INTERNAL REVENUE SERVICE

IRS News Release

Media Relations Office	Washington, D.C.	Media Contact: 202.317.4000
www.IRS.gov/newsroom		Public Contact: 800.829.1040

Tax Time Guide: Protect Personal, Financial, Tax Information and Computers

IR-2017-55, March 9, 2017

WASHINGTON — The Internal Revenue Service today reminded taxpayers to be cautious and protect personal, financial and tax information, particularly at tax time.

This is the sixth in a series of 10 IRS tips called the Tax Time Guide, designed to help taxpayers navigate common tax issues. This year's tax-filing deadline is April 18.

The IRS urges taxpayers to be safe online and reminds them to take steps to help protect personal information and guard against identity theft. This is true all year long, but particularly at tax time, when taxpayers may anticipate hearing about a tax refund or the status of their return.

"The IRS works year-round to protect taxpayers against scams and identity theft," said John Koskinen, IRS Commissioner. "But we can't do this alone. Taxpayers can do their part by taking certain precautions to stay ahead of these would-be con artists."

Treat personal information like cash – don't hand it out to just anyone. Social Security numbers, credit card numbers, bank and utility account numbers can be used to steal money or open new accounts. Every time a taxpayer receives a request for personal information, they should think about whether the request is truly necessary. Scammers will do everything they can to appear trustworthy and legitimate.

Avoid Phishing Scams

The easiest way for criminals to steal sensitive data is simply to ask for it. Taxpayers should learn to recognize phishing emails, calls or texts that pose as familiar organizations such as banks, credit card companies or even the IRS. These ruses generally urge taxpayers to give up sensitive data such as passwords, Social Security numbers and bank account or credit card numbers. They are called phishing scams because they attempt to lure the receiver into taking the bait. The subject line may suggest the recipient just won a free cruise or that they must immediately update an account. Never open a link or an attachment from a suspicious email. It may contain malware.

Also, don't assume internet advertisements, pop-up ads or emails are from reputable companies. Check out companies to find out if they are legitimate. When online, a little research can save money and reduce security risks. If an ad or offer looks too good to be true, take a moment to check out the company behind it. Type the company or product name into a search engine with terms like "review," "complaint" or "scam."

Never download "security" software from a pop-up ad. A pervasive ploy is a pop-up ad that indicates it has detected a virus on the computer. It urges users to download a security software package. Don't fall for it. It most likely will install some type of malware. Reputable security software companies do not advertise in this manner.

Protect Personal Data

Taxpayers should not carry Social Security cards with them or any documents that may include this number. Provide Social Security numbers only when necessary. Occasionally businesses will request it when it is not essential.

Give personal information over encrypted websites only. Shopping or banking online should be done only on sites that use encryption. To determine if a website is encrypted, look for “https” at the beginning of the web address (the “s” stands for secure). Some websites use encryption only on the sign-in page. If any part of the session isn’t encrypted, the entire account and the included financial information could be vulnerable. Look for “https” on every page of the site.

Use Strong Passwords

The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users. Mix letters, numbers and special characters. Try to be unpredictable – don’t use names, birthdates or common words. Don’t use the same password for many accounts. If the password is stolen — it can be used to take over multiple accounts. Don’t share passwords on the phone, in texts or by email. Legitimate companies will not send messages asking for passwords. Receiving such a message probably means it’s a scam. Keep passwords in a secure place.

Set password and encryption protections for wireless networks. If a home or business Wi-Fi is unsecured it also allows any computer within range to access the wireless network and potentially steal information from connected devices.

Use Security Software

Make sure you have security software installed on all of your devices that connect to the internet. Many computers come pre-installed with firewall and anti-virus protections. A good broad-based anti-malware program should provide protection from viruses, Trojans, spyware and adware.

Set security software to update automatically so it can be upgraded as threats emerge. Also, make sure the security software is “on” at all times. If retaining important financial documents, such as prior-year tax returns, consider investing in encryption software to prevent unauthorized access by hackers or identity thieves.

Make sure security software has parental control options to protect children from malicious websites. Educate children about the threats of opening suspicious web pages, emails or documents.

Back Up Files

No system is completely secure. Copy important files, including federal and state tax returns, onto a removable disc or a back-up drive, and store it in a safe place. Save tax returns and records. Federal and state tax returns are important financial documents that a taxpayer may need for many reasons, ranging from home mortgages to college financial aid applications. Print out a copy and keep it in a safe place. Make an electronic copy in a safe spot as well. These steps also can help taxpayers more easily prepare next year’s tax return. If storing sensitive tax and financial records on a personal computer, use a file encryption program to add an additional layer of security.

The IRS, state tax agencies and the tax industry recently launched a public awareness campaign called Taxes. Security. Together. It provides additional safety tips for taxpayers. Also, see Publication 4524, Security Awareness for Taxpayers.

—30—