

Attorney General Jon Bruning
Guest Column: March 5, 2007
Contact: Holley Hatt, 402-471-2067

Beware of Tax Refund E-mail Scams

It's tax season. Of course, we're all hoping for a refund, but don't let the lure of a little extra cash in your wallet hook you into a phishing scam. In a phishing scam, thieves pose as legitimate organizations to steal a person's identifying information through an e-mail solicitation.

This year, we've seen an increase in the number of tax refund scams. Thieves are posing as the Internal Revenue Service (IRS) and sending e-mails to consumers. The e-mails notify consumers that they are eligible to receive a tax refund for a specific amount and ask them to fill out an online form to receive their money.

Although the form looks like an authentic IRS form, it is not. The IRS does not communicate with taxpayers or request personal information via e-mail. Consumers end up turning over their personal information to thieves. Instead of receiving a refund, they lose their identities and their money.

Here are some tips to avoid becoming a victim of a phishing scheme:

- Treat unsolicited e-mail requests for financial information or other personal data as suspicious.
- Do not respond to an unsolicited e-mail or click on a link within the e-mail. The link may be corrupted and send you to a bogus Web site. Instead, delete it.
- Contact the actual government agency or business to find out if the e-mail is genuine. Call the IRS at (800) 829-1040 to check the validity of an e-mail you receive.
- Check your monthly credit card and bank statements for suspicious transactions.
- Check your credit report every year for free at www.annualcreditreport.com.

For more information about tax refund or phishing schemes, contact the Attorney General's Consumer Protection Division, toll free at (800) 727-6432 or by visiting our Web site at www.ago.ne.gov.