From: LCOM Office of the Dean
Sent: Friday, October 30, 2020 3:13 PM
Subject: On Behalf of Assistant Dean for Technology Services ~ Community Awareness of Phishing Emails

Dear LCOM Community,

UVM Health Network has experienced a cyberattack. This comes at a time when leading security experts are warning of a coordinated criminal cybersecurity campaign targeting hospitals and healthcare providers across the country, specifically through ransomware attacks.

These attacks start as clever, *highly tailored* phishing emails that typically request your network username and password or trick you into opening or downloading a file with a malicious virus. Once the malicious virus is downloaded, it can attack your computer or move through the systems your computer is attached to. Ransomware typically encrypts data and requires payment before you can access it again. Minimally, it requires significant downtime to recover.

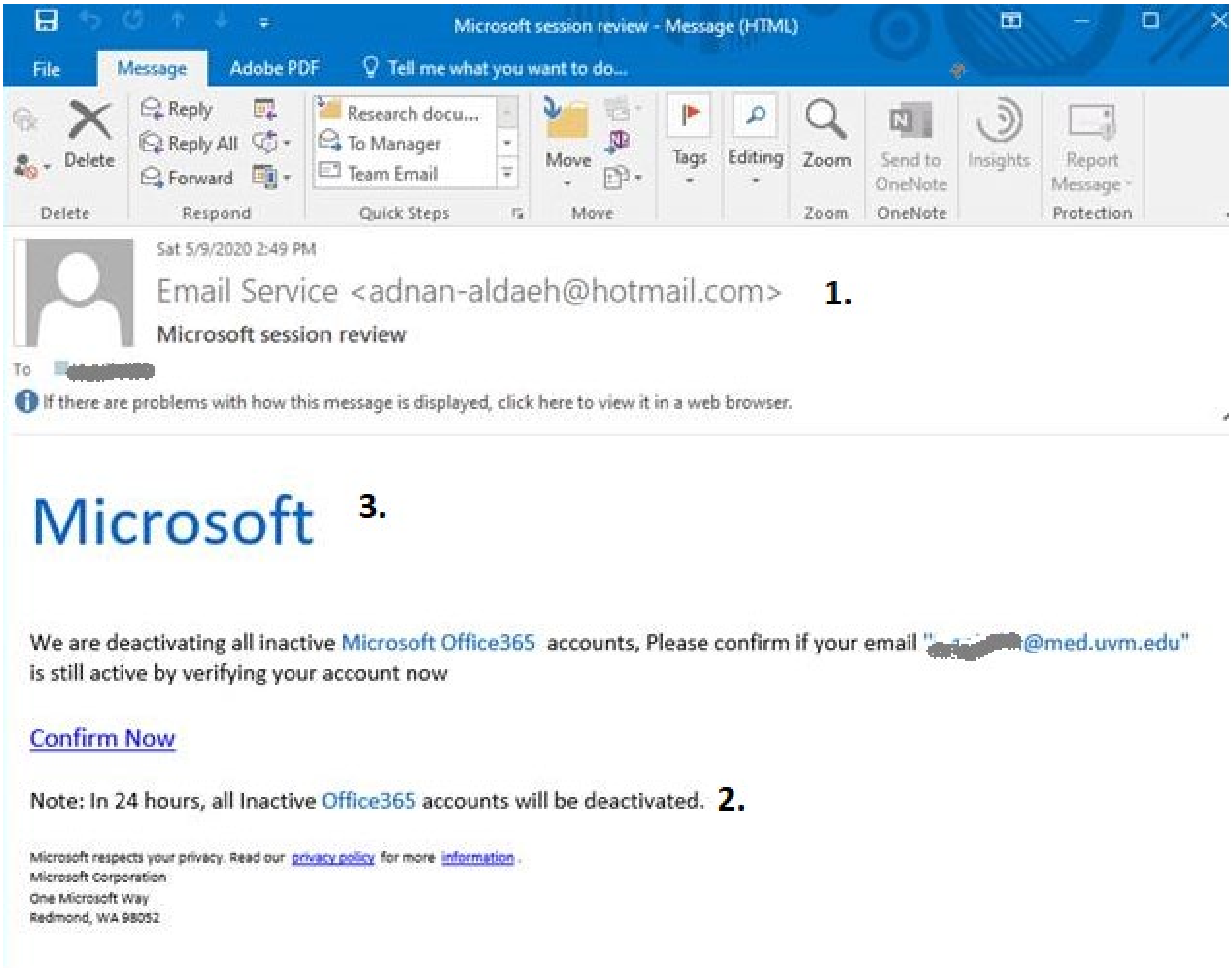
While we have safeguards that help block many of these types of emails before they get to you, we need your continued vigilance to fight off these attempts. Be sure to take the necessary extra time to carefully review your emails - even if they appear to be from someone within our organization. Verify messages that ask for a particular action like clicking links or opening attachments whether they come externally or internally. If you are unsure, ask – don’t respond to the email you have but rather ask in a separately addressed message using the Global Address List or UVM Directory (for internal messages) or from a known good address (for external messages) or call the person.

If you receive a suspicious email, forward the email as an attachment to abuse@uvm.edu and infosecurity@med.uvm.edu.

These precautions are imperative to ensure not only our institution, but our students, research and administrative data are safeguarded from these malicious attacks. Remember, you are our first line of defense against threats to our security. We will continue to keep you informed as we gain additional insight on these attacks.

Things to look for:

1. Do you recognize the email address (not just the display name) for this type of message? If not, proceed with caution.
2. Is there an emotional reaction designed to make you click on a link? Stop and take time to verify the authenticity of the message.
3. Are you expecting this message or this file from this sender? Evaluate all incoming emails and do not click on links or open attachments that you were not expecting.



Sat 5/9/2020 2:49 PM

Email Service <adnan-aldaeh@hotmail.com> **1.**

Microsoft session review

To [redacted]

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

Microsoft **3.**

We are deactivating all inactive Microsoft Office365 accounts, Please confirm if your email "[redacted]@med.uvm.edu" is still active by verifying your account now

Confirm Now

Note: In 24 hours, all Inactive Office365 accounts will be deactivated. **2.**

Microsoft respects your privacy. Read our privacy policy for more information .
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Thank you for the continued efforts and vigilance in helping to protect our organization.

Jill Jemison
Assistant Dean for Technology/CIO
Larner College of Medicine
University of Vermont
D104B Given
89 Beaumont Ave.
Burlington, VT 05405
(802) 656-0076
She/her

The Robert Larner, M.D.
College of Medicine
THE UNIVERSITY OF VERMONT

LCOM Remote Toolkit: https://med.uvm.edu/techservices/comis/remote_toolkit