2005

Types of Online Deception

Rowe, Neil C.

Monterey, California. Naval Postgraduate School

This article appeared in the Encyclopedia of Virtual Communities and Technologies, Hershey, PA: Idea Group, 2005.
http://hdl.handle.net/10945/36833

Types of Online Deception

Neil C. Rowe

U.S. Naval Postgraduate School
Code CS/Rp, 833 Dyer Road, Monterey, California 93943 USA
ncrowe@nps.edu

ABSTRACT

Deception in virtual communities can be a serious issue. We present three approaches to characterizing online deception: by the appearance, by the motivation, and by the mechanism. Appearances include identity deception, mimicking, lying (by insincere statements, false excuses, or false promises), and fraud. Motivations can be both aggressive and defensive. Mechanisms are analyzed using concepts from case grammar in linguistics. Fundamentally new forms of deception not in these taxonomies are unlikely in virtual communities.

This article appeared in the *Encyclopedia of Virtual Communities and Technologies*, Hershey, PA: Idea Group, 2005.

INTRODUCTION

Like all societies, online communities can be victimized by deception by their members. It is helpful to identify the forms in which deception can occur ("taxonomies") to better prepare responses. While deception can often be ignored in informal interaction, it is more serious when online communities, subgroups, or pairs of members attempt to accomplish tasks together.

BACKGROUND

Online deception can occur in many ways. Many of these are "lies", false statements intended to gain some advantage to the liar (Bok, 1978), but deception includes indirect methods too. Common forms of deception in virtual communities are (Grazioli & Jarvenpaa, 2003):

- Identity deception, pretending to be a different person or kind of person than one really is (Donath, 1998). This is intrinsic to online fantasy worlds but occurs not infrequently in other interactions, as when participants in a discussion group pretend to a different gender, background, or personality than their true one (Cornwell & Lundgren, 2001). It can also occur in failure to reveal a critical bias, as when an employee of a company endorses their company's product in a discussion group without revealing their employment ("shilling"). The frequent lack of aural and visual clues in cyberspace particularly facilitates identity deception.
- Mimicking of data and processes. Examples are fake Web pages intended to steal credit-card numbers, fake bills for services not rendered, and hijacking of sites and connections. Such events are increasingly common.
- Insincere responses to other people, including posturing and exaggeration of responses. This can include

substitution of a different emotional response for the one actually felt (Ford, 1996), or "trolling" by deliberately seeming stupid to provoke people (Donath, 1998). Insincerity is also facilitated by the lack of visual and aural feedback.

- False excuses. Alleged reasons for not doing something (Snyder, Higgins, & Stucky, 1983) are common online because they are often hard to confirm.
- False promises. False advertising is an example, where limited ability to view and feel a product online permits inflated claims by the seller. In news groups due to the sporadic appearance of members of a virtual community, there may not be as much social pressure to fulfill commitments as in the real world. This can lead to strange phenomena such as fake virtual suicide (Brundage, 2001).
- Coordinated ?disinformation? campaigns to convince people of something false (Floridi, 1996).
- Other forms of fraud, attempts to fool people to achieve criminal ends (McEvoy, Albro, & McCracken, 2001; Mitnick, 2002), either directly (like fake investments or fake charities) or indirectly (like stealing credit-card numbers or sending email with implanted viruses).

MOTIVATION FOR DECEPTION

Another way to classify deception is by its motivation. (Ford, 1996) and (Eckman, 1991) enumerate reasons for lying, most of which apply to nonverbal deception as well.

- Lies to avoid punishment, as when a member of a virtual community violates its rules about secrecy and denies it.
- Lies as an act of aggression, as when a member lies to someone by whom they have been hurt.
- Lies to create a sense of power, as when a member lies to provoke a reaction from another.
- Lies as wish fulfillment, as when a member lies about their job or sex.
- Lies to assist self-deception, as when a member lies about the state of their marriage to justify an extramarital affair to themselves.
- Lies to help someone, as when a member feigns interest in a subject important to a friend.
- Lies to assist another's self-deception, as when a member lies to approve of lies by a friend.
- Lies to resolve role conflict, as when a member pretends to enjoy an exercise to impress other members.
- Lies for enjoyment, as when a member enjoys tricking a new member.

MECHANISMS OF ONLINE DECEPTION

Deception can be classified with respect to mechanism used. (Whaley, 1992) proposes a six-part taxonomy with "masking", "repackaging", and "dazzling" as forms of "hiding the real", and "mimicking", "inventing", and "decoying" as forms of "showing the false". (Grazioli & Jarvenpaa, 2003) suggests for online deception the categories of "masking", "dazzling", "decoying", "mimicking", "inventing", "relabeling", and "double playing", and gives statistics of their online use. (Rowe & Rothstein, 2004) proposes a comprehensive taxonomy based on case grammars for linguistics, or ways to categorize how events can have associated concepts:

- deception involving the participants
    - agent (the person who initiates the action), as when a person pretends to be someone else (easy to do online);
    - beneficiary (the person who benefits), as when someone lies that they to do something for another person;

    - experiences (a psychological feature associated with the action), as when someone pretends to be angry (easy to do online);
    - instrument (some thing that helps accomplish the action), as when someone lies about the method they used to reach a Web site;
    - object (what the action is done to), as when someone lies about fixing a bug;
    - recipient (the person who receives the action), as when someone lies about whose approval they obtained.
- deception in space (rarely relevant in cyberspace because 'locations" are abstract)
- deception in time (rarely relevant in cyberspace because of automatic timestamping of messages)
- deception in causality
    - cause, as when someone lies about their system crashing to excuse their absence, or lies about why they joined a newsgroup (easy to do online)
    - contradiction (what this action contradicts if anything), as when someone claims installing certain software will protect your system and it actually makes it more vulnerable
    - effect, as when an email attachment installs a virus (hard to do online because of available confirmation)
    - purpose, as when someone lies about why they want you to open a file
    - precondition, as when someone lies that they cannot download your file (easy to do online)
- deception in quality
    - accompaniment, as when someone sends an email with an attachment containing a virus
    - content, like an email containing a picture instead of text as stated (easy to do online)
    - manner, as when someone dumps email into a directory rather than forwarding it as stated
    - material, as when someone sends a file in Spanish rather than English as stated
    - measure, as when someone labels a ten-page message as a "short message"
    - order (not applicable online because action sequences can be changed by the system)
    - value (not applicable online because distortion cannot occur in transmission of messages)
- deception in essence
    - supertype, as when someone sends a useful program that deliberately damages your computer system
    - whole, as when a useful free program primarily is intended to spy on the user's activities

Besides these general mechanisms, there are additional opportunities for deception in particular virtual communities. (Mintz, 2002) surveys common deceptions on the World Wide Web, including misleading Web sites and Web scams like the many forms of the "Nigerian letter" soliciting money for bogus enterprises. (Mitnick, 2002) provides a good survey of "social engineering" deceptions aimed at stealing information and money from computers by manipulating the people that use them. (Cohen, 1999) provide a general taxonomy of malicious deceptions used to attack computer systems themselves.

FUTURE TRENDS

As a broader range of society is represented in virtual communities, deception will become more prevalent. New deception methods are unlikely to appear ? plenty of good scams from millenia of deception have already been conceived. But many old scams and ploys will appear in new disguises in cyberspace.

CONCLUSION

Many forms of deception are possible in virtual communities, due to the difficulties of confirming

information about the participants (although certain details, like when someone has been present, are easier to confirm for online activity). It is important for all members of virtual communities to be aware of the major kinds of deception as a first step toward combatting it. With such awareness, countermeasures can be developed such as requiring additional authentication and confirmation before taking actions.

REFERENCES

Bok, S. (1978). *Lying: moral choice in public and private life*. New York: Pantheon.
Brundage, S. (2001, February). Playing with death. *Computer Gaming World*, 29-31.
Cohen, F. (1999). Simulating cyber attacks, defenses, and consequences. Retrieved May 16, 1999 from all.net/journal/ntb/simulate/simulate.html.
Cornwell, B., & Lundgren, D. (2001). Love on the Internet: Involvement and misrepresentation in romantic relationships in cyberspace versus realspace. *Computers in Human Behavior, 17,* 197-211.
Donath, J. (1998). Identity and deception in the virtual community. In Kollock, P., & Smith, M. (Eds.*), Communities in Cyberspace.* London: Routledge.
Eckman, P. (2001). *Telling lies: clues to deceit in the marketplace, politics, and marriage*. New York: Norton.
Floridi, L. (1996). Brave.net.world: the Internet as a disinformation superhighway? *The Electronic Library, 14,* 509-514.
Ford, C. (1996). *Lies! Lies!! Lies!!! The psychology of deceit*. Washington, DC: American Psychiatric Press.
Grazioli, S., & Jarvenpaa, S. (2003, December). Deceived: under target online. *Communications of the ACM, 46* (12), 196-205.
McEvoy, A., Albro, E., & McCracken, H. (2001, May). Dot cons -- auction scams, dangerous downloads, investment and credit-card hoaxes. *PC World, 19* (5), 107-116.
Mitnick, K. (2002). *The art of deception*. New York: Cyber Age Books.
Mintz, A. P. (ed.) (2002). *Web of deception: misinformation on the Internet*, CyberAge Books, New York.
Rowe, N., & Rothstein, H. (2004, July). Two taxonomies of deception for attacks on information systems. *Journal of Information Warfare, 3* (2), 27-39.
Snyder, C. R., Higgins, R. L., and Stucky, R. J. (1983). *Excuses: masquerades in search of grace*. New York: Wiley.
Whaley, B. (1982, March). Towards a general theory of deception. *Journal of Strategic Studies, 5* (1), 179-193.

TERMS

case grammar: A linguistic theory of the ways in which an action can be associated with other concepts.
deception: Conveying or implying false information to other people.
disinformation: False information repeatedly provided in a coordinated campaign.
excuses: Reasons for not doing something.
identity deception: Pretending to be someone or some category of person that one is not.
lies: False statements known by the utterer to be false.
shilling: Making claims (pro or con) for something without revealing that you have a financial stake in it.
social engineering: Using deception to steal information like passwords from people.
trolling: Acting in a deliberately inflammatory way to provoke a response online, usually in a newsgroup and usually with insincerity.

ACKNOWLEDGEMENT

This work was supported by the National Science Foundation under the Cyber Trust program.