# BlueOrange Alert:

## Work from Home User Concerns

There has been a rise in cybercrime threats taking advantage of the current COVID-19 pandemic. Malicious actors have been exploiting consumer-grade network equipment such as small office/home office routers, publishing malware-infused mobile applications to the Android App Store and deploying phishing campaigns used to steal credentials or install malware on Windows-based systems. With an increased number of users working remotely, an organization should:

- If an organization's users are permitted to utilize personal phones, computers, or other devices for remote access to the organization's systems and data, configure remote access solutions to require and check for security protections such as installed anti-malware software, secure connection protocols, and restrict the saving of screenshots or application output to the local device storage
- If possible, obtain remote users' external IP addresses to ensure that remote connections are only originating from known locations
- Proactively monitor the account activity of any users authorized to work from home to ensure that it aligns with their assigned roles and the organization's expectations

**About BlueOrange Compliance:**

*BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits. BlueOrange Compliance provides this alert for educational purposes only without warranty and specialized advice should be sought about your specific circumstances.*