

Book Reviews

AKERLOF, George and Robert SHILLER, 2015, *Phishing for Phools: The Economics of Manipulation and Deception*, Princeton, Princeton University Press. 288 pp.

The authors, both Nobel prize winners, deliberately chose a peculiar title using **ph** instead of **f** in order to underline "the economics of manipulation and deception" (both terms used in the sense of "deceit") and not without reason, since this book concentrates on the manner that individuals are the victims of deceit in a system of "free markets" that supposedly precipitate such situations. Thus, while the authors express their admiration for the free market, in line with the economics of behavior, they present cases and examples of scams to which individuals who are not well informed and have psychological limitations fall victim.

The word *phishing* originally referred to how the unscrupulous attempted to cajole internet users, which is why the authors use the word *phools* and not *fools*. Beyond semantics, Akerlof and Shiller question the rationality of economic agents in the "traditional economy" and expressly seek to alert people to the various forms of manipulation and deception being practiced.

They decide to start off by creating a straw man when they refer to the "traditional economy," a term they do not define but which seems to refer to the most elemental economic models - those that one typically starts with in order to then develop more complex and realistic models. It does not bear repeating that no one considers individuals to be calculating machines that take completely rational decisions in markets without transaction costs and this is why the authors, when they create their straw man, conveniently underestimate advances in economic theory, especially the economics of

organizations and the interactions between various economic agents when there are transaction costs; this creates the impression that they are developing innovative ideas.

Akerlof and Shiller distinguish between informational *phools* and psychological *phools*. The first are "fished" because they only have access to partial information, while the second incorrectly evaluate the available options because of cognitive limitations or because they get carried away emotionally. The supposed result is a *phishing equilibrium* in a competitive system in which *phishing* constantly occurs. Under the authors' definition of this concept, the *phools* lose when they are scammed.

This book presents various interesting and valuable cases and examples of *phishing*. However, at the beginning it discusses the case of slot machines in casinos and the consequences of addiction to them – this is not the best example given that their definition of *phishing* does not allow for the individual subject to deception winning as a result of it. Might it not be the case that even when the gamblers lose money, in some sense they feel that they won because they enjoy gambling? The authors would have done better to present, especially at the beginning, a case in which the *phish* are unmistakably the victims of deception, rather than one in which the perpetrators assume that their targets are deceived, given that not everyone who appears to be a *phool* really is one.

Other examples in the book are more interesting and relevant, such as those in which the authors describe *phishing* situations in the financial market (this should come as no surprise, since one of the authors researched the financial debacle in 2008), the real estate market, the advertising industry, auto sales (which should also not come as a surprise since one of the authors investigated the so-called "market for lemons" in auto sales), the pharmaceutical industry, the tobacco and alcohol markets, innovation, and even political markets in which politicians deceive voters. However, many of these cases, despite their attractiveness, are not original. Akerlof and Shiller reuse cases and examples that have already been discussed, some for decades (such as the harm generated by the consumption of cigarettes, fraudulent medicines, and persuasive publicity). Given this approach, the authors may be directing their book at younger readers that do not know or remember these older cases but, at the same time, they bring together many examples to demonstrate that *phishing* can happen in a range of situations.

One of the important concepts in the book is *phishing equilibrium*. However, this equilibrium is not covered rigorously. For example, the competition that dissipates income resulting from deceiving victims is not described. Surprisingly, the bibliography does not include literature about *rent-seeking* or about competition for dissipating earnings from *phishing*, which includes alerting possible victims to the consequences of falling into traps. They also

do not consider those *phools* who learn from their errors or the consequences of repeating experiments that show how persons are cheated. It is easier to describe a scam that *phools* experience than to show repeated scams. It would have been useful to analyze the impact that learning about *phishing* can have and to study the conditions that make it easier, which type of people are most likely to fall for scams repeatedly, and the characteristics of the situations in which such people fall into traps several times.

Varied examples in the book illustrate the importance of legal measures that would make *phishing* more difficult; however, cases in which regulations introduce new incentives for scams are not highlighted. The authors display a bias in favor of regulations even though many private organizations can also act against scams. For example, they consider illogical the argument that we should not have fire stations because this would lead people to be less careful. Nevertheless, *phools* can change their behavior if they believe that regulators protect them. In addition, the authors do not investigate the possibility that regulation can displace private organizations that might offer better protection. The authors should have noted the difficulty of reaching an equilibrium when regulation supposedly defends the *phools*. It also would have been useful to present more cases in which regulators themselves are *phools* or *phishers*, or both at the same time, especially since not everybody necessarily loses when *phishing* occurs. For example, in the chapter about pharmaceutical *phishing*, it would have been useful to evaluate the way in which the regulation of drugs also generates a cost to society. Additionally, just as it is suggested that the state should intervene to control *phishers*, why not talk about the cases where regulators are both *phishers* and *phools*?

This book, more than being innovative for the ideas it contains, is useful as a compilation of a variety of cases of *phishing*. The more than 400 bibliographic references spanning 24 pages, complemented by another 52 pages of endnotes (which make up approximately two-thirds of the book), make *Phishing for Phools* more of an annotated bibliography and a guide to reading than a new contribution. While some readers will think that they have been *phished* when they bought this book, despite private reviews of it, one cannot but recommend it.

Folke Kafka*

Katz Graduate School of Business, University of Pittsburgh, Pittsburgh

* Email: fkafka@katz.pitt.edu
DOI: <http://dx.doi.org/10.21678/apuntes.79.873>