BlueOrange Alert:

Phishing

There has been a rise in cybercrime threats taking advantage of the current COVID-19 pandemic. Malicious actors have used healthcare-themed masking techniques for delivery of phishing and malware campaigns, including impersonation of public health officials and spoofed health advisory notifications to increase likelihood of victim engagement.

An organization should:

- Continue (or implement) regular training to help users identify phishing attempts, simulation of spoofed communications that they may receive from malicious actors during the pandemic
- Implement of tools that block suspected phishing emails or that allow users to report and quarantine them
- Make users aware of social engineering tactics aimed at revealing sensitive information not only via email but also by phone calls ("Vishing") or social media ("Smishing")
- Monitor, identify and suspend the access of users exhibiting unusual activity

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.