Deception in Electronic Goods and Services

Neil C. Rowe
U.S. Naval Postgraduate School, USA

INTRODUCTION

Deception is a frequent but under appreciated aspect of human society (Eckman, 2001). Deception in electronic goods and services is facilitated by the difficulty of verifying details in the limited information available in cyberspace (Mintz, 2002). Fear of being deceived (often unjustified) is in fact a major obstacle to wider use of e-commerce and e-government by the public. One survey reported consumers thought fraud on the Internet was 12 times more common than offline fraud, and 3 out of 5 people thought their credit card number could be stolen in most online transactions (Allen, 2001); both are over-estimates. We assess here the nature of the deception threat, how deception can be detected, and what can be done about it.

BACKGROUND

Deception is common in many areas of human endeavor (Ford, 1996). Deception is in fact essential to the normal operation of business, law, government, and entertainment as a way to manipulate people (Nyberg, 1993). But there is a complex boundary between acceptable deception and unacceptable or illegal deception.

Deception can occur with either the purveyor (offeror) of goods or services or with the customer (buyer), and it strongly affects trust in a transaction (Friedman, Kahn, & Howe, 2000). Some examples in online activities include:

- A customer provides a fake credit card number for a transaction.
- A Web site takes a customer's money but never provides a promised good or service.
- A Web site solicits a customer's e-mail address for spamming them but claims it is for potential "problems with your order".
- A Web site incorrectly says they can legally sell you a drug without a doctor's prescription.
- A customer with a grudge posts false health reports about a product on a Web bulletin board.

Usually the motivation for deception in goods and services is financial gain, but other reasons include revenge and self-glorification.

Unfortunately, the rather anonymous nature of cyberspace encourages deception. One problem is that the communications bandwidth, or amount of information that can be transmitted between people, is considerably less than in face-to-face human interactions, even with videocameras. Studies indicate that people are more deceptive the smaller the bandwidth (Burgoon, Stoner, Bonito, & Dunbar, 2003); for instance, people are more deceptive on the telephone than in videoconferencing. The detection of deception in online interactions is made difficult by the absence of many useful visual and aural clues; careful studies of consumer behavior have confirmed this difficulty (Grazioli & Jarvenpaa, 2000). This raises problems for electronic commerce and government.

DECEPTION METHODS AND COUNTERMEASURES

Categories of Deception in Electronic Goods and Services

We can distinguish five major categories of deception in online transactions: Puffery or overstated claims, insincerity of promises or claims, trespassing, masquerading, and fraud (Grazioli & Jarvenpaa, 2003). Most instances happen with the World Wide Web, with some occurring in e-mail and other uses of the Internet.

Puffery includes mostly advertising since it rarely accurately summarizes the merits of a product or service. Deceptive advertising is encouraged by the nature of online interaction: It is hard for a customer to know with whom they are dealing. An impressive Web site is no guarantee of a reliable business, unlike an impressive real-world store or shop. Furthermore, the customer cannot hold and touch the merchandise, and the images, audio, or video provided of it are typically limited. So it is tempting for an online purveyor to make unsupportable claims. Puffery also includes indirect methods such as a Web site for a children's television show that is designed to sell a particular toy, or people who endorse products in online discussion groups without revealing they work for the purveyor ("shilling").

Insincerity has many forms online. Many Web search engines list pages they have been paid to display but that are not the best matches to the given keywords. A purveyor can promise "extras" to a sale they have no intention of delivering, or a customer can promise large future purchases. Emotions can also be faked, even love (Cornwell & Lundgren, 2001). False excuses like "being busy" are easy to make on the Internet. Negative puffery, where a customer or other business says bad things about a product or service (Floridi, 1996), as for revenge or to manipulate stock prices, are another form of insincerity. And "Remove me from the mailing list" links can actually be scams to get your name onto a mailing list.

Trespassing is breaking into computer systems to steal its time, memory, or other resources, and is usually by deception. It is commonly associated with "hackers", people breaking in for fun, but is increasingly practiced by spyware, and by criminals to obtain staging sites for attacks on other computers (Bosworth & Kabay, 2002; Chirillo, 2002).

Masquerarding or "identity deception" is pretending to be someone that one is not. There are many forms online:

- Customers can steal passwords or identification numbers, then use them to steal goods and services.
- Purveyors can also pretend to be a different entity than they really are. This is facilitated by the lack of regulation of Web sites and their claims, and by the ability to give false return addresses in e-mail and false link text on Web sites.
- A serious problem of this type is "phishing", inviting or threatening people to induce them to visit a decoy Web site where they are asked to supply personal data such as credit card numbers and bank-account numbers for subsequent theft. An example enticement is to claim to be the government tax office needing information about a tax return.
- Counterfeit Web sites try to mimic familiar Web sites to steal from customers. Classic tricks are names confusable with those of well-known sites, like "googl.com" instead of "google.com", or numbers in the address instead of letters to prevent recognition.
- Both deceptive Web sites and deceptive e-mail can steal professional-looking graphics and fonts from legitimate sites and e-mail to look more convincing.
- A site may even "hijack" business from another by using the same Internet (IP) address, but this will only work for a short time before it is discovered and stopped.
- Data, such as credit card numbers could possibly be stolen from packets traversing the Internet, but this is becoming very difficult as many commercial sites now encrypt such sensitive data.
- Fake online documents are hard to detect, since most clues to forgeries like handwriting style and provenance are not available, but style inconsistencies can still help (Kaza, Murthy, & Hu, 2003).

The most serious electronic deceptions in goods and services are crimes of fraud (Boni & Kovachich, 1999; Loader & Thomas, 2000). McEvoy, Albro, and McCracken (2001) and Fraudwatch (2005) survey specific popular techniques. Unscrupulous Web purveyors can collect money without providing a promised good or service since it is easy to appear and disappear on the Web; fake charities are a notorious example. Purveyors may not feel much consumer pressure because it is hard for customers to complain about long-distance transactions. The Internet is well suited to many classic scams, notably the many forms of the "Nigerian letter" asking for money in the promise of receiving much more money in the future. Electronic voting is a special concern for fraud (Kofler, Krimmer, & Prosser, 2003).

The Ethics and Legality of Deception

Online transactions benefit from the trust of the participants. Deception subverts trust and makes online businesses less efficient because of the subsequent need to check credentials and promises. Because of similar costs to society in general, ethical theories usually claim that most forms of deception are unethical (Bok, 1999), and laws in every society identify some forms of deception as fraud legally. American law uses the doctrine of "implied merchantability" to say that a contracted good or service must be provided adequately or the money must be refunded. Waivers of responsibility that consumers must approve before proceeding on a Web site do not have much weight in court because consumers rarely can be said to give informed consent. But there are many other issues; see the many Internet-related publications of the U.S. Federal Trade Commission (FTC, 2005).

Detecting Deception in Goods and Services

Studies have shown that most people are poor at detecting deception (Ford, 1996). Thus in cyberspace with its limited bandwidth, deception is even more of a problem. Most training of people (such as law-enforcement personnel) to recognize deception in human interactions focuses on clues that are absent in cyberspace such as the visual ones of increased pupil dilation, blinking, and self-grooming, and vocal clues such as higher voice pitch, more frequent speech errors, and hesitation. However, some traditional clues to deception do apply to cyberspace (Zhou & Zhang, 2004), including: