Trusting the Internet:
Cues Affecting Perceived Credibility

Michael S. Wogalter, North Carolina State University, USA

Christopher B. Mayhorn, North Carolina State University, USA

ABSTRACT

Positive beliefs about the validity and reliability of website information are important for users and the success of a site. Users may use these beliefs in making judgments about the veracity of the informational content that they encounter on the Internet. This research examined several components associated with Web sites that could affect credibility beliefs about Web site information: domain suffixes (e.g., .com, .edu), quality seals, and organizations/domain names. Two studies were carried out involving a total of 433 participants. One had 247 participants (171 undergraduates and 76 non-student adults) and the other had 186 participants (89 undergraduates and 97 non-students). Results indicated that participants who reported spending greater time on the Internet showed significantly higher trust ratings on several components than those who reported spending less time on the Internet. Participants had difficulty discriminating between actual and fictitious quality seals and organization/domain names, with several fictitious ones judged as or more trustworthy than actual ones.

Keywords: *beliefs; credibility; computer security; distrust; domain names; domain suffixes; fraud; internet; quality seals; trust; Web site; World Wide Web (WWW)*

INTRODUCTION

A growing number of people around the world are using the rapidly-expanding Internet (WWW) to research various topics, purchase goods, and conduct other activities (U.S. Department of Commerce, 2002). Unfortunately, the quality of and validity of information on the Internet is highly variable. Web sites vary in their accuracy, comprehensiveness, and currency of content (Corritore, Kracher, & Wiedenbeck, 2003). For this reason, trust involving information on the Internet is an important issue as the Internet becomes an increasing part of people's lives.

Research on trust stems from a variety of academic disciplines such as philosophy, psychology, economics, and management information systems. Therefore, it is not surprising that "trust" is a topic of considerable discussion with no universally accepted scholarly definition (Grabner-Kraeuther, 2002; Rousseau, Sitkin, Burt, & Camerer, 1998). Some treat trust as static, and some posit more dynamic development over time (Gallivan & Depledge, 2003; Gefen, 2000).

It has been argued that online trust is qualitatively different from the trust developed through continuous face-to-face interactions,

because in the latter, there is an opportunity for repeated interactions and bidirectionality (Rousseau et al., 1998). During the initial phase of trust formation, informational exchange can be hindered by information asymmetry (Ba & Pavlou, 2002) due to incomplete or distorted information provided on the Internet. Indeed, authors of Web site information can be just about anyone, and they can put just about anything online (although there may be some exceptions such as child pornography, and governmental and industrial secrets) without any apparent risk to themselves. Indeed, it is unclear whether it is possible to regulate what can be placed on the Web, which means information quality can never be assured. Anyone with a registered domain name and minimal Web development skills can post a Web site, and the information posted on the site may not all be true (Alexander & Tate, 1999). Unlike peer-reviewed, refereed journal articles and other verified materials involving high standards of the journalism profession or other ethical report-writing disciplines, a substantial portion of the "facts" on the Web may never have been reviewed, edited, or checked for accuracy (Johnson & Kaye, 1998), or if done so at one time, may not be updated to maintain accuracy. Because many reputable organizations post information to the Web, a substantial amount of Web material is likely to be reasonably accurate, but the point here is that some may contain errors. While some of the false information may be simply unintentional due to bad writing or poor editing, other information on the Web may be purposely conceived to be inaccurate, biased, or misleading (Flanagin & Metzger, 2000). Such malicious uses of Web publishing may pose a serious security threat because it potentially exposes Internet users to security risks such as online privacy violations and identity theft schemes designed to exploit them (Miyazaki & Fernandez, 2001; Schultz, Proctor, Lien, & Salvendy, 2001).

Recent evidence suggests that Internet users may fall prey to such security risks because they often fail to verify the quality of the information that they have encountered online (Metzger, Flanagin, & Zwarum, 2003). In these instances, users of search engines may "find" information, but the pages brought forth as a result of the search should probably not be considered to be errorless. In some cases, the Web sites appearing in the search may impart inaccurate knowledge to readers without them realizing that the information is untrue, that is, not knowing that they have been deceived. This is the crux of the potential problem.

To illustrate this case-in-point, e-commerce has developed faster than the means of protecting consumers from exploitive entities. Recent estimates indicate that e-commerce sales surpassed $108 billion during 2006 and increased almost 6% from the previous year (U.S. Department of Commerce, 2006). Clearly, people are increasingly using information on the Internet in their purchasing decisions. However, news stories about virus "infected" computers, fraudulent Web sites, and so forth may effect people's beliefs about the medium's trustworthiness. For example, "phishing" schemes in which a realistic looking, but fraudulent, request is made of personal, usually financially-related, information is widespread (Dhamija, Tygar, & Hearst, 2006). As a result of the risk involved in using the Internet, Web designers and security experts are actively working to institute design guidelines to promote trust and information credibility on the Web in an effort to make reputable sites discriminable from bogus ones (Andreou, Kanellis, Martakos, & Papadopoulou, 2001; Nielsen, Molich, Snyder, & Farrell, 2000).

Online trust can be conceptualized from previous, cross-disciplinary literature on trust (Rousseau, et al., 1998). One connecting point concerns the development of system trust by users when they interact with Internet vendors during e-commerce transactions (Pennington, Wilcox, & Grover, 2004). During an electronic transaction, consumers are vulnerable when they interact with an unfamiliar vendor (Gefen, 2000). They are at risk of having personal financial information stolen by hackers or unscrupulous e-vendors (McKnight, Choudhury, & Kacmar, 2002). In this context, Luhmann (1979) suggests that trust is a cognitive mecha-

nism adopted by users to reduce information complexity during transactions where they as the buyer have very little control over the actions of the vendor. Thus, the invocation of trust operates to reduce the amount of risk by reducing perceptions of anxiety and uncertainty. Some research indicates that these transactions are guided by relatively stable psychological traits such as a general predisposition to believe institutions or other people (Bhattacherjee, 2002; Brown, Poole, & Rodgers, 2004). Other efforts in the trust area have focused on how the design aspects of information technology can influence trust (Gefen, Karahanna, & Straub, 2003; Gefen, 2004). For example, consumer acceptance of Web site information has been found to be tied to measures of perceived quality and usability such as navigability, interactivity, and customer relations (Egger, 2001).

Although Web site usability characteristics are an important component of information credibility, it should be noted that addressing the design of a Web site is only a partial solution to building online trust. Personal characteristics of the users such as differences in experience in Internet use and certain demographic attributes (e.g., occupational status, age, etc.) may influence attitudes regarding the need to be attentive and critical of the information being sent or received over the Internet (Metzger, Flanagin, & Zwarum, 2003; Milne, Rohm, & Bahl, 2004). Novice Internet users may have difficulty discriminating fallacious Web interactions and may not know what to watch out for in protecting themselves from unscrupulous entities (Flanagin & Metzger, 2000). In other words, they might not know what information they can trust and which they should distrust and ultimately disregard it. Potentially, assistance might come in the form of cautionary communications communicated through security software and hardware on their computer (Hardee, West, & Mayhorn, 2006). Novices' inexperience with the WWW may allow others to take advantage of or exploit them. Persons with greater Web experience may be better able to discriminate the difference between sites that are more or less trustworthy. Thus, the ability to discriminate credibility among Web sites may be correlated with familiarity. Gefen (2000) illustrated how people's previous experience with an e-vendor acted to build familiarity and trust because it helped to create a conceptual framework where beliefs became more sophisticated. For novices and even heavier users, e-commerce frequently occurs in first-time and single-time only scenarios where users have not purchased items from a particular website in the past. In these instances, the development of trust through familiarity is largely unavailable, except for generalizations learned from previous related experiences.

An important issue suggested by the above analysis is whether people use characteristics of Web domains as cues regarding credibility. Previous research evaluating people's judgments of Web sites found that consumers reported the most important correlate of credibility to be its "design look" (Stanford, Tauber, Fogg, & Marable, 2002). Factors related to the appearance of a Web site such as colors, effective graphics, navigability of menus, and the ease of use along with the absence of obvious errors such as "dead links" and slow download speed, have been identified as design components that users consider when making credibility judgments (Egger, 2001; Wathen & Burkell, 2002). Other Web site aspects are also related to credibility and trust. Lowered perceived credibility for Web sites was associated with the characteristics of being linked with less credible sites, having spelling errors, and lacking reference citations. Rieeigelsberger, Sasse and McCarthy (2003) found that professional-looking page designs were given higher positive trustworthiness ratings. Also, research by Fogg, Soohoo, Danielson, Marable, Stanford, and Tauber (2002) found the design characteristics to be the most important determinant of perceived credibility of Web sites. The next highest factor was layout (another Web site design characteristic). Less important cues were familiarity and reputation of the Web site's host. These relationships between Web site design characteristics and perceptions of institution-based trust were validated in a recent longitudinal study that

tracked self-reported buyer behavior and future intentions of Amazon.com customers (Pavlou & Gefen, 2004).

Trust judgments are also made based on Web site content. One major aspect is the assessment about the expertise/competence of the source or host of the Web site (Wathen & Burkell, 2002). These judgments may be aided by including relevant details about the Web site's source or host (e.g., professional credentials, funding source, etc.). Giving photographs of the host's face or of a representative has been found to enhance trust by making the source appear more human and likeable (Fogg, 2003; Steinbrück, Schaumburg, Duda, & Krüger, 2002). Interestingly, however, this result has not always been found (Straub & Gaddy, 2003). Riegelsberger and Sasse (2001) suggest that face photos can be detrimental to Internet trust, because blatant attempts can misfire. Photos of "too" beautiful people can potentially undermine credibility beliefs. People may also believe commercial Web sites with face photos are strategic or "slick" attempts to manipulate people's trust, reducing people's perceived credibility of the sites (Riegelsberger, 2002; Riegelsberger & Sasse, 2001). Riegelsberger et al.'s (2003) data suggests that photos can add to the trustworthiness of less credible sites and hurt the perceived trustworthiness of credible vendors. The main point here is that research has begun to find that people use cues provided by Web site characteristics that affect perceptions of credibility.

The present research extends previous research on Internet trust by examining participants' beliefs about the credibility of information by examining the role of three Web site aspects in two studies. Study 1 examines perceived trust differences as a function of (a) domain suffixes (e.g., .com, .edu., .gov) and (b) security seals. Study 2 examines (c) organization domain names. The rationale for each of these factors is described in the context of introducing each study.

STUDY 1

Domain Suffixes and Seals of Approval

Study 1 examines people's beliefs about Web site credibility for two kinds of component variations: (a) domain suffixes (.com, .net, .org, .gov, and .edu), and (b) seals of approval. These two components are described below.

Domain Suffixes

Domain suffixes are the abbreviation after the period in the name of the basic Web site URL. They are sometimes an abbreviation that classifies the entity. For example, .gov is government, and .edu is education. Commercial companies in the United States commonly use .com. Suffixes may be cues for credibility judgments because they roughly define the source of message content (Hong, 2006). With respect to commercial entities, Web site users may perceive a profit motivation, and that the information may be incomplete and potentially lacking in information about risks (relative to the benefits). However, with the .gov suffix (usually associated with a U.S. government entity when it is without a country code), a profit motive is likely not to be as strongly associated, but may, due to a stronger connection with responsibility and accuracy, be viewed as having more credible information. Education institutions with .edu (usually colleges and universities) may be seen as credible because the content of Web sites with this suffix tend to be written in the context of information rich environments. Furthermore, the Web site content is usually approved by individuals such as faculty members or administrators who possessgraduate degrees, so users might make the assumption that the information is reasonably accurate except for minor mistakes. Other suffixes are also commonly used. Nonprofit organizations (which of course do not have a profit motivation, by definition) might be considered reasonably accurate. The above descriptions are overall categories. Finally, because of the tremendous growth of the Internet, there has been a need to

increase suffix designations. Some now being used are more difficult to define and are somewhat ambiguous. One is .net, which could yield beliefs that are less certain, and thereby might produce evaluations of credibility between the extremes. The levels of trust that these suffixes engender are examined in Study 1.

Seals of Approval

Another feature that could potentially increase the credibility of a Web site is the presence of seals of approval which suggest the endorsement of information by a presumably neutral third party (Pavlou & Gefen, 2004; Pennington, Wilcox, & Grover, 2003). One study focusing on health-related Web sites indicated that seals of approval were relatively uncommon and were found in only 4.8% of sites examined (Hong, 2006). Seals of approval such as VeriSign and Trust e are created by third party organizations that set some standard or set of protocols for which the users of their seal apparently must follow, usually in relation to the handling of consumer information (Cantrell, 2000). Apparently, Web sites that conform to some set of standards can use an organization's seal, which is supposed to mean that some level of security and confidentiality is being met in collecting and maintaining consumer information by the site's operators so that information theft and inappropriate use of consumer information is reduced. A company potentially benefits from using a seal of approval because it may enhance the perceived credibility of its Web site (Grabner-Kraeuter, 2002; Pavlou & Gefen, 2004).

The present study compared several real seals of approval used on various Web sites together with some fictitious seals that were added to the set and which were made from a few simple, basic graphic components. The fictitious seals were included to determine if they might be perceived to be as credible as actual seals being used in Web commerce. In addition, certain demographic categories were also examined to determine if there were any participant differences.

Method

Participants. The data is derived from the responses of 247 individuals in or around the Raleigh, North Carolina area. Data was collected as part of a larger questionnaire containing items concerning a variety of safety-related topics. The data were collected as part of a research project in which university students in an advanced ergonomics course solicited 10 or more persons to complete the survey. Due to incomplete data in the collected surveys for the items examined, 14% of the returned surveys were not included in the analyses described below. Of the sample, 171 were undergraduate students ($\underline{M}$ = 20.5 yrs., $\underline{SD}$ = 1.8) and 76 were non-students ($\underline{M}$ = 39.4 yrs., $\underline{SD}$ = 13.5), including 125 males and 122 females.

Materials and Procedures

In the questionnaire instructions participants were asked:

A. to estimate how many hours per week they use a computer to connect to the Internet (including email) over the past year
B. to rate how much they trusted the information on the Internet/World Wide Web in general
C. to rate the domain suffixes: .com, .edu, .gov, .net, and .org on the extent to which they would trust the information on a site with that suffix
D. to rate a set of seals of approval according to the extent to which they would trust the information associated with them. The seals as shown in Table 2 were presented in color to participants. Seven were from actual Web-based organizations and three were fictitious. The fictitious ones, constructed from simple graphic components including commonly available Web art, were: (d) Accu-Chek, (h) Web Verification Assurance System, and (i) Honesty and Integrity on the Web.

Accompanying the last three items (B, C, and D) was the instruction to make the ratings on a percentage (%) scale with the following

anchor descriptors given: (0%) "Would not trust at all," (50%) "Would trust about half," and (100%) "Would trust completely."

Results

Participants reported trusting 55% (SD=16.4) of the information on the Internet in general. On average, the participants reported to use the Internet 25.4 hours per week (SD= 30.8). This distribution of hours per week was positively skewed, having a median of 15 hours. Participants were divided into two groups according to hours of Internet usage (i.e., more vs. less than 15 hours per week), and this coding was used as a grouping variable in subsequent analyses.

Analyses of the demographic variables showed significant effects for two categories—hours of usage and occupation. These results are described in the two sections that follow.

Suffix Domains

Table 1 provides the means and standard deviations for domain suffix for participant occupation (college student vs. non-student) and Internet usage hours per week: (low < 15 vs. high > 15). A 2 (hours usage) x 5 (domain suffix) mixed-model analysis of variance (ANOVA) showed a significant main effect of domain suffix, $F(4, 980) = 205.41$, $p < .0001$ and the interaction, $F(4, 980) = 2.62$, $p < .05$, but not a main effect of hours usage, $F(1, 245) = 1.07$, $p > .05$. Tukey's Honestly Significant Difference (HSD) test on the domain suffix means showed that participants gave significantly higher trust evaluations for .edu ($M = 76.8$) and .gov ($M = 75.3$) than the other suffixes, but these two did not differ significantly from each other. The domain suffix .org ($M = 63.8$) was trusted significantly more than .net ($M = 50.1$) and .com ($M = 47.1$). The latter two, .net and .com, were not significantly different. Tests of simple effects revealed that participants who report using the Internet more than 15 hours a week also gave higher trust ratings for the domain suffixes, .edu ($M = 80.4$) and .gov ($M = 78.7$), than participants who reported using the Internet less than 15 hours a week, .edu ($M = 74.9$) and .gov ($M = 73.3$). The remaining comparisons were not significant.

A 2 (occupation: college student vs. non-student) x 5 (domain suffix) mixed-model ANOVA showed a significant main effect for domain suffix, $F(4, 980) = 157.26$, $p < .0001$ and its interaction with occupation, $F(4, 980) = 6.47$, $p < .0001$, but not a main effect of occupation, $F(1, 245) = 1.85$, $p > .05$. The results are very similar to Internet usage analysis described above. Tests of simple effects revealed that the college students reported greater trust of .edu ($M = 80.6$) and .gov ($M = 78.7$) than non-students, .edu ($M = 71.4$) and .gov ($M = 70.3$). No other comparison was significant.

Seals of Approval

Table 2 provides the mean trust ratings and standard deviations for the seals of approval as a function of Internet usage hours per week (low < 15 vs. high > 15) and participant occupation (college student vs. non-student). A 2 (hours of usage) x 10 (seals of approval) mixed-model ANOVA showed a significant main effect of seals of approval, $F(9, 2205) = 24.36$, $p < .0001$, and its interaction with hours of usage, $F(9, 2205) = 2.39$, $p < .01$, but not a main effect of hours of usage, $F(1, 1245) = 1.28$, $p > .05$. Tukey's HSD test showed that participants reported that they trusted (a) VeriSign ($M = 52.8$) significantly more than all of the other seals. The (b) Health Website Accreditation ($M = 47.4$) and (c) Trust e ($M = 43.9$) were trusted significantly more than all of the remaining seals. The next set below these did not significantly differ from one another, except that the lowest (j) Scambusters ($M = 36.0$) was rated significantly lower than (d) Accu-Chek ($M = 42.2$), (e) Health On the Net Foundation ($M = 41.5$), and (f) BizRate.com ($M = 40.8$). Tests of simple effects revealed that participants reporting more online hours per week also gave higher trust ratings of (a) VeriSign ($M = 58.8$) and (f) Bizrate.com ($M = 44.8$) than those spending less time on the Internet per week, VeriSign ($M = 49.5$) and Bizrate.com ($M = 38.3$). The remaining similar comparisons were not significantly different.

Table 1. Mean % trust ratings as a function of hours on the internet and occupation for domain suffix trust (SD in Parentheses)

	Internet/Week Usage Hours		Occupation		
Suffix	Low (<15)	High (>15)	Non-Student	Student	*Mean*
.edu	74.9 (21.3)	80.4 (16.9)***	71.4 (22.3)	80.6 (16.9)***	76.8
.gov	73.3 (23.9)	78.7 (17.6)**	70.3 (23.6)	78.7 (19.3)***	75.3
.org	63.5 (23.3)	64.0 (21.3)	64.3 (22.8)	63.5 (21.9)	63.8
.net	50.8 (18.8)	49.2 (21.7)	50.7 (20.7)	49.6 (20.2)	50.1
.com	46.8 (21.7)	47.1 (21.3)	47.9 (23.3)	46.6 (20.6)	47.1
Mean	61.9	63.9	60.9	63.8	

Note: Higher scores indicate greater levels of trust.
***p<.01. ***p<.001*

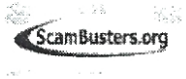
Table 2. Mean % trust ratings as a function of hours on the internet and student status for seals of approval (SD in parentheses)

	Internet/Week Usage Hours		Occupation		
Trust Seals	Low (<15)	High (>15)	Non-Student	Student	*Mean*
(a) VeriSign	49.5 (27.1)	58.8 (25.9)**	43.9 (30.5)	59.0 (23.7)***	52.8
(b) URAC Health Web Site Accreditation	47.2 (28.0)	50.0 (25.0)	39.3 (24.5)	52.9 (24.3)***	47.4
(c) TRUSTe Make privacy your choice.	43.2 (26.1)	46.3 (24.4)	38.7 (26.3)	47.5 (24.3)**	43.9
(d) ^	42.5 (25.7)	43.0 (24.8)	38.6 (26.6)	44.7 (24.4)	42.2
(e) HON @ code Health On the Net Foundation	40.8 (24.8)	43.1 (24.3)	38.2 (24.6)	43.7 (24.3)	41.5

Note: Higher scores indicate greater levels of trust; ^Indicates fictitious seal of approval symbol.
** p < .05. ** p < .01. *** p < .001*

continued on following page

Table 2. continued

(f)		38.3 (23.9)	44.8 (25.0)*	35.9 (27.1)	44.3 (23.1)**	40.8
(g)		40.8 (26.8)	41.7 (25.5)	38.9 (28.8)	42.3 (24.7)	40.9
(h)	 ^	40.7 (24.9)	40.8 (24.2)	35.0 (25.8)	43.3 (23.5)**	40.0
(i)	 ^	40.2 (24.0)	39.6 (25.0)	36.3 (25.3)	41.5 (24.0)	39.4
(j)		34.6 (23.5)	38.9 (24.0)	30.7 (25.5)	39.7 (22.5)**	36.0
Mean		41.8	44.7	37.6	45.9	

Note: Higher scores indicate greater levels of trust; ^Indicates fictitious seal of approval symbol.
** $p < .05$. ** $p < .01$. *** $p < .001$*

A 2 (occupation: student vs. non-student) x 10 (seals of approval) mixed-model ANOVA showed significant effects for both main effects, seals of approval, $F(9, 2205) = 17.08$, $p < .0001$, and occupation, $F(1, 245) = 9.19$, $p < .01$, as well their interaction, $F(9, 2205) = 2.93$, $p < .001$. Tests of simple effects revealed that college students, compared to non-students, reported greater trust for the following seals: (a) VeriSign (M = 59.0 vs. 43.9), (b) Health Website Accreditation (M = 52.9 vs. 39.3), (c) Trust e (M = 47.5 vs. 38.7), (f) BizRate.com (M = 44.3 vs. 35.9), (h) Web Verification Assurance System (M = 43.3 vs. 35.0), and (j) Scambusters.org (M = 39.7 vs. 30.7). Thus for 5 of the 7 real seals, college students gave higher trust ratings than the non-students. Also, 1 of the 3 fictitious seals, Web Verification Assurance System, showed the same significant higher trust by the college students. No other paired comparison was significant.

Discussion

Study 1 examined perceptions of trustworthiness of several domain suffixes and seals of approval. Consistent with the results of Hong (2006) concerning the credibility of health-related websites, participants discriminated among different domain suffixes by showing .edu and .gov to be rated higher than .net and .com, with .org intermediate. This finding roughly follows a positive relation with expertise and a negative relation with profit motive. The two highest rated domain suffixes (.edu and .gov) are usually associated with informational sources possessing higher education and a responsibility to give accurate information. The lower rated suffixes are associated with commercial enterprises with profit goals. Commercial Web sites would be more likely to pursue advertising and marketing schemes that utilize biased informational content that give less emphasis to negatives (including risks) while emphasizing

the positives to persuade consumers to buy their products. The exception is direct-to-consumer advertising (DTC) by drug manufacturers in which the U.S. Food and Drug Administration (FDA) advises and warns manufacturers when their Web content fails to present an equal balance of benefits and risks (FDA, 1999).

Also examined were seals of approval (e.g., VeriSign). Perceived degree of trust was judged for seven real and three fictitious seals. Trust ratings for fictitious seals were in some cases as high as or higher than were elicited by several of the actual seals. More experienced users (as well as the college-student demographic) seemed to be able to better discriminate two of the most common seals than less experienced users (and non-student adults). However, it is interesting to note that experienced users also rated one of the fictitious seals significantly higher than did the less experienced users. The particular trend noted above is consistent with previous research indicating that student populations rely heavily on the Web for personal and academic information, but they are also less likely than non-students to verify the quality of online information (Metzger, Flanagin, & Zwarum, 2003). We will give other implications of these results in the General Discussion section.

STUDY 2

Domain Names

Participants' beliefs about the credibility of information may also be based on names of organizations and their associated Web domain names. The major focus of Study 2 was whether participants would evaluate actual and fictitious organizations (and corresponding Web domain addresses) differently with regard to the amount of trust they would have for the informational content of the Web site. The experimental manipulation was designed to determine whether people could discriminate real organizations and their corresponding Web site domain from fake (bogus) ones through the pattern of their ratings. In half, the organizations (and associated Web address) were real, and in the other half, they were fictitious. The fictitious Web sites were included to determine if they might be perceived to be as credible as actual Web sites.

Method

Participants. A total of 186 individuals participated (101 females and 85 males), with 89 being college students and 97 non-student adults. The college students (M = 21.6, SD = 3.1, ranging from 18 to 34 years) were recruited from introductory psychology courses and received class credit for their participation. The non-students (M = 40.6 years, SD = 15.2, ranging from 19 to 81 years) were volunteers from the Raleigh, North Carolina area who were recruited at various venues. Another smaller group of participants (N = 13) rated the domain names on familiarity.

Stimuli. Sixteen types of domains were used. They were selected to represent a wide range of content areas. Associated with each content domain was a real (actual) organization, together with a basic "home" Internet address. All of the real organizations provide services including the distribution of informational materials (e.g., medical or chemical information) for members within the organization and to outside groups (e.g., concerning medical or chemical information). Companies whose main role is product manufacturing were not included. Paired with every real organization was a fictitious organization appearing to cover a similar content area. Thus, each domain type was associated with one actual (WebMD: www.WebMD.com) and one fictitious (Web Doctor: www.WebDoctor.org) domain name and Web address. This resulted in a total of 32 domain names investigated (16 domain pairs). All participants viewed all 16 domain types. Approximately half the participants saw one set of 16 domain names in which half (8) were actual and half (8) were fictitious. The other half of the participants were given the remaining 16 domain names in which half were real and half were fictitious. Thus, each item of the domain name pairs was seen by about half the participants from balancing their presentation across the two groups of participants. Any given participant saw all 16 domain types, but only

one of its paired domain names: an actual name or a fictitious one.

Procedure. Participants were asked to complete a multi-topic questionnaire. The present research focuses only on those questions involving trust of Web site information and demographics (e.g., age, sex, and occupation).

Initially, participants were given background information that Web sites may be created and maintained by a variety of persons and organizations. Given the list of 16 organizations and Web site addresses, they were asked to provide a percentage estimate (0 to 100%) according to how much they would trust the information presented on the named Web site. Anchor descriptions for the ratings were the same as Study 1's: 0% = would not trust at all; 50% = would trust about half; 100% = would trust completely.

Another group of participants rated the same organizations on familiarity. The 9-point rating scale (0 to 8) had the following word anchors associated with the even-number anchors: (0) not at all familiar, (2) somewhat familiar, (4) familiar, (6) very familiar, and (8) extremely familiar.

Results

Analyses revealed that participants reported on average trusting only 55% of the information across the 16 Web site domains provided. Overall, mean computer use per week was reported to be 25.2 hours (SD = 18.4). There was no significant relationship between hours using the computer and mean trust ratings. There were also no significant relationships for gender and occupation (college student vs. non-student) on computer use, but younger participants tended to use a computer more per week than older participants, $r = -.24$, $p < .01$. Also, there was a relationship between age and trust; younger participants reported higher levels of overall trust to the organizations than older participants, $r = -.16$, $p < .05$.

The data for the trust ratings for the specific actual and fictitious sites are shown in Table 3. Participants rated eight (50%) of the actual Web sites higher on trust than its fictitious pair. They also rated three of the fictitious websites significantly higher than actual websites. For the other five domain types, ratings did not differ between the actual and fictitious websites.

Analyses incorporating demographic categories yielded only a few significant effects. There were no gender effects except for one involving the broker domains. Males tended to trust the fictitious broker organization (American Brokers Counsel) more than females, but there was no gender difference for trust of the actual/real broker organization (American Brokers Corporation). The college student vs. non-student demographic factor also showed no differences except for one regarding ergonomics societies. Non-students trusted the fictitious ergonomics association (National Ergonomics Association) more than the real one (Human Factors and Ergonomics Society); however, there was no difference between the two ergonomics associations for the college students. Additional analyses yielded no other significant correlations or main effects/interactions as a function of other demographic grouping variables.

Also included in Table 3 are mean familiarity ratings. These data were collected from an independent group of individuals from the same pool of participants that evaluated the domain names on percentage trust. These data show that there are some instances where better known organizations (given relatively high ratings of familiarity) such the American Automobile Association and WebMD, were trusted more than the fictitious pairing. However, there were two instances in which participants indicated being significantly more familiar with the fictitious organization than the actual organization. Thus, there is some evidence of a relationship between familiarity and trust; however, correlations between trust and familiarity with actual and fictitious Web site domains considered separately or together failed to show any significant relationships.

Discussion

In some cases, participants gave substantial trust scores to fictitious names of organizations

Table 3. Mean % trust and familiarity ratings for actual and fictitious Web sites/organizations

%Trust	*Actual We bsites*	Familiarity	%Trust	*Fictitious Web sites*	Familiarity
	American Academy of Pediatrics			American Pediatrics	1.44
73%***	www.AAP.org	1.00	53%	www.American-Pediatrics.org	
	Drug Information Association			Medicine Information Association	1.67*
55%	www.DIAHome.org	.95	53%	www.MedInfo.org	
	Advanced Chemical Safety			American Chemical Laboratories	.35
74%***	www.Chemical-Safety.com	.36	54%	www.ACA.org	
	American Association for Retired Persons			Association for Older Americans	.18
64%	www.aarp.org	1.60***	59%	www.olderamericans.org	
	JD Powers and Associates			Consumer Satisfaction Federation	.65
52%*	www.JDPower.com	1.85***	45%	www.ConsumerRight.com	
	National Nutritional Foods Association		51%	American Nutritional Foods Assn	.74
61%**	www.NNFA.org	.82		www.ANAA.com	
	Crash Worthiness			Crash Safety	.85***
38%	www.Crash-Worthiness.com	.22	57%***	www.Crash-Safety.org	
	American Dietetic Association			Dietary Association of America	.70
61%***	www.EatRight.com	2.21***	47%	www.DIAA.com	
	Society for Women's Health Research			Women's Health Association	2.21***
61%	www.Womens-Health.org	1.29	65%	www.WHA.com	

continued on following page

Table 3. continued

	Human Factors and Ergonomics Society			National Ergonomics Association	.36
60%	www.HFES.org	.43	63%	www.NEA.net	
	WebMD			Web Doctor	1.45
60%**	www.WebMD.com	3.49***	49%	www.WebDoctor.org	
53%	National Environmental Education and Training Foundation	.33		American Environmental Education Foundation	.47
	www.NEETF.org		55%	www.AEEF.org	
47%	AAA American Credit Bureau	1.25	60%***	American Credit Foundation	1.73
	www.AAACredit.com			www.ACF.com	
61%***	American Automobile Association	3.49***	48%	National Automobile Counsel	.74
	www.AAA.com			www.NAA.com	
49%**	American Brokers Corporation	.82	39%	American Brokers Counsel	.74
	www.AmericanBrokersCorp.com			www.Abroker.net	
40%	Internet Security Software	.92	52%**	Security Software on the Internet	.36
	www.ISS.net			www.SSI.net	

*$p < .05$; **$p < .01$; ***$p < .001$

and Web sites. The potential problem that this finding highlights is that unscrupulous individuals may put up a Web site that appears to be a reputable source of information on some topic when in fact it is not reputable, and may contain false and deceptive information. For example, a phony organization or business could be formed simply for the purpose of deceiving users (Baker, 1999). Without knowledge that an organization is bogus, people might accept the information provided as authentic and true based on their concept and assumption of system trust (Pennington, Wilcox, & Grover, 2003). Indeed, a mystery organization with the name, National Ergonomics Association, was a party in providing information to U.S. lawmakers about ergonomics. The information, promulgated by this apparent organization, was that there was not enough science to support stronger ergonomics laws. Of some importance and concern in this case is that this lobbying effort might have played a part in the withdrawal

of a proposed overhaul of U.S. Occupational Safety and Health Administration regulations promulgated in 2000 and 2001. The problem with having bogus organizations is that untrained and unaware users might think that the information provided by a seemingly legitimate source represents the current state of the art and basic thinking of professional ergonomists. The information put out under the banner of the National Ergonomics Association may seem like it is coming from a credible and expert source on the topic, and thus, could influence opinion and "knowledge." The main point is that people may have difficulty in differentiating which organizations and Web sites are credible and trustworthy. This issue is particularly important when the information involved concerns topics such as health care where safety and risk factors are involved.

While the present study has clear implications for users of the Internet, the findings also have implications for companies and other hosts of Web sites. For example, illegitimate Web sites that appear similar to legitimate Web sites might detract from the reputation and perceptions of credibility of legitimate sites. Unscrupulous efforts might capitalize on the role of perceived organizational familiarity and trust (Gefen, 2000; Gefen, Karahanna, & Straub, 2003), and through deceit and disguise produce disrepute on legitimate, reputable organizations.

A small but significant negative correlation suggested that older individuals do not trust Web sites as much as younger adults. This finding is consistent with previous research (Karvonen & Parkkinen, 2001), but may also be attributable, at least partly, to a generation gap with respect to computing. There is now a large body of research that demonstrates, contrary to popular belief and early research, that very old adults are willing to learn about the Internet (see Rogers, Mayhorn, & Fisk, 2004 for a review). However, older adults are also more wary in sharing personal information online. Despite the overall lower level of trust by the older-age adults, they had a similar pattern of ratings of the actual and fictitious sites as did younger-age adults.

In some instances better known, more familiar organizations such the AAA and WebMD were trusted more than the fictitious pair. However, moderate and lower levels of familiarity do not seem to have a substantial influence on the extent of trust. Interestingly, in two cases, higher familiarity ratings were sometimes given to the fictitious organization (Women's Health Association and Crash Safety) than the actual organization (Society for Women's Health Research and Crash Worthiness). Clearly, if it is fictitious, it should be considered unfamiliar. Possibly, however, the fake names seemed better. It would be unfortunate if people were misdirected away from real Web sites because the real organizations do not sound as good as fake ones. The familiarity ratings seemed to depend on the name of the organization and domain name seeming authentic and credible. Yet because of the somewhat unclear pattern of findings, the relation between trust and familiarity needs further investigation.

The topic or content domain of the organization appears to play a relatively large role in people's judgments. Medical and health related sites seem to be trusted more than Web sites in other content domains such as organizations comprised of brokers and security software engineers. This suggests that people may believe that certain content areas have some heightened risk associated with them.

GENERAL DISCUSSION

The overall findings of this research are discussed in three parts. In the first, the current findings are summarized, and potential methodological shortcomings are described. In the second, the findings are discussed in terms of how they relate to previous research in the area. Finally, the implications and conclusions section offers implications and suggestions for future research.

Findings from the Current Research

This research suggests that people have a moderate level of skepticism and confidence in the veracity of information on the Internet.

In general, people reported that they trusted only about half of the informational content on the Internet. This was relatively consistent in both studies using different kinds of overall measures of Internet trust.

The results show that reported trust of Internet Web sites differed as a function of domain suffix, seals of approval, and organization domain names. For the domain suffixes, .gov and .edu were rated the highest, and .net and .com were rated the lowest. This finding is sensible in that most information posted by government agencies is accurate and based on considerable internal and external review. The .edu finding also makes sense in that these Web sites are domains of higher education institutions. The finding that .com and .net are lowest probably reflects their commercial nature and the fact that some businesses may not provide reliable and valid information. The finding that .org is in the middle may reflect people's differing experience with (not-for-profit) organizations with respect to the reliability and accuracy of the information they provide.

Additional findings indicate that participants who reported greater Internet usage had greater trust of .gov and .edu domain suffixes than participants with less Internet usage. The same pattern was found for students vs. non-students, who tended to overlap with the above-mentioned usage categories (i.e., students using the Internet more than non-students). This pattern might be explained by differences in exposure to the Internet. In other words, it is likely that the student population sampled in these studies may be more familiar with these types of sites because they frequently access them for academic information (Metzger, Flanagin, & Zwarun, 2003). Persons who use the Internet more may have, over time, learned to trust the quality of information for .gov and .edu sites more than persons who have used the Internet less (Gefen, 2000). Likewise, the trend for non-student adult populations to display less trust than students is consistent with previous work (Metzger et al., 2003).

While these findings are theoretically and practically interesting, the limitations of the present study should be noted. First, the survey methodology used self-report data which might not necessarily reflect objective behavior with regard to online trust by users. Nevertheless, such methods are useful in determining the subjective attitudes of users which has been shown to be a predictor of goal-directed intentionality (Fishbein & Ajzen, 1975). Second, the generalizability of the results might be questioned because the participants were recruited from one area of the world—the United States. While previous research does indicate that the predisposition to trust others has a strong cross-cultural component (Fukuyama, 1995), there is also evidence that standardized interface designs act to facilitate online trust (Gefen, 2000). Because e-commerce is a global construct, it is unclear whether the impact of Web design characteristics will offset cultural differences in trust. This issue is addressable in future empirical research. Lastly, the external validity of using student samples has been questioned by previous investigators. While this concern is valid, it should be noted that both experiments reported here also recruited a substantial number of non-student adults. Also, it might be noted that currently, conventional e-consumers are younger and better educated than other segments of the population who are less apt to conduct e-commerce transactions (McKnight, Choudhury, & Kacmar, 2002). Thus, in this area of research, samples that include university students might reasonably approximate the online consumer demographic.

Placing the Current Findings in the Context of Past Research

As mentioned earlier, previous research suggests that the quality of the user interface of Web sites is a major determinant of a person's initial establishment of trust (Aubert, Dewit, & Roy, 2001; Wathen & Burkell, 2002). However, some of the best (and also some of the worst) interfaces are found in .com Web sites, which in this study were rated lower than .gov and .edu. The latter two domains tend to have more basic (i.e., less elaborate) interface designs. Also, .gov and .edu Web sites may be

subject to usability oversight and regulation. For example, the National Institute on Aging (NIA) has published a set of design guidelines to ensure that designers of US government Web sites are creating interfaces that are usable by older adults (Morrell, Holt, Dailey, Feldman, Mayhorn, Echt, & Podany, 2003). Because .com Web sites are less regulated in terms of design layout and interface, they are highly variable in the amount of trust they elicit. Recent usability testing of e-commerce sites by Nielsen and his associates suggested that average Web sites complied with approximately 55% of the guidelines they developed to enhance online informational trust (Nielsen, Molich, Snyder, & Farrell, 2000). Thus, some cues about trust apparently arise from a variety of Web design components. According to the present results, trust beliefs are cued at least partly by domain suffix.

Seals of approval also influenced Internet trust. The highest trust ratings were for VeriSign. However, this seal and the ones that followed it only received moderate levels of trust. Interestingly, the fictitious seals that were inserted in the set were rated as high, or higher, than some of the seals which are actually used in reputable Web sites. This suggests both a lack of discrimination and a hesitancy to assign substantial credibility based simply on the seals.

Other analyses showed that persons who use the Internet to a greater extent reported greater trust for some seals such as VeriSign and BizRate.com than persons who used the Internet to a lesser extent. These two seals are frequently used by credible, reputable Internet vendors. Previous research suggests trust tends to emerge from a long-term relationship between a person and another entity, in this case that could be the Internet (Corritore, Kracher, & Wiedenbeck, 2003; Goldsmith & Lafferty, 2002). With these two seals, familiarity and their association with good companies may enhance the development of trust. Students vs. non-students showed a similar pattern, but also yielded additional significant differences with students trusting Trust e, BizRate.com, Web Verification Assurance System, and ScamBusters.org more than non-students. While the explanation of familiarity and association with good companies fits the pattern of findings for three of these seals, it does not fit entirely because the Web Verification Assurance System seal is fictitious and should, therefore, be less familiar and not associated with good companies. College students exhibited heightened levels of trust even for a fake seal. The seals of approval results tend to show that people who report greater Internet use have somewhat higher levels of trust, and perhaps too much, as exhibited by the findings for one of the fictitious seals. These seemingly discrepant findings are explainable when placed in the context of Fogg's (2003) framework where he described the source of Internet credibility errors. In this framework, Fogg explained that users who are skeptical of sites in general may make "incredulity errors" when they incorrectly mistrust information from reputable sites. By contrast, other users may commit "gullibility errors" when they are persuaded to accept bogus information.

The relatively moderate levels of rated trust indicates, at least some level of appropriate skepticism, and for good reason, since some companies using the seal have violated their policies (George, 2002) in exposing or selling personal information collected. Such actions along with eavesdropping on user sessions and manipulating data without authorization constitute a threat to information security (Schultz, Proctor, Lien, & Salvendy, 2001). Increasingly, the onus of convincing consumers that the online information they provide on the Internet is valid and reliable rests solely with the company or organization that maintains that Web site. The seals of approval potentially give assurances from a third party that personal information will not be disclosed, but this would only develop if the seals of approval are based on valid criteria that are actually upheld.

IMPLICATIONS AND CONCLUSION

An important implication of this research is that people might be "taken" by a Web site giving deceptive and misleading information—without

their realization. Wrongly assigned trust could translate into misplaced trust and potential susceptibility to security risks such as "phishing" attempts. There is also the potential problem of the incorporation of false information into memory that may be used as some basis for decision making later.

There are several directions that future research might take. Potential follow-up questions include: (a) whether users make the mistake of using misleading information posted on Web sites; (b) whether they use the "information" in making decisions; and (c) whether they realize (without being told) that they have been fed false information. These and other related research ideas warrant future investigation.

Other potential implications include the use of interventions to give users the information they need to verify the validity of the Web sites they use. One initial step in enhancing the credibility of online information is to utilize the existing literature on persuasive message content development. For example, credibility might be enhanced by providing links to other Web sites on the same topic and other reference sources so that users can independently confirm that the information they are reviewing is accurate (Amsbary & Powell, 2003; Fallis, 2004). The presence of statistics and quotations/testimonials from other users who share similar characteristics might be effective in convincing users (Hong, 2006). Interventions could focus on the development of published guidelines to help users evaluate information credibility (Alexander & Tate, 1999; Fallis, 2004). The guidelines might give indicators such as whether the author's credentials are listed, the lack of advertising, the absence of typographical errors, the presence of up-to-date content, and the citation of authoritative references.

As users may be unwilling to follow a checklist every time they search the Internet for information, other researchers such as Wathen and Burkell (2002) have proposed the development of a quality rating scale for Web sites, but they also describe why this approach is premature. Given the current state-of-the-art, which indicates that researchers are still learning about how people make credibility judgments of online information, it is unclear what quality control measures might be evaluated by a rating system. Moreover, because the sheer number of Web sites on the Internet is vast, and participation by Web site designers is voluntary, it seems unlikely that such a rating system will be viable in the foreseeable future.

Because it is unrealistic to presume that people will be constantly on guard to protect themselves from potential online security threats that arise from information credibility issues, perhaps this function should be allocated to the technology involved. The browser or portal engines that allow users access to the Internet might be empowered with computerized algorithms or artificial intelligence routines to provide them with enhanced "awareness" regarding credibility issues. These interventions might take the form of autonomous software programs that automatically perform a "behind the scenes" security check for the user on the legitimacy of the site and possibly past user experiences. Automated checks might also examine available information regarding the background of persons or organizations to which the domain belongs. Conditions to be checked during such an automated "security scan" intervention might focus on the presence or absence of Web site design features such as identifying credible seals and domain suffixes. Concurrently, the automated system might access a variety of user-related criteria such as customer ratings and site owner-related information such as length of time in business. Reputable Web site hosts would benefit since users would be less uncertain about the Web site's credibility and users would be protected from potentially fraudulent sites.

ACKNOWLEDGMENT

Special thanks and gratitude are given for assistance by Eric F. Shaver, Atticus Y. Evil, Christina C. Mendat, and Shana J. Ward. Portions of this research were presented at the Human Factors and Ergonomics Society Annual Meeting in Denver, Colorado, USA (Evil, Shaver, & Wogalter, 2003) and at the International Ergo-

nomics Association 16th Triennial Congress (Wogalter & Mayhorn, 2006), in Maastricht, The Netherlands.

REFERENCES

Alexander, J. E., & Tate, M. A. (1999). *Web wisdom: How to evaluate and create information quality on the Web*. Mahwah, NJ: Lawrence Erlbaum Associates.

Amsbary, J. H., & Powell, L. (2003). Factors influencing evaluations of website information. *Psychological Reports, 93*, 191-198.

Andreou, A., Kanellis, P., Martakos, D., & Papadopoulou, P. (2001). Trust and relationship building in electronic commerce. *Internet Research, 11*, 322-332.

Aubert, B.A., Dewit, O., & Roy, M.C., (2001). The impact of interface usability on trust in web retailers. *Internet Research, 11*, 388-398.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly, 26*(3), 243-268.

Baker, R. C. (1999). An analysis of fraud on the Internet. *Internet Research, 5*, 348-359.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems, 19*(1), 211-241.

Brown, H. G., Poole, M. S., & Rodgers, T. L. (2004). Interpersonal traits, complementarity, and trust in virtual collaboration. *Journal of Management Information Systems, 20*(4), 115-137.

Cantrell, S. (2000). e-Market trust mechanisms. *Accenture Research Note: E-Commerce Networks, 11*, 1-3.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies, 58*, 737-758.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of CHI* (pp. 581-59).

Egger, F. N. (2001). Affective design of E-Commerce user interfaces: How to maximize perceived trustworthiness. In *Proceedings of the International Conference on Affective Human Factors Design.* Asean Academic Press: London.

Evil, A. Y., Shaver, E. F., & Wogalter, M. S. (2003). On trust in the Internet: Belief cues from domain suffixes and seals of approval. In *Proceedings of the Human Factors and Ergonomics Society* (pp. 1346-1350).

Fallis, D. (2004). On verifying the accuracy of information: Philosophical perspectives. *Library Trends, 52*, 463-487.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research.* Reading, MA: Addison-Wesley.

Flanagin, A. J., & Metzger, M. J. (2000). Perceptions of Internet information credibility. *Journalism and Mass Communication Quarterly, 77*, 515-540.

Fogg, B. J. (2003). *Persuasive technology: Using computers to change what we think and do.* San Francisco: Morgan Kaufman.

Fogg, B. J., Soohoo, C., Danielson, D., Marable, L., Stanford, J., & Tauber, E. R. (2002). How do people evaluate a website's credibility? Persuasive Technology Lab Stanford University, Consumer Webwatch, Slice bread Design, LLC.

Food and Drug Administration. (1999). *Prescription drug advertisements* (Federal Register, Title 21 Vol. 4, Parts 200-299). Washington, DC: U.S. Government Printing Office.

Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity*. New York: The Free Press.

Gallivan, M. J., & Depledge, G. (2003). Trust, control, and the role of interorganizational systems in electronic partnerships. *Information Systems Journal, 13*, 159-190.

George, J. F. (2002). Influences on the intent to make Internet purchases. *Internet Research, 12*, 165-180.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega, 28*, 725-737.

Gefen, D. (2004). What makes an ERP implementation relationship worthwhile: Linking trust mechanisms and ERP usefulness. *Journal of Management Information Systems, 21*, 263-288.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90.

Goldsmith, R.E., & Lafferty, B.A. (2002). Consumer response to websites and their influence on advertising effectiveness. *Internet Research, 12*, 318-328.

Grabner-Kraeuther, S. (2002). The role of consumers' trust in online shopping. *Journal of Business Ethics, 39*, 43-50.

Hardee, J. B., West, R., & Mayhorn, C. B. (2006). To download or not to download: An examination of computer security decision-making. *Association of Computing Machinery: Interactions, 13*(3), 32-37.

Hong, T. (2006). The influence of structural and message features on website credibility. *Journal of the American Society for Information Science and Technology, 57*(1), 114-127.

Johnson, T. J., & Kaye, B. K. (1998). Cruising is believing? Comparing Internet and traditional sources on media credibility measures. *Journalism and Mass Communication Quarterly, 75*, 325-340.

Karvonen, K., & Parkkinen, J. (2001). Signs of trust: A semiotic study of trust formation in the web. In M. J. Smith, G. Salvendy, D. Harris, & R.J. Koubek (Eds.), *Usability evaluation and interface design: Cognitive engineering, intelligent agents and virtual reality* (pp. 1076-1080). Mahwah, NJ: Erlbaum.

Luhmann, N. (1979). *Trust and power* [translation from German]. Chichester, UK: Wiley.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-Commerce: An integrative typology. *Information Systems Research, 13*, 334-359.

Metzger, M .J., Flanagin, A. J., & Zwarun, L. (2003). College student Web use: perceptions of information credibility, and verification behavior. *Computers and Education, 41*, 271-290.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs, 38*, 217-232.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs, 35*, 27-44.

Morrell, R. W., Holt, B. J., Dailey, S. R., Feldman, C., Mayhorn, C. B., Echt, K. V., & Podany, K. I. (2003). *Older adults and information technology: A compendium of scientific research and website accessibility guidelines*. Washington, DC: National Institute on Aging.

Nielsen, J., Molich, R., Snyder, C., & Farrell, S. (2000). *E-commerce user experience: Design guidelines for trust and credibility.* Nielsen Norm Group, Feremont, CA. http://www.nngroup.com/reports/ecommerce/trust.html

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research, 15*, 37-59.

Pennington, R., Wilcox, H. D., & Grover, V. (2003). The role of system trust in business-to-consumer transactions. *Journal of Management Information Systems, 20*, 197-226.

Riegelsberger, J. (2002). The effect of facial cues on trust in e-commerce systems. In *Proceedings Volume 2 of the 16th British HCI Conference*, London.

Riegelsberger, J. & Sasse, M.A. (2001). Trust builders and trust busters. *The role of trust cues in interfaces to e-commerce applications*. Paper presented at the 1st IFIP Conference on e-commerce, e-business, e-government, Zurich, Switzerland.

Riegelsberger, J. & Sasse, M. A., & McCarthy, J. (2003). Shiny happy people building trust? Photos in e-commerce Websites and Consumer Trust. In *Proceedings of CHI 2003* (pp. 121-128). Ft. Lauderdale, FL.

Rogers, W.A., Mayhorn, C. B., & Fisk, A.D. (2004). Technology in everyday life for older adults. In S. Kwon & D. C. Burdick (Eds.), *Gerotechnology: Research and practice in technology and aging* (pp. 3-17). New York, NY: Springer Publishing.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*, 393-404.

Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). Usability and security: An appraisal of security issues in information security methods. *Computers and Security, 20*, 620-634.

Stanford, J., Tauber, E. R., Fogg, B.J., & Marable, L. (2002). Experts vs. online consumers: A comparative credibility study of health and finance websites. *Consumer WebWatch*. www.consumerwebwatch.org

Steinbrück, U., Schaumburg, H., Duda, S., & Krüger, T. (2002). A picture says more than a thousand words-photographs as trust builders in e-commerce websites. In *Proceedings of CHI 2002* (pp. 748-749). Minneapolis, MN.

Straub, K. & Gaddy, C. (2003). From bricks to clicks: Building customer trust in the online environment. *UI Design Newsletter*, November, 2003, Insights from Human Factors International. Available online: http://www.humanfactors.com/downloads/nov03.asp

U.S. Department of Commerce. (2002). *A nation online*. Available online: www.ntia.doc.gov/ntia-home/digitaldivide/

U.S. Department of Commerce. (2006). *Quarterly retail e-commerce sales* (4th Quarter 2006). Available online: www.census.gov/mrts/www/nrely.html

Wathen, C.N., & Burkell, J. (2002). Believe it or not: Factors influencing credibility on the web. *Journal of the American Society for Information Science and Technology, 53*(2), 134-144.

Wogalter, M.S., & Mayhorn, C.B. (2006). Is that information from a credible source? On discriminating Internet domain names. In *Proceedings of the XVIth Triennial International Ergonomics Association Congress*. Amsterdam,The Netherlands: Elsevier (on CD only).

Michael S. Wogalter is a professor of psychology at North Carolina State University, and is part of the Ergonomics and Experimental Psychology program. He has held faculty appointments at the University of Richmond (1986-1989) and Rensselaer Polytechnic Institute (1989-1992). He received a BA in psychology from the University of Virginia (1978), MA in human experimental psychology from the University of South Florida (1982), and PhD in human factors psychology from Rice University (1986). Most of his research focuses on issues associated with warnings, risk communication, human-computer interaction, face memory, and information design. He has over 300 peer-reviewed publications, including 6 edited books. He has been on the editorial boards of several journals including Applied Ergonomics, Ergonomics, Journal of Safety Research, *and* Theoretical Issues in Ergonomics Science. *He is a fellow of the Human Factors and Ergonomics Society and the International Ergonomics Association.*

Christopher B. Mayhorn joined the faculty of North Carolina State University in 2002 as an assistant professor of psychology in the ergonomics and experimental psychology program. In 2007, he was promoted to the rank of associate professor of psychology. He received a BA from The Citadel (1992), an MS (1995), a graduate certificate in gerontology (1995), and a PhD (1999) from the University of Georgia. He also completed a Postdoctoral Fellowship at the Georgia Institute of Technology. Dr. Mayhorn's current research interests include everyday cognition, human-computer interaction, safety, and risk communication. His research has been funded by national and private funding organizations such as the National Science Foundation. He has authored over 30 refereed journal and proceedings publications