IMPORTANT INFORMATION ABOUT DATA SECURITY RISKS

At Thomson Reuters, the security of your data and your clients’ data is a top priority—and as data security risks continue to grow for the tax and accounting profession, we’re continuing to take steps to strengthen data security, help protect your practice and comply with recent IRS security requirements.

The State of Security Today—Higher Risk Than Ever

Hackers are specifically targeting tax and accounting firms at increasing rates. This is true of firms that are operating on local networks, as well as those that operate in the cloud. In fact, many security experts believe that firms operating on local networks are even more vulnerable.

And it’s not just the big firms being targeted—tax and accounting firms of all sizes must stay vigilant against threats and take action to keep their businesses and clients safe.

Cybercriminals are becoming more advanced in their methods—from phishing scams where attackers claim to be from (for example) a software vendor in order to trick you into opening a file or clicking on a link containing malware, to illegally accessing firm software and filing fraudulent tax forms. Being unprepared for hackers can result in devastating consequences to your firm.

■ In May of 2015, criminals used information obtained from social media and stole around 724,000 taxpayers’ return data from the IRS’s Get Transcript system.

■ In January of 2016, criminals stole Social Security numbers from elsewhere outside the IRS and used them to obtain IRS e-filing personal identification numbers that could be used to electronically file returns.

How Thomson Reuters Helps You and Your Clients With Data Security

For tax year 2016, Thomson Reuters is working in partnership with the IRS to meet new requirements that strengthen login credentials for all tax-related software for professionals.

1. Login requirements for tax-related professional software—The IRS requires that any tax-related software for professionals must have a login with certain password requirements (regardless of whether the software is accessed via desktop or the cloud). This login functionality for CS Professional Suite® software will become available shortly, starting with our normal software releases in November.

2. Password strength—As defined by the IRS, a strong password must now contain a minimum of eight characters with at least one uppercase letter, one lowercase letter, one number and one special character. The IRS requires that passwords expire after no more than 90 days.

3. Timeout period—After 30 minutes of user inactivity, application access will be suspended and users will be required to re-authenticate using their credentials—although access is suspended, the operation of the software is not, so processes in the software will continue during timeout.

4. Multi-Factor authentication—It is strongly advised that you employ multi-factor authentication for additional security. We’re pleased to introduce Thomson Reuters Authenticator, our new multi-factor mobile app, which provides industry standard authentication factors.

Don’t Get Hooked by a Phishing Scheme—6 Smart Tips From Our Managing Director Jon Baron

1. Be suspicious if the circumstances of the email aren’t well known to you.

2. Hover your cursor over links to look for misspellings in the URL or an unusual address.

3. If in doubt, and you know the person, contact the sender directly to confirm they sent the email.

4. Before you provide your ID or password, stop and think. The IRS does not initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information.

5. Hackers can create fake websites that look like ones you use frequently, so check the URL in the browser to make sure it matches the address you’ve used previously.

6. Make sure that your operating system and browsers are updated automatically, and have the most up-to-date security software on your network and computers—and advise your clients to do the same!

EDUCATE YOURSELF—Learn more about how to protect your clients and your firm by visiting the IRS resources page at IRS.gov/Individuals/Protect-Your-Clients-Protect-Yourself.

FACT SHEET
DATA SECURITY RISKS
PROTECT YOUR CLIENTS AND YOUR FIRM

Tax.TR.com/CS
800.968.0600
TL30525