Tactics Used Against Consumers as Victims of Internet Deception

Stefano Grazioli
The University of Texas at Austin

Sirkka Jarvenpaa
The University of Texas at Austin

Follow this and additional works at: http://aisel.aisnet.org/amcis2001

Recommended Citation
Grazioli, Stefano and Jarvenpaa, Sirkka, "Tactics Used Against Consumers as Victims of Internet Deception" (2001). AMCIS 2001 Proceedings. 158.
http://aisel.aisnet.org/amcis2001/158

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2001 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
TACTICS USED AGAINST CONSUMERS AS VICTIMS OF INTERNET DECEPTION

Stefano Grazioli  
The University of Texas at Austin  
grazioli@mail.utexas.edu

Sirkka Jarvenpaa  
The University of Texas at Austin

Abstract

The Internet has created new forms of consumer fraud and has altered the nature of existing fraud schemes. This paper uses the taxonomy of ‘deception tactics’ proposed by Johnson et al. (in press) to explore which fraudulent tactics are most frequently used against Internet consumers. Propositions about the relative frequency of these tactics are tested by means of data extracted from a database of Internet fraud cases that is being built at the University of Texas.

Introduction

Misrepresentations and frauds in Internet transactions have become a phenomenon relevant enough to warrant the attention of the government and society at large. Complaints from consumers and cases of litigation have grown so numerous that the Federal Trade Commission (Pitofsky, 1998), the Security and Exchange Commission and the Federal Bureau of Investigation have recently started special programs for detecting and prosecuting Internet fraud.1 The European Community is creating legislation to protect Internet consumers from fraud (Burns, 2000). Cases of Internet fraud often populate the front pages of the popular press and IS practitioners’ publications.

Internet deception is of interest to information system researchers for two reasons. The first is that Internet technology has created new forms of a social phenomenon (new forms of crime). The second is that Internet technology has altered the social, legal and economic nature of existing social phenomena. We will illustrate these points with examples in the next section. We argue that IS researchers, with their multidisciplinary focus on the behavioral and technical aspects of information systems, are optimally positioned to investigate this phenomenon and to offer solutions designed to facilitate its detection and deterrence.

Despite widespread agreement that understanding crime is the first step toward detection and prevention (e.g., Gottfredson & Hirshi, 1990; Friedman, 1998), literature searches show that not much scientific knowledge has been produced so far about the phenomenon of Internet fraud (e.g., Grazioli & Jarvenpaa, 2000). This paper seeks to fill this gap in the literature by asking what are the deceptive tactics most frequently used against businesses and consumers transacting over the Internet.

The next section briefly summarizes the body of theory used to generate hypotheses about the distribution of different types of deception across different types of victims. The third section describes the method used to build a database of cases of Internet deception, and the fourth section uses the case data to test the hypotheses. A discussion of the implications of the results concludes this paper.

Internet Deception

We draw from the theory of deception by Johnson et al (in press; also Thagard, 1992; Mitchell & Mawby, 1986). A deception is a cognitive interaction between two parties under conflict of interest. One party, the deceiver, manipulates the environment

---

1http://www.sec.gov/enforce/intrela.htm is the home of the Office for Internet Enforcement of the S.E.C; http://www.usdoj.gov/criminal/fraud/Internet.htm describes the Department of Justice’s Internet fraud initiative; http://www.fbi.gov/programs/ic/ifcc/ifcc.htm is the home of the FBI’s Internet Fraud Complaint Center.
of the other party – the victim – so as to foster in the victim an incorrect representation of his/her situation and therefore a desired action, one that the victim is unlikely to take without the manipulation.

Internet deception is a deception that uses the Internet as a medium to create an incorrect representation of the circumstances of a social exchange. We felt the need to use the term “Internet deception” to distance ourselves from the related concept of Internet ‘fraud,’ which is a legal definition, as well as from the concept of ‘hacking,’ which may or may not involve incorrect representations (i.e., not all hacks are deceptions).

The Internet medium affects the nature of deception because (a) it makes identity (of items of exchange, of individuals, and of organizations) easy to falsify and difficult to authenticate (Jarvenpaa & Grazioli, 1999); (b) it has lowered the economic resources needed to set-up a credible-looking storefront; (c) it has provided deceivers with an extended reach; (d) it has made the proceeds of crime easier to secure not only anonymously but also in jurisdictions where pursuing perpetrators is difficult (Morris-Cotterill, 1999). We argue that, taken together, these considerations set apart Internet deception from deceptions carried through other channels.

The specifics of Internet technology have created new forms of crime. Page-jacking, i.e., the practice of simulating a legitimate page to obtain secrets or business from an unknowing consumer, is an example of such a new form of crime that has been made possible by the Internet (FTC v. Pereira, et. al., 1999). According to the Federal Trade Commission, about two percent of the pages on the web have been targeted by this malicious practice (Berstein, 1999).

Internet technology has also altered the social, legal and economic nature of existing forms of crime. The well-publicized case of the teenager that managed to materially alter the market of several stocks for individual profit is an example of this effect (New York Times, Feb. 25, 2001). Arguably, in a face-to-face world this fraud would not have been feasible. Who would take financial advice from a fourteen-year-old boy?

The theory of deception identifies prototypical ways to perpetrate deceptions across domains of human activity. These ways have been called ‘deception tactics.’ (Johnson et al., in press). Table 1 summarizes the full set of tactics and provides examples of Internet deceptions.

One of the ways in which a deceiver may manipulate the cognitive processes of a victim is by eliminating or erasing crucial information about the item involved in a transaction so that the victim either does not think about key aspects of the manipulated item, or develops incorrect cognitive representations about it. This tactic to deceive is called masking, and the manipulated item is called the deception core. An example of masking is omitting to disclose to Internet newsletters readers (the victims) that the publisher of the newsletter (the deceiver) has received advertisement money from the companies whose stock are recommended by the newsletter. Presumably, readers that trusted the newsletter advice (the core) assumed that it was from an independent source.

Previous research (Johnson et al., 1992), has found that real-world deceptions are often composed of more than one tactic, so than one manipulation corroborates and supports the others. For instance, the example offered above combined elements of masking (failing to disclose information), and relabeling (describing questionable investments as sound).

Tactics Used by ‘Businesses’ Against Consumers

Deception theory does not cover how the tactics might distribute across types of perpetrators and victims. As a first approximation, it seems reasonable to distinguish between individuals (consumers) and businesses. This distinction produces four types of deceptions: B2B, B2C (consumer is the victim), C2B (business is the victim), and C2C. Here we limit our analysis on deceptions perpetrated by ‘businesses’ against consumers.

To understand whether tactics are used differently by different perpetrators against different victims, we need to make a few assumptions about the nature of business and individuals. Looking at business organizations and individual consumers as potential victims, we assume that in general businesses will conduct transactions according to more stringent rationality than individuals (e.g., Simon, 1976). Businesses are more likely to have in place systematic procedures for conducting and controlling business transactions (Kinney, 2001). In addition, businesses have in general greater access to third-party information about the other party in the transaction (either individuals or other businesses) than do individuals. For instance, an Internet retailer may have ready access to reliable credit rating information about a potential buyer, while a private seller on an auction site may not. By contrast, individuals may not be as rational. A survey study of Better Business Bureau officers responsible for monitoring
consumer frauds identified ‘emotional’ (vs. ‘deliberate’) decision making as one of the common characteristics of fraud victims (Langenderfer, 1998).

Comparing businesses and individuals as perpetrators of deception, we assume that malicious businesses have means of manipulating the other party’s trust and risk perception that are normally unavailable to malicious individuals (unless they impersonate a business). Grazioli and Jarvenpaa (2000) have experimentally demonstrated the dangerous effects of maliciously manipulated ‘trust mechanisms’ (e.g., size, physical presence, testimonials) as well as manipulated ‘assurance mechanisms’ (e.g., warranties, news clips, seals) on Internet consumers’ willingness to buy.

These considerations lead us to state that:

(H1) **B2C deception is the most common form of Internet deception.**

Methodologically, we assume a victim’s perspective. Therefore, since the victim believes he is transacting with a business, not with an individual masquerading as one, ‘business’ designates either an actual business or an individual posing as a business. Also note that the unit of analysis is an instance of deception between two parties. There is no reference to how many individuals or businesses are in a party.

The tactic described above, *masking,* works because it can tap into the victim’s (incorrect) expectations about a transaction, and because the victim lacks the knowledge necessary to figure out what is missing. Since we have assumed that businesses are more likely to have in place routine controls and not to develop incorrect expectations about a transaction, we hypothesize that

(H2) **Consumers are more frequently victims of masking than businesses.**

Relabeling is the second tactic described in Table 1. It consists of misdescribing the deception core. *Relabeling* works when the victim believes that the description of the object of transaction provided by the deceiver is fair. To succeed, *relabeling* requires that the victim trust the word of the deceiver at least enough to be willing to transact. Since we assume that businesses have in place more controls and checks than individuals to make sure that the terms of transactions are fair, and that businesses can more readily create fake trust and assurance mechanisms (Grazioli & Jarvenpaa, 2000), we propose that:

(H3) **Relabeling is used more frequently in B2C exchanges than in C2B, C2C, or B2B**

Inventing consists of ‘making up’ an item, or ascribing to it utterly unrealistic characteristics (see Table 1). Upon reflection, we found that in the representationally intensive Internet transactions there is not much difference between *relabeling* and *inventing.* This is because both relabeling and inventing are based on making false or misleading statements about the transaction and require a victim that is somewhat less rational (e.g., a victim conditioned by advertisement, or one that is unable or unwilling to do extensive checking of the other party’s statements). For these reasons:

(H4) **Inventing is used more frequently in B2C exchanges than in C2B, C2C, or B2B**

The next section will describe how we collected data to test these hypotheses.

**Method**

In general, gathering real-world data on deviant behaviors is difficult, since perpetrators actively attempt to hide evidence that the behavior has occurred. Deception is no exception. Traditional criminological sources do not yet cover Internet deception.

This research employs methods used by event research (e.g., Da Motta & Albuquerque, 2000; Kortum, 2000) and content analysis (e.g., Slaughter & Ang, 1996) to gather data to test the proposed hypotheses. First, we searched a broad set of sources to identify known cases of Internet deception, then we applied content analysis method to evaluate them. Limitations of this methodology will be discussed below.

Our set of sources consists of all the documents included in Abi/Inform, Lexis/Nexis, and Dow Jones Interactive, plus the materials published by official Internet sites (e.g., Securities and Exchange Commission - see Footnote 1). This coverage extends to several thousands of publications and includes the major US newspapers, practitioner press magazines, federal and state court proceedings, and academic journals.
In the summer of 2000, three paid graduate research assistants competent in MIS searched for documents containing the keywords “Internet” and either “fraud” or “deception.” These three keywords were selected by one of the authors after extensive piloting of alternatives. The assistants restricted their searches to documents published between 1995 and 2000.

201 distinct cases were identified. For each case we collected a rich set of observations according to a detailed coding scheme that is based on the theory summarized above and not included here for brevity. The coding scheme was also used to assign deception tactics to each case. The reliability of the coding was evaluated by asking a second trained coder to recode the whole set of cases and by computing a measure of interrater reliability (Cohen’s Kappa; Cohen, 1960). The value of Kappa is 0.93 (approx. p<0.000), which is comparable to the values found in similar research (e.g., Johnson et al. 1992), and is generally considered to be fully satisfactory (e.g., Fleiss 1981).

Limitations

We recognize the limitations of the proposed methodology to identify cases of Internet deception. The first limitation is shared across all forms of deviant behaviors: the victim or the monitoring authority may fail to detect the deception or be in error, i.e., they might believe that there is deception where none was attempted (“false positive” errors). Additionally, they might be unwilling to report it. 3

The second limitation applies more directly to the specific measures employed in this research, i.e., published cases of Internet deception. Inferences driven by the data presented here need to be tempered by the consideration that that the press is likely to suffer from saturation effect, i.e., that after a while, news of yet another case of Internet deception is no news anymore. The sample of sources is likely to be skewed towards U.S. events, and is limited to documents written in English.

All but one of these factors (namely, the false positive errors) is skewed towards underreporting instances of Internet deception. While we recognize these limitations, at the same time we emphasize that we do not use our data to reach conclusions about absolute numbers. Rather, we use our database to evaluate hypotheses about the distribution of tactics across types of perpetrator or victims.

A third limitation is the concern that businesses might be less willing to report instances of deception than individual consumers, thereby skewing the results of the analysis presented below. At this time, we have no evidence that businesses are less (or more) willing to report cases in which they have been victimized than consumers are. Arguments can be made in either direction. For instance, while it is plausible that businesses might be concerned about reputation more than individual consumers are (which would lead businesses to report less cases), it is also plausible that businesses prosecute deceivers more aggressively than individuals do, in order to deter other potential deceivers.

Findings

201 cases were identified and collected. Financial data about the extent of the loss suffered by the victims were available for about half of them. The median loss per case (i.e., across victims) is $30,000. The mean is much higher due to the presence of a small number of large total losses. The highest alleged loss surpasses $14 million.

The most frequent case of Internet deception (n=121; 60% of the total) occurs between a consumer and a business (or somebody impersonating a business), with the consumer as the victim. The second most frequent case is the deception perpetrated by a consumer against another consumer (n=50; 25% of the total). B2B deceptions and deceptions by individuals against companies are less frequent and represent 8% and 7% of the total respectively.

The 201 cases contained 296 instances of deception tactics, equal to about 1.5 tactics per case. Most cases (132) included only one tactic, and 13 cases had three tactics associated with them. Table 2 summarizes the results on the distribution of the tactics. Inventing (36%), relabeling (25%) and mimicking (22%) were the most often used tactics, totaling about 82% of the sample. Dazzling and double play were the least used (less than 3% of the time).

3Possible reasons for this unwillingness include fear of losing reputation and fear of showing vulnerability. Likewise, some monitoring authority might opt not to report detected instances because it might be too difficult to prove in court, or because it is outside jurisdiction, mandate, or priorities.
Chi square tests were used to evaluate the hypotheses presented in the theory section. The first test confirmed that B2C is the most common form of Internet deception (H1, p<0.000). The second hypothesis states that consumers are more frequently victims of masking than businesses. The data does not confirm that masking is used more frequently in B2C and C2C cases than in B2B and C2B cases (H2, p=0.23). Despite 25 out of 27 cases of masking are perpetrated against individuals, no strong association is left after correcting for the relative frequency of the deceptions against individuals and against organizations. Hypothesis testing concluded that relabeling and inventing are used most frequently in B2C exchanges (H3, p<0.001; H4 P<0.000).

Conclusions

This paper has explored the nature of Internet deception. It has applied an existing theory of deception to a new domain and has extended the theory by introducing the notion of comparative rationality and trust and insurance mechanisms. The extension has led to the formulation of new hypotheses on the types of deception that are most likely to victimize consumers. The hypotheses were tested using data from a database of cases of Internet deceptions, the first of its kind in the published academic literature. We found that individuals (i.e., consumers) are likely victims of deception, and that the deception tactics used against them distribute in predictable ways.

At the beginning of this paper, we stated that this research has been motivated by the concern expressed by several government agencies about Internet fraud. We have found that consumers are indeed at risk. This research helps focusing the attention and the action of the monitoring agencies toward the most effective direction. We found that the two forms of deception that target more specifically the consumers are inventing and relabeling.

The effectiveness of inventing and relabeling can be reduced by using independent sources to validate the claims of a potential deceiver. Trust and insurance mechanisms are also available, even though these mechanisms can be maliciously manipulated (Grazioli and Jarvenpaa, 2000). Educating the consumer to access independent, third party sources of information is one way to reduce the risk of falling prey of these forms of deception. Educating them on the purpose and functioning of escrow services is a second means to mitigate this risk when dealing with other individuals. Aggressive application of the regulations on misleading and deceptive advertising might help when the potential deceiver is a business. Research is needed to evaluate what works and what does not.

Since masking is detected by realizing that crucial pieces of information are missing, it is important to help the consumer to seek and heed key pieces of information. Consumer education is one means to achieve this objective. Developing industry-specific disclosure standards and monitoring compliance with these standards is another.

We certainly need more research, and we believe that IS researchers are ideally positioned to disentangle the multidisciplinary complexities of Internet deception. We need better measures of crime and criminality. We also need better means to detect deceptions, both at the level of the monitoring agencies and at the level of the individual consumer. Friedman (1998) suggested focusing on how consumers detect deceptions, so that the successful techniques can be taught to populations at risk. This is one of the directions in which our work will go next.

References

Available from the authors upon request.
Table 1. Deception Tactics

<table>
<thead>
<tr>
<th>Definition</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Masking: erasing or eliminating crucial information about the core*</td>
<td>Omitting to disclose to Internet newsletter readers (the victims) that the publisher of the newsletter (the deceiver) has received advertisement money from the companies whose stock are recommended by the newsletter (the core).</td>
</tr>
<tr>
<td>Relabeling: (mis)describing the core in such a way to elicit a desired behavior from the victim</td>
<td>An Internet company described very risky and questionable investments (core) peddled as safe and sound financial opportunities to entice investors</td>
</tr>
<tr>
<td>Inventing: “making up” information about the core. The core might simply not exist, or its characteristics might be utterly unrealistic</td>
<td>Auction sellers promised to sell merchandise (core) that they do not have or do not intend to deliver</td>
</tr>
<tr>
<td>Mimicking: assuming somebody else’s identity or to modify the core so that it copies the features of a legitimate item</td>
<td>Hackers created a ‘mirror’ bank site, virtually identical to the legitimate site. The purpose of the site was to induce bank customers to reveal secrets such as account numbers and passwords to the deceivers</td>
</tr>
<tr>
<td>Dazzling: obscuring or confusing information about the core without eliminating it.</td>
<td>A well-known internet services provider made &quot;free trial” offers (core) to consumers but did not make clear that consumers had an affirmative obligation to cancel the service before the trial period ended. As a result, consumers who failed to cancel were enrolled automatically and began incurring monthly charges. In this case the key information was available, but buried in the fine print.</td>
</tr>
<tr>
<td>Decoying: distracting the victim’s attention away from what is really going on, i.e., from the real nature of the transaction.</td>
<td>An Internet company offered “free stock” to the public. Victims had to register themselves as stockholders with the company, which entailed revealing detailed personal information (the core). The database of that very detailed and presumably highly accurate personal information was what the deceivers were really after.</td>
</tr>
<tr>
<td>Double play: convincing the victim that he/she is taking an unfair advantage on the deceiver, or that the transaction occurs in part against the deceiver’s interest</td>
<td>E-mails designed to look like misdirected memos from well-known investment firms were sent to thousands of potential victims. These messages contained false insider information, maliciously fabricated to induce the recipient to invest in a certain stock.</td>
</tr>
</tbody>
</table>

*The core is the item or items that are involved in the deceptive transaction.

Table 2. Victims, Perpetrators, and Deception Tactics

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventing</td>
<td>6</td>
<td>62</td>
<td>39</td>
<td></td>
<td>107</td>
</tr>
<tr>
<td>Relabeling</td>
<td>3</td>
<td>62</td>
<td>8</td>
<td></td>
<td>73</td>
</tr>
<tr>
<td>Mimicking</td>
<td>11</td>
<td>15</td>
<td>30</td>
<td>9</td>
<td>65</td>
</tr>
<tr>
<td>Masking</td>
<td>2</td>
<td>24</td>
<td>1</td>
<td></td>
<td>27</td>
</tr>
<tr>
<td>Decoying</td>
<td>1</td>
<td>1</td>
<td>12</td>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>Dazzling</td>
<td>3</td>
<td></td>
<td>4</td>
<td>-</td>
<td>7</td>
</tr>
<tr>
<td>Double Play</td>
<td>0</td>
<td></td>
<td>1</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>26</td>
<td>16</td>
<td>195</td>
<td>59</td>
<td>296</td>
</tr>
</tbody>
</table>