From: LCOM Office of the Dean
Sent: Friday, November 6, 2020 1:49 PM
Subject: On Behalf of Assistant Dean for Technology/CIO Jemison ~ Addressing Malware Concerns

Dear LCOM Community,

We know you have questions and concerns in regards to what the cyberattack at the UVM Health Network means to us here at the Larner College of Medicine. We want to stress that caution rather than panic should be how everyone approaches this issue. LCOM has worked hard to minimize the risk of this incident but we know you all have questions especially if you are also receiving communication from the hospital like the one at the end of this message.

Please help us by approaching computer interactions with thoughtfulness and caution. For those spaces in the LCOM buildings that might have access to both hospital and university/LCOM jacks, please don't switch from one network to the other – this increases the risk that malware can cross over to our environment. Don't use additional methods – wifi, VPN, or other – to move between the institutions as this will also increase the risk. Don't use systems outside the clinical environment to perform clinical tasks.

Be patient. We don't know how long the hospital systems will be impacted. We want to assist in your academic, research and administrative tasks here at the LCOM. However, we want to be smart in how we react. If you can survive a few days or a week without access to a resource here, we ask that you consider holding off asking for changes while we devote time into building up our protections. Don't wait until the issue is urgent but, if a delay is acceptable, please consider it.

Be kind. We are all facing some additional and unexpected efforts in 2020. As a community we have had to pivot around working from home more, implementing pandemic back-to-work procedures, social distancing and hybrid classrooms and numerous other changes. We are here to help. Please be receptive to doing things differently.

Be flexible. As the days progress, you will receive additional communications for changes that we will be making in our environment to increase our security posture. Some will be easy, some will be challenging. Please know that we make these changes to help protect you, our community, our students, our research and our institution.

FAQs

What computers are affected?

- According to UVMMC information
  - Windows based computers/devices are at risk
  - Apple laptops are at lower risk – not enough information yet
  - iPads, iPhones, Androids are not at risk

What network connections can I use?

- If you have **not** connected to the hospital network in the last three weeks with an at-risk device
  - You may connect to UVM, LCOM or home wireless
  - Though it is considered safe to use the UVMMC guest wifi, it should be reserved only for urgent and immediate hospital business needs. When finished, disconnect promptly.
- If you **have** connected to the hospital network with an at-risk device in the last three weeks
  - UVMMC guest wireless use only
    - You are not considered at risk. Please note the directions above and follow those guidelines.

        - VPN connection to UVMMC
            - Your computer needs to be scanned for malware. Information below.
        - Plugged into a network connection with a cord or connected to an internal UVMMC wireless
            - Your computer needs to be scanned for malware. Information below.

Can I still use email?

- If you have **not** connected to the hospital network **and** you have **not** checked hospital email on your computer with an at-risk device
    - It is safe to check your UVM or LCOM email
- If you have connected to the hospital network with an at risk device
    - Use a different safe computer to change your LCOM and/or UVM passwords
    - Get your computer scanned for malware but feel free to use other safe computer(s) for LCOM or UVM email
- Please remember that clinical work should **not** shift to LCOM or UVM computers or accounts. While it is difficult at the hospital, the hospital still needs everyone to follow their rules for clinical care

Can I get help scanning my at risk computer for malware?

- For LCOM computer
    - In your system tray (the little icons next to the date/time display) you should see a shield. When you hover over it, a pop up label “Windows Security” should appear. You may have to hit an up arrow to see additional icons.
        - Click on the shield to open it
        - Click on “Virus & threat protection”
        - Look for “Virus & threat protection updates”
            - Please note down the date of last update
            - If it is earlier than today, please click “Check for updates”
            - Make sure it now has today’s date
        - Use the back arrow in the upper left to get to the previous screen
        - Under “Current Threats“
            - Please note down the date of last scan and the results
            - Click on the “Scan Options” link
            - Choose “Full Scan”
                - Full scans can take a significant amount of time so be prepared
                - Click “Scan Now”
        - When the scan is complete, note down any findings
            - If there were 0 threats found, you are done
            - If there was anything other than that, please contact the helpdesk at 488-5553
    - Call the help desk at 488-5553 if you need assistance with scanning
- For personal computer
    - The hospital is recommending you work with a local service provider for scanning and remediation.
    - If that is not possible, minimally take the following steps
        - If you already have a Anti-Virus/Anti-Malware product, be sure it is current and that you have up-to-date virus definitions then run a full scan of your computer (this can take some time so be prepared)
            - As a precaution you may also want to check with a second product like the free version of Malwarebytes as noted below
        - If you do not have an Anti-Virus/Anti-malware product

- considering purchasing one, the purchased products generally have a more robust feature set than free products.
- Windows has some built in tools for real time protection and detection. This, combined with another product, may offer you additional coverage.
- While not an endorsement, the free version of Malwarebytes is one we often help people use as it is fairly easy to install and run.
  - If you run into problems, please call our help desk at 488-5553

Excerpt from a UVMMC message:

IT has received questions about whether personal devices such as laptops, home computers, iPhones, iPads, and Android phones might be impacted by the malware attack. Here are key details provided by Doug Gentile, Network SVP for Information Technology:

- If you have a personal PC or laptop (one that was not issued by the UVM Medical Center), that device is at high risk of infection and should be scanned for viruses if:
  - You logged onto one of the UVMMC Wifi networks in the past 3 weeks or if you plugged directly into the network using an Ethernet cable. The guest Wifi network is separate, so if you only logged on using the guest network, you are not at risk.
  - If you logged in using a virtual private network (VPN).
- If you only logged in through the Citrix access gateway, which is the standard way of logging in from home, you do not need to get your computer or laptop scanned.
- This malware is spread using Windows services, so iPads, iPhones and Android phones are not at risk, even if you logged onto one of our Wifi networks.
- Apple laptops are at lower risk, but we do not have enough data at this point to confidently say they are not impacted. If you logged onto a UVMMC Wifi network with an Apple laptop, we recommend getting it scanned.

UVMMC cannot scan and reimage personal devices. If you have a laptop that needs to be scanned, we recommend taking it to your local computer service provider for a full scan. Your personal anti-virus software may not be robust enough to guarantee your device is not impacted.

Jill Jemison
Assistant Dean for Technology/CIO
Larner College of Medicine
University of Vermont
D104B Given
89 Beaumont Ave.
Burlington, VT 05405
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