The Five-Step Guide to Better Social Media Security

hootsuite | Enterprise™

hootsuite | Enterprise

The Five-Step Guide to Social Media Security

In 2013, there has not been a month without news of a major brand's social media crisis.

From Fortune 100 companies to some of the biggest news agencies in the world, no one has been exempt from social media security threats. Accounts have been hacked, altered and used to spread political and anti-corporate messages. Profiles and followers have been lost, brand images have taken a hit, and even the stock market took a brief tumble as a result of these security issues.maintain clicks-and-mortar solutions without functional solutions.

So what is the solution? Pulling your company off of social media? This simply is not an option, as more and more people flock to the 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. Its role will continue to expand and overtake more and more traditional business tools.

Fear of being victimized by outside parties shouldn't be propagated within enterprises because 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 are decisions that had major consequences on brands' social effort, but ones that could easily have been avoided.

Tools have been created with the specific purpose of thwarting security threats and helping enterprises to protect their social assets. As brands devote more time and effort to social media campaigns, what follows is a natural need to better educate themselves about the risks associated with using social. Once you understand them, you can take the necessary, but fairly simple steps needed to combat them.

The following guide examines the most common security challenges related to social media and provides simple solutions to reduce the risk of them coming to fruition within your company.

1. Educate and Train Employees

The challenge

To fully take advantage of social media, your company needs to entrust employees in all departments to take part in the conversation. Honing in on the expertise of people in the finance, human resources, development, and even sales departments will add a lot in terms of quality and quantity of social messaging. But while those 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 your social assets.

The solution

It all boils down to **training**. If you don't want employees who are unfamiliar with social media to be using those platforms, make them familiar. Educating employees about how to use social media tools helps ensure they are doing so securely. And **structured social media training programs** exist. 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 chose the option that best fits your business.

Employees should also be taught to **click with caution**. Do all people using your social assets know how to spot a malicious link? Spammy links are a common way to hoax or phish in order to compromise social accounts. As employees of the Onion recently found out, all staff should understand the potential consequences of clicking strange links in emails, no matter who is sending them. This is especially those that 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 like social media etiquette and how to use social to attract new clients.

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 powers to more and more employees within your company as you scale. 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 your interns, to participate in social campaigns. As you scale, maintaining control of the multitude of accounts on various social networks becomes more and more difficult.

The solution

Though you do not want social messaging to be centralized, an essential step to securing social media assets within a business is to bring all of your social accounts under central control. Start with **an audit of all the social media accounts** within your enterprise. 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 media management system**.

Social media management systems allow you to draft messaging and publish it 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 systems are also usually equipped with security features (in addition to a number of other features to benefit your campaigns, from message scheduling to analytics). **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. HootSuite also takes additional steps of deleting the offending from the database, and blocking the source domain from accessing Ow.ly. This is a very easy way to help employees avoid ending up on dangerous websites and potentially compromising their accounts. Social media management tools will also notify team leaders if any 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) have become a core part of social campaigns. This billion-dollar business trend is going to work its way into most businesses' 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 tens of thousands, even hundreds of thousands of dollars into banner ads 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 media management system 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 and there is no need for additional passwords associated with paid social platforms.

3. Take the necessary steps to protect passwords

The challenge

Shared social media accounts inevitably mean shared passwords. The more accounts a company has, and the more social networks they are active one, 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, like LastPass or KeePass, 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, to state the obvious, on post-its or other papers left lying around). Again, **a password management tool** like LastPass will store your passwords for you. They also allow you to share passwords without making them physically visible to other members of the team.

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 company social media accounts with the same username and password from their corporate email account. In doing so, the "keys" or passwords to those account remain in the hands of one trusted administrator. You want to ensure that should the password creator leave organization -- for any reason -- that ultimate control and access to your valuable branded accounts remains secure and intact.

A social media management system also allows you to login to your accounts from anywhere, and on almost any device, without downloading and saving valuable data. HootSuite's **HTTPS** settings further protects 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 hundreds or even thousands 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 very, very simple way to reduce the likelihood of a mistweet from ever getting sent out from a corporate account: a **two-step approval process**. Social media management systems offer teams the ability to put in place an approval process 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 or purposefully harmful 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, brands 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. **Limited permissions** 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 permissions levels can follow the natural hierarchy of your company. Staff members can be given the limited permission to draft messages, which must then be fed into an approval queue for senior management to sign off on before publishing. allows you to restrict employees to specific social accounts and abilities. Not only does this reduce the risk of any mis-tweets, it allows employees to be more creative in their messaging and learn from the changes made by higher-ups. 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 did 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. It then breaks down the areas and individuals that need to be better and suggests improvement to the overall crisis plan.

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 media management tools 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 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 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.

Social assets should not be tied to a single location or computer in case the crisis is geographic in nature, like a power outage on major storm. Take advantage of the mobility of social media and be prepared to use laptops or smartphones to execute your crisis response. This also allows you to move around and interact with employees while never leaving your social assets behind.

Conclusion

With these five steps, you can put your c-suite at ease. Your brand's social media assets will be secure, 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 on HootSuite Enterprise visit: enterprise.hootsuite.com