

# What can I learn from looking back on my financial situation in 2017?



If your financial plan for 2017 didn't work out the way you wanted it to, don't beat yourself up. Instead, ask yourself the following questions to determine what you can learn from reflecting on your financial situation in the last year.

**Did you meet your financial goals and expectations for 2017?** Perhaps you started the year with some financial goals in mind. You wanted to establish a budget that you could stick to, or maybe you hoped to build up your emergency savings fund throughout the year. If you fell short of accomplishing these or other goals, think about the reasons why. Were your goals specific? Did you develop a realistic timeframe for when they would be achieved? If not, learn to set attainable and measurable goals for your finances in the new year.

**How did your investments perform?** A year-end review of your overall portfolio can help you determine whether your asset allocation is balanced and in line with your time horizon and goals. If one type of investment performed well during the year, it could represent a greater percentage of your portfolio than you initially wanted. As a result, you might consider selling some of it and using that money to buy other types of investments to rebalance your portfolio. Keep in mind that selling investments could result in a tax liability. And remember, asset allocation does not guarantee a profit or protect against loss; it is a method to help manage investment risk. All investing involves risk, including the possible loss of principal, and there is no guarantee that any investment strategy will be successful.

**Are your retirement savings on track?** Did you contribute the amount you wanted in 2017? Or did unexpected financial emergencies force you to borrow or withdraw money from your retirement savings? In that case, you can help your savings recover by contributing the most you can to your employer-sponsored retirement plan and taking advantage of employer matching (if it's available to you). Contributing to a 401(k) or 403(b) plan can help you save more consistently because your contributions are automatically deducted from your salary, helping you avoid the temptation to skip a month now and then.

# How can I protect myself from digital deception?



Imagine that you receive an email with an urgent message asking you to verify your banking information by clicking on a link. Or maybe you get an enticing text message claiming that you've won a free vacation to the destination of your choice—all you have to do is click on the link you were sent. In both scenarios, clicking on the link causes you to play right into the hands of a cybercriminal seeking your sensitive information. Just like that, you're at risk for identity theft because you were tricked by a social engineering scam.

Social engineering attacks are a form of digital deception in which cybercriminals psychologically manipulate victims into divulging sensitive information. Cybercriminals "engineer" believable scenarios designed to evoke an emotional response (curiosity, fear, empathy, or excitement) from their targets. As a result, people often react without thinking first due to curiosity or concern over the message that was sent. Since social engineering attacks appear in many forms and appeal to a variety of emotions, they can be especially difficult to identify.

Take steps to protect yourself from a social engineering scam. If you receive a message conveying a sense of urgency, slow down and read it carefully before reacting. Don't click on suspicious or unfamiliar links in emails, text messages, and instant messaging services. Hover your cursor over a link before clicking on it to see if it will bring you to a real URL. Don't forget to check the spelling of URLs—any mistakes indicate a scam website. Also be sure to look for the secure lock symbol and the letters https: in the address bar of your Internet browser. These are signs that you're navigating to a legitimate website.

Never download email attachments unless you can verify that the sender is legitimate. Similarly, don't send money to charities or organizations that request help unless you can follow up directly with the charitable group.

Be wary of unsolicited messages. If you get an email or a text that asks you for financial information or passwords, do not reply—delete it. Remember that social engineering scams can also be used over the phone. Use healthy skepticism when you receive calls that demand money or request sensitive information. Always be vigilant and think before acting.

Copyright © 2017 Investor's Capital Management, LLC. All Rights Reserved.

Content Prepared by Broadridge Investor Communication Solutions, Inc. Copyright 2017. All rights reserved.



**Julie Schatz, CFP®**

650.248.6154 CELL  
866.966.9291 x2 VOICE  
650.472.8924 FAX  
[julies@feesonly.com](mailto:julies@feesonly.com)  
Member of NAPFA, FPA,  
Menlo Park Rotary



**Jennifer Cray, CFP®**

866.966.9291 x3 VOICE  
650.472.8924 FAX  
[jennifer@feesonly.com](mailto:jennifer@feesonly.com)  
Member of NAPFA, FPA