Neki Cox Sr. Stakeholder Liaison for Stakeholder Liaison Department in Communication and Liaison (C&L)

Neki Cox is a C&L Division Sr. Stakeholder Liaison in Denver. As a stakeholder relationship manager, she has served as a coordinator for IRS seminars, meetings, and multi-speaker engagements. She focuses on developing communication and educational opportunities with tax practitioner, civic, non-profit and for-profit business organizations in Wyoming and Montana. She leads and coordinates the IRS Disaster Assistance program with FEMA.

Neki began her IRS career in 1995. She has held other positions in the Human Capital Office as a Recruiter and Analyst, in the Taxpayer Advocate Division as a Sr. Taxpayer Advocate, and in the Exam Division as an Office Auditor, Earned Income Credit Coordinator, and an e-File Marketing Specialist. She has prior experience in computer report writing, bookkeeping, collections, purchasing, customer service, sales, and restaurant management.

Neki holds a Bachelor of Science degree in Small Business Management with an emphasis in Accounting from California State Polytechnic University, Pomona.

Tax Security 2.0
A Tax Pro's Security Checklist

Neki Cox 720-956-4447

Topics

- Taxes-Security-Together Checklist
- Outline the “Security Six” basic protections
- Create a written data security plan
- Educate yourself on phishing scams
- Recognize the signs of client data theft
- Create a data theft recovery plan

Deploy the “Security Six” protections:

1. Anti-virus software
2. Firewalls
3. Two-factor authentication
4. Backup software/services
5. Drive encryption
6. Virtual Private Network (VPN)

“Security Six” # 1
Anti-virus software

Scans computer files for malicious software

Automatic scans

Manual scans of email attachments, web downloads, and portable media

Protection against spyware and phishing

“Security Six” # 2 Firewalls

Provide protection against outside attackers

Shield computer or network

Firewalls are categorized as:

Hardware – external devices

Software – built-in or purchase

“Security Six” # 3
Two-factor authentication

Adds an extra layer of protection beyond a password

User must enter credentials

username and password plus another step (such as a security code sent via text to a mobile phone)

Poll Question #1

“Security Six” # 4
Backup software/services

- Critical files on computers should routinely be backed up to external sources
- Backup files may be stored either using an online service or on an external disk
- Encrypt the back-up data for the safety of the information

“Security Six” # 5
Drive Encryption

Use drive or disk encryption software for full-disk encryption

Transforms data on the computer into unreadable files for an unauthorized person

“Security Six” # 6
Virtual Private Network (VPN)

A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the internet and the company network

Search for “Best VPNs” to find a legitimate vendor

How to get started with the ‘Security Six’

Review professional insurance policy

Some offer coverage for data thefts

Review IRS Publication 4557, Safeguarding Taxpayer Data

Small Business information Security – The Fundamentals by NIST

www.nist.gov

Poll Question #2

Step 2: Create a Data Security Plan

Required under federal law

The Gramm-Leach-Bliley (GLB) Act

Federal Trade Commission (FTC) Safeguards Rule

IRS Revenue Procedure 2007-40 for Authorized IRS e-file Provider

Step 3: Educate yourself on phishing scams

Many data thefts start with a phishing email

Click on a link to a fake web state

Open an attachment with embedded malware

Spear phishing email to pose as a trusted source

Account Takeover

Ransomware

Example: Scam Email

Dear Tax Pro,

Your electronic filling identification number (EFIN) has temporary been put on hold due to suspicious activity with your PTIN user.

Did you transmit the below 1040 form?

TranscriptPDF

If this was you, please ignore this message.
If it was not you, please immediately change your password.
Failure to confirm this request will leads to EFIN suspended.

We are trying to protect your e-service and EFIN account.

Sincerely.

Carol A Campbell
IRS.gov e-service

Steps to help protect data

Use separate personal and business emails

Protect with strong passwords

Two-factor authentication

Install anti-phishing tools

Use security software

Steps to help protect data (cont.)

Never open or download attachments from unknown senders

Password-protect and encrypt documents

Do not respond to suspicious or unknown emails; if IRS related forward to phishing@irs.gov

Poll Question #3

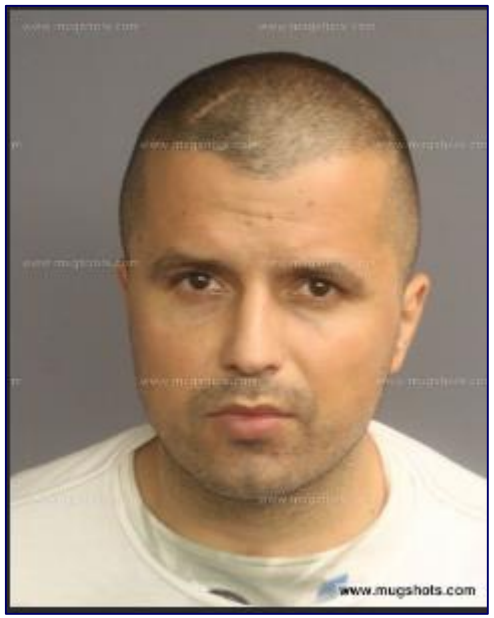
Step 4: Recognize the signs of client data theft

Tax professionals should learn the signs of a possible data theft

Data theft may result in fraudulent tax returns being filed in their clients' names

Cybercriminals are tax savvy in their attempts to gain sensitive tax data

Data Thief gets caught: costs millions



Department of Justice

U.S. Attorney's Office

District of New Jersey

SHARE

FOR IMMEDIATE RELEASE

Thursday, June 2, 2016

Bulgarian Citizen Sentenced To More Than Three Years In Prison For Role In $6 Million Tax Refund Scheme

NEWARK, N.J. – A citizen of the Republic of Bulgaria was sentenced to 46 months in prison today for his involvement in a $6 million fraudulent tax return scheme that used personal identifying information stolen from multiple accounting firm networks, U.S. Attorney Paul J. Fishman announced.

Vanyo Minkov, 33, previously pleaded guilty before U.S. District Judge Jose L. Linares to a superseding information charging him with one count of conspiring to file false and fraudulent tax returns. Judge Linares imposed the sentence today in Newark federal court.

According to documents filed in this case and statements made in court:

In late 2012, Minkov and his conspirators hacked into the networks of at least four accounting firms and stole the 2011 tax filings for over 1,000 of the firms' clients. Minkov and others then used the stolen information to file fraudulent tax returns in the clients' names for the 2012 tax year or sold the information to others for the same purpose. To date, the IRS has identified over $6 million in fraudulent claims made in connection with the scheme.

In addition to the prison term, Judge Linares ordered Minkov to serve two years of supervised release and pay restitution of $2,702,555.

Signs of Client Data Theft

Client e-filed returns begin to reject;

Clients who haven't filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS;

Clients who haven't filed tax returns receive refunds;

This Photo by Unknown Author

Signs of client data theft (cont.)

Clients/Practitioners receive tax transcripts that they did not request;

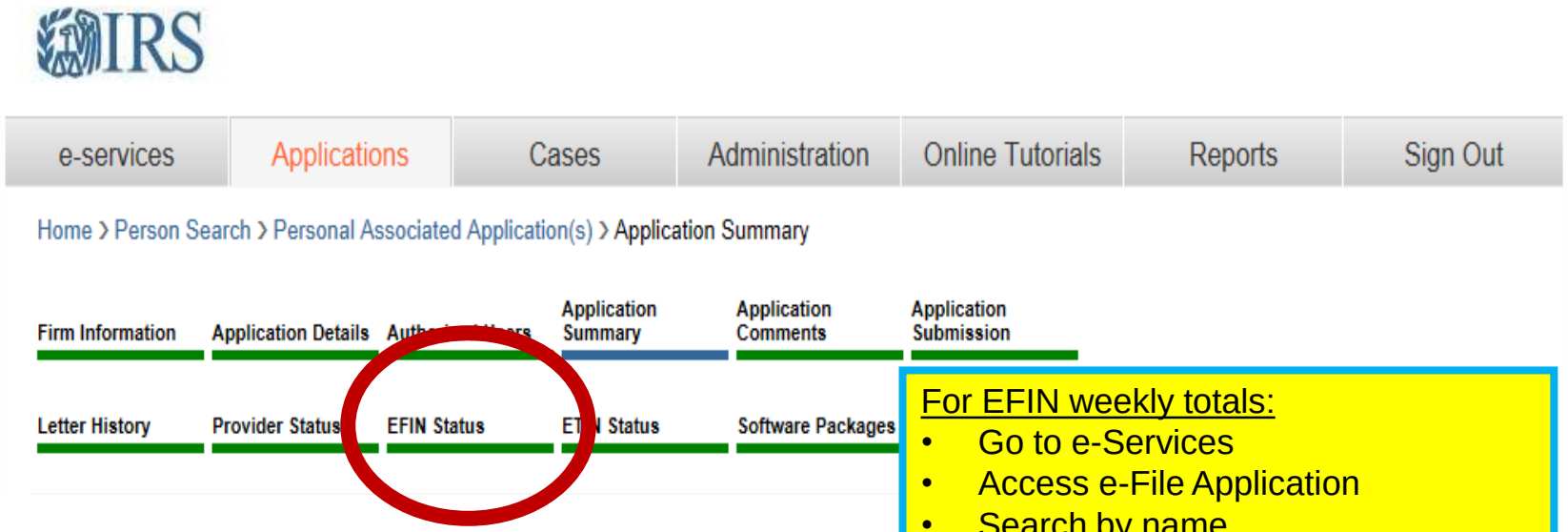
Clients who created an IRS Online Services account are notified that their account was accessed or disabled

Another variation: Clients receive notice that an account was created in their names

Signs of client data theft (cont.)

The number of returns filed with tax practitioner's Electronic Filing Identification Number (EFIN) or their Practitioner Tax Identification Number (PTIN) exceeds number of clients assisted;

Monitor Your EFIN



For EFIN weekly totals:

- Go to e-Services
- Access e-File Application
- Search by name
- Select “EFIN Status”

Report Suspected EFIN Abuse

Electronic Return Originator (ERO) Activity by EFIN/Return Type

The activity shown below by EFIN and Return Type represents the total YTD counts for returns submitted electronically to the IRS.

Customize | Find | View All | First 1-5 of 5 Last

	EFIN	Return/Form Type	Processing Year	Transmitted YTD	Accepted YTD	Rejected YTD
1	555555	1040	2016	51	50	1
2		1041	2016	9	9	0
3		1065	2016	12	12	0
4		1120	2016	10	10	0
5		1120S	2016	10	10	0

- Too many returns filed with your EFIN? Contact e-Help Desk (866) 255-0654

Monitor Your PTIN

Monitor "Returns Filed per PTIN"

Information available via online PTIN system for tax preparers who meet both of the following criteria:

Have a professional credential or are an Annual Filing Season Program participant, **and**

Have at least 50 Form 1040 series tax returns processed in the current year

How to Access PTIN Information

To access “Returns Filed Per PTIN” information, follow these steps:

1. Log into your PTIN account

2. From the Main Menu, find “Additional Activities”

3. Under Additional Activities, select “Summary of Returns Fied.”

Summary of Returns Filed Chart

IRS

Logged in as ***Doe, John***

Main Menu | Edit Login Information | Logon

Summary of Returns Filed

See the chart below for the number of tax returns with your PTIN processed by the IRS **this year**. The data is updated weekly and includes only Form 1040 series returns **processed** through the date specified.

If the number is **substantially higher** than the number of tax returns you've prepared and you suspect possible misuse of your PTIN, complete Form 14157.

If the number is **substantially lower** than the number of tax returns you've prepared, you need to verify that you are entering your PTIN correctly on returns. The most common cause of this problem is the entry of an incorrect PTIN during tax preparation software setup.

Definitions:

- Processing Year: the current calendar year
- Tax Year: the tax year of the returns
- 1040s Processed: includes **only** 1040 series returns (1040, 1040-PR, 1040-SS, 1040A, 1040EZ, 1040EZ-T, 1040NR, and 1040NR-EZ)

51 Returns as of 5/14/2019

Processing Year	Tax Year	1040s Processed
2019	2018	49
	2017	2

Step 5: Create a data theft recovery plan

An action plan can save valuable time and protect your clients and yourself

Make calling the IRS an immediate action item

Data Compromise Action Items

Contact IRS and law enforcement

Tax professionals contact IRS Stakeholder Liaisons immediately

- Search “stakeholder liaisons” on IRS.gov

Data Compromise Action Items – (cont.)

Contact state agencies:

State revenue agencies - email Federation of Tax Administrators for state agency contacts at **StateAlert@taxadmin.org**

State Attorneys General

Contact experts

Security expert

Insurance company

Data Compromise Action Items – (cont.)

Contact clients and other services

FTC for guidance for businesses

- Email: **idt-brt@ftc.gov**

Credit Bureaus

Clients

Review guidance at IRS.gov/identitytheft

Poll Question #4

Questions???

Resource - IRS YouTube Video

Resources

Publication 4557, Safeguarding Taxpayer Data

Publication 5293, Data Security Resource Guide for Tax Professionals

Small Business Information Security – The Fundamentals at NIST.gov

Key Points to Remember

Review and use the “Security Six” for measures to protect your firm.

Have a security plan and refresh your staff on security measures often.

If working remotely, have a secure VPN.

Contact SL if you become a victim of Data Loss or Ransomware.

Thank you for attending todays presentation.