Brinker Capital

MARCH 2020

Protecting against COVID-19 scams

Jim O'Hara, *Information Security Officer,* Brinker Capital

If your work and personal inboxes look anything like mine, everything ranging from the power company to credit card companies to convenient stores have shared information about their response to COVID-19. Fraudsters are also sending emails and making phone calls, hoping to catch individuals off guard during these unusual times. Before you click the link to skip your next mortgage payment or defer the interest on your student loans, consider these tips to keep your personal investment information safe:

- Be wary of unexpected or unusual messages containing links or attachments. Instead of clicking on the links, which can sometimes open the door to cybercriminals, consider typing web addresses and URLs into your browser.
- If you are unsure of an email or electronic communication from a financial institution, call them directly to verify your information verbally.
- Be suspicious of callers claiming to be a bank or credit card company wishing to "verify unusual account activity." In all cases, decline to participate. Instead call the organization's main number and ask to be directed to the fraud department.
- Always access your financial accounts from your home computer or laptop. Avoid using public or shared computers as your information may be stored and accessed by someone else later.
- Apply system updates to your home computer and devices as soon as they become available to improve security and system patches.

If you think you fell victim to a phishing or hacking attempt, take the following immediate action steps:

- Change your email account password(s)
- Change all other online passwords
- Notify all relevant bank or investment institutions to monitor for unusual activity
- Access credit monitoring services to help keep your identity safe

Cyber threats have evolved, and so have we. At Brinker Capital, we are committed to continually improving our technology and security policies in an effort to stay ahead of current cyber threats within the industry. Stay safe (and secure) during these uncertain times.