Cardinal Wealth Management LLC
626 North 4th Street, Suite 101
Steubenville, Ohio 43952

The Key to Unlocking Your Financial Future

Gregory R. Metcalf, RFP®,RFC®,CWS,®AIF®
Owner, Registered Securities Principal,
Financial Life Planner

Richard J. Desman, CFP®,CLU®,ChFC®|
Retired Partner

Sue E Pevac
Financial Advisor

Phone: 740-314-8342
Fax: 740-275-4276
www.cardinalwealthmanagement.com

As of April 15, the Federal Trade Commission (FTC) had received over 18,000 consumer complaints related to the COVID-19 outbreak, with victims reporting losses of more than $13.4 million. I would like to call out a few types of these scams to help you avoid becoming one of their victims. You can find the latest news and updates on the websites for the Federal Bureau of Investigations www.fbi.gov or the FTC www.ftc.gov.

In-demand Products and Bogus Cures
No vaccines or drugs have been approved specifically to treat or prevent COVID-19, but that hasn't stopped fraudsters from flooding consumers with pitches for phony remedies. Other scammers claim to be selling/offering in-demand supplies such as surgical masks, test kits and household cleaners, often in robocalls, texts or social media ads. The Federal Communications Commission (FCC) set up a dedicated website with information on COVID-19 phone scams.

Financial Phonies
With many Americans set to receive stimulus checks under the federal Coronavirus Aid, Relief, and Economic Security (CARES) Act, the IRS warns of schemes promising to speed up your payment. Watch out for calls or emails, purportedly from government agencies, that use the term "stimulus" (the official term is "economic-impact payment") and ask you to sign over a check or provide personal information like your Social Security number.

Crooks impersonating banks and lenders are calling with offers of bogus help with bills, credit card debt or student loan forgiveness and fraudsters are also calling with stock scams.

Phishing Scams
Coronavirus websites, those with “coronavirus” or “COVID” in the domain name, are 50% more likely to be malicious than other domains. When you contact those malicious domains, you could start getting emails from fraudsters in an attempt either to plant malware on your computer or to get your personal information. When you click on an email (it often looks legitimate) or download a file, you could be importing a program that spreads more malware or digs into your personal files looking for passwords and other information for purposes of identity theft.

Be careful when you browse for information about coronavirus. Get your information first from a legitimate source, such as the U.S. Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO). And make sure you are going to the genuine CDC and WHO websites: scammers are impersonating them, too.

Money Mules
Money mule scammers specialize in hacking employer accounts at job recruitment web sites. If you receive a job solicitation via email that sounds too good to be true, it could be related in some way to one of these money-laundering schemes. Money mules — however unwitting — may find themselves in hot water with police and may be asked by their bank to pay back funds that were illegally transferred into the mules’ account.

As always, if you have any concerns or questions, please reach out to us.