Deceived: Under Target Online

STEFANO GRAZIOLI AND SIRKKA L. JARVENPAA

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 "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 small 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."[1]

You've just been "page-jacked" [2]. 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 Web site—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. Studies have shown that even sophisticated, technologically-competent Internet shoppers are relatively easy prey for such deceptive copycat sites [4].

Page-jacking is just one example of a set of deviant behaviors that we call Internet deception (such as fraud, misleading advertisement, manipulations of financial information). 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 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, its rising occurrence is 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]. To counter this

STEFANO GRAZIOLI (grazioli@mail.utexas.edu) is an assistant professor of Information Systems at the McIntire School of Commerce at the University of Virginia.
SIRKKA JARVENPAA (Sirkka.Jarvenpaa@bus.utexas.edu) is the Bayless/Rauscher Pierce Refsner Chair in Business Administration and co-director of the Center for Business, Technology, and Law at the McCombs School of Business at The University of Texas at Austin.

[1] These domain names were active in Feb. 2001.

threat, we need to understand how the deceivers work on the Internet, so that appropriate countermeasures can be taken.

This study aims at understanding the tactics used by deceivers on the Internet. It is motivated by the dearth of empirical studies on the phenomenon. While much has been written on Internet security from a technological standpoint (for example, encryption, firewalls), the cognitive and behavioral aspects of deviant behaviors on the Internet have received much less attention [4, 7]. In addition, the Internet may have introduced an element of novelty to deceptive interactions. For starters, the Internet makes identity (of items of exchange, individuals, and organizations) easier to falsify and more difficult to authenticate than in traditional contexts. Second, it lowers the economic resources needed to set-up a credible-looking storefront. Thirdly, it provides deceivers with an extended reach. Finally, it makes the proceeds of crime easier to secure not only anonymously but also in jurisdictions where pursuing perpetrators is difficult [8]. As a result, new forms of deception, as well as new dynamics for old schemas, may appear.

For these reasons we decided to build a research database of cases of Internet deceptions and to use it to study the kind of deceptive tactics that businesses and consumers use against other businesses and consumers on the Internet. The database is based on the Theory of Deception by Johnson and colleagues [6].

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 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.

Based on a model of human cognition, the Theory of Deception identifies seven deception tactics. These tactics fall into two categories: they work either to prevent the victim from fully understanding the nature of the transaction core (the item involved in the exchange), or to actively induce a faulty representation of the core. Table 1 describes the seven deception tactics and introduces examples of each of them in an Internet context. Often, real-world deceptions are composed of more than one of these tactics, corroborating and supporting each other.

Most of the empirical work on the Theory of Deception has focused on the targets. The Theory has been applied in the past to investigate the determinants of success and failure at detecting deception in professional fields (for example, auditing, commercial lending [6]), as well as deception on the Internet [4]. Current research has incorporated works from the fields of criminology [see 3] and Information System security [as in 11] in examining how deceivers select deception tactics. Deceivers select tactics with an eye to the level of "procedural rationality" of their targets (that is, the extent to which they have in place systematic controls and deliberate decision processes). Because of this, for example, we may expect that Deceivers select "Relabeling" (see Table 1) more frequently against individuals than they do against businesses.

	DECEPTION TACTIC	DEFINITION	INTERNET EXAMPLE
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 do not 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 do not 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.	Emails 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 1. Deception tactics.

Claiming to be a business or an individual consumer also makes a difference in the selection of the tactics, because purported business can more credibly use mechanisms to induce trust and reduce perceived risk (for example, false warranties, fake assurance seals, and so on [4]) than individuals can. For example, deceivers that purport to be businesses will select "Masking" more frequently because they can more easily support this tactic with fictitious trust and risk-reducing mechanisms.

Results: Internet Deceivers at Work

Grounded in the cognitive Theory of Deception by Johnson and colleagues, we conducted a systematic analysis of a broad array of documents (magazines and newspaper articles, court proceedings) and built a database of 201 cases (296 tactics) of Internet deception that occurred between 1995 and 2000. The methodology for the study [5] is described in the accompanying sidebar.

The cases suggest that substantial amounts of money are being lost/stolen through Internet Deception. We 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 1 shows cases of Internet deception plotted with the growth of four commonly used indicators of Internet size: the number of Internet hosts, the

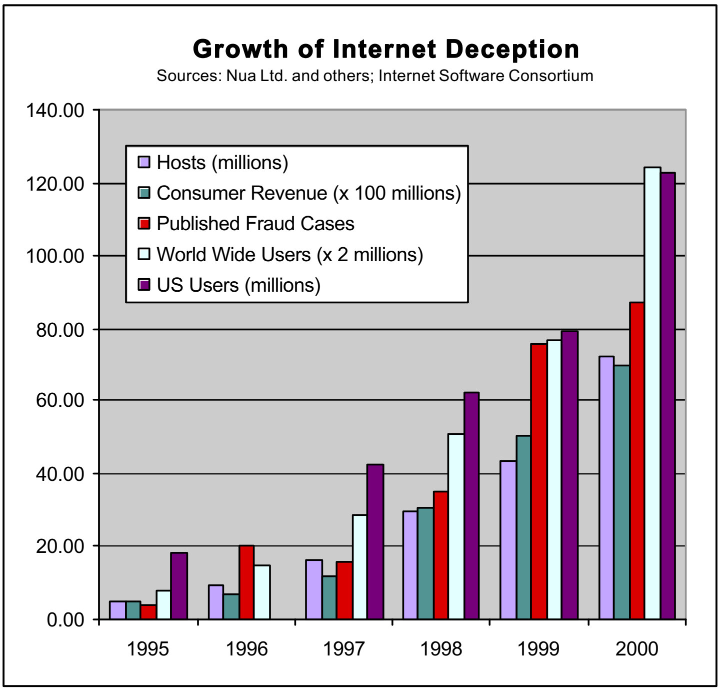

Figure 1. Growth of Internet deception.
Note: The number of U.S. users for 1996 was not available at source. The unit of measure for the indicators here was chosen to facilitate visual comparison.

number of Internet users worldwide, the number of Internet users in the U.S., and the revenue from online retail customers.

Most common Internet deceptions are simple: sellers promising to sell merchandise that they do not possess, or buyers promising to pay with no intention to do so. These results (see Table 2) are consistent with current criminological theories, which argue that most 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%) which are the simplest tactics, account for about 82% of the sample cases. Consumer-to-consumer (C2C) exchanges at auction sites seems particularly fertile terrain for these types of schemes.

Dazzling and double play are the least used tactics (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 in our sample 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 refine their practices, the level of the sophistication of deception may increase.

DATA COLLECTED		EXAMPLE ENTRY
Case	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.
Type	C2C, B2B, B2C – customer is the victim, and C2B – business is the victim	C2C
Deceiver	Nationality (U.S. vs. foreign)	Foreign individual
Victim	Number, Nationality (U.S. vs. foreign)	15 – U.S.
Core	Description of the deception core, i.e. the items of exchange in a deception	Cash for Laptop computers
Loss	Total, Minimum, Maximum, and Mean	Total loss: $60,000 – Mean loss: $4,000
Tactics	The Deception tactics used by the Deceiver (1).	Tactic used: Mimicking (such as copying the features of a legitimate money order)
Detection	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 2. Data collected for each case of Internet deception.

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 15-year-old boy. Arguably, the specifics of the 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 15-year-old?

We also found new forms of deviant behavior that are enabled by the Internet or by the economics of the business models that are associated with the Internet. In addition to page-jacking, which was described earlier, 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 email 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 AND PERPETRATOR				Total
		B2B	**C2B (B-victim)**	**B2C (C-victim)**	**C2C**	
DECEPTION TACTIC	**Inventing**	6		62	39	107
	Relabeling	3		62	8	73
	Mimicking	11	15	30	9	65
	Masking	2		24	1	27
	Decoying	1	1	12	2	16
	Dazzling	3	-	4	-	7
	Double Play	-	-	1	-	1
Total		26	16	195	59	296

Table 3. Victims, perpetrators, and deception tactics.

victim. However, the proportion of instances of B2C deception where the consumer is the victim is decreasing.

The second most frequent case in our sample 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 are sellers. Moreover, 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 also appear frequently as deception cores (15% of the cases). The remaining 17% of the cases involve a wide range of goods and services, each with a much lower frequency of occurrence. Examples include specious business opportunities (for example, work-at-home programs), phony professional services (such as credit restoration services), donations to not-for-profit organizations, miraculous medicaments (like 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 points to the need to take practical action on reducing the occurrence of Internet deception as well as to the need for conducting more in-depth research. A comprehensive strategy must include consideration of deterrence, prevention, and detection [11].

Deterrence consists of measures that reduce the perpetrators' propensity to commit fraud and the victim's propensity to engage in risky behaviors. While there is literature on the factors that affect consumer trust and perceived risk, we know very little on the determinants of deviant behaviors on the Internet: research in this direction is needed, so that effective deterrents can be identified.

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 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 (such as misrepresenting goods). 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 (for example, passwords and PINs), digital certificates and digital signatures within a 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 technology designed to conduct simple checks, such as accessing lists of known questionable sites, whenever a user appears to be initiating a business transaction.[2] However, the effectiveness and usability issues of such remedies remain to be determined. Future Internet security research should identify specific defenses against each of the identified deception tactics, as well as assess the robustness of existing security solutions against these attacks.

When deterrence and prevention are not sufficient, the potential victims or the monitoring agencies need to *detect* attempted deception. 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 (for example, the Federal Trade Commission, the Security and Exchange Commission). During a browsing sweep, the agency staff searches the Web for suspicious activities. These agencies also create 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]. Little is known about the

[2] This idea was suggested to us by Meregalli at Bocconi University.

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 sustained. 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.[3] A large body of research on deception across various contexts has concluded that humans are in general poor detectors of deception, but also that success is possible by appropriate interventions. Further research is needed to identify effective ways to help individuals and businesses to avoid being deceived by malicious individuals setting them up as targets online.

References

1. Akerlof, G. A. The market for "lemons": Quality, uncertainty and the market mechanisms. *Quarterly Journal of Economics 84* (1970), 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), 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), 355–392.

7. Kauffman, R., and Wood, C. Running up the bid: Modeling seller opportunism in Internet auctions. *Proceedings of the 2000 Americas Conference on Information Systems,* Long Beach, CA (Aug. 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), 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., and Kuwabara, K. Reputation systems. *Commun. ACM 43*, 12 (Dec. 2000), 45–48

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

[3] Interestingly, this case includes two distinct mimicking deceptions: one against the eBay bidder and another against the credit card company.

How We Built the Case Database

Gathering real world data on deviant behavior is generally not easy because perpetrators actively attempt to hide evidence that the behavior occurred. Deception is no exception. Established criminological sources do not yet cover Internet deception. The US government annually publishes detailed statistics on occurrences of criminal acts that include fraud and white-collar crimes but do not contain separate statistics for Internet crimes. The National White Collar Crime Center and the FBI have only very recently begun publishing a report on Internet fraud. Web resources (for example, the Internet Fraud Watch) do not provide much data, and generally offer data about unverified complaints. Adjudicated legal cases are scarce, also.

Under these conditions, one viable methodology is to identify cases of Internet deception available in public records and perform content analysis on them. Content analysis develops data sets based on the systematic coding of documentary evidence. The sources for our search included all the newspapers, journals, and legal documents available 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 (such as the FTC).

To identify documents that are candidates for analysis, we searched for documents that contain the keywords "Internet" and either "fraud" or "deception". These three keywords were selected by one of the authors after extensive piloting of alternatives. The selected unit of analysis is the deception "case", which includes use of one or more deception tactics by a deceiver against one or more targets. For each of the candidate documents, we determined whether the elements that comprise the definition of an Internet deception case were present. According to the Theory of Deception, a case must include:

- *Two parties in conflict of interest;*
- *A social exchange, mediated by the Internet;*
- *A cognitive misrepresentation that is induced by the deceiver and that causes the target to act in a way that is unfairly favorable to the deceiver;*
- *a clear indication that the case has actually occurred (for example, names were provided; legal action was undertaken). Cases that were presented as hypothetical, cases that were too vaguely described, and simple complaints were not included in the database.*

We restricted our analysis to documents published between 1995 and 2000. We processed all identified documents. All cases were coded by one of the authors for the presence of one or more deception tactics. Coding was done according to written coding instructions. The coding categories (such as the tactics: mimicking, masking, and so on) are derived from the Theory of Deception. The coding instructions were piloted twice with a random set of 10 cases and iteratively refined before reaching the final form.

To evaluate the reliability of the coding, a competent second coder (an individual with a graduate degree in accounting specializing in fraud detection) was trained on how to assign deception tactics codes. This second coder independently recoded all the cases in the database. An index of inter-coder reliability was then computed. The resulting Kappa value (Kappa = 0.93; approx. p<0.000) is comparable to the values observed in research on similar topics and is considered fully satisfactory. All discrepancies among coders were discussed in detail and resolved by agreement. In the rare cases where agreement was not reached, the code by the first coder (one of the authors) was selected.