Target Markets for Technology Fraud: Who Is Vulnerable?

With the nature of the Internet making it difficult to spot fraud, consumers need to develop a buyer awareness and keep themselves informed on the latest risks of scams and ripoffs with the growing use of computer technology. The panel discusses protections being implemented as well as available resources that consumers may refer to for assistance.

Joan L. Kinney, University of Wisconsin - Madison[1]
Karen P. Goebel, University of Wisconsin - Madison[2]

Katharine Kopp, Senior Policy Analyst at the Center for Media Education (CME), describes the online environment for children with regard to privacy and the collection of personal information. With 14 percent (9.8 million) of all youth online in 1998 and an estimated 42.4 million expected by 2002, the Internet has become the playground for children. Companies in this electronic marketplace view children as prime targets who are avid consumers of electronic media and products and services. So children who influenced the spending of 500 billion dollars in 1997, constitute three markets for business: they buy things with their own money; they are the future market as future consumers; and children's influence has an impact on parents' buying behavior.

CME's research submitted to the 1997 Federal Trade Commission's (FTC) privacy workshop reported 90 percent of the sites analyzed actively collect personal identity information from children with 40 percent of those sites providing incentives such as free merchandise, screen savers and sweepstakes. Often, spokescharacters are used to give the message that you can trust your animated friends. Yet 86 percent of the surveyed sites are collecting personal identity information without obtaining parental consent, and only one site asks children to check with their parents before releasing information. J.D. Power and Associates' poll in April 1997 reported that 80 percent of the net parents said it was not acceptable to ask children their real names and addresses even if that information is only used within the company. That percentage increased to 90 percent when such information is shared or sold to other companies. And 96 percent of the parents said that companies collecting information from children should be made legally liable for violations of their stated policy. Family PC's survey in December 1997 found that 67 percent of the parents were concerned about marketing to children on the Internet. When asked what they found most troubling about the Internet, 88 percent of the parents said it was the use of personal information.

The CME has proposed guidelines for collection limitation; parental consent; disclosure; purpose specification; access, correction and prevention rights; and implementation/enforcement. Children have a right to anonymity and autonomy. If information is collected, parents need to give consent. Sites need to disclose, not only at the home page but wherever information is collected: what information is collected, who is collecting it, who has access to the information, how does the information get collected, how does a parent have means of redress, and how can they get information from the company. Information collected for one purpose should not be used for another purpose. Parents should be able to find out from a company whether information was already collected, to verify the information is correct and, if not, to correct it, and also to prevent future use of that information. These guidelines must be enforceable and punishable.

Policymakers need to be educated. The Federal Trade Commission, following their major analysis of privacy practices, will introduce their recommendations to Congress in June. The Commerce Department will be reporting on self-regulation and privacy to the President in July. CME's intent is to supply further evidence for supporting children's need for special protection.

Phillip McKee, Internet Fraud Watch Coordinator, reports on the National Consumers League's efforts to cover scams in cyberspace. With the creation of www.fraud.org in 1996, consumers from around the world could report and receive tips about fraud. The top ten subjects of reports to Internet Fraud Watch in 1997 include: web auctions (items bid for but never delivered/value of items inflated); Internet services (charges for services not provided or supposedly free); general merchandise (sales of everything never delivered or not as advertised); computer equipment/software (no delivery or misrepresented); pyramids (profits made from recruiting others not sales of goods/services); business opportunities/franchises (empty promises of big profits via pre-packaged opportunities); work-at-home plans (materials and equipment sold with false promise of payment for piece work performed at home); credit card issuing (false promises of credit cards to people with bad credit histories on payment of up-front fees); prizes/sweepstakes (requests for up-front fees to claim winnings that were never

awarded); and book sales (genealogies, self-help improvement books and other publications that were never delivered or misrepresented). There were also plenty of bogus investments, empty travel and vacation offers, fake scholarship search services and illegal advance fee loans.

While many of the scams found online are simply revised versions of the typical telemarketing or mail frauds, the Internet itself creates a whole new set of problems. Anyone can put up a great looking web site making it difficult for the average consumer to determine the site's legitimacy. Consumers buy sight unseen, recourse is not always easy, and consumer protection laws often do not apply. The nature of the Internet makes direct contact of consumers cheaper than ever via mass emailing or posting of messages to different newsgroups allowing crooks to forge headers to mask as well as mislead their real identities and locations.

Creating clear legal ground rules for Internet commerce and the enforcement of those rules are crucial, but public education must be a major component of any effort to curb Internet fraud. Consumers need to know how to check out the offers they see and the companies that make them.

Businesses also need to be educated as to their basic responsibilities. The National Consumers League has taken a leading role on their website in educating the public about Internet fraud by providing a wealth of information on safe cybershopping and tips on how to avoid many different types of common scams as well as warning consumers about new trends, common scams and recent government enforcement actions. Plus consumers can use the web site's links to go directly to other useful resources, such as the Federal Trade Commission or the BBBOnLine program.

Steve Saulter, Project Director for BBBOnLine, reflects on the Better Business Bureau's task of trying to help consumers sort out the good from the bad by helping people to identify the legitimate businesses that are operating online. The BBBOnLine (www.bbbonline.org) --- in operation for less than a year and having signed over 1,000 companies --- has been set up to help businesses self-regulate the Internet and to establish a company's legitimacy.

The BBB's concern for security, privacy and legitimacy in the online environment requires that business participants be members of the BBB, have been in business for at least a year, have passed a visitation to the company's physical site, and have clean and honest advertising. Once online, the participating business' webpage allows consumers to visit the BBB server to find specific information about the company. Even though the BBB seal can be copied, clicking back to the BBB linkage will warn a consumer whether that company has conformed to the BBBOnLine standards. In addition, a webcrawling device monitors the Internet looking for any use of the BBB name. Any questionable findings are turned over to the BBB's legal department.

Every participant has a site visit — the BBB goes to the physical location of every single one of the businesses to check them out. Potential participants are asked for their résumé, client list, references, samples of their work and whatever else is needed to establish their credibility. The BBB then knows where they are and that they can provide what they have promised.

Monitoring advertising claims is a big part of the BBB operations. A thorough review is done on each company's websites. Probably about 15 percent of the applications reviewed need to clarify their advertising. BBB works with the companies to either substantiate claims that they make about their speed of service or the viability of their offerings, and if the company cannot substantiate it, then the ads are not accepted. And if questioned ad is not changed then the company is turned down as a participant.

The BBB has the participating companies sign a participant agreement to resolve disputes informally or if that fails to go to arbitration. This offers consumers who have had non-delivery, or wrong delivery of products a clear path to easily settle those disputes with BBBOnLine participants.

BBB hopes to have over 3,000 participants on BBBOnLine by the end of 1998. Presently the website has a search engine that can search keywords and company name and can cross reference by state. BBB's other website www.bbb.org (the main Better Business Bureau site) gives information on current scams and how to locate the local BBB. Future plans include a related project called the National Information System which will have all BBB reports on companies posted on line for people to see.

Check the BBB website for results of a survey that has been recently commissioned. Findings show that security is a primary issue but reliability is also a big one. When asked "If a company that you didn't know but were considering doing business with online had been checked out by a third party, would you be more confident doing business with that company?" 84 percent of the respondents said yes.

Paul Leuhr, Chair of the Federal Trade Commission's Internet Coordinating Committee, reports that the FTC, having brought over thirty actions against Internet fraud and deception, has been one of the most active Federal agencies in Internet commerce. The FTC is recognized as the general consumer protection agency in the U.S. although it has no jurisdiction over common carriers (telephones, railroads),insurance companies, non-profit agencies (but do go after the fraudulent telemarketers), and banks.

Most of the cases one hears about are labeled as " new wine in old bottles." However, a couple of new types of fraud are referred to as " fraud in the brave new world." An example is the FTC vs. Audiotex case which solicited people to look at adult photos. The people would download a special viewer. Then during the download process their modem speakers would be shut off, their ISP connection severed, and then their modem would silently dial an international phone number in Moldova at a rate of two to three dollars per minute. The phone connection would not be disconnected until the computer was completely turned off . Eventually a timer was added to only keep one connected for an hour ($180). It was implied that one had free access to the browser and pictures. Yet the people who fell for this scam were not the most gullible consumers but rather those that did have some Internet savvy. The bottom line: 38,000 people were taken in and 2.74 million dollars will go back to consumers primarily in the form of telephone credits on their long distance telephone bills.

To conclude with some of the traditional frauds: here are some warning signs. Watch for the generational forgetting such as the pyramid schemes where income comes from recruiting not selling. Avoid the exaggerated claims which lack truthful and substantiated proof. Be aware of credit repair offers that can actually be illegal.

In addition to handling cases, the FTC is heavy engaged in prevention education directed at consumers and businesses. Concern is focused towards privacy and information in the four categories of notice, consent, access, and security. The website www.ftc.gov keeps consumers updated. A recent privacy surf looked at 1200 different websites to investigate whether businesses are posting something about their privacy policy, whether they make notice that they have a privacy policy, and whether they give you information about what the company is doing with this information. If this is lacking, the FTC puts the industry on notice saying "Hey, you'd better get your self-regulatory act together." The FTC has also joined the fraud artists with mimics of real scams with the attempt not to trick the consumer but to find consumers and give them information at what may be called a very teachable moment. FTC would like to see more consumer involvement in notification of problems. Go to ftc.gov to Consumer Line. For concerns about spam send the message to uce@ftc.gov (unsolicited commercial email).

Continue to keep private information private. Be cautious of companies that claim to have overseas connections, ones that don't allow email replies, or have no phone or street address. Think of P.O. boxes as red flags. Question out-of-this-world claims. Use secured connections when using credit transactions and know who it is going to and their reliability. Consider filters for children. Watch out for X-Files which can do nasty things to your hard drive.

Remember that the Internet is a great source of information. Know where you can go for assistance.

Endnotes

1. Lecturer, School of Human Ecology, University of Wisconsin-Madison, 1300 Linden Drive, Madison, WI 53706-1524.
2. Professor and Extension Specialist, School of Human Ecology.