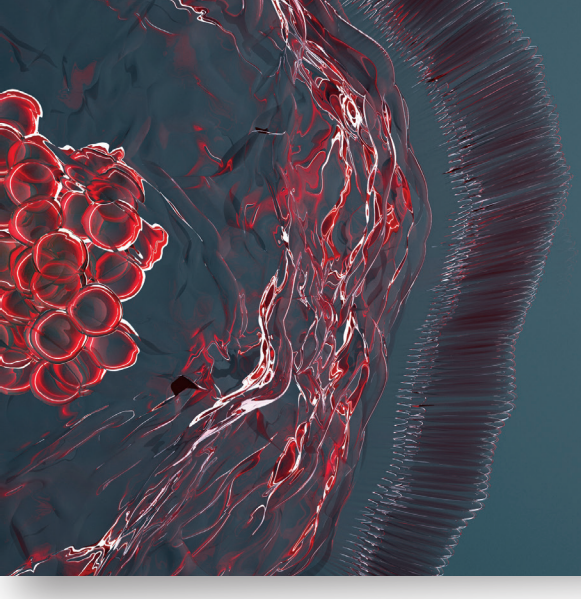

CONNER STRONG & BUCKELEW

IMPORTANT COVID-19 UPDATE

CYBER THREATS ARE HEIGHTENED DURING COVID-19

Time to remind your employees to be extra vigilant.

It has been observed and reported that COVID-19 is being used by cybercriminals as a theme for phishing attempts. Cybercriminals will often use the branding of "trusted" organizations in these phishing attacks, especially the World Health Organization and the Centers for Disease Control and Prevention in order to build credibility and get users to open attachments and click links. These attempts are only expected to increase.

It is important for you to remind your employees to continue to be vigilant with all your cyber security controls. At a minimum, reminded employees to:

- Be extra cautious when opening any attachments or clicking on any links within an email.
- Verify emails that are suspicious by calling the sender with a known phone number.

You should also remind your accounting department that may have modified protocols due to remote working that they should verify by phone any changes in money transfer instructions they receive during this time period.

Lastly, you should ensure your internal and external security personnel are being more attentive to monitoring activity on your network and taking immediate appropriate steps.

This is a time when cybercriminals will try to take advantage of the situation. Keeping with your security protocols even when your employees are working remotely will help to ensure that you do not fall victim to cybercriminals.

Questions

Please reach out to your Conner Strong & Buckelew account representative with any questions.