How to Understand Online Brand Threats

The first step in protecting your brand online is to understand the landscape of modern digital threats. From "super fakes" to sophisticated phishing, scammers are constantly evolving their tactics to deceive consumers and exploit intellectual property.

In today's digital economy, threats are rarely isolated. They often involve complex networks operating across social media, marketplaces, and standalone websites simultaneously. Identifying these patterns is crucial for a robust protection strategy.

Step 1: Identify the "Super Threat"

First, you must categorise the type of infringement. Modern threats often combine multiple tactics to appear legitimate:

- Counterfeits: High-quality "super fakes" that are visually almost identical to genuine products.
- Impersonation: Fake brand profiles using official logos and stolen marketing imagery to build false trust.
- Phishing: Deceptive links and "spoofed" websites designed to steal customer credentials or payment data.

Step 2: Monitor Evolving Tactics

Scammers use advanced technology to bypass traditional detection. You should be aware of these common methods:

- AI-Generated Content: Use of AI to create realistic product photos or "deepfake" endorsements from influencers.
- Hidden Links: Directing users away from regulated platforms to encrypted messaging apps like WhatsApp or Telegram to close a sale.

- Social Engineering: Using high-pressure "flash sales" or "limited time offers" to discourage customers from performing due diligence.

Note: Scammers often target your customers during peak shopping periods, such as Black Friday or seasonal sales. Use a generic company email address for monitoring to keep your primary inbox secure.

Step 3: Document the Evidence

To ensure successful enforcement, you must gather as much detail as possible. When you spot a threat, make sure to note:

- The type of threat (social post, sponsored advert, or marketplace listing).
- A direct link (URL) to the infringing content.
- The name of the account or "storefront" responsible.
- A screenshot of the content, including any engagement (likes/comments) which shows the threat's reach.

Step 4: Assess the Risk Level

Not all threats require the same response. You should prioritise your actions based on the potential impact on your brand:

- High Risk: Content that poses a health and safety risk (e.g., fake pharmaceuticals or electronics) or massive financial fraud.
- Medium Risk: Widespread "super fakes" that dilute your brand equity and divert significant revenue.
- Low Risk: Isolated instances or individual "fan" accounts using copyrighted imagery without malicious intent.

Step 5: Report and Neutralise

Once the threat is documented and prioritised, use the appropriate legal or platform-specific tools to take action. Providing your trademark registration number or copyright certificates is essential for a swift resolution.

What Happens Next?

Monitoring is a continuous cycle. Once a threat is removed, "copycat" accounts may appear. Properly documenting these links allows you to identify the underlying networks. Combining human intelligence with automated monitoring is the most effective way to protect your brand long-term.

Contact Us

Every fake listing or imitation product takes a share of your hard-earned sales.

SnapDragon combines AI-powered detection, expert enforcement, and global experience to keep counterfeits off the market and your genuine products where they belong – in customers' hands.

Talk to SnapDragon about how proactive brand protection can drive stronger, more sustainable growth.

www.snapdragon-ip.com

UK & RoW: +44 131 466 9249
US: +1 857 400 7041

thelair@snapdragon-ip.com

LinkedIn

SnapDragon