Table 4. Financial Aspects of Work-at-Home Email

	Frequency	Percent
Potential Monthly-Earnings		
Range	$160.00–$136,808.00	
Median	$3,200.00	
Associated Fees		
Mentioned	12	6.0
Free	15	7.5
Not Mentioned	173	86.5

there is a true physical location, thus giving potential victims a sense of ease because not only is this potential work opportunity online, but also there is a physical location for the user's security. If anything goes wrong, that address could be reported to law enforcement officials. Slightly over half (54%) of the emails contained a physical address. Only 22.5% gave personal information on the sender.

Misspellings are also a potential identifier of work-at-home scams and should be "red flags" for potential victims. We found that 38.5% of emails contained obvious grammatical and spelling errors. These errors were in the form of Internet shorthand (i.e., leet speak) or a simple misspelling such as "Amerycans."

In Table 4 we summarize key financial aspects of the emails. The "fees required" emails added not only a sense of legitimacy, but also provide an indication of how much financial impact these types of scams may cause. The maximum amount of potential earnings mentioned in the email messages was $136,808.00 and the minimum was $160.00. By having such a large amount advertised, interest in the product may increase, but some people will then believe that the offer is "too good to be true." With median potential monthly earnings of $3,200 per month, it appears that the scammers were somewhat realistic in their promises and generally kept the monthly earnings range between $1,500 and $5,000 per month. Some fees were also mentioned in efforts to boost legitimacy and also to convince victims that paying a small start-up fee is nothing in comparison to the large salaries they will soon be earning. However, the large majority of emails (86.5%) did not mention a fee and 7.5% of the emails stated that the program was free.

Several of the emails contained multiple email addresses, one in the "from," "reply to," and one included in the email body. As displayed in Table 5, these email

Table 5. Branding and Legitimacy of Wor

	Frequency
Established Domains	
Aim.com	1
AOL.com	5
Att.net	4
Bellsouth.net	1
Gmail.com	25
Habitat.org	3
Hotmail.com	14
Live.com	3
MSN.com	1
Yahoo.com	14
Spoofed	
Yes	
Verified	28
Suspected	31
No	142

addresses were analyzed for legitimacy or having
email server such as Google. Domains that are
known as established domains. Some of the do
included: Gmail.com, AOL.com, Bellsouth.net,

Many of the obtained addresses were sent fron
this does not indicate that the program is legitin
available to the public for free and the message h
the email is from a well-known source (Wei, Sp
proximately 14% of analyzed emails were verifi
hide the sender's identity and another 15% we
were unable to be verified. We note that 70%
there are many tools available to scammers to

Table 5. Branding and Legitimacy of Work-at-Home Email

	Frequency	Percent
Established Domains		
Aim.com	1	1.41
AOL.com	5	7.04
Att.net	4	5.63
Bellsouth.net	1	1.41
Gmail.com	25	35.21
Habitat.org	3	4.23
Hotmail.com	14	19.72
Live.com	3	4.23
MSN.com	1	1.41
Yahoo.com	14	19.72
Spoofed		
Yes		
Verified	28	13.9
Suspected	31	15.4
No	142	70.6

addresses were analyzed for legitimacy or having being sent from a well-known email server such as Google. Domains that are well-known for legitimacy are known as established domains. Some of the documented established domains included: Gmail.com, AOL.com, Bellsouth.net, Habitat.org and Hotmail.com.

Many of the obtained addresses were sent from established domains; however, this does not indicate that the program is legitimate as most email accounts are available to the public for free and the message header can be forged to look like the email is from a well-known source (Wei, Sprague, and Warner 2009). Approximately 14% of analyzed emails were verified as being spoofed or forged to hide the sender's identity and another 15% were suspected to be spoofed but were unable to be verified. We note that 70% had not been forged, although there are many tools available to scammers to more thoroughly forge a header.

Analysis of Websites

We separated the website layouts into six categories based on the structure of the webpage (see Table 6). The least common type of website recorded was a legitimate website hosted by a legitimate organization that had nothing to do with the spam email. This is referred to as piggybacking (3.39%). Piggybacking websites (see Figure 1) allows scammers another way of appearing legitimate to potential clients. For example, one email included a link to a prestigious research institute's website and offered a work-at-home position through this website. Victims would then see the website and believe the email to be legitimate even though the "reply to" email address in the original email would not match the address associated with the website. If potential victims visit the research institute's website to confirm the company and details mentioned in the email, the illegitimacy of the promoted organization would be obvious.

Table 6. Layout of Work-at-Home Websites

	Frequency	Percent
Layout		
Piggyback	2	3.39
News Report	6	10.17
Requires information/log in	30	50.85
Regular website advertising a good	5	8.47
Make purchase to work at home	14	23.73
Other/Unknown	2	3.39

Another approach to the website designs was the news report variation (see Figure 2). These websites were created to resemble local news stations' websites. This layout typically included testimonials, multiple images with "clients," checks, comments, headings such as "Local Mom Makes $710/ Week;" and links to legitimate news sites such as Central News Network (CNN). Local news layouts were structured as real news reports and in doing so, may have added a sense of legitimacy to the promoted opportunity. Most even had a

Figure 1. Example of Piggybacki

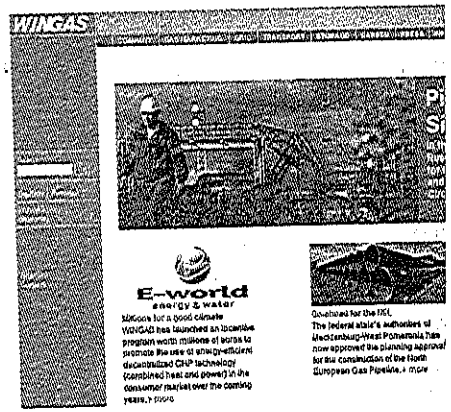
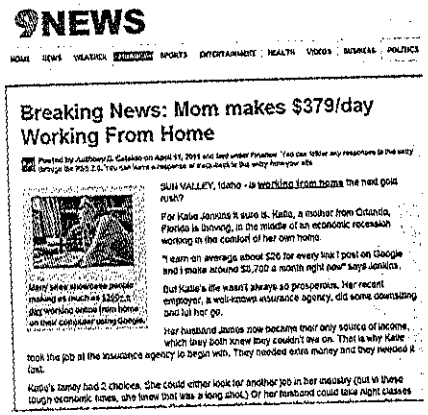


Figure 2. Example of News Rep



number of comments from "readers" at the bo
3). The local news layout comprised about 10%

Just over 50% of the websites required users t
mation (i.e., email address, name, phone numb
and to receive information about the work-at-h
users to sign up for a "risk-free kit" that involve
tion and a small payment (see examples of thes

Figure 1. Example of Piggybacking Website

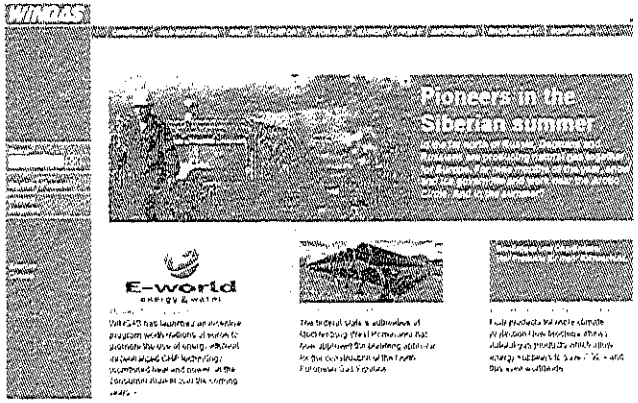


Figure 2. Example of News Report Website

number of comments from "readers" at the bottom of the pages (see Figure 3). The local news layout comprised about 10% of all websites in the sample.

Just over 50% of the websites required users to provide some form of information (i.e., email address, name, phone number) to obtain access to the site and to receive information about the work-at-home opportunity. Many asked users to sign up for a "risk-free kit" that involved providing personal information and a small payment (see examples of these websites in Figures 4 and 5).

Figure 3. Reader Comments from News Report Website

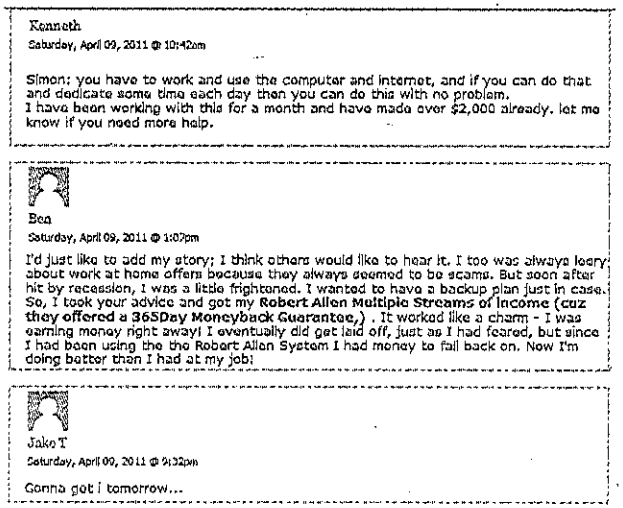
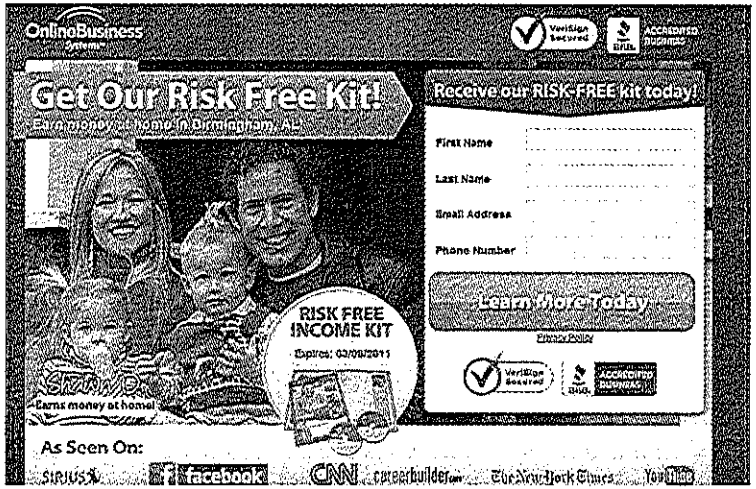


Figure 4. Work-at-Home Website Asking for Personal Information



Another variation of websites that were recorded is the "regular" format. These websites were coded by appearing to be a website simply advertising work at home opportunities and accounted for about 8% of the analyzed sites. These sites con-

tained no mention of purchasing any prod
anything. Figure 6 is an example of what w
The fifth criteria for categorizing a web
advertising goods or services for purchase ir

Figure 5. Work-at-Home Webs

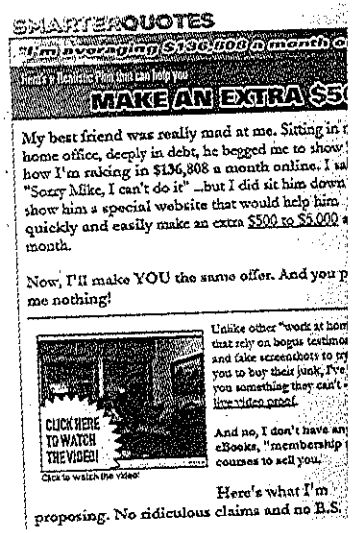
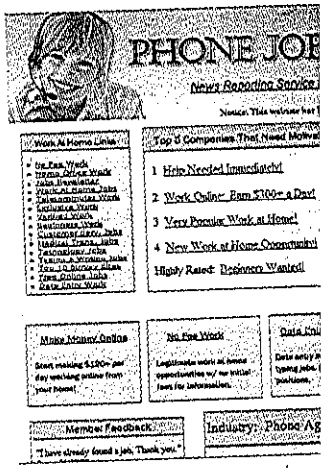


Figure 6. Example of Work-

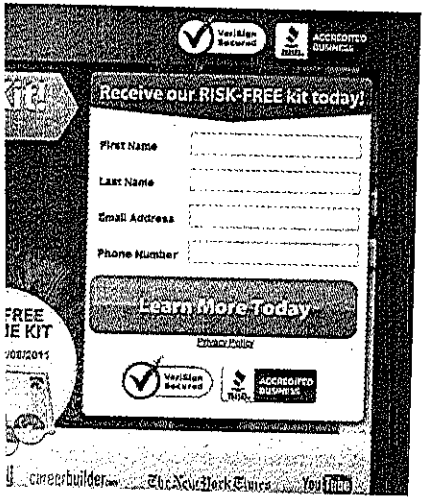


ments from News Report Website

the computer and internet, and if you can do that
then you can do this with no problem.
month and have made over $2,000 already. let me

others would like to hear it. I too was always leery
they always seemed to be scams. But soon after
toned. I wanted to have a backup plan just in case.
Robert Allen Multiple Streams of Income (cuz
ck Guarantee,) . It worked like a charm - I was
ually did get laid off, just as I had feared, but since
on System I had money to fall back on. Now I'm

site Asking for Personal Information



vere recorded is the "regular" format. These
a website simply advertising work at home
t 8% of the analyzed sites. These sites con-

tained no mention of purchasing any products or being required to sign up for anything. Figure 6 is an example of what was considered a "regular" website.

The fifth criteria for categorizing a website was whether or not that site was advertising goods or services for purchase in order to gain access to work at home

Figure 5. Work-at-Home Website Asking for Registration

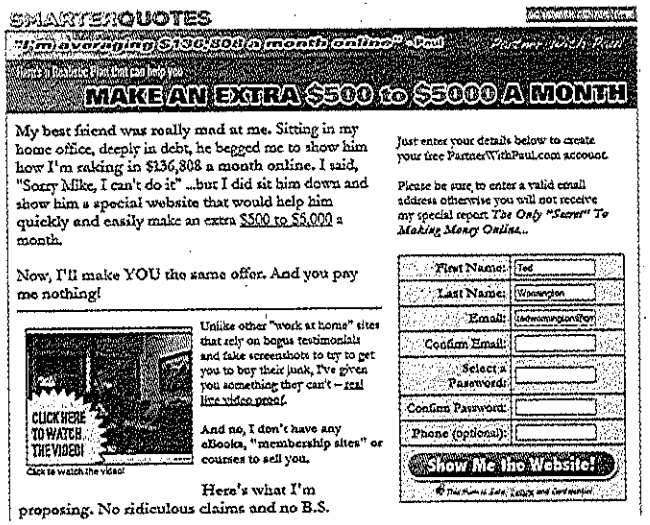
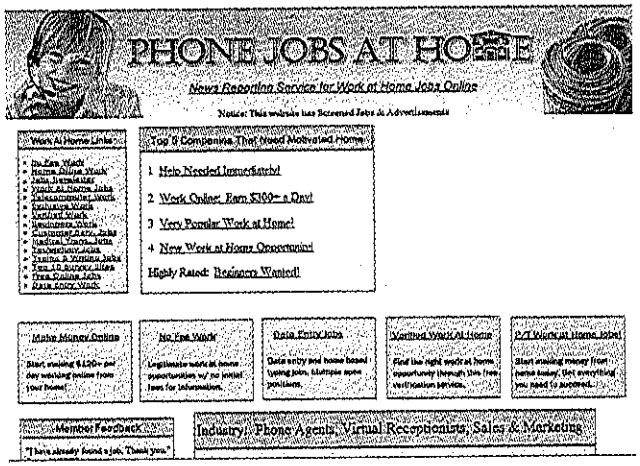
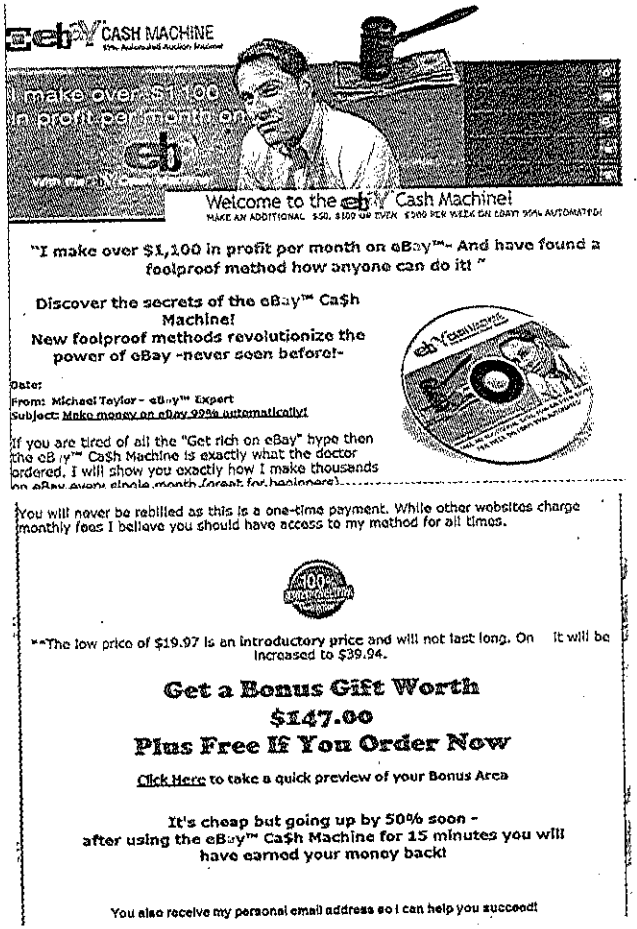


Figure 6. Example of Work-at-Home "Regular" Website



materials. This category accounted for 23.73% of the recorded websites. Websites were classified as requiring payment based on the presence of having to pay a fee whether it was for a membership fee, CD, guide book, or other in order to have access to the advertised work at home materials. Figure 7 is an example of a website classified under this category.

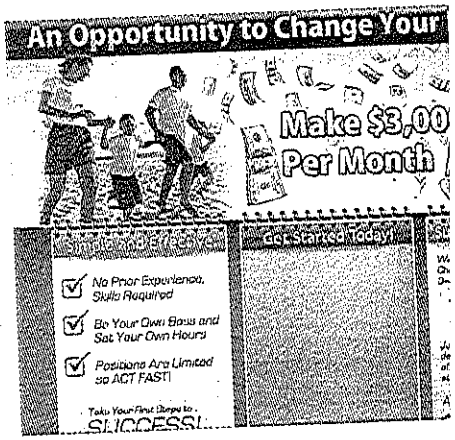
Figure 7. Example of Website Asking to Make a Purchase



The final category of website format was "other." This category accounted for about 3% of the retrieved websites. Websites in this group are those that had errors where no links were available to get any additional information (in-

dicating the site may have been used for malware) o
ing from home but did not actually provide an ave
a work at home scam (i.e., dead links or poorly wr
8 is an example of such a site that had no working
additional information, and did prompt visitors t
up for a membership.

Figure 8. Example of "Other" Type of Wo



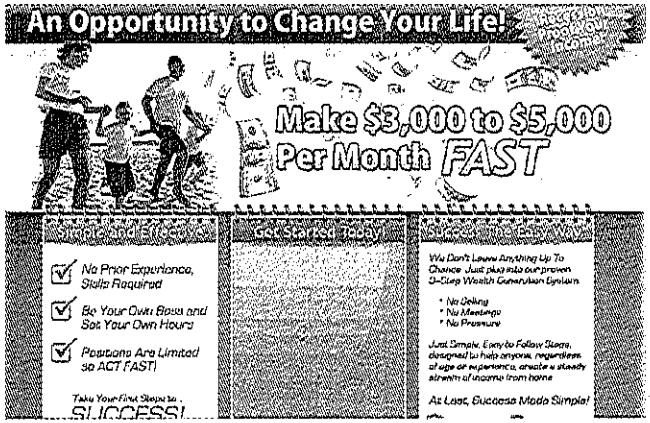
In addition to the layout of the work-at-home
tify the type of work being offered (see Table 7

Table 7. Advertised Work Opportunities in

Layout
Advertising
Work (i.e., typing or telemarketing)
Not specified—purchased required
Not specified—sign up/log in required
Not specified at all
Other

dicating the site may have been used for malware) or the site talks about working from home but did not actually provide an avenue in which to engage in a work at home scam (i.e., dead links or poorly written website code). Figure 8 is an example of such a site that had no working links, did not request any additional information, and did prompt visitors to make a purchase or sign up for a membership.

Figure 8. Example of "Other" Type of Work-at-Home Website



In addition to the layout of the work-at-home websites, we sought to identify the type of work being offered (see Table 7). Many websites advertised

Table 7. Advertised Work Opportunities in Work-at-Home Websites

	Frequency	Percent
Layout		
Advertising	8	13.56
Work (i.e., typing or telemarketing)	6	10.17
Not specified—purchased required	14	23.73
Not specified—sign up/log in required	23	38.98
Not specified at all	3	5.08
Other	5	8.47

work-at-home opportunities and the ability to make large amounts of "easy money," but never elaborated the exact process whereby money could be made. We were, however, able to group the websites into six categories. The first distinct avenue of work was advertising and it accounted for 13.56% of the employment. The work was classified as advertising if the site mentioned anything about gaining popularity for a website, posting links, or distributing advertisements. The second group is called "work" and consists of any website that seemed to offer actual tasks (i.e., typing, telemarketing, survey taking). This group constituted 10.17% of the websites. The third group comprised 23.73% of the websites and work under this category could not necessarily be established because individuals needed to pay a fee to learn the secret or gain access to the work at home materials. The fourth group is largest at 38.98% and is similar in nature in that these work opportunities could not be defined because users had to sign up or create an account to ascertain what the actual job requirements were. The fifth group (5.08%) pertained to websites that did not specify the type of work at all; there were no indications of what participants would be doing. The sixth group (8.47%) is classified as "other." These websites indicated that the work-at-home businesses would soon be in touch with users or other.

In Table 8 we describe the use of testimonials and gender in the sampled websites. The criteria for testimonials on the websites included: number of testimonials, gender, and locations (if they were located in the text, sidebars, or in a comment section). There are more criteria for website testimonials because much of the data was gained through images and emails cannot support such large files.

Table 8. Testimonials and Gender in Work-at-Home Websites

	Frequency	Percent
Testimonial Genders		
Male	13	44.8
Female	16	55.2
Number of Testimonials (Median)		
In the Text	2	
In the Sidebars	5	
In the Comments	8	

Testimonials were included for
popular or legitimate a program s
ple state how easy or effective a pr
a false sense of security by seeing
sites also contained comment sect
their comments, concerns, and pr
cations on work-at-home sites, su
in comment sections. The gender
attributed was not significantly
45% and women comprised the

Next we addressed the financi
sites were coded for the amount
of the page, amounts mentioned
a photo of a check on the websit

Table 9. Financial M

Amount Mentione	
Maximum	
Minimum	
Amount Mentione	
Maximum	
Minimum	
Median	
Check Photo	
Maximum	
Minimum	
Start-up Costs	
Not Mentioned	
Mentioned	
Maximum	
Minimum	

Testimonials were included for coding because of the implication of how popular or legitimate a program seemed. By having seemingly ordinary people state how easy or effective a program is potential victims may be lulled into a false sense of security by seeing other people use this program. Some websites also contained comment sections where potential users or skeptics voiced their comments, concerns, and praise. Testimonials were located in several locations on work-at-home sites, such as the text of the website, in sidebars, and in comment sections. The gender of the person to whom the testimonials were attributed was not significantly different as men were responsible for about 45% and women comprised the remaining 55%.

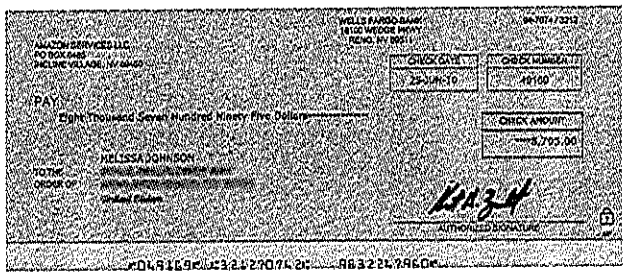
Next we addressed the financial aspects of the websites (see Table 9). Websites were coded for the amount of money mentioned in the title or heading of the page, amounts mentioned in the text, any start up fees, and if there was a photo of a check on the website. The work-at-home websites in our sample

Table 9. Financial Matters in Work-at-Home Websites

	Frequency
Amount Mentioned In Website Title	
Maximum	$136,808.00
Minimum	1,000.00
Amount Mentioned in Text	
Maximum	$136,808.00
Minimum	800.00
Median	5000.00
Check Photo	
Maximum	$8782.57
Minimum	400.00
Start-up Costs	
Not Mentioned	42
Mentioned	17
Maximum	$100.00
Minimum	7.00

contained more references to financial matters than emails because the websites were able to host more content in different forms, such as pictures of money, large fonts at the top of the website indicating how much money a person could make, the amount of startup costs, and pictures of earned checks. In many cases, these websites had a title at the top of the page that stated the name of the program and how much a person can make using the advertised product. The maximum amount mentioned in the website headings was $136,808.00 and the minimum recorded was $1,000.00. The text consisting of the body of the website also contained potential earning amounts with a maximum of $136,808.00, minimum of $800.00, and median of $5,000.00. Scammers also included images of checks (see Figure 9) with the highest amount recorded as $8,782.57 and the lowest as $400.00. However, to make the promised money and to receive a check with your name on it, some scams required start-up or membership fees. Most of the websites did not mention any fees[7] (71.2%), but there was a smaller percentage (28.8) that did and those start-up fees ranged from $7.00 to $100.00.

Figure 9. Image of Check Found on Work-at-Home Website



You could be making checks like this

As summarized in Table 10, claims of legitimacy were also made in the website content, although it was more common (57.6%) for a scammer to avoid mentioning a legitimate company on the site than it was for them to make their websites look supported by reputable companies (42.4%). The same pat-

7. It is important to note that some of the work-at-home websites required potential users to create a log-in account before any details of the program were released. It would be ideal to register at each site that required a log in so to uncover any start up fees, but for each site the authors would have to enter an email address, wait for the confirmation email, sign in, and such. So as this is a pilot study, it has been left to future research to undertake that task.

Table 10. Legitimacy of Work-a

	Fr
Legitimate company mentioned	
Yes	
No	
Mentions other scams or the program's legitimacy	
Yes	
No	
Number of companies mentioned	
In Text	
Median	
In Header	
Median	

tern follows in whether a scammer mentione
gitimacy of the program being promoted.
other scams or defend the legitimacy of thei
(37.3%). Websites that included a compan
groups in the text and five groups in the he
tised groups were Apple, ABC, Adidas, and

In Table 11 we include other important
history of the websites. Of the 59 sampled w
were unique and 4 were repeated. There w
duplicated IPs that originated from over 30
created September 28, 1996, the newest v
2010, and the most common year of creatio
is significant because work-at-home websit
rate of turnover. The age of the domains n
1) the original website had been hacked tc
website owner was unaware, 2) the scamm
one complained about the site to an Intern
mer constantly updated and changed the a

Table 10. Legitimacy of Work-at-Home Websites

	Frequency	Percent
Legitimate company mentioned		
Yes	25	42.4
No	34	57.6
Mentions other scams or the program's legitimacy		
Yes	22	37.3
No	37	62.7
Number of companies mentioned		
In Text	1–7	
Median	2	
In Header	1–7	
Median	5	

tern follows in whether a scammer mentioned a different scam or stated the legitimacy of the program being promoted. More offenders did not mention other scams or defend the legitimacy of their own (62.7%) than those who did (37.3%). Websites that included a company name typically mentioned two groups in the text and five groups in the header. The most commonly advertised groups were Apple, ABC, Adidas, and MSNBC.

In Table 11 we include other important information about the source and history of the websites. Of the 59 sampled websites, 55 of the website domains were unique and 4 were repeated. There were 49 unique IP addresses and 10 duplicated IPs that originated from over 30 countries. The oldest website was created September 28, 1996, the newest website was created December 07, 2010, and the most common year of creation for these websites was 2000. This is significant because work-at-home websites typically have an extremely high rate of turnover. The age of the domains may indicate several things, such as 1) the original website had been hacked to suit the scammer's needs and the website owner was unaware, 2) the scammer was exceptionally lucky and no one complained about the site to an Internet Service Provider, or 3) the scammer constantly updated and changed the appearance of the website thus mak-

Table 11. Information About Work-at-Home Websites

	Frequency	Percent
Website Link		
Unique Sites	55	92.7
Repeated Sites	4	7.3
IP Address		
Unique	49	83.1
Repeated	10	16.9
Length of Existence		
Oldest	September 28, 1996	
Newest	December 07, 2010	
Most common year of creation	2000	

ing it more difficult to identify as illicit. The IP addresses were also entered into the UAB Geolocator to identify where the websites were being hosted. The results of this query indicated that the websites were registered to a total of 5 countries (United States, Germany, China, United Kingdom, and British Columbia) with 49 of the 59 websites hosted through companies in the United States.

Finally, in addition to using Whois.domaintools.com for domain information, Compete Rank was used to identify the standing of each possible domain (see Table 12). Compete Rank is an online ranking system that ranks each website based on the number of unique visitors it receives each month. The highest ranking for the analyzed sites w visitors each month. The lowest rec only 43 unique visitors to the webs 83,043 with 23,366 unique visitors

Table 12. Compete Rankings of Work-at-Home Websites

	Rank	Visitor Count
Compete Rank		
Maximum	1,597	1,217,570
Minimum	4,617,375	43
Average	400,862	134,541
Median	83,043	23,366

Discussion

The goal of this paper was to prov emails and websites. Through this characteristics for this type of frau the offenders to make the solicitatio indicates that a typical work-at-ho an unspecified recipient. Email su the likelihood that individuals will plied and active) and then fall pr consist of text and, in some cases, formation about the scam. The len without any misspellings. The en such as a testimonial, mention of of a reputable company. Additiona been spoofed. There may be som being "easy money" and even inc the email typically will not list the

Work-at-home websites are typ advertisements, or piggybacking most part, not elaborate on how t requiring a startup fee or the creat contain monetary amounts that c as within the text or sidebars. Add tures. Similar to the email conten through the form of testimonials reputable companies.

Before offering the research a that readers may question whethe ness arrangements as fraudulent opportunity is a scam. Legitima cult to identify because of the vast Chief Executive Officer of StaffC based careers, recently noted tha

ork-at-Home Websites

Frequency	Percent
55	92.7
4	7.3
49	83.1
10	16.9
aber 28, 1996	
iber 07, 2010	
2000	

IP addresses were also entered websites were being hosted. The es were registered to a total of 5 nited Kingdom, and British Co- gh companies in the United States. itools.com for domain informa- tanding of each possible domain cing system that ranks each web- receives each month. The high-

rk-at-Home Websites

Visitor Count
1,217,570
43
134,541
23,366

est ranking for the analyzed sites was 1,597, with a total of 1,217,570 unique visitors each month. The lowest recorded rank was 4,617,375, with a total of only 43 unique visitors to the website each month. The median ranking was 83,043 with 23,366 unique visitors per month.

Discussion and Conclusions

The goal of this paper was to provide an exploratory analysis of work-at-home emails and websites. Through this analysis, we sought to identify the common characteristics for this type of fraud, as well as common techniques used by the offenders to make the solicitations attractive to potential victims. Our study indicates that a typical work-at-home email is from an unspecified sender to an unspecified recipient. Email subjects are worded persuasively to increase the likelihood that individuals will open the email and visit the website (if supplied and active) and then fall prey to the fraud. The work-at-home emails consist of text and, in some cases, hyperlinks to a website with additional information about the scam. The length of the message will usually be short and without any misspellings. The email will contain some claim of legitimacy, such as a testimonial, mention of another scam, or mention/ impersonation of a reputable company. Additionally, the "From" information is likely to have been spoofed. There may be some mention of the work-at-home position as being "easy money" and even include a potential earning amount; however, the email typically will not list the start-up fees.

Work-at-home websites are typically found in three layouts: news reports, advertisements, or piggybacking. The content for the websites will, for the most part, not elaborate on how to achieve work-at-home success without first requiring a startup fee or the creation of a log-in account. Website content will contain monetary amounts that can be found at the top of the websites as well as within the text or sidebars. Additionally, most websites will not include pictures. Similar to the email content, legitimacy claims are common on websites through the form of testimonials and either mentioning or displaying logos of reputable companies.

Before offering the research and policy implications of our study, we note that readers may question whether we are generalizing all work-at-home business arrangements as fraudulent. We are aware that not every work-at-home opportunity is a scam. Legitimate opportunities exist, but they can be difficult to identify because of the vast number of illegitimate ones. Christine Durst, Chief Executive Officer of StaffCentrix, a company that specializes in home-based careers, recently noted that among "the 5,000 home job leads StaffCen-

trix screens weekly, there is a 54 to 1 scam ratio" (Blake 2009). This means that individuals looking for work-at-home opportunities must exercise extreme caution when searching for employment. This could include looking at the job requirements, because if there are none or the company is requiring participants to pay upfront fees then it is most likely fraudulent. Individuals can also call the advertised company's main office to verify its existence and location. This should always be performed no matter how well-known the company is and if there is still doubt, individuals can contact the Better Business Bureau or the Federal Trade Commission. Another indication of a scam is the trite, yet accurate, guideline that "if it sounds too good to be true, it probably is." As a general rule, businesses are not going to pay someone with no experience an inordinate amount of money to perform a menial task for only a few hours of work per day.

The area of work-at-home spam is relatively new and offers many avenues for additional research. With larger sample sizes over longer periods, a more accurate portrait of work-at-home spam could be formed. Trends within spam campaigns could be identified though larger sample sizes obtained over a greater time period by identifying when a spam campaign is the most popular, such as news reports being more prevalent during the spring, or piggybacking scams being noticed more in the fall. The domain names for work-at-home websites could be monitored for repeat usage or similarity. Also, patterns between email senders' IP addresses could be established by identifying which IP is responsible for which specific work-at-home campaign. This data could also assist in establishing spam campaign trends. By working with agencies, such as the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3), researchers may also be able to gather information from the victims of these scams. If victim contact is made, then it would be possible to obtain first-order accounts of why victims fell prey to these scams. There are myriad research opportunities in the field of work-at-home fraud and this exploratory study was intended to catalyze this line of research.

Our findings point to several policy implications. First, results from our study could be used to create or supplement educational programs about online fraud more generally, and work-at-home fraud specifically. These programs could contain information we found regarding the structure, format, goals, and impact of the fraudulent emails and websites we analyzed. Such educational programs could be offered by the law enforcement community, consumer protection agencies, and university researchers, and could increase awareness of fraud as well as offer steps to avoid falling prey. In addition to creating awareness and resistance strategies for online fraud, our study results could be used to promote appropriate consumer responses to victimization.

Online fraud victims often are reticent to report, and even w
struggle to identify the proper authorities or organizations to wh
report. National victimization reporting databases such as the
Complaint Center (www.ic3.gov) could be better publicized, as
regional efforts such as Operation Swordphish in Alabama
phish.cis.uab.edu/new).

Second, our results could be used to facilitate a cooperative
law enforcement officials (in particular at the federal level) and
search providers (e.g., Google) to prevent and control online work
For example, our study found a consistent pattern in the ima
and website testimonials in many work-at-home frauds. If thes
terns were shared with law enforcement officials and Google, i
the fraudulent websites could be flagged and/ or deleted from
index much sooner than in the past. Our findings may also h
identify the source of online kits that contain files needed to
home scams.

References

ABC News. "Cops Warn of 'Secret Shopper' Scam." March 7,
news.go.com/TheLaw/wireStory?id=4407858.
ABC News. "Google work-at-home scammers hauled to cou
2009. http://www.abs-cbnnews.com/technology/12/09/0
home-scammers-hauled-court.
Baker, Wayne E., and Robert R. Faulkner. "Diffusion of Frau
Economic Crime and Investor Dynamics." *Criminology* 41 (2
Blake, John. CNN, "How I got taken by a work-at-home scam
January 07, 2009. http://articles.cnn.com/2009-01-07/livi
1_work-at-home-scammers-data-entry-job?_s=PM:LIV
Edelson, Eve. "The 419 Scam: Information Warfare on the S
Proposal for Local Filtering." *Computers & Security* 22 (2
Grabosky, Peter N., Russell G. Smith, and Gillian Dempsey.
Unlawful Acquisition in Cyberspace. Cambridge, UK: Ca
sity Press, 2001.
Harley, David and Andrew Lee. "A Pretty Kettle of Phish: S
in your Email? What you Need to Know about Phishing
tivirus and Security White Papers. Accessed March 2
go.eset.com/us/resources/white-papers/Pretty_Kettle_of

Online fraud victims often are reticent to report, and even when motivated struggle to identify the proper authorities or organizations to whom they should report. National victimization reporting databases such as the Internet Crime Complaint Center (www.ic3.gov) could be better publicized, as could state and regional efforts such as Operation Swordphish in Alabama (https://swordphish.cis.uab.edu/new).

Second, our results could be used to facilitate a cooperative effort between law enforcement officials (in particular at the federal level) and major Internet search providers (e.g., Google) to prevent and control online work-at-home fraud. For example, our study found a consistent pattern in the images, email text, and website testimonials in many work-at-home frauds. If these common patterns were shared with law enforcement officials and Google, it is possible that the fraudulent websites could be flagged and/ or deleted from an online search index much sooner than in the past. Our findings may also help these groups identify the source of online kits that contain files needed to create work-at-home scams.

References

ABC News. "Cops Warn of 'Secret Shopper' Scam." March 7, 2008. http://abcnews.go.com/TheLaw/wireStory?id=4407858.

ABC News. "Google work-at-home scammers hauled to court." December 9. 2009. http://www.abs-cbnnews.com/technology/12/09/09/google-work-home-scammers-hauled-court.

Baker, Wayne E., and Robert R. Faulkner. "Diffusion of Fraud: Intermediate Economic Crime and Investor Dynamics." *Criminology* 41 (2003): 1173–1206.

Blake, John. CNN, "How I got taken by a work-at-home scam." Last modified January 07, 2009. http://articles.cnn.com/2009-01-07/living/home.scams_1_work-at-home-scammers-data-entry-job?_s=PM:LIVING.

Edelson, Eve. "The 419 Scam: Information Warfare on the Spam Front and a Proposal for Local Filtering." *Computers & Security* 22 (2003): 392–401.

Grabosky, Peter N., Russell G. Smith, and Gillian Dempsey. *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge, UK: Cambridge University Press, 2001.

Harley, David and Andrew Lee. "A Pretty Kettle of Phish: Something Phishy in your Email? What you Need to Know about Phishing Fraud." ESET Antivirus and Security White Papers. Accessed March 25, 2012. http://go.eset.com/us/resources/white-papers/Pretty_Kettle_of_Phish.pdf.