WHITE PAPER

The Five Step Guide to Better Social Media Security

A Hootsuite White Paper

Hootsuite™

The Five Step Guide to Better Social Media Security

A Hootsuite White Paper

In 2013, not a single month went by without news of a major brand's social media crisis. From Fortune 100 companies to some of the biggest news agencies in the world, social media security threats affect everyone.

Social media accounts have been hacked, altered, and used to spread political and anti-corporate messages. Profiles and followers have been lost, brand images have taken hits, and even the international stock market took a brief tumble as a result of security issues.

So what is the solution? Pulling your company off of social media? This is simply not an option, as more and more people flock to social networks and use them to follow, talk about, and buy from their favorite companies and brands. Social media has become a pillar of business, and is expected to unlock value in excess of $1.3 trillion in coming years. Social's role will continue to expand and overtake more traditional business tools.

Enterprises should not forgo the benefits of social media due to fear of being victimized by outside parties. In reality, the majority of the above-mentioned security issues were the result of very simple scams and a lack of individual caution: suspicious emails and websites that employees visited without thinking twice; passwords being shared via email; untrained staff using corporate social channels. These decisions had major consequences on brands' social media activities and could easily have been avoided.

The good news is platforms have been created with the specific purpose of thwarting security threats and helping enterprises protect their social assets. As brands devote more time and effort to social media integration, what follows is a natural need to better educate themselves about the risks associated with using social. Once these risks are understood, you can take the necessary and simple steps needed to protect yourself.

The following guide examines the most common security challenges related to social media and provides simple solutions to reduce risk within your organization.

1. Educate and Train Employees

The challenge

To fully take advantage of social media, your company needs to entrust employees to take part in the conversation. Widening social participation beyond marketing to finance, human resources, development and sales will add value in terms of quality and quantity of social messaging. But while those currently in charge of social media may know the ins and outs of the networks and how to use them securely, employees across the company may not be in the same position. A staff member unfamiliar with how to post or someone who cannot see the signs of a suspicious link, email, or social message may act as the entryway for a hacker looking to gain access to corporate social assets.

The solution

It all boils down to **education**. Make your employees familiar with social media before they begin using those platforms. Educating employees about how to use social media tools ensures they are doing so securely. **Structured social media training programs** exist, such as **Hootsuite University**. With a minimal financial and time investment, employees can learn the best practices for utilizing social networks for the benefit of your company while maintaining secure control. These tools often come in a variety of formats, from webinars to white papers, meaning you can choose the option that best fits your business.

Employees should also be taught to **click with caution**. Spammy links are a common way to hoax or phish users into compromising social accounts. All staff should understand the potential consequences of clicking strange links in emails, no matter who is sending them. This is especially important to keep in mind when the links lead to pages which prompt them for usernames and passwords.

In addition to increasing basic security, social media education can also help improve the overall performance of your social media campaigns. Training programs extend beyond basic education into advanced themes, such as social media etiquette or how to build social followers.

2. Centralize Social Media Channels

The challenge

Part of growing a social presence for your business involves creating multiple accounts on multiple social networks. It also involves extending social media access to more employees within your organization. Perhaps some employees have created a variety of corporate social media accounts on Facebook, LinkedIn and Twitter without official permission. You may also need staff at all levels of the company, from your CEO to interns, to participate in social campaigns. As you scale, maintaining control of the multitude of accounts on various social networks becomes more difficult.

The solution

In building a social organization, an essential step is to bring all corporate branded social accounts under central administration. Start with an **audit of all the social media accounts** within your enterprise to discover branded accounts that are operating outside of your scope. Take note of who manages them and who has access to them. Delete any extraneous accounts and remove permission from anyone who shouldn't have it. Once you do this, the simplest way to centralize control is to consolidate these accounts within a social relationship platform.

Social relationship platforms allow you to draft messages and publish to several accounts and several social networks from one interface.

They also allow responsible parties to monitor all social messaging and activity in one place, simplifying what used to be a laborious and time-consuming task.

These platforms are usually equipped with security features. Built-in malware and spam tools can notify users when they click a suspect link. Hootsuite automatically quarantines abusive links hidden with Ow.ly URLs with a safety warning, using Google Safebrowsing to determine whether a link may be unsafe.

This an easy way to help employees avoid ending up on dangerous websites and potentially compromising their accounts. Social relationship platforms will also notify team leaders if suspicious activity is taking place on their accounts, which would allow them to shut down any potential security threats.

The need to bring all social accounts into one space has grown as **paid social media** (like Twitter's Promoted Products and Facebook's Promoted Posts) has become a core part of social campaigns. This billion-dollar industry has worked its way into most business' social strategy, and the financial implications associated with paid social has become another factor worth considering when centralizing control over social assets. You don't want your brand to invest thousands of dollars into Promoted Accounts or Promoted Tweets only to have your investment ruined by an inappropriate tweet from someone who gains access to your account. Thankfully, choosing a social relationship platform that allows you to buy ads from within the platform brings all of the above-mentioned security to your paid social efforts. Purchases of paid social can be monitored by responsible parties within your organization, with no need for additional passwords associated with paid social platforms.

3. Take the Necessary Steps to Protect Passwords

The challenge

In the past, shared social media accounts inevitably meant shared passwords. The more accounts companies have, and the more social networks they are active on, the more passwords they will need to create and share amongst all those participating in social campaigns, from interns to top executives. Each of these passwords is information that needs to be protected, lest it falls into the wrong hands. But how do you keep them secure when they're being passed from employee to employee, or even from branch to branch?

The solution

The first step in password protection is actually taking the time to **build a strong and complex password**. With your reputation on the line, short passwords of a few characters simply aren't going to cut it. The most common password in 2012 was still, sadly, "password". Consider implementing a **password management tool** which can generate complex passwords on your behalf.

Once you've created a strong password, employees should be certain to never store the password on shared computers, within emails or on mobile devices that could ever be stolen or lost (and not on post-its or other papers left lying around). A password management tool can also store your passwords for you, and allow you to share them to other members of the team without making them public.

Single sign-on (SSO) technology is another effective way to reduce the number of passwords floating around, and the associated risks. SSO allows employees to sign into Hootsuite with the same username and password from their corporate email account. In doing so, the "keys" or passwords to those accounts remain in hands of one trusted administrator. You want to ensure that should the password creator leave your organization, ultimate control and access to your valuable branded accounts remains secure and intact.

A social relationship platform also allows you to log in to your accounts from anywhere, and on almost any device, without downloading and saving valuable data. Hootsuite's **HTTPS** settings further protect your passwords and profiles while using Hootsuite on public wifi.

4. Institute a Messaging Approval System

The challenge

We are all human. That's part of what makes us effective on social media, since people enjoy conversations and content that they can relate to. But it also means we make mistakes. No one is immune, and no one should be expected to be. When a large enterprise has the majority of employees posting to social networks, mistakes are likely going to happen. If you're not prepared, a mistweet can be costly for your organization, both in terms of your brand image and, in the worst case scenario, financially. So how do you mitigate that risk on such a large scale?

The solution

There is a simple way to reduce the likelihood of a mistweet from ever getting sent out from a corporate account: enforce an approval process. Social relationship platforms offer teams the ability to put an approval process in place for all social messaging. This means that two sets of eyes will see every Tweet and Facebook post before they become public, drastically reducing the likelihood of an accidental mistweet from getting through. This process also allows social media managers to edit posts for spelling errors, double-check links, and generally ensure that messaging meets the company standard.

When your brand has thousands, even millions of social media followers, you will also want to make sure that only a select few people have message-posting capabilities, even if a large number of people are involved in message drafting. **Read only** settings, like those offered by Hootsuite, serve to mitigate the risk of entrusting the keys to these accounts to entry-level employees or interns. The different permission levels can follow the natural hierarchy of your company. Staff members can be given limited permission to draft messages, which must then be fed into an approval queue for senior management to sign off on before publishing. Limited permissions also allows you to restrict employees to specific social accounts and abilities. Not only does this reduce the risk of any mistweets, it allows employees to be more creative in their messaging and learn from the changes made by colleagues. In the end, this will help you scale your team when the need presents itself.

5. Prepare for the Worst

The challenge

No matter how many security measures you take, there is always a chance, however slim, that something could still slip through the cracks. A button can be clicked by accident, the senior employee in charge of message approvals might miss a critical error, or an intelligent intruder can find backdoor access into one of your accounts. So what do you do when something goes sour on social media?

The solution

Be prepared.

Improving your social media security does not mean you can neglect to prepare for a social media crisis. Every enterprise should have a specific crisis plan in place in case something goes wrong. This means employees should be trained very specifically on how to respond quickly and effectively during a crisis. Plans should be simple and flexible, since crises tend to be unpredictable. Have a contingency plan built as well. Hootsuite runs **crisis simulations** for Enterprise clients, testing and evaluating the emergency response of your social team. Our team of consultants then breaks down the areas and individuals that need work and suggests improvement to the overall crisis plan.

Hootsuite also offers optional security services for Enterprise clients. Hootsuite Managed Services helps you deploy the right mix of policies, technologies, and procedures to keep your brand and data safe. With our help, you can minimize social media crises, account hackings, and compliance breaches that cost time, money, and brand reputation. With Hootsuite Managed Services, you gain full awareness and control of your organization's social media accounts. A secure publishing environment is established, which ensures all outbound messaging is on-brand, compliant, and malware-free. Training is provided to empower your team with the training needed to execute a secure social media strategy.

Even if social media has caused a problem, it can also help you get out of it. Social media happens in real time, which means that a company needs to respond to a situation in real time as well. Social relationship platforms can serve as a command center, allowing you to oversee all communications at once. These tools can alert you of a potentially harmful situation or odd activity

on your accounts. They also allow you to monitor how the public is reacting to the issue and to quickly assign messaging to team members so that they can respond to questions and comments from followers and clients, or deal with any public-facing issues as they arise. Brands should also have an outreach plan. Social media allows you to reach a massive number of followers quickly to notify them of the problem and how you're working to resolve it.

Conclusion

With these five steps, you can put your C-suite at ease. Your brand's social media assets will be secure, and your employees trained on how to use them. And should the worst-case scenario come to be, you will be prepared to respond quickly and efficiently. Social media will be one of your company's biggest assets moving forward. Take the time to protect it.

For more information, visit enterprise.hootsuite.com

About Hootsuite Enterprise

Partner with Hootsuite to accelerate your social transformation

Hootsuite Enterprise empowers organizations to execute business strategies for the social media era. As the world's most widely used social relationship platform, Hootsuite Enterprise enables global businesses to scale social media activities across multiple teams, departments, and business units. Our versatile platform supports a thriving ecosystem of technology integrations, allowing businesses to extend social media into existing systems and programs.

We help organizations create deeper relationships with customers and draw meaningful insights from social media data. Innovating since day one, we continue to help businesses pioneer the social media landscape and accelerate their success through education and professional services.

Request a custom demo today by visiting enterprise.Hootsuite.com

Trusted by 744 of the Fortune 1000

WWF · Virgin · HBO · EUROSTAR · FOX · CBS Interactive

Allianz · IKEA · NHL · Nintendo · VICTORINOX · Mashable