Please Be Alert: Phishing Scam Emails

Phishing scams can be spotted easily by hovering over the "From" email address or web link. If they do not match a known legitimate address, it's likely a fraud and should be deleted. Other computer and email safety tips include:

- Treat all embedded links as suspicious.
- Avoid clicking on links from any of the above mentioned institutions and simply go directly to their website by entering the URL manually.
- When in doubt, either delete suspicious emails, or forward to your Cox Help Desk for further analysis.
- Avoid use of public WiFi Networks as hackers can easily intercept your data and gain access to your computer. Use your cell phone's data plan, by turning off the WiFi for immediate need of financial transactions.
- Opt not to save passwords in your browser, especially for critical sites like financial institutions.
- Keep your antivirus software up to date.

What You Should Do If You Receive a Phishing Email:

- If you receive or have received one of these emails, **DO NOT CLICK ON THE LINK** or reply in any manner.
- Please forward any suspicious phishing emails to your Cox Help Desk. CEI Corporate Security is currently working in conjunction with the United States Secret Service to identify the source of these fake emails. Your Cox Help Desks are taking appropriate actions to block the sending email account and prevent potential victims from accessing the fake Vanguard website address.
- Please note, Vanguard and our other business partners do not send out unsolicited emails asking for personal information.

If you have questions, please feel free to contact Cox Enterprises Corporate Security at (888) 351-5567 or by email at CEI.Investigations@coxinc.com. Visit CoxAlert.com for more information on phishing scams.

COX ENTERPRISES CORPORATE SECURITY SERVICES