Market Risks May Be Moderating & Ways To Avoid Cyber Scams

August 3, 2022

Join Our Mailing List!

After a terrible start to 2022, markets rebounded in July. U.S. and developed international markets were up by 5 percent or more, with only emerging markets trailing. The primary driver here was the Fed. It has raised interest rates close to a neutral level, and markets are anticipating the worst of the tightening cycle has passed. But with the U.S. economy contracting for the second quarter in a row, can the rebound continue? Tune-in to the latest Market Thoughts to find out.

Commonwealth

What are Social Engineering Cyber Scams—and How Can You Avoid Them?

You receive an email from a website you regularly use asking you to click a link to change your password due to suspicious activity. You take a phone call from the IRS asking you to verify your bank account or social security number. You get a text saying a family member was in an accident and they need money for emergency room bills.

These requests appeal to your sense of trust and seem like legitimate things to ask of you, so there's a good chance you'll respond or comply. But beware; these are common social engineering scams, which are ploys to access your sensitive information or obtain money using psychological manipulation.

Educate Yourself
The best way to avoid being a victim of this type of attack is to recognize the signs and know how to protect yourself. Here are the most common social engineering scams:

Phishing, smishing, vishing. These words may sound like nonsense, but they're all widely used ways to trick you into giving away your personal information. Phishing occurs when a scammer sends you an email with a seemingly legitimate link to click, such as an email requesting a password change. Once you click and enter your password, bank account number, or other sensitive information, scammers receive

access—and you might not even realize it. Smishing is a similar scam via text, and vishing is via phone or voicemail.

- **Protect yourself**. Don't click links from someone you don't know, or even from an organization that might look legitimate. Go to the actual website and reach out using their posted contact information. Similarly, if someone calls you out of the blue and requests information, tell them you'll call their organization back using a verified number. If you call the IRS, for example, they'll likely tell you it wasn't actually their representative calling to solicit information from you. If you receive a text and don't recognize the sender's phone number, don't respond, even if the text indicates it's from someone you know.

Baiting or quid pro quo. As the term suggests, this method offers some form of bait to tempt you into divulging information or handing over money. It could be physical bait, such as a flash drive that seems legitimate, or digital bait, such as an enticing advertisement to click or a music download. In reality, these drives or links infect your computer with malware or direct you to unsecure websites.

Quid pro quo uses a similar tactic whereby the scammer offers a service or monetary incentive in exchange for your information.

- **Protect yourself**. Simply stated, don't take the bait. Remain suspicious of any link or ad sent to you. If you're interested in finding out more, you can always Google the company or product and find their official contact information. Don't insert flash drives into your computer if you don't know for certain what is on them or who has had access to them before you. Be wary of anyone requesting personal information, passwords, or login credentials from you, even if they claim to be an IT specialist or government official. Verify a person's identity before responding to a request.

Piggybacking or tailgating. To carry out this type of attack, the perpetrator will try to gain physical access to a restricted space or device by following an authorized person. Think about a delivery driver asking you to hold a door open so they can deliver a package to someone in the building or an innocent-seeming stranger at a coffee shop asking to borrow your phone or laptop to look up information. Once given access, the scammer can steal your private information in a short amount of time.

- **Protect yourself**. Get in the habit of politely declining requests like these. You might want to be helpful and accommodating, but those are the precise traits attackers seek to exploit. You can always offer to look up directions or a phone number yourself, rather than allowing someone access to your device. And you can tell the delivery driver to phone the

package recipient to gain entry to the office. Don't be the person who falls for the trick just because you were trying to be kind to strangers.

Scareware. Social engineering scams aim to make you act quickly based on emotion, and this form of attack does exactly that. You're working on your laptop and suddenly see a pop-up warning you that your computer has multiple viruses. It instructs you to download software immediately to protect your personal information and files. This is how they put the scare in scareware. It's natural to click as quickly as possible to prevent the issue from worsening; however, by doing so, you've exposed your computer to the malware you were trying to avoid.

- **Protect yourself**. First, be sure to install legitimate antivirus/antimalware software on your device and ensure that it's always up to date to block pop-ups from coming through in the first place. If one does appear, allow yourself time to assess the situation and think things through before acting.

Scammers are hoping you'll panic and react quickly, but if you pause for a moment you'll probably be able to spot an attack. Look for misspellings, lots of exclamation points, altered logos, or unprofessional words that a software company likely wouldn't use. If you see one of these pop-ups, don't click it—don't even click the "X" button to close it. Instead, close your browser window and force quit through the task manager (Ctrl + Alt + Delete on Windows).

Recognize the Tactics
Overall, the best way to stay safe from social engineering scams is to recognize these tactics, verify information and sources before acting, and avoid clicking or acting quickly based on emotion. Remain calm, evaluate the originator of any request for money or information, and don't comply until you're sure the request is legitimate.

My staff and I deeply appreciate the continuing opportunity to work with you. Please let me know if you have any questions or requests. Thank you.

Sincerely,

Paul Bonapart, JD, RFC, AIF®
Accredited Investment Fiduciary, President
Financial Security Planning Services, Inc.
520 Tamalpais Drive, Suites 103 & 104
Corte Madera, CA 94925
(415) 927-2555
www.FinancialSecurityPlanning.com
CA Insurance License No. 0808412

- Registered Representative with/and offers securities through Commonwealth Financial Network, member FINRA/SIPC, a Registered Investment Advisor.
- Advisory services offered through Financial Security Planning Services, Inc., a Registered Investment Advisor, are separate and unrelated to Commonwealth Financial Network.
- Fixed insurance products and services offered through CES Insurance Agency.
- Indices are unmanaged and cannot be invested into directly. Past performance is not indicative of future results.

Delivering financial confidence since 1992