

Tax Time Scams You Should Avoid

Whether it's phishing, identity theft or hidden fees, tax season can bring out the scammers in full force. Learn how to protect yourself from the most common tax scams.

Let's face it: most people dislike tax season. It can be stressful, confusing and financially painful.

There are some people, though, who enjoy it: scam artists. For these unscrupulous characters, tax season brings with it limitless opportunities to prey on the innocent and rob them of their hard-earned money.



Scam artists are experienced in a variety of schemes that earn them millions of dollars every year. They take advantage of the trusting nature of people who are too baffled by the tax code to realize when they are being swindled.

If you know what to look for—simple signs that betray the scam artist's deception—you can survive tax season unscathed.

Scammers play on fears, vulnerabilities -

Phishing and identity theft are the most common tax scams. Phishing can take many forms, but typically it's done through phony emails. Scam artists adopt false identities as a way to extract personal information from their targets or to plant destructive software into a person's computer.

They often pretend to be IRS agents, informing their targets of problems with their returns or refunds and telling them that the only solution is to send their Social Security numbers or bank account information. Or the email will include a link that, when opened, installs into the victim's computer spyware or malware that can then mine all their files and personal data.

Unfortunately, this scam is often successful because people tend to be scared of the IRS.

This scam is easy to spot, however, because the IRS never contacts people via email.

Continued on the next page.



Nancy Phelan	22 years
Gerianne Kohut	20 years
Dave Wall	16 years
Cortney Meng	13 years
Loreen Primiano	4 years



2.65% APY
17 month CD

\$50,000 minimum deposit to open and obtain the APY. Offer begins on February 10, 2019. Annual Percentage Yield is realized when a principal deposit and all interest earned is left on deposit for one year. Fees could reduce earnings on the account. Early withdrawal penalties may be imposed. New money only. Offer expires 03-31-2019.



Tax Scams (continued)

Once they have a Social Security number in hand, the scammers can file a phony tax return in the victim's name, claiming a large refund and having it sent to a false address.

More red flags to watch for -

Another red flag is a tax preparation fee based on a percentage of the return instead of a flat fee. The IRS doesn't prohibit it. However, those may be fraudulent returns, because there is a financial incentive for the preparer to induce you to claim funds you're not entitled to.

Beware the refund anticipation loan -

When it comes to collecting their refunds, people are often given the option to either wait several weeks for the Internal Revenue Service to mail a check or to pay a tax preparer or financial institution a fee to receive it right away.

This is called a refund anticipation loan, a short-term loan backed by an expected tax refund. It is perfectly legal, but it can be very costly.

Some companies who offer these types of loans will give a taxpayer a debit card to withdraw the cash from their tax refund. Each ATM withdrawal, however, has a maximum that may be withdrawn at one time and carries a fee of up to \$2.50 paid to the lender (tax preparation service) and an additional fee of up to \$2.50 paid to the ATM operator. By the time all of the refund is retrieved using multiple withdrawals, these fees may absorb more than 10 percent of the original amount.

The bottom line is, if it sounds too good to be true, it probably is! Seek professional advice from the IRS or a tax professional before you partake in any scheme. What to do if you think you've become a victim of a tax scheme?

Report all unsolicited email claiming to be from the IRS or an IRS-related function to phishing@irs.gov. If you've experienced any monetary losses due to an IRS-related incident, please report it to the Treasury Inspector General Administration (TIGTA) at treasury.gov and file a

complaint with the Federal Trade Commission (FTC) at ftc.gov to make the information available to investigators. (source: irs.gov)

How can we help you?

As always, please also contact The Milford Bank if you think you may be the victim of a scam. We can help to safeguard your bank accounts, report fraudulent activity to the credit agencies and walk you through filling out the appropriate paperwork.

What can you do to avoid becoming a victim?

Here at The Milford Bank, we have an array of free services to help keep your financial information safe!

We recommend you sign up for:**eStatements:**

eStatements offer you the convenience of keeping all of your account information in one secure place, get your statements earlier and no risk of losing them in the mail.

CardValet:

The power to manage your debit card on-the-go is now available in our mobile banking app. See transactions in real time with instant alerts. Turn payments on or off, which is handy when you can't locate your card. Set a location (geographic) boundary where the card can be used. Restrict card use to certain types of businesses. (Enable grocery store while turning off restaurants.)

Notifi:

This service in your mobile banking app allows you to set real-time alerts, notifying you when certain transactions occur. You can set up the following alerts to receive updates on your account activity: Daily Balance Alert, Balance Alert, Transaction Alerts, Overdraft Protection Alert, and an Insufficient Funds Alert.

Security Tips eNewsletter:

Learn about the latest scams and what you can do to avoid them.

Find instructions to sign up for these valuable safety tools on our website or call or stop by and office for details!

Mark your calendars! The Milford Bank's next shred event will be held on Saturday, May 4th from 10 am until 1 pm at our Post Road West Office, located on 295 Boston Post Road. Look for more information in next month's customer newsletter.

