

# Anatomy of a Phishing Scam

## Identity thieves claim IRS owes avatar a refund

by Pollywog Gardenvale



Pollywog Gardenvale is publisher of *The Seventh Sun*. She is also *Milliner in Residence* for *The Mad Haberdasher* and develops unusual strains of cybrid peonies.

When I checked my e-mail this morning, I found an urgent message from the IRS that said I was due an income tax refund of \$192.81. I was instructed to click a link to access the tax refund form and also warned—in rather peculiar English—that if I made any “deliberate wrong inputs,” I would be “criminally pursued and indicated.”

Although I hadn’t yet had my morning cup of coffee, I realized that it was highly unlikely that the IRS owed me any money, or that they would close such a notice with, “Regards, The Internal Revenue Service.”

So I did Google “IRS email scam” and out of 1,070,000 results, chose an

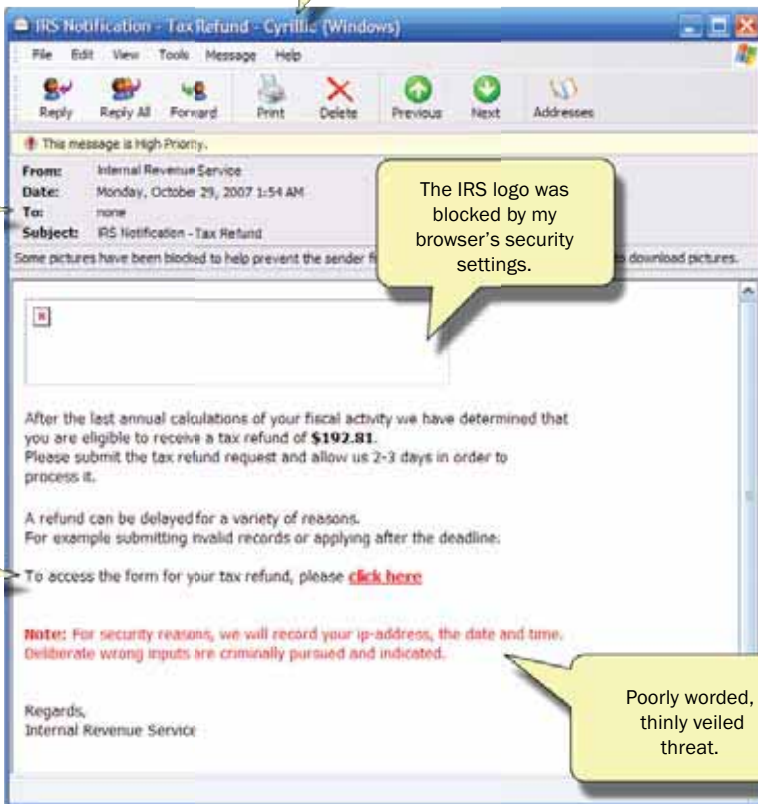
article called “Suspicious Emails and Identity Theft” on the IRS site. It began by saying:

“The Internal Revenue Service has issued several recent consumer warnings on the fraudulent use of the IRS name or logo by scamsters trying to gain access to consumers’ financial information in order to steal their identity and assets. When identity theft takes place over the Internet, it is called phishing.

“Identity theft occurs when someone uses your personal information such as your name, Social Security number or other identifying information without your permission to commit fraud or other crimes. Typically, identity thieves

use someone’s personal data to empty the victim’s financial accounts, run up charges on the victim’s existing credit cards, apply for new loans, credit cards, services or benefits in the victim’s name, file fraudulent tax returns or even commit crimes. People whose identities have been stolen can spend months or years—and their hard-earned money—cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn’t commit

See **Phishing 33**



A Cyrillic character set was used to compose the message.

The “To” line is blank.

The IRS logo was blocked by my browser’s security settings.

Do not follow any “click here” instructions.

Poorly worded, thinly veiled threat.

# Phishing

CONTINUED FROM 32



The IRS website tells how you can help catch the bad guys.

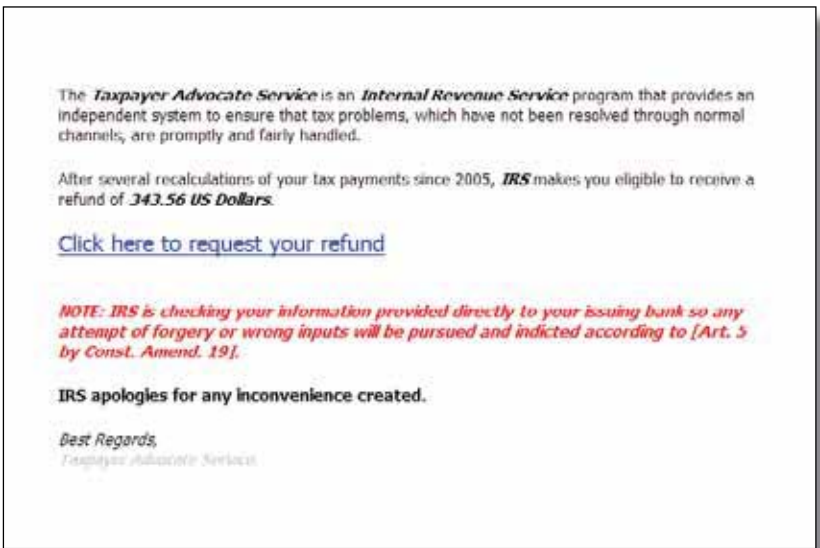
<http://www.irs.gov/newsroom/article/0,,id=155682,00.html>

Some key points to remember:

- The IRS does not initiate contact with taxpayers via e-mails.
- The IRS does not request detailed personal information through e-mail or ask taxpayers for the PIN numbers, passwords or similar secret access information for their credit card, bank or other financial accounts.
- Do not open any attachments to questionable e-mails, which may contain malicious code that will infect your computer.

An e-mail message can be traced to its point of origin if the header information is preserved. The article provides e-mail client-specific instructions for capturing the header information and forwarding it to the Internet fraud investigation team.

I tried the first method they recommended, which is to create a new message and drag the suspicious email to the body of the message, where it becomes an (.eml) attachment. However, this didn't work for me because the resulting message was too big to send.



Several days later I received this letter with a new threat to “indicate” any “wrong inputs” according to Amendment 19, Article 5 of the US Constitution. (Article 5 establishes that a two-thirds majority of both Houses is required to pass an amendment.)

(This was strange because it seemed on the surface to be a very small message, but it obviously contains some hidden goodies.)

The second method is to open the suspicious message and on the File menu, click Properties. Then select the text that is displayed on the Details tab and send it to the Internet fraud investigation team at the IRS.

The header includes the IP address (in dotted-quad notation) of the Internet service provider that sent the message, as well as the IP address of your own service. This information can be used to trace the hosting Web site and in turn, alert authorities to the scam.

Only after viewing the header information did I realize that this message had been sent to my avatar. (This is the real world me speaking now.) And I can guarantee that Pollywog Gardenvale has never filed a tax return and could therefore not possibly be entitled to a refund.

I took a closer look at the original message and noticed the text in the title bar said, “IRS Notification - Tax Refund - Cyrillic (Windows)” which means that the message was sent from a computer that had the Russian character set installed. I also noticed that the “To” line was blank which meant the message was probably part of a mass mailing.

So I decided to dig a little deeper and clicked the Message Source button to examine the underlying HTML. That's when I discovered that the Click here link was going to a domain called “axiome-informatique.fr” which was registered in France. It was linked to a .php page, (which is typical for a data entry form that feeds into a backend

database). Although it might have been risky to follow the link, I decided to take a peek at the axiome-informatique home page, just to see if it looked like a real business. All it contained was the following message:

“En cour de maintenance ...”  
Undergoing maintenance? Right.



A simple search on a French Whois registry revealed the name of the person to whom the domain is registered, the administrative contact, and the name of the company that hosts the domain.



The French Whois reveals the identifies of the people responsible for the website.

Also interesting is the fact that the IRS logo was read into the message from a direct link that is four levels deep within the actual IRS website. Could this be an inside job? Nah! All they did was go to the IRS web site and View Source. The path to the IRS logo is there for all the world to see.

So to make a long story short, I sent the header text to the Internet fraud investigation team at the IRS. And for good measure, I also sent it along to Inspector Clouseau, because he will certainly know how to “criminally pursue and indicate” them. ☹