WEBSITE CREDIBILITY
A Proposal on an Evaluation Method for e-Commerce

Katsuya Watanabe, Masaya Ando and Noboru Sonehara
National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, Japan

Keywords: Information credibility, website credibility, web trust.

Abstract: This paper introduces a research for clarifying the structure of the website credibility. The users with low information literacy cannot have difficulty making use of e-Commerce services because they cannot judge the credibility of websites appropriately. Conventional approaches to evaluate the credibility of a website have been based on aspects like the design of the website or the usage of information security technologies. However, it is not sufficient for users with low information literacy to distinguish ill-intentioned sites based on the site design and security technologies alone. In this paper we examine a more comprehensive analysis and evaluation method which is based not only on evidence internal to the site, but also on third-party information about the site provider.

1 INTRODUCTION

Access to and use of the Internet has spread widely and swiftly in a decade. Especially, Consumer Generated Media (CGM) services such as Weblog and Social Networking Service (SNS) have been getting more familiar to general internet users. As users send messages actively on the web, the number of cybercrimes such as a phishing has increased. Information security services and technologies like WebTrust for CA (Certification Authority) are provided to take measures against it. However all users don’t necessarily know the meaning of these information security services and technologies (Dhamija et al., 2006). Therefore "information credibility study" became the main controversial themes in the field of Human –Computer Interaction.

The first study on the credibility of web sites was done by Fogg et al. (Fogg et al., 2001a; 2001b; 2002; 2003). Through questionnaires and experiments, they showed that the factors that effected a user's evaluation of the credibility of a site most strongly were the design and the information provided. The authors have also adopted an approach similar to Fogg et al., deriving a method which evaluates website credibility from elements including design and information provided (Watanabe et al., 2007).

However, evaluating based only on design and content is not able to identify ill-intentioned sites posing as trustworthy sites, such as phishing sites.

This research focuses on the verifiability of the information used to evaluate trustworthiness, and studies ways of evaluating the trustworthiness of a website more accurately by using third-party information about the site information provider.

2 USER BEHAVIORS IN EVALUATING CREDIBILITY

The authors studied specific credibility evaluation models used on e-Commerce (EC) and Non-Profit Organization (NPO) websites, based on questionnaires and the results of experiments using real subjects (Watanabe et al., 2007). We observed the behaviour of subjects when evaluating credibility and explain it in terms of a three-step process.

1) Check consistency with the basic message pattern

First the website is examined and evaluated as to whether the basic information that one would naturally assume to be provided (the "basic message pattern") is actually present in an appropriate form. If there is inconsistency with the pattern the credibility evaluation drops considerably.

Watanabe K., Ando M. and Sonehara N. (2008).
WEBSITE CREDIBILITY - A Proposal on an Evaluation Method for e-Commerce.
In *Proceedings of the International Conference on e-Business*, pages 484-487
DOI: 10.5220/0001913104840487

2) Evaluate production elements

In addition to the basic message, elements of the website such as the design, usability and detailed information are evaluated. If the elements are appropriate for the website, the site is deemed more trustworthy, but if there are inadequacies, the evaluation suffers.

3) Check information reliability from outside the website

The evaluation in 1) and 2) is based on information found in the site itself. Users also look-for and check third-party information outside of the site in question to confirm and complement this evaluation. External information tends to be consulted especially if the evaluation in 1) and 2) is not particularly good, but all users do not always perform this step.

Of the three steps above, the authors have derived an evaluation model corresponding to 1) and 2) earlier, but did not consider the process of checking external indicators as in 3). The research due to Fogg et al. also did not consider the factors in step 3).

The information on a website consists of the site's own statements about itself, so actually, a verifiably correct evaluation based only on this information is not possible. In real society, we also do not evaluate credibility based on a person's own statements about themselves, but generally seek third-party information to verify it.

However, in the experiments we have conducted so far, there are in fact very few users that actually use external information to check the credibility of a website.

3 CREDIBILITY EVALUATION FRAMEWORK

It is difficult to identify ill-intentioned websites, such as phishing sites, when evaluating the credibility of the site based only on clues in the site itself.

In experiments in which subjects were shown a website and asked to determine whether it was a phishing site (Dhamija et al., 2006), 23% of the subjects only looked at the site content, and did not check other factors like the contents of the address bar or whether the SSL-lock icon was displayed. Most of the subjects did not understand the meaning of the SSL warning messages, and they reported that, indeed, elaborate phishing sites with well designed logos and icons were able to fool 90% of the subjects.

In other words, there are limitations to users' ability to recognize phishing sites, and those with a design that simply looks trustworthy may often be successful.

The experiments also showed that no matter how much the content of the site is analyzed, it will not be possible to accurately evaluate the reliability of the site.

The goal of our research is not to identify phishing sites, but to more-accurately evaluate the credibility of websites, and study schemes to support the users' ability to make this judgment. In particular, we expect to be able to support users with particularly low Internet literacy in this way.

Towards this goal, the authors considered the following three approaches to determining the credibility of a website.

1) Evaluate clues internal to the website

This is also done by Watanabe et al. (2007). The first thing the user sees is the website itself, so evaluating it is essential to evaluating the credibility of the site.

2) Evaluation of the information provider based on third-party information

Examining the details of information provided on third-party websites referencing the site in question should be helpful in evaluating the credibility of the site. As mentioned earlier, however, the number of users checking third-party information is not particularly high.

As such, it should be helpful, particularly for users with low information literacy, if the system can perform this type of evaluation and display the results to the user on a regular basis.

3) Evaluation based on hyperlink structures

Phishing sites often use the names of reliable information providers while carrying on fraudulent behavior, so it is difficult to correctly evaluate credibility based on name alone.

According to a survey by the Anti-Phishing Working Group (APWG) in the USA, the average amount of time a phishing site exists is very short; about four days (APWG, 2007), so it is not likely that there will be any links from other sites to the site. It may be possible to evaluate the credibility of a site by analyzing the structure of hyperlinks to the site.

As mentioned in the definitions earlier, credibility is something that the user him/herself must decide. There is a need to support better decision making about credibility, and evaluating websites based on the above three points and having the result displayed for the user should help even low-information-literacy users make appropriate decisions about the credibility of websites.

In this paper, we discuss evaluation based on third-party information about the information provider in particular detail.

4 WAYS TO EVALUATE CREDIBILITY OF THE INFORMATION PROVIDER

User reviews have become a widely-used approach to evaluating the credibility of websites using third-party information. Some EC websites incorporate comments and ratings from users that have already made purchases through the site. Displaying evaluations from existing customers is an indirect way of expressing the credibility of the product or site operator itself, but there are still the problems of whether the provider of the comment or the comment itself is actually reliable.

As an example, one could search the web for the name of the business in order to gather third-party information about the operator of an EC website, but it is still difficult to determine which of the results are reliable.

So, the authors focused on any public activities of the business or organization acting as the information provider. In other words, we looked at references to the name of the organization in information published on the websites of organizations that are more public in nature.

4.1 Validity of the Evaluation Method

For this study, we targeted businesses operating e-Commerce (EC) websites. EC sites will have been legally required to register or apply for various permits and licenses, file reports, and have a history of affiliation with public institutions and business associations. Businesses working with public institutions are also often required to go through an investigation process. At minimum, insubstantial companies and organizations are not likely to be able to work with public institutions. Much of this sort of public activity is recorded on the websites of public institutions such as governments, municipalities and other administrative organizations.

Other information like certification levels (ISO9000, ISO14000, Privacy Certification, etc.) can also be used. These are systems for certifying organizational activities, so they can also be a source of information to verify the credibility of the information provider.

4.2 Preliminary Research

EC sites are not necessarily operated by major companies, and in fact, many are operated by small and medium-sized businesses. Because of this, there is some doubt about whether a given company's name will be referenced on government or municipal websites, so we performed a survey using a sample of real companies.

4.2.1 Method

We first selected an arbitrary 246 Japanese EC websites, being sure to also include sites that are less well-known.

We then used a search engine (Google), searching for the company's official name to examine the amount of information available on government sites (go.jp domain), regional municipality sites (le.jp, pref.*.jp, etc.), and websites of public organizations (or.jp).

Then we looked at up to 100 results more closely, and classified them according to type of reference.

Note that domain names in these domains can only be obtained by organizations of certain types, and organizations must provide documentation that they qualify for the domain name.

4.2.2 Results

This investigation is still in progress, so the results below represent only a partial survey.

Overall, 226 of the 246 companies (91.9%) were referenced on other websites with public domain names, which is relatively high (see Table 1).

Table 1: Rate of reference in public domain sites.

Domain	go.jp	or.jp	lg.jp	pref. jp
Rate of appearance (%)	76.4	89.4	46.7	67.5
Avg. no. of references	598.3	372.3	18.4	73.9

(N=246)

The content of the references were classified into the 15 categories below (Table 2).

As can be seen from this classification, even in references in websites with public domains there are items related to credibility and others that are not. If the evaluation can be done in consideration of this type of difference in the references it should be possible to further improve the accuracy.

Table 2: Avg. number of appearances per company.

Type	Number	Type	Number
Permit	0.57	Organization introduction	20.20
Registration	4.21	Committee	11.32
Certification/ Authorization	3.92	Financial Reporting	2.67
Commendation/ Award	2.59	Bankruptcy/ Litigation	0.25
Member of a public agency	4.70	Recalls, etc.	3.81
Bidding/Contracts	5.74	others	6.11
Delivery/ Provisioning	1.09	outside object	22.76
Participation in public activities	14.60		

(N=246)

4.2.3 Challenges

This method also has limitations. One limitation is that the name of the organization may not necessarily be unique in Japan, and it may be difficult to distinguish between organizations in these cases. In this study, we were able to reduce the amount of this sort of confusion by using the official name of the organization, but it will be necessary to study more-accurate and effective ways to resolve this difficulty.

5 DISCUSSION

In this paper we have proposed a method for evaluating the credibility of websites that uses third-party information to verify the credibility of the site's information provider in addition to the site design and the information provided on the website itself.

As discussed in the definitions section, credibility is something that users must decide for themselves, but as shown in this paper, we believe that gathering appropriate third-party information can help users make this sort of determination more accurately.

More specifically, the user's evaluation of the credibility of a website can be verified using third-party information. If the evaluation is correct, the user's confidence can be raised by the amount and quality of the information from third-party sources. In other words, if there is very little information available from third-party sites, there is more risk regarding whether the user's evaluation is correct or not.

From this perspective, integrating third-party information provides another indicator to support decisions about credibility for low-information-literacy users.

6 FUTURE WORK

In the future, we plan to develop a system which implements the three approaches described here and to evaluate the effectiveness of the methods.

REFERENCES

Fogg, B. J., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., Paul, J., Rangnekar, A., Shon, J., Swani, P., Treinen, M. (2001) *What makes Web sites credible?: a report on a large quantitative study*, Proceedings of the SIGCHI conference on Human factors in computing systems, pp 61-68.

Fogg, B. J., Kameda, T., Boyd, J., Marshall, J., Sethi, R., Sockol, M., Trowbridge, T. (2002) *Stanford-Makovsky Web Credibility Study 2002: Investigating what makes Web sites credible today*, A Research Report by the Stanford Persuasive Technology Lab & Makovsky & Company. Stanford University.

Watanabe, K., Hara, Y., Hasegawa, A. and Sonehara , N. (2007) *Evaluation model of Web page credibility*, Proceedings of the First Workshop on Information Credibility on the Web (WICOW), pp49-56.

Dhamija, R., Tygar, J. D. and Hearst, M. (2006) *Why phishing works*, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM Press, New York, NY, USA, pp581-590.

Anti-Phishing Working Group (2007) *Phishing Activity Trends: Report for the Month of February, 2007*, Available at www.antiphishing.org