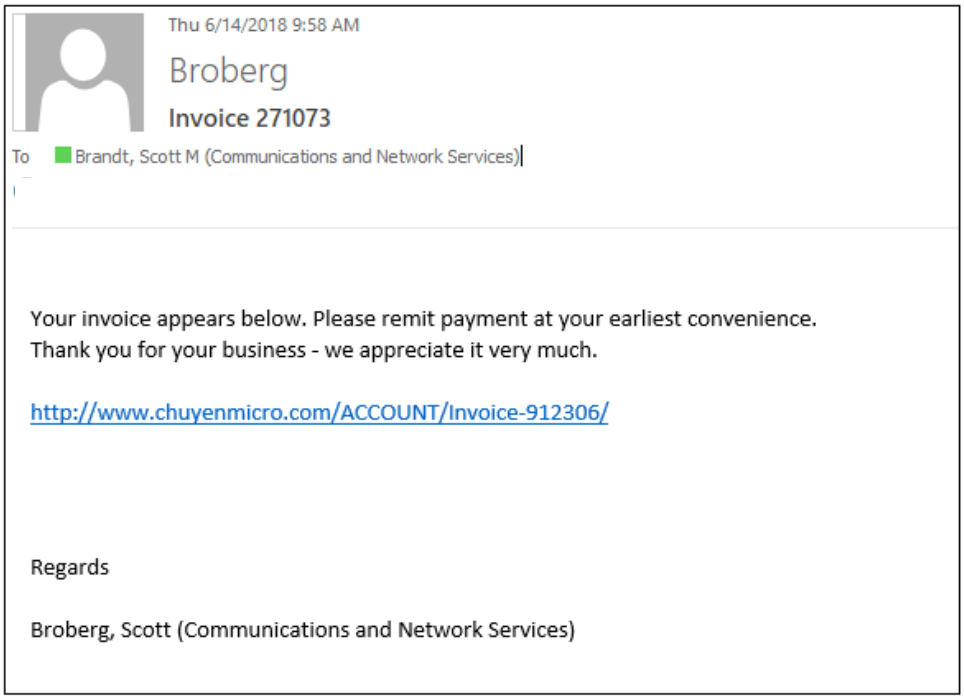
The cyber criminals have been sending out spoofing emails where they are pretending to be someone at MCC. Lately, this type of email has been extremely common at MCC.

The spam below is hard to spot because it looks like it has been sent from someone in the college. To determine this is spam look at the "From" field. Usually the from field has a 'Last, First' name format. As you can see in the following emails only the last name of the person is shown. When receiving an email stating there is an invoice DON'T CLICK ON THE LINK until you ask yourself:

1. "Why would this person be sending me an invoice?" If it seems strange call the employee sending the invoice.
2. Anyone who sends you an invoice should state what the invoice is for in the email and they should include their contact information. When that information is missing call the individual or company to confirm it is an actual invoice before clicking on the link or opening the attachment.



Thu 6/14/2018 9:58 AM

Broberg

Invoice 271073

To Brandt, Scott M (Communications and Network Services)

Your invoice appears below. Please remit payment at your earliest convenience.
Thank you for your business - we appreciate it very much.

http://www.chuyenmicro.com/ACCOUNT/Invoice-912306/

Regards

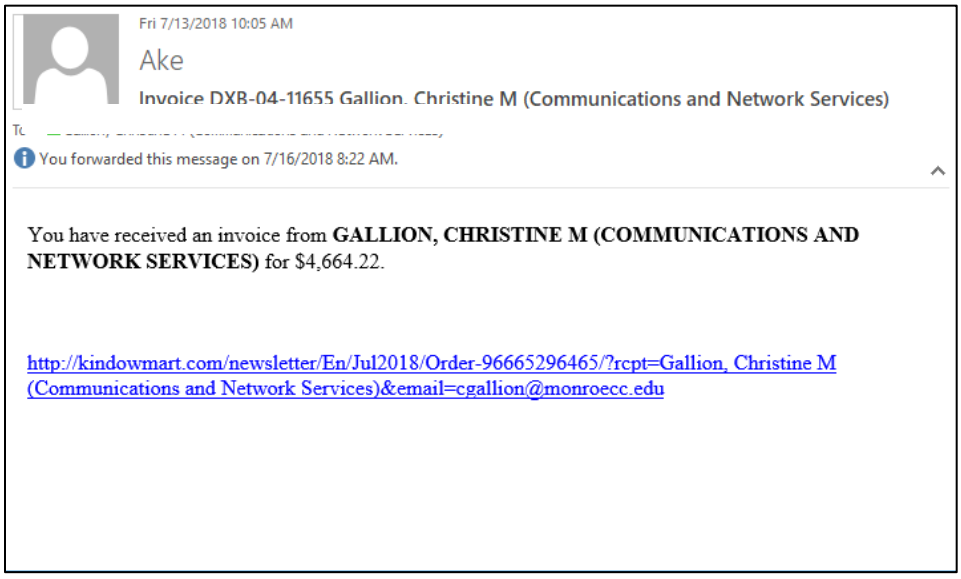
Broberg, Scott (Communications and Network Services)

Continued on next page…

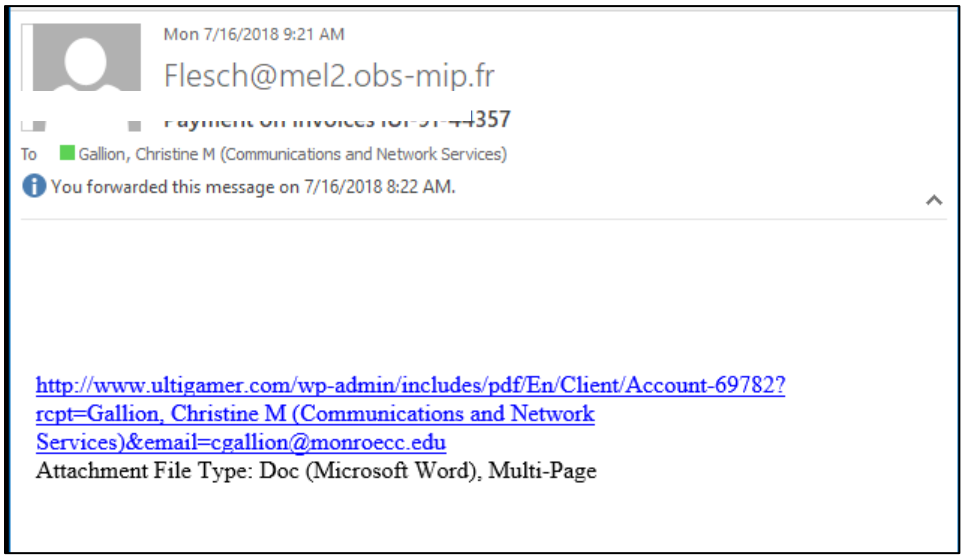
This email is similar to the last one. It has been made to look like it is coming from someone at the college. Again, there is no information in the signature other than a name. The “From” field only contains a last name. Why would someone from “Chemistry and Geosciences” be sending an invoice to Veteran Services? The difference with this one is that the virus is contained in the attachment. If you were to open it your computer would be infected.

Continued on next page…

This next piece of spam should be easy to spot.

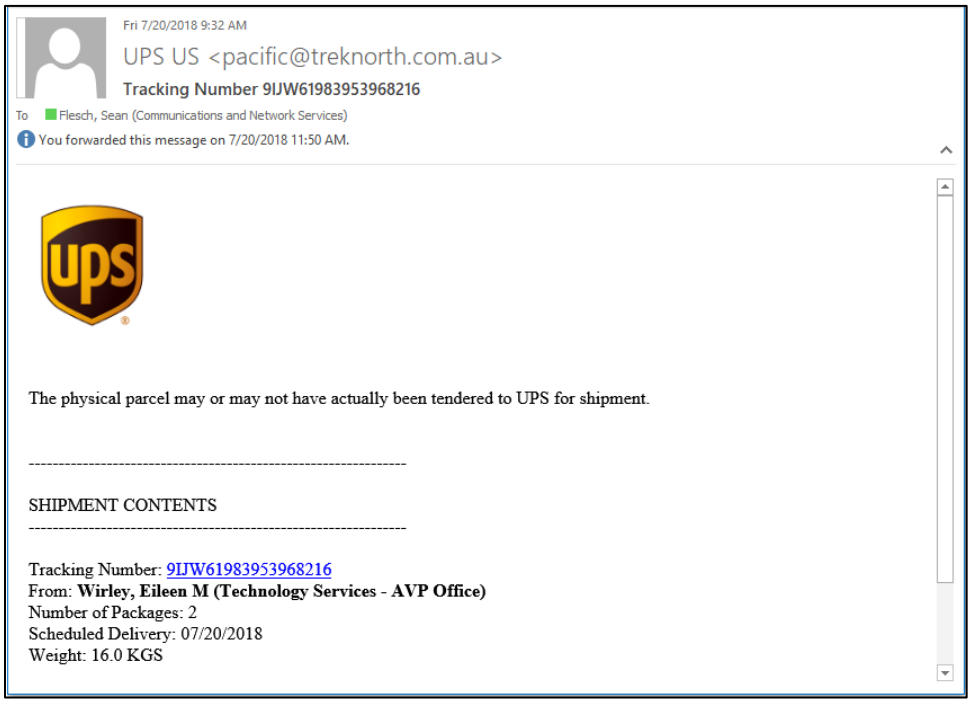


In the next email, the cyber criminals used an employee's name but did not use an @monroecc.edu email account. Internal invoices would not be coming from an "@mel2.obs-mip.fr" address.



Continued on next page…

MCC employees are still receiving other types of spoofed email like the one below claiming to be from UPS or other businesses. UPS would not be using the email “pacific@treknorth.com.au.” Additionally the employee who received this email does not deal with receiving or sending packages off campus. This gave them a red flag and they did not click on the tracking number link.



Spoofed email can be hard to spot. If you receive any type of spam, help our spam filters work better by forwarding the email to spamsubmission@monroecc.edu and then delete the email from your Outlook account. If you are not sure if it is spam DO NOT CLICK ON THE LINK OR OPEN THE ATTACHMENT, instead call technical support at x8324, option 3 and a technician can assist you in determining if the email is legitimate.