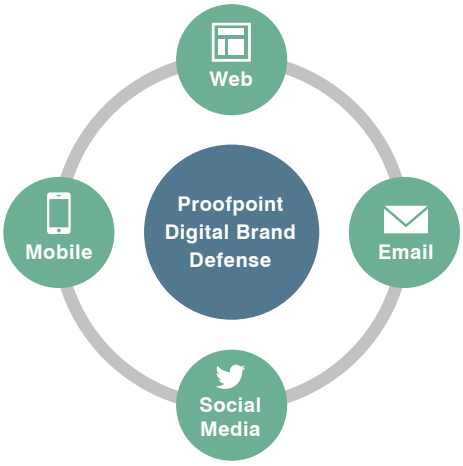
proofpoint

PROOFPOINT FRAUD PROTECTION

AN OMNICHANNEL SOLUTION TO BRAND FRAUD

Enterprise brands are using new digital marketing tools to drive productivity, improve efficiency, and lower costs. At the same time, they're expanding into new digital channels to build an omnichannel presence. While this trend improves customer engagement and experience, it also exposes companies to brand fraud across web, email, social, and mobile channels.



Digital risk has become a pervasive problem and cyber fraud is on rise. Criminals masquerade as your brand to bait your customers with scams, phishing, and offers for counterfeit products and services.

Protecting your brand and your customers in this dynamic environment requires a more holistic approach. Proofpoint looks beyond your perimeter to deliver real-time, omnichannel protection from brand fraud. With our solution, you can engage with your customers across web, email, mobile, and social media with confidence.

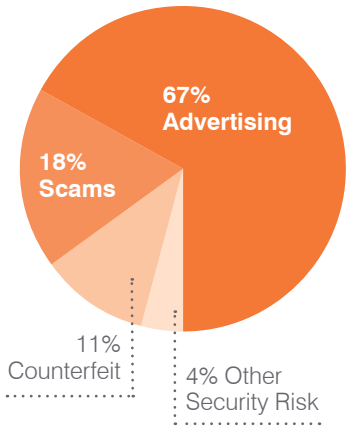
FAKE SOCIAL MEDIA ACCOUNTS

Consumers turn to social media to engage with their favorite brands. And 74% of consumers rely on social media to guide their purchases.[1] It's no wonder cyber criminals are cashing in too. A recent Proofpoint study reported 19% of social media accounts associated with the 10 biggest brands are fraudulent.[2]

Fraudsters try to take advantage of your customers by distributing scams, counterfeit goods, phishing, and junk ads. Scammers set up fake social media accounts to masquerade as corporate brands and defraud fans with fake sweepstakes. Hackers create fake customer support accounts to phish credentials. No matter what form it takes, social brand fraud hurts your customers and damages your brand.

To help you combat social media risks, Proofpoint automatically detects accounts using your brand on social media. Plus, our angler phish protection is the only patent-pending solution that protects your fans from fake customer care accounts. When someone using a lookalike service account contacts your customers, we notify you immediately and can help you take down the account.

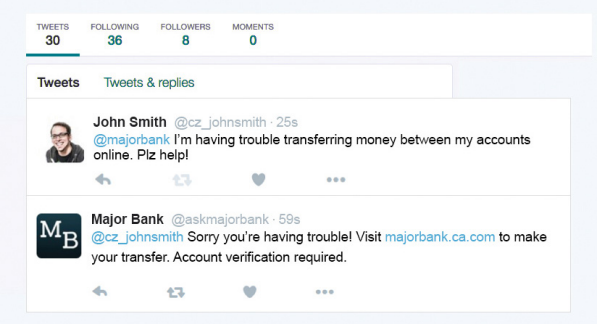
FRAUDULENT ACCOUNT TYPES
10 Top Brands



Scams and counterfeit products and services account for nearly 30% of fraudulent social media accounts in our research on top brands.

RISK SPOTLIGHT—ANGLER PHISHING

Angler phishing is one of the most dangerous variants of social media fraud. This attack gets its name from the anglerfish, a fish that uses a glowing lure to bait and attack smaller prey. In angler phishing attacks, the lure is a fake customer service account.



Example of an angler phishing attack on Twitter

The attacker waits for your customers to reach out to your real support account with a help request. Angler phishers often strike on evenings or weekends when your customer support team is less likely to monitor social media. When the criminal sees a customer trying to contact your brand, they hijack the conversation, responding directly to the customer through the lookalike social media account.

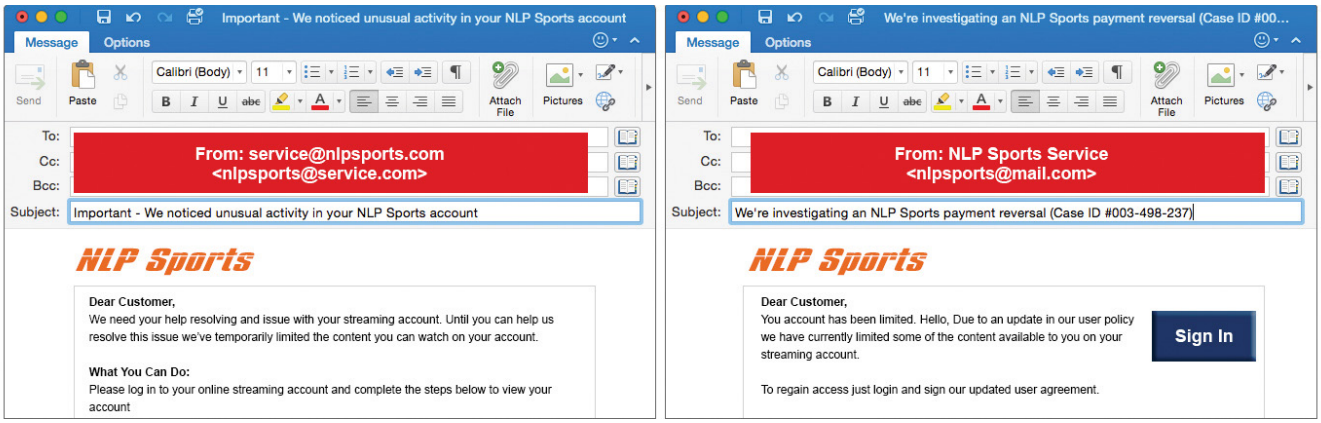
The bogus support link in the message leads to a convincing but fake version of your company's website. The website asks for the customer's online credentials, security questions and answers, social security number, or other sensitive information.

PHISHING EMAILS

Email marketing delivers business value. It drives more leads, conversions, and revenue than any other marketing channel. And customers prefer it: 72% of consumers rate email as their most preferred method of communication.[3] That's why fraudsters are taking advantage of this trusted communication vehicle between brands and buyers.

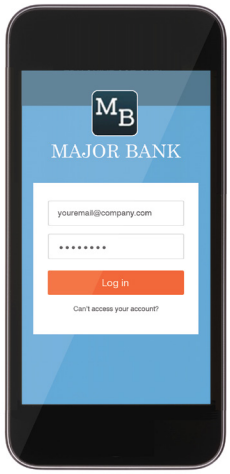
Criminals have developed sophisticated ways to dupe consumer mailbox providers into delivering malicious emails. Messages that spoof your brand can trick your customers into giving up their sensitive information.

We empower you to identify and respond to email threats targeting your customers in real-time. Using data from over 2 million consumer inboxes and more than 70 mailbox providers, we uncover phishing emails spoofing your domains.



Fraudsters use fake emails to target your customers. Both of these emails use display name spoofing to trick customers into believing the emails are real. Note the domains (@service.com and @mail.com) do not belong to the real company.

FRAUDULENT MOBILE APPS



Making purchases and managing bank transactions through mobile apps on smartphones and tablets has become standard practice. Consumers like the convenience of shopping and managing their accounts on the go. As a result, mobile apps are now a rich arena for brand fraud.

Criminals create applications that imitate your brand. When your unsuspecting customers install the app, it can steal their credentials, distribute malware, and access data stored on the device.

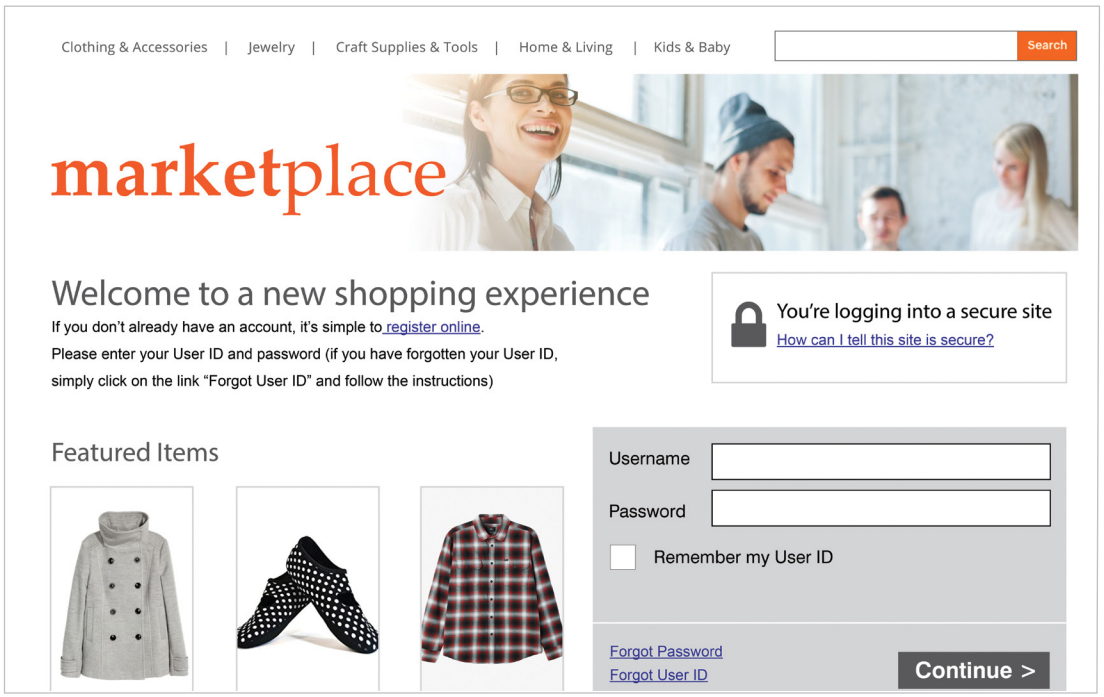
The size and dynamic nature of the global app store ecosystem make it difficult for companies to keep track of their mobile presence and to identify fraudulent brand apps. We monitor hundreds of app stores and detect unauthorized apps impersonating your brand.

FAKE WEB PAGES

Cyber criminals use social media, mobile apps, and emails as the lures in their brand fraud attacks. Often, these attacks lead to fake web pages hosted on spoofed or lookalike domains. Hackers use techniques like typosquatting to queue up multiple domains for future phishing schemes.

In addition to phishing, fraudulent sites can imitate your brand to sell knockoff or stolen versions of your products, steal intellectual property, or deliver a cyber-attack. Many organizations struggle to keep up with the vast amounts of web data needed to identify this brand threat. We help you manage this risk.

We analyze a vast body of data and examine new domains as they are registered to uncover domains that pose a risk to your brand and customer experience. When we discover a fraudulent web page, we notify you and help you get it taken down immediately.



MAKING DIGITAL BRAND DEFENSE A REALITY

Managing a brand's digital presence has traditionally been a manual, ad hoc effort. Processes are often reactive and focus only a specific channel. But external threats and brand fraud occur over multiple vectors. For example, a customer support interaction on social media may direct your customer to a bogus web page. Or a fake email may encourage users to download a fraudulent mobile app. Hackers are coordinating their attacks on multiple channels, so you need to make sure your security covers social media, email, mobile, and web.

Proofpoint Fraud Protection is the only solution that protects your customers and your brand reputation on all these vectors. By correlating data across channels, we give you complete visibility into brand fraud attacks. When we see a malicious URL in a phishing email, we can immediately search the social media sphere for fake pages using the same malicious domain. We centralize all this data in a single, integrated dashboard for a seamless user experience.

Once we find fraudulent activity, we help you put a stop to it immediately. We offer managed takedown services and we can work with your existing takedown partners to remove fraudulent domains.

You can deploy Digital Risk Defense across social, email, mobile and web in less time than you think. Connect with us to request a risk assessment and learn how we can protect your digital brand.

LEARN MORE

To learn more about Proofpoint Brand Fraud Protection visit:
www.proofpoint.com/digital-risk

KEY BENEFITS

DETECT AND PROTECT AGAINST DIGITAL RISKS

Real-time discovery and remediation for brand fraud that hurts your customers and reputation

OMNICHANNEL COVERAGE

A holistic approach to protecting your brand and customers from digital risks across web, email, mobile, and social media

COMPLETE VISIBILITY

A vast data corpus and advanced analytics provide the insights you need to stop digital risks

1. Akino Chikada (MarkMonitor). "Brand Abuse Lurking on Social Media." October 2015.
2. Proofpoint Social Media Brand Fraud Report, August 2016.
3. Daniel Burstein (Marketing Sherpa). "Marketing Research Chart: How do customers want to communicate?" February 2015.