CYBERSECURITY FOR ACCOUNTANTS

3 WAYS TO PROTECT YOURSELF AND YOUR CLIENTS ONLINE

SmartVault

BY GABRIELLE FONTAINE, PB, ABSC

A NOTE FROM THE AUTHOR

This is a *huge* topic with many aspects that we as accountants should be aware of. While we can't cover everything in this eBook, we'll focus on what's most important for virtual accountants.

KEEP READING TO:

Recognize the very real security risks we face online as accountants and our role in protecting sensitive information.

Discover specific areas of concern specifically for accountants, and steps we can take to lower the risks of breach.

Walk away with a 3-part plan that you can implement right away, whether a solo accountant or working in a multi-member practice.

LEGAL DISCLAIMER

This is not legal advice and I am not a cybersecurity expert. This is information based on my own experience & research. If you have questions on what is the best course of action in your situation, consult your lawyer and/or a cybersecurity expert who can advise you specifically.

COMMON CYBER-ATTACKS

The first step to creating a safer accounting practice is to understand the common ways cybercriminals get access to sensitive information.

MALWARE

Malicious software, including spyware, ransomware, viruses, and worms.

Infections typically happen from clicking on a link or opening an infected email attachment (PDF or other documents or files).

PHISHING

Fraudulent email that's designed to steal sensitive data or to install malware on the victim's machine.

RANSOMWARE

Encrypts user files and presents an ultimatum: pay a fee (usually in crypto-currency) or lose the data indefinitely.

Only 20% of those who pay ever get their data back.

SQL INJECTION (database)

When an attacker inserts malicious code into a server that uses SQL, they force the server to reveal information it normally would not expose.

Pay attention to the tech that you use to know whether it's using SQL. For example, did you know that if you have a WordPress website, it uses a SQL database?

MAN-IN-THE-MIDDLE (MitM)

Also known as an eavesdropping attack.

This can happen when you use mobile devices and connect to the Internet using an unsecure public Wi-Fi.

The attacker gains access in between the user's device and the network. All information passing from the user to the internet goes through the attacker's view without the victim ever knowing.

Additionally, the attacker may install software to access all of the victim's information without being detected. Scary, huh?

WHY ACCOUNTANTS ARE AT RISK

Attackers usually ‘follow the money.’

Large corporate targets are getting harder to penetrate since they have the resources to constantly upgrade and improve security systems.

Small business is the next best target, since they are far less aware of the tactics attackers are using so are easier to breach.

Phishing especially targets financial professionals.
accountants are a key target!

“43% OF ATTACKS ARE TARGETED AT SMALL BUSINESS.”
SYMANTEC

WHERE ARE THE RISKS?

THE BIGGEST RISK IS HUMAN ERROR!

- Phishing / Email
- Login & Password Handling
- Document Management & Sharing
- Credit Card Information Handling

ACCESSIBILITY OF SENSITIVE INFORMATION

- Local vs. cloud
- Some small businesses think they are ‘safer’ by NOT using the cloud, but in some ways they are even MORE at risk! Within an office there are generally far fewer security measures to prevent both physical and electronic unauthorized access to sensitive information.

WHERE ARE ACCOUNTANTS VULNERABLE?

We need to pay attention to the methods we're using to handle sensitive info. That includes:

- Tools we use (hardware and software)
- Operations (including our team, both in-house and virtually)
- Policies (or lack thereof)
- Our clients' handling of sensitive information
- Ours and our clients' vendors' handling of sensitive information

We need to stop and think through the entire journey that sensitive information follows in the course of our accounting services and beyond.

STORIES FROM THE TRENCHES

PHISHING EMAIL

I was traveling out of my office all day, and in the afternoon checked email via my phone.

One of my clients, a consultant, who I knew was also traveling at the time, sent an email asking for "the account balance for today."

First Red Flag: My client is on QuickBooks Online and can check her balances at any time. It seemed strange, but I responded, letting her know that I would be back in my office at the end of the day and would provide the information requested then. I asked if that would be too late for her purposes. (I was guessing that she could not access QuickBooks Online for some reason.)

I continued to think about how strange it was, knowing my client as I do.

Upon return to my office and looking at the message again, I noted it did not have my client's logo in the email signature (she always uses that) and the style of writing was not typical for her.

CONTINUED

STORIES FROM THE TRENCHES

PHISHING EMAIL (CONTINUED)

I picked up the phone to call my client to speak with her about it and confirm it was truly from her. However, she was traveling and did not answer her phone.

I contacted her virtual assistant who manages my client's schedule to confirm her status and learned that some other strange email messages had been sent to others as well.

Second Red Flag: Shortly thereafter I received another email saying it was not too late, requesting the bank balance again, and saying that I was to send a wire on the client's behalf once the balance was known.

Clearly her email had been hacked and while the client was not reachable, her virtual assistant and I secured her accounts, changing all passwords immediately. We also notified her IT professional who was able to secure her email account.

Upon my client's return she explained that she was not surprised that the incident had happened since she remembered clicking on an email and provided requested login information. It was only after doing so that she realized it seemed suspicious.

STORIES FROM THE TRENCHES

✓ LESSON LEARNED

- Clients may do dumb things with their sensitive information without thinking about what they're doing!
- Clients often do not communicate with us when that happens.
- We need to listen to our gut when something doesn't seem right and pay attention to what your clients do normally vs. what seems unusual.
- We need to *pick up the phone* and confirm requests for non-routine instructions received via email or text.
- We need to be alert to educate and protect our clients proactively and on an ongoing basis.

3 WAYS TO PROTECT YOURSELF & YOUR CLIENTS

1 **EDUCATE YOURSELF, YOUR TEAM, AND YOUR CLIENTS**

2 **ASSESS YOUR EXPOSURE**

3 **IMPLEMENT PROTECTIVE MEASURES**

IT STARTS WITH AWARENESS

"...it is necessary to have cybersecurity training so that [we] understand how minor mistakes or simple oversights might lead to a disastrous scenario regarding the security or bottom line of [our] organization."

BO YUAN, PH.D., PROFESSOR, DEPARTMENT OF COMPUTING SECURITY AT ROCHESTER INSTITUTE OF TECHNOLOGY

001

EDUCATE

Do everything you can with the resources that are already available to you.

- Government resources (free).
  - → There is much available from government websites to help.
  - → Example: **Homeland Security > Cybersecurity** (link)
- Google is your friend.
  - → With a little searching on phrases or questions related to cybersecurity, you can find a lot of free help and resources.
  - → For example: Search for “How to protect small business from hackers” brings up current information you can use and help stay on top of trends and varying strategies.
- Resources provided through the profession.
  - → Industry conferences and association websites often provide educational information on how we in the accounting profession can protect ourselves and our clients with cybersecurity best practices. Use these wherever possible and ask questions.
  - → **AICPA Cybersecurity Resource Center** (link)

EDUCATE

GDPR and Cybersecurity:
They’re not the same, but they do overlap.

- GDPR (General Data Protection Regulation) applies to companies who do business with individuals located in the European Union. It is designed to protect personal data and its handling.

- Anyone who handles the personal information of any EU and/or UK citizen is subject to GDPR (that includes even just names and email addresses).

- GDPR requires company policies and procedures that include:
  - → Ownership of responsibility – who is in charge of being sure that GDPR is adhered to in the company?
  - → Knowing what information the company has and how it’s being protected
  - → Reviewing and documenting all of the people and vendors who have access to the data and their systems for protecting it
  - → Documented policies and procedures for every aspect of how the information is collected, handled, protected, referenced, stored, and disposed of.
  - → How staff (even if you’re a company of one) is trained regularly on security policies and procedures

EDUCATE

There are helpful online resources for how to implement procedures and tools that are compliant with GDPR.

- **The Institute of Chartered Accountants in England & Wales** (ICAEW)
- **The National Cyber Security Center** (UK government site)

ASSESS YOUR EXPOSURE

Map out your data, apps & workflow.

- Awareness is the first step in protection! Review the flow of information you receive about and from your clients all the way through to when you are done with it and storage. Document as much as possible about how it is cared for and accessed.
  - → Example: Where is your client data stored? Online? Offline? Locally? In the Cloud?
  - → Example: What apps are you using and where are they located? Cloud? Desktop?
- Set apps, browsers and operating systems to automatically update wherever possible and practical.
  - → Consider if it can be scheduled so as not to interfere with productive periods.
  - → Example: Windows updates can be scheduled for low activity hours.

ASSESS YOUR EXPOSURE

Consider virtual staff protocol and policies.

If you work virtually, then you do not have as much control over who potentially has access to client information. Having standards and checking in with your team to be sure they are being followed is important.

→ Example: How are passwords being handled and who else (if anyone) at each staff's location potentially has access to the information and is adequate security in place?

→ Use of LastPass where your staff does not actually see the login credentials is much better than providing a protected document in the cloud that lists the logins. While it may be protected in cloud storage, who else may see that information on screen if your teammate steps away from the computer? Or do your team members know to not store a copy of the cloud-based document on their local drive, mobile devices or on handwritten documents easily accessed at their desk?

ASSESS YOUR EXPOSURE

Is there a single point of failure?

Identify any and all potential points of failure in workflow, systems, or personnel.

→ If all vital information is stored in only one place, what would happen if that access failed or was destroyed?

→ For example, if you are using an encrypted hard drive, by the computer where it is located got infected with ransomware so that in effect all information was lost, would you be able to recover it from another secure, cloud-based backup?

→ This also applies to people. Is vital or sensitive information only known by one person so that if that person left the company (yours or your client's) that information would be lost or difficult to recover or reconstruct?

IMPLEMENT PROTECTIVE MEASURES

Set a recovery plan.

> “AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE.”
> BENJAMIN FRANKLIN

- Nowhere is that more true than in your security and disaster planning!
- Set up a response & communication plan:
  - → When something goes wrong do you and your team know what to do?
  - → Much like having a fire drill or evacuation route, there should be simple instructions and protocol that each person on your team knows about and has easy access to so that matters can be handled, protected, contained and reported quickly and properly

IMPLEMENT PROTECTIVE MEASURES

Consider insurance beyond Professional Liability.

- Insurance is a necessary safety net in business. As accountants and bookkeepers, it is a best practice to carry professional liability / errors and omissions insurance. But you should also seriously consider a cybersecurity policy as well. It can either be a separate policy or one added to your liability coverage.
- Check with your E&O insurance carrier first, or research new options, since this is a fast growing area in insurance for business.
  - → Not all coverage is the same, so do check details as to what is and is not covered in the case of a security breach.
  - → Also ask about recommendations for recommended practices that could lower your risk and your insurance premium.

IMPLEMENT PROTECTIVE MEASURES

Upgrade equipment and keep software updated.

- Technology is constantly changing and that means that old hardware, software, and operating system security may not be adequate after more than a few years.
- Consider upgrading at least every 3-5 years:
  - → Modems / routers
  - → Hardware firewalls
  - → Computer CPUs
- Keep your security software up to date – use auto-update if available.
  - → Virus checkers
  - → Firewall
  - → Malware protection
- Don’t forget mobile devices.
  - → Keep your apps and operating systems updated.
  - → Use passcodes and encryption as well as password managers here too.

003

IMPLEMENT PROTECTIVE MEASURES

Regularly change passwords & review systems for handling and changing them.

- Don’t use the same password for multiple logins!
  - → Each site you log into should have a unique password.
  - → Educate your clients on this point too.
  - → If one login is somehow hacked, it will prevent further access to other logins.
- Use passwords that are not easily broken.
  - → TIP: Use a password manager that generates random passwords for you and remembers them, so you don’t have to!
  - → If you must make up a password that you need to memorize, use phrases that only make sense to you and include special characters and numbers.
- Set a policy for changing passwords to your most important logins regularly, such as every 90 days.
  - → A password manager can help with this too.

CONCLUSION

SUMMARY

As technology continues to change, hackers will continue to look for new and more sophisticated ways to hack in and access sensitive information.

Our best defense is continued education and implementation of best practice. We want to do whatever we can to protect our clients and ourselves against attack, as well as take steps to prepare for the worst and survive a breach if it happens

Remember these three steps for safer virtual accounting:

1 EDUCATE YOURSELF, YOUR TEAM, AND YOUR CLIENTS

2 ASSESS YOUR EXPOSURE

3 IMPLEMENT PROTECTIVE MEASURES, INCLUDING REGULAR REVISIONS

ABOUT THE AUTHOR

GABRIELLE FONTAINE, PB, ABSC

Gabrielle Fontaine is a freelance Professional Bookkeeper and Advanced Certified QuickBooks ProAdvisor who assists tech-savvy consultants and self-employed professionals to save taxes, maximize cash flow, and grow profits using the power of online apps. Gabrielle has been in business for over 29 years, and has worked 100% virtually since 2003. She is the author of the popular blog, **The Freelance Bookkeeper**, and produces online training programs specifically designed for accounting professionals. She is a frequent guest speaker on business and accounting webinars and podcasts, as well as accounting technology conferences.

SmartVault

Cybersecurity threats will only continue to increase, and accountants are particularly at risk. Protect yourself and your clients with an all-in-one solution for online document storage and secure file sharing – SmartVault.

SCHEDULE A ONE-ON-ONE CHAT →