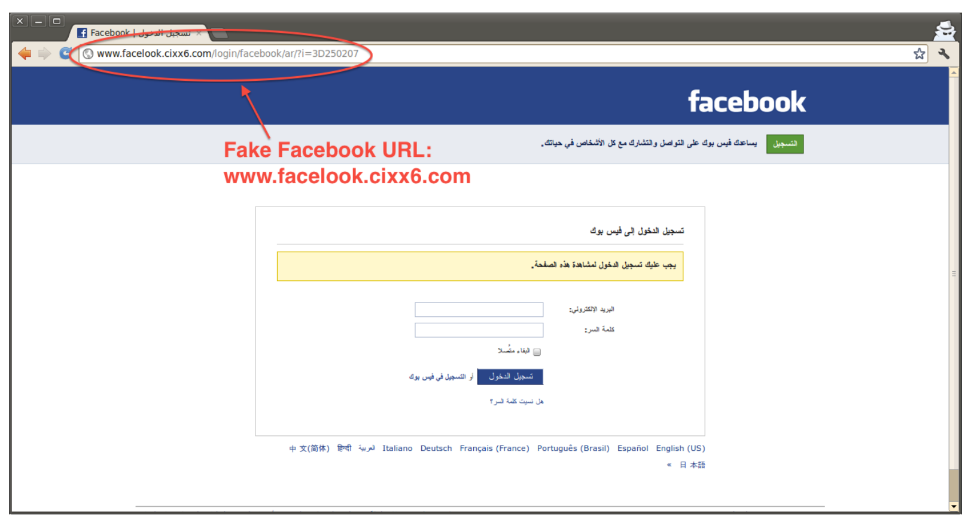
UNIVERSITY OF CAMBRIDGE

Understanding scam victims

Seven principles for systems security

Frank Stajano and Paul Wilson


Facebook | تسجيل الدخول

www.facelook.cixx6.com/login/facebook/ar/?i=3D250207

يساعدك فيس بوك على التواصل والتشارك مع كل الأشخاص في حياتك.

Fake Facebook URL: www.facelook.cixx6.com

تسجيل الدخول إلى فيس بوك

يجب عليك تسجيل الدخول لمشاهدة هذه الصفحة.

البريد الالكتروني:

كلمة السر:

□ البقاء متصلا

تسجيل الدخول
أو التسجيل في فيس بوك
هل نسيت كلمة السر؟
中文(简体) हिन्दी العربية Italiano Deutsch Français (France) Português (Brasil) Español English (US)
« 日本語

E. Galperin, M. Marquis-Boire

Check out this EFF-reported Facebook phishing attack targeting Syrian activists in 2012: the page looks like Facebook but was set up by pro-Syrian-government hackers to entrap Syrian activists.

Security engineers build system defenses largely based on how *they* think users should respond to threats. From the engineer's viewpoint, just reading the URL would tell you straight away that this isn't Facebook. But normal users are not engineers: they respond differently. They don't understand the syntax of URLs, nor the difference between the HTTPS padlock and a picture of a padlock in the page itself. As a result of this mismatch, systems are vulnerable.

We need to understand how users *really* behave, and what psychological traits make them vulnerable. Engineers don't understand user psychology too well. Fraudsters, however, do! Therefore engineers had better learn from fraudsters, if they want to build secure systems.

The Real Hustle, a BBC3 TV show by Paul Wilson and Alex Conran that aired for 11 series between 2006 and 2012, documented hundreds of actual scams and frauds, recreating them for hidden cameras. Were all these scams completely original or did they reuse a few basic ideas? Suspecting the latter, we set out to identify some kind of a "basis" for the "vector space of frauds". We identified seven principles that explain fundamental "system vulnerabilities" of the human psyche that fraudsters have been exploiting long before computers were invented. An understanding of these principles is necessary to build secure systems. Not just computer systems: any systems that involve people.
Our contributions: we documented existing scams; we extracted underlying principles; and we applied them to strengthen systems security.

We observed and documented hundreds of frauds, but almost all of them can be reduced to a handful of general principles that explain what victims fall for.

The exact set of principles is not as important as the idea that almost all scams can be reduced to a few principles (cfr table below). These principles are also responsible for vulnerabilities in computer systems, but they were exploited by fraudsters for centuries before computers were invented. They are *rooted in human nature*.

It is arrogantly idiotic for security engineers to whinge that "users are gullible". Certain behavioural patterns are simply human nature. Smart security engineers must acknowledge their inevitability and design the system to prevent their exploitation.

Principles to which victims respond, as identified by three sets of researchers.

Principle	Cialdini (1985–2009)	Lea et al. (2009)	Stajano-Wilson (2009)
Distraction		~	●
Social Compliance (a.k.a. "Authority")	●	○	○
Herd (a.k.a. "Social Proof")	●		○
Dishonesty			●
Kindness	~		●
Need and Greed (a.k.a. "Visceral Triggers")	~	●	○
Scarcity (related to our "Time")	●	○	~
Commitment and Consistency	●	○	
Reciprocation	●		~

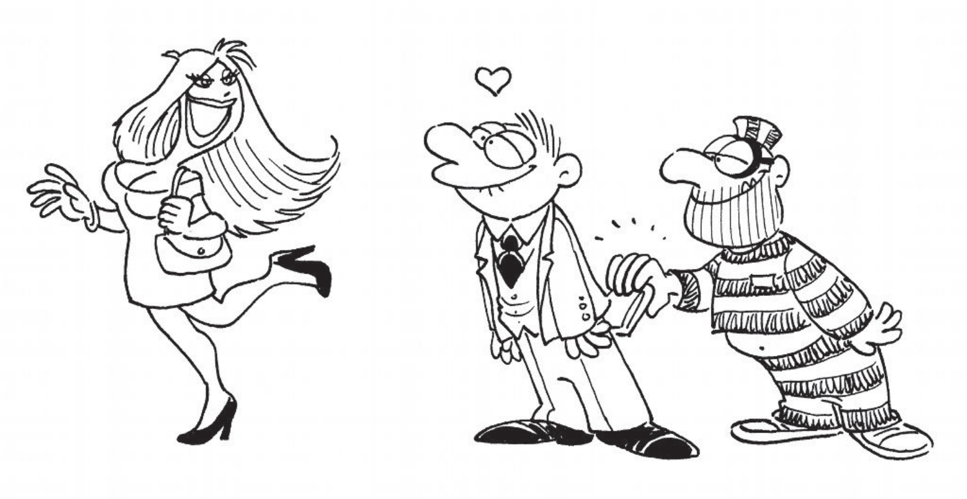
- ● First identified this principle
- ○ Also lists this principle
- ~ Lists a related principle

After distilling our initial set of principles by observing fraudsters, we discovered striking similarities with the principles that Cialdini identified by observing salesmen (*Influence: science and practice*, 1985; 5th edition 2009). That's appropriate: after all, the techniques of fraudsters and pushy salesmen are very similar; perhaps the main difference is that, at least sometimes, what the salesmen do is legal...
Another relevant work was by Lea et al, who studied mass-marketed scams in their 2009 report on "The psychology of scams" for the Office of Fair Trading.

We first published this work in 2009 as a tech report and then in a journal two years later after peer review. By 2015 it had over 75 citations on Google Scholar. We gave over a dozen invited talks on this research in four continents: USENIX Security, CMU, MIT, Columbia, ETHZ, EPFL, Google, StackOverflow, Blackfoot, EU FIA Budapest, ISSA Ireland, Università di Roma La Sapienza, Athens University of Economics, Keio, AusCERT...

Comms ACM 54(3):70-75, March 2011.
DOI: 10.1145/1897852.1897872.
URL: http://www.cl.cam.ac.uk/~fms27/papers/2011-StajanoWil-scam.pdf.

University of Cambridge Computer Laboratory Technical Report 754, August 2009. URL: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf.



Distraction

While you are distracted by what retains your interest, hustlers can do anything to you and you won't notice.

Social Compliance

Society trains people not to question authority. Hustlers exploit this "suspension of suspiciousness" to manipulate you.

Herd

Even suspicious marks will let their guard down when others next to them appear to share the same risks. Safety in numbers? Not if they're all against you.

Dishonesty

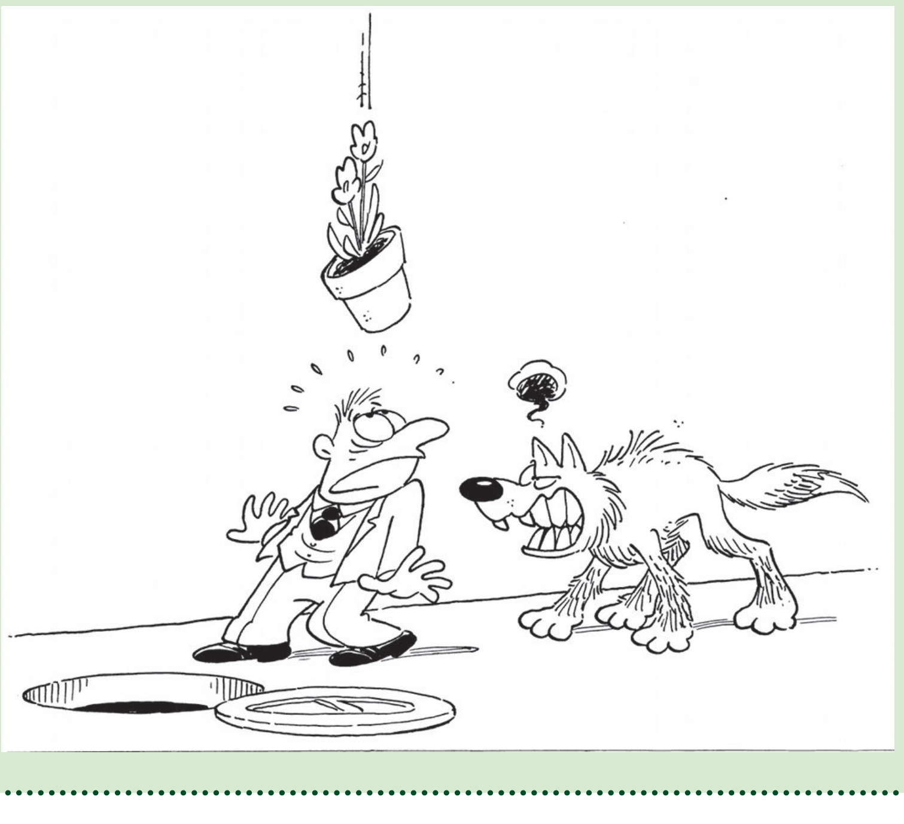
Your larceny is what hooks you. Thereafter, anything illegal you do will be used against you by the fraudster.

Kindness

People are fundamentally nice and willing to help. Hustlers shamelessly take advantage of it.

Need and Greed

Need and greed make you vulnerable. Once hustlers know what you want, they can easily manipulate you.



Time

When you are under time pressure to make an important choice, you use a different decision strategy. Hustlers steer you towards a strategy involving less reasoning.

Cartoons by Silvia Ziche

2015-08-18