



"IRS" Refund Phishing Scam

This scam is on the rise and there are several variations. However, the underlying theme remains the same – the scam tries to convince unsuspecting taxpayers into believing that they are due a refund. The victims are then directed to an authentic looking website to provide personal information to receive such refund.

Initial contact is made via e-mail that is phishing for personal information. Scams related to IRS refunds have been around as long as we have been paying taxes. This particular scam originated from the United States and first became noticed in November of 2005.

How it Works:

This scam frequently uses the following tactics:

- Potential victims receive an e-mail that looks very official claiming to be from the U.S Internal Revenue Service.
- The e-mail claims that the recipient is eligible for a tax refund.
- The e-mail purports to be from tax-returns@irs.gov, with a subject line of "IRS Tax Refund."
- A link is provided in the e-mail to an access form that the victim is told is required to be completed in order to receive the refund.
- The taxpayer then provides their name, address, social security number and credit card information via this website interface. The criminal has then captured personal information of the victim that can be used to perpetuate identity theft and other crimes of fraud.
- The victim is then notified that they will be receiving their refund in several weeks.

Impact:

This is an advanced phishing scheme. The victims were originally taken to an actual IRS website and then redirected to the criminals site. The criminals were able to achieve this due to a configuration issue on the government site. Now that the configuration issue has been remediated, potential victims are taken to a phony site. Albeit not as advanced as when the scam originally surfaced, it continues to be effective.

There are now reported incidents of identity theft and account fraud related to this scam.

Sample:

There are now several variations of this scam. Some of the details will vary and the following sample should only be used as an example to illustrate what such an e-mail may look like:

You are eligible to receive a tax refund for \$571.94

To access the form for your tax return use the link below:

victims are then instructed to copy and past the link into the address list of their browser

12 days left to apply for your refund. You may not receive your refund as quickly as you expected. A refund can be delayed for a variety of reasons. For example, a name and Social security number listed on the tax return may not match the IRS records. You may have failed to electronically sign the return or applied after the deadline.

This email has been sent by the Internal Revenue Service, a bureau of the Department of the Treasury.

If you believe that you may be a victim of this scam, or other crimes of identity theft or fraud, use the following guidelines and resources to report your incident;

1. Do not open any attachments in this e-mail, in case they contain malicious code that may infect your computer.
2. Contact the IRS at 1-800-829-1040 to determine whether the IRS is trying to contact you about a tax refund. Remember though, the IRS will never try to contact you about a refund through an e-mail.

Source: About.com, By Brian Koerner