THE PENNSYLVANIA
LAWYER
MAY | JUNE 2012

Scammers Are Targeting You

How to avoid becoming a victim of 'phishing'

How to Avoid Becoming a Victim of Phishing

Be aware that scammers often use fake IRS notices or requests as bait

By Phyllis Horn Epstein

Cybercrime is the evil twin of cyber communications. Electronic communications have become as much a part of our existence as plastic wrap or cartridge pens. But the ease of communications and availability of information has a darker side when left to the machinations of cybercriminals intent on stealing financial information and your identity.

Phishing is a play on the word "fishing." In the process of phishing, criminals cast their lines with enticing bait hoping to lure an unwitting guppy into biting on a malevolent attachment or link that will enable their financial crimes. The Internal Revenue Service is the bait in the latest round of phishing, with potentially disastrous results.

Phishing is the cyber search for personal information under the guise of a seemingly legitimate inquiry designed to acquire information to enable further crimes or theft through access to bank accounts and credit cards. With information obtained through phishing, criminals are capable of identity theft, using that information to take out bank loans, apply for benefits, commit crimes or file fraudulent tax returns. Phishing activities may damage your computer by introducing viruses to your hardware or by surreptitiously allowing password access by a remote thief.

Is This Communication for Real?

The IRS never initiates contact with a taxpayer through email. The IRS would never ask for or seek confirmation of your tax ID number, PINs, bank accounts, passwords or any other financial information through electronic communications. In short, you will never be asked for personal or financial information through an IRS email.

A message that appears to be from the IRS either promising you a refund or warning of an investigation is almost certainly phishing. Some contain a link to a form that purports to allow you to claim a refund. Invitations to participate in an online IRS-sponsored survey are also phishing. Another scam reports that your electronic federal tax payment was rejected and directs you to a website for additional information where malware will be downloaded to infect your computer. Frequently the scam message contains a link to a fraudulent, imitation IRS website where personal information such as a Social Security number is requested.

You will never be asked for personal or financial information through an IRS email. Any communication from the IRS will be through the U.S. Postal Service.

Often the purpose of phishing is to secure enough information to enable the thief to file a second tax return and steal the tax refund that might otherwise be due.

These fraudulent sites often bear the IRS logo. They are deceptively close copies of legitimate IRS Web pages. The IRS has posted samples of phishing on its official website at www.IRS.gov. Websites or Web communications that end with ".com" or ".net" or ".org" are *not* the IRS. They are fraudulent imitations.

Some phishing emails may have incorrect grammar or spelling because they originate from outside the country. Reportedly the U.S. Treasury's inspector general for tax administration has identified phishing sources in more than 64 countries, including Argentina, Aruba, Australia, Austria, Canada, Chile, China, England, Germany, Indonesia, Italy, Japan, Korea, Malaysia, Mexico, Poland, Singapore and the United States.

In reality the IRS will never call or write for proprietary information in any form, even by fax. Scams can arrive by mail, telephone and fax with the same nefarious purpose. In fact it is just the opposite because any communication from the IRS will be through the U.S. Postal Service and will always include the name of the author, an employee ID number, telephone and fax numbers and the appropriate Social Security number or employer identification number of the taxpayer.

What to Do If You Suspect Phishing

If you are contacted by electronic means from what appears to be the IRS, the IRS offers the following advice:

- Do not reply to the message.
- Do not open any attachments. Attachments may contain malicious code that will infect your computer.
- Do not click on any links. If you have clicked on links in a suspicious email or phishing website and entered confidential information, go to the IRS website and enter the search term "Identity Theft" for more information and resources to help.

You should also report any phishing attempts to the IRS. A suspicious email should be forwarded to phishing@irs.gov and then deleted. If you encounter a website that you suspect is not legitimate, the IRS recommends that you send the URL to phishing@irs.gov with the words "Suspicious Website" in the subject line. The IRS has received more than 30,000 messages concerning suspected phishing and uncovered nearly 2,000 phishing sites.

Suspicious letters, calls or faxes can be reported to the IRS at 800-829-1040 where you can discover if there is a legitimate IRS inquiry under way. The IRS recommends the following procedure for telephone calls during which someone purports to be from the IRS:

- Ask for a call-back number and employee badge number.
- Contact the IRS to determine if the caller is an IRS employee with a legitimate need to contact you.
- If you determine that the caller is an IRS employee with a legitimate need to contact you, call the person back.
- If the call, letter or fax turns out to be a scam, the IRS recommends that you report it to the U.S. Treasury's inspector general for tax administration at 800-366-

4484 and fax the materials to (202) 927-7018.

If you receive an unsolicited email or fax regarding a stock purchase, the IRS recommends the following.

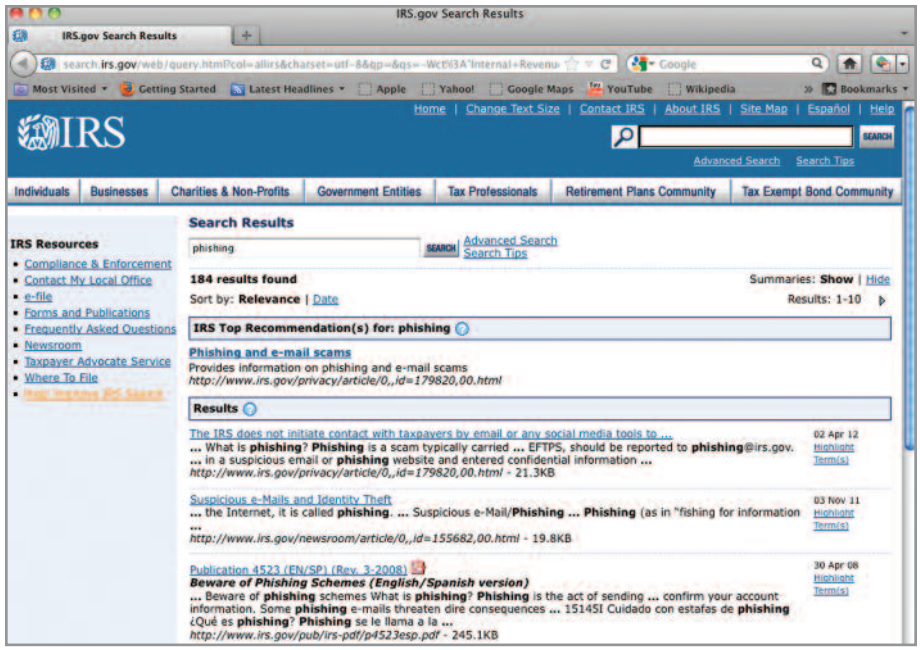
If you are a U.S. citizen residing in the United States or abroad:

- File a complaint form with the U.S. Securities and Exchange Commission (SEC).
- Forward email to phishing@irs.gov with the word "Stock" in the subject line.
- If you are a victim of monetary theft, file a complaint with the Federal Trade Commission (FTC).

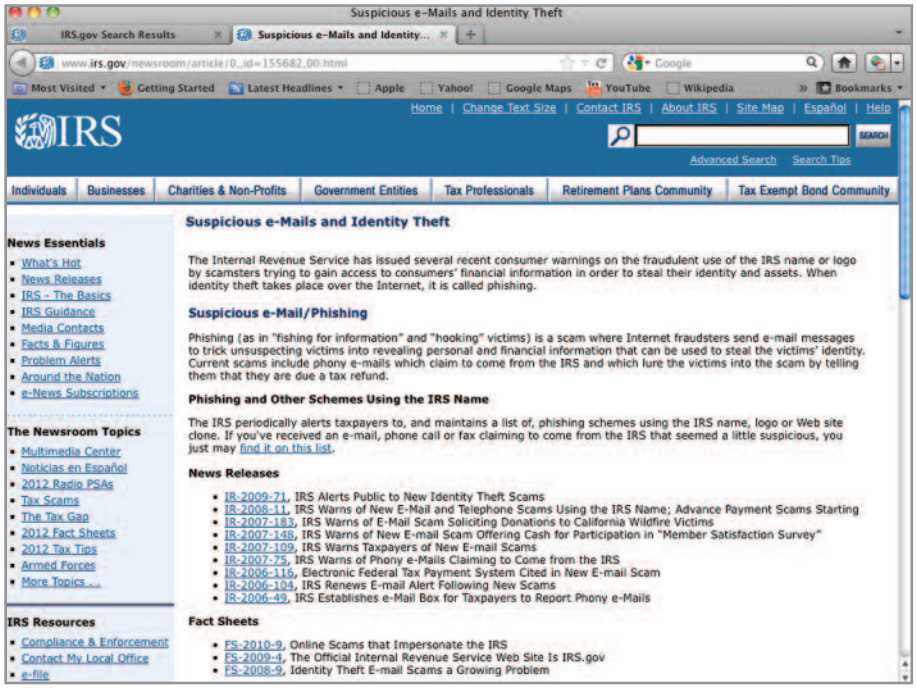
If you are not a U.S. citizen and reside outside the United States:

- File a complaint form with the SEC.
- File a complaint with your securities regulator.
- Forward email to phishing@irs.gov with the word "Stock" in the subject line.
- If you are a victim of monetary theft, file a complaint with www.econsumer.gov.

Another frequent scam is the delivery of a fake form W-8BEN by email or fax. Form W-8BEN is the Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding and is completed by foreign nationals who must pay tax through withholding in the United States. Form W-8BEN is completed by the person's employer and is never received by email or fax. The fake documents solicit additional information such as a mother's maiden name, passport number, date of birth, PINs and pass codes — none of which is required on a legitimate form W-8BEN. Some scams claim that this information is needed to comply with anti-money-laundering regulations or to confirm tax exemption on earnings. Fake forms should be reported to the IRS at phishing@irs.gov. If fake forms are received by fax, include the word "Fax" in the subject line of your email report to the IRS.



A recent search for the word phishing on the IRS website, www.IRS.gov, produced 184 results.



A compilation of IRS publications and resources on suspicious email and identity theft is posted on the IRS website at www.irs.gov/newsroom/article/0,,id=155682,00.html.

IRS Publication 4535, "Identity Theft Prevention and Victim Assistance," is posted on the IRS website at www.irs.gov/pub/irs-pdf/p4535.pdf.

The IRS has devoted new energy to combating identity theft, creating a new IRS Identity Protection Specialized Unit.

What to Do If You Become a Victim

Because criminals act fast, you should act fast to limit the damage that might be done. In addition to reporting all theft and scams to law enforcement, you should take other immediate action. Because cybercriminals may use your information to charge on your credit cards or open new cards in your name, you should get a copy of your credit report from one of the major credit bureaus to check on activity. A free report can be ordered at www.annualcreditreport.com. Report any unauthorized activity to the credit bureaus and credit card companies.

If you believe that you have unwittingly disclosed personal information through phishing or theft, secure your tax account by reporting the incident to the IRS at 800-908-4490 and complete and file Form 14039, the IRS Identity Theft Affidavit. For identity theft, you should file a complaint with the FTC at www.ftc.gov.

Recently the IRS has devoted new energy to combating identity theft, creating a new IRS Identity Protection Specialized Unit available at 800-908-4490. You can call the unit to report concerns if you are at risk for identity theft or have not been otherwise successful in your attempts to report a theft. In 2011 the IRS issued some taxpayers an additional IP-PIN, or Identity Protection Personal Identification Number, for use when filing their tax returns. In 2010 the IRS instituted a pilot program to prevent misuse of identification numbers of deceased taxpayers. The IRS is also minimizing use of full Social Security numbers for identification purposes. In May of 2007 the Office of Management and Budget issued memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," directing all federal agencies to take steps to safeguard Social Security numbers. The IRS is following this directive by reducing its use of full Social Security numbers on all communications, including forms and letters sent to taxpayers and others.

A suspicious email should be forwarded to phishing@irs.gov and then deleted. If you encounter a website you suspect is not legitimate, send the URL to phishing@irs.gov.

The IRS tries to minimize errors and tax refund fraud through new screening filters used to spot false returns before they are even processed. Often the purpose of phishing is to secure enough information from the taxpayer to enable the thief to file a second tax return and steal the tax refund that might otherwise be due to the legitimate taxpayer. You may only learn of this when your return is rejected or a notice is sent from the IRS letting you know that a tax return was already filed under your ID number. You may also learn of tax return fraud when you discover corrections to your return with income information that is clearly not yours.

At this writing there are 27 states that have separate criminal statutes that specifically address phishing, although Pennsylvania is not among them. The federal government missed an opportunity to make phishing a separate crime by failing to enact the Anti-Phishing Act of 2005, which would have imposed fines of up to $250,000 and prison terms of up to five years. Without a phishing statute, relief is only available for actual victims of cybercrimes.

You or someone you know may have been the target of cybercrime, either because of hackers who steal whole databases from merchants or through simple negligence by the keepers of information. Some of us will recall nostalgically the theft of credit card numbers from old carbon paper copies on credit card receipts before the day when carbon paper was


Beware of phishing schemes

What is phishing?

Remember these tips:

Beware of phishing schemes involving the IRS

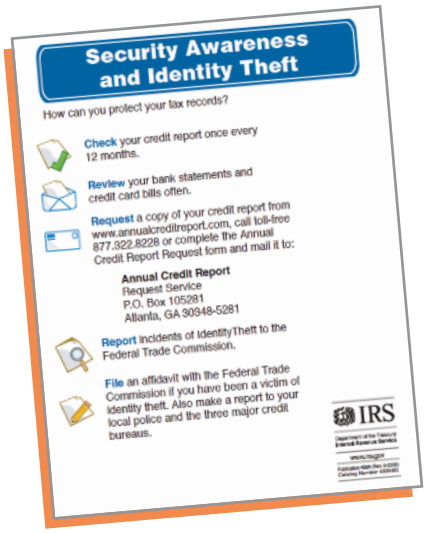
What if you believe you've been a victim of a scam?

What if you become aware of an IRS-related phishing scam?

How do I report other IRS scams?

How do I report tax fraud?

IRS Publication 4523, "Beware of Phishing Scams," is posted on the IRS website at www.irs.gov/pub/irs-pdf/p4523esp.pdf.


Security Awareness and Identity Theft

How can you protect your tax records?

Check your credit report once every 12 months.

Review your bank statements and credit card bills often.

Request a copy of your credit report from www.annualcreditreport.com, call toll-free 877.322.8228 or complete the Annual Credit Report Request form and mail it to:

Annual Credit Report
Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

Report incidents of identity theft to the Federal Trade Commission.

File an affidavit with the Federal Trade Commission if you have been a victim of identity theft. Also make a report to your local police and the three major credit bureaus.

IRS

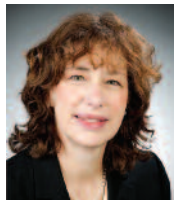
IRS Publication 4524, "Security Awareness and Identity Theft," is posted on the IRS website at www.irs.gov/pub/irs-pdf/p4524.pdf.

eliminated and security digits placed on the back of cards. Some have suffered the misappropriation of private information by dishonest store merchants or vendors.

What Inquiries Are Legitimate?

How can you determine what is a legitimate IRS inquiry and what is not? It is important to remember that the IRS will never contact you by email or fax. Any inquiries, notices, offers or surveys you receive purporting to be from the IRS either by email or fax are going to be part of a scam. The legitimate website for the IRS is www.IRS.gov. Any variation on that identity is not a legitimate website.

The IRS will initiate contact with taxpayers by letter and may follow up with a call from an authorized agent who will be required to give you his or her employee identification number. If you have any concern about the identity of the person, get his or her ID number and call back to the IRS number below to confirm that the person is a reputable agent. If you have any doubt or suspicion about a call, regular mail inquiry, fax or email, do not hesitate to confirm that the IRS is engaged in a legitimate inquiry by calling 800-829-1040. ✦


Phyllis Horn Epstein

Phyllis Horn Epstein is PBA treasurer and a partner with Epstein, Shapiro & Epstein PC in Philadelphia. You can contact her at phyllis@eselaw.com.

If you would like to comment on this article for publication in our next issue, please email us at editor@pabar.org.