Protect Your Clients; Protect Yourself
A Security Summit campaign to increase awareness among tax professionals

Date: October 20th, 25th, 27th

Shawn Savage
Senior Stakeholder Liaison
The risk is real; preparers are prime targets for identity thieves

Cybercriminal tactics constantly evolve

Data loss can occur so many ways:
- Burglar steals office computers
- Cybercriminal breaches your systems using phishing and malware schemes
- Disgruntled employees steals client info
- Dispose of old devices without erasing data
Data Theft Tactics

• Phishing emails, text or calls
  – Pose as trusted organizations
  – Embed links to fake websites
  – Use malware-infected attachments
• Risks of opening phishing scams
  – Account take-overs (Banks, IRS e-Services, Tax Software)
  – Computer breaches
• Educate employees on scams/risks
Emerging Scams

- Phishing emails posing as IRS e-Services
- Phishing emails posing as new clients
- Spoofing emails to payroll personnel requesting all employee Forms W-2
- Remote takeover of tax preparer computers
- Variations constantly emerge
- Know your clients; know your employees
IRS reviewing improvements to EFIN safeguards

- Stepped up efforts to expel EFIN abusers;
- Increased on-site visits as part of monitoring process

EFIN holders should review return numbers during filing season

- e-Services Account updated weekly
- Excessive numbers can be reported to e-Help Desk
Steps to Protect Client Data

- Read Publication 4557, Safeguarding Taxpayer Data
- Review current security measures
- Create a security plan
  - Use top-notch software security
  - Educate all employees
  - Use strong passwords
  - Secure Wi-Fi
  - Encrypt PII emails
  - Backup files
Plan Ahead for Data Loss

• Create a reaction plan for data theft
  —Call IRS Stakeholder Liaison (found on IRS.gov)
  —Notify your State Tax Agency

• Review Federal Trade Commission’s “Business Center” to assist businesses with data losses
  —Notify police
  —Notify businesses
  —Notify clients
Help Educate Clients

- IRS, state tax administrators and tax industry working together to increase public awareness about security protections online and at home.
- Review Publication 4524, Security Awareness for Taxpayers
- Consider printing and sharing this one-page guide with your clients
Protect Your Clients; Protect Yourself

• New awareness campaign underway
• Protect Your Clients; Protect Yourself page on IRS.gov
• News releases, fact sheets, tips and alerts
• Other resources:
  — e-News for Tax Professionals;
  — Twitter.com/IRStaxpros;
  — Facebook.com/IRStaxpros
Summary

- The risk is real
- Make a security plan
- Make a data loss plan
- Contact Stakeholder Liaison if you experience a data compromise
- Search terms “Stakeholder Liaisons Local Contacts” on IRS.gov
Contact Information

Name: Shawn Savage, Sr. Stakeholder Liaison
Phone Number: 304.579.6873
E-Mail Address: shawn.s.savage@irs.gov