

## DECEIVED – UNDER TARGET ON LINE

Stefano Grazioli and Sirkka L. Jarvenpaa

MSIS Department, CBA 5.202, B6500

McCombs School of Business, University of Texas at Austin

Austin, TX

[Stefano.grazioli@bus.utexas.edu](mailto:Stefano.grazioli@bus.utexas.edu); [sirkka.jarvenpaa@bus.utexas.edu](mailto:sirkka.jarvenpaa@bus.utexas.edu)

Suppose you're trying to access your favorite search engine. You haven't bookmarked it, so you type 'google.com' in your browser. Accidentally, you mistype and enter 'gogle.com' instead. Your browser brings you to a page that looks just like Google's but is connected to a competitor's search engine. At the bottom of the page there is some faint print warning that the site you're viewing is *not* affiliated with google.com. Did you take time to read it? Probably not. Something similar would have happened if you had typed 'gugle.com', 'guggle.com' or 'goggle.com'<sup>1</sup>.

You've just been 'page-jacked'. While the negative consequences from this particular incident are probably not very serious, it is easy to imagine what might have happened if a criminal tried to simulate your bank website? in particular the page where you log-in your account number and your password. Actually, there is no need to imagine it. It has already happened. Page-jacking—the practice of simulating a legitimate page to obtain secrets or business from an unsuspecting Internet user—is an example of Internet deception [2]. Studies have shown that even sophisticated, technologically competent Internet shoppers are relatively easy prey for such deceptive copycat sites [4].

More broadly, page-jacking is just one example of a set of deviant behaviors that we call Internet deception (e.g., fraud, misleading advertisement, manipulations of financial information). In fact, the Internet may offer more fertile grounds for deception than other channels of commerce and may have fundamentally altered the social, legal, and economic distribution of deceptive practices. For starters, the

---

<sup>1</sup> These domain names were active in February 2001.

Internet makes identity (of items of exchange, individuals, and organizations) easy to falsify and difficult to authenticate. It also lowers the economic resources needed to set-up a credible-looking storefront and provides deceivers with an extended reach. Finally, the Internet makes the proceeds of crime easier to secure not only anonymously but also in jurisdictions where pursuing perpetrators is difficult [8].

In the period from 1996 to 1999, the number of reports to Internet Fraud Watch (IFW), a research organization funded by a major credit card network, grew on average more than 250% annually. Consumer complaints have grown so numerous that several federal agencies—the Federal Trade Commission, the Securities and Exchange Commission, and the Department of Justice—have started specialized programs for the detection and prosecution of Internet fraud.

While Internet deception is troubling in its own right, an increase in its occurrence signals a threat to Internet commerce. When buyers have trouble discriminating between good and bad products, even a small number of deceptive sellers might ‘poison’ a market? driving out good products and eventually the consumers [1, 7]. Growth of Internet deception may increase entry barriers to new businesses that don’t have an established brand name and may eventually encourage governmental regulation and oversight, which in turn increases the cost of doing business online and decreases channel competitiveness.

To counter these threats, we initiated a research project to understand how the deceivers work on the Internet. A better understanding of this criminal behavior is a critical first step toward more effective detection and protection programs. We used the Theory of Deception [6] to understand the kind of deceptive tactics businesses and consumers use against other businesses and consumers on the Internet. We built a database of 201 publicly reported cases of Internet deception, and our analysis of the cases identified both old and new forms of deception. Next, we describe the theory, followed by results and conclusions.

## **Deception Tactics**

According to the Theory of Deception, a deception is a cognitive interaction between two parties under conflict of interest. One party? the deceiver? manipulates the environment of the other party? the victim? so as to foster an *incorrect representation* of the victim's situation in order to instigate a desired action, one the victim would unlikely take without the manipulation.

Deception works because it exploits systematic weaknesses in our cognitive systems. Researchers argue that deception is the inevitable price that we must pay to cope with the complexity of the world. To gain efficiency, well-designed cognitive mechanisms take representational shortcuts, assumptions about the world that are generally true but that may occasionally fail. Deceivers intentionally exploit these weaknesses.

The Theory of Deception identifies seven common tactics that fall into two categories: they work either to prevent the victim from fully understanding the nature of the transaction or to actively induce a faulty representation of the core (the item involved in the exchange between deceiver and victim). Often, real-world deceptions are composed of more than one of these tactics, thus one manipulation corroborates and supports the others. Table 1 describes the seven deception tactics and introduces examples of each of them.

As the Theory of Deception focuses almost exclusively on deceivers and their tactics, and the process of detecting deception by the victims, we augmented our study by incorporating works from the fields of criminology [3], and information system security [11].

## **Results: Internet Deceivers at Work**

Based on the systematic analysis of a broad array of documents (magazines and newspaper articles, court proceedings), we have built a database of 201 cases of Internet deception that occurred between 1995 and 2000. The methodology for the study is described in more detail in Figure 1.

The cases in our database suggest that Internet deception is serious; substantial amounts of money are being lost/stolen through such activities. Our study found a median loss per victim of \$722 and the highest alleged loss over \$14 million. As suggested by criminological theories, the occurrence of Internet deception is increasing at approximately the rate of growth of the Internet itself. Figure 2 shows cases of Internet deception plotted with the growth of four commonly used indicators of Internet size: the number of Internet hosts, the number of Internet users worldwide, the number of Internet users in the U.S., and the revenue from on-line retail customers.

Our study suggests that most common Internet deceptions are simple, almost primitive—sellers promising to sell merchandise that they don't possess, or buyers promising to pay with no intention to do so. These results (see Table 2) are consistent with current criminological theory on crime, which typically finds that the majority of criminal acts are the result of poorly conceived actions motivated by greed and the need for an easy and immediate gratification, rather than the result of brilliant criminal minds conceiving diabolical plans [3]. Indeed, inventing (36%), relabeling (25%) and mimicking (22%) are the most often used tactics, accounting for about 82% of the sample cases. Consumer to consumer (C2C) exchanges at auction sites seem particularly fertile terrain for these types of unsophisticated schemes.

Dazzling and double play are the least used (less than 3% of the time). We argue that dazzling, decoying, and double play are seen less frequently because they are more sophisticated tactics that require a more subtle understanding of the potential victims' cognitions. For this reason they might need more time to be learned and perfected (and detected and reported). The good news is that there is no evidence that deceptions are becoming more sophisticated over time. However, as potential victims become more sensitive to the issue of Internet deception and learn how to better protect themselves, and as deceivers learn more effective practices, the level of the sophistication of deception may well increase.

Many of the cases we observed are variations of well-known deceptions already used in non-Internet contexts. However, we have also identified cases in which the Internet has altered the social dynamics of old tactics. A good example is the case of a self-proclaimed investment expert who used the

Internet to promote stocks he owned, selling them as soon as their market price increased as a result of his boastful postings, a practice long known on Wall Street as “pump-and-dump.” The new spin to this old deception is that the defendant in the cease-and-desist order issued by the Security and Exchange Commission is a fifteen-year-old boy who traded from his bedroom in a New Jersey suburb. Arguably, the specifics of Internet technology played a crucial role in the deception, allowing anonymous interactions between the deceiver’s multiple identities and his victims. In a brick-and-mortar world, this particular deceiver would have likely not succeeded. After all, who would take financial advice from a fifteen-year-old?

Even more interesting, we found new forms of deviant behavior emerging that are enabled by the specifics of the Internet or by the economics of the business models that are associated with the Internet. In addition to page-jacking, which was described above, new forms of deception include “line-jacking” (disconnecting a victim’s modem from the legitimate ISP telephone line and reconnecting it to a more expensive one) and “false-bill baiting” (sending an intentionally incorrect bill to a victim via e-mail and asking her to call if she has any problem with the bill. When the victim actually calls, she reaches a pay service and incurs charges that are billed to her phone company).

Looking at victims and perpetrators we discovered that not all forms of deception are created equal. In our sample, Internet deception occurs most frequently between a business (or somebody impersonating a business) and a consumer, with the consumer as the victim. However, the proportion of instances of B2C deception where the consumer is the victim is decreasing.

The second most frequent case is the deception perpetrated by a consumer against another consumer. Perhaps because deceivers see consumers as easier prey than businesses or because the Internet is allowing consumers to transact with each other in increasing numbers, the proportion of instances of C2C deceptions over the total is increasing. B2B deceptions and C2B deceptions (where a business is the victim) are much less frequent.

The spectrum of goods and services that compose the core in our sample of cases is very wide and suggests that no transaction is safe. There are, however, some recurring themes. A third of the deception cases we analyzed had investments, securities, or credit as their core. Auctioned items, ranging from consumer electronics to collectibles to works of art, also appeared frequently as a core. Further, our case data suggests that auction buyers are more likely to be victimized than sellers are. Kauffman & Wood [7] have theorized that Internet auctions increase information asymmetry between sellers and buyers and increase the incentive for sellers to behave opportunistically. What's more, the number of deceptions in which the core is an auctioned item is increasing in both absolute numbers and in proportion to the total number of deceptions in our sample.

Retail consumer goods appear frequently as deception cores (15% of the cases). A final 17% of the cases involve a wide range of good and services, each with a much lower frequency of occurrence. Examples include specious business opportunities (e.g., work-at-home programs), phony professional services (e.g., credit restoration services), donations to not-for-profit organizations, miraculous medicaments (e.g., shark cartilages), sexually explicit materials, travel arrangements, and imitation luxury goods.

### **Deterrence, Prevention and Detection**

Our study confirms early suggestions that the perils of the Internet are real and point to the need for monitoring agencies to take practical action on reducing the occurrence of Internet deception. Target actions include, but are not limited to: 1) deterrence, 2) prevention, and 3) detection [11].

*Deterrence* consists of measures that reduce the perpetrators' propensity to commit fraud and the victim's propensity to engage in risky behaviors. Education can raise the awareness of consumers and businesses regarding the tactics used by deceivers as well as those business models and industries that are at risk. Our study results suggest that Internet auctions and the trading of financial instruments are

particularly at risk, but also that no one industry seems to be deception-free. Therefore, interventions designed to raise awareness of tactics used should begin with? but not stop at? these two arenas.

We have seen that businesses are vulnerable to mimicking deceptions, in which the deceiver assumes an otherwise legitimate identity or forges a deception core. Thus, businesses need to be especially alert to the possibility that their customers are not who they claim to be. Consumers, on the other side, are vulnerable to relabeling and inventing deceptions. These tactics are based on misrepresenting goods or services, or even lying about their existence. Monitoring agencies and responsible companies have started campaigns to sensitize the public and their own employees to these risks.

*Preventive measures* are active countermeasures with the capacity to ward off abuse. This is the realm of technological solutions, such as secure protocols and encryption. Mimicking, the most serious threat to businesses, can be prevented by implementing stronger forms of authentication, which is particularly difficult in Internet environments. Solutions include the use of traditional checks based on personal secrets (e.g., passwords and PINs), digital certificates and digital signatures within a comprehensive Public Key Infrastructure, and biometric techniques. Implementing these solutions, however, requires balancing the need for accountability with the social desire for privacy and anonymity.

Inventing and relabeling, which prevalently affect individual consumers, are harder to fight because detection requires assessing the content of an offer to transact via the Internet. Reputation systems and performance histories are means of preventing consumers from being victimized by misrepresentations of goods and services that have recently been the object of scientific investigation [10]. Other remedies may also exist. One suggestion is to include in every browser a relatively straightforward technology designed to conduct simple checks, such as accessing lists of known questionable sites, whenever a user appears to be initiating a business transaction. However, the effectiveness and usability issues of such remedies remain to be determined.

When deterrence and prevention are not sufficient, the potential victims or the monitoring agencies need to *detect* that a deception has been attempted. Customer complaints to authorities appear to be the most likely means of detection. Other means of detection are the ‘browsing sweeps’ conducted by various monitoring agencies (e.g., the Federal Trade Commission, the Security and Exchange Commission). Browsing sweeps are periods of time in which an agency uses large amounts of resources to search the web for suspicious activities. These agencies are also charged with creating visible locations for gathering tips and complaints from victims. The Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) have created the Internet Fraud Complaint Center. From May to November 2000, the Center received 37.5 million visits and over 20,000 complaints [9]. However, little is known about the methods monitoring agencies use to scan the Internet, their effectiveness, or the nature and characteristics of the gathered Internet user complaints.

In most cases, detection occurs only after the victim has sustained a loss. Sometimes Internet consumers are able to protect themselves, noticing inconsistencies that lead to detection before a loss is borne. In one case, the targeted victim noticed that a digital camera allegedly sold by an individual on a major auction site came in a box from a well-known Internet retailer. Suspecting foul play, the victim contacted the retailer and found the camera had been bought with a credit card in her own name on an account that she had never opened<sup>2</sup>. Again, education of consumers about how deceivers operate and how to identify their tactics may be the key to help individuals successfully detect deception.

---

<sup>2</sup> Interestingly, this case includes two distinct mimicking deceptions: one against the eBay bidder and one against the credit card company. Case described in Interactive Week from ZDWire “Net Posses Saddle Up Against Cybercrooks” 10/18/1999.

## References

1. Akerlof, G. A. "The market for 'lemons': Quality, Uncertainty and the market mechanisms," *Quarterly Journal of Economics* (84), 1970, pp. 488-500.
2. FTC v. Pereira, et al. "Complaint for Permanent Injunction and other Equitable Relief", *Case No. 99-1367-A*, U.S. District Court, E. D. Alexandria, VA, 1999.
3. Gottfredson, M., and Hirshi, T. *A general theory of crime*, Stanford University Press, Stanford, CA, 1990.
4. Grazioli, S., and Jarvenpaa S. "Perils of Internet fraud", *IEEE transactions on Systems, Man, and Cybernetics* (30:4), 2000, pp. 395-410.
5. Hodson, R. *Analyzing Documentary Accounts*, Sage, Thousand Oaks, CA, 1999.
6. Johnson, P. E., Grazioli, S., Jamal, K., and Berryman, G. "Detecting deception: Adversarial problem solving in a low base rate world," *Cognitive Science* (25:3), 2001, pp. 355-392.
7. Kauffman, R. and Wood, C. "Running Up the Bid: Modeling Seller Opportunism in Internet Auctions," *The Proceedings of the 2000 Americas Conference on Information Systems*, Long Beach, CA, August 10-13, 2000.
8. Morris-Cotterill, N. "Use and abuse of the Internet in fraud and money laundering", *International Review of Law Computers and Technology* (13:2), 1999, pp. 211-228.
9. National White Collar Crime Center and the Federal Bureau of Investigation. *Internet Fraud Complaint Center: Six Months Data Trends Report*, 2001.
10. Resnick, P., Zeckhauser, R., Friedman, E., Kuwabara, K. "Reputation systems". *Communications of the ACM* (43:12), 2000, pp. 45-48

11. Straub, D. W., and Welke, R. J. "Coping with systems risk: Security planning models for management decision-making," *MIS Quarterly* (22:4), 1998, pp. 441-469.

**Table 1. Deception Tactics**

	<b>DECEPTION TACTIC</b>	<b>DEFINITION</b>	<b>INTERNET EXAMPLE</b>
Prevent an accurate understanding of the deception core.	Masking	Eliminating or erasing crucial information so that representation of key aspects of the item does not occur, or produces an incorrect result.	Failing to disclose to Internet newsletter readers that the publisher of the newsletter receives advertisement money from companies whose stocks the newsletter recommends.
	Dazzling	Obscuring or blurring information about the deception core, without eliminating it.	"Free trial", offers that don't make clear that consumers had to cancel the service before the trial period ended. Consumers who fail to cancel are enrolled automatically and begin incurring monthly charges.
	Decoying	Distracting the victim's attention away from what is really going on.	"Free stock," offers that require consumers to register themselves as stockholders with the company, which entails revealing detailed personal information (the core). The deceivers really want the very detailed and highly accurate personal information.
Actively induce faulty representations of the deception core	Mimicking	Assuming somebody else's identity or modifying the core so it copies the features of a legitimate item.	The creation of a 'mirror' bank site virtually identical to the legitimate site. The site induces bank customers to reveal secrets such as account numbers and passwords.
	Inventing	"Making up" information about the core. The core might not exist, or its characteristics might be utterly unrealistic.	Electronic auction sellers who simply don't have the merchandise that they promise to sell; or allegedly miraculous medicines sold to cure very serious illnesses.
	Relabeling	Describing the core and its characteristics expressly to mislead.	Describing very risky or questionable investments peddled over the Internet as sound financial opportunities.

	Double Play	Convincing the victim that he/she is taking unfair advantage of the deceiver.	E-mails designed to look like internal memos sent by mistake by well-known investment firms. These messages contain false insider information, fabricated to induce the recipient to invest in a certain stock.
--	-------------	---	---

**Table 2 – Data Collected for Each Case of Internet Deception**

<b>DATA COLLECTED</b>		<b>EXAMPLE ENTRY</b>
<b>Case</b>	A brief textual description of the case, the reference publication, and the date of publication	CASE #113 – The deceiver scanned online classified ads on America Online and UseNet. He would e-mail individuals advertising laptop computers, offer to buy them, and ask the seller to have them sent to a FedEx office in New York City, promising cash on delivery. He would then pay for them with worthless counterfeit money orders from Emigrant Savings Bank in New York – The Dallas Morning News – 1997 --
<b>Type</b>	C2C, B2B, B2C – customer is the victim, and C2B – business is the victim	C2C
<b>Deceiver</b>	Nationality (U.S. vs. foreign)	Foreign individual
<b>Victim</b>	Number, Nationality (U.S. vs. foreign)	15 – U.S.
<b>Core</b>	Description of the deception core, i.e. the items of exchange in a deception	Cash for Laptop computers
<b>Loss</b>	Total, Minimum, Maximum, and Mean	Total loss: \$60,000 – Mean loss: \$4,000
<b>Tactics</b>	The Deception tactics used by the Deceiver (1).	Tactic used: Mimicking (i.e., copying the features of a legitimate money order)
<b>Detection</b>	How the case was detected, and whether it was legally prosecuted	It is not known how the case was detected. Case has been prosecuted.

**Table 3 – Victims, Perpetrators, and Deception Tactics**

		VICTIM AND PERPETRATOR				Total
		B2B	C2B (B-victim)	B2C (C-victim)	C2C	
DECEPTION TACTIC	<b>Inventing</b>	6		62	39	107
	<b>Relabeling</b>	3		62	8	73
	<b>Mimicking</b>	11	15	30	9	65
	<b>Masking</b>	2		24	1	27
	<b>Decoying</b>	1	1	12	2	16
	<b>Dazzling</b>	3	-	4	-	7
	<b>Double Play</b>	-	-	1	-	1
<b>Total</b>		26	16	195	59	296

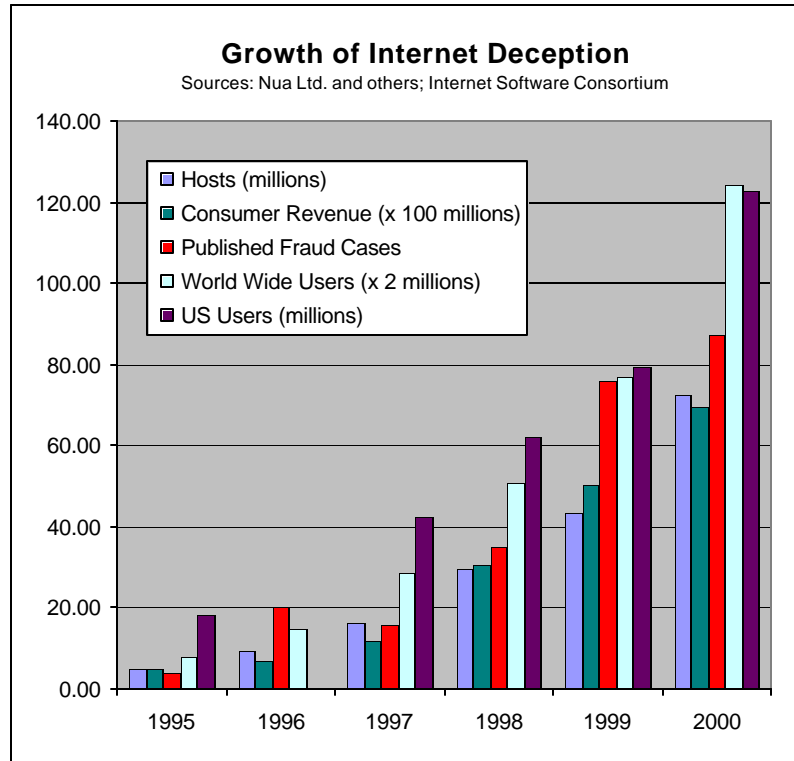
### How the Study was Done

The study used a methodology known as systematic analysis of documentary evidence [4; Krippendorff, 1980). The findings discussed in this article result from the analysis of hundreds of published documents describing cases of Internet deception that occurred between 1995 and 2000. The search for sources included all the newspapers, journals, and legal documents included in ABI/Inform, Lexis/Nexis, and Dow Jones Interactive, which are three of the largest electronic databases covering business and socioeconomic events. In addition, we searched the Internet sites of the main monitoring agencies involved in Internet deception (e.g., the Department of Justice, the FBI, the Securities and Exchange Commission, and the Federal Trade Commission).

To be included in the study, the cases had to include: 1) two parties in conflict of interest [in an Internet context there are four types of deceptions: Business to Business (B2B) where a business is the victim, Business to Consumer (B2C) where a consumer is the victim, Consumer to Business (C2B), and Consumer to Consumer (C2C)]; 2) a social exchange, mediated by the Internet; 3) a cognitive misrepresentation that is induced by the deceiver and that causes the victim to act in ways that are unfairly favorable to the deceiver; and 4) a clear indication that the case has actually occurred (e.g., names were provided; legal action was undertaken).

We identified 201 cases of Internet deception. For each case we collected a brief summary, several descriptive observations, and the deception tactics used by the deceiver. The tactics used in each case were identified according to a set of reliable coding rules. The 201 cases contained 296 instances of deception tactics. These data are listed in Table 1, along with an example case.

### Figure 1. Methodology



**Figure 2. Growth of Internet Deception<sup>1,2</sup>**

(1) - The number of U.S. users for 1996 was not available at source.

(2) - The unit of measure for the indicators in the Figure was chosen to facilitate visual comparison.