

ONLINE BRAND IMPERSONATION TRENDS



Even if you've done nothing wrong, the majority of people (63%!) hold your organization responsible for phishing attacks and spoof websites that impersonate your brand.

IMPERSONATION ATTACKS ARE SURGING

- #1 SOURCE OF CONSUMER FRAUD LOSS IN U.S. according to the FTC¹
- \$2+ BILLION IN U.S. CONSUMER LOSSES TO IMPERSONATION FRAUD – an increase of 85%²
- 12,396 FAKE WEBSITES PUBLISHED EACH DAY, an 18-year record³

TYPES OF ONLINE BRAND IMPERSONATION ATTACKS

Fraudsters will clone a number of digital assets in order to exploit trusted relationships with a brand. Here are the most prevalent examples of online brand impersonation attacks.

SCAM WEBSITES

Scammers invite potential victims to a fake website via SMS, e-mail, search engine results, malicious digital ads, QR codes, and more to defraud the visitor or steal sensitive data. While this includes "typosquatting" and "cybersquatting," adversaries have evolved beyond simple permutations of domain names.

FAKE SOCIAL MEDIA ACCOUNTS

Fraudsters impersonate brands, executives, spokespeople, fan clubs, etc. to exploit trust and trick people into disclosing credentials, payment information, and more. Meta, for example, took action on 16 billion fake Facebook accounts in Q1 2022.⁴

ROGUE MOBILE APPS

Adversaries create and publish apps masquerading as that of a reputed brand but with malicious functionality injected. A user logging into the fake app reveals their account credentials and payment information to the fraudster.

NO INDUSTRY IS IMMUNE

Scammers target a variety of industries.



MOST TARGETED INDUSTRIES⁵

- Financial Services [23.6%]
- Software-as-a-Service [20.5%]
- E-Commerce & Retail [14.6%]
- Social Media [12.5%]
- Cryptocurrency [6.6%]
- Payments [5.0%]
- Logistics/Shipping [3.8%]
- Other [13.4%]

28.3 MILLION LUXURY BRAND SPOOFS ON TIKTOK IN 24-HOUR PERIOD

Top targets included Gucci, Rolex, Louis Vuitton, Dior, and Chanel⁶

\$36 MILLION IN CONSUMER LOSSES TO AMAZON IMPERSONATORS

5,411 people in the U.S. lost an average of \$6,653⁷

300% INCREASE IN IMPERSONATION CASES

and an average of \$4,859 lost per victim according to TSB Bank⁸

COSTS OF BRAND IMPERSONATION

Brand impersonation schemes cost fraudsters little, but cost brands a lot.

63% OF CONSUMERS HOLD BRANDS RESPONSIBLE FOR SPOOF WEBSITES⁹

66% OF FRAUD VICTIMS CHANGE ONLINE BUYING BEHAVIOR

if they experienced financial loss.¹⁰

32% OF CONSUMERS WILL LEAVE A BRAND AFTER A BAD EXPERIENCE¹¹

-15% REDUCTION IN CUSTOMER SPEND DUE TO DISTRUST

and those customers are likely to dissuade others from buying.¹²

-38% REDUCTION IN RETENTION DUE TO DISTRUST – More than one third of

consumers report closing a financial account due to fraud.¹³

-25% IMPACT ON ANNUAL REVENUE DUE TO DISTRUST¹⁴

+19.8% INCREASE IN FRAUD COSTS – A dollar in fraud costs retail /

e-commerce merchants \$3.75, approximately 20% more than before the pandemic.¹⁵

25% OF CONSUMERS HAVE PURCHASED A FAKE PRODUCT ONLINE

according to the Better Business Bureau.¹⁶

71% OF CMOs BELIEVE LOSS OF BRAND VALUE TO BE THE GREATEST COST OF

A SECURITY INCIDENT along with reputation damage, loss of customers, and loss of revenue.¹⁷

FAILINGS OF TRADITIONAL APPROACHES

Traditional approaches to the problem, (i.e., looking for permutations of a URL similar to a brand name and sending lawyers to address a scam), miss the majority of online impersonations, take too much time, and cost too much.

71% OF SPOOF SITES ARE MISSED BY TRADITIONAL DOMAIN MONITORING

Looking for domain name permutations alone misses the majority of scams.¹⁸

75% OF VICTIMS VISIT A SCAM SITE DURING ITS FIRST 10 HOURS ONLINE¹⁹

>\$14,700 COST OF MITIGATING A SINGLE IMPERSONATION INCIDENT

which takes 150+ hours of an analyst's time and at least 24 hours of a lawyer's time²⁰

>\$150,000 COST OF ANALYST TIME (1.5 FTEs) HUNTING BRAND

IMPERSONATIONS includes 3,000 hours monitoring the web, investigating possible impersonations, and initiating takedown.²¹

TIME TO MODERNIZE ONLINE BRAND PROTECTION.

Forrester estimates that opting for a third-party brand protection service over a DIY approach achieves an ROI of 225% over three years.²² Allure Security online brand protection-as-a-service uses machine learning to understand a brand and automate the continuous analysis of 70+ million online assets each day to identify brand threats.

DETECT MORE SCAMS EARLIER

Our detection engine analyzes 70+ million artifacts a day, renders content as a browser would, reviews content as a human would, and results in our technology finding 15-20% more online impersonation threats compared to competing alternatives.

UNIQUELY EFFECTIVE MITIGATION

Our unique multi-pronged approach to online brand impersonations – deceptive decoys, blocklisting & takedown – results in higher success rates and faster takedowns (in some cases reduced from weeks to minutes).



IMPERSONATION THREATS DETECTED/MITIGATED BY ALLURE SECURITY

- Online brand impersonations
- Phishing sites
- Scam sites
- Fake e-commerce shops
- Social media brand abuse
- Trademark infringement
- Malicious digital ads
- Stolen content
- Unauthorized mobile apps
- Malicious mobile apps
- Executive impersonation
- Employee impersonation

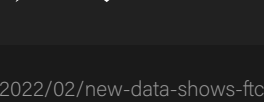
<https://www.alluresecurity.com>

<https://www.linkedin.com/company/alluresecurity>

<https://www.twitter.com/alluresecurity>

Spoof Response Assistance: 877-699-8883 | response@alluresecurity.com

sales@alluresecurity.com



¹ <https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0>

² https://docs.apwg.org/reports/apwg_trends_report_q1_2022.pdf

³ <https://www.statista.com/statistics/1013474/facebook-fake-account-removal-quarter/>

⁴ <https://www.thefashionlaw.com/gucci-rolex-louis-vuitton-top-list-of-brands-most-frequently-targeted-by-counterfeiters-on-tiktok/>

⁵ <https://www.freep.com/story/money/personal-finance/susan-tomp/2022/07/12/amazon-scams-prime-day-deals/10011793002/>

⁶ <https://www.independent.co.uk/business/bank-warns-over-impersonation-fraud-as-cases-soar-by-300-b2061294.html>

⁷ <https://techmonitor.ai/technology/cybersecurity/phishing-scams-can-destroy-consumer-trust>

⁸ https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness_documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

⁹ <https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/future-of-customer-experience.html>

¹⁰ <https://www.forrester.com/blogs/the-decline-of-consumer-trust-and-what-to-do-about-it/>

¹¹ <https://javelinstrategy.com/press-release/total-identity-fraud-losses-soar-56-billion-2020>

¹² <https://www.forrester.com/report/How-To-Build-Customer-Trust-Faster/RES137801>

¹³ <https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#ecommerce>

¹⁴ <https://www.bbb.org/content/dam/0734-st-louis/counterfeit-goods-scam/bbb-study-of-counterfeit-goods-sold-online.pdf>

¹⁵ <https://ponemon.sullivanreport.com/2017/11/how-data-breaches-affect-reputation-and-share-value/>

¹⁶ https://www.usenix.org/system/files/sec20fall_oest_prepub.pdf

¹⁷ https://www.usenix.org/system/files/sec20_slides_oest-sunrise.pdf

¹⁸ <https://www.marketscreener.com/quote/stock/MIMECAST-24949015/news/ROI-Analysis-Keeping-Brands-Safe-from-Digital-Impersonation-33005970/>