

Trust in the Wired Americas



July 2000

255 Shoreline Drive
Suite 100
Redwood Shores
California 94065
phone 650.802.2100
fax 650.593.1125
www.cheskin.com

Cheskin Research

Cheskin Research is a leading strategic market research and consulting firm helping companies compete in the new global Internet economy. For over 50 years, Cheskin has been recognized for contributing to competitive breakthroughs in product development, branding, positioning, packaging and media. With the support of a diverse multilingual research staff representing over 20 different countries and cultures, Cheskin focuses on helping clients gain an intuitive and analytical understanding of their customers in multicultural markets. They in turn use that understanding to develop relationships based on trust, uniqueness and mutual benefit.

For more information on Cheskin Research or to learn more about how we can help you connect with your customers and markets, visit our website at www.cheskin.com, or contact us at:

Phone 650.802.2100

Fax 650.593.1125

Email: info@cheskin.com

1999 eCommerce Trust Study

A free copy of last year's collaborative study on e-commerce trust by Cheskin Research and Studio Archetype/Sapient, referenced in this study, can be downloaded at www.sapient.com/cheskin/.

Upcoming TrustIndex Study

How trustworthy is your website or brand? Cheskin can help you learn the answer to this increasingly important question. Our TrustIndex study can quickly and cost effectively assess your site or brand's strengths and weaknesses in a variety of areas directly related to trust. Contact Steve Diller at sdiller@cheskin.com for cost options, timing and availability.

Other available studies

We enjoy exploring issues that we think others ought to be thinking about. With our publicly released studies we hope to inspire further conversation and exploration into these areas. To see previous studies we've released, visit our website at www.cheskin.com/think/thinking.html.

Table of Contents

Background: The Necessity of Trust4

Research Objectives5

Research Methodology6

 The New Study - 20006

 The First Study - 19996

Highlights of the Study7

Detailed Findings10

 1. The Way Consumers See the Online World10

 Database security11

 The Perception of Surveillance12

 A Strong Sense of Risk16

 2. The Ways Websites and Others Try to Affect Trustworthiness18

 Laws and Government18

 Private Institutions18

 Design Options23

 3. The Ways Consumers Respond to Websites' Efforts26

 Comfort and Acclimation26

 Online Buying Behavior26

 Most Trusted Websites29

 Most Trusted Website Categories30

Demographics of the Sample in the Two Trust Studies32

TRUST IN THE WIRED AMERICAS

Background: The Necessity of Trust

As the Internet develops and matures, its success will largely depend on gaining and maintaining the trust of visitors. Such trust will be paramount to sites that depend on consumer commerce.

The concept of trust is crucial because it affects a number of factors essential to online transactions, including security and privacy. Trust is also one of the most important factors associated with branding. Without trust, development of e-commerce cannot reach its potential.

In a joint research project conducted by Cheskin Research and Studio Archetype/Sapient and released in January 1999, the factors that produce a sense of trustworthiness on a website were identified. In a follow-up study begun early in 2000, Cheskin Research probed the dimensions of online trust across the Americas.

While the US leads the way in terms of growth of e-commerce, the rest of the world may only be a few clicks behind. Little is known about the online population in Latin America and Brazil except that they are entering the online world rapidly. IDC projects that the online population in Latin America will more than double to 29.6 million by 2003. By linking the learnings in both studies, our understanding of the nature and dynamics of website trust can be dramatically enhanced.

Research Objectives

The new Cheskin “Trust in the Wired Americas” study was undertaken to extend the learning from the initial Trust Study, where the specific elements that communicate trustworthiness in e-commerce sites were identified. The new research explores the dimensions of online trust in the US, Spanish-speaking Latin America and Brazil. Specific objectives include:

- Exploration of how trust online is viewed among the online population in the Western Hemisphere;
- Identification of the most trusted websites in the Americas;
- Investigation of the most recognizable and trusted symbols of online security in the Americas; and
- Comparison of online behavior between users in the US, Spanish-speaking Latin America and Brazil.

This report brings together the information acquired in the new Trust study with that from the first study. The ultimate goal is to provide a comprehensive picture of consumer attitudes about trust, and the ways in which a sense of trustworthiness can be enhanced. Like our first Trust study in 1999, we offer this current study as a pioneering piece examining this vital issue and inspiring continued conversation.

Research Methodology

The New Study - 2000

An online survey was conducted among 2,681 Internet users including 1,837 from the US, 522 from Spanish-speaking Latin America and 248 from Brazil. Respondents were asked a series of questions about:

- Privacy and trust online;
- Their most trusted websites;
- The most familiar seals of approval (e.g., VISA, TRUSTe etc.);
- Their online behavior; and
- Their demographic characteristics.

Note: For the purposes of this report, respondents from Spanish-speaking Latin America will be referred to as “Latin Americans” and respondents from Portuguese-speaking Brazil will be referred to as “Brazilians.”

The First Study - 1999

A four-phase process was employed to acquire the understanding sought:

- Phase 1: Snapshot of Consumer Attitudes
- Phase 2: Secondary Research
- Phase 3: Expert Interviews. This and the first two Phases were used to develop a hypothetical model of the building blocks of trust. Then, the model was validated in Phase 4.
- Phase 4: Quantitative Evaluation. In this Phase, eight commercial Websites were selected by Studio Archetype and Cheskin that represented the “strong” and the “weak” for the three key components of Web trust identified in earlier Phases: brand, fulfillment and navigation.

In addition, respondents evaluated the trustworthiness of many additional sites, as well as “seals of approval” such as VISA and VeriSign. Altogether, 463 Web users and a wide range of experts in the worlds of e-commerce, website development and academia contributed to the 1999 study. To access the study in its entirety, please see <http://www.studioarchetype.com/cheskin/>.

Highlights of the Study

1. A Sense of Anarchy Permeates Attitudes about the Web

Across the Americas, consumers believe that there are essentially no rules to the way information is managed and protected across cyberspace. In the absence of such rules, consumers feel a heightened sense of risk when engaging in transactions.

2. The “New Risk” in the Online World

In cyberspace, consumers encounter a new type of risk – *identity risk*. This risk involves the possibility of misuse of personal information by a wide variety of individuals and institutions. For most consumers, the key concern involves hackers making their way into corporate and governmental databases. People consider security of their identity as important as the security of their money. Web commerce may never reach its true potential until this new risk, unknown to any previous model of commerce, is successfully minimized.

3. Big Brother is Watching

Perceptions of online privacy vary slightly across the Americas. Online users in the US believe privacy is mostly non-existent. Latin Americans and Brazilians are a little less cynical about online privacy. Governments are widely believed to be able to easily monitor everyone’s activities. Those same governments are also seen as unable to protect anyone’s privacy.

4. “Little Brothers” Can Ease the Fear

The perception that it’s not the government who’s overseeing our every move online, but rather, marketers and advertisers, has given rise to the idea that it’s not “Big Brother” but websites themselves (“Little Brothers”) who are really watching. In addition, they are seen as ineffectual in the face of hackers. Websites can ease fear by stressing that personal information is treated with care and by prominently displaying assurances of the use of secure technologies.

5. Younger Expert Users Will Consider Trading Privacy for Lower Prices

For the most part, people are not yet willing to sacrifice their online privacy for the sake of a better price. However certain groups of consumers across the Americas are more willing to trade privacy for lower prices. Those who consider themselves Internet experts, between the ages of 19 and 25, particularly males in this category, were willing to make this trade.

6. Private Institutions Enhance Financial and Functional Trustworthiness

The Seals of Approval of some private institutions, including banks and privacy organizations, significantly reduce the sense of financial risk, especially for newcomers to e-commerce. Credit card companies are at the top of this list for those less comfortable with web commerce. VISA is the most trusted symbol in Latin America, while TRUSTe ranks highest in the US. Websites should consider clearly displaying credit card symbols on their homepages in order to enhance the communication of trustworthiness.

7. Cultural Differences Require Different Responses to Minimize Risk...

US and Brazilian consumers tend to be more cynical about the ability of governments and websites to control identity and other forms of risk than Spanish-speaking Latin Americans. At the same time, Latin Americans and Brazilians gain more from the presence of credit card symbols on sites than US residents do. These differences in perception, as well as many other distinctions, will require that website companies and other organizations concerned with security begin to tailor their efforts to the specific perspectives of each region more fully.

... and A Global Market Requires Universal Symbols of Security

Some security-oriented seals of approval reduce the perception of at least some types of risk. VeriSign is a recognized symbol of security, to a certain degree, across the Americas. It's likely that the reason is in part due to the similarity of the name "VeriSign" to "verdad," the Spanish word for "truth" ("verdade" in Portuguese, and in Latin "veritas"). TRUSTe, in contrast, isn't nearly as readily recognized in Latin America and Brazil as it was in the US. Other symbols, such as TRUSTe, will need to consider symbols that can be understood globally. All security symbols need to do more to communicate an ability to provide some measure of identity security.

8. Six Design Elements Communicate Reduction of Functional Risk

Effective branding, navigation, fulfillment, presentation, up-to-date technology, and seals of approval constitute the essential formal characteristics of sites that can be trusted to deliver what consumers want. These forms, in turn, can be divided into a total of 28 components that can be used to communicate functional trustworthiness.

9. Effective Navigation Must be Present to Communicate Trust...

Effective navigation is a necessary pre-condition to successful communication of a site's trustworthiness. Having a well-known brand is also tremendously important. Generally speaking, effective navigation combined with a well-known brand is the best way of communicating trustworthiness. Combining strong navigation with effective fulfillment can also achieve this.

... and a Lesser-Known Brand Must Have Quality Navigation and Fulfillment to Compete

For lesser-known brands, navigation of and fulfillment from their website play significant roles in establishing trust. Any new Web-based brand **MUST** build in excellent navigation and fulfillment if it is to be trusted.

10. Website Categories and Trust

A few key website categories are repositories of consumer trust. This trend cuts across geographic boundaries. A few notable regional trends include:

- Brazilians trust bank websites more than others types of websites;
- Latin Americans trust search engines more than other sites;
- Retail is emerging as the most trusted category online in the US; and
- Retail ranks second in both Latin America and Brazil, suggesting they are on the heels of the e-commerce trend in the US

11. Most Trusted Websites Across the Americas

Yahoo! is the clear winner in the US as the most trusted website, and ranks closely with Hotmail/MSN in Latin America. In Brazil, however, the top two most trusted websites are banks, possibly due to the fact that they often function as ISPs to account holders. Amazon makes a good showing on all three lists. Across the Americas, over 600 different websites were mentioned as most trusted.

Detailed Findings

1. The Way Consumers See the Online World

The study of trust in commercial transactions long ago recognized four types of risk consumers seek to reduce, as follows:

- financial (risk of losing money or paying too much)
- functional (risk of receiving the wrong or a malfunctioning product);
- social (risk of using a product that reflects poorly on its user); and
- physical (risk that we might be harmed by the product).

It's generally recognized that, in order to comfortably purchase, consumers look for cues that tell them risk has been reduced to tolerable levels. When risk reduction reaches a certain threshold, trust becomes easier to give.

The perception of risk reduction can happen in a wide variety of ways, from government regulation to the actions of market forces. Regardless of how it occurs, though, risk reduction generally includes some sort of consistency and order in a marketplace.

Information Anarchy Online

In the case of the current development of the web, there is a perception of anarchy when it comes to information management regardless of age, gender, expertise or region. Web users generally feel that the online environment is an uncontrolled place where almost anything goes. They also feel that websites are not held to a very high standard of consumer protection. These attitudes are consistent across all geographic regions.

	Total Sample
Personal information I give on a website may be sold for marketing purposes	6.3
The information may be sold to another company or website	6.5
A great deal of information about me is gathered without my permission	6.2
Abuses of personal information are rampant	5.7

Note: Mean scores are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

Database security

One notable exception to the general consensus about anarchy in the online environment was found in the perceptions about database security. There are significant differences by region in perceptions of the security of personal information kept in databases. This may point to perceptual differences in what a database is, and how information is stored.

	US	Latin America	Brazil	Total Sample
"Personal information I give on a website resides on a server or in a database that is secure from unauthorized people, such as hackers."	3.8	5.3	3.3	4.1

Note: Mean scores are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

This finding suggests that a website can boost trust among users by clearly addressing how it handles database security. Given the generally low level of trust in the security of databases, websites that offer the security of a "banker's vault" will go a long way toward promoting trust.

Recommendations:

Websites should communicate to users that they take database security seriously, and that they have measures in place to protect the information in their databases. It should be clear to website visitors from their first contact with the site that database security is priority one.

One way websites might accomplish this is by developing specific seals of database security which can be placed on the site to symbolize a high standard of protection of information.

Another way to communicate the seriousness of efforts to protect information stored in databases is to place links to security statements on the site. These would be statements spelling out what level of security is being offered. In this way, users can read more about what measures are being taken to protect their personal information.

It will become increasingly clear that far more needs to be done to secure databases against intrusions from hackers. It may be that such efforts will require international cooperation. A forum for discussing the issue needs to be established, if not by governments, then at minimum by the major website and software players.

The Perception of Surveillance

Privacy online as compared to the telephone

There was a great deal of skepticism across the board about how much privacy exists on the Internet, with a few notable exceptions.

People in the US don't believe that email and instant messages are as private as a phone call. But among Latin Americans and, to a slightly lesser extent, those in Brazil, email and IM's are believed to approach the privacy level of a phone call.

	US	Latin America	Brazil	Total Sample
Email is just as private as a phone call	4.8	6.8	5.8	5.3
Instant message is just as private as a phone call	4.8	6.9	5.8	5.3

Note: Mean scores are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

Internet access in Latin America is largely being provided by telephone companies. The recent joint venture between Microsoft and Telmex, to expand Internet access in Mexico, may help explain why Latin Americans associate the Internet more closely with the telephone than do people in the US. Another explanation may be that Latin Americans are less exposed to the media hype surrounding Internet and email privacy than are people in the US.

“Big Brother”

There is general agreement among users that one's activities online are monitored by the government. Among those in the US, the belief that the government can track online activities is significantly higher than among those in Latin America or Brazil.

	US	Latin America	Brazil	Total Sample
The government is able to track where we go on the Internet	7.2	5.3	6.0	6.7
When you are online your activities are monitored	5.9	5.1	5.5	5.7
Public office seekers and holders can get information about me	5.4	5.6	5.8	5.5

Note: Mean scores are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

The differences found between people online in the US, Latin America and Brazil probably represent basic cultural differences simply extended to the Internet.

People in the US have far more exposure to the Internet environment, from its early days to today's rapid growth. Media reports in the US have often highlighted examples of online monitoring and abuses of personal information. This may affect perceptions among users in the US and may lead to a sense of being “jaded” about the probability of online surveillance.

“Little Brother”

The perception that it’s not the government who is overseeing our every move online, but rather, marketers and advertisers, has given rise to the idea that it’s not “Big Brother” but “Little Brother” who is really watching. Some have predicted that the value added through innovations such as *personalization* may overcome consumers’ resistance to Little Brother’s online surveillance. The findings here do not support this prediction. For the most part, people are not yet willing to sacrifice their online privacy for the sake of price or personalization.

	US	Latin America	Brazil	Total Sample
The biggest threat online comes from marketers and advertisers who might sell my name to other companies.	6.5	6.5	5.7	6.4
I would not mind giving more personal information on a website if I could get a better price on purchase	4.4	4.1	4.3	4.3

Note: Means are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

Younger Experts and Privacy

There are certain customer segments, however, that are more open to exchanging their personal information for price reductions. Regardless of region, self-described Internet experts who are between the ages of 19 and 25 are much more likely to make this trade; males of this segment even more so.

"I would not mind giving more personal information on a website if I could get a better price on a purchase."

Respondent profile	Mean
Beginner Internet users	4.0
Expert Internet users	5.1
Expert Internet users, 19-25 years old	5.8
Expert Internet users, 19-25 years old, male	6.1
Expert Internet users, 19-25 years old, female	5.3

Note: Means are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

These respondents are among those with highest confidence in their online skills. Since they feel less vulnerable than people with less experience, they may be more willing to make a trade of personal information for price reductions because the risk seems manageable.

These people with more online experience may also represent early adopters. If this is the case, it bodes well for the future of personalization online. It may be that, as people become more comfortable online, they will feel less vulnerable and more willing to trade information for personal benefits. It may also be the case that, because they grew up with the technology, they simply have a greater degree of comfort with the “rules.”

Recommendations:

The study identified two ways in which sites can ease fear. First, it should be made plain that personal information is treated with care. In addition, sites can explicitly promise not to use personal information for marketing or other purposes unless consumers agree to it, in exchange for a tangible financial benefit. Clearly allowing users an opt-in/opt-out preference is important. Also, several sites have already begun to give consumers access to a portion of their personal profile data. An expansion of this policy could be highly beneficial.

Second, sites can stress their use of effective firewalls. Websites should consider developing seals of database security and displaying them prominently on the homepage. There should also be links to database security statements consumers can easily access and read. The key isn't the elimination of risk; it's the reduction of risk.

It's worth noting the approach the Europeans are taking. Currently, their primary focus has been on preventing misuse of personal data by the websites that collect such information. Although such efforts may succeed in reducing identity risk to some extent, they ignore the more frightening issue of hackers invading database security. In the future, the protection effort will clearly need to be broadened in some way.

A Strong Sense of Risk

Despite willingness among a small segment of consumers to trade personal information for lower prices, the perceived, overall sense of risk posed by the Internet seems to be universal. There are no significant differences found based on age, gender, income, online expertise or geographic region.

However, not all threats are equal. The perceived threat from hackers is substantially greater than the perceived threat from institutions. This threat primarily involves a risk to one's personal information, though financial risk is close behind.

Predatory Individuals

The biggest threat is from:	Total Sample
Hackers who will steal my personal information	8.1
Hackers who will steal my money	7.6
Dishonest companies or people who might cheat or con me	7.5
Politicians who will get personal info about me	4.8

Note: Mean scores are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

Predatory Institutions

The biggest threat is from:	Total Sample
Dishonest companies or people who might cheat or con me	7.5
Marketers and advertisers who will sell my name	6.4
"Unfulfillment" -- can't return an item you bought	5.9
Insurance companies who will get personal info about me	5.4

Note: Mean scores are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

As noted earlier, users feel personal information is often sold to marketers and advertisers, and that abuses are rampant. However, they don't worry about the threat from institutions as much as the perceived threat from individuals. There may be a level of acceptance of institutional "threat," but a more visceral fear of the "threat" from individuals.

Recommendations:

Websites that can offer users a sense of protection from the threat posed by “individual” intruders will go a long way toward enhancing their trustworthiness.

One way they can do this is by telling consumers what types of technology and legal protections they offer. Another way involves periodically communicating any upgrades and enhanced protections that are implemented on the site.

2. The Ways Websites and Others Try to Affect Trustworthiness

Within the fields of website development and e-commerce, a wide variety of efforts have been made to reassure consumers about all five types of perceived risk in the online world. The consumer responses to those efforts are discussed below.

Laws and Government

There is little faith that the legal system or the government offers protection to individuals online. However, as the chart below indicates, the primary reason for such low expectations of government is a belief that protection simply isn't possible.

I believe that:	Total Sample
Protection of my personal information is impossible	6.1
Websites are free to do what they like with my personal information	4.0*
Personal information is protected by privacy laws	4.7
There are international laws governing how personal info is handled	4.1
The legal system protects my personal information online	3.4

Note: Mean scores are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

* The belief that websites are free to do what they want with personal info is higher (4.4) among people in the US.

Private Institutions

Although there is little evidence that people trust the government or the legal system to protect them online, many respondents feel that private institutions, namely, credit card companies, lower financial risk if not other types of risk.

If someone uses my credit card online without my permission, I will be liable for 100% of the	Internet Use			Have Purchased Online		Total Sample
	Light	Medium	Heavy	Yes	No	
		4.3	3.3	3.4	3.3	3.9

Note: Means are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

Less than a quarter of the overall sample strongly believed they would be liable for 100% of the amount if someone used their credit card online without their permission. There were no significant differences in this belief based on age, gender, expertise or region.

Recommendations:

It appears that credit card companies play the biggest role in offering a sense of security and protection in online financial transactions. Websites should clearly display credit card symbols on their sites in order to enhance trustworthiness. The credit card companies have a major opportunity to be lead in building online trust, by emphasizing that they cover all of the risk.

Recognition of "Seals of Approval"



Of the 5 seals tested, the Visa symbol was most recognized overall, followed by MasterCard, TRUSTe, VeriSign, and BBBOnline.

Visa and MasterCard were universally recognized throughout the Americas. TRUSTe and VeriSign, well-known "security symbols," were more highly recognized in the US than in Latin America, and VeriSign was more highly recognized than TRUSTe in Latin America. BBBOnline was also more highly recognized in the US than in Latin America, however it was the least recognized symbol in all the Americas.

This represents a change from 1999 for all seals. Recognition of Visa, TRUSTe, VeriSign and BBBOnline all increased among US users, while recognition of MasterCard decreased. TRUSTe's recognition increased most dramatically, by nearly 60 percentage points.

The numbers below represent the percentage of individuals who recognize seals of approval. As the chart indicates, overall recognition of seals of approval increased rapidly from 1999 to 2000.

Have seen	US 1999*	US 2000	Latin America	Brazil	Total Sample
Visa	70%	89	90	85	89
MasterCard**	79	63	77	67	66
TRUSTe	10	69	26	20	56
VeriSign	36	59	39	40	53
BBBOnline	18	37	16	12	31

* Data from the 1999 Trust Study conducted by Cheskin and Studio Archetype/Sapient.

** The Visa and MasterCard symbols from year to year were not identical.

Privacy Statements Irrelevant

Very few respondents claimed to have read the privacy statements associated with each symbol. Visa's statement recognition scored highest overall, with TRUSTe following. Credit card privacy statements are read more in Latin American countries than security symbols' statements. This may be due to the higher familiarity of these logos and institutions in Latin America.

The chart below indicates the relative insignificance of the statements attached to specific seals of approval.

Have read Statement of:	US	Latin America	Brazil	Total Sample
Visa	27%	29	18	27
TRUSTe	25	5	2	19
VeriSign	21	11	10	18
MasterCard	15	22	13	16
BBBOnline	10	3	0	8

Effects on Perceived Trustworthiness

Compared to finding from the 1999 eCommerce Trust study, perceived trustworthiness has increased significantly in the US for all Seals of Approval, particularly TRUSTe, VISA and BBBOnline. While VeriSign elicited the highest trust response last year, TRUSTe now ranks higher.

Significant differences are seen between the US and Latin America in perceptions of symbol trustworthiness.

Security Symbols Matter in the US. Security symbols increase trust more than credit card symbols in the US. Of these, TRUSTe rates highest, while MasterCard rated lowest.

Credit Card Symbols Matter in Latin America. VISA is significantly the most trusted symbol in Latin America and Brazil. Security symbols have far less significance than credit card symbols. Of the three security symbols tested, VeriSign did rate significantly higher than TRUSTe. This may be due to the word itself, which in Spanish can appear related to the word “verdad” (“verdade” in Portuguese), or the concept of truth.

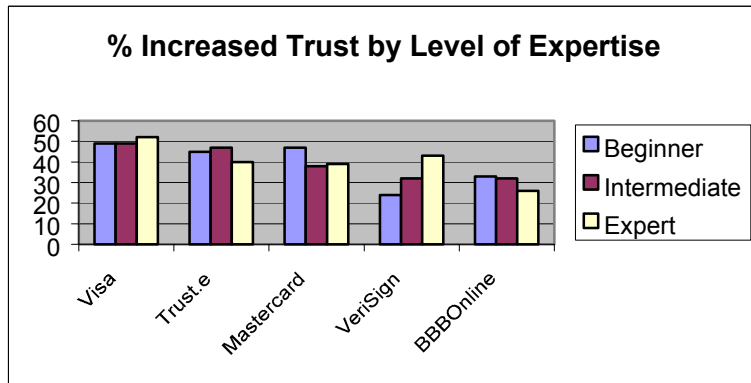
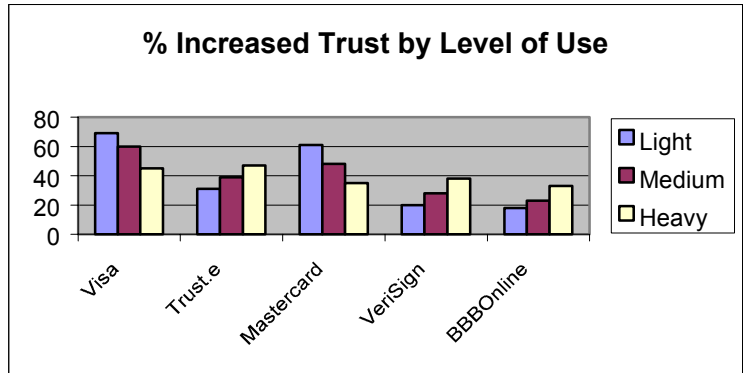
The chart below indicates the percentage of people who feel the presence of a particular symbol increases the trustworthiness of a site.

Percent Reporting Increased Trust					
Symbol	US 1999*	US 2000	Latin America	Brazil	Total Sample
VISA	11%	38	80	78	50
TRUSTe	9	55	19	19	45
MasterCard	13	27	72	65	40
VeriSign	25	38	25	32	35
BBBOnline	16	40	04	05	30

* Data derived from 1999 study conducted by Cheskin and Studio Archetype/Sapient.

The Greater the Experience, the Less the Need for Seals of Approval

As illustrated in the two charts below, one's experience online tends to be related to the amount of trust a seal of approval offers. Light users, those with less expertise and those who have never purchased online, agree that credit card symbols, especially VISA, would increase their trust. Additionally, younger users, age 25 or less, report that credit card symbols inspire more trust than security symbols. On the other hand, heavy users of the Internet agree that security symbols would increase their trust, more so than for light or medium users.



Recommendation:

In order to attract newcomers to websites, the seals of approval need to be easily seen. In particular, credit card symbols can be helpful. Over time, users may become somewhat inured, but the seals are crucial for those coming online without prior exposure and experience.

Design Options

Building Blocks of Trustworthiness

The 1999 study identified six primary components of websites that play a major role in communicating trustworthiness when well-designed:

- Seals of Approval
- Brand
- Technological sophistication
- Navigation
- Presentation
- Fulfillment

The six primary components break down into a total of 28 different ways in which trustworthiness may be established. Each are briefly addressed in the following chart.

SEALS OF APPROVAL	Information about other companies that specialize in assuring the safety of Websites
Network Level 1	Icons symbolizing security of the computer network as a whole, such as TRUSTe, or VeriSign
Network Level 2	Text accompanying the icons
Technology Level 1	Icons symbolizing commerce-enabling functions, such as MS Commerce Server, ICAT, IBM e.business mark, and Browser compatibility marks
Technology Level 2	Text accompanying the icons
Merchant Level 1	Icons symbolizing merchant service security like MasterCard, VISA, Amex
Merchant Level 2	Text accompanying the icons
BRAND	Importance of the company's reputation in choosing to do business with them
Overall Brand Equity	Consumer awareness of what this company does for consumers outside of the Web
Web Brand Equity	How well the company's Website fits with consumers' sense of what the company is about generally
Benefit clarity	On one's first visit to the site, how easy it is to discern what the site is promising to deliver
Portal/Aggregator Affiliations	Mention of an affiliation to portals and aggregators such as Yahoo!, eXcite, ivillage, Lycos, etc.
Co-op Third Party Brands	Promotion of "third-party" quality brands
Relationship Marketing	Sending updates and other notices to consumers
Community Building	Facilitating interactions between individual shoppers
Depth of Product Offering on the Site	How many varieties of product types the site contains
Breadth of Product Offering on the Site	How many types of products the site contains
NAVIGATION	The ease of finding what the visitor seeks
Navigation Clarity	Terminologies for navigation and content are apparent for the user to differentiate
Navigation Access	The navigation system placement is consistent, persistent and easy to find.
Navigation Reinforcement	There are prompts, guides, tutorials, instructions to aid and inform the user to perform transaction and or search task on the site.
FULFILLMENT	The process one works through from the time a purchase process is initiated until the product is received
Protection of Personal Information	The information one provides is guaranteed to be used for no purpose other than what one gave it for, without their approval
Tracking	The site provides feedback or a confirmation number once the order is placed
Recourse	The transaction process allows for recourse if one has a problem at any time during the process
Return Policy	How clearly the return policy is explained
Simplicity of Process	How simple it is to buy something
PRESENTATION	Ways in which the look of the site, in and of itself, communicates meaningful information to you.
Clarity of Purpose	The visuals/layout effectively convey the idea and the purpose of the site. Consumers would know they can purchase products when they get to the site
Craftsmanship	The degree to which, when one first views the homepage, one believes that the Website developers were skilled in their efforts
Resembles other Trusted Sites	How much the site resembles others consumers have come to trust
TECHNOLOGY	The ways in which the site technically functions
Functionality	Overall, how well the site seems to work
Speed	How quickly each page, text and images appears

The six different major components that communicate trustworthiness interact with each other in complex ways. The 1999 study sought to determine how three of them – brand, navigation and fulfillment – interact. It's important to note that these six components, when handled correctly, will largely defuse the four traditional risks of commerce. They don't, however, necessarily deal with the issue of identity risk.

The findings from the 1999 study are summarized below.

Effective Navigation Is the Key to e-Commerce Trust

Effective navigation and a well-known brand, when viewed as isolated elements, both communicate trustworthiness. Fulfillment, viewed in isolation, has relatively little impact.

When they are viewed as interacting elements, though, the picture changes. Strong navigation can best be understood as the foundation of communicating trustworthiness. Generally speaking, effective navigation needs to be joined to either a well-known brand or effective fulfillment if consumers are going to perceive the site as trustworthy. As long as effective navigation is one of two components in place, a site is significantly more likely to be considered trustworthy than a site with only one component in place, or a well-known brand with strong fulfillment but weak navigation.

However, even when a site has a well-known brand, is easily navigable and offers a simple transaction process, it still may not be considered more trustworthy than sites without all three components in place. For instance, a site with a well-known brand, strong navigation and strong fulfillment was found to be less trustworthy than a site of another well-known brand with poor navigation but strong fulfillment. In short, even if a company can combine a well-known brand, strong navigation and strong fulfillment, it can't ensure that its site will be perceived as trustworthy if its brand isn't considered trustworthy.

Lesser-Known Brands Must Build Sites with Strong Navigation and Fulfillment

Since newer brands, by definition, are lesser-known, the only way they can compete with better-known brands is to make sure that both navigation and fulfillment work well for visitors. For these brands, navigation and fulfillment are equally important in building trust. As navigation or fulfillment improves, so does trust.

Recommendations:

Any site, if it wants to be perceived as trustworthy, must, at minimum, have effective navigation. In addition, it needs to include either effective branding or simple fulfillment.

3. The Ways Consumers Respond to Websites' Efforts

Comfort and Acclimation

Overall, users report high levels of comfort and acclimation when it comes to getting information on the Internet. This finding holds true across all sub-groups.

However, when it comes to comfort when purchasing online, the US audience is significantly more comfortable purchasing online than Latin American and Brazilian audiences.

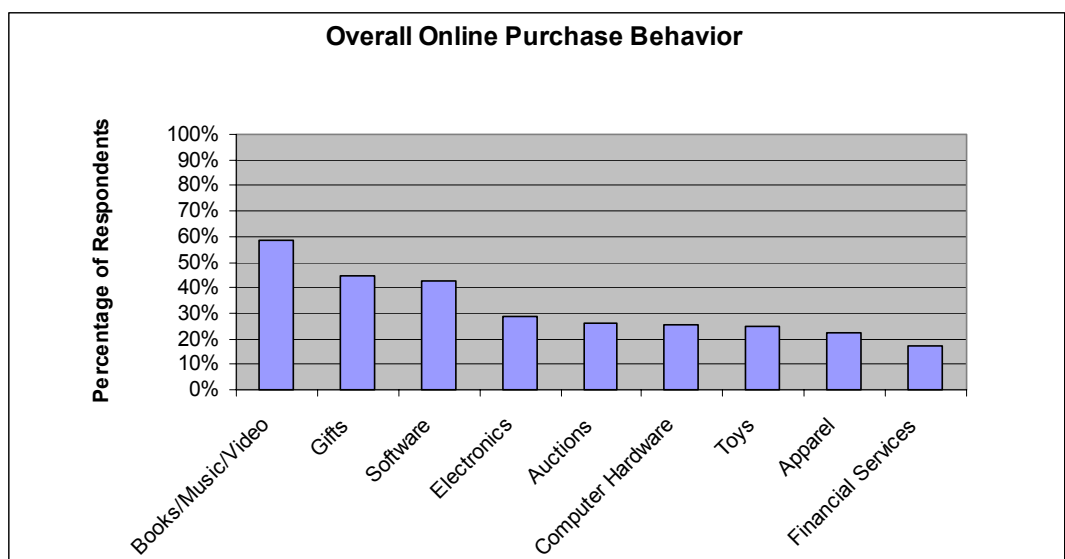
I am comfortable:	US	Latin America	Brazil	Total Sample
Getting information	8.7	9.1	8.4	8.8
Researching products	8.8	8.7	8.4	8.7
Purchasing online	5.9	4.6	4.4	5.5

Note: Mean scores are based on an 11-point scale where 0 means "strongly disagree" and 10 means "strongly agree."

Online Buying Behavior

In total, approximately 75% of the respondents have made purchases online. Books, music, video, and software are among the most popular online products purchased. Financial services are the least used, but may have the biggest potential, since financial service websites were among the most trusted. It seems clear that the four traditional risks have been successfully addressed by at least some e-tailers, who have made extensive use of effective branding, seals of approval, and well-designed navigation or fulfillment.

The chart below shows the percentages of total respondents who made purchases of various types of products.

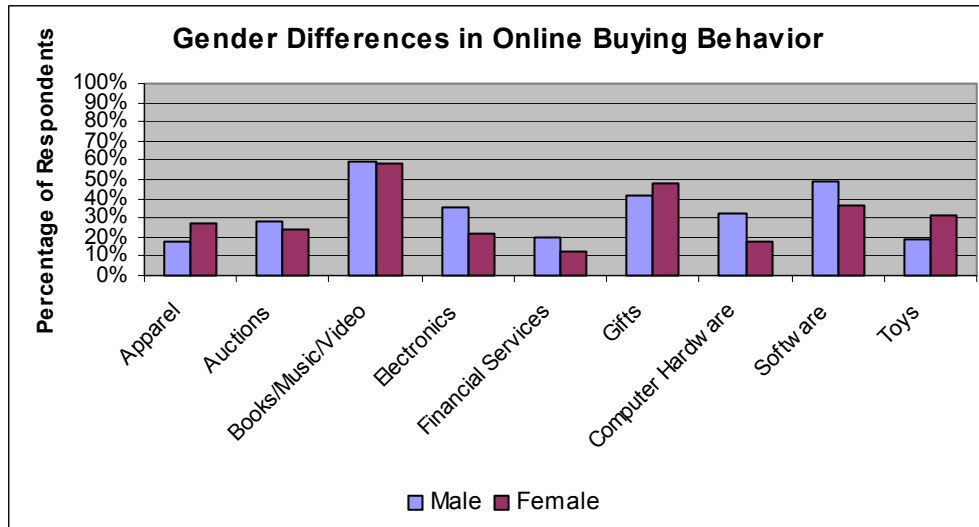
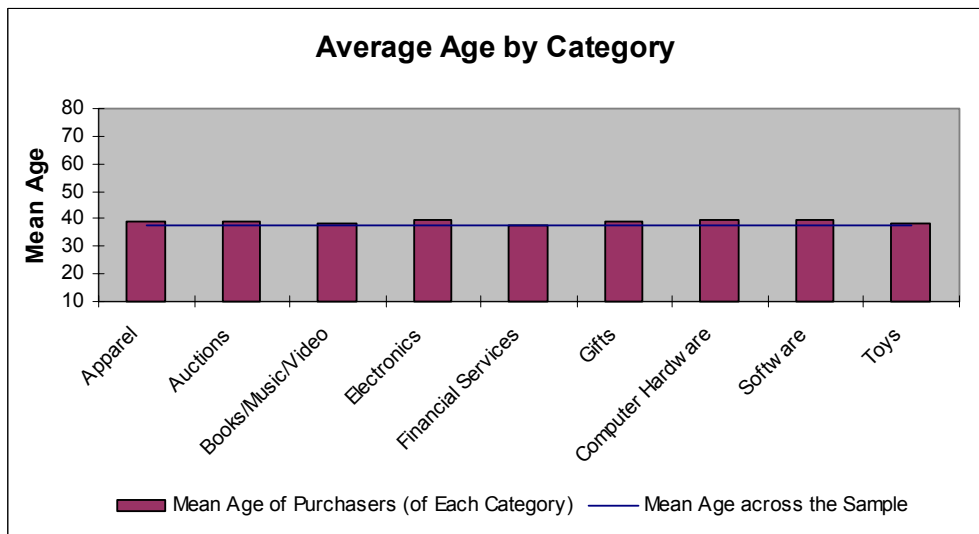


Demographic Profiles of Online Buying

Five demographic characteristics are investigated in the survey, including age, gender, income level, technical expertise and country of residence. Some demographic influences are more significant than others. Overall, gender and country of residence have a stronger influence than age, technical expertise and income on consumer purchase behavior. The role of “trust” in category purchase patterns seems less significant than the demographic differences themselves.

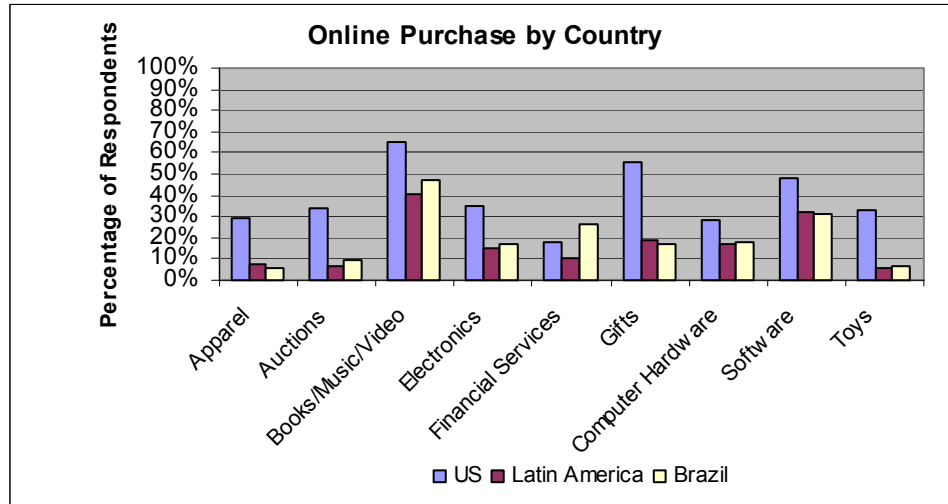
Age and Gender

The charts below show the influence of age and gender on buying behavior online. Age and gender are not strong factors, however. Slightly more men over age 38 buy computer hardware, software and electronics, while women generally purchase more apparel and toys.



Country of Residence

The chart below shows that US consumers are consistently more active in their online purchases than Latin Americans and Brazilians for most product categories. This is not surprising given the origins of e-commerce in the US



With a few exceptions, it appears the patterns of online buying beyond the US borders are generally following the trail being blazed in the US. E-commerce in Latin America and Brazil may likely evolve much the same as it has in the US in terms of consumer demand.

However, in terms of facilitating the transactions for buying online, there may be substantial differences due to the low levels of credit card activity in Latin American countries. To the extent that e-commerce can find ways to facilitate the transactional side of e-commerce in Latin America, the consumer demand for products and services will likely follow. The research strongly suggests that, if credit cards don't become central to online buying in Latin America, e-tailers will need to find another way to reduce financial risk. Understanding the differences in fulfillment issues across cultures will be critical as well.

Most Trusted Websites

Yahoo! is the clear winner in the US and shows up strongly in Latin America as does Hotmail/MSN. In Brazil, however, the top two most trusted websites are banks. This may be due to the fact that banks often serve as primary consumer ISPs to account holders in Brazil. Amazon makes a good showing on all three lists.

The chart below indicates the relative ranks of the top most trusted sites in each of the major regions. This was an open-ended question, allowing any possible choice to be mentioned. The most significant finding to note is that while a few sites stand out, responses to this question included a breadth of sites from a variety of categories. In total, over 600 different sites were mentioned in the study, indicating that website trust may be more of a personal issue than currently assumed. No individual site garnered over a 15% response.

US	Latin America	Brazil
Yahoo!	Yahoo!*	Bradesco (bank)
Amazon	Hotmail/MSN*	Bancobrazil
Hotmail/MSN	Amazon	Hotmail
eBay	Starmedia	Zipmail
AOL	Microsoft	Amazon
iwon		Itau.com (bank)
Microsoft		Unibanco (bank)
		Zaz mail

* The percentages of respondents in Latin America who mentioned Yahoo! and Hotmail/MSN as most trusted site showed no significant difference.

Most Trusted Website Categories

The most trusted websites are those with strong brand presence in the online world. This suggests that brand awareness and familiarity continue to drive website trust, a trend which cuts across geographic boundaries.

The chart below presents, in descending order, the most trusted categories of services offered on the web for each of the three regions studied. The dominant players in each category are noted in parentheses.

Top Website Categories		
US	Latin America	Brazil
retail (Amazon)	search engines (Yahoo!)	banks (Bradesco)
search engines (Yahoo!)	retail (Amazon)	retail (Amazon)
financial services	email (Hotmail)	ISPs
banks (no dominant)	banks	email (Hotmail & Zipmail)
incentives (Iwon)		search engines
auctions (eBay)		government
email (Hotmail)		
ISPs (no dominant)		

A number of interesting trends emerge, specific to particular regions, as follows:

- Banks in Brazil have been highly active in cultivating the online banking category, which explains the strong showing of banking websites among Brazilians.
- Search engines are the most trusted category among Latin Americans, which may be an indication of their early stage of experience online.
- Retail emerges as the most trusted category online in the US, most likely reflecting the more advanced stage of online experience.
- Retail ranks second in both Latin America and Brazil, further suggesting they are on the heels of e-commerce trends in the US.

Appendix

Demographics of the Sample

Demographics of the Sample in the Two Trust Studies

The First Study (1999)

- 56% male / 44% female;
- Average age was 30 years;
- Average income was \$38,000;
- Average Web usage was 20 hours per week and;
- 66% of the respondents had made at least one purchase online.

The New Study (2000)

- 52% male / 48% female;
- Average age was 38 years;
- Average income was over \$40,000;
- 61% of the respondents spend more than 10 hours per week online; and
- 75% of the respondents have made at least one purchase online.

Note: Respondents who were more experienced users of the Web were specifically recruited for the first study so they could easily evaluate navigational and design elements on the selected websites. A broader base of respondents spanning several national borders were recruited for the New Study in order to get a comprehensive read on perceptions and behaviors about trust on the Web across the Americas.