THE FINE PRINT

Be on alert for the IRS's 'dirty dozen' tax scams

With the filing deadline less than two week away, criminals are busy trying to steal your money.

By Sean P. Murphy
Globe Staff,Updated May 4, 2021

E-mails seeking personal information such as a Social Security number are a common tactic of tax scammers. Jenny Kane/Associated Press

With the deadline for filing income tax returns looming on May 17 — it was extended by a month because of the pandemic — the Internal Revenue Service is warning of scam artists constantly trying to steal your money and your personal financial information — now and year-round.

"Be on guard at all times and look out for others," particularly seniors and others who may be especially vulnerable, the IRS says.

Tax time or not, it's always important to be vigilant.

"Nobody is immune to scams," said Lucilia Prates, statewide director of Senior Medicare Patrol, a Lawrence-based nonprofit that counsels seniors. "Everyone is vulnerable."

Unscrupulous tax return preparers

Watch out for any preparers who won't sign your tax return, known as "ghost preparers." They may expose you to serious filing mistakes as well as possible tax fraud and loss of your refund.

Unscrupulous preparers may promise inflated refunds by claiming fake tax credits. Avoid preparers who ask you to sign a blank return, promise a big refund upfront, or charge fees based on a percentage of the refund.

The IRS has a searchable **listing** of preparers who are currently recognized by the IRS. You can also do a background check on a preparer by looking online for reviews. The Better Business Bureau may be a good place to start.

Resolving tax debt

If you owe back taxes, be wary of any company making promises about getting it resolved. These companies may exaggerate their ability to settle tax debts, while charging pricey fees to submit an application to the IRS for relief. The IRS accepts very few of these cases (known as its "offer in compromise" program).

Prates said consumers should be similarly on guard when callers offer to reduce their credit card debt.

If you owe taxes, you can use an IRS online tool to see if you **pre-qualify** for the offer in compromise program.

Fake payments with repayment demands

Sometimes criminals put a bogus refund into a taxpayer's bank account, then call the target posing as the IRS. The taxpayer is told that there's been an error and that the IRS needs the money returned immediately to avoid penalties and interest. The taxpayer is instructed to buy gift cards for the amount of the refund.

Anytime someone asks you to buy a gift card and give them the serial numbers on the back, that's a red flag, Prates said.

Threatening impersonator phone calls

A popular ruse used by criminals is to call claiming to be the IRS and demanding money. (The latest wrinkle to this is "spoofing," in which clever scammers manage to have a local telephone number, or even the name of a government agency, utility, or other entity pop up on your screen, to trick you into answering their calls.)

Callers may threaten deportation or license revocation, trying to stir up fear in their targets. The threats may come from "robocalls," voice recordings left on phones with instructions for returning the call.
The scammers are well practiced on how to manipulate you.

"They're very good at it," said said Betsey Crimmins, a Greater Boston Legal Services attorney. "They know just what to say."

Best thing to do? Just hang up or don't answer at all if you don't recognize the number.

Payroll and HR scams

Scammers may target your employer to steal tax information and compromise business e-mail accounts. With access to your e-mail, the con artists may change your direct deposit information to reroute deposits to an account they control.

Make sure to monitor your bank accounts closely for any possible irregularities.

Phishing

Is that e-mail in your inbox really from whom it appears to be from? Is that text message on your phone screen legit?

Phishing is when criminals impersonate legitimate organizations via e-mail or text message to steal your sensitive information, such as passwords, account numbers, or Social Security numbers.

They create e-mail accounts for themselves that, at first glance, look like the real thing, but are different by one letter or by the domain name (.com, .org, .gov and so on).

Unless you are certain of their origin, don't reply to e-mails, and don't click on links or attachments in those e-mails.

Fake charities

Have you received a telephone call or e-mail asking you to donate to a charity that you are familiar with? Pause and consider whether it's a charity that merely *sounds* like the one you are familiar with.

Con artist frequently set up fake charities and then solicit donations by telephone, text, social media, e-mail, or even in-person. Often the names they choose mimic the names of legitimate charities.

Before making that donation, talk about it with a family member, friend, or other person you trust.

"Don't be in a hurry," Prates said. "A legitimate charity can always wait another day or week."

Social media scams

Scammers cruise public social media sites in a cunning strategy to find the kind of information that may fool you. For example, they may learn your grandson's name and the name of the college he's attending.

One familiar scam is to call a grandparent to say their grandson has been arrested and needs money to be bailed out, while adding a sense of legitimacy by casually referencing his name and college.
In one case I recently learned of, the scammers brought an "attorney" on the phone line to "explain" the situation.

Check out the privacy settings on the social media site you use and consider limiting the amount of personal information you post.

Stimulus or refund theft

One reason criminals steal identities is to file false tax returns to divert stimulus and refund checks to the wrong addresses and bank accounts.

Anyone who believes they may be a victim of identity theft should consult the Taxpayer Guide to Identity Theft on IRS.gov.

Senior Fraud

Seniors are more likely to be targeted and victimized by scammers than others.

"Older adults are targeted because they may be retired and at home to pick up the phone, and because they often have assets," said Odette Williamson, a staff attorney at the National Consumer Law Center in Boston.

Seniors need to be alert to scammers trying to steal personal information by calls, and by fake e-mails, text messages, websites, and social media.

Seniors are also susceptible to fraud in personal and professional relationships. Having a trusted friend or family member involved in a senior's affairs may be a deterrent.

Scams and frauds against seniors are vastly underreported because many victims feel too embarrassed to admit it and fear doing so could lead to a loss of independence.

Scams targeting non-English speakers

Like seniors, those with limited English proficiency are heavily targeted by scammers intent on stealing personal financial information. Sometimes, the con artists may already have pieces of information — the last four digits of their Social Security number, for example — to make themselves look legitimate.

Malware and ransomware

Malware is a form of invasive software that may be inadvertently downloaded by a user. Once downloaded, it tracks computer activity, and may lock critical or sensitive data with its own encryption.

Victims may receive a ransom request in a pop-up window demanding payment in virtual currency such as Bitcoin in exchange for release of the encrypted data. Scammers often use phishing e-mails to trick victims into opening links or attachments containing the ransomware.