

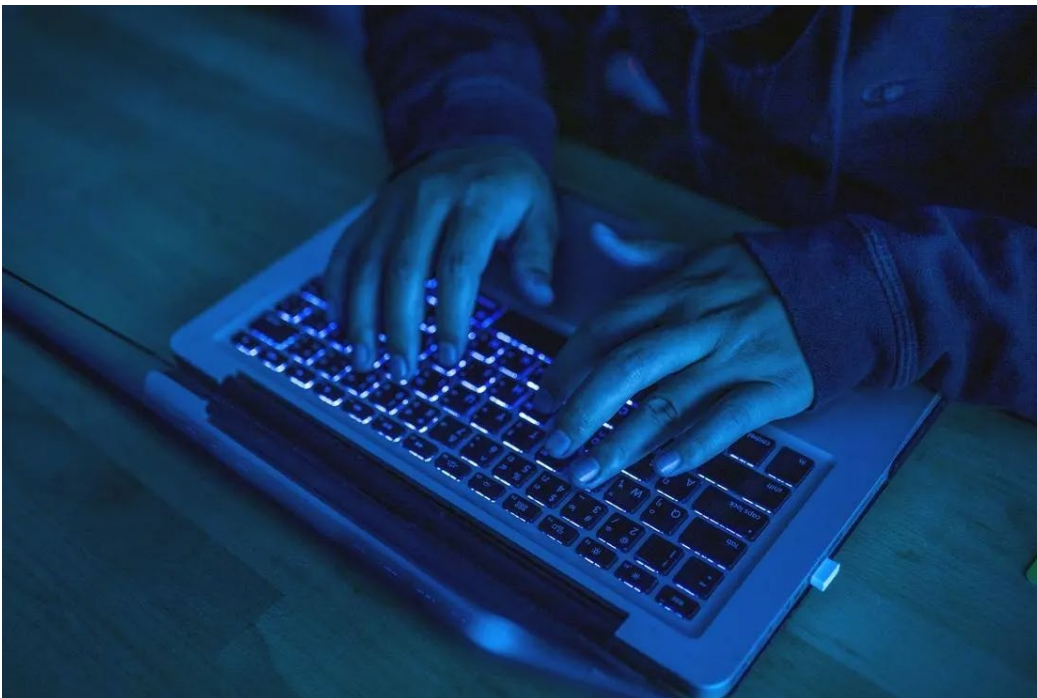
How One Small Click Led To Big Headaches For A Tax And Accounting Firm

The Internal Revenue Service has been warning tax professionals to watch out for filing season-related email schemes. An Austin based CPA firm learned firsthand how devastating the consequences can be.

Kelly Phillips Erb Forbes Staff

I write about tax news, tax policy and tax information.

Feb 2, 2024, 07:00am EST



Hacker stealing password and identity, computer crime. GETTY

It started with an email.

A part-time employee at Salling Madeley, PLLC, a full-service accounting firm serving clients throughout the Austin area, received a reminder to renew her password. In the middle of a busy tax season, it would only take a few seconds—and just one click.

The email looked legitimate and hit all the right notes. It looked something like this:



Password Expiration - Authentication Service

Hi User,

Password for your account will expire today. Please follow the link to update your account password.

[Keep same Password](#)

Support Service Desk Microsoft

[Please See Attached](#)

[Please See Attached](#)

Email scam CATHARINE DRAKE MADELEY

So, she clicked.

Shortly after, leaders in the firm received a notification that certain documents had been uploaded and downloaded. That set off alarms for Catharine Drake Madeley, who immediately recognized that the part-time employee did not work on those files.

The firm shut down the employee's access to email, but not before the part-time employee had received an email asking her to reset her password to the firm's portal, allowing the hacker to gain entry. That access, too, had to be shut down. But the damage had already been done—they'd been hacked.

A flurry of activity followed. The firm contacted their information technology vendor and their insurance company. Fortunately, Drake Madeley says, they did have cyber insurance coverage.

They also reached out to local law enforcement, the Federal Bureau of Investigation, and their IRS stakeholder liaison. They also called their lawyer.

Eventually, they made the calls they dreaded the most: notifying clients. The forensics team had carefully combed through the firm's files and cross-checked manual hits to data sets. They had a list of clients that the hacker had potentially accessed. And they had a list of taxpayers that had not yet filed returns. That combination was important because hackers targeting taxpayer data tend to move quickly to file to claim fraudulent refunds. "Why would a hacker target a tax firm?" Drake Madeley asked. "Because they want tax data."

Armed with that data, they urged their affected clients to file as soon as possible. Having a legitimate tax return on file would largely mitigate the damage.

The firm also offered credit monitoring to the exposed clients. That benefit was covered through the firm's cyber insurance.

Also covered? The data forensics work—the process of reviewing the files took months. Cyber insurance also paid the cost of notifying the affected clients.

Remarkably, the firm didn't lose a single client. "Most were appreciative that we responded quickly," Drake Madeley says.

The Scam

The scam that snared Drake Madeley's firm has been making the rounds in the tax world, so much so that last month, the IRS alerted tax professionals to watch out for a new round of filing season-related email schemes.

***"Why would a hacker
target a tax firm?
Because they want tax
data."***

Typically, the new client scam peaks during tax season, which runs from January through April. Not only are tax professionals expecting new clients to reach out, but folks in the industry are busy—that can make it tempting to simply scan an email and click.

The new client scams have similar patterns with an occasional twist to set them apart. In one variation, a scammer will reach out and ask whether a tax professional can help with their taxes—the original

email will either include a link or file to review the documents, or the scammer will send the link or file in a follow-up email after the tax professional responds.

One that landed in my inbox advised, "I want a quote and I would like to know your availability so that I can send you the necessary documents..." (Remember that spelling and grammar mistakes are often red flags.) A file was attached.

Another variation added in details to make it appear more legitimate:

Hello,

Please are you accepting new client for individual 1040 tax return filling ?

We file 2021 as family married with our children age range 8 years old and 17 years old just we acquired some 5 new air b and b in Florida Naples last year we also have in Arizona as well as well we have others rental properties, Schedule C-small business stock sales.

Please let me know if you want me to send our tax organizer and personal statement 1040 and 1099 if anything else needed let me know so i can share them with you via secure file or if you have your internal sharing platform you can send me the link to upload them directly.

Awaiting your response.

Email scam screenshot KELLY PHILLIPS ERB

Sometimes, the scammer appears to be responding to the tax professional's request for information—something along the lines of "Here's a copy of the tax return you requested."

The goal is to get you to click on a link or a file. Clicking on the link or file allows cybercriminals to collect your email address, password, and possibly other information, or load malware onto your computer to gain system access. That's precisely what happened to Drake Madeley's firm.

Setting up two-factor or multi-factor authentication with your email provider can reduce the risk of having your email account compromised. Stan Sterna, Esq., Vice President at Aon **AON +0.5%** in Chicago, Illinois, notes there are other measures firms can put in place, like installing, maintaining, and regularly updating anti-virus/anti-phishing software that scans and blocks malicious links, attachments, or accounts, as well as using a VPN (Virtual Protected Network) to mask employees' identities so would-be attackers can't intercept communications, especially when employees are using public WiFi. With remote work here to stay, Sterna also recommends encrypting mobile devices, such as firm laptops and smartphones, and restricting the amount of work-related information employees can share online to cut down on social engineering risks.

"These intricate email scams pose a real risk to tax professionals and the taxpayers they represent," said IRS Commissioner Danny Werfel. "Cybercriminals try to capitalize on tax season by masquerading as real taxpayers looking for help. What they really want to do is help themselves to the sensitive client data of tax professionals. We urge tax professionals and their employees to be extra cautious when receiving unexpected email solicitations and avoid clicking on links or opening attachments."

Cyber Insurance

Drake Madeley is thankful that she opted in on cyber insurance since it covered many of the expenses associated with the breach. Coverage had been offered through her insurance provider, and she said yes. It saved the firm potentially hundreds of thousands of dollars.

Jennifer Wilson, Cyber Leader at Newfront, a San Francisco-based insurance brokerage, believes that cyber coverage can be valuable, but warns consumers to be smart when choosing coverage. "Everyone wants to be in cyber," she says, "because there's so much money to be had in the space."

To ensure that you're getting the best coverage, you'll want to talk through options and find out what's available. For example, first-party coverage will cover extortion or ransom costs, data restoration, and business interruption (the average downtime from a ransomware attack, she notes, is 22 days). Your coverage should also include the cost of a good privacy attorney—laws governing notification following a data breach may vary from state to state, and you'll want someone on board who understands those requirements.

Cyber insurance may also help you pay costs incurred in defending suits from customers who may have had their data stolen or compromised, as well as the expense of forensics experts who can backtrack through your data to find out what the threat actors accessed.

Importantly, not all riders or policies will offer complete coverage.

The cost of picking up a policy can depend on a number of factors, but Wilson says many insurers will focus on record count—how many records is your firm responsible for? The higher the number of records, the more exposure you have.

Jessica Thayer, SVP, Financial Institutions Practice Leader at Starkweather & Shepley Insurance, a Rhode Island-based brokerage firm, agrees that many factors go into pricing—including revenues and the number of records. But, she notes, the cyber security protocols you have in place and training that is provided to the employees also heavily impact the premium. Firms without multi-factor authentication or end point detection (continuous monitoring of devices) will be expensive, she says, and those deductibles will be high. Not having those two cyber security measures makes it difficult to get insurance—if they can get it at all.

The goal, Thayer says, is to get the most competitive pricing with the broadest terms and conditions. That includes paying attention to coverage provisions—some provisions may have a limit that's less than the policy's overall aggregate limit. That's sometimes referred to as a sublimit—when reduced coverage is available to cover a specific type of loss. For example, Thayer notes that many claims involve extortion incidents and insurers often try to sublimit this coverage to much less than the overall aggregate. Your broker may be able to negotiate the full limit for extortion coverage.

So how do you find a policy or rider? Sterna advises partnering with a qualified insurance broker or agent to determine the best coverage for your firm. But, he warns that you should “make sure the broker or agent employs professionals experienced in serving the accounting profession and understands your business, potential risks, and how similar accounting firms approach their cyber coverage.” In other words—not all cyber insurance is created equal across all business sectors. Working with someone who understands the needs of the tax and accounting industry will help you make informed decisions about your insurance needs.

Additionally, when comparing carriers and policies, he suggests checking to see if they have a list of vetted and approved vendors like data breach coaches, attorneys, and public relations representatives with pre-negotiated rates. You should also, he advises, assess the experience of the carrier in the cyber space as well as their financial stability, as well as the experience of their cyber claim team. In the unfortunate event that you have a claim, he says, you want to work with a claim professional with experience handling cyber matters and working with data security experts and legal counsel.

Moving Forward

As for Drake Madeley's firm? They've since made significant changes. They routinely use two-factor authorization, when available, and other safeguards to make it more difficult to gain entry into systems. They've also changed their record retention policy, shortening the time that clients have access to data. Staff training has increased—and so has internal monitoring. And, they now consult with a cybersecurity specialist to stay on top of developments that could impact their systems.

It was an incredibly stressful time for the firm, but Drake Madeley has learned a great deal. “All it takes,” she notes, “is one little wrong click. One careless moment.”

Like many of us, she still gets those emails every day—it's endemic in the tax and accounting worlds. They take up, she says, at least half of her spam box on a regular basis. Now, she knows how dangerous they can be.

Looking back, Drake Madeley found a silver lining. Needing to pivot quickly has not only been good for data security, but also for customer service. "It has made the firm better," she says. "We are better advisors to our clients, to other CPAs and our peers."

Today, she doesn't shy away from telling her story because she hopes she can help others avoid the financial and emotional headaches that she and her firm experienced. Awareness is key.

"I used to think that our firm was small, so they're not coming for us," she says. "I was wrong."



Kelly Phillips Erb

I focus on tax law including tax planning and tax

Contact Jessica Thayer to learn more:

Jessica Thayer SVP & Financial Institutions Leader

(774) 241-3121

jthayer@starshep.com

About S&S Financial Institutions Practice Group

The FI Group at Starkweather & Shepley Insurance Brokerage, Inc. is committed to providing hands-on service, collaborating closely to identify competitively priced coverage tailored to your firm's liability needs in the Investment Industry. With over \$450 million in premiums placed, our Financial Institutions Practice serves over 2,100 investment advisors and fund complexes nationwide. We offer knowledgeable advice on insurance, including Directors & Officers Liability, Errors & Omissions, Cyber Liability, ERISA Bonds, Fidelity Bonds, and Property & Casualty coverage, with access to major domestic and international insurers. Beyond coverage, we provide consultation on limit adequacy, claims handling, captive structures, manuscript policy language, and creative policy structures, ensuring your peace of mind in the dynamic financial landscape.

ⁱForbes Article: "How One Small Click Led To Big Headaches For A Tax And Accounting Firm"

ⁱ <https://www.forbes.com/sites/kellyphillipserb/2024/02/02/how-one-small-click-led-to-big-headaches-for-a-tax-and-accounting-firm/?sh=4322cc99758f>