Secure Your Brand and Reputation on Social Media

TECHNOLOGY SPOTLIGHT

What Does Social Media Mean to Your Business?

In the current operating environment, customers expect businesses to have an online social presence with which they can engage. In fact, 71% of customers who had a positive experience with a brand on social media are likely to recommend that brand to their friends and family.[1] Yet less than 64% of small businesses even have a website.[2] Therefore, having a strong brand and reputation on social media can be a competitive advantage for small businesses. In fact, the value impact of a reputational hit has doubled since the advent of social media.[3] With that in mind, it is worth exploring social media to find out how CPAs can help their organizations leverage social media without undue risk to the brand.

Importance

> It takes 20 years to build a reputation and five minutes to ruin it. – *Warren Buffett*

The key to success for any business is to scale its ability to manage relationships with audiences and to grow a vast customer base of one-on-one transactional relationships. The currency of social media is not money but trust. Commercial activity is the by-product of trust-based relationships that successfully identify demand and offer a convenient supply of goods and services while mitigating the risks of abuse. A professional social media strategy without an adequate plan to minimize risk can result in public embarrassment, financial loss or both.

1 www.lyfemarketing.com/blog/social-media-marketing-statistics

2 https://clutch.co/website-builders/resources/small-business-websites-2018

3 www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf

Unfortunately, recent studies indicate that social media data breaches accounted for 56% of all data breaches in 2018.[4] Perhaps for CPAs, social media strategy is not so much a matter of marketing and alignment as of simply avoiding disastrous mistakes that lead to the erosion of trust and data breaches.

Business Benefits and Considerations

Social media is often an integral part of an organization's digital footprint. It is more than just a marketing tool; when used properly, social media can:

- help communicate fresh content quickly to a wide audience
- put the brand in front of the world easily and inexpensively
- serve as an interactive platform for customer support
- help to generate new business leads
- set aside a dedicated corner of the Web to call your own.

However, organizations need to be aware that while a social media presence can be effective in building trust and reputation, it can destroy them even faster if not properly managed. For organizations of all sizes, social media management has become part of doing business. Even a simple social media policy helps all employees manage their online conduct, sensitizes users to reputational risk and enforces consistent discipline about the use and sharing of sensitive content. Trust – as both a metric and a digital currency – remains an elusive factor acquired at a premium and easily compromised.

So, what are the security risks associated with an online social presence? The following table provides a list of social media mistakes to avoid; they all have to do with preserving reputation, building your brand and fostering public trust.

4 www.itweb.co.za/content/G98YdqLxZZNqX2PD

Top 10 Social Media Risks	Risk Mitigation Strategies
Social media impersonation	• Make it official: reserve your own social media name for future identity protection. • Monitor your name using Google Alerts so you are notified if your identity is used in the media. • Even if you are not using a particular social media website, consider reserving your name to future-proof your online activity.
"Malvertising" instead of advertising	• Malicious advertising is becoming more prevalent. Stay clear of risky sites and keep your audiences away from them as well. • Pay attention to which search engine ads get associated with searches of your services and your name. • If your site hosts ads or you advertise on another site, be sure to associate only with well known brands and advertising platforms.
Social media profile hijacking	• Some of the world's largest, most well respected organizations have had their social media profiles stolen. Protect the account that manages your professional social media presence accordingly. • Periodically review your user roles and trusted accounts to ensure no new administrators have been added to your firm's social media profile. • Keep a list of support numbers, emails and links handy. Time is of the essence. If your sites get hijacked, you will want to take down the unauthorised content as soon as possible.
Website infection through vulnerable plug-ins	• Blog-enabled sites and Wordpress templates are popular because they allow companies to create and publish fresh content. However, the functionality is often provided by independent developers whose code may present a cybersecurity vulnerability to your site. • Social media pages often point to your site's forms or updates. Be sure to periodically scan your Wordpress plug-ins for bugs and infections before exposing potential clients to injections. • Tools such as Cloudflare or Comodo can protect your site from attacks and infections before social media users arrive. Use them to ensure your site is protected around the clock.

Top 10 Social Media Risks	Risk Mitigation Strategies
Account brute-forcing with stolen passwords	• Password reuse (i.e., the risky practice of using a password on more than one site) is one of the most significant causes of social media account takeovers (ATO) and website breaches. When passwords are compromised, attackers simply test them on other popular sites until they gain access. To assist with the task of keeping track of numerous passwords, organizations and individuals should select a trustworthy password management database and use it randomly to select, securely store and easily manage unique account credentials. • Protect your brand and corporate identity with social media policies that enforce unique passwords and avoid sharing them among team members. • Look for and enable multifactor authentication (MFA) where possible.
Newsfeeds polluted with malicious links	• A social media presence is a business responsibility. Carefully monitor and respond to public posts while remaining considerate of divergent views. • Always be ready to remove malicious posts; they can infect your customers and damage your reputation. Ban and report malicious accounts. • Do not be quick to censor. The public watches as you carefully address public views and enforce social media policies.
Domain squatting can forward users to malicious destinations	• Domain typo-squatters often register similar domains to those of legitimate companies to catch users who accidentally mistype your company's site. Register a few popular misspellings of your site's name to ensure they all point to your page. • Keep an eye on those domain expiry dates. Domain squatters have advanced tools to snatch expired domains and even hold them for ransom. In the meantime, all traffic to your site may be redirected to malicious destinations; confidential emails could be intercepted by criminals. • When used in conjunction with hijacked social media pages or malicious posts on your legitimate newsfeed, illegitimate domains can also hijack and damage your client relationships. Be sure to monitor links and notify users if additional vigilance is warranted.

Top 10 Social Media Risks	Risk Mitigation Strategies
Domain name hijacking can interrupt your business and intercept your communications	• Your company's domain name can be your most valuable asset. You can create infinite subdomains and email addresses, but if your domain name falls into the wrong hands, it can damage your business and interrupt online activity. • Securely maintain your domain registration and always review renewal notices before sending any payment or granting account access to management interfaces. • Do not expect your domain registrar or reseller to secure your domain for you. Be sure to enable multifactor authentication and watch for unauthorized login attempts that can indicate potential attack activity.
Website data theft at rest and in transit	• Encryption is the world's most trusted safeguard for preserving confidentiality and enabling privacy. Because web browsers now flag sites that do not encrypt transmissions with SSL or TLS certificates, be sure to provide that basic level of assurance to your site visitors and watch for unauthorized links that send users to sites that lack that all-important "S" after HTTP in the web address. • Many companies now use their social media presence to share documents, manage email and instant messaging, and even accept payments. Be sure to always provide these services with the strongest encryption levels possible from trusted organizations. • Does your web presence include cloud services in addition to social media? Because the integration is often seamless to users, be sure to guarantee all sensitive data stored at rest (e.g., files, payments and personal information) is encrypted on the target servers either by your organization or your trusted service provider. Regardless of who you are, your brand and image are always at stake.

Top 10 Social Media Risks	Risk Mitigation Strategies
Failure to get consent before making contact	• Many companies believe consent simply means "permission" (i.e., the act of being "allowed" to handle information either implicitly or by default unless told otherwise). That is often a mistake. Users expect not only to be explicitly asked but also to provide *informed consent*. They have a need to know what will happen to their information while in your custody. • Consent is a user's legal right to know that an organization that is borrowing their information will not share it without authorization. Guard client data and protect it from being discussed online, posted on social media or kept for so long it will get swept up in a future data breach. • Remember to always educate users while informing them of the risks to their data and how you mitigate those risks better than anyone else. Do not gloss over or minimize threats to information. Respect client consent. It will pay off in the trust you build.

Conclusion

Social media has evolved into the must-have tool for businesses who want to be accessible, connected and competitive. Like any storefront, it oozes relevance and trendiness, but it can also increase the attack surface for organizations unprepared to actively manage it with regular updates, newsfeed monitoring and security best practices. Include these activities in your online business plan and reap the continuous benefits of a healthy online presence with a resilient, controlled and fresh approach to social media management.

This publication is part of the **Technology Spotlight series**.

The entire series covers technology trends that impact CPAs and are available on our website.