



Deceptive Technologies: Cash, Ethics & HCI

by Florian N. Egger

Everyone working on web projects will have noticed how HCI and marketing get increasingly integrated to deliver positive and memorable experiences to users. Since my research has looked at the factors that make people trust e-commerce sites, I've had many opportunities to observe how simple design tricks can affect people's attitude towards a website. Ultimately, my findings will help online businesses implement a communication strategy geared to minimise perceived risks and increase their professionalism.

This is not dissimilar to the work on credibility done by Fogg's captology group at Stanford. They claim to design persuasive technologies that bring about positive changes in the users' attitudes and behaviours. But who says the same principles could not be used to misinform people? The truth is: The science of persuasion is intimately linked to that of deception.

User experience manipulation happens all the time. Let's take an example from the gambling industry. In the course of a study into what makes people trust online gambling sites (cf. our short paper at CHI 2002), I came across the following story in a book called *BeatWebCasinos.com* (Bill Hayward, RGE Publishing)

Imagine you want to try out your luck online. You browse the web for casino websites and notice that several sites feature a Safebet trust seal. Such a seal can't be a bad thing, you think, and you click on it. As expected, you leave the casino for the Safebet site, where you see that the casino is indeed registered with that trusted-third party. You explore the site that says it is a non-profit, independent organisation that provides certification and dispute resolution services to help regulate the industry and protect the interests of the players. It even has its own team of mathematicians to analyse whether the casinos' odds are fair. So far, so good.

However, a simple whois search revealed that the person who registered the safebet.org domain also

registered 51 casino domain names. It turned out that these folks made up a phoney certification scheme and proudly featured the allegedly independent seal on their own gambling sites. No doubt the average surfer would not have double-checked the legitimacy of the seal and would have been very easily deceived by this little design trick. Let's consider another example.

Imagine a foreign person who wants to work in the States but only possesses vague information about the green card lottery. She runs a web search and finds the site of the USA Immigration Services in Washington D.C. The name certainly sounds blandly official and the site name ends in .org. Its logo features the eagle and the American flag. The site's graphic design looks professional and includes the hyper-linked logos of the USA Freedom Corps, The White House and FirstGov (the US e-government portal). There's plenty of information about the green card lottery and even a neatly designed eligibility checking system. Fill in a form, pay a processing fee and you're all set. But things are not as they seem. Unless you read the terms and conditions, you may never know that this is not an official government agency but only a for-profit intermediary—participation in the lottery is actually free! Exploiting the target audience's poor familiarity with US institutions, this website might mislead people into thinking they're dealing with the Immigration and Naturalization Service.

There can be a fine line between user experience design and user manipulation. Indeed, our insights into the psychology of computer-mediated communication can easily be misused by individuals with less noble intentions. However, HCI research could also benefit from studying these 'dirty tricks'. If we had more knowledge about their user experience strategies, we would be able to better educate web surfers on the one hand and, on the other, recruit some persuasive designs for more legitimate causes.