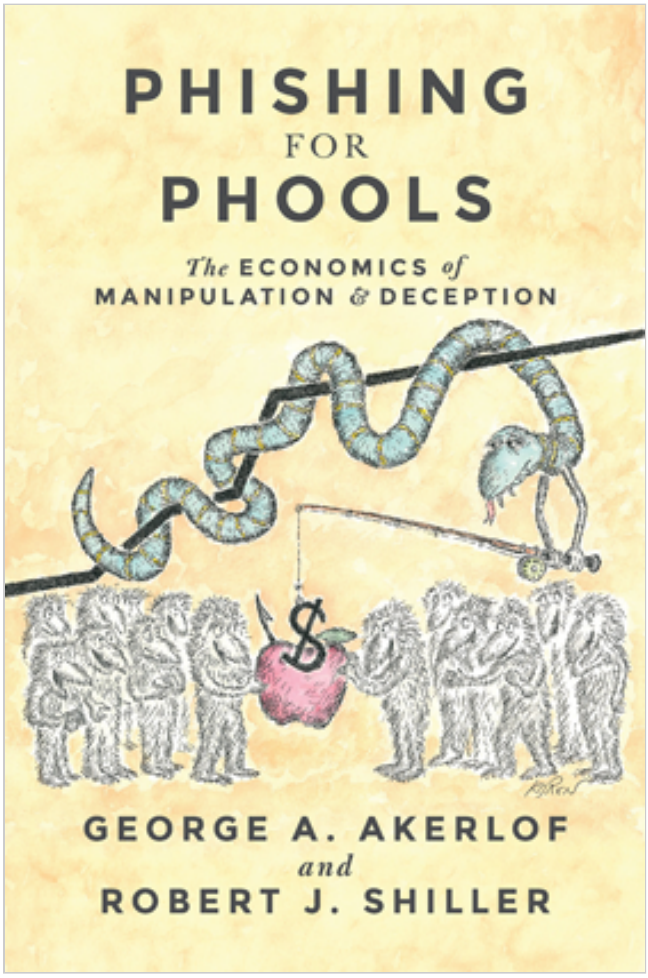
Monthly Labor Review

BLS

June 2016

Are you being taken for a phool?

Phishing for Phools: The Economics of Manipulation and Deception. By George A. Akerlof and Robert J. Schiller. Princeton, NJ: Princeton University Press, 2015, 288 pp., $24.95 hardback.



Richard Hernandez
hernandez.richard@bls.gov

Richard Hernandez is an economist in the Office of Publications, U.S. Bureau of Labor Statistics.

Take a stroll with me down memory lane, and let's remember our economics 101 class about decisionmaking and budget quandaries. If we were to go to the supermarket with a fixed budget to buy strawberries and blackberries, our goal would be to obtain a combination that makes us happiest (maximizing our utility function). This strategy is part of rational choice theory, according to which a person is believed to always be making logical choices that provide him or her the most satisfaction. However, there is a tendency to overlook irrational behavior in mainstream economic theory. What if I do not stick to that budget? Rather than doing what standard economics teaches us, suppose I pay with a credit card and exceed my fixed budget. In this scenario, the credit card industry exists as long as there is a profit to be made from providing credit because enough people demand to go beyond their budget. In the book *Phishing for Phools: The Economics of Manipulation and Deception*, George Akerlof and Robert Schiller dive deeper into the realm of behavioral economics. They make a case for why free markets that provide people what they want (as long as there are incentives in place) at an equilibrium level can be manipulated or distorted, thereby creating a new equilibrium that they call a "phishing equilibrium."

Let's start by defining the relevant terms found throughout the book. A *phish* is defined as the means by which a *phisherman* (the agent performing the phish) gets his or her target to do what the phisherman wants. (The phishing discussed in this book is not to be confused with that in the field of information and computer technology, whereby individuals attempt to acquire sensitive information, such as Social Security numbers and passwords, or even money by masquerading as a trustworthy source in an electronic

communication environment.) A *phool* is someone who has been successfully phished. There are two types of phools. The psychological phool can be phished by one of two methods: either by having a cognitive bias that is exploited or by giving in to emotions despite an awareness of the situation at hand. The information phool acts on facts that are purposely intended to be misleading. The authors also delve into four areas in which they believe that "NOBODY-COULD-POSSIBLY-WANT" to be phooled—areas where it makes no sense not to have optimal outcomes: our health, the quality of our government, market stability, and personal financial security. With all these terms, the authors relate stories in many settings, ranging from consumer and financial markets to congressional elections, to prove their theory of phishing equilibrium.

Taking us on a discovery ride into advertising, the authors provide ample examples from the minds of advertising "gurus" such as Albert Lasker and David Ogilvy. Crafting the right story and creating an accurate message that leads to customer engagement with a product is something marketers are able to master. So, how do they come to sell you that product? Simply by finding out what works and what doesn't, using trial-and-error statistical tests. Did you ever wonder why advertisements provide different redemption codes? The answer is that there is no better way to target an advertiser's audience than by testing which codes work and which do not. If the redemption code for a product touted in advertisement A was redeemed more often than the code for a product extolled in advertisement B, then a logical conclusion would be to run only advertisement A in the future. This consideration is one of many aspects of *phishing equilibrium*, meaning that, if there is a way to make a profit from our tastes, then the phisherman will keep trying until he or she finds it. In our era of big data, marketers have become increasingly knowledgeable about our preferences and are better capable of exploiting them. They are getting better and better at playing to our human nature of wanting a product rather than needing it. At its core, the book is trying to flesh out the idea that there is a narrative in our minds which leads us to make irrational decisions—an idea that standard economics misses. Akerlof and Schiller tie it back to the strawberries-and-blackberries example: Say the blackberry marketers crafted the narrative that blackberries are superior in taste to strawberries. Then, even though we wouldn't be maximizing our utility by purchasing only blackberries, we end up doing so because the monkey-on-the-shoulder tastes created by advertisers establish a new market equilibrium. In this regard, the authors conclude that free markets allow people to choose between their "real tastes" and "monkey-on-the-shoulder-tastes," and then people are freely available to be phished.

Certainly, Akerlof and Schiller do not attack the free market; rather, they argue that free markets have systemic flaws. They maintain that free markets are still the best economic means of raising living standards for all, but there are some unwanted externalities that the phishermen take advantage of in plying their "trade." For example, deregulation of the banking industry led to the savings-and-loan crisis of 1986–95, and that crisis in turn brought about the recession of 1990–91. In that scenario, the externality was the inflation-adjusted cost of $230 billion on the backs of taxpayers that was caused by the failure of the savings and loans, which became "tools for the phishermen."

The book offers various examples of phools being phished in many settings in a very easy-to-read way. With regard to phishing equilibrium, one may ask what the authors consider to be fair or unfair in the marketplace. The book does not define or explore what constitutes fair or wanted outcomes. Instead, it leaves the reader wanting resolutions of some issues. For example, is merely having an awareness that there are deficiencies in the market enough for people to modify their behavior so that they don't get taken for a phool? How do we go about solving the problem of companies getting around certain legislation? Moreover, does it really matter if I buy more blackberries than strawberries? I am the only person affected by that decision. However, in a different scenario,

one in which the player learns to phish in a way that affects us all (e.g., by crashing the financial markets), minimizing market inefficiencies does matter. And that is where the real lesson of this book comes into play: we should always be aware that we can get phished, and we must find ways to minimize that possibility.