CYBER READINESS
INSTITUTE

A New Reason to Dread Tax Season: Cybersecurity Attacks

The tax filing deadline is rapidly approaching. You're searching through the papers spread over the dining room table trying to find the missing tax form. For the past week, you've been getting a steady stream of emails from your accountant asking for missing pieces of information. They need this form; they need that receipt; they need you to categorize an expense. You're getting frustrated and distracted.

Another email comes in from your accountant. This one is asking you to click a link and provide your social security number. You stop searching through the papers and reflexively start to click the link.

But something comes over you and you pause. "My accounting firm knows my social security number. They did my taxes last year." So instead of clicking the link, you start to reply to the email, but then it dawns on you. "If it's a phishing email and if I reply, it'll go back to the hackers."

You wisely decide to pick up the phone and call your accounting firm. They frantically tell you they've been hacked and the same phishing email went to all of their clients. They can't use email to warn their clients, so they've been calling them one by one and praying that no one clicks on the link.

At the accounting firm, it is total chaos. Tax season is always insanely busy, but the cyber attack is pushing them over the edge. Not only was their email compromised, but the hackers are demanding a ransom to unlock all of their client data.

When the attack started no one knew what to do. They had never even heard of a cyber incident response plan. They frantically called their IT consultant, who asked them if they had current back-ups of the client data. "I thought you were doing that!" they screamed at the IT consultant. "No. That's your responsibility," was the calm reply.

The IT consultant said that all of the software was up-to-date, so the hackers probably entered the accounting firm's system through weak passwords or someone clicking on a link.

The accounting firm started calling their clients to tell them about the fake social security request email. They had to warn each client that their personal information may be compromised, and explain that they would need to file an extension for filing their taxes. Twenty years of building a trusted client base jeopardized in one horrible day. The partners vowed to become cyber ready by following the advice below.

6 Essential Cybersecurity Tips for Tax Season

Advice for Individuals and Tax Preparers

Use Strong Passwords: Ensure you are using a 15-character, or more, passphrase, for your programs and that you are using unique passphrases across your accounts. Enable multi-factor authentication on your accounts, whenever possible.

Update Software: Enable auto-update and ensure your software patches are installed, particularly before tax season each year. Given how much business is conducted online during tax season, everyone is vulnerable.

Secure file exchange: Never give or ask for a SSN - or any other sensitive financial data - via email or online. Validate any requested financial transaction (e.g., wire transfer, direct deposit) or soliciting of personal information with a phone call to the individual who is requesting it. Ensure your file exchange/online portal is secure and encrypted.

Backup and Test: Backup your critical data regularly and test your backups every month.

Have a Plan: Ensure you have a tested incident response plan for your organization. In the event a breach does occur, it is critical to have a response and recovery plan you can activate immediately. Communication between you and your clients is also critical in the event of a breach.

Be Cautious: You already know that the IRS will never contact individuals by phone or email. But be cautious about emails from your tax preparer. If something doesn't look right, don't open the email before you call to verify that it's legitimate. This is a popular time of year when cyber crooks try to fool individuals into sending personal financial information.

About CRI

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit www.BeCyberReady.com.