GUIDE

How to Protect Your Brand on Social Media

Strategies to prevent the 6 biggest brand disasters on social

Hootsuite®

How to Protect Your Brand on Social Media

Strategies to prevent the 6 biggest brand disasters on social

Contents

Introduction

The huge opportunity offered by social media is not without its risks. Brands now carry the responsibility that accompanies an “always-on” presence on social media.

But that doesn’t mean you should fear or forego a social presence. In fact, not being responsive can harm your brand more—as Lockheed Martin learned the hard way after U.S. President Donald Trump’s tweet caused their stock to plummet by 4 billion dollars.

With the right strategies, your brand can be active on social media without falling victim to brand-damaging events. That’s why 81 percent of executives now consider online brand protection a top priority.

To help you navigate the world of online brand protection, this guide provides an overview of everything you need to know:

- Why social media security is important for brands
- Six common social media risks and threats—and how to deal with them
- What to do when you’re facing a social media crisis
- How to plan for the future and minimize your risk

Why protect your brand on social media?

While it's essential for brands to be on social media, it's becoming more important than ever to approach it with a security mindset.

Social media security threats continue to grow year over year. Scams on social media grew by 150 percent across Twitter, Facebook, and LinkedIn in 2016. And Proofpoint's 2017 Quarterly Threat Report shows a trend towards more diversified and sophisticated attacks on social.

This increase in security threats on social media directly correlates with how much time we spend online. As Norton's 2016 Cyber Security Insights Report reveals, the need for "constant connectivity" leaves millions of people exposed to security breaches every year, costing billions of dollars. In 2016, 689 million people experienced cybercrime—a 10 percent increase from 2015.

And while cyberattacks and hackers often make the most headlines, the biggest risks often come from neglect and human error within an organization. This is often due to a lack of education around social media threats and protocols.

That's why it's essential that you identify risks and implement a brand protection plan for social media. As Gartner's 2016 Planning Guide for Security and Risk Management suggests, "the emergence of the 'Internet of Things' is elevating the importance of security and risk management as foundations."

The risks of not being secure on social media

- **Eroded brand trust:** Security breaches can have a serious negative impact on your brand. According to a study by FireEye Inc., 36 percent of respondents said that their perception of a brand had diminished after a security incident, and one third said they felt negatively about a brand.
- **Revenue damage:** The cost of a security issue or a misstep on social media can be astronomical. Billions of dollars are spent each year dealing with IT breaches and crisis communications.
- **Decreased ROI:** Brand-damaging events on social media chip away at the important investment that your company has made. Instead of increasing your bottom line, you're spending money on damage control.

The biggest risk is doing nothing at all

As compliance expert Joanna Belbey points out, the biggest risk to your organization is doing nothing.

If you're not implementing processes, tools, and educational programs to keep your brand protected and secure on social, you'll be much more vulnerable to social media risks and threats. By knowing about—and managing—common threats, you can safely and securely run your social media accounts.

Six common social media risks and threats

While there hundreds of different online threats that may affect your organization, risks on social media fall into six main categories you need to know about.

1. Account neglect

If your organization has social media accounts but you aren't actively monitoring or responding to conversations, that's account neglect. This leaves your brand vulnerable to unaddressed customer complaints, product issues, or spam, which can be extremely damaging to your brand.

Whether you're active on social or not, people will engage with your brand. When customers ask questions on social, they expect a response within a few hours—and 82 percent of customers say that having a fast response time is essential for a positive brand experience.

2. Human error

When security processes break down, we may be tempted to blame faulty systems and networks—but often, people are responsible.

When someone accidentally uploads the wrong image for a social post, shares information from the wrong account, or unknowingly shares sensitive data, that's human error.

According to a Forbes Insights Report, human error is the threat with the highest economic impact. It's behind one third of IT disruptions, and it's the leading cause of those disruptions. If you don't have tools and processes in place to catch these errors, a single error can have disastrous consequences for your brand.

For example, a copy and paste error by U.S. Airlines' Twitter account has been dubbed one of the biggest brand fails of all time. In a response to a customer complaint, they accidentally pasted a pornographic link in their tweet. With a proper approval system, this incident could have been avoided altogether.

3. Compliance violation

A compliance violation occurs when you break rules laid out by your company or regulatory body. According to a report by Proofpoint, there are over 12 regulatory bodies (including FINRA, FTC, FDA, and SEC) that have defined rules around what businesses can do on social media.

As Proofpoint's white paper The State of Social Media Infrastructure states, "regulators recognize social media as a public communication channel subject to existing earnings disclosure, truth in advertising, and data privacy regulations. These requirements are designed to protect consumers from being misled or defrauded."

Your team needs to understand what these policies are and how they affect your social activity. Without an approval process to safeguard social media interactions and catch violations, you're subject to hefty fines and lengthy investigations.

Learn how Spectrum Health remains compliant on social media with over 23,000 employees.

4. Phishing

Phishing scams are a way for cybercriminals to steal sensitive information like banking details. There are hundreds of phishing ploys on social media—in fact, the number has risen by 150 percent in the last year.

A common phishing scam on social media is the fake social media customer service account, which is designed to get people to click a fraudulent link and enter banking information. When someone tweets at your brand, for example, the imposter account will intercept and reply with a link for that person to enter their personal information.

5. Account hacks

An account hack happens when a cybercriminal takes over your social media account and sends out messages that are nasty, inappropriate, or otherwise off-brand.

When branded accounts get hacked, it's a costly PR nightmare, as the response from customers can be swift and severe. According to a report by ZeroFOX, the 2016 hack of NFL player Laremy Tunsil's social accounts caused around $21 million in damages.

Account hacks are not uncommon—they happen to big brands every day, as McDonald's learned when a hacker used their Twitter account to post about American politics.

6. Malware

Malware (short for "malicious software") is designed to gain access to your computer systems and data through malicious software code. It can lead to temporary or permanent loss of your brand's proprietary data.

Ransomware—malware that locks or encrypts your computer data and prevents entry until you pay a ransom demanded by the criminal—is also becoming increasingly common. According to a report by the U.S. Justice Department, there were over 4,000 ransomware attacks every day in 2016. That's a 300 percent increase since 2015.

Strategies to protect your brand on social media

By understanding the risks that face your organization on social media, you can better prepare your team to implement strategies in a safe and secure way.

The following six strategies will help you reduce the risk of human error and will allow you to identify and diffuse issues before they become a problem.

1. Identify and remove neglected social accounts

If you don't understand what social accounts are associated with your brand or how they're being perceived, you're at high risk for brand-damaging incidents.

By identifying and shutting down accounts that don't add value to your business, you can ensure a consistent brand voice across all your social channels.
For example, multibillion-dollar hospitality organization Delaware North unified their social presence by identifying and dealing with over 40 rogue accounts. By doing a basic inventory, they were able to remove inactive and low-value accounts—and invest more in high-value ones.

2. Update your password policy

A password policy is an important but often overlooked aspect of protecting your brand. Implementing a strong password policy makes it harder for people to hack your company's accounts and impersonate your brand.

Everyone using your organization's social accounts should be subject to this policy, which should include at least the following minimum requirements:

- **Complex passwords:** Passwords should be between eight and 20 characters, and should include uppercase, lowercase, and special characters.
- **Two-factor authentication:** A two-factor authentication system adds a second level of authentication when you sign in. For example, after signing in with your password, you may be required to enter a code sent to your mobile phone. This adds an extra layer of security to your sign-in process.
- **Single sign-on:** Single sign-on (or SSO) reduces the number of passwords floating around by allowing you to sign in to multiple systems using a single set of credentials. For example, you can sign in to Hootsuite with the same username and password as your corporate email account, so there are fewer sets of account credentials to maintain and keep secure.

Passwords should be updated regularly and managed by a single administrator or group within your organization. You should limit access strictly to ensure that passwords remain confidential.

3. Create a social media policy

To reduce security risks and ensure consistent behavior across your company, you should create a social media policy.

By creating a social media policy, you establish a set of processes and protocols for your brand channels. Most importantly, you make all employees accountable for protecting your brand from malicious behavior.

While social media policies will vary depending on the company, your policy should clearly emphasize the importance of protecting your brand's integrity, reputation, and values.

Here are some starting points for an effective policy:

- Brand guidelines and best practices
- Roles and responsibilities for social media
- Examples of appropriate (and inappropriate) behavior
- Consequences for social media misuse
- Security protocols and processes
- Applicable industry regulations and laws

Update your policy regularly to reflect your company's changing habits on social media. It may be beneficial to treat it as a "living document," like Cambridge University does, which helps employees feel more confident engaging with the University's content.

4. Train your employees

The new reality of bring your own device (BYOD) policies significantly increases security risk. That's why all employees should undergo basic social media awareness training, regardless of whether they use your organizational accounts or not.

Without employee training and education on social media, you'll struggle to implement your company policies successfully across your organization.

Employee training should include:

- Best practices and appropriate use of social networks
- An overview of your company's social media policy
- A list of common risks involved with using social media
- How to comply with company guidelines and mitigate risk

Learn how to run effective social media training for employees in our Hootsuite Academy course.

Learn more in our guide to creating a social media policy.

5. Set up an approval hierarchy for social media outreach

All of your company's branded social accounts should be protected by a clear approval system to ensure nothing goes on social media without the right approval. This significantly reduces the risk of human error.

If you're using Hootsuite, you can set up a double approver system with permissions and roles for individual employees. That means you can control who has full access to social content, who can post content, who can submit draft content for approval, and who has limited, read-only access. If you're using third-party apps or integrations like Brandwatch, you can also set up systems to flag potentially sensitive content and automatically stop it from being published.

6. Use social listening

Social listening is a technique you can use to "hear" the unfiltered conversations happening on social around your business. It's an excellent way to uncover new opportunities, but also an important aspect of protecting your brand on social media.

Social listening sets you up to address complaints, negative brand sentiment, or spammy messages before they escalate.

Using your social media management software, set up streams or alerts to listen for conversations that include the following:

- **Company name (and common misspellings):** Start by listening for direct mentions of your brand, and for customers trying to contact you directly. This is a first step toward gauging general sentiment around your brand and addressing any immediate issues issues. Be sure to include variations of your brand name (e.g., for Coca-Cola, include Coca Cola, Coke, Cola, and so on) along with common misspellings.
- **Industry keywords and hashtags:** Monitoring industry-specific terms and hashtags lets you engage with broader conversations and trends happening in your space. For example, if there's a discussion on social around a competitor's product recall, people may be wondering if your product has similar issues, or they may be asking questions about switching to a different product. By following conversations outside your direct brand circle, you can catch these issues, offer facts, and build trust with your community.
- **Campaign keywords and hashtags:** It's important to monitor campaign keywords so you can understand how people engage with your campaign. For example, Dove's Real Beauty Bottles campaign quickly snowballed into negative commentary on social. Many of the tweets responding to Dove's ad (that have been featured in articles) have no response from Dove. Without actively listening to your campaign's keywords and hashtags, you risk letting the conversation get away from you and damage your brand reputation.
- **Sentiment:** Using social media sentiment analysis tools allows you to monitor sentiment around your brand across across the globe and in multiple languages. You can get real-time feedback on how your social content is perceived, allowing you to adjust your messaging accordingly.

Learn more about our social media listening in our complete guide.

How to manage a social media crisis

Whether it's an ill-timed brand tweet, an irate post from an angry customer, or a suddenly viral video of a public relations blunder by your company, negative events can quickly spiral out of control on social media. To be prepared and handle the situation appropriately, you need a crisis management plan.

A crisis management plan helps you minimize risk by clearly outlining roles, responsibilities, protocols, and messaging—all of which are things you won't have time to plan during an emergency.

Your social media crisis management plan should address four key points:

1. Social monitoring protocol

Monitoring for negative mentions of your brand will at least give you the opportunity to address an emerging issue before it escalates into a public-facing crisis. Your protocol should include what's being monitored, who's monitoring activity, and instructions on how to deal with common or foreseeable issues.

2. Roles and responsibilities

To move quickly when a crisis happens, you'll need a list of key decision-makers, along with their roles and responsibilities. These should be people who are authorized to communicate external messaging on behalf of your brand. For example, you may have a key contact for approving all media relations messaging on social media, along with a secondary contact listed in case they are unavailable.

3. Potential scenarios and examples

To educate your employees on how to manage a crisis, include examples of potential social media crises in your crisis management plan, along with information on how they might be handled.

By running training sessions and simulation exercises for potential scenarios, you'll help employees understand the risks your brand faces and how they should respond. You'll also get a more realistic idea of how much time crisis management requires—and you'll have a great opportunity to identify any gaps or weaknesses in your plan.

4. Preapproved messaging

Your social media team leads should work with your PR team to develop preapproved messages that you can use in each scenario you've outlined.

Your preapproved messaging document messaging should be readily available for your social team to use, and should clearly indicate signoff from stakeholders.

A crisis management plan should allow you to:

- **Act quickly.** Acting quickly and effectively can make all the difference in handling a crisis on media. As crisis management expert Duncan Gallagher points out, 28 percent of crises spread internationally within one hour—yet it takes an average of 21 hours before companies have messaging ready. This is an area where most brands could improve significantly.
- **Be transparent.** Be open and honest with your customers when discussing issues on social. When it's possible, take the discussion offline to resolve a customer's issue. If it's reached a point where that isn't an option, you'll need to address questions publicly with as much information as you can legally provide.
- **Communicate internally.** During a PR crisis, your employees need to be updated regularly about what is going on and how they should respond to any questions they receive from the public. By communicating across your organization, you can significantly reduce the risk of having ill-informed employees spread misinformation.
- **Build trust.** When a crisis happens, there's an opportunity for you to build trust with your community. For example, when Morris County was hit by Hurricane Sandy, the city used their social media accounts to alert citizens and distribute reliable and accurate information, saving lives and helping prevent further devastation.

Review and revise your plan after any crisis

When the dust has settled after a social media crisis, you should hold a debriefing session with relevant team members and explore what went well and what you can improve. This will help you identify parts of your crisis management plan that need to be updated.

Get more resources on crisis management

- Guide on social media crisis management
- Webinar on dealing with a PR crisis
- Academy course on crisis preparedness

Planning for the future: Investing in social media protection

Each year, organizations spend billions of dollars responding to online security issues. Without the right tools and processes, you significantly increase the risk of costly brand-damaging incidents—which can have a long-term negative impact on your business.

By making brand protection a priority for your social accounts, you can stop harmful behavior, minimize the cost of brand incidents, and stop disasters early.

Invest in a secure future for your organization.

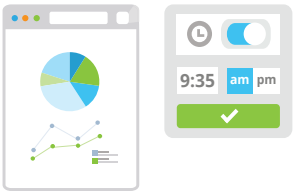
Protecting your brand should be a company-wide effort. Hootsuite Enterprise allows you to safely engage audiences across all your social networks while guarding against hackers, minimizing the risk of employee error, and remaining compliant.

We work with partners to keep your business secure on social media.

About Hootsuite Enterprise

Partner with Hootsuite to accelerate your social transformation

Social Marketing



Social Selling

Employee Advocacy

Social Customer Service

Hootsuite is the most widely used platform for managing social media, loved by over 15 million people around the globe and trusted by more than 800 of the Fortune 1000. Hootsuite Enterprise empowers organizations to execute business strategies for the social media era and scale social media activities across multiple teams, departments, and regions. Our versatile platform supports a thriving ecosystem of social networks complemented by 250+ business applications and integrations, allowing organizations to extend social media into existing systems and programs.

Along with our channel and agency partners, we help organizations build deeper relationships with customers, stay connected to the needs of the market, grow revenue, and draw meaningful insights from social media data. Innovating since day one, we continue to help organizations pioneer the social media landscape and accelerate their success through product training, group training and tailored organizational training, as well as security and compliance services.

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

Trusted by over 800 of the Fortune 1000

WWF · Carnegie Mellon University · VISA · Expedia · Sony Music · PayPal

Allianz · British Columbia · HBO · Novartis · Porsche · Monster

Hootsuite®