Ron Lykins CPA's (614) 891-1041
"Trusted Tax Advisors since 1969"
45 W. Main Street • Westerville, Ohio 43081

HOW TO PROTECT YOUR IDENTITY FROM SCAMMERS, THIEVES, AND CRIMINALS

STAY SAFE WITH THESE 7 PROACTIVE STRATEGIES

A SPECIAL REPORT FROM RON LYKINS, CPA, MBA, PHD.

MARCH | 2017

It's an unfortunate fact of life.

The bad guys are getting smarter.

And it's getting harder to keep ahead of them.

Increased technology use, personal details being shared more frequently online, and hackers wanting to steal your confidential information – all create a "perfect storm" for your identity being stolen.

Could it happen to you? ***Absolutely yes!***

Imagine... you just retired from the table after a delicious dinner with your family.

Suddenly, the phone rings and you answer it. A stern voice on the other end asks if they're speaking to "Your Name" and you say yes. They then inform you that they are the IRS and claim you owe them thousands of dollars.

Worse, if you don't pay them, the person threatens to re-possess your home, your car, and garnish your wages.

First, don't panic. I'll explain why in a moment.

Second: carefully read these tips. They can protect you from unscrupulous attempts to steal your identity and potentially bring a big financial headache your way.

Tip #1: Don't Fall For Suspicious Phone Calls

One of the most important things that you and your family should know is: if you get a telephone call or email that claims to be from the IRS, immediately hang up without talking and notify our office.

The IRS never initiates contact with taxpayers by telephone or email. If you receive a call from someone who identifies himself/herself and provides their badge number and alleges you owe IRS money and must pay immediately or they will penalize you – HANG UP and call our office.

Tip #2: Protect Your Devices and Track Them Carefully

Do you protect your devices and keep them in a safe place?

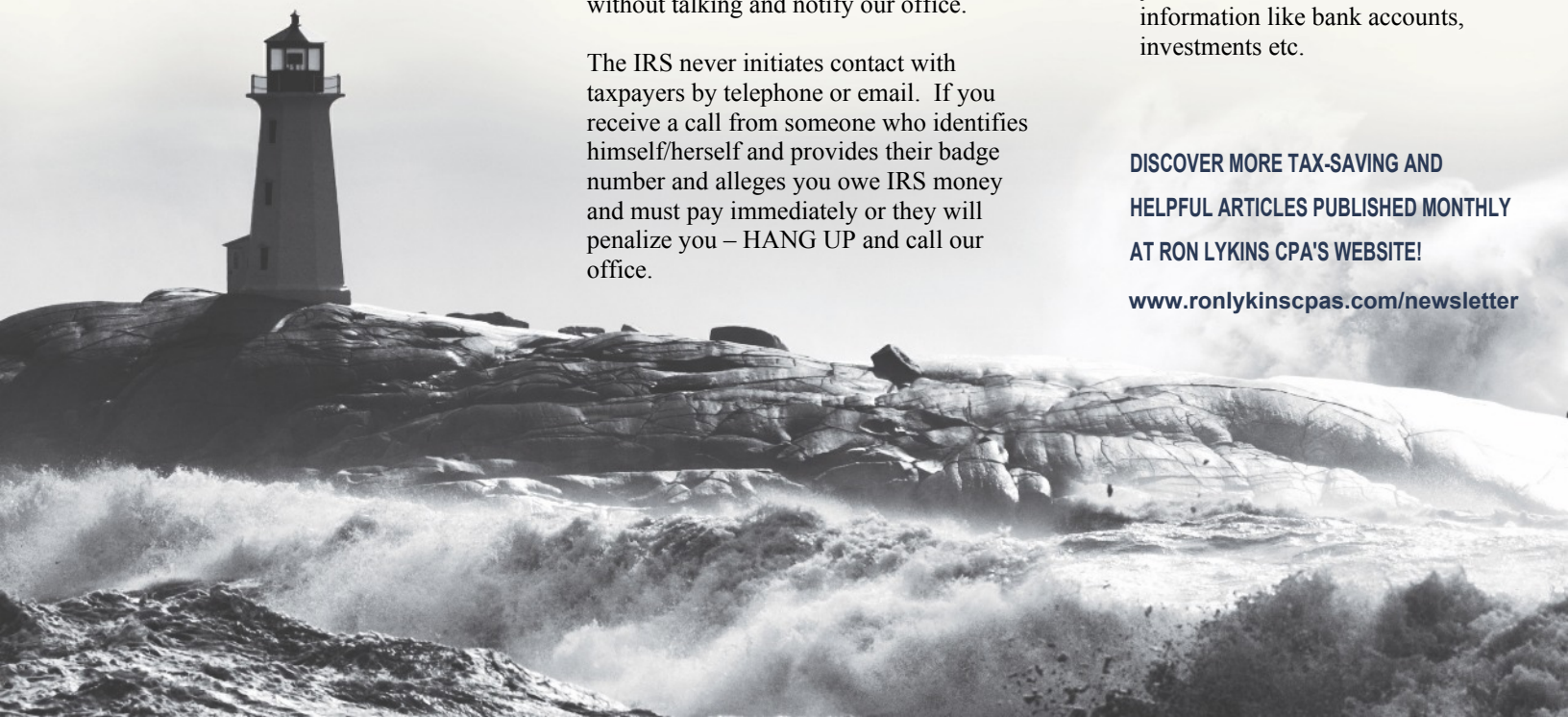
Here's a "newsflash": Almost 50% of identity theft is obtained from lost or stolen mobile devices, smart phones, tablets, laptops, and desk computers.

Obviously you need to monitor these devices. Take these steps to ensure you and your family's personal information stays safe:

- If your mobile device is lost or stolen, immediately wipe it clean and restore its factory settings.
- Use a strong password for all of your mobile devices and financial information like bank accounts, investments etc.

DISCOVER MORE TAX-SAVING AND HELPFUL ARTICLES PUBLISHED MONTHLY AT RON LYKINS CPA'S WEBSITE!

www.ronlykinscpas.com/newsletter



- Consider using a "password vault" that stores all of your passwords in one place and can even generate "hard to break" passwords. (Example: KeePassX, LastPass, Norton Identity Safe)

- When replacing your mobile devices, make certain the hard drive is cleaned and the device properly disposed of.

- Make sure you use essential tools for safeguarding computer information by using a firewall, virus protection, and file encryption for sensitive data etc.

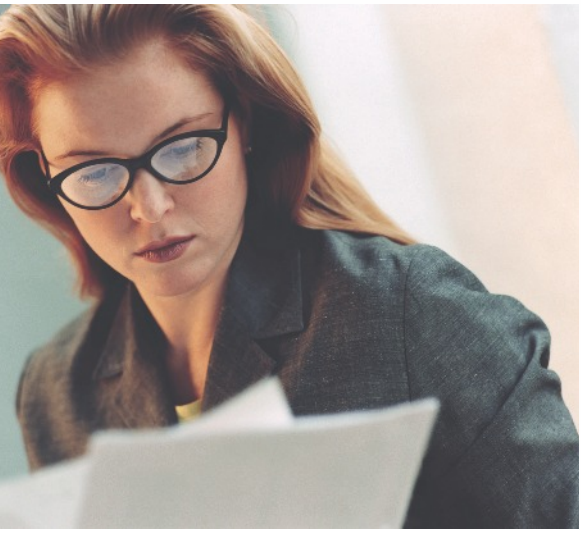
Tip #3: Keep a Close Eye On Your Credit Card Usage

Credit cards – most of us have them, but are you closely tracking their use?

Another large percentage of identity theft is related to credit cards. With just an extra bit of attention, you can reduce the possibility of credit card theft. A few tips:

- Review each of your credit cards to determine if you really need it. Many people have far too many credit cards. Obviously, the more credit cards, the higher the risk of credit card information theft.

- Never give your credit card number over the phone unless you are absolutely certain you know who you are dealing with.



- If you are making a telephone payment by credit card, ask the service provider to destroy all references to your credit card.

- Never use your credit card to order merchandise on the Internet unless you are certain the web site is secure and your credit card number and other personal information is encrypted.

  Look for a lock image in the URL address bar and also the https://www... address for the website.

- Immediately review and check your credit reports, if you have not done so in the past year. A surprising number of people have never personally reviewed their credit report line by line.

Federal law allows you to get a free copy of your credit report from each of the credit bureaus every 12 months. Go to www.annualcreditreport.com

- Consider putting a security lock on all your credit reports. Then there can be no additional activity on your reports until you unlock the account.

- If you suspect identify theft, contact the fraud department of the three major bureaus, Equifax, Experian, and TransUnion

- If your credit card is lost or stolen, immediately report it to your credit card provider. Make a list of all your credit cards front and back and store in a safe place that you can always access. This will enable you to quickly cancel your credit card if lost or stolen.

- Many credit card companies enable text and mobile alerts. These services can notify you every time your credit card is used. This is a great way to track and prevent potential fraud in real time.

Tip #4: Protect the Most Important 9-Digit Number You Have

It's the most important piece of information a thief wants.

Your social security number.

If someone is able to steal your social security number, they're able to open a new credit card, drain your bank account, conduct business and more – all under your name. Take the following precautions:

- Do not carry your social security card with you.

- Store your social security card in a safe deposit box.

- Make a copy of your social security card and store in a second safe place.

- Block out or encrypt your social security number on all your tax returns, stored records and applications for credit etc.

Perhaps the best idea of all to minimize social security fraud is to decline giving out your number unless it is absolutely necessary. Many people do not know they can simply decline to give out this sensitive information.

Tip #5: Pay Attention to Your Email

For the identity thief, email is one of their favorite tools.

Email phishing schemes are the most common method they use to steal your identity.

With these schemes, criminals will send emails to consumers that look like valid emails from reputable retailers and banks. When users click on the link, it can result in a piece of malware or adware getting downloaded into your computer or device, or it can take the user to a site the criminal runs to gain access to your personal data.

WEALTH-BUILDING TIP:

TAKE WHAT WOULD TYPICALLY BE YOUR TAX REFUND AND PUT THE MONIES TO GOOD USE. FOR EXAMPLE, ESTABLISH AN AUTOMATIC SAVINGS/INVESTMENT ACCOUNT, FUND AN IRA, INVEST IN A COLLEGE SAVINGS ACCOUNT SUCH AS THE OHIO 529 PLAN, PAY DOWN DEBT.

However, take heart. If you follow the precautions below, you'll greatly decrease the risk of falling for an email scam:

- Never respond to any email that asks for your social security number. This is true even if it is the company you work for. If you receive such a letter, contact your payroll department immediately.
- Don't open attachments, or click on links in emails unless you know who sent it and what it is. Especially be suspicious of emails that only have a file attached without a message.
- Never send personal information via an email.

Tip #6: Ensure Your Service Providers Are Protecting You, Too

We all have to share personal and confidential information with various businesses. Know which professionals have your personal information, including social security numbers.

For example, CPA's, tax preparation firms, attorneys, doctors, dentists all keep personal records. Take the following precautions:

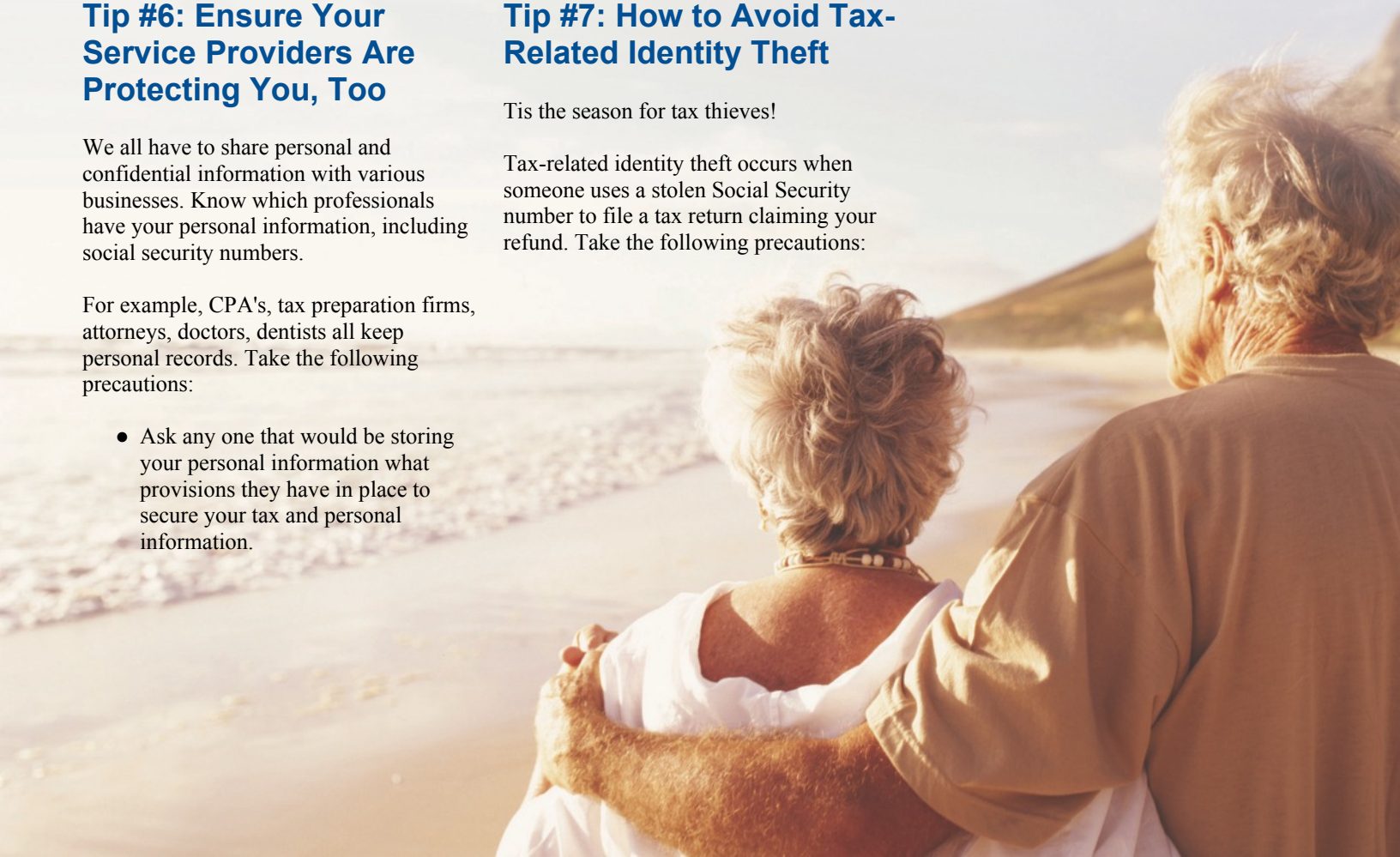
- Ask any one that would be storing your personal information what provisions they have in place to secure your tax and personal information.
- Ask how they would alert you if their files are hacked. Request a written copy of their policies regarding protection of files. A favorite source of social security information is for thieves to hack the files of a company. This could happen to the company you work for or do business with.
- Be especially concerned if you are dealing with small firms that have your personal information. They often do not have the knowledge or resources to adequately protect their files.
- Be alert in the news media regarding stories of companies that have been hacked.

Tip #7: How to Avoid Tax-Related Identity Theft

Tis the season for tax thieves!

Tax-related identity theft occurs when someone uses a stolen Social Security number to file a tax return claiming your refund. Take the following precautions:

- File your tax returns as early as possible. IRS will issue refunds to the first person filing with your Social Security number.
- Before a thief claims your refund, adjust your payroll withholding and any estimated tax payments to make certain you do not get a large refund.
- Take what would typically be your tax refund and put the monies to good use, for example, establish an automatic savings/investment account, fund an IRA, invest in a college savings account such as the Ohio 529 plan, pay down debt, etc.



IDENTITY THEFT PREVENTION TIPS

In summary, all of us can reduce the possibility of identity theft by implementing the ideas suggested here.

Don't think for a minute that identity theft cannot happen to you.

It can, and if it does, know that it is almost certain that the IRS can take well over a year or more to give victims their refunds.

In addition to refund delays, there are many hours of work and lots of frustration for you and your CPA. Save yourself from this potential nightmare by being proactive with protecting your confidential information.

Forewarned is forearmed!

DID YOU ENJOY THESE TIPS?

DISCOVER MORE TAX-SAVING AND HELPFUL ARTICLES

PUBLISHED MONTHLY AT RON LYKINS CPA'S WEBSITE! VISIT:

WWW.RONLYKINSCPAS.COM/NEWSLETTER.PHP

Ron Lykins CPA's

"Trusted Tax Advisors since 1969"

45 W. Main Street • Westerville, Ohio 43081

(614) 891-1041