



# **The Damaging Effects of Online Impersonation on Your Brand's Integrity**



# The Importance of Brand Integrity

Brand integrity is a company's commitment to upholding its core values, promises, and brand identity in **every interaction** and **engagement**. This dedication is based on a culture of honesty, transparency, and ethical conduct, ensuring that **every action** reflects the company's stated **mission** and **values**. By consistently demonstrating this commitment, the company builds trust and credibility with its customers, stakeholders, and the broader community, establishing strong and **enduring connections** with its brand.

Every employee at your company plays a crucial role in shaping the brand experience for your customers and prospects. Their dedication and hard work ensure a **consistent** and **positive brand experience**.

Every customer and prospect who engages with you comes with an **expectation** that you will provide an **exceptional experience** and keep their data and transactions safe.

Unfortunately, it only takes one cybercriminal to damage your brand's integrity.





# A Quick Explanation of Online Impersonation

Online impersonations of your brand are not just a minor inconvenience. They occur when a cybercriminal 'borrows' your logo, creative imagery, and likeness and sets up digital assets (websites, social media accounts, mobile applications, etc.) to defraud the visitor or steal sensitive data. This can lead to a significant and immediate harm to your brand's reputation, a risk that cannot be underestimated.

Over 252,000<sup>1</sup> new websites are set up daily. And over 350,000 phishing websites, are detected each month.<sup>2</sup> These **fake websites** (spoofs) are designed with a high level of sophistication to look as authentic as possible. Invitations, including SMS and e-mail, are sent to customers and prospects from the schemers posing as the actual company. Cybercriminals are exploiting search engine results, digital ads, QR codes, and more, intending to defraud visitors or steal sensitive data.

**Fake social media accounts** impersonate your brand, executives, spokespeople, and influencers to exploit trust and trick people into disclosing credentials, payment information, and more.

**Rogue Mobile Applications** are created and published as those of a reputed brand but with malicious functionality injected. A user logging into the fake application reveals their account credentials and payment information to the fraudster.

These impersonations threaten your brand's reputation and significantly impact customer and prospect interaction. If they encounter these fake representations, the damage to their experience and perception of your company is not something you can afford to ignore.



# Customer Loyalty and Retention

The issue of brand impersonation is inherently unjust. Consumers often associate the fraudulent activities with the authentic brand, even though the latter is not involved in the impersonation. The perception of consumers becomes their reality, especially if they have been subjected to deception and fraud.

The repercussions of brand impersonation extend beyond immediate revenue loss. It can result in the propagation of false information, ultimately leading to a significant decline in customers' trust in your brand. It is crucial to address instances of brand impersonation promptly.

Customers who have endured negative encounters due to impersonation may switch to a competitor, leading to heightened churn rates, reduced customer lifetime values, and diminished long-term profitability for your brand. Therefore, combating brand impersonation is essential to safeguard revenue and maintain customer trust and loyalty.

## 63%

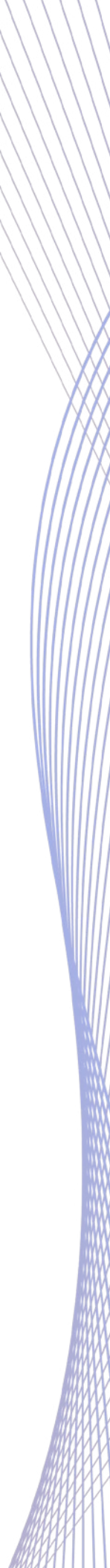
**Hold the brand accountable for spoofed websites<sup>3</sup>**

## 2X

**Likelihood of dissatisfied customers telling people about their experience compared to satisfied customers<sup>4</sup>**

## 81%

**Consumers who need to trust a brand to do what is right in order to remain loyal to it<sup>5</sup>**





# Financial

Online impersonations can have a significant impact on a brand's valuation. A brand's financial worth is intricately tied to various factors, including its reputation, customer trust, and market position. Brand valuation models, such as those used by Brand Finance, assign significant importance to customer trust and loyalty in determining a brand's financial standing.

When fake online representations divert sales from legitimate websites, it can lead to direct revenue loss for the authentic company. This loss often prompts brands to incur increased operational costs to mitigate the risks and handle the damage with customers. These costs may include expenses for monitoring and taking down fake websites, legal fees, and heightened customer service to address the concerns of customers who believed they were engaging with a legitimate company only to discover they weren't.

Additionally, customers may shift their loyalty to competitors perceived as more secure. This can result in market share loss, ultimately impacting the brand's market position and valuation. Thus, the financial impact of online impersonations extends beyond immediate revenue loss to include increased operational costs and long-term repercussions on the brand's standing in the market.

---

**25%**

**Impact on annual revenue due to distrust<sup>6</sup>**

**17B**

**Lost revenue due to online payment fraud which includes fake websites<sup>7</sup>**

**71%**

**CMOs who believe loss of brand value to be the greatest cost of a security incident<sup>8</sup>**



# Customer Acquisition

The impact of dissatisfied customers must also be considered. Customers are twice as likely to share negative experiences, leading to a broader negative perception of the brand. This erosion of trust can substantially impact the company's ability to attract new customers. Marketing efforts may fail if potential customers are apprehensive about encountering fake websites. Even well-executed marketing campaigns can't succeed if the brand's credibility is questioned.

To mitigate the negative impact and negative publicity, companies may need to allocate additional resources to marketing and public relations efforts to rebuild trust and attract new customers. This could substantially increase customer acquisition costs, which can be a significant financial burden. According to Forrester Research, the cost of acquiring a new customer can be five times higher than retaining an existing one. Moreover, additional costs to counteract the impact of online impersonations only compound this already heavy financial burden. Research by the CMO Council emphasizes the significance of trust in marketing effectiveness. A decline in trust can result in reduced marketing return on investment (ROI).

## 5X

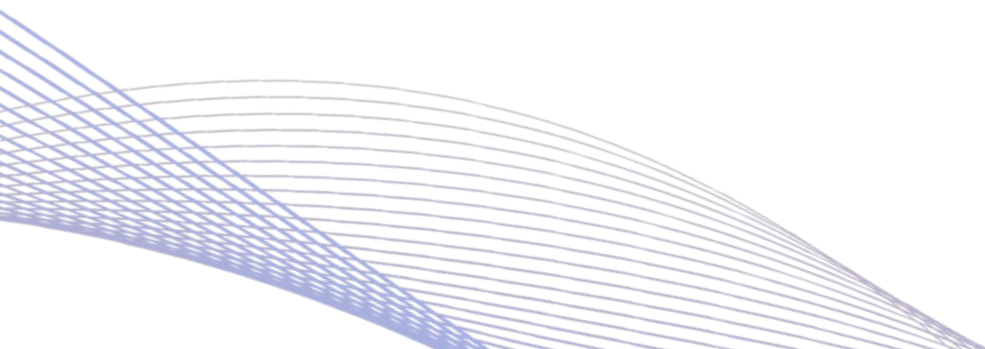
**Typical costs of acquiring a new customer versus retaining one. Costs increase when trust needs to be rebuilt.<sup>9</sup>**

## ↓ ROI

**Impact of erosion of trust on marketing campaigns.<sup>10</sup>**

## 87%

**Will take their business elsewhere if they don't trust a company to handle their data responsibly.<sup>11</sup>**





# Employee Recruitment and Engagement

Damage to a company's reputation caused by online impersonation affects its ability to attract and retain customers and employees. Prospective employees often research a company before applying, and negative news can discourage them from pursuing opportunities with the company.

To counteract the negative impact of online impersonations, companies may need to invest more in recruitment marketing, employee branding, and public relations to rebuild their reputation. The Society for Human Resource Management (SHRM) notes that the cost per hire can significantly increase if a company needs to overcome a damaged reputation.<sup>12</sup>

Online impersonation can also undermine trust among current employees. Employees who actively work to maintain your brand's integrity may be disappointed in the company's failure to protect its customers and integrity. They may also feel insecure about the company's stability and reputation. Research by the International Journal of Human Resource Management shows that employee morale and job satisfaction are closely linked to company integrity and security perceptions.<sup>13</sup>

Impersonation-related legal challenges and damage to the company's reputation can increase HR workloads as they must address the concerns of potential candidates and current employees.

**91%**

Job seekers who consider a company's reputation as a critical factor in their decision to apply.<sup>14</sup>

**87%**

Job seekers who take a company's reputation and trust-worthiness into account when making employment decisions.<sup>15</sup>

**67%**

Candidates who are hesitant to join companies with ongoing legal problems.<sup>16</sup>



# Business Resiliency

A company's business resilience, referring to its ability to adapt, recover, and maintain operations in challenging circumstances, is tested when dealing with online impersonations. This can result in financial losses, damage to reputation, and harm to customer relationships. Additionally, operational disruptions can impact the human resources department and customer service. Online impersonations often lead to increased customer service inquiries and complaints, which can overwhelm customer service teams and result in operational inefficiencies. According to a study by the Human Capital Institute, crises such as fraud can significantly increase customer service teams' workload and stress levels.<sup>17</sup>

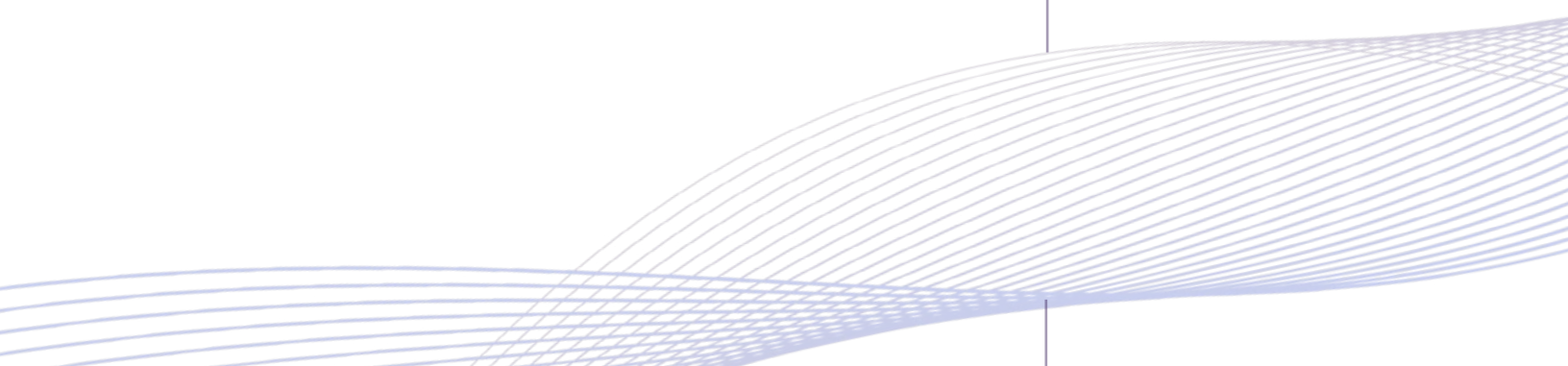
Continuous crisis management and the need to rebuild the organization's reputation can lead to resiliency erosion. The National Institute of Standards and Technology (NIST) reports that operational inefficiencies due to lack of resilience can significantly impact business continuity and productivity.<sup>18</sup> Research conducted by McKinsey & Company indicates that companies with solid resilience strategies are better positioned to outperform their competitors in stable and volatile markets.<sup>19</sup>

## 87%

**Executives who consider reputational risks to be more important than other strategic risks.<sup>20</sup>**

## 21%

**Higher profitability and lower turnover rates in businesses with higher employee engagement and better crisis management practices experience.<sup>21</sup>**







# How to Minimize the Impact of Online Impersonations on your Brand's Integrity

## Enhanced Cybersecurity Measures

- Use sophisticated tools to continuously monitor and remove online impersonators of websites, social media handles, and executive communications.
- Implement two-factor authentication and other security measures.
- Pollute their stolen data with decoy data rendering it unusable.

## Customer Engagement

- Make it clear to customers which are your official online communication channels and that you will not communicate or direct them to channels other than those.
- Maintain clear and regular communication with customers about steps to protect them from fraud.

## Improve Customer Service

- Ensure that customer support teams are well-trained and equipped to handle inquiries related to online impersonations promptly and effectively.
- Reach out proactively to customers who may have been affected by online impersonators and offer assistance and reassurance.

## Legal and Regulatory Compliance

- Pursue legal action against the operators of online impersonations to deter future fraud.
- Work with regulatory bodies and law enforcement to address and prevent fraudulent activities.

## Employee Engagement

- Keep current employees informed about security measures and company efforts to combat fraud to maintain morale by keeping employees informed about security measures and company efforts to combat fraud.
- Use employee ambassadors to promote the company's positive aspects and counteract negative publicity.

## Enhanced Recruitment Efforts

- Invest in employer branding initiatives to highlight the company's strength and commitment to integrity.
- Use targeted recruitment marketing to reach potential candidates and reassure them of the company's stability and security.

## Strengthen Internal Processes

- Develop and regularly update crisis management plans to address potential fraud-related activities effectively.
- Train employees on the importance of cybersecurity and how to recognize and report potential fraud.





# Sources

- <sup>1</sup> Siteefy "Forbes Advisor Top Website Statistics for 2024"
- <sup>2</sup> Anti-Phising Working Group "Phising Activities Trends Report 4th Quarter 2023"
- <sup>3</sup> Tech Monitor 2023 "Customers are Unforgiving of Brands Spoofed in Phishing Scams"
- <sup>4</sup> Harvard Business Review 2007 "Understanding the Customer Experience"
- <sup>5</sup> Edelman Trust Barometer "2020 Edelman Trust Barometer"
- <sup>6</sup> Forrester "How to Build Customer Trust Faster" 2021
- <sup>7</sup> Juniper Research "Online Payment Fraud Emerging Threats, Segment Analysis & Market Forecasts 2020-2024"
- <sup>8</sup> Ponemon-Sullivan "How Data Breaches Affect Reputation and Share Value" 2017
- <sup>9</sup> Forrester "The Cost of Customer Acquisition" 2019
- <sup>10</sup> CMO Council "How Brands Annoy Fans" 2018
- <sup>11</sup> PwC "Consumer Intelligence Series: Protect.me" 2017
- <sup>12</sup> Society for Human Resource Management "Human Capital Benchmarking Report" 2016
- <sup>13</sup> International Journal of Human Resource Management "Employee Morale and Job Satisfaction" 2018
- <sup>14</sup> CareerArc "The Future of Recruiting Study" 2019
- <sup>15</sup> PwC "Workforce of the Future: The Competing Forces Shaping 2030" 2017
- <sup>16</sup> Glassdoor "What Job Seekers Really Think: Employer Branding Study" 2018
- <sup>17</sup> Human Capital Institute "HR Challenges in Times of Crisis" 2018
- <sup>18</sup> National Institute of Standards and Technology (NIST) "Guide to Business Continuity Planning" 2016
- <sup>19</sup> McKinsey & Company "Risk, Resilience, and Rebalancing in Global Value Chains" 2020
- <sup>20</sup> Deloitte "Global Risk Management Survey" 2020
- <sup>21</sup> Gallup "State of the Global Workplace Report" 2020