Red, Blue, & YOU!

Here we are again, and another election is upon us. There have always been tumultuous events surrounding elections. There are wars, inflation, civil unrest/protests, labor market struggles (too many or insufficient workers), weather-related calamities, pandemics, and market declines/recessions. In times like this, we need to examine your long-term and time in the market. Fear is always there, and we can always think of a reason not to invest. Time is the best friend if you are a die-hard politician from either party. Time heals all wounds. Statistically, both parties have bragging rights because they have the long term as the sampling size. However, statistics are not as kind if a party controls the executive and legislative branches. The market tends to like a split Congress and executive branch. This way, one party can't make too many changes when in power. Historically, a President can only make so many changes, and those can only amount to about 20% of what was forecasted or requested when the party is running for office. Is it different this time?

Instead of the elections, I'm focusing on Cybersecurity Awareness Month this October 2024. This is the 21st year. There has been an increasing collaboration between the public and private sectors to fight this battle. The goal is to increase awareness and reduce your online risks. We all need to be concerned about and vigilant about this. These online scams can sometimes lead to Identity Theft. Here are four inexpensive ways that may help.

1. Use strong passwords. This means changing them frequently, making them long, and using symbols.
2. MFA—This is Multi-Factor Authentication. It means that when you log in to your site, a code will be sent to your phone, either by text or email, to confirm that you are the user.
3. Phishing—Be aware of messages asking you to confirm and order. You may think it is from one of your frequented websites. When in doubt, please do not click on it and delete it.
4. Regularly check that your software is updated. This can also be tricky as some software may not be on your computer, but someone may want you to install it. When in doubt, don't download!

If you have been a victim of cybercrime, there are several steps that should be taken. The first is to place a fraud alert at all three credit bureaus. The three credit bureaus are: Equifax, Experian, and TransUnion. One idea is to log on to each so that when/not if you have to protect yourself, that you can log in as you have already established an account. If a specific account has been compromised, make sure that account gets closed. Depending on the severity of the breach, it may be also prudent to file a report with the Federal Trade Commission (FTC). The link is reportfraus.ftc.gov. In some situations, it also may be necessary to file a report with your local Police Department.

As always, please be vigilant for your own accounts as well as the elderly relative that may need your assistance. As people age, the logistics of these scams gets more and more involved. Please be an advocate for those in need.

Sincerely,

Andrew Wade
President