

**Useful Links:**IRS.gov[Help For Hurricane Victims](#)**News Essentials**[What's Hot](#)[News Releases](#)[IRS - The Basics](#)[IRS Guidance](#)[Media Contacts](#)[Facts & Figures](#)[Around The Nation](#)[e-News Subscriptions](#)**The Newsroom Topics**[Multimedia Center](#)[Noticias en Español](#)[Radio PSAs](#)[Tax Scams/Consumer Alerts](#)[The Tax Gap](#)[Fact Sheets](#)[IRS Tax Tips](#)[Armed Forces](#)[Latest News](#)**Issue Number: IRS Security Awareness Tax Tip Number 7****Inside This Issue****Tips to Protect Your Personal Information While Online**

The IRS, the states and the tax industry urge you to be safe online and remind you to take important steps to help protect your tax and financial information and guard against identity theft. Treat your personal information like cash – don't hand it out to just anyone.

Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. Every time you are asked for your personal information think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy.

The IRS has teamed up with state revenue departments and the tax industry to make sure you understand the dangers to your personal and financial data. [Taxes. Security. Together.](#) Working in partnership with you, we can make a difference.

Here are some best practices you can follow to protect your tax and financial information:

Give personal information over encrypted websites only. If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for "https" at the beginning of the web address (the "s" is for secure). Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account and your financial information could be vulnerable. Look for https on every page of the site you're on, not just where you sign in.

Protect your passwords. The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home

IRS Resources

[Compliance & Enforcement News](#)

[Contact Your Local IRS Office](#)

[Filing Your Taxes](#)

[Forms & Pubs](#)

[Frequently Asked Questions](#)

[Taxpayer Advocate Service](#)

[Where to File](#)

[IRS Social Media](#)

users. Mix letters, numbers and special characters. Try to be unpredictable – don't use your name, birthdate or common words. Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts. Don't share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it's probably a scam. Keep your passwords in a secure place, out of plain sight.

Don't assume ads or emails are from reputable companies. Check out companies to find out if they are legitimate. When you're online, a little research can save you a lot of money and reduce your security risk. If you see an ad or an offer that looks too good, take a moment to check out the company behind it. Type the company or product name into your favorite search engine with terms like "review," "complaint" or "scam." If you find bad reviews, you'll have to decide if the offer is worth the risk. If you can't find contact information for the company, take your business and your financial information elsewhere. The fact that a site features an ad for another site doesn't mean that it endorses the advertised site, or is even familiar with it.

Don't overshare on social media – Do a web search of your name and review the results. Mostly likely, the results will turn up your past addresses, the names of people living in the household as well social media accounts and your photographs. All of these items are valuable to identity thieves. Even a social media post boasting of a new car can help thieves bypass security verification questions that depend on financial data that only you should know. Think before you post!

Back up your files. No system is completely secure. Copy important files and your federal and state tax returns onto a removable disc or a back-up drive, and store it in a safe place. If your computer is compromised, you'll still have access to your files.

Save your tax returns and records. Your federal and state tax forms are important financial documents you may need for many reasons, ranging from home mortgages to college financial. Print out a copy and keep in a safe place. Make an electronic copy in a safe spot as well. These steps also can help you more easily prepare next year's tax return. If you store sensitive tax and financial records on your computer, use a file encryption program to add an additional layer of security should your computer be compromised.

To learn additional steps you can take to protect your personal and financial data, visit [Taxes. Security. Together](#). You also can read [Publication 4524](#), Security Awareness for Taxpayers.

Each and every taxpayer has a set of fundamental rights they

should be aware of when dealing with the IRS. These are your [Taxpayer Bill of Rights](#). Explore your rights and our obligations to protect them on IRS.gov.

Additional IRS Resources:

- [IRS Commissioner Koskinen's Statement on the Security Summit Group Public Awareness Campaign](#)
- www.irs.gov/identitytheft
- [IR-2015-129](#), IRS, States and Tax Industry Announce New Steps to Help Public to Protect Personal Tax Data
- [Fact Sheet 2015-23](#), IRS, States and Industry Partners Provide Update on Collaborative Fight Against Tax-Related Identity Theft
- [IRS and Partner Statements on the October 2015 Security Summit Meeting](#)

IRS YouTube Video:

- Taxes. Security. Together. – [English](#)

[Back to Top](#)

Thank you for subscribing to IRS Tax Tips, an IRS e-mail service. For more information on federal taxes please visit IRS.gov.

This message was distributed automatically from the IRS Tax Tips mailing list.
Please Do Not Reply To This Message.