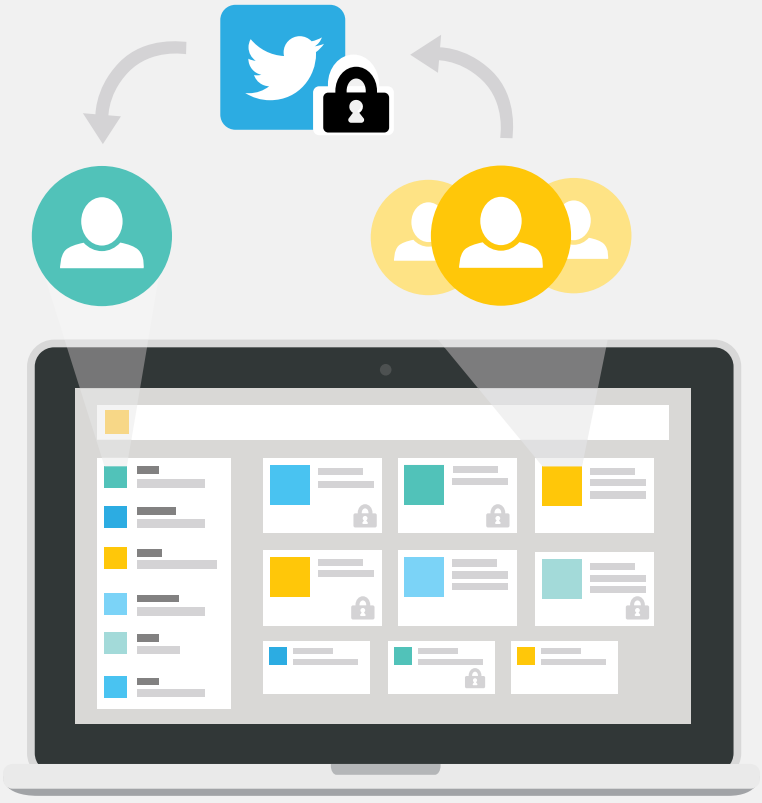
GUIDA

# Come proteggere il tuo brand sui social media

## Le strategie per prevenire le principali minacce sui social per i brand



Hootsuite®

# Come proteggere il tuo brand sui social media

Le strategie per prevenire le principali minacce sui social per i brand

# Indice


1. Introduzione ..... 3
2. Perché dovresti proteggere il tuo brand sui social media? ..... 4
3. I rischi e le minacce più comuni sui social media ..... 5
4. Strategie per proteggere il tuo brand sui social media ..... 7
5. Come gestire una crisi sui social media ..... 10
6. Pensare al futuro: investi sulla sicurezza dei social media ..... 12


# Introduzione

## L’incredibile opportunità rappresentata dai social media non è priva di rischi: i brand devono infatti fare i conti con una presenza continua e sempre attiva sui social.

Questo però non significa che si deve rinunciare a essere presenti sui social. Anzi, non essere prontamente reattivi può risultare ancora più controproducente, come ha imparato a proprie spese la Lockheed Martin, quando il presidente Donald Trump con un solo tweet ha fatto crollare le sue azioni di 4 miliardi di dollari.

Con la giusta strategia, il tuo brand può essere attivo sui social media senza incappare in eventi che possano danneggiarlo. Ecco perché l’81% dei dirigenti oggi considera la protezione del brand una priorità assoluta.

Questa guida rappresenta una panoramica completa di tutto quello che devi sapere per proteggere il tuo brand online:

- Perché la sicurezza dei social media è importante per i brand
- Quali sono i rischi e le minacce più comuni e come affrontarli
- Come comportarsi di fronte a una crisi sui social media
- Come programmare il futuro minimizzando i rischi

## Perché dovresti proteggere il tuo brand sui social media?

Se da un lato è fondamentale essere presenti sui social media, per i brand è altrettanto importante non perdere mai di vista la sicurezza.

Le minacce alla sicurezza sui social media continuano a diventare più preoccupanti di anno in anno. Nel 2016, le truffe sono aumentate del 150% su Twitter, Facebook e LinkedIn. E quanto emerge dal 2017 Quarterly Threat Report di Proofpoint dimostra che gli attacchi sui social si fanno sempre più vari e sofisticati.

Questo aumento delle minacce alla sicurezza sui social media è direttamente proporzionale al tempo che trascorriamo online. Come riportato nel Cyber Security Insights Report 2016 di Norton, ogni anno la necessità di essere "sempre connessi" espone milioni di persone a violazioni della sicurezza, con un costo di diversi miliardi di dollari. Nel 2016, 689 milioni di utenti sono stati vittime di crimini informatici: il 10% in più rispetto al 2015.

Anche se sono gli attacchi informatici e gli hacker a fare più notizia, in genere i rischi maggiori derivano da negligenze ed errori umani interni alle organizzazioni, spesso legati a una formazione inadeguata sui protocolli e le minacce dei social media.

Ecco perché è importante identificare i rischi e implementare un piano di protezione del brand sui social media. Come suggerito dalla Planning Guide for Security and Risk Management 2016 di Gartner, "l'emergere dell'Internet of things ha fatto aumentare l'importanza della sicurezza e della gestione del rischio.

**Le conseguenze di un'inadeguata protezione sui social media**

- **Indebolimento della fiducia nei confronti del brand:** una violazione della sicurezza può avere un effetto molto negativo sul brand. Secondo uno studio di FireEye Inc., il 36% degli intervistati ha dichiarato che la loro percezione di un determinato brand era peggiorata dopo che questo aveva sperimentato problemi di sicurezza. Inoltre, un terzo degli intervistati ha affermato di avere ora un'opinione negativa sul brand.
- **Danni economici:** i costi di un problema di sicurezza o di un errore sui social media possono essere astronomici. Ogni anno si spendono miliardi di dollari per far fronte alle violazioni informatiche e alle crisi nelle comunicazioni.
- **Diminuzione del ROI:** ogni evento che danneggia il brand sui social media va a influire sugli investimenti effettuati in quel campo, soprattutto quando ci si ritrova a dover spendere denaro per limitare i danni.

**Il rischio maggiore è rimanere inerti**

Come sottolineato dall'esperta in materia di conformità Joanna Belbey, i rischio maggiore per un'organizzazione è non fare niente.

Se non si implementano procedure, strumenti e programmi formativi per mantenere protetto il proprio brand, si finisce per essere molto più vulnerabili a rischi e minacce. Conoscere e gestire le minacce più comuni, invece, consente di occuparsi dei propri account social in tutta sicurezza.

## I rischi e le minacce più comuni sui social media

La tua azienda potrebbe essere soggetta a centinaia di minacce online, ma in genere i rischi dei social media sono ascrivibili a sei grandi categorie che è importante tenere presente.

### 1. Account trascurati

Se la tua azienda possiede degli account sui social media, ma non li controlla attivamente e non risponde alle conversazioni, il rischio è che la tua pagina venga invasa da spam, o da reclami e segnalazioni di problemi rimasti senza risposta, cosa che può risultare estremamente dannosa per la tua immagine.

A prescindere dal livello di attività sui social, gli utenti cercheranno sempre di interagire con un brand. Quando un cliente pone una domanda sui social, si aspetta una risposta nel giro di poche ore e l'82% dei clienti afferma che una risposta in tempi brevi è fondamentale per un'esperienza positiva con un'azienda.

### 2. Errore umano

Ogni volta che una procedura di sicurezza fallisce, si tende a cercare una spiegazione in eventuali falle nei sistemi. In realtà, però, spesso i veri responsabili sono gli utenti stessi.

Caricare l'immagine sbagliata per un post sui social, condividere informazioni dall'account sbagliato o comunicare accidentalmente dati sensibili sono tutti errori umani.

Secondo il Forbes Insights Report, l'errore umano è la minaccia che ha il maggiore impatto a livello economico: di fatto, è il fattore scatenante di un terzo dei disservizi informatici. Se non si dispone di strumenti e procedure per rimediare prontamente, si rischia che un solo errore abbia conseguenze disastrose per il brand.

Per esempio, un banale errore di copia e incolla sull'account Twitter di U.S. Airlines si è trasformato in uno degli sbagli più madornali di tutti i tempi: nel rispondere al reclamo di un cliente, hanno accidentalmente inserito nel tweet un link pornografico. Con un sistema di approvazione adeguato, un incidente del genere non si sarebbe mai verificato.

### 3. Violazioni delle norme di conformità

Una violazione di conformità si verifica quando non si rispetta una regola stabilita dall'azienda o da un ente normativo. Secondo un report di Proofpoint, esistono oltre 12 enti normativi (tra cui FINRA, FTC, FDA e SEC) che hanno che le aziende possono o non possono fare sui social media.

Come menzionato nel report di Proofpoint The State of Social Media Infrastructure, "gli organi regolatori riconoscono i social media come un canale di comunicazione pubblica, soggetto alle normative sulla trasparenza delle entrate, la veridicità degli annunci pubblicitari e la riservatezza dei dati. Tali requisiti sono stati concepiti per evitare che i consumatori possano essere indotti in errore o soggetti a frode".

Il tuo team deve capire in cosa consistono queste norme e come influiscono sulla tua attività sui social. Senza una procedura di approvazione che protegga le interazioni sui social media e ne individui le eventuali violazioni, si rischia di essere esposti lunghe indagini e multe salate.

Scopri come Spectrum Health è riuscita a mantenere la conformità sui social media anche con 23.000 dipendenti

## 4. Phishing

Il phishing è un tipo di truffa tramite cui i criminali informatici riescono a sottrarre dati sensibili come quelli sui conti bancari. I social media sono un terreno fertile per questo genere di frode, che di fatto nell'ultimo anno ha fatto registrare un aumento del 150%.

Una delle modalità di phishing più comuni sui social media è la creazione di un account fake per l'assistenza clienti, progettato per spingere gli utenti a cliccare su un link fraudolento e inserire i loro dati bancari. Un tweet al profilo del tuo brand, per esempio, potrebbe venire intercettato e il mittente potrebbe vedersi arrivare una risposta con un link in cui gli si chiede di inserire i suoi dati personali.

## 5. Account violati

Un account viene hackerato quando un criminale informatico riesce a prenderne il controllo, mandando messaggi negativi, inappropriati o comunque contrari ai valori del brand.

La violazione dell'account di un brand è un vero incubo per gli addetti alle pubbliche relazioni e può rivelarsi estremamente dispendiosa, perché i clienti reagiscono in modo rapido e inesorabile. Secondo un report di ZeroFOX, la violazione dell'account social del giocatore della NFL Laremy Tunsil, nel 2016, ha causato circa 21 milioni di dollari di danni.

Gli account hackerati sono un problema piuttosto comune, soprattutto per i grandi brand, come ha potuto sperimentare McDonald's quando un hacker ha utilizzato il suo account Twitter per pubblicare commenti sulla politica statunitense.

## 6. Malware

I malware (o "software dannosi") sono progettati per accedere ai sistemi e ai dati del tuo computer tramite codice. La violazione può portare alla perdita temporanea o permanente dei dati di proprietà del tuo brand.

I ransomware - malware che bloccano o codificano i dati del tuo computer, solitamente impedendoti di accedere finché non paghi un "riscatto" richiesto dai criminali informatici—sono un altro tipo di attacco sempre più comune. Secondo un report del Dipartimento di Giustizia degli Stati Uniti, nel 2016 ci sono stati più di 4000 attacchi ransomware al giorno, con un aumento del 300% rispetto al 2015.

## Strategie per proteggere il tuo brand sui social media

Facendo comprendere i rischi che l'azienda si trova ad affrontare sui social media, puoi preparare al meglio i tuoi team per l'implementazione di strategie di sicurezza.

Le sei strategie illustrate di seguito aiutano a ridurre il rischio di errori umani, oltre che a identificare e contenere i potenziali problemi prima che diventino incontrollabili.

### 1. Identificare e rimuovere gli account social abbandonati

Se non sei sicuro di quali account social siano legati al tuo brand e di come vengano percepiti dal pubblico, sappi che l'immagine del tuo brand sta già correndo un grosso rischio.

Identificare e chiudere gli account che non aggiungono valore alla tua attività sono azioni che contribuiscono a creare una voce del brand più coerente su tutti i canali social. Per fare un esempio, il colosso alberghiero e di ristorazione Delaware North ha unificato la propria presenza sui social identificando ed eliminando più di 40 account non legittimi. Grazie a un semplice inventario, sono riusciti a rimuovere i profili inattivi o di basso valore, concentrando i propri investimenti su quelli più redditizi.

### 2. Aggiornare i criteri di creazione delle password

I criteri di creazione delle password sono un aspetto importante e spesso sottovalutato nella protezione di un brand. Impostare un certo tipo di criteri per la creazione delle password fa sì che sia più difficile hackerare gli account e spacciarsi per la voce ufficiale del brand.

I criteri dovrebbero applicarsi a chiunque utilizzi gli account social aziendali e dovrebbero includere i seguenti requisiti minimi:

- **Password complesse:** ogni password dovrebbe avere una lunghezza compresa tra gli 8 e i 20 caratteri e includere lettere maiuscole, minuscole e simboli.
- **Autenticazione a due fattori:** un sistema di autenticazione a due fattori consente di aggiungere un secondo livello di autenticazione all'accesso. Per esempio, dopo aver effettuato l'accesso con la password si potrebbe dover inserire un codice numerico inviato sul proprio cellulare. In questo modo si aggiunge un livello di protezione in più all'accesso.
- **SSO:** la SSO, o autenticazione singola, riduce la quantità di password utilizzate, consentendoti di accedere a sistemi diversi utilizzando un solo set di credenziali. In questo modo si può accedere a Hootsuite con il nome utente e la password usati per l'account di posta elettronica aziendale, così da avere meno credenziali da tenere a mente e proteggere.

Le password andrebbero aggiornate regolarmente e gestite da un solo amministratore o gruppo all'interno dell'organizzazione. L'accesso a questi dati va limitato il più possibile per far sì che le informazioni rimangano confidenziali.

## 3. Creare una policy per i social media

Per ridurre i rischi legati alla sicurezza e garantire un atteggiamento coerente in tutta l'azienda, sarebbe opportuno provvedere alla creazione di una policy aziendale per i social media.

In questo modo, sarà possibile stabilire una serie di protocolli e processi da seguire su tutti i canali del brand, oltre ad attribuire ai propri dipendenti la responsabilità di proteggere il brand da azioni fraudolente.

Anche se le policy per i social media variano da un'azienda all'altra, ogni policy dovrebbe focalizzarsi comunque sull'importanza della sicurezza del brand, la sua reputazione e i suoi valori.

**Di seguito, riportiamo alcuni punti fondamentali per una policy efficace:**

- Linee guida e best practice per il brand
- Ruoli e responsabilità per i social media
- Esempi di comportamenti appropriati o meno
- Conseguenze dell'uso improprio dei social media
- Procedure e protocolli di sicurezza
- Leggi e norme applicabili al settore

Aggiorna regolarmente la tua policy in modo che rispecchi i cambiamenti della tua azienda sui social media. L'ideale sarebbe trattarla come un documento "vivo", come quello della Cambridge University, che aiuta i dipendenti a sentirsi più a loro agio nell'interagire con i contenuti pubblicati.

## 4. Formare i propri dipendenti

La nuova pratica del BYOD (Bring Your Own Device), che consente l'utilizzo dei dispositivi personali da parte dei dipendenti, ha fatto aumentare notevolmente i rischi per la sicurezza. Ecco perché tutti i dipendenti dovrebbero ricevere una formazione base sui social media, anche se non hanno accesso agli account aziendali.

Senza una formazione e un addestramento adeguati, far applicare le policy aziendali in tutti i dipartimenti risulterà molto più difficile.

Una buona formazione per i dipendenti dovrebbe includere:

- Best practice e uso adeguato dei social media
- Una panoramica sulla policy aziendale sui social media
- Un elenco dei rischi più comuni a cui ci si espone utilizzando i social media
- Come rispettare le linee guida aziendali riducendo i rischi

Scopri come offrire una formazione adeguata ai tuoi dipendenti con il nostro corso di Hootsuite Academy.

Ulteriori informazioni nella nostra guida alla creazione di una policy per i social media.

## 5. Impostare un sistema gerarchico di approvazioni per i contenuti sui social media

Tutti gli account social del brand andrebbero protetti con un sistema di approvazioni ben definito, per essere sicuri che niente possa essere pubblicato senza l'assenso del personale autorizzato. In questo modo, il rischio di errori umani si riduce in modo significativo.

Tramite Hootsuite, è possibile impostare un doppio sistema di approvazioni con autorizzazioni e ruoli per ogni singolo dipendente. In questo modo, si può decidere a chi permettere di accedere a tutti i contenuti social, pubblicare contenuti, inviare bozze per l'approvazione o visualizzare i post in modalità di sola lettura. Con app o integrazioni di terzi come Brandwatch, inoltre, è possibile impostare un sistema che contrassegna contenuti potenzialmente sensibili e ne blocca la pubblicazione.

## 6. Fare Social Listening

Il Social Listening è una pratica di monitoraggio che può essere utilizzata per seguire le conversazioni sui social riguardanti il tuo brand. Oltre a essere un ottimo modo per individuare potenziali clienti e opportunità, è una parte fondamentale della protezione del brand sui social.

Il Social Listening ti consente di rispondere a reclami e lamentele, contrastare brand sentiment negativo e gestire lo spam prima che diventi un problema.

**Con il tuo software di gestione dei social media è possibile impostare stream o notifiche per seguire le conversazioni che includono i seguenti elementi:**

- **Nome dell'azienda (inclusi gli errori ortografici più comuni):** inizia a seguire le menzioni dirette del tuo brand e i clienti che cercano di contattarti direttamente. In questo modo potrai misurare il sentiment e risolvere i problemi più immediati. Non dimenticare di includere le variazioni più comuni sul nome della tua azienda (es. Coca-Cola includerà anche Coca Cola, Coke, Cola e simili).
- **Parole chiave e hashtag del settore:** monitorare gli hashtag e i termini specifici di un dato settore consente di essere più coinvolti nelle conversazioni più popolari nel proprio ambito. Per esempio, se c'è una discussione sul ritiro di un prodotto da parte di un brand concorrente, gli utenti potrebbero chiedersi se anche i tuoi prodotti abbiano problemi analoghi e se sia il caso di passare a qualcosa di diverso. Seguendo conversazioni esterne alla cerchia ristretta del proprio brand, quindi, è possibile individuare problemi, presentare dati e aumentare la fiducia della propria community.
- **Parole chiave e hashtag delle campagne:** tenere sotto controllo le parole chiave delle tue campagne pubblicitarie è molto importante per capire in che modo interagire con gli utenti. Per fare un esempio, la campagna Real Beauty Bottles di Dove è diventata rapidamente oggetto di commenti negativi sui social. Molti dei tweet in risposta alla pubblicità della Dove (riportati anche in diversi articoli), non hanno mai ottenuto risposta dall'azienda. Se non si seguono le parole chiave e gli hashtag legati al brand, si rischia di perdere il controllo su conversazioni rilevanti, con forti ripercussioni sulla reputazione aziendale.
- **Sentiment:** utilizzare strumenti per l'analisi del sentiment sui social media consente di tenere sotto controllo la percezione del brand in tutto il mondo, in lingue diverse. In questo modo puoi ottenere un feedback in tempo reale e regolare i tuoi messaggi di conseguenza.

Ulteriori informazioni su come monitorare i social media nella nostra Guida.

## Come gestire una crisi sui social media

Un tweet pubblicato su un canale ufficiale nel momento sbagliato, il post di un cliente arrabbiato o il video di un errore madornale che improvvisamente diventa virale, sono tutti esempi di eventi negativi che possono finire rapidamente fuori controllo sui social media. Per essere sempre pronti ad affrontare la soluzione al meglio, è bene preparare un piano di crisis management.

In questo modo, potrai minimizzare i rischi assegnando in anticipo ruoli, responsabilità, protocolli e tipologia di messaggi, da essere già pronto in caso di emergenza.

Un buon piano di crisis management sui social media dovrebbe includere i seguenti punti chiave:

### 1. Protocollo di monitoraggio dei social

Tenere sotto controllo le menzioni negative del brand ti consente di affrontare eventuali problemi tempestivamente, prima che si trasformino in vere e proprie crisi. Il protocollo dovrebbe specificare cosa viene monitorato, chi ne è responsabile e come deve occuparsi delle problematiche più comuni o prevedibili.

### 2. Ruoli e responsabilità

Per agire rapidamente in caso di crisi, dovrai preparare un elenco di decisori chiave, con ruoli e responsabilità ben delineati. Queste persone saranno autorizzate a inviare comunicazioni esterne a nome dell'azienda: per esempio, potresti identificare un contatto chiave che approvi tutti i messaggi social diretti ai mass media, inserendo anche un contatto secondario nei casi in cui il primo non sia disponibile.

### 3. Potenziali scenari ed esempi

Per preparare al meglio i tuoi dipendenti per affrontare una crisi, puoi inserire nel piano esempi concreti di possibili problemi, insieme alle istruzioni su come affrontarli.

Le sessioni di training e gli esercizi di simulazione sono un ottimo modo per aiutare i tuoi dipendenti a capire quali rischi si può trovare ad affrontare l'azienda e come è bene rispondere. Inoltre, consentono di avere un'idea più realistica delle tempistiche necessarie per reagire, e di identificare eventuali falle o mancanze del piano.

## 4. Messaggi pre-approvati

I responsabili del team social dovrebbero lavorare insieme al team delle pubbliche relazioni per sviluppare dei messaggi predefiniti da utilizzare in ognuno degli scenari previsti.

Il documento contenente questi messaggi dovrebbe essere sempre a disposizione del team social e specificare in maniera evidente le autorizzazioni delle parti interessate.

**Un piano di crisis management dovrebbe consentire di:**

- **Agire rapidamente:** le azioni rapide ed efficaci possono fare davvero la differenza nella gestione di una crisi sui social media. Come sottolineato dall'esperto di crisis management Duncan Gallagher, il 28% delle crisi si diffonde a livello internazionale già nel giro di un'ora, ma in media ce ne vogliono 21 perché le aziende riescano a controbattere. Questo è un primo aspetto su cui si potrebbe migliorare notevolmente.
- **Essere trasparenti:** nel discutere un problema sui social, è bene essere aperti e onesti con i propri clienti. Se possibile, è bene portare la discussione offline, ma se si è arrivati a un punto in cui non è più possibile, bisogna affrontare la questione pubblicamente, fornendo quante più informazioni possibile nei limiti della legalità.
- **Comunicare internamente:** nel corso di una crisi, i dipendenti vanno aggiornati con regolarità su quanto sta succedendo e su come rispondere a eventuali domande provenienti dal pubblico. Comunicare queste informazioni a livello dell'intera organizzazione consente di ridurre i rischi di avere del personale disinformato o di diffondere informazioni errate.
- **Alimentare la fiducia:** una crisi può anche essere una buona occasione per alimentare la fiducia della propria comunità di riferimento. Quando la provincia di Morris è stata colpita dall'uragano Sandy, per esempio, il comune ha usato i propri account social per avvertire i cittadini e diffondere dati precisi e affidabili, salvando delle vite e limitando ulteriori danni.

## Verifica e rivedi il tuo piano dopo ogni crisi

Una volta che le acque si sono calmate, dopo una crisi, è bene riunire i membri dei team coinvolti e verificare cosa ha funzionato e cosa invece si può migliorare. In questo modo, sarà possibile capire su quali parti del piano di crisis management è ancora necessario lavorare.

### Ulteriori risorse sul crisis management

- Guida al crisis management sui social media
- Webinar sulla gestione di una crisi sui social
- Corso di Academy sulla preparazione alle crisi

## Pensare al futuro: investi sulla sicurezza dei social media

Ogni anno, le aziende spendono miliardi di dollari per rispondere a problemi di sicurezza online. Senza le procedure e gli strumenti adeguati, aumentano i rischi di incidenti a danno dei brand, che possono avere effetti a lungo termine.

Rendere la protezione del brand una priorità anche sui propri account social consente di prevenire comportamenti rischiosi, minimizzare i costi degli incidenti e intervenire tempestivamente nei momenti di crisi.

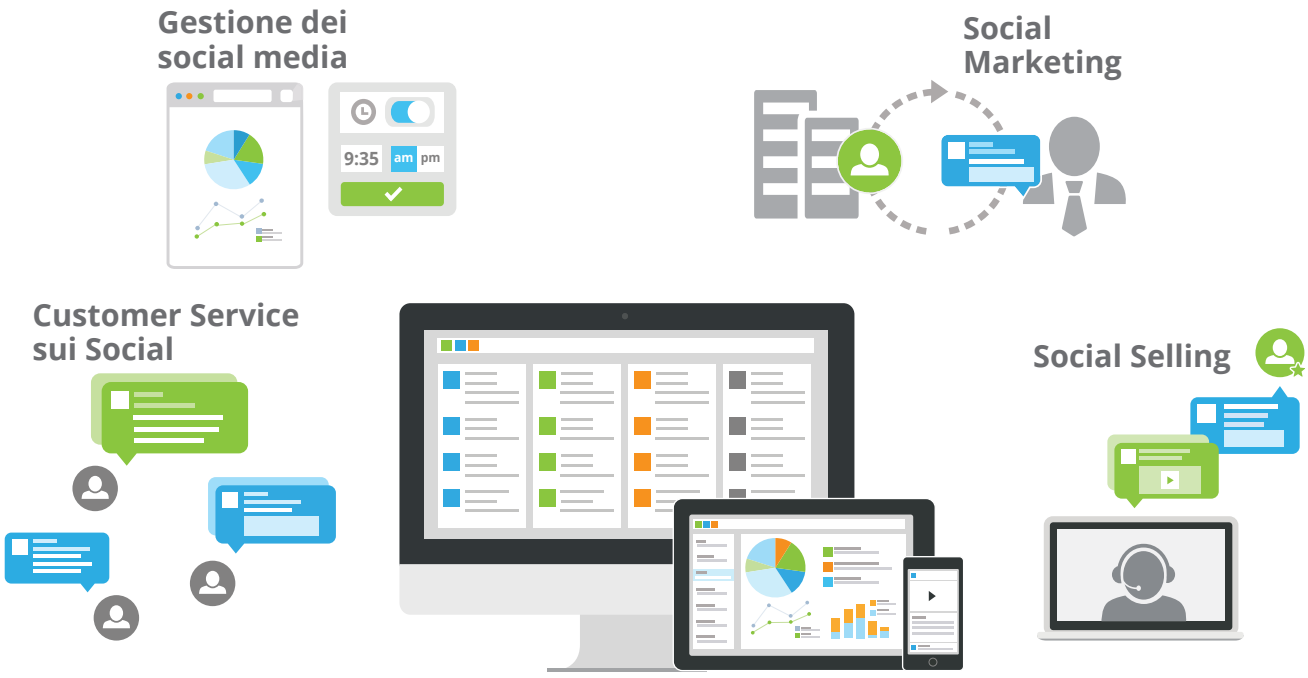
Investi in un futuro sicuro per la tua organizzazione

Proteggere il tuo brand dovrebbe essere un impegno che coinvolge l'intera azienda. Hootsuite Enterprise consente di interagire con il proprio pubblico su tutti i social media difendendosi dagli hacker, minimizzando i rischi di errori umani e mantenendo la conformità alle normative.

Lavoriamo con diversi partner per garantire la sicurezza della tua azienda sui social.

# Informazioni su Hootsuite Enterprise

Diventa partner di Hootsuite per accelerare il tuo successo sui social




Hootsuite Enterprise aiuta le aziende ad attuare strategie di business nell'era dei social media. Hootsuite Enterprise, la piattaforma per le relazioni sui social più usata al mondo, consente alle aziende di gestire le attività social su più team, dipartimenti e unità aziendali. Con la massima versatilità, la nostra piattaforma supporta un fiorente ecosistema di integrazioni tecnologiche, che consentono alle aziende di integrare l'uso dei social media con sistemi e programmi già esistenti.

Con il nostro aiuto, le imprese possono instaurare legami più stretti con i loro clienti e trarre insight significativi dai dati sui social media. Da sempre in cerca di innovazioni, aiutiamo le aziende a esplorare il panorama dei social media, accelerandone il successo tramite la formazione e servizi di livello professionale.

Richiedi subito una demo, su enterprise.hootsuite.com

## Più di le imprese presenti nella Classifica Fortune 1000 si fidano di Hootsuite

WWF · Virgin · Expedia · ACCOR HOTELS · Allianz · PORSCHE

SONY MUSIC · MONSTER · VISA · BNP PARIBAS · SWAROVSKI · PayPal