Does COVID-19 raise any particular cybersecurity risks about which we should be vigilant?

Updated as of March 6, 2020:

Be alert for increased phishing attempts. Threat actors are notorious for using crisis moments to their advantage. They may try, for example, to send a spoofed email that looks like an emergency alert from a trusted executive asking employees to log in with network credentials to receive the latest information or otherwise turn over private information. These fake emails can be sophisticated and on a good day can dupe unsuspecting employees. During a crisis, it's even easier for employees fall victim to a scam while caught up in stress, fear or panic. Alert employees to these increased risks and consider friendly reminder campaigns about security and being on the lookout for phishing attempts.

Remote working arrangements can introduce new vulnerabilities – take steps to plan, prepare and defend against them. With the potential for high volumes of employees working remotely, network systems and support may be strained. Information security teams should consider how to identify potential increased risks of these arrangements, prepare to defend against those risks, and evaluate whether and how the incident response team can deploy communications and a rapid response should the need arise.