Don’t Take the Bait, Step 1: Avoid Spear Phishing Emails

IR-2017-119, July 11, 2017

WASHINGTON — The IRS, state tax agencies and the tax industry today warned tax professionals to beware of spear phishing emails, a common tactic used by cybercriminals to target practitioners.

Spear phishing emails, often tailored to individual practitioners, result in stolen taxpayer data and fraudulent tax returns filed in the names of individual and business clients.

Information about spear phishing kicks off a new “Don’t Take the Bait” awareness campaign aimed at tax professionals. This is the first of a special 10-part series that will run each week through mid-September.

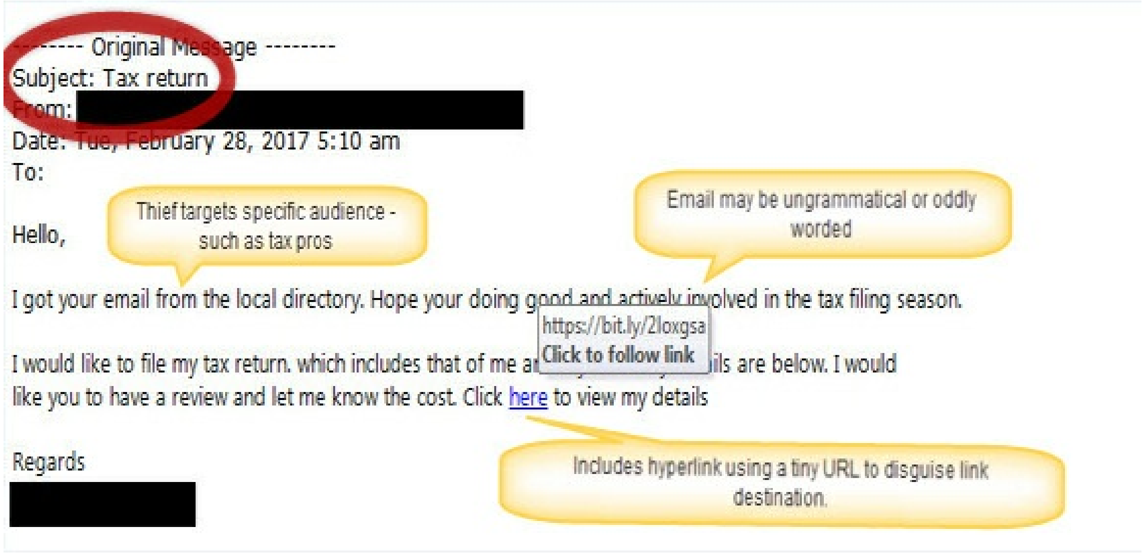
“We are seeing repeated instances of cybercriminals targeting tax professionals and obtaining sensitive client information that can be used to file fraudulent tax returns. Spear phishing emails are a common way to target tax professionals,” said IRS Commissioner John Koskinen. “We urge practitioners to review this information and take steps to protect themselves and their clients.”

The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to learn to recognize and avoid spear phishing emails. See Protect Your Clients; Protect Yourself for more information.

Phishing emails target a broad group of users in hopes of catching a few victims. Spear phishing emails pose as familiar entities, and the cybercriminals have done extensive research and homework in order to target a specific audience. Tax professionals and taxpayers are among the groups that regularly receive phishing emails.

The security software firm Trend Micro reports that 91 percent of all cyberattacks and resulting data breaches begin with a spear phishing email. The email, disguised as being from a trusted source, may seek to have victims voluntarily disclose sensitive information such as passwords. Or, it may encourage people to open a link or attachment that actually downloads malware onto the computer.

Here’s an example of a spear phishing email that targeted a tax professional during the 2017 filing season. Note the use of “Tax return” in the subject line to bait the tax preparer as the sender impersonates a prospective client:



-------- Original Message --------
Subject: Tax return
From: [redacted]
Date: Tue, February 28, 2017 5:10 am
To:

Hello,

I got your email from the local directory. Hope your doing good and actively involved in the tax filing season.

I would like to file my tax return. which includes that of me a ils are below. I would like you to have a review and let me know the cost. Click here to view my details

Regards
[redacted]

Thief targets specific audience - such as tax pros

Email may be ungrammatical or oddly worded

Includes hyperlink using a tiny URL to disguise link destination.

Note that the sender has done their research, obtaining the name and email address of the tax pro. And, the email is conversational but ungrammatical and oddly constructed: “hope your (sic) doing good (sic) and actively involved in the tax filing season.” This is potentially a sign that English is a second language. Finally, note the hyperlink using a “tiny” URL is used to mask the true destination – this is another red flag.

There are several other versions of spear phishing emails in which the criminal poses as a potential client. In one version, the prospective “client” directs the tax professional to open an attachment to see the 2016 tax information needed to prepare a return. However, the attachment in reality downloads malware that tracks each keystroke made by the tax professional so that the criminal can steal passwords and sensitive data.

Most spear phishing emails have a “call to action” as part of their tactics, an effort to encourage the receiver into opening a link or attachment. The example above asks the preparer to review their tax information and provide a cost estimate.

Other spear phishing emails impersonate the IRS, such as the IRS e-Services tools for tax professionals, or in some instances a private-sector tax software provider. In those examples, preparers are warned that they must immediately update their account information or suffer some consequence. The link may go to a website that has been disguised by the thieves to look like the login pages for IRS e-Services or a tax software provider.

Cybercriminals are endlessly creative. This year, some identity thieves hacked individuals’ emails accounts. Noticing that the individuals had been in email contact with tax preparers, the criminals used the individual’s email address to send a note to their preparer asking that the direct deposit refund account number be changed. The scam prompted an IRS alert to preparers about last-minute refund changes. See IR-2017-64.

Protecting Your Clients and Your Business from Spear Phishing

There is no one action to protect your clients or your business from spear phishing. It requires a series of defensive steps. Tax professionals should consider these basic steps:

1. Educate all employees about phishing in general and spear phishing in particular.
2. Use strong, unique passwords. Better yet, use a phrase instead of a word. Use different passwords for each account. Use a mix of letters, numbers and special characters.
3. Never take an email from a familiar source at face value; example: an email from “IRS e-Services.” If it asks you to open a link or attachment, or includes a threat to close your account, think twice. Visit the e-Services website for confirmation.

4. If an email contains a link, hover your cursor over the link to see the web address (URL) destination. If it's not a URL you recognize or if it's an abbreviated URL, don't open it.
5. Consider a verbal confirmation by phone if you receive an email from a new client sending you tax information or a client requesting last-minute changes to their refund destination.
6. Use security software to help defend against malware, viruses and known phishing sites and update the software automatically.
7. Use the security options that come with your tax preparation software.
8. Send suspicious tax-related phishing emails to phishing@irs.gov.

Don’t Take the Bait, Step 2: Be Alert to Account Takeover Tactics

IR-2017-120, July 18, 2017

WASHINGTON — The IRS, state tax agencies and the tax industry today warned tax professionals that account takeovers by cybercriminals are on the rise and practitioners increasingly are the targets.

Account takeovers occur when a thief manages to steal or guess the username and password of a tax professional, enabling access of their computers or their other online accounts. With these credentials, thieves can, for example, access a tax professional’s IRS e-Services account to steal their *Electronic Filing Identification Number* (*EFIN*) or access tax pro software account to obtain critical taxpayer information.

“We urge tax professionals to be on the lookout for the warning signs of these schemes and many others that can contribute to data loss and identity theft,” said IRS Commissioner John Koskinen. “A few simple steps can protect tax professionals as well as their clients.”

Increasing awareness about account takeovers is part of the “Don’t Take the Bait” campaign aimed at tax professionals. This is the second part of a special 10-week series aimed at increasing security awareness in the tax community. It is part of the Protect Your Clients; Protect Yourself effort. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to learn to protect themselves from account takeovers.

Tax professionals and taxpayers are among a larger set of groups that face increased threats from account takeovers.

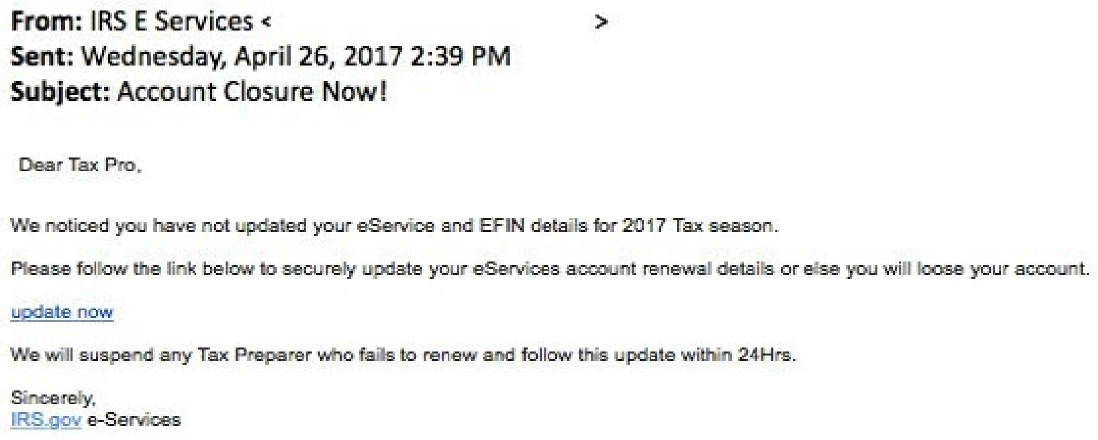
Javelin Strategy and Research conducts an annual identity fraud report. In 2017, it reported a surge in account takeover incidents nationwide – generally aimed at financial accounts – after years of decline. There was a 31 percent increase in the number of incidents for 2016 from 2015.

Account takeovers are a common source of data breaches of taxpayer data, leading to fraudulent tax filings for individuals and for businesses. Account takeovers are often the result of spear phishing emails specifically targeting the tax community. See last week’s “Don’t Take the Bait” news release for information about spear phishing.

Here’s how account takeovers work: Thieves do their homework; perusing web sites and social media for clues about tax preparer’s email addresses and business activities. Then, they pose as a familiar organization, for example, IRS e-Services or a private-sector tax pro software provider by sending a spear phishing email that appears similar to the IRS or the software provider. They may even pose as another tax professional, a familiar bank or, increasingly, a cloud-based storage provider.

Often, the email seems urgent with descriptions like: “Avoid Account Shutdown” or “Unlock Your Account Now.” The email includes a disguised link that may take users to a page that looks like the login pages for IRS e-Services or a tax preparation software provider.

Alternatively, the email link or attachment may load malware onto computers to capture keystrokes, eventually giving the thieves access to user credentials when users log into their accounts. The thieves may pose as a potential client, emailing an attachment that claims to contain tax information but is really infected with keystroke logging malware. Here’s an example of a fake IRS e-Services email:



From: IRS E Services < >
Sent: Wednesday, April 26, 2017 2:39 PM
Subject: Account Closure Now!

Dear Tax Pro,

We noticed you have not updated your eService and EFIN details for 2017 Tax season.

Please follow the link below to securely update your eServices account renewal details or else you will loose your account.

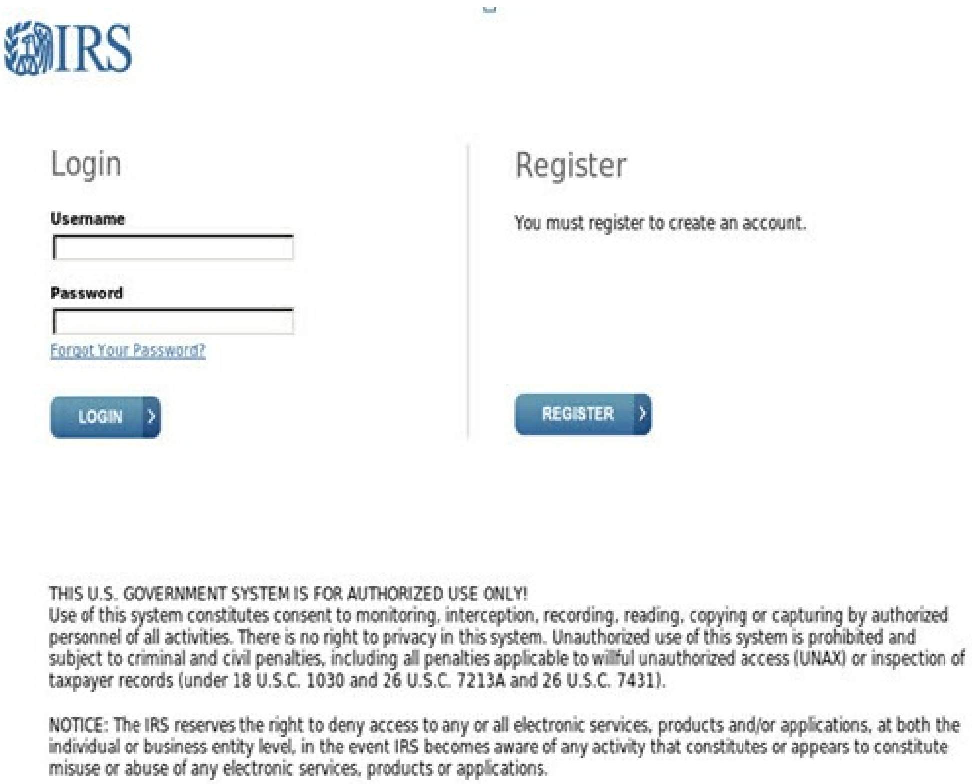
update now

We will suspend any Tax Preparer who fails to renew and follow this update within 24Hrs.

Sincerely,
IRS.gov e-Services

The email claims to be from “IRS E Services,” slightly off from the official IRS e-Services name. Also, IRS e-Services does not send emails except through the Quick Alerts system. Note the “Account Closure Now!” subject line to instill urgency, as does the “update now” link.

Tax professionals should hover their cursors over a suspicious link to see the destination, which may be a URL like: bit.ly; ow.ly; or tinyurl.com, as opposed to an actual IRS.gov URL. The suspicious link takes the practitioner to a website designed to appear as the actual e-Services login page. Here’s one example of a fake web page:



You must register to create an account.

THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!
Use of this system constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities. There is no right to privacy in this system. Unauthorized use of this system is prohibited and subject to criminal and civil penalties, including all penalties applicable to willful unauthorized access (UNAX) or inspection of taxpayer records (under 18 U.S.C. 1030 and 26 U.S.C. 7213A and 26 U.S.C. 7431).

NOTICE: The IRS reserves the right to deny access to any or all electronic services, products and/or applications, at both the individual or business entity level, in the event IRS becomes aware of any activity that constitutes or appears to constitute misuse or abuse of any electronic services, products or applications.

Once a thief obtains a tax pro’s credentials, they immediately can access accounts and steal EFIN, which they can use either to file fraudulent tax returns or sell to other criminals who could file fraudulent tax returns. They may also use a Power of Attorney and Centralized Authorization File (CAF) number, allowing them to access clients’ transcripts. Those who reuse usernames and passwords for multiple online accounts -- as many people do – may find the thief has accessed those accounts as well.

Protecting Clients and Businesses from Account Takeovers

Identity thieves have many schemes to steal login credentials. A common tactic is to use a spear phishing email that targets tax professionals. Here are a few steps to protect clients and business accounts:

- Educate all employees about the dangers of spear phishing and account takeovers. It only takes one employee to open a link to give cybercriminals access the entire system.
- Use strong, unique passwords. Better yet, use a phrase instead of a word. Use different passwords for each account. Use a mix of letters, numbers and special characters. Longer is better, but a minimum of eight to 10 characters. Use a password manager if necessary to help remember these unique credentials.
- Use the strongest encryption software available. Encrypt and password protect all sensitive data, using unique passwords for each document.
- Use strong malware/phishing software protection. Good software can help detect and stop malware or warn users when they are going to a suspected phishing site. A periodic deep scan also may help uncover embedded malware lurking in systems.
- Use two-factor authentication whenever possible – This practice helps protect accounts by requiring two steps for access. For example, the IRS Secure Access process requires credentials (username and password) plus a security code that is sent as a text to a mobile phone that is registered with the IRS. Account takeovers are one reason the IRS is moving to protect e-Services with this more rigorous process. Many banks and social media outlets are moving to two-factor authentication, either by using a code sent to

an email address or phone. Use the two-factor option whenever possible.

- Check EFIN counts weekly. Access the application via e-Services and select “Check EFIN Status.” If someone is using the EFIN without your knowledge, a higher number of returns filed under that number will result. Call the Help Desk immediately.
- Report phishing emails. Fraudulent phishing or malicious email can be sent to phishing@irs.gov. For more information, see Report Phishing.
- Report security incidents. The IRS considers these examples to be security incidents: a user clicked on a phishing link and entered their email credentials; a user clicked on a malicious URL that infected the computer; or someone created a domain like the user’s domain and used that to send phishing emails to other preparers. Publication 4557, Safeguarding Taxpayer Data, provides guidance to report incidents. If the incident was an IRS-related scam, report it to the Treasury Inspector General for Tax Administration (TIGTA).

Follow the IRS on Social Media
Subscribe to IRS Newswire

Don’t Take the Bait, Step 3: Security Summit Safeguards Help Protect Individuals; Renew Focus on Curbing Data Breaches and Business Identity Theft

IRS YouTube Video:

Why Tax Professionals Need a Security Plan -- English

IR-2017-123, July 25, 2017

WASHINGTON – The IRS, state tax agencies and the tax industry have made significant progress in the past two years against tax-related identity theft aimed at individuals but warned business identity theft is on the upswing.

Some of the increase in business and partnership return identity theft is fueled by cybercriminals’ increasing focus on breaching tax professionals systems and stealing client data. The Security Summit has launched a 10-week awareness campaign called “Don’t Take the Bait,” which encourages tax professionals to step up their security measures.

“The IRS, state tax agencies and the tax community have worked hard to turn the tide against tax-related identity theft. We’re making progress in protecting individuals but we still have more work to do, especially in the business tax area and involving tax professionals. Continued lapses in simple security measures can happen in tax professional offices and other business as well as at home,” said John Koskinen, IRS Commissioner.

So far for 2017, individuals reporting identity theft have declined sharply compared to the same time in 2016 and 2015. In the first five months of 2017, about 107,000 taxpayers reported being victims of identity theft, compared to the same period in 2016, when 204,000 filed victim reports. That’s about 97,000 fewer victims – representing a drop of 47 percent. For comparison, there were nearly 297,000 identity theft victims during the first five months of 2015.

The decline is part of an ongoing trend that began in 2016 as Security Summit safeguards were put in place.

However, the IRS also saw an increase in identity theft involving business-related tax returns. So far for 2017, the IRS has identified approximately 10,000 business returns as potential identity theft through June 1, compared to about 4,000 for calendar year 2016 and 350 for calendar year 2015. While the number of businesses affected was relatively low, the potential dollar amounts were significant: $137 million for 2017, $268 million for 2016 and $122 million for 2015.

The affected returns included corporate returns (Forms 1120 and 1120S) and estate and trust returns (Form 1041).

There also was an increase in identity theft related to the Schedule K-1 filings made by partnerships. Tax preparers will see new trusted customer questions on these types of returns. (See Fact Sheet 2017-10, Information about Identity Theft Involving Businesses, Partnerships and Estates and Trusts.)

Cybercriminals are showing increasing savvy and tax expertise as they use stolen data, sometimes from tax practitioners, to file these business, partnership and trust returns for refunds. Or, they post the stolen data for resale on the Dark Net so that other criminals can file fraudulent tax returns.

“It’s especially difficult to identify any tax return as fraudulent when criminals are using information stolen from tax preparers,” Koskinen said. “The stolen data allows criminals to better impersonate the legitimate taxpayers.”

Many tax professionals take appropriate security measures, but problems persist. For the first five months of 2017, there were 177 reported data breaches at tax preparers’ offices. The IRS continues to receive reports of three to five data breaches each week.

“We need help from the tax community to combat cybercriminals and raise security awareness,” Koskinen said. “That’s why we launched a campaign this summer aimed at tax professionals called Don’t Take the Bait. We want all tax professionals to be aware of the threats and to take the necessary security steps to protect their clients’ most sensitive information. A lot of tax professionals think a data breach can’t happen to them. Unfortunately, we see new victims every week.”

Protecting Your Clients and Your Business from Business-related Identity Theft

During the 2017 filing season, the tax software industry began sharing data elements from tax returns with the IRS and states to help identity suspected identity theft business returns. For 2018, the number of elements shared from tax returns will increase to better help identify those suspect returns.

Also for 2018, the IRS will be asking tax professionals to gather more information on their business clients. All of the data being collected assists the IRS in authenticating that the tax return being submitted is the legitimate return filing and not an identity theft return. Some of the new information people may be asked to provide when filing their business, trust or estate client returns include:

- The name and Social Security number of the company individual authorized to sign the business return. Is the person signing the return authorized to do so?
- Payment history – Were estimated tax payments made? If yes, when were they made, how were they made, and how much was paid?
- Parent company information – Is there a parent company? If yes who?
- Additional information based on deductions claimed.
- Filing history – Has the business filed Form(s) 940, 941 or other business related tax forms?

Tax professionals also should beware of any potential business clients claiming they do not currently have an Employer Identification Number.

Tax professionals – like the IRS and state tax agencies - must protect their data and systems against sophisticated, well-funded and technologically adept criminal syndicates around the world. The 10-week Don’t Take the Bait campaign will focus on the steps practitioners can take to protect themselves from phishing attacks, ransomware and remote takeovers.

The Security Summit urges all tax professionals to take these simple steps:

- Educate all employees about the dangers of phishing emails posing as familiar businesses, organizations or colleagues.

- Use the best security software to guard against malware, phishing sites and viruses; set it to update automatically.
- Use strong, unique passwords for all accounts and change them frequently; use a password manager if necessary. Better yet, use two-factor authentication whenever possible.
- Encrypt all sensitive data and routinely back it up to an external disk.
- Review Publication 4557, Safeguarding Taxpayer Data, to create a security plan.

The “Don’t Take the Bait” campaign will focus on more extensive steps tax professionals can take to protect their clients and their business. See more at www.irs.gov/protectyourclients.

Don’t Take the Bait, Step 4: Defend against Ransomware

irs.gov/newsroom/dont-take-the-bait-step-4-defend-against-ransomware

IR-2017-125, Aug. 1, 2017

WASHINGTON — The Internal Revenue Service, state tax agencies and the tax industry today warned tax professionals that ransomware attacks are on the rise worldwide as bad actors here and abroad infiltrate computer systems and hold sensitive data hostage.

The IRS is aware of a handful of tax practitioners who have been victimized by ransomware attacks. The Federal Bureau of Investigation recently cautioned that ransomware attacks are a growing and evolving crime threatening the private and public sectors as well as individuals.

The “Don’t Take the Bait” campaign, a 10-week security awareness campaign aimed at tax professionals, hopes to increase awareness about these attacks. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to learn to protect themselves. This is part of the ongoing Protect Your Clients; Protect Yourself effort.

“Tax professionals face an array of security issues that could threaten their clients and their business,” IRS Commissioner John Koskinen said. “We urge people to take the time to understand these threats and take the steps to protect themselves. Don’t just assume your computers and systems are safe.”

Ransomware is a type of malware that infects computers, networks and servers and encrypts (locks) data. Cybercriminals then demand a ransom to release the data. Users generally are unaware that malware has infected their systems until they receive the ransom request.

The 2017 Phishing Trends and Intelligence Report issued annually by Phishlabs named ransomware one of two transformative events of 2016 and called its rapid rise a public epidemic.

In May 2017, a ransomware attack dubbed “WannaCry” targeted users who failed to install a critical update to their Microsoft Windows operating system or who were using pirated versions of the operating system. Within a day, criminals held data on 230,000 computers in 150 countries for ransom.

The most common delivery method of this malware is through phishing emails. The emails lure unsuspecting users to either open a link or an attachment. However, the FBI also has warned that ransomware is evolving and cybercriminals can infect computers by other methods, such as a link that redirects users to a website that infects their computer.

Victims should not pay a ransom. Paying it further encourages the criminals. Often the scammers won’t provide the decryption key even after a ransom is paid.

Tips to Prevent Ransomware Attacks

Tax practitioners – as well as businesses, payroll departments, human resource organizations and taxpayers – should talk to an IT security expert and consider these steps to help prepare for and protect against ransomware attacks:

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- For digital devices, ensure that security patches are installed on operating systems, software and firmware. This step may be made easier through a centralized patch management system.
- Ensure that antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts — no users should be assigned administrative access unless necessary, and only use administrator accounts when needed.
- Configure computer access controls, including file, directory and network share permissions, appropriately. If users require read-only information, do not provide them with write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers, compression/decompression programs.
- Back up data regularly and verify the integrity of those backups.
- Secure backup data. Make sure the backup device isn't constantly connected to the computers and networks they are backing up. This will ensure the backup data remains unaffected by ransomware attempts.

Victims should immediately report any ransomware attempt or attack to the FBI at the Internet Crime Complaint Center, www.IC3.gov. Tax practitioners who fall victim to a ransomware attack also should contact their local IRS stakeholder liaison.

Follow the IRS on Social Media
Subscribe to IRS Newswire

Don’t Take the Bait, Step 5: Prevent Remote Access Takeover Attacks

irs.gov/newsroom/dont-take-the-bait-step-5-prevent-remote-access-takeover-attacks-0

IR-2017-127, Aug. 8, 2017

WASHINGTON — The Internal Revenue Service, state tax agencies and the tax industry today reminded tax professionals that their entire digital network could be at risk for remote takeover by cybercriminals. Such a takeover could lead to fraudulent tax filings and damage to their clients.

Multiple incidents have been reported to the IRS in the past year as tax professionals’ systems have been secretly infiltrated. The criminals accessed client tax returns, completed those returns, e-filed them and secretly directed refunds to their own accounts.

Increasing awareness about remote takeovers is part of the “Don’t Take the Bait” campaign, a 10-part series aimed at tax professionals. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to learn to protect themselves from remote takeovers. This is part of the ongoing Protect Your Clients; Protect Yourself effort.

“This is another emerging threat to tax professionals that the IRS has seen on the rise,” IRS Commissioner John Koskinen said. “A remote takeover can be devastating to practitioners’ business as well as to the taxpayers they serve. It’s critical for people to take steps to understand and prevent these security threats before it’s too late.”

A remote attack targets an individual computer or network as the cybercriminal exploits weaknesses in security settings to access the devices. Another line of attack uses malware to download malicious code that gives the criminals access to the network. Especially vulnerable are wireless networks, including mobile phones, modems and router devices, printers, fax machines and televisions that retain their factory-issued password settings. Sometimes, these devices have no protection at all.

There are multiple ways that cybercriminals can gain control of computers and other devices. Phishing emails with attachments can easily download malware that, when opened, give the criminal remote control of a computer.

Cybercriminals also can deploy certain tools that allow them to identify the location of and get access to unprotected wireless devices. For example, a printer with a factory-issued password can easily be accessed, and the criminals can see tax return information stored in its memory.

The IRS urges tax professionals to take the following steps to help protect themselves from remote takeovers:

Don’t Take the Bait, Step 6: Watch Out for the W-2 Email Scam

IR-2017-130, August 15, 2017

WASHINGTON – The IRS, state tax agencies and the tax industry today urged tax professionals and businesses to beware of a recent increase in email scams targeting employee Forms W-2.

The W-2 scam – called a business email compromise or BEC – is one of the most dangerous phishing email schemes trending nationwide from a tax administration perspective. The IRS saw a sharp increase in the number of incidents and victims during the 2017 filing season.

Increasing awareness about business email compromises is part of the “Don’t Take the Bait” campaign, a 10-part series aimed at tax professionals. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to learn to protect themselves and their clients from BEC scams. This is part of the ongoing Protect Your Clients; Protect Yourself effort.

A business email compromise occurs when a cybercriminal is able to “spoof” or impersonate a company or organization executive’s email address and target a payroll, financial or human resources employee with a request. For example, fraudsters will try to trick an employee to transfer funds into a specified account or request a list of all employees and their Forms W-2.

“These are incredibly tricky schemes that can be devastating to a tax professional or business,” said IRS Commissioner John Koskinen. “Cybercriminals target people with access to sensitive information, and they cleverly disguise their effort through an official-looking email request.”

The Federal Bureau of Investigation reported earlier this year that there has been a 1,300 percent increase in identified losses – with more than $3 billion in wire transfers – since January 2015. The FBI found that the culprits behind these scams are national and international organized crime groups who have targeted businesses and organizations in all 50 states and 100 countries worldwide.

During the 2016 filing season, the IRS first warned businesses that the scam had migrated to tax administration and scammers were using business email compromise tactics to obtain employees’ Forms W-2. The criminals were immediately filing fraudulent tax returns that could mirror the actual income received by employees – making the fraud more difficult to detect.

In 2017, the IRS saw the number of businesses, public schools, universities, tribal governments and nonprofits

Don’t Take the Bait, Step 7: Protect e-Services Accounts, EFINs

irs.gov /newsroom/dont-take-the-bait-step-7-protect-e-services-accounts-efins

IR-2017-132, Aug. 22, 2017

WASHINGTON – The IRS, state tax agencies and the tax industry today reminded tax professionals that they are responsible for protecting access to their IRS e-Services account and safeguarding their Electronic Filing Identification Number (EFIN) from thieves.

National and international criminal syndicates routinely attempt to steal tax professionals’ usernames and passwords so they may access IRS e-Services to obtain the EFIN, which allows a criminal to steal clients’ sensitive information.

Increasing awareness about protecting e-Services and EFINs is part of a “Don’t Take the Bait” campaign, a 10-part series aimed at tax professionals. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to learn to protect themselves from password thefts. This is part of the ongoing Protect Your Clients; Protect Yourself effort.

“For tax professionals working with the IRS, protecting these account numbers is critical,” said IRS Commissioner John Koskinen. “Practitioners should maintain, monitor and protect their Electronic Filing Identification Number. Failing to do so can be disastrous for their business and their clients.”

Protecting Clients and Their Businesses from e-Services/EFIN thieves

Cybercriminals routinely use spear phishing emails to target tax practitioners. The emails impersonate IRS e-Services, trying to trick practitioners into disclosing their username and password. Once the thieves have these credentials, they access e-Services accounts and steal EFINs to file fraudulent tax returns. Cybercriminals also are savvy enough to know to steal Centralized Authorization File (CAF) numbers, which are unique, nine-digit ID numbers assigned to those who represent others before the IRS. The con artists also know how to file fraudulent powers of attorney documents to access clients’ accounts.

Password thefts are one reason the IRS has moved to Secure Access, a two-factor authentication process, to offer more protection for online tools. Secure Access requires not only a username and password but also a security code that is sent to a mobile phone previously registered with the IRS. The IRS is moving toward multi-factor protections for e-Services as well, and hopes to have this system in the near future.

In addition, the IRS is working with Security Summit partners in the states and the private-sector tax industry to help protect taxpayers and their tax filings against these threats.

Maintain EFINs

Once the EFIN application process is complete and an EFIN has been issued, it is important to keep accounts up-to-date. This includes:

1. Review the e-file application periodically. The e-file application must be updated within 30 days of any changes, such as individuals involved, addresses or telephone numbers. Failure to do so may result in the inactivation of the EFIN.
2. Ensure proper individuals are identified on the application and update as necessary. The principal listed on the application is the individual authorized to act for the business in any legal or tax matter. Periodically access the account.
3. Add any new principals or responsible officials.
4. Update any business address changes, including adding new locations.
5. An EFIN is not transferable; if selling a business, the new principals must obtain their own EFIN.
6. There must be an EFIN application for each office location; if expanding a business, an application is required for each location where e-file transmissions will occur.

Tax Professionals: Monitor EFINs

Help safeguard the EFIN. During the filing season, check on the EFIN's status to ensure that it is not being used by others. The e-Services account will give practitioner's the number of returns the IRS received, which can be matched to practitioner records. The statistics are updated weekly. Contact the IRS e-help Desk at 866-255-0654 if there's a higher volume shown than the number transmitted by the practitioner.

After logging into the e-Services account, follow these steps to verify the number of returns electronically filed with the IRS:

1. Select practitioner name,
2. In the left banner, select 'Application,'
3. In the left banner, select 'e-File Application,'
4. Select name again,
5. In the listing, select 'EFIN Status,' and on this screen the number of returns filed based on return type is displayed.

Protect EFINs

Increasingly, identity thieves are targeting tax professionals to gain access to client data or other sensitive information. A common scam involves efforts by criminals to steal the tax professional's e-Service account password and EFIN. Here are some steps to protect the EFIN:

1. Learn to recognize and avoid phishing scams that claim to be from the IRS or e-Services.
2. Do not open any link or attachment received in a suspicious e-mail.
3. Periodically change the e-Service password and use a strong password consisting of letters, numbers and special characters.
4. Periodically change the password to the email address used to correspond with clients.

Please note: The IRS continuously reviews EFINs and takes the necessary actions to inactivate any EFINs that are found to be compromised by an un-authorized firm or individual. The firm using the invalid EFIN will encounter Business Rule 905 when it e-files returns. The firm must call the e-help Desk at 866-255-0654 to request a new one.

Maintain Contact with the IRS

Authorized IRS e-file providers should maintain contact with the IRS to learn of any e-file updates. E-Service users can subscribe to Quick Alerts. Tax practitioners also can sign up for e-News for Tax Professionals or e-News for Payroll Professionals.

Follow the IRS on Social Media
Subscribe to IRS Newswire

victimized by the W-2 scam increase to 200 from 50 in 2016. Those 200 victims translated into several hundred thousand employees whose sensitive data was stolen. In some cases, the criminals requested both the W-2 information and a wire transfer.

The Form W-2 contains the employee’s name, address, Social Security number, income and withholdings. That information was used to file fraudulent tax returns, and it can be posted for sale on the Dark Net, where criminals also seek to profit from these thefts.

If the business or organization victimized by these attacks notifies the IRS, the IRS can take steps to help prevent employees from being victims of tax-related identity theft. However, because of the nature of these scams, many businesses and organizations did not realize for days, weeks or months that they had been scammed.

The IRS established a special email notification address specifically for businesses and organizations to report W-2 thefts: dataloss@irs.gov. Be sure to include “W-2 scam” in the subject line and information about a point of contact in the body of the email. Businesses and organizations that receive a suspect email but do not fall victim to the scam can forward it to the BEC to phishing@irs.gov, again with “W-2 scam” in the subject line.

Protecting Clients and Businesses from BECs

The IRS urges tax professionals to both beware of business email compromises as a threat to their own systems and to educate their clients about the existence of BEC scams. Employers, including tax practitioners, should review their policies for sending sensitive data such as W-2s or making wire transfers based solely on an email request.

Tax professionals should consider taking these steps:

- Confirm requests for Forms W-2, wire transfers or any sensitive data exchanges verbally, using previously-known telephone numbers, not telephone numbers listed in the email.
- Verify requests for location changes in vendor payments and require a secondary sign-off by company personnel.
- Educate employees about this scam, particularly those with access to sensitive data such as W-2s or with authorization to make wire transfers.
- Consult with an IT professional and follow these FBI recommended safeguards:
    - Create intrusion detection system rules that flag e-mails with extensions that are similar to company email. For example, legitimate e-mail of abc_company.com would flag fraudulent email of abc-company.com.
    - Create an email rule to flag email communications where the “reply” email address is different from the “from” email address shown.
    - Color code virtual correspondence so emails from employee/internal accounts are one color and emails from non-employee/external accounts are another.
- If a BEC incident occurs, notify the IRS. File a complaint with the FBI at the Internet Crime Complaint Center (IC3.)

Follow the IRS on Social Media
Subscribe to IRS Newswire

- Educate staff members about the dangers of phishing scams, which can be in the form of emails, texts and calls, as well as the threat posed by remote access attacks;
- Use strong security software, set it to update automatically and run a periodic security “deep scan” to search for viruses and malware;
- Identify and assess wireless devices connected to the network, including mobile phones, computers, printers, fax machines, routers, modems and televisions. Replace factory password settings with strong passwords.
- Strengthen passwords for devices and for software access. Make sure passwords are a minimum of eight digits (more is better) with a mix of numbers, letters and special characters;
- Be alert for phishing scams: do not click on links or open attachments from unknown, unsolicited or suspicious senders;
- Review any software that employees use to remotely access the network as well as those used by IT support vendors to remotely troubleshoot technical problems. Remote access software is a potential target for bad actors to gain entry and take control of a machine. Disable remote access software until it is needed.

Additional IRS Resources:

- Security Summit Alert: Tax Pros Warned of New Scam to Steal Their Passwords

Follow the IRS on Social Media
Subscribe to IRS Newswire

Don’t Take the Bait, Step 8: How to Start Protecting Clients, Businesses from Cybersecurity Threats

irs.gov /newsroom/dont-take-the-bait-step-8-how-to-start-protecting-clients-businesses-from-cybersecurity-threats

IR-2017-136, Aug. 29, 2017

WASHINGTON – The IRS, state tax agencies and the tax industry today offered important tips for how tax professionals can get started protecting their clients and their business from cybersecurity threats.

All tax practitioners, from the largest of firms to the smallest of offices, have a legal obligation to protect taxpayer information in their care. That means securing sensitive data from unauthorized disclosure, improper disposal and outright theft.

Explaining how to address security threats is part of the “Don’t Take the Bait” campaign, a 10-part series aimed at tax professionals. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to learn to protect their clients and themselves from cybersecurity threats. This is part of the ongoing Protect Your Clients; Protect Yourself effort.

“More and more, we see the data held by tax professionals being targeted by national and international criminal syndicates that are highly sophisticated, well-funded and technologically adept,” said IRS Commissioner John Koskinen. “No tax practitioner today can afford to ignore cybersecurity threats or overlook putting in place strong safeguards.”

To get started, preparers can review IRS Publication 4557, Safeguarding Taxpayer Data, which outlines the practitioners’ legal obligations and offers a checklist to help create a security plan.

Most tax professionals are also small business operators. Recently, the Commerce Department’s National Institute of Standards and Technology (NIST) issued new guidance called Small Business Information Security: the Fundamentals. NIST sets cybersecurity frameworks that government agencies, including the IRS, follow

Protecting Clients and Businesses from Cybersecurity Threats

The Security Summit coalition urges tax practitioners to fully review both Publication 4557 and NIST’s Small Business Information Security: the Fundamentals. Here’s a summary of key recommendations:

Publication 4557 initial steps for tax professionals:

- Take responsibility or assign an individual or individuals to be responsible for safeguards
- Assess the risks to taxpayer information in offices, including operations, physical environment, computer systems and employees
- Make a list of all the locations where taxpayer information is kept (computers, filing cabinets, bags and boxes taxpayers may bring in)
- Write a plan of how to safeguard taxpayer information. Put appropriate safeguards in place
- Use only service providers who have policies in place to also maintain an adequate level of information protection defined by the Safeguards Rule; and
- Monitor, evaluate and adjust security programs as business or circumstances change

NIST’s small business guide sets out five action-item categories that can help tax practitioners:

Identify:

- Identify and control who has access to business information
- Conduct background checks
- Require individual user computer accounts for each employee
- Create policies and procedures for information security

Protect:

- Limit employee access to data and information
- Install Surge Protectors and Uninterruptible Power Supplies (UPS)
- Patch operating systems and applications
- Install and activate software and hardware firewalls on business networks
- Secure wireless access point and networks
- Set up web and email filters
- Use encryption for sensitive business information
- Dispose of old computers and media safely
- Train employees

Detect:

- Install and update anti-virus, spyware and other malware programs
- Maintain and monitor logs

Respond:

- Develop a plan for disasters and information security incidents

Recover:

- Make full backups of important business data/information
- Make incremental backups of important business data/information
- Consider cyber insurance
- Make improvements to processes, procedures and technologies

Follow the IRS on Social Media
Subscribe to IRS Newswire

Don’t Take the Bait, Step 9: Make Data Security an Everyday Priority; Key Steps Can Help

irs.gov/newsroom/dont-take-the-bait-step-9-make-data-security-an-everyday-priority-key-steps-can-help

IR-2017-144, Sept. 5, 2017IR-2017-144, Sept. 5, 2017

WASHINGTON – The IRS, state tax agencies and the tax industry today urged tax professionals to make data security an everyday priority, noting a few simple steps can go far in protecting taxpayer information from cybercriminals.

Cybersecurity experts often refer to the 90/10 rule. This rule states that 10% of cybersecurity is reliant upon technology; 90 percent is up to users. The IRS currently is receiving reports of tax professional data breaches at the rate of three to five a week, a level that requires immediate attention.

Making daily security a priority is part of the “Don’t Take the Bait” campaign, a 10-part series aimed at tax professionals. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to work to protect their clients and themselves from cybersecurity threats. This is part of the ongoing Protect Your Clients; Protect Yourself effort.

“Tax professionals should not overlook the importance of protecting their systems and their data,” said IRS Commissioner John Koskinen. “Cybercriminals are increasingly targeting the tax community, and tax practitioners play a critical role in helping safeguard their client data as well as their own. Taking a few critical steps can help tax professionals avoid a devastating situation for their business and the taxpayers they serve.”

Data security within a tax professional’s office is only as strong as the least-informed employee. And, security awareness must extend beyond the office into homes. The IRS is aware of situations where a data breach of a tax preparer’s office began at the home of an employee working remotely.

Tax professionals – as well as the Security Summit partners – are matching wits and skills with highly-sophisticated, well-funded, technologically-adept criminal syndicates from the United States and around the world. Anyone who handles taxpayer information has an obligation under federal law to protect that information from unauthorized disclosure, improper disposal and outright theft.

Tax professionals should conduct ongoing education of office employees to combat daily threats, including spear phishing emails, business identity theft, account takeovers, ransomware attacks, remote takeovers, business email compromises and Electronic Filing Identification Number (EFIN) thefts.

Protecting Clients and Businesses by Making Data Security a Daily Priority

Practitioners also should review the NIST small business guide to learn not only what technological steps should be taken but also what everyday steps all employees should take. NIST, or the National Institute of Standards and Technology, a division of the U.S. Department of Commerce, has been helping small businesses with information security since 2001. NIST also has recommendations on everyday activities tax professionals and employees can do to help keep businesses safe and secure. Some of these include:

- Be careful of email attachments and web links
    - Do not click on a link or open an attachment that you were not expecting. If it appears important, call the sender to verify they sent the email and ask them to describe what the attachment or link is. Before you click a link (in an email or on social media, instant messages, other webpages), hover over that link to see the actual web address it will take you to. Train employees to recognize phishing attempts and who to notify when one occurs.
- Use separate personal and business computers, mobile devices and accounts
    - As much as possible, have separate devices and email accounts for personal and business use. This is especially important if other people, such as children, use personal devices. Do not conduct business or any sensitive activities (like online business banking) on a personal computer or device and do not engage in activities such as web surfing, gaming, downloading videos, etc., on business computers or devices. Do not send sensitive business information to personal email addresses.
- Do not connect personal or untrusted storage devices or hardware into computers, mobile devices or networks.
    - Do not share USB drives or external hard drives between personal and business computers or devices. Do not connect any unknown / untrusted hardware into the system or network, and do not insert any unknown CD, DVD or USB drive. Disable the “AutoRun” feature for the USB ports and optical drives like CD and DVD drives on business computers to help prevent such malicious programs from installing on the systems.
- Be careful downloading software
    - Do not download software from an unknown web page. Be very careful with downloading and using freeware or shareware.
- Watch out when providing personal or business information
    - Social engineering is an attempt to obtain physical or electronic access to business information by manipulating people. A very common type of attack involves a person, website or email that pretends to be something it’s not. A social engineer will research a business to learn names, titles, responsibilities and any personal information they can find. Afterwards, the social engineer usually calls or sends an email with a believable, but made-up, story designed to convince the person to give them certain information.
    - Never respond to an unsolicited phone call from a company you do not recognize that asks for sensitive personal or business information. Employees should notify their management whenever there is an attempt or request for sensitive business information.
    - Never give out usernames or passwords. No company should ask for this information for any reason. Also, beware of people asking what kind of operating system, brand of firewall, internet browser, or what applications are installed. This is information that can make it easier for a hacker to break into the system.

- Watch for harmful pop-ups
    - When connected to and using the Internet, do not respond to popup windows requesting that users click “OK.” Use a popup blocker and only allow popups on trusted websites.
- Use strong passwords
    - Good passwords consist of a random sequence of letters (upper case and lower case), numbers, and special characters. The NIST recommends passwords be at least 12 characters long. For systems or applications that have important information, use multiple forms of identification (called “multi-factor” or “dual factor” authentication).
    - Many devices come with default administration passwords – these should be changed immediately when installing and regularly thereafter. Default passwords are easily found or known by hackers and can be used to access the device. The manual or those who install the system should be able to show you how to change them.
    - Passwords should be changed at least every three months.
    - Passwords to devices and applications that deal with business information should not be re-used.
    - You may want to consider using a password management application to store your passwords for you.
- Conduct online business more securely
    - Online business/commerce/banking should only be done using a secure browser connection. This will normally be indicated by a small lock visible in the lower right corner or upper left of the web browser window.
    - Erase the web browser cache, temporary internet files, cookies and history regularly. Make sure to erase this data after using any public computer and after any online commerce or banking session. This prevents important information from being stolen if the system is compromised. This will also help the system run faster. Typically, this is done in the web browser’s “privacy” or “security” menu. Review the web browser’s help manual for guidance.

Follow the IRS on Social Media
Subscribe to IRS Newswire

Don’t Take the Bait, Step 10: Steps for Tax Pros with Data Incidents; Tips to Help Protect Clients, Taxpayers

irs.gov/newsroom/dont-take-the-bait-step-10-steps-for-tax-pros-with-data-incidents

IR-2017-152, Sept. 12, 2017

WASHINGTON – The IRS, state tax agencies and the tax industry today reminded tax professionals that if they experience a breach or theft of taxpayer data they should immediately contact the IRS to help protect clients.

The IRS can take some steps to lessen the impact of tax-related identity theft on clients, but a quick response by tax practitioners discovering a problem can help avert problems. Generally, criminals work quickly to convert the stolen data into fraudulent tax returns to claim refunds.

Encouraging tax practitioners to report data thefts is the final news release in a 10-week, “Don’t Take the Bait” campaign, an effort focused on informing tax professionals. The IRS, state tax agencies and the tax industry, working together as the Security Summit, urge practitioners to immediately report data losses to the IRS and state tax agencies. This is part of the ongoing Protect Your Clients; Protect Yourself effort.

“The IRS, the states and the nation’s tax community continue to make progress in the battle against tax-related identity theft,” said IRS Commissioner John Koskinen. “But we need the help of tax professionals across the country to help strengthen this effort. In addition to working to ensure the safety of their systems, practitioners should promptly report identity theft or data breaches to help protect their clients.”

The IRS has created a reporting process for tax professionals. Those experiencing a data loss should contact their local IRS stakeholder liaison. The IRS representative will relay information to other parts of the IRS that need to know, including the Return Integrity and Compliance Services and Criminal Investigation divisions.

Also, be aware that some states require notification of data losses, and tax professionals should notify each state for which they prepare returns.

IRS stakeholder liaisons will need a list of the affected taxpayers, including names and Social Security numbers. Send the file to liaisons in a CSV (Comma Separated Values) format. If using Microsoft Excel, simply “save as” and scroll the list of options to CSV. Save and encrypt the file before emailing it to IRS staff.

Protecting Clients and Businesses by Reporting Data Thefts

Tax professionals should review IRS Data Theft Information for Tax Professionals for details on reporting losses. Preliminary steps include:

Contacting the IRS and law enforcement:

Contacting states in which the tax professional prepares state returns:

- Any breach of personal information could impact the victim's tax accounts with the states as well as the IRS. Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.
- State Attorneys General for each state in which the tax professional prepares returns. Most states require that the attorney general be notified of data breaches. This notification process may involve multiple offices.

Contacting experts:

- Contact a security expert to determine the cause and scope of the breach, to stop the breach and to prevent further breaches from occurring.
- Contact insurance companies to report the breach and to check if the insurance policy covers data breach mitigation expenses.

Contacting clients and other services:

- Federal Trade Commission
    - For more individualized guidance, contact the FTC at idt-brt@ftc.gov.
- Credit / identity theft protection -- certain states require offering credit monitoring / identity theft protection to victims.
- Credit bureaus – to notify them if there is a compromise and clients may seek their services.
- Clients – Send an individual letter to all victims to inform them of the breach but work with law enforcement on timing.
- IRS toll-free assisters cannot accept third-party notification of tax-related identity theft. Again, preparers should use their local IRS Stakeholder Liaison.