

A vulnerability has been discovered with the Zoom client for Windows PC's. This vulnerability allows people to send links in zoom chat that can appear harmless but potentially give the requester stored information that would allow them to potentially gain access to Shodair Network. We are asking all Zoom users to follow these steps to ensure we are doing all we can to remain secure.

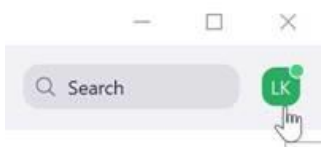
**Step 1.**

Do not engage in chats on zoom with anyone you do not KNOW. Do not click ANY links shared within the zoom chat service.

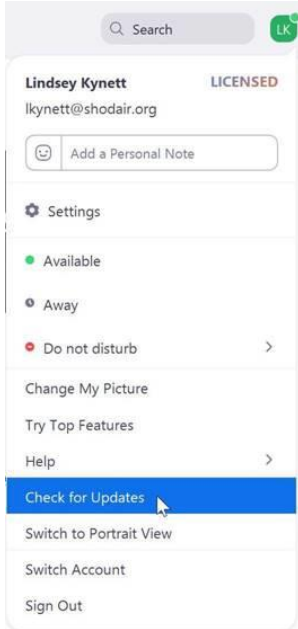
**Step 2.** To prevent 'zoom bombing' or potentially having people in your waiting rooms and meetings that were not invited, require a password for all zoom meetings going forward.

**Step 3.** Follow the instructions below to update the Zoom application on your Windows devices. (laptops, surface pro's, desktop computers, etc).

**Sign-In to the zoom application and locate your initials in the top right corner of the window and click that icon.**



**Then click the 'Check for updates' option. It will tell you if you are up-to-date or require an update. If there is an update available please install it.**



**If you require any assistance with this please contact Help Desk staff at Shodair immediately.**