Scammers are at it again!

The IRS recently released a statement regarding continual scams that are increasing during the tax season. Besides the usual phone scams aiming individuals, thieves are also stealing client information from tax accountants to use it to file fraudulent tax returns. They use the client's bank account information for the deposit, then utilize numerous methods to access the accounts and steal the funds.

Tax preparers and businesses should ensure that they have adequate security to protect their clients' tax and financial information from cyber-attacks. Some of these protections could include an annual review of the security of workstation and server computer systems as well as any cloud service providers (Microsoft Office 365, Google Apps Suite, and others), internal policies and procedures (password policies), software application security (remote access software, anti-malware, server operating system updates) and employee training programs (phishing emails, scams and malware).

If you are a *self-preparer* and possibly your computer has been compromised, some of the procedures for a tax office could be a good policy for yourself. If your tax accountant's files have been victimized, there are steps to consider taking to protect yourself.

If you receive a phone call, do not give out any information over the phone. Read this article, for more information for your protection: link. Reminder to use any of the IRS' recommended steps:

1. Contact the IRS, FBI and local police right away.
2. Report the data theft to state agencies (state tax returns).
3. Contact and engage a forensic computer expert to determine the cause and scope of the theft.
4. Notify credit reporting agencies.
5. Contact relevant software portal providers to reset passwords and prevent the compromised account from being accessed by an attacker.

Mir Taxes LLC www.mirtaxes.com