

**From:** dopmannouncement <dopmannouncement@uabmc.edu>  
**Sent:** Thursday, August 29, 2019 1:12 PM  
**To:** DOPM All Users <DOPMAllUsers@uabmc.edu>  
**Subject:** Computer Tip of the Week -- That email will cost you \$2,500,000

## That email will cost you \$2,500,000

Brought to you by  
**Lisa Schwaiger**  
- DOPM HelpDesk Triage and  
Computer Tech in MT-403



### QUESTION:

I keep hearing stories about Ransomware but it's been about city and town governments. That could never affect us here at DOPM/UAB, right? Or could it?

### ANSWER:

Ransomware attacks often begin after employees click on links or download attachments containing malicious code from seemingly harmless emails.

While the top-notch IT folks at UAB do everything they can to prevent such things, there is no guarantee we might not be the next target.

So, please always be aware and appropriately suspicious before you download attachments or click on links in emails. This is especially true regarding emails you are not expecting, even if they are from someone you know.

(The bad guys are often able to impersonate other people.)

If interested, here are some news stories about it:

- <https://www.houstonchronicle.com/news/politics/texas/article/Hackers-seek-total-of-2-5-million-in-ransomware-14368812.php>
- <https://www.cnn.com/2019/08/20/politics/texas-ransomware-cyber-attack/index.html>
- <https://www.cbsnews.com/news/texas-ransomware-attack-more-than-20-texas-local-governments-are-facing-a-ransomware-attack/>

Was this helpful? Do you have suggestions for a future Tip of the Week? Do you have any other comments?  
Let us know at [dopmHelp@uabmc.edu](mailto:dopmHelp@uabmc.edu)

To see an archive of past Tips of the Week: <http://www.uab.edu/medicine/dopm/help/totw>