# Don't be a victim...

## Providing useful information to help you recognize criminals and the hallmarks of their scams.

You may not think twice of an individual from the IRS asking for personal information that initially seems harmless, or even an email from a recognizable organization asking you to confirm a password. However, you may not realize that these requests could be coming from potential scammers.

Arthur Bell CPAs understands the serious risk that scammers pose for families, which is why we have created this Don't Be A Victim series to include tips for recognizing and preventing phone scams, email phishing, identity theft, and 5 common protection measures for information security.

The level of sophistication that is being employed by modern-day scammers requires more discretion than in previous years, and this series shares with you the hallmarks of current scams to ensure you don't fall victim to these unscrupulous characters.

Arthur Bell CPAs takes great pride in looking out for our clients and protecting their private information. If you have questions for concerns regarding your financial safety or privacy, please contact your Arthur Bell advisor at (855) 787-0001, or via email at contactus@athurbellcpas.com.

### PHONE SCAMS

Your day seems like any other day until the phone rings, and the caller ID shows it's the IRS. You answer and are berated by an aggressive individual claiming you owe additional taxes and are facing jail time unless you pay up. Panicked, you provide personal information to try and resolve the matter over the phone, but this leads to more questions, including requests for bank information.

This may seem unlikely, but phone scams of this nature are on the rise. In the midst of tax season, individuals need to be vigilant for sophisticated scammers attempting to obtain information that can be used to harm them. Anyone could fall victim to evolving scamming techniques; many are hard to detect. Arthur Bell CPAs takes our clients' privacy and financial safety seriously.

CONTINUED

This article is intended to give individuals tips on how to spot a tax-related phone scam before providing any valuable information.

Generally, phone scams involving the IRS will include an aggressive individual claiming he (or she) works for the IRS either stating that the individual owes additional tax that is due immediately or that the individual is entitled to a large refund. If the targeted individual does not provide the information requested, the scammer generally becomes threatening and insulting. Often the scammer will threaten the individual with criminal charges, shutting off the individual's utilities, having the individual's driver's license revoked, or deportation (if a non-U.S. citizen).

The characteristics of this type of scam may include:

- The scammer will provide a fake name (such as Steve Smith) and IRS badge number;
- The IRS toll-free number will appear on the caller ID as if the IRS is calling. This is known as "spoofing;"
- The scammer will furnish personal information about the targeted individual generally obtained through fraudulent means, such as the last four digits of the individual's social security number;
- A legitimate looking email may accompany the phone call to "support" the scammer's claim;
- Background noise on the call may mimic a call center;
- The scammer may abruptly hang up and have one of his accomplices call back pretending to be the local police or the DMV (the caller ID will show the appropriate number); and
- If the scammer is accusing the individual of owing additional tax, the scammer will demand immediate payment over the phone via a debit or a pre-paid card; or
- If the scammer is stating that the individual is entitled to a refund, he will request bank account information for a direct deposit, which he may then use to withdraw funds.

All should be aware that the IRS initiates contact in writing when dealing with a refund or taxes due. Additionally, the IRS will never specify the form of payment or demand immediate payment over the phone. Do not confirm any of the information the scammer furnishes and do not provide any new information to the scammer. If you receive a phone call that you believe may be a scam, hang up and report the incident to TIGTA (Treasury Inspector General for Tax Administration) at 1-800-366-4484.

## EMAIL PHISHING

In recognition of tax identity theft week, this article provides useful information to our clients on how to recognize criminals before falling victim to their scams. One current scam that is surging around the country is email phishing. Email phishing has been around for decades, but the tricks used by scammers have come a long way from the prince in a war-torn country needing your help to move his fortune. Imposters are using advanced techniques to trick unsuspecting individuals into providing personal information or into unknowingly downloading malicious software. This article is intended to provide tips on how to spot an email phishing scam.

Email phishing is a scam in which the targeted recipient receives an email that appears to be from a legitimate source requesting personal information or financial information in an attempt to steal the recipient's identity or money. The sender's email address may appear to be from a trusted source, but there will usually be a slight difference, such as one letter misplaced. The phishing email may contain a logo or official seal of the business or government agency the scammer is attempting to imitate. Additionally, these emails mimic the terminology that the actual business or government agency may use as a way to appear legitimate.

Many of the email phishing scams currently in circulation are unsolicited emails requesting information or inviting you to subscribe to a product. If you believe that the email may be legitimate but want actual confirmation, you could Google the phone number of the actual company the email is purporting to be sent from and compare it to the phone number included in the email (if listed). If the email seems to be from a company you regularly do business with, call your representative to confirm the email is legitimate. Always closely review the sender's email address for errors before you click on any links to ensure the email is from a trusted source.

In the fast-paced world we live in today, it is easy to overlook the error in the sender's email address or to click on a link without first reviewing the email, and therefore it is important to have a backup system in place in case you make that mistake. Anti-virus software may be able to alert you if an

email contains malicious code and may stop the code from being downloaded even if you click the link. Because most computers do not already contain long-term anti-virus software off the shelf, it is important to install this protective software before browsing the internet or opening emails.

Although, email phishing can impersonate many different businesses and government agencies, the remainder of this article will focus on email phishing imitating the IRS. It is important for every individual to know the IRS does not initiate contact with individuals via email. If you receive an email that purports to be from the IRS requesting personal information or financial information, please take the following steps:

1. Do not reply;
2. Do not open any attachments. They may contain malicious code that may infect your computer, hand held device, or mobile phone. Such malicious code may go unnoticed if its main objective is to collect information rather than to destroy your software;
3. Do not click on any links or enter any personal information. This includes the "unsubscribe to this email" link generally contained at the bottom of an email;
4. Forward the suspicious email as-is directly to the IRS at phishing@irs.gov; and
5. Delete the original email.

If you receive an email you believe to be fraudulent that is not impersonating the IRS, follow the steps listed above and forward the email instead to reportphishing@antiphishing.org.

## IDENTITY THEFT

You receive an unexpected notice from the IRS regarding your tax return, which you confirm with your Arthur Bell advisor has not yet been filed. Your Arthur Bell advisor contacts the IRS and discovers someone has fraudulently filed a tax return in your name. You quickly realize your social security number has been compromised and your identity has been stolen. This is the nightmare that over 9 million Americans go through each year. The unfortunate reality is that identity theft is the fastest growing crime and can affect more than your finances; it can also ruin your reputation. This article is intended to inform you about the different types of identity theft and how to protect your personal and financial information.

Identity theft occurs when an individual fraudulently obtains someone's personal information and uses the information to commit fraud or other crimes, generally for economic gain. Your personal information includes your name, social security number, date of birth, address, and phone number. With your stolen personal information, identity thieves often access lines of credit or obtain a driver's license in the victim's name, siphon funds from existing financial accounts, apply for Social Security benefits, and collect fictitious tax refunds. If a criminal misappropriates your personal information, they may rack up a large amount of debt and engage in illegal activities in your name within a short period of time. If a scammer obtains your social security number, it is usually not an option to obtain a new one, making the fight against identity theft a life-long struggle.

### IRS pilot program helps fight identity theft

The IRS has started a pilot program that allows identity theft victims whose social security numbers have been compromised to obtain additional six-digit Identity Protection Pins (IP PINs) to use when filing their tax returns. The IP PIN allows victims of resolved identity theft cases to avoid delays and other issues when filing their returns and receiving refunds. This program is currently implemented in Florida, Georgia, and Washington, DC; however, individuals from other states may be eligible if the IRS identifies indications of suspicious activity on their accounts.

### How criminals obtain your information

Criminals can obtain a taxpayer's personal information in various ways, including phone scams, email phishing, medical record theft, eavesdropping in public, and finding discarded documents that have not been shredded. If your mailbox is not secured with a lock, some ID thieves will complete a change of address request and have your bills rerouted, delaying your discovery of the fraud. Additionally, hacking of businesses servers, such as the Target or Anthem breaches, may release your personal information to criminals looking to make a profit from your identity.

### Protecting yourself

What can you do to prevent identity theft? Do not give out your personal information over the telephone, through the mail, or on the internet unless you initiated contact and are sure you know who you are communicating with. Some scammers will create fake websites that impersonate a real business in an attempt to obtain your personal information. Therefore, you need to exercise caution when entering your personal information online. Do not use the same password for your personal accounts and ensure the passwords you choose are hard to guess. In the event of a breach of security at a business which has copies of your personal information, ensure you change any passwords or credit cards that may be compromised. Lastly, shred any documents containing personal information prior to throwing them away.

### How to stop identity thieves that obtain your personal information

What are the first steps you need to take if you discover your identity has been stolen?

1. First, file a police report in case the person that stole your identity is committing crimes under your name.
2. Contact the IRS Identity Protection Specialized Unit at 1-800-908-4490 and report the fraud using Form 14039, Identity Theft Affidavit.
3. Alert the Federal Trade Commission at www.identitytheft.gov.
4. Change your passwords and notify your bank and other financial institutions of the theft.
5. Immediately put a fraud alert on your credit reports maintained by Equifax, Experian, and TransUnion, so you will be alerted if someone tries to open a line of credit in your name.
6. Finally, order your credit reports and review them to ensure that the only existing lines of credit are those you yourself opened. You can access your credit reports for free once a year by visiting www.annualcreditreport.com.

Being a victim of identity theft can be a violating experience; however, if you act quickly and take the necessary steps, you may be able to limit and then repair the damage.

## 5 COMMON PROTECTION MEASURES FOR INFORMATION SECURITY

Cyber attacks, which have been making headlines in the news, have evolved significantly over the last two decades. However, many of the counter measures used to protect against these threats have stood the test of time. In this article we'll discuss five of the most common measures both individuals and businesses should use to protect themselves against data loss.

### Use an anti-virus program

A good anti-virus (AV) program is critical to protecting your systems and data. Most modern AVs do more than just scan for viruses. They may include items such as a firewall, anti-spyware capabilities, or email filters for spam. AVs have gotten better over the years, but generally they are reactive to incoming threats. Some AV packages are proactive using profiling or Heuristics, but they are imperfect and may cause other issues if they are too aggressive. Whatever AV vender you select, always make sure you are regularly updating the program and running periodic scans.

### Keep good backups

This is one of the biggest mistakes individuals and businesses make. Failure to save current backups opens you up to the possibility of losing your important information in the blink of an eye, either through a natural catastrophe or theft. Ransomware has been on the rise in the last few years. Ransomware is when a hacker encrypts all of the data stored on your computer and demands payment for the "key" to unlock your data within a short period of time. If you don't pay up, your information will be deleted. Criminal actions such as ransomware are a major reason that it is imperative to frequently save current backups of all your critical files. This can be accomplished any number of ways including through hardware (external hard drive, tapes, DVDs) or software (online backups). Most modern operating systems such as Windows have built-in backup software, and many third-party backup packages offer additional features and levels of protection.

### *Elevate the security of your passwords*

In many cases a password is the only protection mechanism for your data. Use complex passwords and replace them regularly. Avoid using the same password for multiple sites. Good passwords avoid dictionary words, include both letters and numbers, possess both (upper and lower) case letters, and where possible, use a non-alpha numeric character (example: !,#,*). Try not to use personal information including date of birth or your children's names. These are more easily guessed than you think because hackers often have this information. Also, remember to keep these passwords secure and out of sight from hackers looking for files or papers marked with the password. If you are notified of a data breach from any company that holds your information, change your password immediately.

For accounts with highly sensitive or personal data, you may want to use multi-factor authentication that requires more than one verification method to confirm you as an authorized user of that account. A common multi-factor authentication technique requires a password and then a unique code texted to your phone in order for you to log in to the account. You can ask your financial institution and other account providers how they approach multi-factor authentication.

### *Limit exposure to your email address*

What does this mean? The longer an email address exists on the internet, the more likely it is to get harvested for spam including email phishing. It may be worthwhile to use a separate email address for website registrations or newsletters that you wish to subscribe to. If you receive suspicious email that you weren't expecting, delete it and certainly do not click on links or download any attachments that you don't know are safe.

### *Encrypt data wherever you can*

Encryption is the process of making data unreadable to an outside party unless they have the proper "key" to read the data. Encrypting data is a universal practice and reduces the threat of lost or stolen data being exploited by unwanted parties. Encryption can be applied to data that is transmitted (network/Wifi) or to data being stored on your hard drive. Always secure your wireless connection with the security options available for it. For instance, if you have to connect to remote data over a public network such as the Internet, encrypt your connection to that data. Most companies accomplish this through the use of a Virtual Private Network (VPN). If you have to transmit private financial data to a third party, ensure it is encrypted before sending it using tools like Winzip.

The five measures presented here will not make your data fully impenetrable. However, they are a good start and provide protection against many of today's threats.

As a firm focused on giving clients and investors "peace of mind," Arthur Bell CPAs understands the importance of protecting our clients' private information. Dedicated to the alternative investment industry for over forty years, we perform specialized and highly detailed work, allowing our clients to overcome difficult and complex obstacles. By listening and responding to clients, we have earned an outstanding reputation for delivering great results. We also understand what is critical to our clients and the industry so we can help clients grow personally, professionally, and profitably.

We develop our services around the needs of the alternative investment industry. If you need support in the areas of personal privacy and security, tax planning and compliance, audit and assurance, operations consulting, outsourced accounting, performance reporting, investor representation, and family office services, please contact your Arthur Bell advisor at (855)-787-0001 or at contactus@arthurbellcpas.com.





1-855-787-0001
CONTACTUS@ARTHURBELLCPAS.COM
WWW.ARTHURBELLCPAS.COM