

Chapter 1.9

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 overestimates. 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).

Masquerading 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.

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/deception-electronic-goods-services/9455

Related Content

The Dynamic Impacting Study of Competitive Strategies to Import Retail E-Commerce Sellers

Xuanxuan Zhang (2018). *Journal of Electronic Commerce in Organizations* (pp. 53-66).

www.irma-international.org/article/the-dynamic-impacting-study-of-competitive-strategies-to-import-retail-e-commerce-sellers/214001

Teaching And Learning Of E-Commerce Courses Via Hybrid E-Learning Model In Unitar

Mohd. Taha Ijab, Rina Anwarand Suraya Hamid (2004). *Journal of Electronic Commerce in Organizations* (pp. 78-94).

www.irma-international.org/article/teaching-learning-commerce-courses-via/3431

An Advanced Watermarking Application for the Copyright Protection and Management of Digital Images of Cultural Heritage Case Study: "Ulysses"

Georgios Stiliosand Dimitrios K. Tsolis (2009). *Digital Rights Management for E-Commerce Systems* (pp. 263-279).

www.irma-international.org/chapter/advanced-watermarking-application-copyright-protection/8503

International Lessons and Adaptations Examining Global CBDC Implementations and Extracting Insights for India's Digital Rupee

Amit Kumarand Vinit Sikka (2024). *Exploring Central Bank Digital Currencies: Concepts, Frameworks, Models, and Challenges* (pp. 224-244).

www.irma-international.org/chapter/international-lessons-and-adaptations-examining-global-cbdc-implementations-and-extracting-insights-for-indias-digital-rupee/341672

The Moderating Roles of Income and Age in Mobile Commerce Application

Uchenna Cyril Ezeand Yew Siang Poong (2013). *Journal of Electronic Commerce in Organizations* (pp. 46-67).

www.irma-international.org/article/the-moderating-roles-of-income-and-age-in-mobile-commerce-application/84046