IRS Nationwide Tax Forum 2021

Treasury Inspector General for Tax Administration
Helping You and Your Clients Steer Clear of Fraud and Scams

Wednesday, August 4, 2021

Start Time: 11:00am Eastern / 10:00am Central
9:00am Mountain / 8:00am Pacific

Note: You should be hearing music while waiting for webinar to start.

Having Technical Issues?
View the "Technical Issues" troubleshooting guide in the Materials drop-down menu on the left side of this page

Today our webinar will:

- Define TIGTA's role in protecting the integrity of tax administration;
- Clarify TIGTA's Main Components;
- Discuss preparer ethics and misconduct issues; and
- Discuss scams and cyber-fraud activity targeting tax professionals.

What is TIGTA?

- Provides independent oversight of the IRS;
- Protects the integrity of Federal tax administration;
- Detects and prevents waste, fraud, and abuse at the IRS;
- Has three primary operating divisions:
  - Office of Audit;
  - Office of Inspection and Evaluations; and
  - Office of Investigations.

Office of Audit

- Promotes the economy, efficiency, and effectiveness of tax administration;
- Provides recommendations to improve IRS systems and operations and to ensure the fair and equitable treatment of taxpayers; and
- Audit recommendations result in:
  - *Cost Savings*
  - *Increased Revenue Protection*
  - *Protection of taxpayers' rights and entitlements*
  - *More efficient use of resources.*

Examples of TIGTA Audits

- IRS Processing of Economic Impact Payments (EIPs) -
  - Alerted the IRS of EIPs that had been issued to potentially ineligible individuals. In response to our alert, the IRS added instructions to IRS.gov to inform these types of individuals of their ineligibility and the need to return these payments, including the process to be followed. As of October 1, 2020, individuals voluntarily returned 65,447 payments totaling more than $80 million.

- IRS Compliance Efforts Regarding High-Income Taxpayers -
  - Recommended that the IRS emphasize the use of income information to identify high-income taxpayers who have the ability to pay their delinquent taxes, establish high-income balance due cases as a higher collection priority, and develop a strategy for working high-income balance due cases. Also, that the IRS implement controls that will assist to identify and prioritize high-income nonfilers who are repeat offenders.

- IRS Strategy for Gig Economy Workers -
  - Determined that almost $481 million in self-employment taxes could have potentially been assessed if the IRS had a strategic plan to address gig economy taxpayer noncompliance.

Inspections and Evaluations

- Inspections and Evaluations provide factual and analytical information, assess the effectiveness and efficiency of programs and operations, and inquire into allegations of fraud, waste, abuse and mismanagement. These reviews often result in recommendations to streamline operations, enhance data quality, and minimize inefficient and ineffective procedures.

Inspections and Evaluations (Cont.)

- Recent Inspections and Evaluations -
  - *Oversight of Reported Sexual Harassment Allegations Needs Improvement (March 2021)*
  - *The IRS Leveraged Its Telework Program to Continue Operations During the COVID-19 Pandemic (March 2021)*
  - *Controls Over the Pseudonym Program Need Improvements (June 2020)*

Office of Investigations

- Identifies and investigates IRS employee misconduct;
- Protects the IRS from external threats and corruption;
- Protects the integrity of IRS programs, operations, critical infrastructure; and
- Detects and prevents waste, fraud, and abuse.

Disclosure Restrictions

- As a component of the Treasury Department with tax administration duties, TIGTA is bound by Title 26, United States Code, Section 6103 (Section 6103), the tax information confidentiality law; and

- Section 6103 prohibits the disclosure of tax returns or return information, except as authorized by an exception contained in the statute, or as made public record in a tax administration proceeding.

Ethics and Integrity

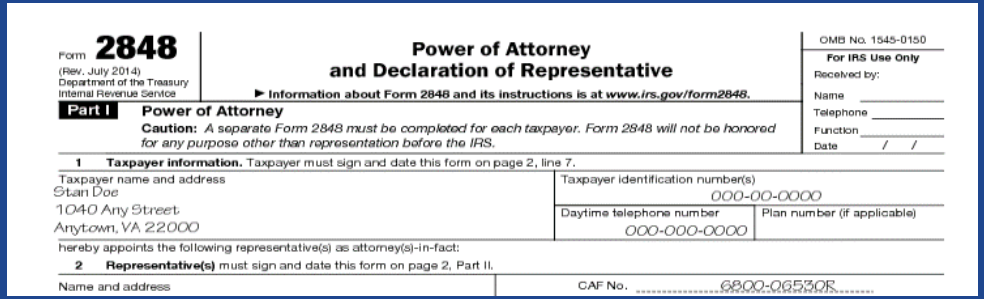
- Ethics[1]: A set of moral principles. A theory or system of moral values.
- Integrity[2]: Firm adherence to a code of moral or artistic values. Incorruptibility.
- MEANING always doing the right thing, even when no one is watching.

Circular 230

- Circular 230, also known as Subtitle A, Part 10 of Title 31 of the Code of Federal Regulations (CFR);
- Sets forth rules under which tax preparers can represent clients before the IRS; and
- IRS' Office of Professional Responsibility (OPR) oversees most preparer conduct.

Preparer Misconduct Examples

- False statements on IRS Form 2848, *Power of Attorney and Declaration of Representative*; and



Form **2848** (Rev. July 2014)
Department of the Treasury
Internal Revenue Service

Power of Attorney and Declaration of Representative

▶ Information about Form 2848 and its instructions is at *www.irs.gov/form2848.*

OMB No. 1545-0150

For IRS Use Only
Received by:
Name
Telephone
Function
Date / /

Part I **Power of Attorney**

Caution: *A separate Form 2848 must be completed for each taxpayer. Form 2848 will not be honored for any purpose other than representation before the IRS.*

1 Taxpayer information. Taxpayer must sign and date this form on page 2, line 7.

Taxpayer name and address	Taxpayer identification number(s)	
Stan Doe 1040 Any Street Anytown, VA 22000	000-00-0000	
	Daytime telephone number 000-000-0000	Plan number (if applicable)

hereby appoints the following representative(s) as attorney(s)-in-fact:

2 Representative(s) must sign and date this form on page 2, Part II.

Name and address	CAF No.
	0800-06530R

- Failure to disclose that preparer is disbarred or otherwise unauthorized to appear before the IRS;

Preparer Misconduct Examples (Cont.)

- Sending e-mails or fabricating documents purporting to be from the IRS;
- Improper disclosure of a client's tax information;
- Fraudulent levy releases; and/or
- Unauthorized disclosure of protected tax information.

IRS Nationwide Tax Forum | 2021

Tax Preparer Sentenced to Two Years' Imprisonment for Tax Fraud

- On December 14, 2020, a tax preparer was sentenced to two years imprisonment for conspiracy to defraud the United States. He was initially charged with aiding the filing of a false tax return and conspiracy to defraud the United States.

- The tax preparer added false income information such as wages, fictitious businesses, and erroneous tax credits to his clients' tax returns without their knowledge or consent. The tax preparer kept a portion of the fraudulent tax refunds for himself. Upon learning the IRS froze several of his clients' tax returns, he furthered the conspiracy by filing a complaint with the Treasury Inspector General for Tax Administration (TIGTA).

- The tax preparer was sentenced to 24 months' imprisonment, three years' of supervised release, and ordered to pay $110,840 in restitution.

IRS Nationwide Tax Forum 2021

Volunteer Income Tax Assistance Return Preparers Indicted for Defrauding the IRS

- On December 9, 2020, two tax preparers, were indicted for jointly conspiring to commit wire fraud and wire fraud in connection with the submission of a false application to the Internal Revenue Service (IRS) for the Volunteer Income Tax Assistance (VITA) grant .

- The tax preparers applied for and was awarded a grant for $50,000 from the IRS' VITA Program. Upon review, it was discovered that tax preparers provided false information in their VITA grant application, failed to disclose a relevant personal relationship, and submitted fabricated receipts and volunteer logs to the IRS.

- If convicted, both tax preparers could individually receive a statutory maximum penalty of 30 years' imprisonment and/or a fine of up to $1 million.

Tax Preparer Sentenced for Wire Fraud in Theft of Economic Impact Payments

- On February 24, 2021, a tax preparer was sentenced for wire fraud related to a scheme to defraud the Internal Revenue Service (IRS) and obtain money by filing fraudulent tax returns. The tax preparer had previously been indicted on June 18, 2020, for wire fraud, theft of Government money, and aggravated identity theft.

- The tax preparer allegedly unlawfully obtained Personal Identification Information (PII) of individuals, which included their names, birth dates, and Social Security Numbers from his employer, and other sources. The tax preparer also unlawfully obtained IRS Electronic Filing Numbers assigned to tax preparation firms, which they were not affiliated, to electronically file the returns and claim false tax refunds totaling $7,814. The filing of the false tax returns also triggered the issuance of Economic Impact Payments totaling $3,400.

- The tax preparer received six months' imprisonment, three years of supervised release, ordered to pay $5,800 in restitution, and a $100 assessment fee.

IRS Impersonation Scam

- One of the largest telephone scams;
- Calls received by taxpayers in every State;
- Callers claim taxpayers owe taxes and must pay immediately; and
- Callers are aggressive and threatening.

TIGTA's Approach

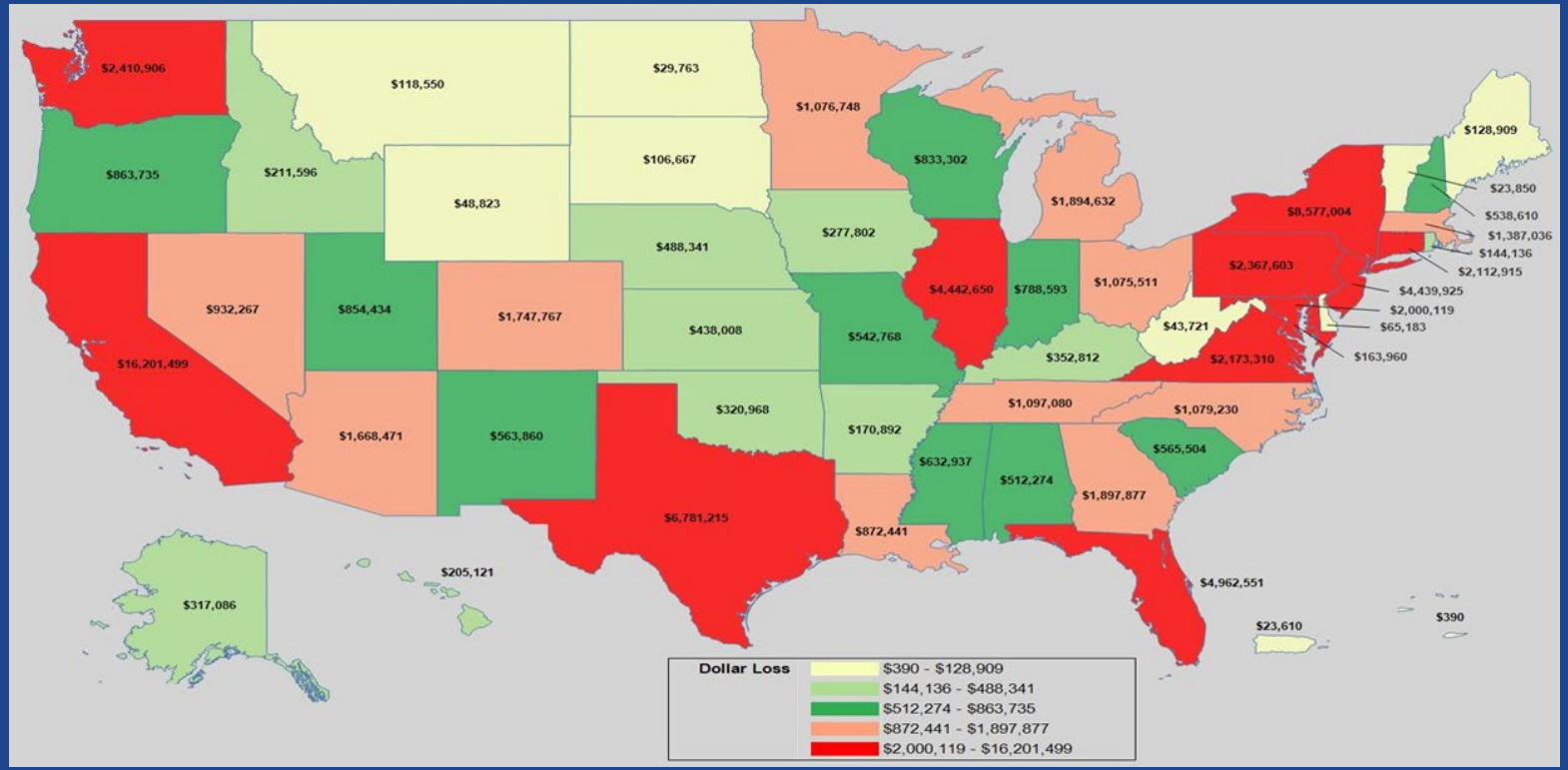
- TIGTA is dedicated to educating the public to prevent fraud against the IRS and to protect taxpayers;
- PSAs are available on YouTube in English and Spanish; and
- "Advise and Disrupt" strategy created to help combat the impersonation scam.

Traits of Scam Callers

- May know information about the intended victim – such as digits of Social Security Number, address, banking information, etc.;
- May spoof caller identification information to appear as if calling from the IRS;
- May demand payment via wire transfers or a prepaid money card such as: Green Dot®, iTunes®, MoneyGram®, or Western Union®;
- May send bogus IRS e-mails to legitimize the scam; and
- May follow-up with subsequent calls, claiming to be the police, Department of Motor Vehicles, or the IRS to verify initial debt claims and confirm threatened legal action.

IRS Nationwide Tax Forum | 2021

Losses by State



IRS Impersonation Scam Investigations

- November 30, 2020: Telemarketing Call Center Owner and Director plead guilty in the Eastern District of New York, to conspiracy to commit wire fraud in connection with a fraudulent scheme directed at thousands of individuals in the United States.

- October 21, 2020: Man and Voice over Internet Protocol (VoIP) provider were indicted in the Northern District of Georgia, in connection with facilitating the passage of tens of millions of scam calls to American taxpayers on behalf of phone scammers.

- July 9, 2020: Man pled guilty in the Northern District of Georgia, for his role in a wire fraud conspiracy to defraud U.S. citizens. He used approximately 15 false identities to pick up wire transfers, in multiple States, from victims of the scams.

- May 28, 2020: Woman was indicted in the District of Oregon, with bank fraud, while on pre-trial release for other Federal offenses. She created a fictitious IRS identity to conceal her role in a scheme to defraud a former employer by stealing more than $1 million, over several years.

- July 21, 2020: Woman pled guilty in the District of Nevada, to conspiracy to commit wire fraud and aggravated identity theft for her role in a scheme. She admitted to being a leader in the conspiracy, recruited at least 10 additional runners, and directed others to recruit more.

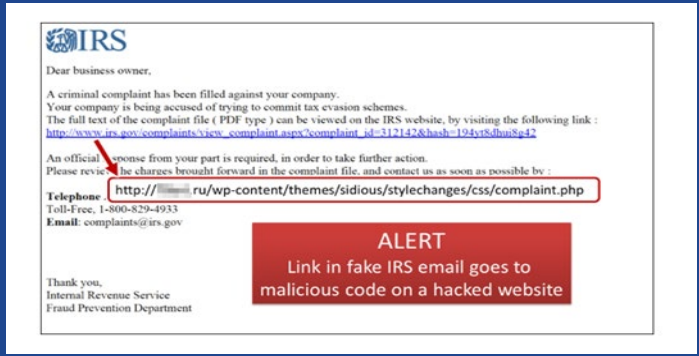
Other Impersonation Scams

"LOTTERY" Scam

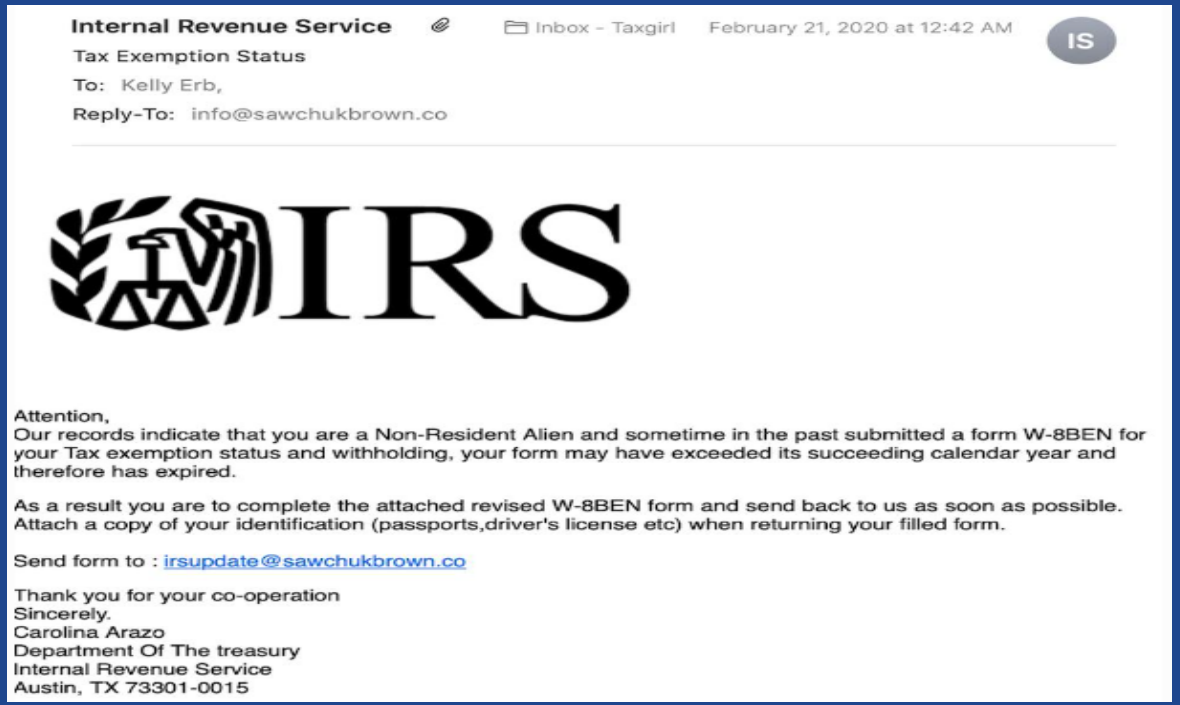
- On March 11, 2020, in the District of Connecticut, five individuals were charged, in an 11 count indictment, for their roles in defrauding elderly victims of more than $4 million.
- Some victims were told they had won the lottery, but must send payment for taxes and other fees before receiving winnings.
- The defendants could each face 10 years, or more, of imprisonment for each count.

Other Impersonation Scams (Cont.)

- False IRS websites;
- Hyperlink on spam e-mail; and
- Phishing.



Official IRS E-Mail?



Internal Revenue Service Inbox – Taxgirl February 21, 2020 at 12:42 AM

Tax Exemption Status

To: Kelly Erb,

Reply-To: info@sawchukbrown.co

IS

IRS

Attention,
Our records indicate that you are a Non-Resident Alien and sometime in the past submitted a form W-8BEN for your Tax exemption status and withholding, your form may have exceeded its succeeding calendar year and therefore has expired.

As a result you are to complete the attached revised W-8BEN form and send back to us as soon as possible. Attach a copy of your identification (passports,driver's license etc) when returning your filled form.

Send form to : irsupdate@sawchukbrown.co

Thank you for your co-operation
Sincerely.
Carolina Arazo
Department Of The treasury
Internal Revenue Service
Austin, TX 73301-0015

Steps for Handling Suspicious "IRS" E-Mails

1. Forward the suspect e-mail(s) to **phishing@irs.gov**;

2. Delete it from your computer; and

3. **DO NOT** reply, open any attachments, or click on any links.

IRS Nationwide Tax Forum | 2021

NEW SCAM ALERT

IRS Role in Coronavirus Aid

- The Coronavirus Aid, Relief, and Economic Security (CARES) Act was signed into law on March 27, 2020;
- The American Rescue Plan Act (ARPA) was signed into law on March 11, 2021; and
- The IRS has implemented a plan to deliver economic impact payments to eligible taxpayers and individuals receiving Social Security benefits.

IRS-Related Coronavirus Scams Need to Knows

- The Treasury Department and the IRS **will not** call, text, e-mail, or mail individuals claiming to offer coronavirus-related grants or economic impact payments in exchange for personal financial information; and

- The IRS will not request a fee, or the pre-payment of taxes, to receive a qualifying economic impact payment, including the purchase of gift cards.

IRS-Related Coronavirus Scams Need to Knows (Cont.)

- Anyone who receives an e-mail, text message, or phone call claiming to help get them benefits **should not** respond;
- Anyone eligible to receive an economic impact payment will have it deposited into the account annotated on their last filed tax return from 2018 or 2019; and
- Anyone whose last filed tax return did not list a bank account will have a check mailed to their last address of record.

IRS Coronavirus Scams Investigations

- May 19, 2020: Man charged in the in the Eastern District of Texas, wire fraud, bank fraud, false statements to a financial institution, and false statements to the Small Business Administration in connection with the Coronavirus Aid, Relief, and Economic Security (CARES) Act. He allegedly obtained an Employer Identification Number (EIN) from the Internal Revenue Service (IRS) in March 2020 in order to document a business to use in fraudulent CARES Act-related loan applications.

- May 22, 2020, Man charged in the Western District of Washington, with wire fraud and bank fraud in connection with the CARES Act. He obtained EINs from the IRS in April 2020 to document two fictitious entities. He then submitted fraudulent CARES Act-related loan applications in the names of these entities.

- April 29, 2020: Man charged in the Eastern District of New York, with theft of mail, including multiple economic impact payments from the United States Treasury Department, otherwise known as “stimulus payments.”

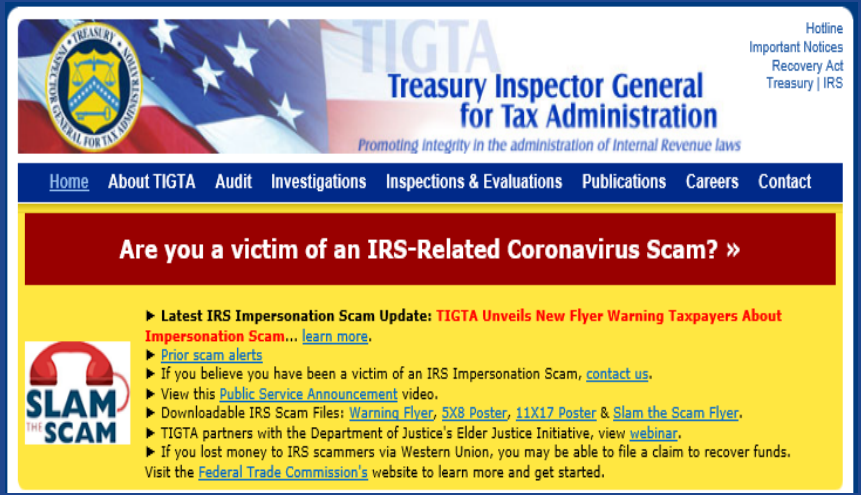
IRS Related Coronavirus Scams
What Should You Report?

Any individuals or businesses that:

- Purport to be from/working with the Treasury Department or IRS and ask for personal information to receive a qualifying economic impact payment;
- Offer early check delivery in return for personal information; and
- Say that pre-payment of taxes and/or fees are required in order to receive a qualifying economic impact payment.

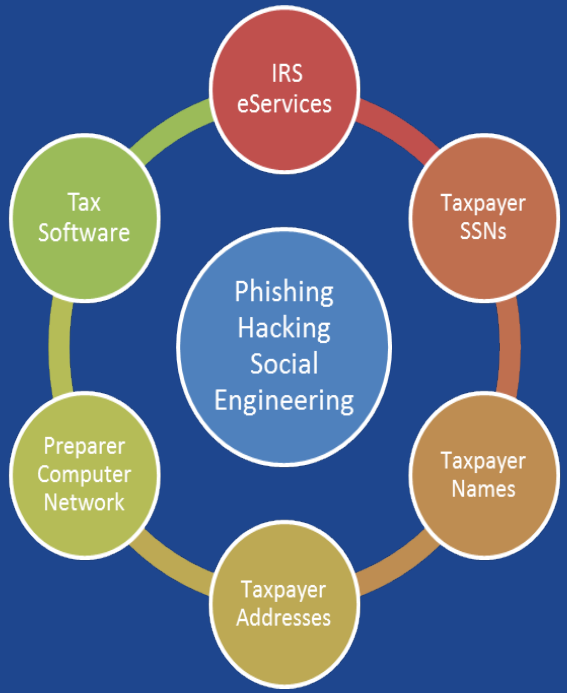
Reporting IRS-Related Coronavirus Scams

- Report potential IRS-related coronavirus scams at **https://tips.tigta.gov**



IRS Nationwide Tax Forum 2021

Cyber-Fraud Targeting Tax Preparers



"IRS, Security Summit Partners Warn Tax Professionals of high risk of data theft attacks"

IRS Press Release IR 2018 245, December 7, 2018

"Consumer Alert: IRS Warns Taxpayers, Tax Pros of New e-Services Scam"

IRS Press Release IR 2017 170, Oct. 11, 2017

The IRS today warned all e-Services users to beware of a new phishing scam that tries to trick tax professionals into "signing" a new e-Services user agreement. The phishing scam seeks to steal passwords and data.

Cyber-Fraud Statistics

2020 Reports to Federal Bureau of Investigation Internet Crime Complaint Center (IC3):

- Business Email Compromise (BEC)
  - 19,382 victims with $4.9 billion in losses
- Technical Support Fraud
  - 15,780 victims with $412 million in losses
- Corporate Data Breaches
  - 2,796 victims with $2.2 billion in losses
- Phishing/Vishing
  - 241,347 victims with $1.2 billion in losses
- Government Impersonators
  - 12,841 victims with $8.1 billion in losses
- Malware
  - 1,429 victims with $14 million in losses

Primary Cyber-Fraud Targets

- Financial and personal information:
  - On preparer's local computer network
  - In preparer software containing/processing Personally Identifiable Information (PII)
  - In preparer's IRS eServices account

- Please, always ensure that the numbers in the IRS system match what you are filing.

Common Cyber Scams

- Phishing email scams to harvest user account information;
  - "Unlock" tax software accounts
  - Posing as state accounting or professional associations
- Malicious software (malware) designed to steal financial and network account passwords;
- Advanced cyber attacks against poorly secured networks; and
- Ransomware designed to encrypt network devices.
  - Attacker offers to send key to unencrypt for a fee

Cyber Warning Indicators

- Suspicious activity indicating compromise of local network;
- IRS eServices shows login history;
  - Report dates showing login activity not made by you
- Unusual Centralized Authorization File activity;
- Take note of unauthorized IRS Form 8821, *Tax Information Authorization*, or IRS Form 2848, *Power of Attorney and Declaration of Representative*, filed in your name;

Cyber Warning Indicators (Cont.)

- Electronic Filer Identification Number (EFIN) or Preparer Tax Identification Number activity higher than the number of returns you submitted;
  - Can be viewed through eServices
- Customers receiving mailed, unsolicited tax transcripts from previous years;
- Customers receiving notification of the establishment of an eAuthentication account which they did not create; and
- Tax software vendor (*e.g.,* Drake, Intuit, etc.) advises a fraudulent IRS document with your EFIN has been submitted to secure a software purchase.

Cyber Warning Indicators What to Report to TIGTA?

- Suspicious logons or activity on your eServices account not accomplished by you;
- Submission of fraudulent IRS Forms 8821/2848 to the IRS;
- Fraudulent IRS EFIN memos sent to software vendors; and
- Customers who receive unsolicited transcripts or notices for IRS eAuthentication accounts they did not create.

Helpful IRS Publications

- Publication 4557, *Safeguarding Taxpayer Data*
- Publication 5293, *Data Security Resource Guide for Tax Professionals*
- Publication 3112, *IRS e-File Application and Participation*
- Publication 1345, *Handbook for Authorized e-File Providers of Individual Tax Returns*

What Else Can You Do to Help Protect Federal Tax Administration?

- Report instances of tax preparer or IRS employee misconduct;
- Report potential threats to IRS employees and facilities;
- Warn colleagues and clients about scams; and
- Update client address of record, Form 8822.

How to Contact TIGTA

E-mail: complaints@tigta.treas.gov

Telephone: 1-800-366-4484

Internet: http://www.tigta.gov