

bizink

practiceprotect

Stand out by being secure

How security is a point of difference
in marketing your accounting firm

www.bizinkonline.com



MARKETING FOR BUSY ACCOUNTANTS & BOOKKEEPERS • **b~**

Here at bizink~ we've worked with accountants and bookkeepers from all over the world. Our experience with websites and marketing has given us a clear idea of what works and what doesn't. We've taken the best and presented it in this guide, so that you can get the most out of your marketing.

Practice Protect is the world's #1 data security platform for accounting firms. The platform grants complete control over your firm's access of client data and passwords thanks to enterprise-level automation, application security, and human-powered support. Operating on the 'more trust, less risk' system, Practice Protect eliminates the need for a password manager and provides a powerful data security platform built for the future of accounting.

About the authors **Jon Melloy, & Matthew Wilkinson**

Jon is Head of Business Development at Practice Protect, the world's #1 data security platform for accounting firms. Since 2017, Jon has been working with accountants and bookkeepers to help them get complete control over the access of client data and passwords—all on the Practice Protect platform. **Schedule a demo with Practice Protect to find out more.**

Matt is the founder and CEO of Bizink and has helped hundreds of accounting and bookkeeping firms worldwide with their marketing. Known for his practical advice on marketing, he's spoken at Xerocon and several other accounting conferences worldwide. **Book some time with our team to find out more.**



Introduction

Let's face it, it's hard to find a unique selling point for your accounting firm. Standing out in a 'sea of sameness' is challenging when most accountants offer similar services, packages and pricing.

While your team and service are likely what makes your particular firm unique, finding another point of difference could be what catches the attention of someone seeking your services.

And when you take time to think about what matters to your clients, security is high on the list.

You don't have to look far before you come across conversations about data breaches, security concerns and vulnerabilities – especially when it comes to financial data.

While many of your clients are likely keen to embrace technology as a way to help manage finances and accounting administration, they may also be conscious of the risk that comes with operating online.

This is why, as a firm, putting emphasis on your efforts around security through your marketing and sales messaging could be what helps your firm stand out from the rest.

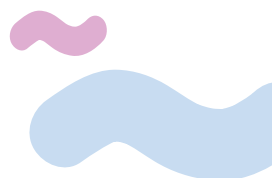
On the following pages, we'll explore why security is so important then how you can use good security practices to promote your firm and cement existing client relationships.

Why does security matter?

More and more aspects of our day-to-day lives are moving online. We've come to love the convenience of this digital connectivity, it does come with risk. Hearing about the impacts of high-profile cyber-attacks or perhaps experiencing fraudulent activity ourselves has made us increasingly conscious of where our personal data ends up, and who might have access to it.

No matter what business you're in, taking measures to protect both your own data and that of your customers, has never been more important – especially if you're dealing with financial or commercially sensitive information. As technology evolves, so too does the intelligence of hackers, who are actively on the lookout for vulnerabilities in businesses like accounting firms because of the amount of sensitive data they have access to.

Cyber-security is about putting practices in place that protect data and mitigate opportunities for cyber attacks, data breaches or even accidental internal security lapses as a result of human error. As a trusted partner to your clients' businesses, we know you understand your role in identifying and mitigating risk, and keeping their sensitive data safe. Security policies are also not a set-and-forget entity either. It's important to regularly check-in, update policies and educate your team on the latest security best-practice.





Why does marketing matter?

Word-of-mouth might have gotten you this far, but referrals alone are not a scalable or predictable way to grow your business. Even when you're busy, investing resources into marketing is important to keep a strong pipeline of work coming through. Educating, building awareness, establishing relationships and connections all involve a long-term game, as you build trust and brand equity in the market.

With a good marketing pipeline, you're also in a better position to choose the kind of clients you really want to work with. It's easier to hire and scale your business in line with demand, and with a proven system for acquiring new clients, good marketing also adds to the overall value of your firm.

Six ways to make your firm more secure

Having good security policies in place is the first step in keeping your business and your customers protected. How we work has changed in the past years, with some firms having remote teams or employees.

Here are six basic security measures that every accounting firm should have in place:

1. Set strong passwords and use multi-factor authentication

Don't underestimate the importance of a strong password as a critical line of defence. Passwords should always be unique to each application they are used for. Too often, passwords are short, simple and easily guessed. Hackers will use bots to break into accounts, so the more complex the password, the harder it will be to crack. Aim for 11+ characters, using a mix of letters, numbers and symbols. Place the same amount of importance on all passwords, regardless of what system they are used for; even non-critical systems can allow access to sensitive information. Enabling multi-factor authentication adds another layer of protection from password theft by requiring extra information to access an account. This could be something sent via an app, text message or security fob, or it could be answering further questions to authenticate who you are.

2. Lockdown access to your email systems

Due to the amount of data stored in them, email systems are one of the most commonly breached platforms, so to reduce your risk of exposure, ensure you have robust security around them, including strong password policies for all personnel. Integrating robust security features, such as location control, access tracking and two-factor authentication can help lock-out unauthorised access to email accounts.

3. Train your team so they are cyber-security assets, not risks

Embed security training as a part of your employee onboarding process, as well as ongoing training. As technology and threats evolve, your firm will need policies in place that keep your team up-to-date with the latest changes and necessary actions. Ensure they're aware of red flags, best practices and common mistakes to avoid. Your goal is that your firm is seen as proactive, rather than reactive, when it comes to security.

4. Know your obligations and put policies in place to be compliant

A good policy will take into account both the technology and human factors of cyber-security. Start with a risk audit so that you understand where you may currently have vulnerabilities in your defence. Create a clear outline of dos and don'ts for all personnel to follow, as well as the requirements of third party access. Put a response plan in place in the event that you do experience a breach.

5. Secure your devices and information not in the cloud

So much of our day-to-day work takes place in the cloud, and while lapses in cloud security can leave you open to attack, it's not the only place you need to consider protection. Your on-premise technology, such as devices (computers, smartphones), software, hardware, storage, networks and file settings can all come with their own risk, and therefore need to be considered as part of your security policy. Ensure anti-virus protection is installed and all software is running with the latest updates. Configure secure networks and establish clear employee protocol around things like downloads, file sharing, file storing and admin access.

6. Secure your remote team members

Ways of working have changed, and with more employees working remotely, it's necessary for accounting firms to adapt their security measures to account for both work-from-home and hybrid working arrangements. Home networks and home devices tend to be less secure than business IT environments, and therefore there are additional steps you'll need employees to take which should be outlined in a work-from-home policy. This could include providing all staff with a dedicated business computer, ensuring they run a malware scan, and installing password management tools.

How to use security in your marketing

Marketing is all about understanding your customers' challenges, motivations and desires, and positioning your offering in a way that addresses those to give them the confidence that you're the right person to help them.

With the knowledge that security is a top priority for your potential clients, incorporating messaging around your efforts to protect their personal and financial information could help address concerns before your audience even has a chance to raise them.

Most firms don't use security in their marketing so it's an opportunity to stand out from the pack. You probably offer accounting, tax and maybe bookkeeping services. Same as most firms! But if you can package those along with rock-solid security, it could be what makes a prospect choose you over rival firms.

Here are some ways to include security into your marketing:

Make mention on your website

Let potential clients know your position on security up-front by including a section on your website about your approach. This proactive transparency will instil confidence that security is something you take seriously.

Create helpful blog content

Educate your clients and prospects with information about cyber-security, particularly about protecting their own data in their business. Creating content will help you become known as the go-to firm for security expertise.



Reach out via email

Keep your clients and prospects up-to-date with the latest changes and security best practices via helpful email content with actionable tips and advice for their own business, as well as updates around what your firm is implementing.

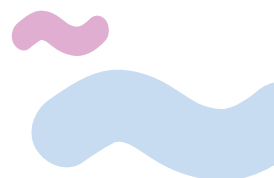
Spread the word on social media

Leverage your social channels to start conversations, raise awareness and educate your audience about the importance of cyber-security. Consistency is key to building a reputation, so include the topic of security into your regular social content calendar.



Run an event or webinar

Webinars or events are a great opportunity to grow your reach to a new audience. Prepare a presentation that offers high-value advice around data protection, and then consider offering a discount or deal to attendees.



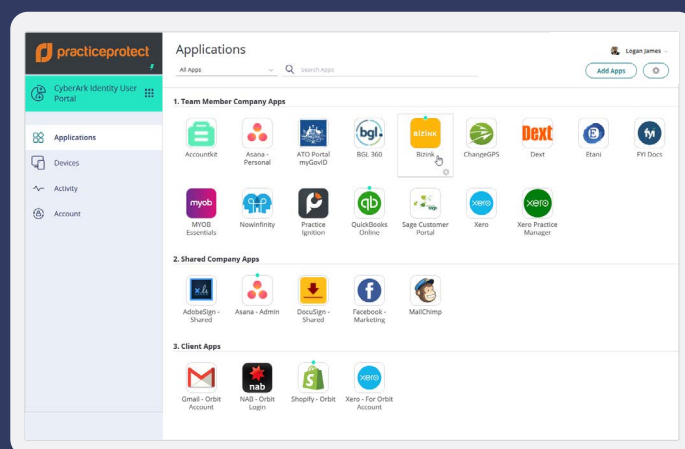
How to use security in your sales process

Security is also a conversation to carry through from your marketing to your sales. This is when you'll have an opportunity to talk in more detail about the measures you take to protect client data.

Consider including a section in your client proposal that further outlines the steps you take, and the steps required of them as a client, to ensure security obligations are being met.

You can also leverage conversations about security in your sales follow up, reiterating the emphasis that your firm puts on data protection as a key point of difference to other firms.

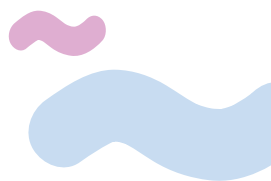
Showing is more powerful than telling. You could even demo your security features as part of your sales meeting



If that sounds like overkill, consider this section from one of the greatest books on marketing ever written, *Scientific Advertising* by Claude Hopkins:

“When you once get a person’s attention, then is the time to accomplish all you ever hope with him. Bring all your good arguments to bear. Cover every phase of your subject. One fact appeals to some, one to another. Omit any one and a certain percentage will lose the fact that might convince...So present to the reader...every important claim you have.”

Security is a pressing concern for many business owners. That makes it perfect to use as part of your sales pitch.



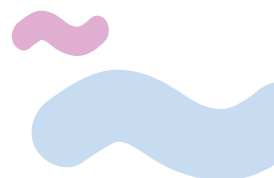
How to use security to wow your existing clients

Taking a proactive approach to talking about security and data protection will remind your clients about the additional benefits of partnering with you.

Include a section in your engagement letter about security to let your clients know seriously you take their data security.

As a trusted advisor to their business, you have an opportunity to position yourself as an expert by educating your clients on security best practices.

Become an authority by staying ahead of trends and topical scams. Be proactive with your communication, letting your clients know what to look out for when it comes to common phishing scams or data vulnerabilities.



Next steps

By protecting your data, you can appeal to clients who want to do business with companies that take security seriously. Here's what you can do next:

1. Conduct a Security Risk Assessment / Audit

First, take the time to understand where your firm is currently at with security and data protection by undertaking a security risk assessment. This is essentially an audit that takes into account both technology and human factors involved in protecting business and client information, and how well your business is currently performing.

2. Schedule a Security Consultation

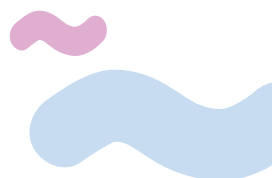
This will give you an idea of where you need to improve, or what further policies you need to put in place. Practice Protect [offer a free consultation which you can book here.](#)

3. Look at Sales & Marketing Resources

If you're ready to step up your game when it comes to promoting your security practices to clients, Bizink and Practice Protect have put together [these handy sales and marketing resources that can be adapted to suit your firm.](#)

4. Talk to us at Bizink

Finally, if you'd like it all taken care of for you, [talk to us at Bizink!](#) We can ensure that your firm is communicating the right messages to both clients and prospects in a way that helps your business stand out from the rest.



We hope this guide has shown you the possibilities of marketing automation for accountants. Bizink's website and digital marketing platform has automation built in. Book some time with our team to find out more.

www.bizinkonline.com

