Cybersecurity awareness has always been a critical factor in mitigating risk to your business; however, now more than ever, as the world reacts to the ever-changing effects of COVID-19, it's so important to ensure your corporate IT environment is secure **AND** your employees are educated in avoiding clicking on harmful emails. IntraSystems is here to assist you with ensuring your organization has the proper tools in place to ensure a productive and secure workforce.

Cyber criminals are more active than ever due to COVID-19 and unfortunately, cyber-attacks have increased dramatically during this crisis. Criminals have used COVID-19 emails as a driving force in their various phishing campaigns.

Below are some **key strategies** to utilize in avoiding cyber-attacks:

- Be extremely observant for any request asking you to click on a link, open an attachment, or reply with sensitive information. Be sure to closely look at the address of the individual sending you this information and always ask yourself if you were expecting this email from this person at this time. Many times, their email address contains an extra letter so that at a quick glance, it appears to be accurate, but isn't.
- If you are working on a home computer or loaner and not your usual company-assigned system, be sure that your antivirus, firewall and other security solutions are enabled and up-to-date.
- In addition to phishing attacks (email), cyber criminals are also using vishing (phone calls) and smishing (text messages) attacks to mislead you into revealing sensitive information, such as your passwords, etc. Additionally, there have been multiple reported cases of malicious COVID-19-related Android applications that give attackers access to smartphone data or encrypt devices for ransom. Never provide this information without speaking directly to your IT team first.
- Connect to company resources using a secure network connection and avoid free or unsecured Wi-Fi.
- Avoid using computers with out-of-date operating systems, such as Windows 7, as they no longer receive security patches - making them more vulnerable to attack.
- Be sure to have the contact information for the individual in charge of your company's security in the event you experience an attack or need to report an incident.