Mountain Plains Journal of Business and Technology

Volume 1 Article 5

Date Published: 2000

E-Commerce as a Competitive Advantage for Small Businesses: Overcoming Privacy and Security Issues

Ron Lennon
Barry University

Julisse Oquist
Barry University

E-COMMERCE AS A COMPETITIVE ADVANTAGE FOR SMALL BUSINESSES: OVERCOMING PRIVACY AND SECURITY ISSUES

RON LENNON AND JULISSE OQUIST
BARRY UNIVERSITY MIAMI, FL

I. INTRODUCTION

The Internet and the World Wide Web (WWW) trend have captivated people in every corner of the world. The presence of both individuals and businesses on the Internet grows every day. For example, in 1998 businesses' presence on the Internet grew so much that many described 1998 as the ".com" year. But why is it that the Internet is so attractive to all of us? The reason lies in the ease of use of the Internet, the speed of obtaining results, the amount of information available, and the global reach that the Internet has. For all these reasons, the Internet has become one of the most important marketing strategies available. By publishing information on the WWW, small businesses now have the opportunity to reach millions of people around the world, and more importantly, they can do so for a fraction of the cost of other advertising methods.

So where is e-commerce headed? One of the arguments is that small businesses will move to one-to-one marketing, where small businesses solicit demographic data to offer customized customer service and sales. This will not only increase sales by targeting the right sectors, but also by offering individualized service to current customers. Others argue that e-commerce's global nature will force small businesses to better identify their core competencies to be able to compete in the global market place. One way or another, small businesses are using e-commerce to please the "web customer" who wants reliable and accurate information about products and services any time, any where and at no cost.

II. PURPOSE

The purpose of this paper is to help small businesses understand the major hurdles and obstacles they must overcome to be a competitive force in the E-Commerce marketplace.

III. E-COMMERCE AS A COMPETITIVE ADVANTAGE FOR SMALL BUSINESS

Competitive advantage refers to the ability of a company to respond to the changes in the environment, and develop a strategy that adapts to these changes in order to outperform its rivals and maximize profits. It is important to think about electronic commerce as a way to integrate technology to business processes and improve services, so that market position can be improved as well. At the same time, it is very important to achieve speed, modularity and completeness when using electronic commerce, so that it can be properly implemented as part of the overall corporate strategy. By doing this, small businesses can use electronic commerce to increase flexibility and better respond to market changes.

With the implementation of electronic commerce as a competitive advantage, small businesses can gather more and more reliable information that can be used internally to develop strategies, or can be sold to other small businesses and individuals. Also, small businesses can both improve service and expedite responses to customers, and appeal to and attract new customers. This way, small businesses are both reducing costs and maximizing profits with the use of electronic commerce.

Developing an E-Commerce strategy can be difficult, time consuming and costly for a small business, therefore, instead of "reinventing the wheel", small businesses could model their strategies based on those of medium-large sized businesses. Dell Computer was once a small business and was able to grow through its mail-order strategies, however, Dell, has now also grown into a competitive force in E-commerce.

With the use of Dell's Internet sales system, Dell has been able to achieve strategies that have given them a cost and differential advantage over their competitors. Dell uses an electronic commerce strategy based on providing excellent service to their customers. They do this by providing a "virtual shopping mall" where customers can build their systems with the requirements they want, at the price they can afford, and with the payment method of their choice. Dell Internet sales system also offers the opportunity of processing computer leases online for the convenience of its customers. Once an order has been placed customers also have the opportunity of checking on the progress of the order up to the day the product is delivered. With their Web site, Dell also has the opportunity for knowledgeable customers to obtain support for their systems without having to spend hours on the phone with tech support. They also have created special sites for their "big" customers where employees can download new software to their PCs and order software to upgrade their computers (using company standards) without even leaving their desks. With this sales and support strategy, Dell has been able to differentiate their products by providing outstanding service and support, which in turn has given them an advantage that so far other computer companies have not been able to fully imitate. Today, the direct PC seller's Dell.com site racks up sales of $14 million a day making it one of the busiest vendors

online. These Internet sales make up for almost 50% of Dell's total sales and Dell hopes this percentage will increase to 70%. On average Dell.com receives some 25 million visitors a day. (Dell,1999)

In order to maintain an alive and successful electronic commerce strategy, Dell has announced a new Internet site, Gigabuys.com, hoping to take online computer shopping to a new level. On this site, they will offer customers a wide range of software, peripherals, and accessories as well as Dell systems.

As can be seen, Dell's e-commerce strategies have been able to transform the company into a computer giant in a short period of time. The increase in market exposure as well as the increase in sales made Dell a winner player in the computer industry.

IV. LIABILITY CONCERNS

Most organizations have failed to formulate and standardize laws and regulations that control the liability for the content of what is posted on the Internet. As a result many small businesses have had to face legal consequences for the contents of their web pages or links, even if the persons responsible for the site did not authorize the content posted on the page. Today, liability on the Internet is a serious risk that small businesses have to face; they can be penalized for libelous activities, copyright infringement, pornography and fraud. The problem lies in that it has not yet been established how legally responsible companies are for the content and links to their web pages. Here is a list of what management of a small business can do to protect themselves from possible lawsuits resulting for Web page content:

· Stay abreast of changes in global industry regulations related to the Web. By doing so, small businesses will be able to use these regulations to help create their web pages and will be able to know what content could result in legal reprimands.

· Small businesses should define to what extent they are responsible for the "hot links" in their web pages and the content of the pages it connects to. Similar to advertising in magazines, small businesses need to know who they are doing business with and consider if it is beneficial for their image to be associated with certain organizations.

· Small businesses should have tight controls for regulating what their employees post on line and should establish guidelines for limited or no liability for the content of what employees post without the company's authorization.

· Small businesses should be aware of the changes in technology that can help in regulating the content of what is posted on the company's web page, and the technology that could be used by others to harm the hosting company.

It is only by doing this that small businesses will be able to prevent legal action for the contents of their web pages. As long as small businesses don't have total control of what is actually posted on their web pages and as long as global standards have not yet been developed, small businesses should protect themselves by reducing their liability for the content posted on the World Wide Web.

V. SECURITY AND PRIVACY CONCERNS

The Internet has opened the door to a new economy and a new way to do business for small businesses. The open nature of the Internet, and the ease of gaining anonymity on it, has lowered the cost of entry for scam artists. But the Net also makes the job easier for law enforcement agencies, according to Richard Walker of the SEC. (Crime and Punishment, 1999). It is for this reason that new concerns have arisen about how to protect small businesses and customers from savvy hackers and e-thieves.

One study shows that six million Internet users claim to have been victims of credit card fraud over the web. This number seems very high, but in reality, it only represents 7% of the Internet credit card transactions. This issue scares many consumers. Small businesses need to be able to adapt their e-commerce strategies to deal with this fear. This is crucial for the future of e-commerce because in one survey, about 73% of respondents reported not being comfortable with giving their credit card information to online businesses. (Masterson, 1999). What happens is that most Internet users are unaware of the capabilities of the encryption technologies that most companies offer on their web sites. For this reason, small businesses need to promote their encryption and security capabilities as part of their e-commerce strategy.

In addition to the privacy and fraud concerns, the future of e-commerce also faces the obstacles that the government poses for online transactions. Today, laws in the United States prohibit companies from proliferating the use of state of the art encryption technologies. Government officials feel that this proliferation of encryption technologies could pose a security threat to the nation, and therefore are resistant to change.

Legislation is now being revised in Congress that will allow for the use of sophisticated encryption technologies over the Internet, but so far there has been no resolution. On the other hand, many believe that national laws governing taxation,

encryption, and import over the Net can hold back the growth of the Internet economy.

Based on research conducted in 1999, Figure 1 indicates that a large percentage of online shoppers (53%) are very concerned about the security of online transactions and about giving out private information over the Internet. It is important to note, taking into account the factors in this study, the concern for online privacy and security represents not only the highest percentage alone, but also a higher percentage than all the other factors combined.

It is for these reasons that small businesses especially need to pay attention to their customers concerns and perceptions about conducting transactions online. Addressing these factors can represent the difference between a successful and an unsuccessful Internet presence.

Figure 1

Source: NetZero Report, April 1999

1. SECURITY METHODS

To ensure the security of online transactions, many different technologies have been put in place like firewalls, encryption, and other transaction security methods such as authentication software. Here is a short description of these:

1. Firewalls & Network Security- Firewalls function as the Internet and Intranet traffic cops. They are the first step or "wall" in the security path of a small business. Based on predetermined rules, the firewall determines who and what type of traffic can enter or leave the network. Usually, firewalls allow people in the network to have access to all the outside public networks, but lately many small businesses are restricting this access not only for security reasons, but also for employee control issues. "A firewall is not simply hardware or software, it is an approach to implementing a security policy that defines the services and access to be permitted to various users." (Kalakota, 1997, p. 47).

2. Transaction Security- Refers to the security that online vendors can provide to their customers, which is based on privacy, confidentiality and integrity of the information provided by the customer. These issues are usually addressed with encryption technologies that small businesses utilize to guard their customers' data.

3. Encryption-A technology utilized by online vendors and other companies to create "secret codes" that only authorized users can decrypt and read to prevent critical information from falling into the wrong hands. The goal of encryption is not to prevent hackers from obtaining the message over the network, but to make it impossible for them to read or decipher the content of the message. Many different encryption technologies exist today following the new format of "public-key encryption" where both the sender and receiver receive a different "key" to decrypt the message.

2. DEVELOPING ONLINE SECURITY & PRIVACY POLICIES

It is crucial for any company to consider and to use online security & privacy policies that not only protect the personal information of clients, customers, users, and employees, but also critical company records. To be able to have efficient online security & privacy policies, small businesses must take the following steps:

1) Follow the fair information practices developed by the Organization for Economic Cooperation and Development (OECD) (Merkow, 1999) which states:

a. Guarantee openness: availability to establish the existence and nature of personal information and its purpose.

b. Communicate purpose specification: communicate the purpose of collecting personal information at the time of collection.

c. Agree to collection limitation: collect only information needed for the purpose with the consent of the subject.

d. Agree to use limitation: agree to not disclose information for secondary purposes.

e. Guarantee individual participation: allow subjects to view and correct personal information.

f. Guarantee quality of information.

g. Guarantee security of personal information.

h. Agree to accountability for the security of personal information collected.

2) Hire personnel to be in charge of data security.

3) Restrict physical access to databases containing critical information, by establishing personnel passwords and security badges.

4) Encrypt sensitive and critical information.

5) Conduct systems penetration tests to prevent hackers from breaking into systems.

6) Establish norms for preventing leakage of information.

7) Communicate the policies throughout the company.

8) Train employees never to leave critical information unattended .

9) Establish a schedule for record retention/disposal.

10) Establish procedures for erasing hard disks containing critical information.

11) Mark all confidential material as confidential.

12) Establish norms for disclosing information via cellular phones and e-mail.

VI. CREATING AND MAINTAINING A TRUSTING RELATIONSHIP WITH ONLINE CUSTOMERS

" A report from Jupiter Communications found that 64 percent of online consumers are unlikely to trust a website, even if the site prominently features a privacy policy." (Consumers, 1999). It is for this reason that small businesses need to create and establish strategies for maintaining a trusting relationship with online customers. This way, online customers can feel more secure and relieved about giving out critical information (credit cards, account numbers) online. By maintaining a trusting

relationship, small businesses can increase their online sales with existing customers and create new opportunities with new users. This is more important for smaller companies than for larger ones since the smaller ones usually do not have a widely known reputation or brand name that customers trust.

Following are recommendations for small businesses to build and maintain a trusting relationship with online customers:

· Maintain an ongoing dialogue with customers about security and privacy issues.

· Create trusting relationships with customers.

· Release improvements in technological devices or processes that improve security and privacy.

· Promote online privacy and security efforts.

· Become involved in creating and modifying security and privacy regulations.

· Integrate a strategy of how to build and maintain online customer relationships in the overall company's Internet marketing plan.

Figure 2 shows the results of a study completed in 1999. Based on this research, a large percentage of companies (45%) do not integrate their online customer relationship strategy to their overall e-commerce marketing plan, on the contrary, most companies try to build this relationship reacting to their customers or industry concerns as opposed to planning them. Also, a significant percentage of companies (26%) do not even address their customers security and privacy concerns either in their e-commerce marketing plans or in any other way. Only 29% of companies address security and privacy issues in their Internet marketing plans and follow strategies to minimize online customers' concerns.

Figure 2- Building Customer Relationships

Source: E-Trailers,1999.

VII. SUCCESSFUL E-COMMERCE STORIES

"Security is a sensitive subject that many companies are reluctant to discuss." (IT Security, 1999). It is for this reason that most small businesses that are not up-to-date about security methods tend to avoid the subject, while companies that have spent a great amount of time and money on these methods, tend to promote them heavily. Companies like IBM, Compaq, Hewlett Packard, Microsoft and Intel realized this and as a result became part of an industry alliance to create better security for e-commerce transactions. Security and privacy are such important topics that not only are these companies promoting their own online security methods, but they are also joining in the research for the development of new technologies. These companies recognize the immense opportunities lost everyday due to online customers' security and privacy concerns. This alliance has realized that the success of e-commerce transactions is found in the level of confidence of the customer, and in satisfying the areas of authentication, privacy, and non-repudiation.

Table 1 shows a group of companies that have implemented and promoted security and privacy methods, and the results they have obtained from these methods:

Table 1 - Security and Privacy Services

COMPANY	PRODUCTS	PRICING	CUSTOMERS
BBB Online Arlington, VA	Applicants for the BBB Online Privacy seal, or the stricter Kids' Privacy seal, must promise that their own data practices match BBB Online's privacy policies, such as giving customers a chance to opt out of information collection. The program leans heavily on self-regulation.	The initial application fee is $75. To cover multiple sites, add $10 per URL. For a separate policy on each site, there is a per-domain license fee based on company revenue.	Forty-seven companies have received a total of 51 seals.
CPA Webtrust New York	Requiring an external audit from a CPA, this certification seal is considered the most rigorous of the three "trustmarks"; BBB Online and TrustE are the other two. After an	The cost of an audit depends on a company's size and complexity but is orders of magnitude higher than the TrustE and BBB programs. Webtrust is looking at	So far, 20 companies have received Webtrust seals.

	initial audit, a company must undergo quarterly reviews to keep its certification.	ways to lower its price to make the program more accessible.	
Deloitte Touche Tomatsu Wilton, CT	Like the other big five CPA firms, Deloitte is qualified to award a Webtrust seal. Deloitte's Secure E-Business group works with companies with low regulatory oversight; for financial service, health care and other regulated industries, Deloitte uses its compliance group.	A Deloitte Webtrust certification can range from $40,000 to $250,000, with quarterly updates costing $15,000 to $110,000.	Works on privacy with clients in e-commerce and other highly regulated sectors like health care and financial services. Clients include Arthur Andersen and E-Trade.
Direct Marketing Association New York	The DMA's Web site contains lots of privacy resources, including a questionnaire to help Web businesses create a policy.	These services are offered free to DMA members and nonmembers alike.	More than 4,100 members. Staffers say 1,500 policies were created from Nov. 1998 to May 1999.
Ernst and Young New York	E&Y's E-Risk Solutions offers Web-sites certification. E&Y also helps companies earn a third-party certification, such as Webtrust.	Depending on complexity, E&Y's services range from $20,000 to $500,000.	Roughly 15 privacy customers, including Bell Canada and MatchLogic.
KPMG Montvale, NJ	With worldwide headquarters in Amsterdam, KPMG has a decade of work with European privacy issues. It began its U.S. privacy consultancy two years ago under the auspices of its Information Risk Management practice.	The Privacy Awareness program starts at $25,000 for initial analysis, and can climb to $300,000 or more. A recent client spent $1 million on a data-security implementation.	Customers include First Union Bank.
MSN LinkExchange Redmond, WA	Part of Microsoft's MSN portal, LinkExchange provides	Free to LinkExchange members.	More than 4,000 people or companies have

	a Privacy Wizard - a series of templates to guide you through the process of drafting a privacy policy and posting it on your site. "Write a policy in 30 minutes!" it promises. But be careful: Before making privacy promises, it's wise to get legal advice.		used the Wizard since its June debut.
PricewaterhouseCoopers New York	PWC's Privacy Risk Management group handles privacy and related consulting.	One customer just paid $150,000 for an initial month-long review and $20,000 a quarter for regular reviews.	PWC has done more than 100 "Internet assurance" audits, for companies like E-Loan.
TrustE Cupertino, CA	To earn a TrustE seal, companies must create a privacy statement and comply with a set of standards. TrustE also offers a special seal for meeting children's privacy requirements, which are stricter. Consumers can file complaints on one of the TrustE certified companies, opening an investigation into the company's practices.	Charges a per-domain license fee based on company revenue, ranging from $299 to $4,999. There's a 20 percent discount for nonprofits and discounts for multiple domains.	At least 588 companies have received TrustE seals.

Source: Lash &Black, 1999.

Many companies have implemented security and privacy methods like the ones shown in table 1 and have made great efforts to keep up with technological changes in this area. For example, Amazon.com, American Online and American Express have promoted their security and privacy methods to their clients both online and in printed material. So far there has been no research on the effectiveness of this type of promotion, but the continual success of these websites, it could be concluded that promotion of their security methods influenced online customers to trust these websites.

At the same time, table 2 shows that 85% of the companies surveyed have made an effort to make their customers aware of their privacy and security policies. However, these companies have done so through links on their websites instead of direct promotions. Again, there has been no research conducted in the relationship between sales or profitability of these companies in relationship to those companies who have not implemented and published their privacy and security methods.

Table 2 - Privacy Practices

Privacy Practices at Selected Sites	**Number of Companies**	**Percent of Sample**
Site has link from homepage to privacy policy	39	45%
Site has link from homepage to privacy policy with a section on children's privacy	9	11%
Site has link from homepage to privacy policy including seal(s)	25	29%
Site has a policy but no link from front page	8	9%
Company has no privacy policy or is working on one	5	6%
Total Companies	86	

Source: Lash, 1999.

1. CREDIT CARD TRANSACTION FOR SMALL BUSINESS: AN E-COMMERCE STRATEGY

Credit Card processing has become an essential part of any business on the World Wide Web. Today, most web users expect to go to a Web site see something they like, and have the chance to purchase the item using a credit card. So it is important for every business on the Web to provide credit card processing in their web sites.

But how can a small business be able to offer credit card processing on their web site if they don't have the technological or financial resources to build a very sophisticated web site? Fortunately for these small businesses there is a simple solution. Many companies have emerged that specialize in providing credit card processing for small business at a reasonable cost. These companies use secure transaction technology that consists of software that supports both the cardholder and the merchant sides of the transaction to guarantee both security and authentication. Usually, the customer's credit card information is encrypted using Secure Sockets Layer (SSL) protocol that is implemented by Netscape and Internet Explorer. SSL provides three important things: Privacy, Authentication, and Message Integrity.

In an SSL connection each side of the connection must have a Security Certificate, which each side's software sends to the other. Each side then encrypts what it sends

using information from both its own and the other side's Certificate, ensuring that only the intended recipient can de-crypt it. This way, the other side can be sure the data came from the place it claims to have come from, and that the message has not been tampered with.

The information remains encrypted throughout the transaction except when being sent over dedicated phone lines to the processing bank. This is equivalent to how credit card processing terminals at retailers work today.

Most of the companies that provide this credit card processing service, knowing that small businesses have fewer resources, provide a secure database of credit card numbers at the processing bank instead of having to build a database at the client's site. This also reduces the costs that businesses incur in maintaining and securing the database.

Recently, credit card processing companies have opted for not emailing any of the information used in the transaction to either the merchant or the customer. The reason is that email is a very insecure transaction in which the message is transmitted through non-secure methods that are widely open for anyone to intersect it. Once an order has been placed and the credit card has been cleared, the merchant is sent a purchase order and the customer a receipt. Neither one receives any critical information like the credit card number or the like. The payment is automatically deposited into the business account and it is usually available 24 to 48 hours after the transaction has been cleared.

The cost of this type of credit card transaction processing is on average about 1% of the transactions processed. Added to this, there is usually a $200 - $300 setup fee paid up front. Taking these costs into consideration and comparing them with the increase in sales that small businesses can experience from accepting credit card payments, it is clear that small businesses should invest in credit card processing services.

VIII. CONCLUSION

Electronic commerce is dominating business today worldwide. As a result, both small and large businesses have had to become an active part by jumping into the electronic marketplace one way or another. But the difference between those who have had successful e-commerce stories and those who have not, is greatly characterized by the vision pursued by the e-commerce strategies and the types of security and privacy methods that the companies implemented and promoted on their websites and their overall e-commerce transactions. It is for this reason that companies, especially small companies, need to pay very close attention to maintaining a trusting relationship with their customers so that they won't feel that their privacy is threatened when purchasing

or conducting transactions online. To do so, small businesses should promote their online privacy and security methods as well as become involved with industry research on these topics. It is only in this way that small business can build a trusting image in the e-commerce market.

At the same time, for all the new .com Internet startups it becomes crucial to integrate these privacy and security efforts into their overall strategies and marketing plans.

REFERENCES

· Anthes, Gary H. (1999, September 27).Your Web site may be a Spy Magnet. Computerworld v.33 n.39, pp. 62-63.

· Bloomberg News. (1999, October 11). Big names join forces for e-commerce security. CNET News.com [online], (one page). Available: news.cnet.com/category/0-1007-200-815712.html [1999, October 11].

· Consumers Don't trust web sites. (1999, August 19). Cyberatlas Internet News.com. [online], (one page). Available: cyberatlas.internet.com/markets/retailing/print/0,1323,6061_185931,00.html. [1999, November 19).

· Crime and Punishment: CNET Special Reports (1999, October 14) CNET News.com [online], (two pages). Available: aolsvc.cnet.com/specialreports/0-6014-7-123218.html [1999, October 15].

· Dell Computer Website. Available:dell.com [1999, December 15]

· E-Trailers Lack Customer Relationship Plans. (1999, June 29). Cyberatlas Internet News.com.[online], (one page). Available: cyberatlas.internet.com/big-picture/demographics/article/0,1323,6061_153571,00.html [1999, November 19].

· Gottesman, Ben Z.; Morris, John; Lipschutz, Robert P.;Roberts-Witt, Sarah L; et.al. (1999, September 1) 30 Tips to Protect You and Your Business. PC Magazine v.18 n15, pp. 139-144.

· IT Security Challenge: Protecting the Wired World (1999). White Paper. CIO Executive Intelligence Research. Boston, MA.

· Kalakota, Ravi & Andrew Whinston. Electronic Commerce: A Manager's Guide. Addison-Wesley, Reading, MA. 1997.

· Labich, Kenneth. (1999, July 19). Attention Shoppers: This man is watching you. Fortune v.140 n.2, pp.131-134.

· Lash, Alex (1999, July 23). Privacy, Practically Speaking The Standard.com [online] (seven pages). Available: thestandard.com/article/display/0,1151,5613,00.html. [1999, December 9]

· Lash, Alex and Black, Kathi (1999, July 26). What Price Privacy? The Standard.com [online] (three pages). Available: thestandard.com/article/display/0,1151,5614,00.html. [1999, December 9]

· Lashinsky, Adam. (1999, September 27). The end of the Net honeymoon. Fortune v.140 n.6, p.312.

· Masterson, Michele. (1999, May 20) Study: Six Million Victimized By E-Commerce Fraud. E-Commerce News [online] (two pages). Available: internetnews.com/ec-news/print/0,1089,4_123241,00.html [1999, November 1]

· McCausland, Richard. (1999, September). Cashing in on E-Commerce. Accounting Technology v.15 n.8, pp.36-45.

· Merkow, Mark (1999, September 24). Information Privacy: The other side of the E-commerce coin. E-Commerce Guide [online] (nine pages). Available: ecommerce.internet.com/outlook/print/0,1282,7761_207511,00.html [1999 , November 19]

· Miller, Michael J. (1999, September 1). Are you Really Safe Online? PC Magazine, v.18 n.15, p.4.

· Morris, John; Seltzer, Larry, Haskin, David, Randall, Neill; et al. (1999, September 1). Protect Your PC And Your Privacy. PC Magazine v.18 n15, pp.107-136.

· NetZero Report (1999, April) as cited in: Privacy Survey Results. ZDNet-PC Magazine [online] (two pages) (1999, August). Available: zdnet.com/pcmag/stories/reviews/0,6755,2311786,00.html. [2000, February 10]

· Rash, Wayne. (1999, September 13). Politics and Marketing Team on the Internet. Internetweek v.780, p.78.

· Wilcox, Joe. (1999, September 27). IBM to offer e-commerce security standard. CNET News.com [online], (two pages). Available: news.cnet.com/news/0-1007-202-201240.html [1999, October 11].

· Wilder, Clinton.(1999, September 13). E-Transformation. Information Week v.752, pp. 44-46.

· Wolverton, Tray & Greg Sandoval. (1999, October 12). Net crime poses challenge to authorities. CNET News.com [online], (two pages). Available: news.cnet.com/news/0-1007-202-850601.html [1999, October 14].