Increased Awareness of Cyber Security During COVID-19

Cyber criminals will no doubt be taking advantage of the heightened opportunity and attempt accessing computer systems and stealing identities by enticing you to click on links within fraudulent emails, social media posts and news updates. With more and more organizations generating email updates regarding measures they are taking to protect clients and avoid service disruption, the likelihood of you receiving a fraudulent email just increased. Be cautious. Grammatical errors and misspellings in subject lines are common red flags. Use extreme care when opening emails or articles and clicking on links.

Here's a few tips:

- Avoid clicking on links in unsolicited emails and be wary of email attachments. See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.
- Use trusted sources—such as legitimate, government websites like the Center of Disease Control and World Health Organization to obtain fact-based information about COVID-19.
- Never reveal personal or financial information in 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.