

## Scammers Lurk at Tax Time

During tax-filing season, scammers and hackers may try to put your potential refund in their pocket.

### How It Works:

Tax identity theft occurs when someone steals your Social Security number to file a fraudulent tax refund or to get a job. There are also computer viruses out there (the “Emotet” virus for one) that can send emails supposedly from the IRS with a fake copy of your tax return. Once you click it, you may become vulnerable to hackers.

And of course, the ever-present IRS impostor scam calls tend to be much more common this time of year.

### What You Should Know:

- If the IRS receives a duplicate tax return filing using your Social Security number, you will receive a written notice through the mail.
- Likewise, the IRS will send a notice if you have unreported income or that you and someone else are claiming the same dependents.
- The IRS will *not* initiate contact with you by e-mail, text or social media. The IRS will not call you unless you have first heard from them by mail, and will **never** insist on wired money payments, cash or gift cards/pre-paid money cards.

## Potential Ways to Reduce Your Risk of Being Victimized:

- Submit your tax return as early in the tax season as possible.
- Be careful what you share – don't give out your personal information unless you know who is asking and why, and don't be shy about refusing.
- Never open e-mail attachments that are not from a verified sender.
- Dispose of sensitive information safely – shred it with a micro-cut shredder.
- Know your tax preparer.

Check the status of your refund after filing at [www.irs.gov/refunds](http://www.irs.gov/refunds). If you receive notice from the IRS that you are a victim of identity theft, call the number on the notice or 800-908-4490 right away. Learn more at [www.identitytheft.gov](http://www.identitytheft.gov).

You have the power to protect yourself and your loved ones from scams. Please share this alert with friends and family.