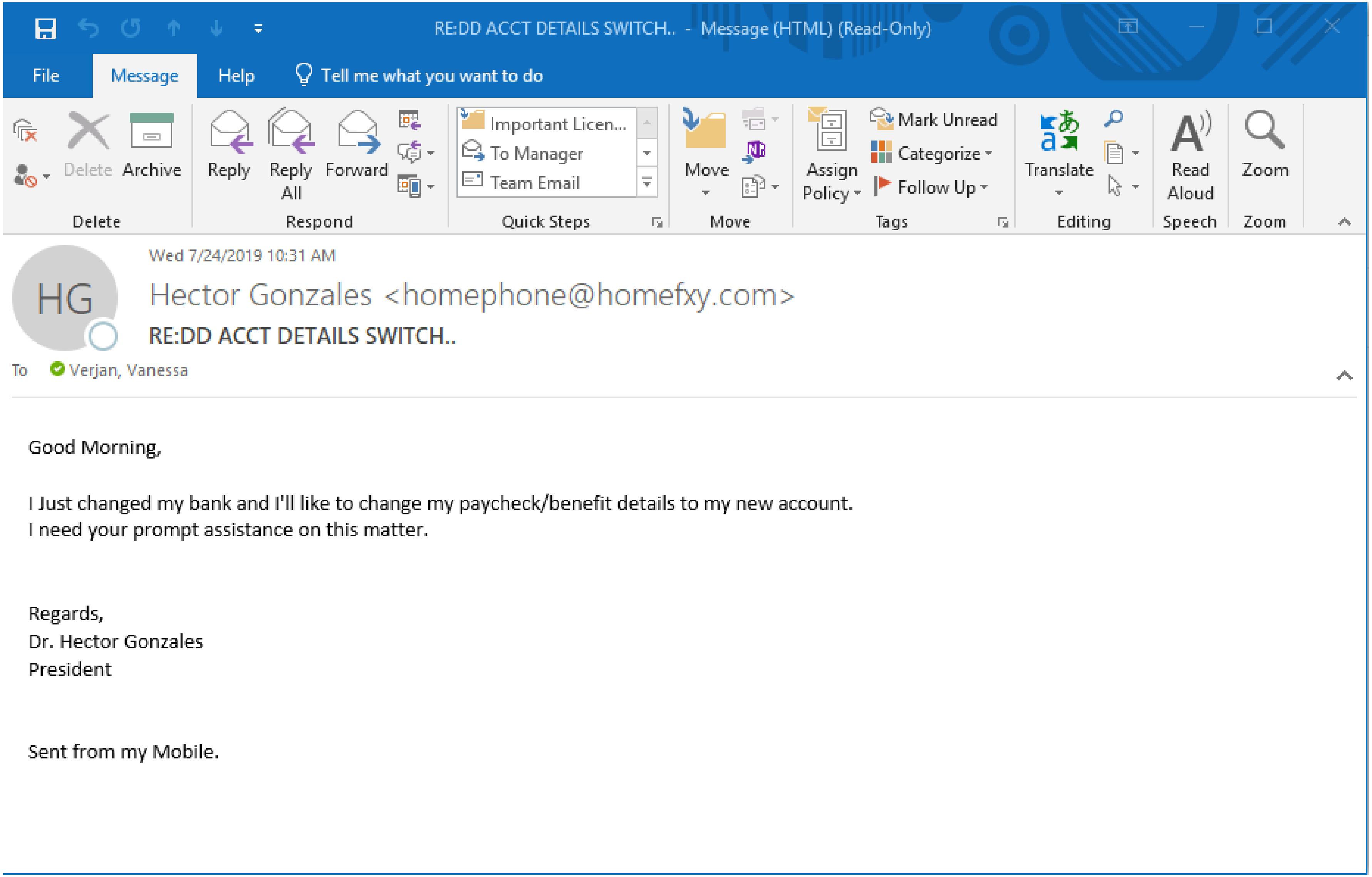
Southwest Texas Junior College

EMAIL SECURITY BEST PRACTICES

The Dos and Don’ts

ALWAYS… check the email “from” field to validate the sender

This “from” address can be easily spoofed. Spoofing is simply a means of disguising an email to make it look like it was sent from someone you know and trust. You can validate the sender by hovering your mouse over the “from” name field, which will then show you the actual email address of the sender. If the email address doesn’t match the person or company that believe sent the email, it’s likely a fraudulent email and should be marked as SPAM and deleted. Also, if the subject line or content in the body of an email makes you question why you received it, or why that particular individual sent it to you, then you should look more closely to confirm the sender before taking any action. It’s likely that person didn’t really send it to you.



Wed 7/24/2019 10:31 AM

Hector Gonzales <homephone@homefxy.com>

RE:DD ACCT DETAILS SWITCH..

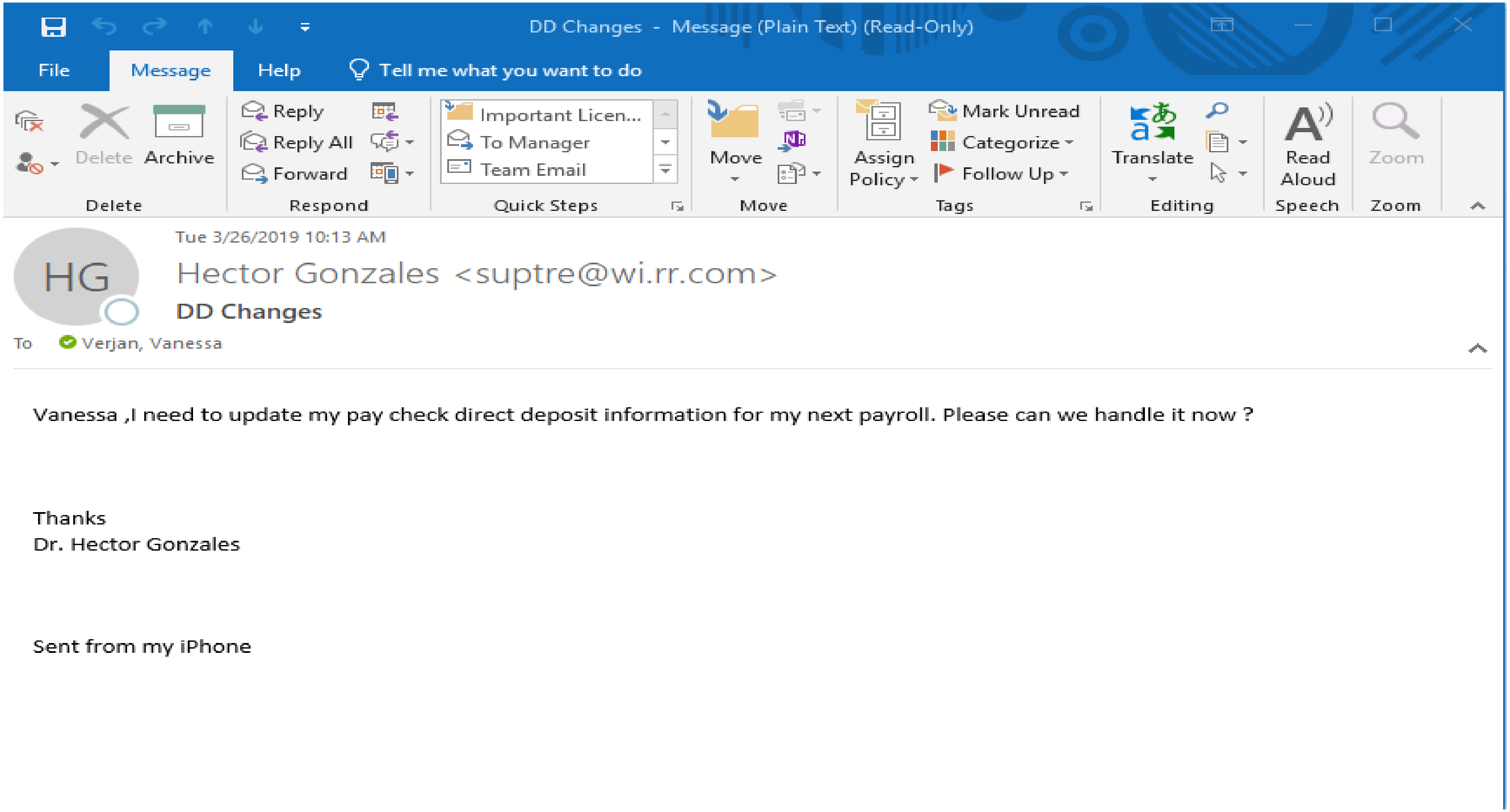
To Verjan, Vanessa

Good Morning,

I Just changed my bank and I'll like to change my paycheck/benefit details to my new account.
I need your prompt assistance on this matter.

Regards,
Dr. Hector Gonzales
President

Sent from my Mobile.



Tue 3/26/2019 10:13 AM

Hector Gonzales <suptre@wi.rr.com>

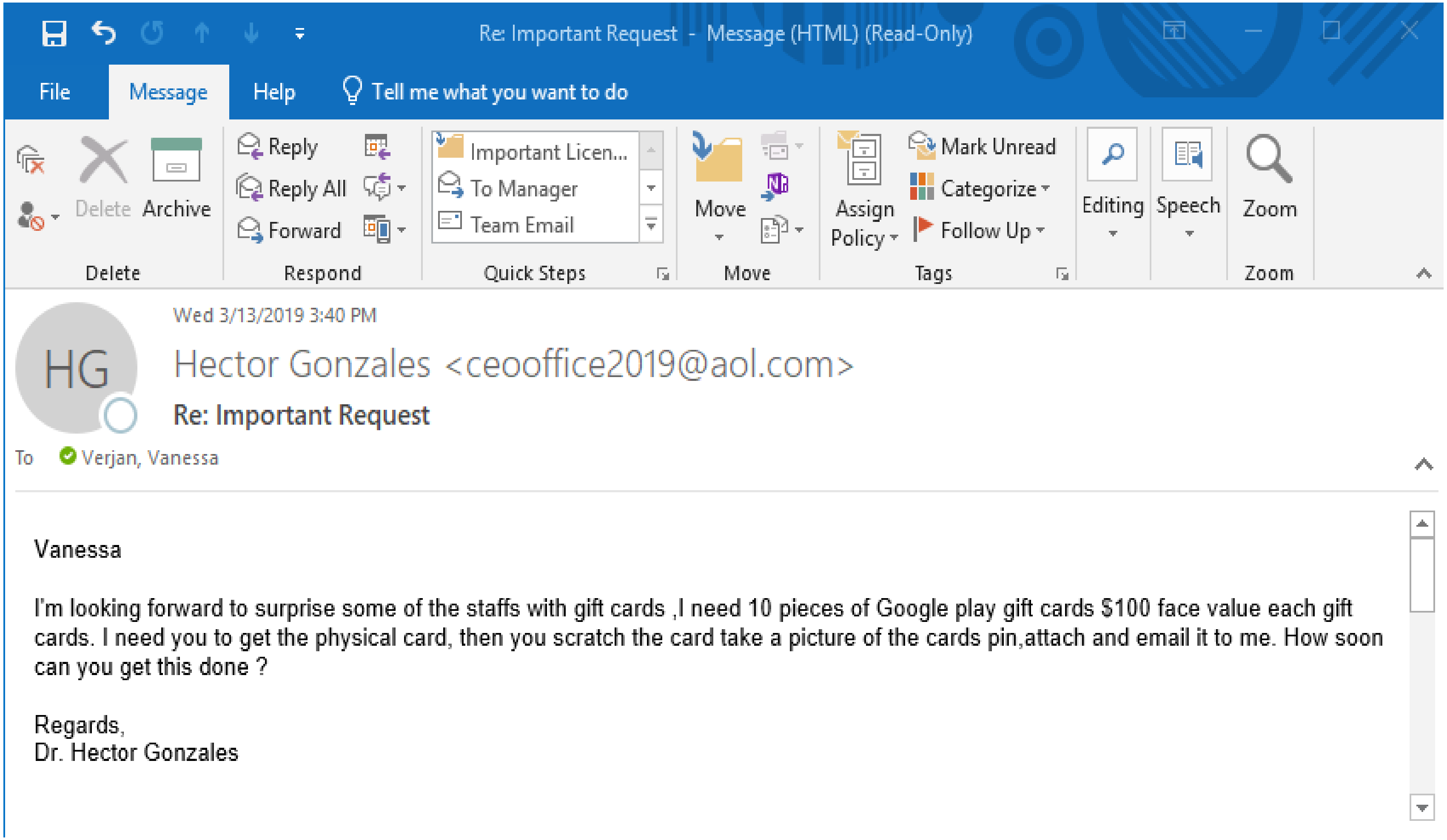
DD Changes

To Verjan, Vanessa

Vanessa ,I need to update my pay check direct deposit information for my next payroll. Please can we handle it now ?

Thanks
Dr. Hector Gonzales

Sent from my iPhone



Wed 3/13/2019 3:40 PM

Hector Gonzales <ceooffice2019@aol.com>

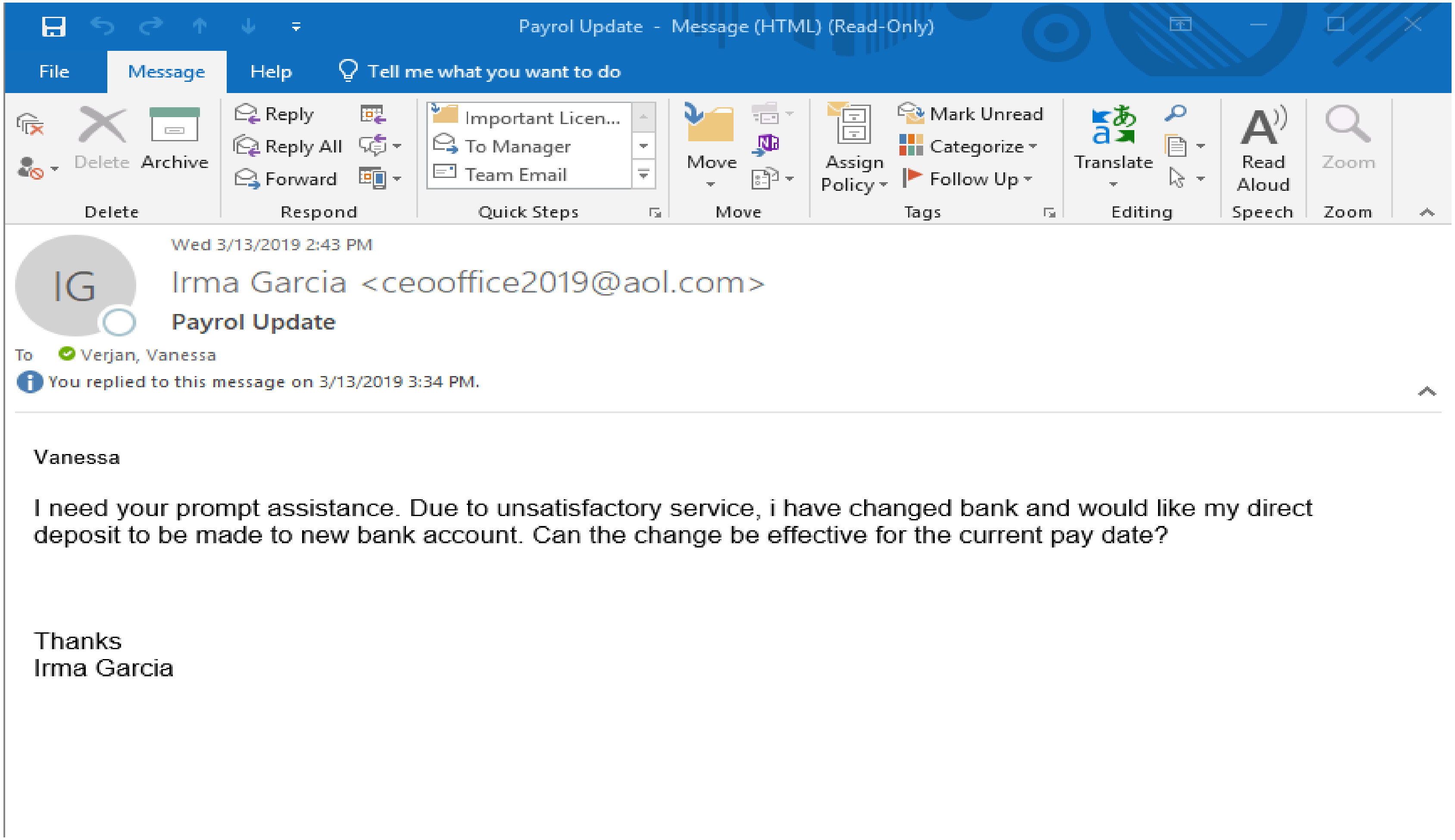
Re: Important Request

To Verjan, Vanessa

Vanessa

I'm looking forward to surprise some of the staffs with gift cards ,I need 10 pieces of Google play gift cards $100 face value each gift cards. I need you to get the physical card, then you scratch the card take a picture of the cards pin,attach and email it to me. How soon can you get this done ?

Regards,
Dr. Hector Gonzales



Wed 3/13/2019 2:43 PM

Irma Garcia <ceooffice2019@aol.com>

Payrol Update

To Verjan, Vanessa

You replied to this message on 3/13/2019 3:34 PM.

Vanessa

I need your prompt assistance. Due to unsatisfactory service, i have changed bank and would like my direct deposit to be made to new bank account. Can the change be effective for the current pay date?

Thanks
Irma Garcia

ALWAYS…check for files with a "double extension"

Although a text file named "safe.txt" is safe, a file called "safe.txt.exe" is not. The key is to closely look at the file name and extension to see it's being disguised as something safe. If you ever receive an email with an attachment that you were not expecting, you should look closely at the file name of the attachment before ever deciding to open it.

ALWAYS… look closely at website addresses (URL) that are included in an email

Note that ***microsoft.com*** and ***www.support.microsoft.software*** are two different domain names (and only the first is real). Fraudulent websites can have domain names that look legitimate, but are actually created to trick you into believing they are. By visiting the spammers website, you're giving them information about your geographic location (calculated based on your IP address), as well as your computer operating system and your browser. You also run the risk of the website infecting your computer with Malware. Bottom line, look closely at any URL and hyper link before clicking on them. If you suspect the website is fraudulent, you should contact your IT support team before just visiting the website.

ALWAYS… report suspicious emails to your Information Technology Help Desk

It’s very important for your IT department to be aware of suspicious activity so they can evaluate the email for potential threats, and also work to prevent malicious emails from entering the network in the future. It’s best to not simply forward the email, but to call your IT support team to make them aware of the situation so they can provide the proper guidance.

DO NOT… open any email attachments that end with .exe, .scr, .bat, .com, or other executable files that you do not recognize

You should also be very cautious about opening MS Word, MS Excel, and Adobe PDF files. There are several studies that show an increasing number of viruses and malware are being spread through these file types. Just about any email attachment can be malicious, so you need to be vigilant about opening email attachments. If you receive an email that you weren't expecting, even from a person you know, you should be highly critical of whether it is legitimate, and take additional precautions.

DO NOT… ever click embedded hyperlinks within email messages without first hovering your mouse over them to see where they will take you

By hovering over the hyperlink you will see the URL, which provides detailed information about network domain, website, or network location. If the URL doesn't look like it will take you to the appropriate business, website, or Internet location that you would expect, then do NOT click on the link.

Examples

www.swtjc.edu www.swtjc.edu

DO NOT… respond or reply to spam in any way

Instead, use should mark the email as “SPAM” or “junk” in your email client, or work with your IT department to make adjustments to your SPAM filter to capture email from this sender in the future.