# Tax Season Security Tips for 2022

March 21, 2022

We're kicking off accounting's favorite time of the year: tax season (cue the memes). Accountants aren't the only busy people. The financial data surrounding returns makes the industry a prime target for cyber criminals.

Bad actors are evolving their methods. Modern attacks range from calls from fake IRS agents, to spear-phishing emails that trick recipients into downloading ransomware. The goal of these attacks is often to steal identities, submit fraudulent returns, and collect refunds.

Even smaller firms have access to sensitive data of high net worth individuals, so it's critical for all accountants to create a tax season security plan. In this post, we'll cover the most common vulnerabilities to be aware of while preparing and filing taxes, and introduce ways to utilize your technology and human capital to prevent data breaches.

## Understand the Ways Cyber Criminals Try to Swindle Consumers

### Phishing, and Its Variants

You're likely familiar with phishing emails: ones that appear to come from a legitimate sender like "IRS Tax E-Filing." Most phishing emails are caught by spam filters, but professional cybercrime gangs use social engineering to mount personalized, effective phishing attacks on high-value targets.

This directed form of attack is known as spear-phishing. It has worked even on behemoths like Facebook and Google, who were duped out of $100 million between 2013 and 2015 (CNBC). Spear-phishing attacks can attempt to scam accountancies, businesses, or individuals by tricking them into transferring money to the scammer. They can also be part of identity theft schemes by tricking tax professionals into verifying their EFIN and CAF numbers.

Voice-related phishing ("vishing") is also on the rise, with 400 vishing scams reported in 2020 (IRS). While phone-related tax scams are overall on the decline, the IRS cautions that it generally contacts people first by mail and will never request personal information by email or text.

### Ransomware: One Click Away

Ransomware attacks continue to rise across various sectors including governmental entities and financial institutions. The goal of these attacks is to encrypt data on the target's systems and require a ransom to restore access. Ransomware typically infects systems through links

in phishing emails. Swizznet recently saw such an attack firsthand in a state-based construction company client.

### Two Attack Methods, One Common Trait: They're Easier to Prevent Than Clean Up

Each of these attacks sound simple enough to avoid, but they are lucrative ways for bad actors to breach their targets' data and infrastructure. Companies who are hit with ransomware attacks often pay the ransom rather than risk losing sensitive data and damaging their reputation. The most common ransomware payment was $10,000 in 2020 (Sophos).

Both phishing attacks and ransomware take advantage of weak systems and human mistakes, so a tax season security plan requires securing technology and training human resources to recognize these attack methods.

## Secure Your Technology

Securing data used to mean locking files up in a cabinet inside a secured office. With remote work becoming mainstream, tax information is increasingly dispersed. Team members often use the same device for personal and business activities. This makes it imperative to develop and enforce policies around mobile and BYOD devices. This includes:

- Keeping software updated on all devices
- Backing up critical files and software on computers and hard drives
- Encrypting drives so only authorized people can access sensitive information
- Using applications with built-in partitions from the rest of the device
- Using anti-virus software and firewalls
- Establishing a virtual private network (VPN) for colleagues and clients to use while collaborating remotely

Technology companies are creating sophisticated solutions that combine financial data in a single source of truth, as Wes Stillman, Founder of RightSize Solutions, recently shared on Swizznet's blog. But often the weakest link is the humans that prepare and submit returns. Let's explore how to incorporate humans into your tax season cybersecurity plan.

## Build a Human Firewall

It may seem impossible to train employees to become part of your cybersecurity defenses. The good news is they don't need to become experts to play a useful role. It's key that they understand the most common threats and vulnerabilities in their remote workflows, such as knowing how to spot phishing attacks and avoid downloading ransomware.

Access-based controls are another layer of the human firewall. Develop and enforce policies

around strong passwords and multi-factor authentication.

Finally, onboard a dedicated cybersecurity professional, or form a relationship with a cybersecurity firm. Accountants need not take the place of cybersecurity professionals. These professionals can develop customized protocols then enforce them throughout the organization.

## SwizzStack: Swizznet's Contribution to Tax Season Cybersecurity

All this may sound overwhelming — we get it. Security challenges are heating up at the same time as organizations are struggling to fill positions. Who has the time?

After years of hosting QuickBooks and Sage software on the cloud, Swizznet began to see a need among accountants and accounting clients for a more comprehensive solution to their IT needs. One they can rely on for their accounting software as well as broader IT support.

We responded by developing SwizzStack, a full stack of services that includes everything you need to run your IT infrastructure no matter where your team members and clients work. SwizzStack includes our leading cloud hosting for QuickBooks and financial applications.

We customize a cloud environment based on your requirements, all backed with our bank-grade security. Unlike some other options, we host the full desktop version of QuickBooks using Citrix which gives you the same experience you're used to on desktop.

It's backed by our 24/7 Obsessive Support® which is available to help with all your IT needs.

If you're interested in learning more about the security threats facing accountants, CPAs, and bookkeepers, take an in-depth look in this eBook, which you can download here.