

Watch Out For IRS Phishing

The Internal Revenue Service, noting an increase in identity-theft scams, is raising alarms about emails designed to dupe taxpayers into disclosing personal financial information.

IRS and Treasury Department officials have noticed an increase this winter in the frequency and sophistication of "phishing" schemes that use the tax agency's logo to lure victims.

The Treasury Inspector General for Tax Administration, which investigates groups or individuals impersonating the IRS, found 12 Web sites hosting such schemes operating in 11 countries.

In a "phishing" scam, identity thieves send emails masquerading as official communication from a government agency, bank or other institution in an attempt to solicit personal data. The data could include financial account numbers, passwords or credit-card numbers. The thieves use the information to steal a person's identity and commit financial crimes, such as using the victim's credit cards or opening new ones, applying for loans or filing fraudulent tax returns.

"Phishing" emails purporting to come from the IRS often tell taxpayers they are due a refund and direct them to a false IRS Web site. The email address may include "irs.gov," such as tax-refunds@irs.gov or admin@irs.gov.

Taxpayers who file their tax returns electronically might get an email acknowledgment when the tax return is accepted, but that email would come from the company providing tax software or professional preparation services, not the IRS.

Taxpayers can check the status of their refund through the IRS Web site (www.irs.gov). That tool asks taxpayers for their Social Security number, filing status and the exact refund due.

Those who receive fraudulent IRS email can contact the Treasury Inspector General for Tax Administration at 800-366-4484.