P.O. BOX 479 | SEARCY, AR 72145 | PHONE (501)305-9110 | FAX (501)268-5877

ASA NEWS

News & Information for Accounting Professionals

ARKANSAS SOCIETY OF ACCOUNTANTS

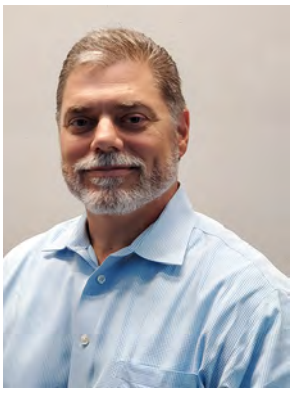
RESPECTED ACCOUNTING PROFESSIONALS SERVING OUR COMMUNITIES

Notes from ASA President - Chris R. Clatworthy

Our last newsletter started by describing the times we are living in as: difficult, scary, unusual, and strange. I think it is safe to say that these terms still apply. Many of these terms apply to the decisions facing your ASA Board as they try to make decisions that are in the best interest of our membership. With that being said, the balance of our continuing education seminars for 2020 will only be offered via webinar. While many of us enjoy the live seminars, we feel it is safest, and in everyone's best interest, to use webinars for the rest of the year. Our next webinar will be the 8-hour *Compilation and Review Webinar* on July 27, 2020.

As you are aware, we had to cancel our June 1, *2020 Estate and Trust Seminar*. We have been able to replace that seminar with an 8-hour webinar *Preparing for 2020 Returns NOW Webinar* on August 14, 2020 that will cover PPP loan forgiveness rules, CARES Act 2020 changes, working remotely, and upcoming changes to estate and gift taxes. Please be sure to register for this webinar to get an update on many of the changes caused by the COVID pandemic. The *Business Entities Webinar* will then be held on September 28, 2020.

Our *1040 Individual Tax Webinar* will be held on November 2-3, 2020. While we usually conduct this seminar in two locations each year, we will only be able to offer the webinar once this year on the dates mentioned. Be sure to look at the ASA website for dates and changes to our continuing education program.



Chris R. Clatworthy, CPA

We certainly realize that these changes to our continuing eduction program can be difficult, but once again, we felt it was in everyone's best interest to make these changes. I hope everyone stays safe and positive as we all work through these difficult times.

It is an honor to serve as your president.

Thanks,
Chris R. Clatworthy, CPA, CPCU, ARe, ACU

2020 ASA Seminars

- **TaxSpeaker Compilation & Review Webinar**
  July 27, 2020
  - 8 hours

- **TaxSpeaker Preparing for 2020 Returns NOW Webinar**
  August 14, 2020
  - 8 hours

- **TaxSpeaker Business Entities Webinar**
  September 28, 2020
  - 8 hours

- **TaxSpeaker 1040 Individual Tax Webinar**
  November 2 & 3, 2020
  - 16 hours

Unless otherwise noted, seminars will begin at 8:00 am and conclude at 4:00 pm.

Register online at: arksocietyofaccountants.com or call 501-305-9110 for additional information.

State Board of Accountancy Rule Change Highlights

A brief review of the most substantive changes

- Allowing CPA exam candidates to re-take a section of the CPA exam as soon as their scores have been released. This will eliminate the 3-month exam window and blackout periods where the exam was not given at the end of each window.

- Changing CPE rules so that those working in public accounting must get 40% of their hours in content areas of Tax, Accounting & Auditing, and Ethics. Those not working in public accounting are required to obtain 20% of their hours in Tax, Accounting & Auditing, and Ethics. Previously, all active CPAs were required to obtain 50% of their hours in the specified subject areas. The Board will also now accept up to 4 hours of nano learning CPE per year, which is CPE given in 10-minute increments. Finally, the Board reduced the group-study CPE requirement from 16 hours to 8 hours per year. These CPE changes are effective retroactive back to January 1, 2020.

- Creating a process for those with a criminal background to petition the Board to determine if they would be eligible to become a CPA despite their criminal history.

IRS Announces PTIN Fees for 2021

The IRS recently announced the annual fee for 2021 that tax preparers must pay to apply to renew their PTIN. According to final regulations, the fee will be $35.95 for obtaining or renewing a PTIN beginning this fall.

Anyone who prepares or helps prepare any federal tax return or claim for refund for compensation must have a valid PTIN from the IRS. The PTIN must be used as the identifying number on returns prepared. Failure to have and use a valid PTIN may result in penalties.

The annual renewal of PTINs ensures the IRS has up-to-date identifying information about each return preparer, which is essential for timely communication of important information. The program helps protect both return preparers and taxpayers and prevent the unauthorized use of PTINs.

PTINs expire on December 31 of the year for which they are issued. You can renew your PTIN online at www.irs.gov/ptin by logging into your PTIN account or by submitting a paper Form W-12 with the "Renewal" box checked.

New Seminar Added

ASA had added a new webinar, *Preparing for 2020 Returns NOW* to our seminar schedule to be held on August 14.

The webinar will guide attendees through the PPP Loan Forgiveness App, addressing the rules, the forms and offering examples, in order to maximize your clients' tax benefits.

On March 27, 2020, the President signed the CARES Act, the biggest funding bill in the history of the United States. Over 880 pages deep, there is an incredible amount of information, 50% of which will affect tax professionals. This class will review the significant retirement withdrawal changes for loans, penalties and RMD's; the Recovery for Rebate checks –who gets what, when, and how; the 50% employee retention credit; the small business loan program; changes to NOL and business interest deductions; and more.

The seminar will also address state and gift tax changes as established by Congress, along with basic gift and estate tax rules and planning concepts. How to work remotely and securely will be discussed, as well. A telecommuting policy guide will be provided, along with hardware and software recommendations.

Register for this important webinar online at: arksocietyofaccoutants.com or call us at 501-305-9110.

IRS & Security Summit Focuses on Tax Pro Security During Coronavirus with New Series on Working Virtually

The following article is from the first of the IRS' five-part summer series "Working Virtually: Protecting Tax Data at Home and at Work"

Many tax professionals have expanded telework options this year as firms, like other businesses, work to keep personnel safe, practice recommended safety guidelines and use technology to virtually serve their clients. During this period, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) have urged organizations to maintain a heightened state of alert as cybercriminals seek to exploit Covid-19 concerns.

To assist tax professionals with the security basics, the IRS, state tax agencies and nation's tax industry are launching a five-part series called *Working Virtually: Protecting Tax Data at Home and at Work*. The special series is designed to help practitioners assess their home and office data security. The first recommendation covers the "Security Six" – basic steps that should be taken for every work location. The series will continue each Tuesday through August 18.

"The Security Summit partners urge tax professionals to take time this summer to give their data safeguards a thorough review and ensure that these protections are in place whether they work from home or the office," said IRS Commissioner Chuck Rettig.

Although the Security Summit – a partnership between the IRS, states and the private-sector tax community – is making major progress against tax-related identity theft, cybercriminals continue to evolve. They are aware that tax practitioners and their systems may be more vulnerable this year during COVID-19, especially if they are working remotely.

The following are the basic "Security Six" protections that everyone, especially tax professionals handling sensitive data, should use:

1. Anti-virus software

Although details may vary between commercial products, anti-virus software scans computer files or memory for certain patterns that may indicate the presence of malicious software (also called malware). Anti-virus software (sometimes more broadly referred to as anti-malware software) looks for patterns based on the signatures or definitions of known malware from cybercriminals. Anti-virus vendors find new issues and malware daily, so it is important that people have the latest updates installed on their computer. Once users have installed an anti-virus package, they should scan their entire computer regularly by doing:

Automatic scans – Most anti-virus software can be configured to automatically scan specific files or directories in real time and prompt users at set intervals to perform complete scans.

Manual scans – If the anti-virus software does not automatically scan new files, users should manually scan files and media received from an outside source before opening them. This manual process includes:

- Saving and scanning email attachments or web downloads rather than opening them directly from the source.
- Scanning portable media, including CDs, for malware before opening files.
- Sometimes the software will produce a dialog box with an alert that it has found malware and asks whether users want it to "clean" the file (to remove the malware). In other cases, the software may attempt to remove the malware without asking first.

When selecting an anti-virus package, tax professionals should learn about its features, so they know what to expect. Remember, keep security software set to automatically receive the latest updates so that it is always current.

A reminder about spyware, a category of malware intended to steal sensitive data and passwords without the user's knowledge: Strong security software should protect against spyware. But remember, never click links within pop-up windows, never download "free" software from a pop-up, and never follow email links that offer anti-spyware software. The links and pop-ups may be installing the spyware they claim to be eliminating.

A reminder about phishing emails: A strong security package also should contain anti-phishing capabilities. Never open an email from a suspicious source, click on a link in a suspicious email or open an attachment – to avoid being the victim of a phishing attack and having clients' and firm data compromised.

- Continued on page 4

- Continued from page 3

2. Firewalls
Firewalls provide protection against outside attackers by shielding a computer or network from malicious or unnecessary web traffic and preventing malicious software from accessing systems. Firewalls can be configured to block data from certain suspicious locations or applications while allowing relevant and necessary data to pass through, according to CISA. Firewalls may be broadly categorized as hardware or software. While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type used:

Hardware – Typically called network firewalls, these external devices are positioned between a computer and the internet (or another network connection). Hardware-based firewalls are particularly useful for protecting multiple computers and control the network activity that attempts to pass through them.

Software – Most operating systems include a built-in firewall feature that should be enabled for added protection even if using an external firewall. Firewall software can also be obtained as separate software from a local computer store or software vendor. If downloading firewall software from the internet, make sure it is from a reputable source (such as an established software vendor or service provider) and offered via a secure website.

While properly configured firewalls may be effective at blocking some cyber-attacks, don't be lulled into a false sense of security. Firewalls do not guarantee that a computer will not be attacked. Firewalls primarily help protect against malicious traffic, not against malicious programs (malware), and may not protect the device if the user accidentally installs malware. However, using a firewall in conjunction with other protective measures (such as anti-virus software and safe computing practices) will strengthen resistance to attacks.

The Security Summit reminds tax pros that anti-virus software and firewalls cannot protect data if employees fall for email phishing scams and divulge sensitive data, such as usernames and passwords. The Summit reminds the tax community that users, not the software, is the first line of defense in protecting taxpayer data.

3. Two-factor authentication
Tax software providers, email providers and others that require online accounts now offer customers two-factor authentication protections to access email accounts. Tax professionals should always use this option to prevent their accounts from being taken over by cybercriminals and putting their clients and colleagues at risk.

Two-factor authentication helps by adding an extra layer of protection beyond a password. Often two-factor authentication means the returning user must enter credentials (username and password) plus another step, such as entering a security code sent via text to a mobile phone. The idea is a thief may be able to steal the username and password but it's highly unlikely they also would have a user's mobile phone to receive a security code and complete the process.

The use of two-factor authentication and even three-factor authentication is on the rise, and tax preparers should always opt for a multi-factor authentication protection when it is offered, whether on an email account, tax software account or any password-protected product. IRS Secure Access, which protects IRS.gov tools including e-Services, is an example of two-factor authentication. Using the two-factor authentication options offered by tax software providers is critical to protect client data stored within those systems. Tax pros also can check their email account settings to see if the email provider offers two-factor protections.

4. Backup software/services
Critical files on computers should routinely be backed up to external sources. This means a copy of the file is made and stored either online as part of a cloud storage service or similar product. Or, a copy of the file is made to an external disk, such as an external hard drive with multiple terabytes of storage capacity. Tax professionals should ensure that taxpayer data that is backed up also is encrypted – for the safety of the taxpayer and the tax pro.

5. Drive encryption
Given the sensitive client data maintained on tax practitioners' computers, users should consider drive encryption software for full-disk encryption. Drive encryption, or disk encryption, transforms data on the computer into unreadable files for an unauthorized person accessing the computer to obtain data. Drive encryption may come as a stand-alone security software product. It may also include encryption for removable media, such as a thumb drive and its data.

6. Virtual Private Network
This is critical for practitioners who work remotely. If a tax firm's employees must occasionally connect to unknown networks or work from home, establish an encrypted Virtual Private Network (VPN) to allow for a more secure connection. A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the company network. Search for "Best VPNs" to find a legitimate vendor; major technology sites often provide lists of top services.

How to get started with the "Security Six"
All tax professionals also should review their professional insurance policy to ensure the business is protected should a data theft occur. Some insurance companies will provide cybersecurity experts for their clients. These experts can help with technology safeguards and offer more advanced recommendations. Having the proper insurance coverage is a common recommendation from tax professionals who have experienced data thefts.

Additional resources
Tax professionals also can get help with security recommendations by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data (PDF), and Small Business Information Security: The Fundamentals (PDF) by the National Institute of Standards and Technology.Publication 5293, Data Security Resource Guide for Tax Professionals (PDF), provides a compilation data theft information available on IRS.gov. Also, tax professionals should stay connected to the IRS through subscriptions to e-News for Tax Professionals and Social Media or visit Identity Theft Central at IRS.gov/identitytheft.