



**Taxable Income: US Tax Scams**  
**infectionvectors.com**  
**March 2006**

**Overview**

The often-repeated quotation, “nothing is certain but death and taxes,”<sup>1</sup> comes to the minds of most United States citizens this time of year as their annual income tax payments need to be reconciled with the Internal Revenue Service (IRS) by April 14. After observing the unrelenting surge of tax-related scams, it appears that phishing could be added to Benjamin Franklin’s famous phrase. Tax refund scams are an intriguing medium for criminals as virtually every US adult is a “customer” of the IRS (unlike banking scams where most of the recipients are not account holders and would likely delete the message), not to mention that offering someone money is a good way to increase the readership of such email messages. This report examines one IRS-based scam and the difficulty in stopping such attacks.<sup>2</sup>

**Your \$63.80**

The sample for this report is one many people have seen and reported over the last month, the promise of \$63.80 in refunds letter. The amount is recycled in each iteration of the attack (which has at least 4 stages as seen later). It is an interesting choice by the criminal(s) behind the scam. The initial reaction may be that the amount is too low to lure anyone into clicking the accompanying link, especially considering the average reported refund size in the US (last year the IRS noted a figure of approximately \$2,000).<sup>3</sup> However, it may be that the low amount is actually much more believable to most Americans while sifting through their email. The grandiose amounts in the “You Won the International Lottery,” and “Please help me transfer funds out of my country,” attract a certain audience, it is possible that the \$63.80 attracts another. In either case, the criminals in question never changed the amount, a trivial editing task, over the month that this scam was tracked. That is quite possibly because the scheme was working as well as they hoped (or better) with the text exactly as it was.

The email itself reads:

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of \$63.80. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline. To access the form for your tax refund, please click here.

The message appears as the following in HTML-enabled mail clients:



After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of **\$63.80**. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please [click here](#)

Regards,  
Internal Revenue Service

© Copyright 2006, Internal Revenue Service U.S.A. All rights reserved..

It is not the most official looking email, however the logo (lifted from the real IRS site by the message), copyright information, and reasonably accurate grammar (even using terms such as “fiscal activity”) make the message believable. There are no glaring spelling errors, oddly formatted paragraphs, or strange requests (at this time). If the recipient had not yet calculated their tax refund (or the actual refund amount was close, or the recipient believed they had to pay the IRS additional taxes), the amount of \$63.80 may sound like a sensible amount. The message, beyond the fake IRS link, includes some unseen tracking information as well. The tag, appended to the letter in early as well as later copies of the email<sup>4</sup>, shows the Geocities counter information, which will log the address, browser type, etc. of the visitor:

```
<!-- text below generated by server. PLEASE REMOVE --><!--  
Counter/Statistics data collection code --><script  
language="JavaScript"  
src="http://hostingprod.com/js_source/geov2.js"></script><script  
language="javascript">geovisit();</script><noscript></noscript>  
<IMG SRC="http://geo.yahoo.com/serv?s=76001524&t=1140391544&f=p6w5"  
ALT=1 WIDTH=1 HEIGHT=1>
```

If this is used by the criminal for research and planning, or was left in the code after a hosting attempt will not be known with certainty unless the attacker is apprehended. However, it does offer a clue as to some of the mechanisms that the phisher employed while crafting his scheme.

The “click here” link itself is not encoded or otherwise obfuscated. When a reader’s mouse hovers over the link, they see the exact destination, in this case: <http://ppp-202.133.189.250.revip.asianet.co.th/pms/.../IRS/refund/caseid1796433/index.html>.

“Asianet.co.th” (Thailand) should sound like a strange place for the IRS to be hosting a web site. As we know from the profitability of phishing, readers are not always so careful. If one was to follow the link (prior to the server being disabled), one would have found the following (a file named pas.php):

The screenshot shows the IRS.gov website interface for requesting a tax refund. At the top, the IRS logo and "Internal Revenue Service IRS.gov" are displayed, along with "DEPARTMENT OF THE TREASURY". A navigation bar includes links for "Home", "Get Tax Refund on your Visa or MasterCard", and "Refund Help". The main heading is "Tax Refund". Below this, the section is titled "Get Tax Refund on your VISA or MasterCard". A note asks for a Social Security Number and a valid VISA or MasterCard number, with a link to a "Privacy Notice". The form fields include: "Social Security Number" (with a sub-label "or IRS Individual Taxpayer Identification Number" and a link "shown on your tax return"), "Credit/Debit Card" (with a sub-label "Name on card:"), "Card Number:", "Expiration Date:" (with "Month" and "Year" dropdowns), "CVV Code:" (with a small card icon), and "ATM Card PIN:". At the bottom, the "Refund Amount" is shown as "\$ 63.80" and a blue "Submit" button is present.

This is built by the index.htm page linked to above:

```
<html>
<head>
<meta http-equiv="refresh" content="0";
url=pas.php?certegy_vm=trueportlet_change_1_actionOverrideFchaseonlineF
changeFsigninDetails_windowLabel_portlet_signin_pageLabel_page_signin">
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-
1">
</head>
</body>
</html>
```

Note the PHP command uses “actionOVERRIDEFchaseonline” indicating that this, like so many other scams was built on a recycled attack, this time taking what was a phony Chase Bank scheme and simply swapping the page for the IRS site.

The page above, lifted from the real IRS website, is clearly a good likeness (the most important change, the POST method adjustment is unseen by the reader). It is a simple form asking for the credit/debit card of the reader’s choice as well as their Social Security Number. The amount of refund has also been hard coded into the form, an attempt to make the viewer believe it is a unique page (as details such as the tax payer’s name would obviously not be available to the criminal). Compare the page to a page at the real IRS site:

**Internal Revenue Service IRS.gov**  
DEPARTMENT OF THE TREASURY

[Home](#) | [Get Refund Status](#) | [Refund Help](#)

## Refund Status

### Get Refund Status

Please enter your Social Security Number, your Filing Status and the amount as shown on your tax return.  
\*See our [Privacy Notice](#) regarding our request for your personal information.

---

**Social Security Number** ▶  
or IRS Individual Taxpayer Identification Number [shown on your tax return.](#)

-  -

---

**Filing Status** ▶  
Please select the Filing Status [shown on your tax return.](#)

Single  
 Married-Filing Joint Return  
 Married-Filing Separate Return  
 Head of Household  
 Qualifying Widow(er)

---

**Refund Amount** ▶  
You must enter the exact whole dollar amount [shown on your tax return.](#) Providing the exact whole dollar amount is essential to receiving the correct response.

\$ 


▶ Note: For security reasons, we recommend that you close your browser after you have finished accessing your refund status.

[IRS Privacy and Security Policy](#)

## International Post

How did the scam evolve? Clearly the scam is built like many others, and even shows signs of being a recycled effort for the criminal in question. As mentioned at the outset, this text was used for approximately one month prior to the publication of this article. The example described above was at least the 4<sup>th</sup> incarnation of the attack, counted by the use of the same email/server text but different hosting locations. As the crime fighters of the Internet are becoming more and more efficient at removing fake sites from the Web,

the scammers are becoming increasingly adept at standing up new servers and distributing email very quickly.

On February 16, 2006 the first report of this text was entered. The server used for the scam was located in Mexico (148.233.143.241):

<http://karims.com.mx:81/irs>

The use of a domain name allows the scammer to have multiple servers, possibly spread out to multiple locations and the ability to make tactical changes to DNS entries. That indicates a long-term investment, something that is clearly not the interest of the criminals continuing this scam. Some iterations of the crime hard code IP addresses into the URL, preventing the use of multiple addresses/locations, but also dodging DNS server blocks that may be used to protect users. Both mechanisms have advantages, and may just be the taste of the coder. To be sure, there is no indication that the same person is perpetuating all of these incarnations of the IRS \$63.80 con. Anyone could copy the email and web pages for their own server. The ease with which this could be done has been described in other articles and should be fairly apparent based on the review of the crime above.

A server established in South Korea around February 23rd followed the first location. This incarnation of the scam was the first to use the “caseid” directory name, a fairly clever attempt to make the page look more unique to the user:

<http://211.38.41.205/IRS/refund/caseid886432/index.html>

At least the country code for Korea is not displayed in the URL. The page, as is the case for each of the revisions of the scam, is the same as the example. A day later, on February 24, the phony site appeared on another Korean-based server:

<http://ns.hasom.com/IRS/refund/caseid886432/index.html>

This domain was found at 211.234.84.2 at the time of investigation. Two days later, on February 26, the version seen in the preceding section was delivered. It pointed to:

<http://200.21.49.67/IRS/refund/caseid886432/index.html>

This is registered to Colombia; the scam has now changed continents again, returning to South America. The following day, February 27, the scheme was found on a server in Germany, with the following URL sent with the email:

<http://ifen.bauv.unibw-muenchen.de/IRS/refund/caseid886432/index.html>

It is also interesting to note that none of the sample emails found while researching this attack came from any of the countries that hosted the scam, with phony messages from France, the United States, and Australia all carrying the con. That involves at least four

continents, six countries, and countless computers. Undoubtedly the recipient list for the scam is in the millions of inboxes.

### **Audit**

The scam is not complex; it involves no new phishing tricks. Social engineering remains one of the most lucrative means of making money online as it relies on no particular technology and therefore works on all types of platforms, readers, and in spite of most security software. Awareness remains the biggest foe of the phisher, a commodity in seemingly short supply among Internet users.

The IRS, like other financial and government institutions, warns users about the threat of phishing, although, they may well have fewer readers of their site than the phisher does of the above email. The IRS makes a point of saying that they do not use email to communicate with taxpayers. That is echoed by most organizations, as email has proven to be simply too insecure to conduct business with. News media often report on specific phishing attempts, warning users that some email messages are counterfeit. This plays to an incorrect assumption though, that email is trust worthy, but there are some scams out there. The message, rather, should be that all email is untrustworthy unless you are given some type of authenticating mechanism (which involves a complementary, but external technology to SMTP). That type of default position, that every email is suspect unless proven otherwise, will be slow in coming. It is likely that it won't be until a new generation of Internet users that email scammers run into a population that is hardened against phishing.

Current technical efforts to defeat attacks like that outlined above are not going to end phishing. As can be seen, scammers are capable to distributing round after round of email and moving servers between continents well before law enforcement could remove an offending server. The attitudes of email readers (as well as users of similar technology like instant messaging, voice over IP, etc.) will have to be reshaped.

## References

1. This quote is attributed to Benjamin Franklin,  
[http://www.brainyquote.com/quotes/authors/b/benjamin\\_franklin.html](http://www.brainyquote.com/quotes/authors/b/benjamin_franklin.html).
2. IRS scams have also been discussed in the infectionvectors.com report “Customer Advocate,” available at: <http://www.infectionvectors.com/emergprep/advocate.htm>.
3. Average refund information:  
<http://www.irs.gov/newsroom/article/0,,id=136386,00.html> &  
<http://www.forbes.com/personalfinance/funds/newswire/2004/05/10/rtr1366398.html>.
4. Some of the phishing samples can be found by searching:  
<http://groups.google.com/group/news.admin.net-abuse.sightings?hl=en>.

Copyright © infectionvectors.com 2006.