Beware of This New Identity Theft Scam

We usually warn you about cybercriminals who use emails and social media to steal your identity. The bad guys in this new scam use a different approach – a delivery service.

In this recent scheme, the bad guys send a letter "from the IRS" in a delivery service cardboard envelope. The letter indicates that the recipient has an outstanding tax refund but needs to provide proof of identity. Such proof includes pictures of the taxpayer's driver's license, bank account information, and social security number.

If you've read any of our scam alert articles, you know what to look for to determine whether requests for personally identifiable information are legitimate:

- **Does the request make sense in the context of who's asking for the information, the type of information requested, and the purpose?** In this case, it could make sense that the IRS would notify you about an outstanding refund, but the request for your bank account and social security number is not reasonable, as the IRS should already have that information on file for you.
    - Also beware of messages that look like they come from a trusted source (friends, family, co-workers) that request confidential information. When in doubt, proceed cautiously and independently verify the request (i.e., contact the sender in a different manner rather than replying to the original message) before taking any action or providing information.

- **Is the request worded in a professional manner?** That means the communication should be written with good grammar, including no typos or proofreading mistakes. In this case, the letter is full of poorly written sentences such as "Once You Send All The Information Please Try to Be Checking Your Email for Response From the Agents Thanks".

- **Is the request sent in an appropriate manner?** The IRS communicates with taxpayers regarding tax bills and refunds using snail mail. That doesn't include a delivery service, so that would wave another red flag regarding this letter.

Criminals are always looking for creative ways to steal your money. While this latest scheme comes from a different angle, the cautions are the same. Don't respond to messages (however the delivery method) that request confidential information unless you're absolutely, positively, 100% certain the request is legitimate. Scammers can even pose as a trusted source, such as your bank, a friend or family member, or even your boss. Always proceed cautiously. If you have any doubts, contact the sender using a different communication method (i.e., if the message comes by email, pick up the phone and call the sender using a phone number you've independently verified).

More information about tax-related scams can be found on the IRS website by clicking here [https://www.irs.gov/privacy-disclosure/report-phishing].