GUIDE

Brand Protection for Modern Enterprises

Protecting your brand from internal and external threats on social media

ZEROFOX

Hootsuite®

Brand Protection for Modern Enterprises

Protecting your brand from internal and external threats on social media

Contents

What is brand protection?

The term "brand protection" has been around for decades. The underlying concept hasn't changed: a company's brand creates immense value for the company, so it must be protected from risks that might damage or devalue it. However, what has changed radically in recent years are the risks to the brand: how they manifest themselves, the media on which they occur, and what can be done to mitigate them.

In our connected world, most consumers engage with brands online. 81% of consumers' purchasing decisions are influenced by their friends' social media posts, and according to Google, 67 percent of buyers are influenced by review sites. Brands have taken note. According to CMO Survey, 22.4 percent of marketing budgets is spent on social media—and 93 percent of companies use social media to target buyers.

Although traditional advertising and TV spots still comprise a significant portion of consumer mindshare and brand awareness, it's online where opinions are expressed and the battle for brand truly plays out. The rise in social networks has magnified consumers' ability to criticize or promote a brand. It has also opened the floodgates for cybercriminals to exploit what should be positive engagements between brands and their customers.

These risks can have massive financial impact. According to Kaspersky, the global, annual cost of phishing attacks on social media is $1.2 billion. ZeroFOX estimates that financial scams on Instagram alone cost brands roughly $420 million each year.

Getting the right people to the table and building a strong but flexible brand protection program is a critical initiative for all modern enterprises. This guide outlines why organizations need a brand protection program, the risks to brands, who needs to be involved, and a step-by-step process for getting a brand protection program off the ground.

Why you need to protect your brand

A company's brand is its public face for customers and the world. Impressions of the brand can tip the scales in favor of meteoric growth—or toward the dustbin of failed businesses.

In industries with fierce competition (think food and beverage companies, car manufacturers, airlines, fast food chains, or cellphone carriers), a brand's reputation is perhaps its greatest asset in winning market share. Companies like Apple, Dollar Shave Club, and McDonald's have built their entire business on a strong, consistent brand. Protecting that asset is vital to their continued success.

The advent of social networking has brought new opportunities, risks, and complexity to the world of brand management. A brand is built on different media, encompassing individual impressions and engagements at a global scale. Social media has magnified the scale of those impressions and engagements to mind-blowing proportions.

Now when something goes amiss, such as Pepsi's Kendall Jenner TV ad or United's treatment of passengers on overbooked flights, consumers are quick to vent their frustration online. Brand risks go viral and the reputational damage can spiral out of control.

Even when an organization hasn't made a grievous public mistake, social media allows anyone to actively criticize a brand. Consumers vent about bad experiences, criticize organizations for political or social reasons, or simply bash brands they don't like. Brands that don't respect this new balance of power risk lasting damage to their reputation.

Consumers can be much more outspoken when they're commenting from behind a keyboard (or mobile phone). The sentiment surrounding a brand online is a major indicator of the health of the brand, and organizations need to keep a pulse on this metric as they launch new campaigns, make social and political statements, or approach new markets.

An often overlooked reason to protect the brand—especially online—is the threat of cybercrime. Where brands create value, there is an opportunity to exploit that value for a quick buck. Scammers imitate brands or support agents to coerce buyers into disclosing credit card information or sending money. Crimes like these erode brand reputation, and organizations must take an active stance in protecting both their brand and their customers.

Negative consumer sentiment, cybercrime, and a number of other factors combine to make protecting the brand essential in the age of social media. To protect your brand effectively, you need to understand the risks, prioritize them based on the threat they pose to your organization, and develop an action plan.

Risks to a brand

The first step in developing a brand protection plan is understanding the nature of the risks brands face on social media.

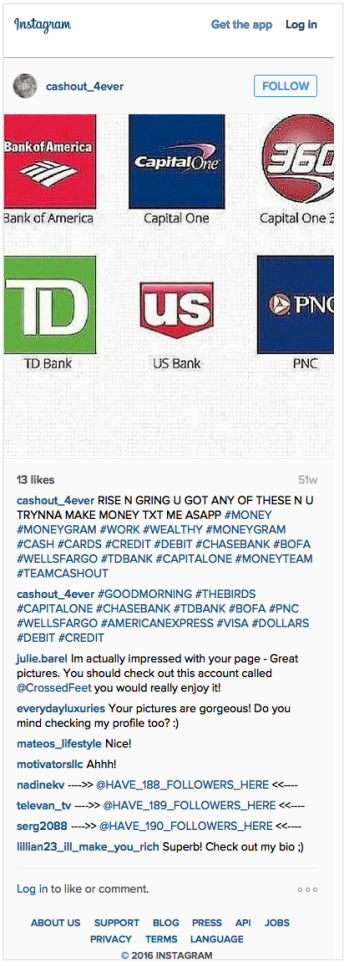
The types of risk you'll face vary from industry to industry. The following list describes the most common threats to brands on social media.

Negative sentiment

Sentiment is the overall attitude of the conversations surrounding a topic or brand. If it's negative, it can have lasting and damaging effects that are difficult to address.

Scams

Scams are attempts by criminals to fool customers into believing they are interacting with your organization, only to steal or extort data or money.



Financial scammers post on social networks, hoping to extort data and money.

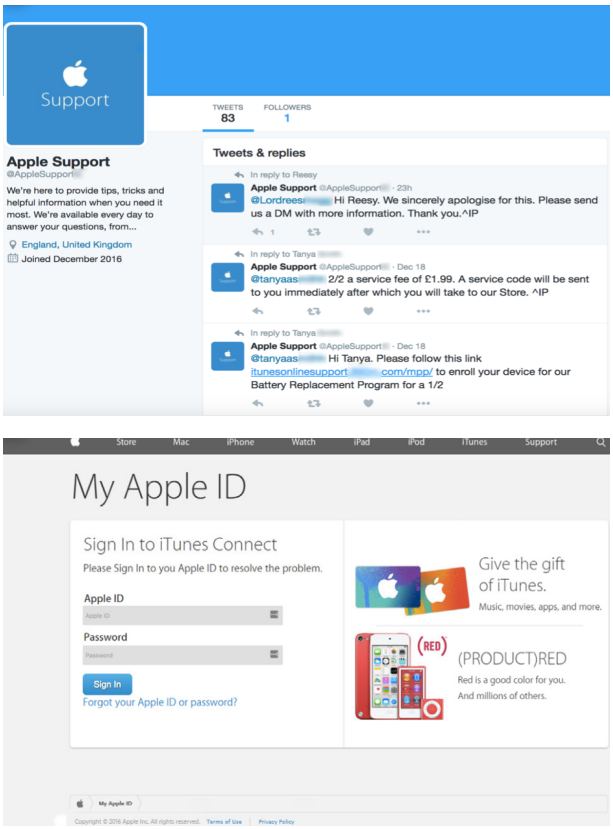
Account hijacking

Account hijacking involves breaking into a social account to post malicious, slanderous, or embarrassing content.

A hijacked account can damage your brand and compromise the security of your customers' data.

Fraudulent accounts

Fraudulent accounts are any fake account masquerading as the brand or an official representative of a brand, such as a customer support agent—usually with the intent of scamming customers or initiating cyberattacks.



Fraudulent websites and social accounts can be difficult for consumers to identify.

Offensive content

Offensive content can be any inbound content posted by an outside source to owned pages that violates brand or community guidelines around profanity, pornography, racism, violence, and so on. This might include a disgruntled follower or troll posting racial slurs on a Facebook page, a scam posted in a YouTube comments, or a customer unwittingly disclosing personally identifiable information (PII) on LinkedIn.

Cyberattacks

Cyberattacks are malicious activity intended to breach the security of corporate network, compromise customer or employee data, or otherwise access and use private company data and resources by digital means.

Cybercriminals share misleading content in an attempt to get targets to click unsafe links.

Employee risks

Employee risks are a class of risks resulting from a company's employees publicly posting offensive, noncompliant, sensitive, or slanderous content.

Compliance violations

Compliance violations occur on social media when a company representative violates regulatory requirements (for example, by posting confidential patient information or customer credit card numbers).

The benefits of brand protection

Depending on your industry, the size of your organization, and the extent to which you are already active on social media, brand protection can bring a number of distinct benefits.

Improve reputation
Protecting the brand enables your reputation to grow while minimizing risk, allowing your marketing team to reap all the benefits of digital and social media marketing. A customer base that is not being targeted by scammers and has never witnessed a PR fiasco following the hacking of a brand account is much more likely to follow, engage with, and ultimate purchase from an organization.

On social media, threats to the brand play out in the public sphere. As such, brand protection programs have the dual benefit of not only mitigating the direct, immediate cost of risk, but reducing the reputational fallout that occurs as your customers witness the entire process. Consumers almost universally check review sites and other aggregators before buying; in a world where direct, public customer feedback is a given, maintaining a good reputation has never been more crucial.

Protect brand investment and increase social ROI
Organic and paid social media campaigns continue to play a greater role in marketing and sales revenue channels, and businesses' spend on social media is increasing. Businesses that invest in empowering both the owners of the corporate accounts and individual employees in revenue-driving roles (like sales representatives, support staff, and customer success or partner managers) often see a significant return on investment. A brand protection program safeguards this tangible and valuable line of revenue for the business.

Prevent and mitigate external compliance violations
Risk can come from the inside as well. By identifying and dealing with noncompliant posts immediately—whether on official brand accounts or employees' accounts—legal and compliance professionals can mitigate costly violations before they result in crises.

Grow community and engagement
Your community is your greatest asset on social media. Protecting and fostering this community is a key way to ensure your social ecosystem remains a profitable and growing business asset.

Customers who have a positive experience with the brand online are far more likely to engage again in the future. Having a firm, appropriate policy in place for all staff that use social channels to engage with customers and prospects is a must.

Protect customers
One of the easiest and most lucrative ways to exploit a brand is to go directly after customers. Scammers regularly impersonate brands to commit fraud, identity theft, and other crimes.

Ensure internal policy adherence
Marketing, customer success and support professionals all need firm, centralized guidelines established by the company to ensure nothing goes amiss while interacting online.

The current state of brand protection

Many organizations have spent the past half decade coming to terms with the effects of internet connectivity on their ability to assess and mitigate brand risk. Social media simultaneously simplifies and complicates this challenge: now a brand's health can be measured by sentiment, and buyers provide feedback in real time on a public platform, but at the same time, the challenges of collecting data at scale, identifying scams, and assessing and managing risk have never been more difficult.

In the past two years, fraudulent brand accounts—just one of many social media risks—have increased more than tenfold. As the risk grows, so must investment in brand protection.

Although assessing general sentiment about a company, hashtag, or topic on social media is a well-established practice, few brand protection programs drill down to the level of individual posts or remediate more dangerous risks like fraudulent brand accounts, compliance violations, and phishing attacks on their customers.

Account hijacking is becoming an increasingly popular type of cyberattack. In response to this threat, marketing teams have started using additional security measures such as two-factor authentication to harden their accounts. This is an excellent step in the right direction, but needs to be coupled with more comprehensive processes for identifying and dealing with hijacked accounts. The New York Post reports that 160,000 Facebook accounts are hijacked daily.

Of course, brand protection goes beyond social media. Organizations need to continue monitoring for fake websites, domain squatters, malicious posts on review sites, and other digital threats to brands. The broad scope of all the places that a modern brand lives further complicates the challenge of protecting it.

Building a brand protection program

Once you've determined that it's time for your organization to begin developing a brand protection program for social media, there are three main steps to get started:

Step 1: Identify program stakeholders

Step 2: Equip your team with the right tools

Step 3: Design and implement your brand protection program

Step 1: Identify program stakeholders

Getting the right people to the table is fundamental for a successful brand protection program. While marketing generally leads a brand protection program, there are stakeholders from several departments who need to be on call for risks as they arise. The group should meet regularly, either monthly or quarterly, to review the health of the brand, trends, goals, and priorities.

Depending on the organization's size, industry, structure, and social media usage, the composition of the brand protection group will vary. Certain industries face challenges that require different stakeholders.

In general, all brand protection programs require a marketing lead for day-to-day maintenance, a marketing executive to help facilitate the program, public relations experts, and interdepartmental stakeholders to handle and advise on specific types of risk. Of these stakeholders, information security and fraud can expect to be the most involved, although this may vary based on industry and use case.

Marketing Champion

- **Primary role:** Daily maintenance of program; primary driver of regular recaps; consistent communication to other stakeholders; work with security teams to harden accounts; work with governance, risk management, and compliance (GRC) to establish corporate posting policies; issue takedowns of malicious content or profiles in violation of networks' terms of service.
- **Level of effort:** High
- **Frequency of activity:** Daily

Marketing Executive

- **Primary role:** Regular check-ins with the marketing champion; gatekeeper to raising issues with outside stakeholders or executive team; overarching decision-making power for the program at large; help establish corporate posting policies.
- **Level of effort:** Medium–High
- **Frequency of activity:** Weekly, or as needed

Public Relations

- **Primary role:** Help draft crisis plan; handle press during a crisis; manage all press-related inquiries; assist in any public-facing risk mitigation.
- **Level of effort:** Medium–High
- **Frequency of activity:** Weekly, or as needed

Customer Success

- **Primary role:** Establish a policy for dealing with customer feedback and reviews; train employees on brand protection; engage with customers on social media; issue takedowns of malicious content or profiles in violation of networks' terms of service.
- **Level of effort:** High
- **Frequency of activity:** Daily

Fraud

- **Primary role:** Take lead on issues involving fraudulent accounts or attacks against customers.
- **Level of effort:** Low–Medium
- **Frequency of activity:** Biweekly, or as needed

Information Security

- **Primary role:** Take lead on issues involving cyberattacks, phishing, malware, and data loss; work closely with marketing to harden accounts against these potential risks.
- **Level of effort:** Medium
- **Frequency of activity:** Biweekly, or as needed

Governance, Risk, and Compliance

- **Primary role:** Take lead on malicious or noncompliant posts and other risks to the business.
- **Level of effort:** Low–Medium
- **Frequency of activity:** Monthly, or as needed

Corporate Security

- **Primary role:** Take lead on issues involving the physical security of the company's people or locations.
- **Level of effort:** Low–Medium
- **Frequency of activity:** Monthly, or as needed

Legal

- **Primary role:** Take lead on risks with legal implications and work with compliance to mitigate regulatory violations.
- **Level of effort:** Low–Medium
- **Frequency of activity:** Monthly, or as needed

Step 2: Equip your team with the right tools

Effective brand protection programs are typically built on a suite of three core platforms for social media management, listening, and risk management.

Platform	Example	What it does
Social media management	Hootsuite	Gives your organization a platform to manage all social media activity in one place, improving productivity, compliance, and return on investment in social
Social media listening	Hootsuite Insights Brandwatch, Talkwalker	Enables you to listen to social conversations about your brand, products, and campaigns across social networks.
Social media risk management	ZeroFOX	Helps you detect and remediate threats and security risks to your business on social, mobile, web, and collaboration platforms

Risk management and listening tools address some of the same issues. If you're a smaller organization or just starting out, invest in social media management and risk management tools first. Listening tools are best for larger organizations with enough social media activity to warrant distillation and analysis.

Most importantly, brand protection programs require buy-in across many departments. This can often be the most difficult hurdle in getting your brand protection program started. Work with executive marketing staff to start the conversation and get the program funded and prioritized.

Step 3: Design and implement your brand protection program

With an understanding of the risks your organization faces and the tools and platforms that are available, you're ready to begin designing and implementing your brand protection program.

1. Assemble a task force

Expect the kickoff meeting to be a lengthy, in-depth conversation. Marketing should plan to begin educating stakeholders about the purpose of a brand protection program before exploring possible goals and responsibilities. The key deliverable for this meeting is documented processes and policies.

2. Assess and prioritize risks

Depending on your industry, the size of your organization, and your current presence on social media, the frequency and severity of the risks you face will vary.

The organization's active social media users (typically marketing and customer success) should come prepared with information and examples of known risks. For a full risk profile of the organization, work with a brand protection or social media risk management vendor to create an initial assessment.

Most brand protection task forces assess the risk to the organization based on frequency of risks and severity of risks. Account hijacking, for instance, has a low frequency but an incredibly high severity. Assigning some comparative qualifications for risk allows for prioritization of risk.

Other organizations, especially those with more resources or more robust risk management protocols, can assess desired risk levels, existing risk levels, and methods of harmonizing the two. The more rigorous the approach, the better the company will be able to implement efficient, economical tools and policies to protect the brand adequately.

3. Decide on roles and responsibilities

At the initial meeting, the main objective is to collectively agree on roles and responsibilities. This entails identifying what risks to the brand exist, which are worth addressing, and which are the most urgent.

Based on this prioritization, it should become clear clear which stakeholder is tasked with identification and remediation. For instance, identifying customers leaking PII or credit card information may be the responsibility of the customer success team, but it will be up to to fraud and legal to remediate the leak.

4. Establish processes and policies

The core initial deliverable for a brand protection task force is documented processes and policies.

- **Processes** describe workflows for each risk, stakeholder engagement, remediation and takedown, and review.
- **Policies** provide guidelines for key stakeholders and for active social media users at the company. They also lay out game plans for executive social media usage, training programs, and regulatory guidelines where applicable.

5. Train relevant staff

A critical component of a brand protection program is training for relevant staff on policies defined by the brand protection task force.

This is especially critical for marketing and support staff who actively engage with prospects or customers. Ensuring that your support staff is engaging appropriately can be the difference between return customers or a social media catastrophe. Be sure to establish a process, update it regularly, and develop an enforcement mechanism to ensure it's being upheld effectively.

6. Monitor and address risk

This phase is the continuous enforcement of the policies and procedures. Active social media practitioners within the organization—generally marketing and customer success—should use social media management, listening, and risk management tools to identify risks, assess sentiment, and manage risks accordingly.

The speed and efficiency of monitoring and damage control are critical, as risks can go viral in minutes. Stopping the bleeding as quickly as possible is crucial. Brand protection tools need to be set up in accordance with the priorities laid out in the initial meeting and deployed to the correct stakeholders. Content in violation of a social network's terms of service can be flagged for removal.

7. Schedule recurring check-ins

Schedule regular monthly or quarterly check-ins. At these meetings, review trends, discuss wins/losses, and update goals based on feedback.

8. Report and review

Establish a framework for metrics and reporting to be circulated to stakeholders at a consistent cadence. Work with your social media management, listening, and risk management vendors on analytics and reporting. These metrics will guide the review process and should show where progress is being made, where is it not, and gaps in the program.

Conclusion

Brand protection matters. Social media is the latest tool in the evolution of the brand, and as such, represents a key component of a brand protection program. Expect nearly all negative feedback and digital risks to ultimately manifest themselves on social media. However, don't forget the other digital channels and ways in which the brand might be harmed.

According to Forrester, organizations that create brand value through social media reputation have vastly outperformed the market (growing 103% in market value vs. 63% for the S&P 500 and 30.3% for the MSCI World Index) since the launch of Facebook in 2004. The best time to start a brand protection program would have been then. The second best time is now.

About Hootsuite

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 100. 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.

About ZeroFOX

ZeroFOX, the innovator of social media & digital security, protects modern organizations from dynamic security, brand and physical risks across social, mobile, web and collaboration platforms. Using targeted data collection and artificial intelligence-based analysis, ZeroFOX protects modern organizations from targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, executive and location threats and more.

Recognized as a Leader in Digital Risk Monitoring by Forrester, the patented ZeroFOX SaaS platform processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Twitter, HipChat, Instagram, Reddit, Pastebin, Tumblr, YouTube, mobile app stores, the deep & dark web, domains and more. Led by a team of information security and high-growth company veterans, ZeroFOX has raised nearly $100M in funding from NEA, Highland Capital, Silver Lake Waterman, Redline Capital and others, and has collected top industry awards such as Red Herring North America Top 100, the SINET16 Champion, Dark Reading's Top Security Startups to Watch, Tech Council of Maryland's Technology Company of the Year and the Security Tech Trailblazer of the Year.

To learn more about protecting your brand on social–and how Hootsuite and ZeroFOX can help–contact sales@hootsuite.com.