

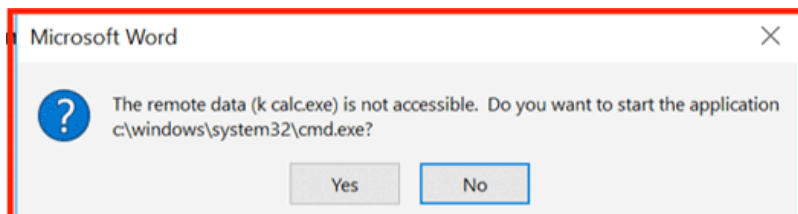
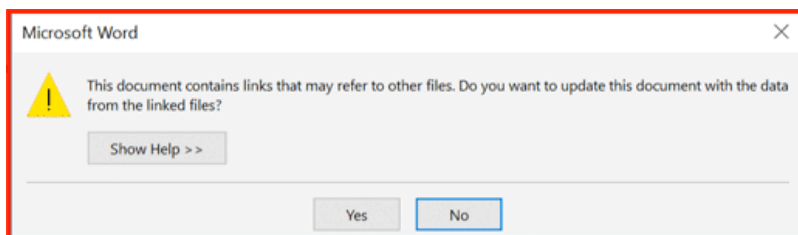
CYBERSECURITY COMMUNICATION

Please circulate

November 14, 2017

TO: University Systems Cybersecurity Communications
FROM: University Systems
RE: **Microsoft Office Document Attachments**

A security vulnerability was identified in Microsoft Office applications last week that affects documents with live data linkage to other documents. We have been made aware that other institutions are being affected by this vulnerability through phishing scams and malicious attachments. If you are prompted with notifications such as those below when opening Microsoft Office document attachments (Word, Excel, OneNote, etc.), do not accept them.



University Systems recommends that Macros be disabled and that the auto-update feature of linked data in Microsoft Office applications be set to manual. University Systems will apply this setting to clients supported by Desktop Support Services (DSS) today at 3:00pm.

If you have any questions or concerns related to this change, please contact your Desktop Support Services (DSS) support person or contact the Computer Help Desk.

Regards,
Chandra



Chandra Beaveridge
Cybersecurity Working Group

University Systems
[University of Victoria](http://www.uvic.ca)

To verify the authenticity of this message, visit:
www.uvic.ca/systems/verify