

ブランドなりすましの現状

ブランドのなりすましは広範囲に及び、問題は拡大する一方です。フィッシング攻撃の成功率を高めるために、顧客がその製品やサービスに抱いている親近感が悪用されています。このような攻撃は、メール、テキスト、ソーシャルネットワーク、広告などを通じて実行され、顧客とブランドの双方に大きな損害を及ぼす可能性があります。


1,270,883

拡大する問題

2022年第3四半期に観測されたフィッシング攻撃は、1,270,883件にのぼり、新記録となりました¹


40%

攻撃の成功要因

40%の消費者は、好きなブランドから届くメール内のリンクを、ためらうことなくクリックします

フィッシング+ブランドなりすまし = 攻撃成功率の上昇

15%

全フィッシングメールのうち、ブランドになりすましたメールの割合²

34%

フィッシングおよび同様の犯罪の前年比増加率³

69億ドル

2021年におけるインターネット犯罪被害者の被害額

ブランドなりすましが最も多い業界

 23.2%

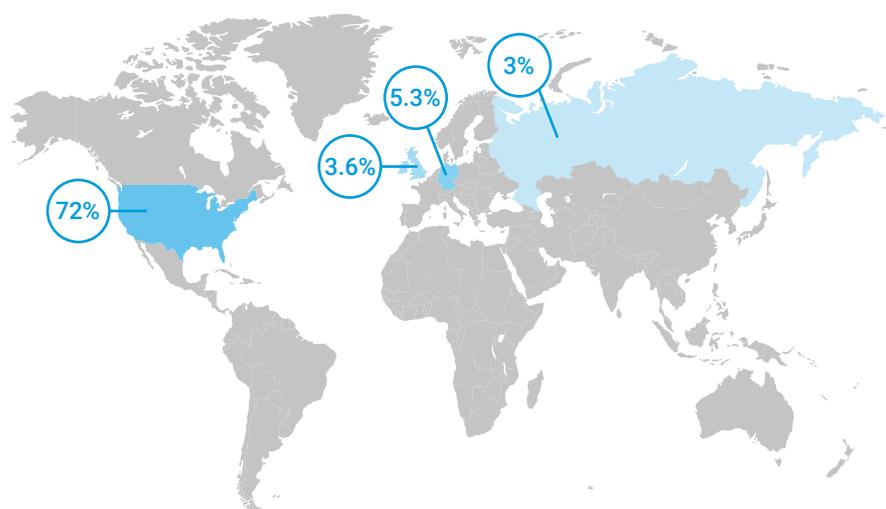
全フィッシング攻撃のうち、金融業界で見られた攻撃の割合¹

 14.6%

全フィッシング攻撃のうち、小売/eコマース業界で見られた攻撃の割合¹

時期と場所

フィッシングサイトのホスト国上位20のうち、米国には72%のサイトがホストされています。続いて、ドイツ(5.3%)、英国(3.6%)、ロシア(3%)です。



2022年にブランドなりすまし攻撃が最も活発だった月は11月で、月間平均件数の202%でした。活動が最も少なかった月は6月でした。⁴

企業による対策

42%

自社のブランドになりすました偽のWebドメインが前年と比較して増えたと答えた企業の割合

45%の中小企業 47%のエンタープライズ

ブランドなりすましによる顧客へのフィッシングを最重要課題と考えている企業の割合⁵

攻撃者に対抗するため、今後3年間にセキュリティ支出は最大14%増大すると見込まれます

ブランドなりすましリスクの緩和



ブランドなりすまし攻撃は、いつも機密データを狙ってフィッシングをしているわけではありません。米国の消費者の52%が、オンラインで偽物を購入した後に、ブランドに対する信頼を失っています。

Akamaiのブランドなりすまし防止策

ブランドの不正利用を確実に検知することで、評判の低下や収益の損失を防ぐことができます。Akamai Brand Protectorは、独自のインテリジェンスと検知アルゴリズムにより、ノイズやフォールス・ポジティブ(誤検知)を排除します。検知にかかる時間が短縮され、重大度スコアに基づき優先順位付けされた正確な検知により、1日わずか数分でブランドの不正利用を把握できます。統合緩和オプションでは、サイト閉鎖サービスとステータスの追跡を提供しています。

Akamai Brand Protector

[詳細はこちら](#)

1. APWG、Phishing Activity Trends Report、2022年第3四半期
2. Abnormal、Research Reveals 265 Different Brands Impersonated in Phishing Attacks、2022年

3. 米国連邦捜査局(FBI)、Internet Crime Report、2021年
4. Akamai Brand Protector

5. Kaspersky、IT Security Economics 2022、Executive Summary