In an effort to increase security awareness, please review the below about how to avoid Phishing, scams, and social engineering. **This is required reading**. There will be a small quiz to test your knowledge sent next week.

Key points relating to Spectrum Therapy employees:

* Unexpected emails or text messages are almost always phishing attempts. If you did not expect to hear from someone or some entity, then do not engage with these messages.
* Never click a link from an unknown text message. No organization is going to sent you a text asking you to click a link. If you get a text like the one below, these are always scams. Never engage them. (Example to be sent in another email) This example is not loading.
* If you ever get an email with a link to update information, confirm a password, or a seemingly urgent email saying money has been moved in your account, never engage those emails. Always navigate to the site yourself or use the company app to get directly to the legitimate organizations website or app and confirm for yourself.
* Never call a number presented on a webpage saying you need to call to get help. Many scam webpages will present fake errors and popups stating to call a number to get a hold of Microsoft support. These call centers are fake and the scammers will try to get control of your PC via Social Engineering methods.
* Watch this Training video: [https://youtu.be/XBkzBrXlle0](https://urldefense.proofpoint.com/v2/url?u=https-3A__youtu.be_XBkzBrXlle0&d=DwMFaQ&c=euGZstcaTDllvimEN8b7jXrwqOf-v5A_CdpgnVfiiMM&r=bvGiUlmPP_yGof1x-FJWrDbjdn8QuDP856Zhz3q7GZc&m=Ak7QHpxsLfct8ojbnYHhVaQD_d2Gh9Exzcrb-tiBYrSuu9LRQRS2v7ShM51G8KfH&s=_kI_A_3k9I-EEct5o3Z-Gh1Ed6kDT51UEMrUHARy_yc&e=)

Please let me know if you have any questions.