KAUFMAN | DOLOWICH

WATCH OUT FOR SMOOTH CRIMINALS: REMAIN VIGILANT WITH CYBERSECURITY DURING THE PANDEMIC

Stay vigilant. As many people in the world find ways to continue to work, cybercriminals likewise will continue to work. In fact, under current conditions, with people and businesses distracted and disrupted by the health and financial threats of COVID-19, bad actors will certainly take advantage of this perceived weakness.

On March 6, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released an alert reminding individuals to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19). Click here for the link to the CISA warning. CISA recommends that users should:

• Avoid clicking on links in unsolicited emails and be wary of email attachments.
• Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
• Do not reveal personal or financial information in an email, and do not respond to email solicitations for this information.
• Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information.
• Review CISA Insights on Risk Management for COVID-19 for more information.

Your cybersecurity is only as strong as its weakest link. As the private sector and government response to COVID-19 has evolved into an unprecedented number of people working remotely, it is important for companies to make the proper adjustments in their approach to cyber-security. We encourage all companies to:

• Maintain and enforce your already established robust cybersecurity protocols.
• Remind employees that privacy laws such as HIPAA, CCPA, and GDPR still apply while working from home.
• Remind employees of the need to be careful and of the possibility of increased threats during the pandemic.
• Find out the security of the servers and workspaces used by employees remotely and inform employees of steps they should be taking to protect their system and the company's private information.
• Assist employees in strengthening such security.
• Develop a protocol to discover and respond to data privacy breaches that may occur remotely.
• Remind employees that company owned devices should be used for work and not shared with other household members.

Although our normal routine has been disrupted, now is not the time to relax on cybersecurity. In fact, now is the time for extra vigilance.

Please contact Eric Stern (estern@kaufmandolowich.com) or Avery Dial (adial@kaufmandolowich.com) if you have any questions regarding Cybersecurity or Data Privacy.