Beware Of The Fake Tax Form Scam

Tax season means a paperwork blizzard. Often, someone loses a copy of an important document and needs it to be re-issued. Naturally, everyone's too busy to verify the authenticity of each request.

That's what scammers are counting on with a recent ploy targeting people who prepare tax forms. In this scheme, the scammer sends an email claiming to be a hired company or someone from the IRS requiring duplicate copies of W-2s. An overworked clerk fears noncompliance with the tax authority and sends the forms.

Those forms contain personally identifiable information, including a name, address and a Social Security number. With that information, fraudsters can open fake credit cards, apply for loans, or file a fraudulent tax return in an attempt to grab a refund check.

If you're targeted

If you prepare W-2s, be on guard for these fake emails. Here's the sample text from one such message:

"ATTN: Due to some complains (sic) we had concerning the W-2 mismatch, We advice (sic) you to send your 2015 filled W-2 form in (PDF) format for confirmation."

Notice the abbreviations, the typographical errors, and the poor punctuation. These should tell you this isn't the professional work of the IRS.

You may also get a similar message that appears to be from your boss. Watch for the same typos and always confirm these requests in another message. Also, look out for emails from former employees. Scammers may be relying on outdated information.

If someone really needs another copy, it's safest to mail it to them. Email is never fully secure. It's also unlikely that someone would need duplicate copies of ALL W-2s. Be suspicious of any such request.

If your information has been compromised

If your information has been unwittingly released by your employer, don't panic. Minimize the impact of this data breach with these three steps:

First, call one of the major credit bureaus: Experian, Equifax or TransUnion to request a fraud alert on your account. This will force anyone who wants to issue credit in your name to verify their identity.

Next, order a copy of your credit report to see all the accounts open in your name. If there's anything you don't recognize, immediately close the account. Also, review statements for the accounts you have. If you see any charges you don't recognize, call the issuing institution and shut the account. Alerting them about fraud as soon as possible limits your liability.

Third, file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov. This will create a fraud affidavit, a document certifying that fraud occurred. This will help when you need to file a police report.

It's worth filing your taxes early. If a thief tries to file a tax return using your information after you've already done so, the IRS will be alerted to the fraud.