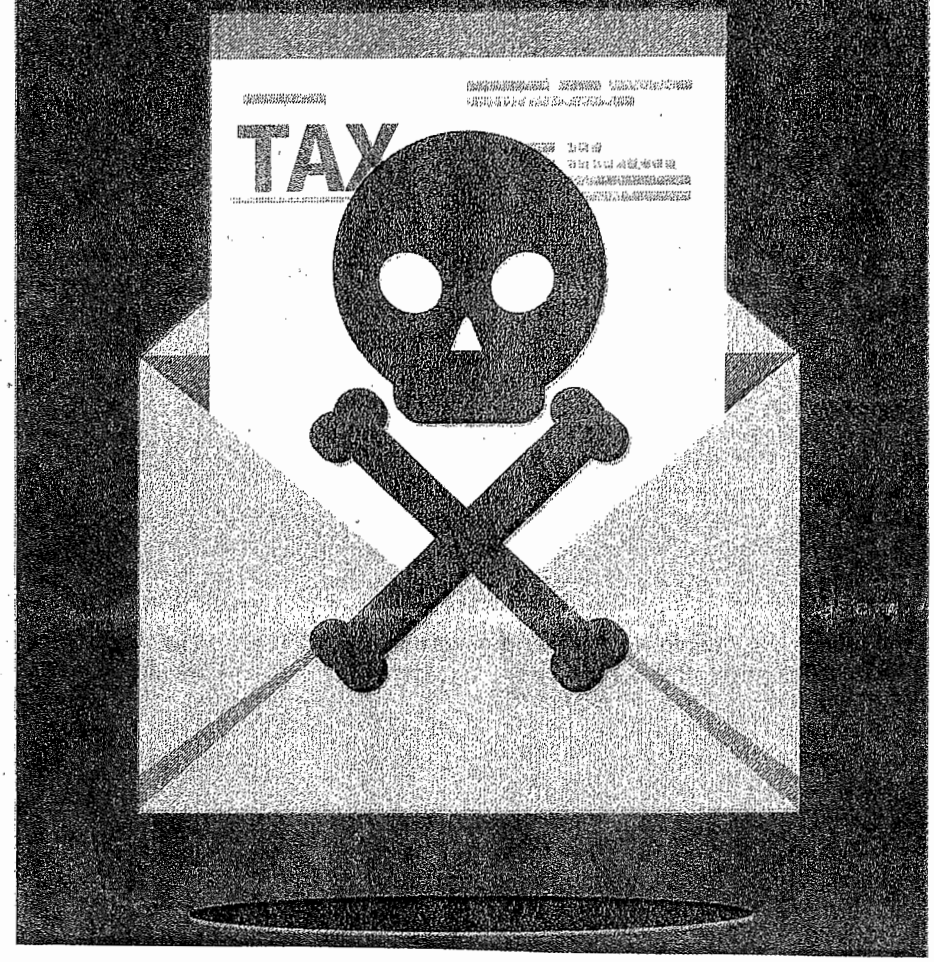
WATCH OUT FOR THESE TAX SCAMS

Hackers and crooks will be busy long before the April 15 deadline



Most of us find it nerve-wracking enough that we're forced to focus on gathering our piles of paperwork to fill out our tax returns.

Now adding to our stress, we must watch out for tax season scam artists, too. The crooks are everywhere from the gym parking lot to the latest emails and text messages.

A new trend: Expect an increase in ransomware attacks in 2020 on tax preparers where time-sensitive files may be frozen and only thawed when tax preparers pay a ransom to the hackers, according to Adam Levin, founder of CyberScout, which offers identity theft protection and data security.

Levin said sometimes a ransom is paid, the files are released and the hackers still use data that has been stolen to file false tax returns.

Fraudsters want your Social Security number and other key personal information in order to file fake tax returns as early as they can in the season to claim inflated tax refunds.

So, the con artists will be busy long before the April 15 tax deadline.

The crooks want to e-file tax returns before you do because they know that the Internal Revenue Service system will reject a tax return when the IRS has already received another return using the same Social Security number. The IRS will first process e-filed tax returns Jan. 27.

One huge red flag for ID theft: You discover that you can't e-file your tax return because of an issue relating to a duplicate Social Security number. (The IRS also will re-

ject an e-filed return for basic errors, such as if you misspelled the name the IRS has on file, but you would be able to resubmit an e-file in many cases if the issue is properly corrected.)

If you discover that a fraudulent tax return has been filed with your Social Security number, you must first file IRS Form 14039 to alert the IRS that you're a victim of ID theft.

In 2018, the 649,000 confirmed fraudulent returns attempted to claim $3.1 billion in refunds, according to the IRS.

The IRS said it stopped 597,000 tax returns filed by identity thieves claiming $6 billion dollars in tax refunds 2017. As part of a Security Summit Initiative, the IRS is working with representatives of state tax agencies, tax preparation firms, payroll processors and others to combat tax refund fraud that hinges on stolen personal information.

The crooks get a leg up by stealing key information to make their fake returns look more legitimate. Much financial information already is out there after major data breaches such as those at Equifax, the U.S. Office of Personnel Management and Anthem. But cybercriminals are still actively seeking Social Security numbers and other data, too, with tricks as common as a phishing email that targets tax professionals, retirees or business owners.

Here's a rundown on some of the latest scams:

They're calling about your Social Security

Crooks are claiming that there is a problem with your Social Security account. Some may tell you that your Social Security number has been suspended. It's another attempt to scare you into returning a robocall.

Many demand action now. Some want you to "verify" your financial information, such as your Social Security account and banking information. Others might demand money on a gift card or Bitcoin.

In January, the Inspector General of Social Security warned that telephone scammers may take the next step by sending phony documents by email to convince potential victims that they must comply with the fraudster's demands. The attachments may involve letters that appear to be from Social Security or the Social Security Office of the Inspector General. But retirees and others shouldn't be fooled by official-looking letterhead and government jargon.

A new online system was announced in November to report Social Security scams online at oig.ssa.gov.

Never provide sensitive information – or authenticate yourself – to someone who contacts you out of the blue, Levin said. Don't trust caller ID.

Does that IRS notice seem weird?

ID thieves are increasingly showing sophisticated knowledge of the tax code and even aiming to file fraudulent tax returns relating to a business or partnership, according to the IRS.

Business owners are warned that one sign of trouble is that the company may fail to receive routine correspondence from the IRS because the thief has changed the address for the business. Or you might receive an IRS notice that doesn't seem to make sense based on your business or tax situation.

Tax preparation software for business-related returns now requests more information to protect the tax filer, including the name and Social Security number of the company executive authorized to sign the corporate tax return.

Sophisticated phishing scams are targeting payroll offices, too, and requesting W-2 information. Scammers might pose as the CEO or vice president of the company's payroll organization trick someone with access to data into disclosing sensitive information for the entire workforce.

"This scam has emerged as one of the

most dangerous phishing emails in the tax community," according to H&R Block's Tax Institute.

The W-2 scam has hit all types of organizations – big corporations, small businesses, public schools, universities, hospitals, tribal governments and charities.

"Never click on a link or open an attachment without independent confirmation of the sender," Levin warns.

Cybercrooks are engaging in social engineering to make some emails seem more legitimate. Some may reach out to you directly by name to sound like your boss, such as: "Dear Chris: You really messed up this time. See attached."

Or you might receive a text, robocall or email that's supposedly from the security department of your bank or the board of elections to "confirm your information on file." A text may even say your account has been frozen due to suspicious activity and ask you to click on a link and enter your USER ID in order to resolve the issue.

Don't be fooled. Contact your bank directly if you're concerned.

Levin warned that some of the malware-laden links may include authentic-looking graphics, excellent grammar and no misspellings.

"Often the only way to tell something is amiss is by looking at the URL – but even that can be misleading," Levin said.

Is your tax preparer about to get scammed?

Fraudsters have really narrowed their focus on tax preparers, not only to steal client data but also to get their hands on information from the professional, such as e-service passwords, said Andy Phillips, director of H&R Block's Tax Institute.

"If a fraudster is able to hack into a tax preparer's network, they may be able to steal personal information of all clients that have filed with that preparer," Phillips said.

Some fraudsters, he said, have even found ways to change refund account information to ensure that the fraudster gets the tax refund.

No, the IRS isn't emailing you a tax transcript

ID thieves are crafting phishing emails to trick users into giving up passwords and other information, perhaps by even impersonating your tax provider. And they're sending attachments hoping that you'll be duped into downloading malware.

One scam involves emails that pretend to be from the "IRS Online." The scam email carries an attachment labeled "Tax Account Transcript" or something similar, and the subject line uses some variation of the phrase "tax transcript."

Phillips, of H&R Block, said other examples of imposter IRS emails include phrases such as "Automatic Income Tax Reminder" or "Electronic Tax Return Reminder."

The pitch might look more legitimate because of links that show an IRS-like website and details pretending to be about a taxpayer's income tax refund or e-filed return. Some emails contain a "temporary password" to access the files.

"But when taxpayers try to access these, it turns out to be a malicious file," Phillips said.

You can forward malicious emails to phishing@irs.gov.

ID thieves still steal purses and wallets

Crooks can go the old-fashioned route by breaking into unlocked cars in a subdivision or lockers at the local gym to steal personal ID information too, such as a Social Security card or an old Medicare card that includes your Social Security number in your wallet.

It should go without saying but you need to make sure that you don't leave tax returns on the kitchen table or sitting on the front seat of your car where crooks could access that information too.