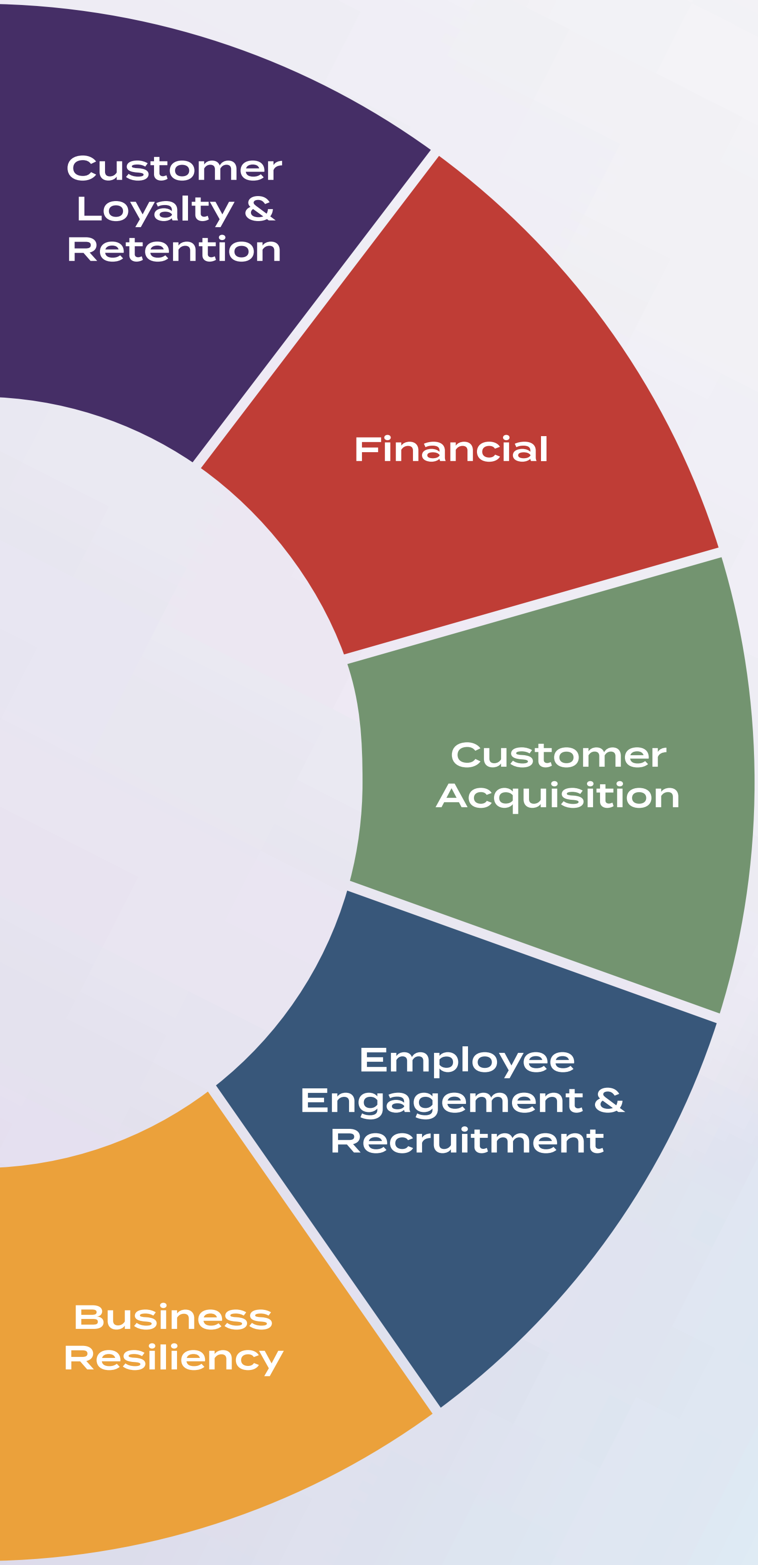
ALLURE SECURITY



Customer Loyalty & Retention

Financial

Customer Acquisition

Employee Engagement & Recruitment

Business Resiliency

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

alluresecurity.com

The Importance of Brand Integrity

Brand integrity is the trust and creditability a company builds with its customers, stakeholders, and the broader community. It is the enduring connections that the company forms through honesty, transparency, and ethical conduct in every interaction. By consistently demonstrating these values, the organization can foster a reputation that drives growth and longstanding relationships with customers.

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 consistent with your brand integrity. Part of that expectation is that the company will keep their data and transactions safe.

Unfortunately, brand integrity is fragile. It only takes one cybercriminal to change minds.

A Quick Explanation of Online Impersonation

Online impersonations of your brand occur when a cybercriminal creates websites, social media accounts, mobile apps, and other digital assets to defraud the visitor or steal sensitive data using your logo, creative imagery, and likeness. This can lead to a significant and immediate harm to your brand's reputation, a risk that cannot be underestimated.

Over 252,000[1] new websites are set up daily. And over 350,000 phishing websites, are detected each month.[2] 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 by the schemers posing as the actual company. They exploit search engine results, digital ads, QR codes, and more to deceive their targets and accomplish their goals.

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 as copies of legitimate business applications, but with malicious functionality injected. When the user logs into the fake application, the fraudster can collect their account credentials and payment information.

These impersonations threaten your brand's reputation and significantly impact customer and prospect interactions. If they become the target of 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

Brand impersonation is not the company's fault, but it is their responsibility to address. Consumers often associate the fraudulent activities with the authentic brand, even though it is not involved in the impersonation. The perception of consumers becomes their reality, and if they have been subjected to deception and fraud, they will blame the brand more often than not.

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 before it can shape the impressions of would-be prospects.

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[3]

2X

Likelihood of dissatisfied customers telling people about their experience compared to satisfied customers[4]

81%

Consumers who need to trust a brand to do what is right in order to remain loyal to it[5]

Financial

Online impersonations can have a significant impact on a brand's valuation, revenue and costs, as well as market share.

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 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 became the targets of brand impersonation attacks.

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.

25%

Impact on annual revenue due to distrust[6]

17B

Lost revenue due to online payment fraud which includes fake websites[7]

71%

CMOs who believe loss of brand value to be the greatest cost of a security incident[8]

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 impact and negative publicity, companies may need to allocate additional resources to rebuild trust and attract new customers. 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). This means substantially increased customer acquisition costs. 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.

5X

Typical costs of aquiring a new customer versus retaining one. Costs increase when trust needs to be rebuilt.[9]

↓ROI

Impact of declining trust on marketing campaigns.[10]

87%

Will take their business elsewhere if they don't trust a company to handle their data responsibly.[11]

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 negative reputation costs companies at least 10% more per hire.[12]

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.[13]

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 reputation as a critical factor in their decision to apply.[14]

87%

Candidates say they wouldn't work for a company with a bad reputation, even for a pay increase.[12]

67%

Candidates who are hesitant to join companies with ongoing legal problems.[15]

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. These attacks are a threat to everything that helps a business thrive, leading to 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 result in increased customer service inquiries and complaints, which can overwhelm customer service teams. According to a study by the Human Capital Institute, crises such as fraud can significantly increase customer service teams' workload and stress levels.[16]

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.[17] Research conducted by McKinsey & Company indicates that companies with solid resilience strategies are better positioned to outperform their competitors in stable and volatile markets.[18]

87%

Executives who consider reputational risks to be more important than other strategic risks.[19]

21%

Higher profitability and lower turnover rates in businesses with higher employee engagement and better crisis management practices experience.[20]

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 stolen data with decoy data to render it unusable.

Customer Engagement

- Make it clear to customers which online communication channels are official and that you will not communicate in or direct them to any alternative channels.
- 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

- 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 strengths 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.

Preserve Your Brand's Integrity
alluresecurity.com

Sources

[1] Siteefy “Forbes Advisor Top Website Statistics for 2024”

[2] Anti-Phising Working Group “Phising Activities Trends Report 4th Quarter 2023”

[3] Tech Monitor 2023 “Customers are Unforgiving of Brands Spoofed in Phishing Scams”

[4] Harvard Business Review 2007 “Understanding the Customer Experience”

[5] Edelman Trust Barometer “2020 Edelman Trust Barometer”

[6] Forrester “How to Build Customer Trust Faster” 2021

[7] Juniper Research “Online Payment Fraud Emerging Threats, Segment Analysis & Market Forecasts 2020-2024”

[8] Ponemon-Sullivan “How Data Breaches Affect Reputation and Share Value” 2017

[9] Forrester “The Cost of Customer Acquisition” 2019

[10] CMO Council “How Brands Annoy Fans” 2018

[11] PwC “Consumer Intelligence Series: Protect.me” 2017

[12] Society for Human Resource Management “Use Your Company's Brand to Find the Best Hires” 2019

[13] International Journal of Human Resource Management “Employee Morale and Job Satisfaction” 2018

[14] CareerArc “The Future of Recruiting Study”

[15] Glassdoor “What Job Seekers Really Think: Employer Branding Study” 2018

[16] Human Capital Institute “HR Challenges in Times of Crisis” 2018

[17] National Institute of Standards and Technology (NIST) “Guide to Business Continuity Planning” 2016

[18] McKinsey & Company “Risk, Resilience, and Rebalancing in Global Value Chains” 2020

[19] Deloitte “Global Risk Management Survey” 2020

[20] Gallup “State of the Global Workplace Report” 2020