

➤ BRIEF

Brand Protection Trend Report

B-2023-07-31a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Brand, Impersonations, Fraud



July 31, 2023

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 4:00 PM (EDT) on July 14, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Brand Protection Trend Report

Executive Summary

An organization's brand is the key to its success—public perception of that brand can significantly impact its bottom line. A brand is not just a product or service; a brand is made up of key personnel, publicity, cyber hygiene, customer sentiment, and many more factors of an organization's digital footprint. Thus, how an organization protects its brand is impactful.

Protecting an organization's brand has never been more crucial as external cybersecurity threats toward brands continue to increase significantly. From the first to the second quarter of 2023, ZeroFox saw a 164 percent increase in verified external cyber threats against brands. Breaking it down, the most significant change in the threat landscape was related to fraud, scams, and piracy – verified alerts for those threats increased 35 percent quarter-over-quarter across the ZeroFox customer base. Impersonations also saw a nearly 20 percent increase from Q1 to Q2, as cybercriminals utilized the value of impersonating already-established brands to appear more legitimate.

In this trend report, ZeroFox researchers examine the major events and associated trends observed in the second quarter of 2023 and provide recommendations so that organizations can proactively address potential issues and threats to their brands.

| Analyst Observations

Domain-Based Threats

Combating suspicious domain registrations is an ongoing battle for many organizations. The return on investment for threat actors leveraging lookalike or spoofed domains remains high, with many displaying the tenacity and forethought to register domains months or even years ahead of utilizing them in malicious campaigns. Threat actors are well-versed in which hosting providers and domain registrars are the most flexible to leverage in terms of restrictions and pressure (or lack thereof) to remove offending content, as well as which present the most challenges for any remediation efforts. In addition, threat actors frequently leverage special registration promotions and schedules in order to limit their financial output when registering domains. In the second quarter of 2023, a widespread campaign targeting retailers was identified that had been ongoing for months and is still continuing. This campaign involved a combination of registering impersonation domains months (or even years) ahead of time with random country TLDs (top-level domains), manipulating search engine optimization (SEO) rankings, and gathering victims' emails, passwords, credit card numbers, and possibly other personal information for financial gain.¹

ZeroFox Intelligence observed nearly a 20 percent increase in spoofed domains in the second quarter of 2023 versus the first quarter, with just over one-third tied to phishing campaigns.² Organizations operating in the United States and the United Kingdom continued to be heavily targeted in the second quarter; however, organizations in Greece saw a whopping 95 percent increase in domain issues, which is likely tied to the social unrest and legislative elections that occurred there during the quarter.³⁴ In addition, Ireland and Austria continued to be on the list of the top-five countries impacted by spoofed domains in the second quarter.

¹ [hXXps://cybernews\[.\]com/editorial/nike-adidas-massive-scam-campaign/](https://cybernews.com/editorial/nike-adidas-massive-scam-campaign/)

² ZeroFox Internal Collections

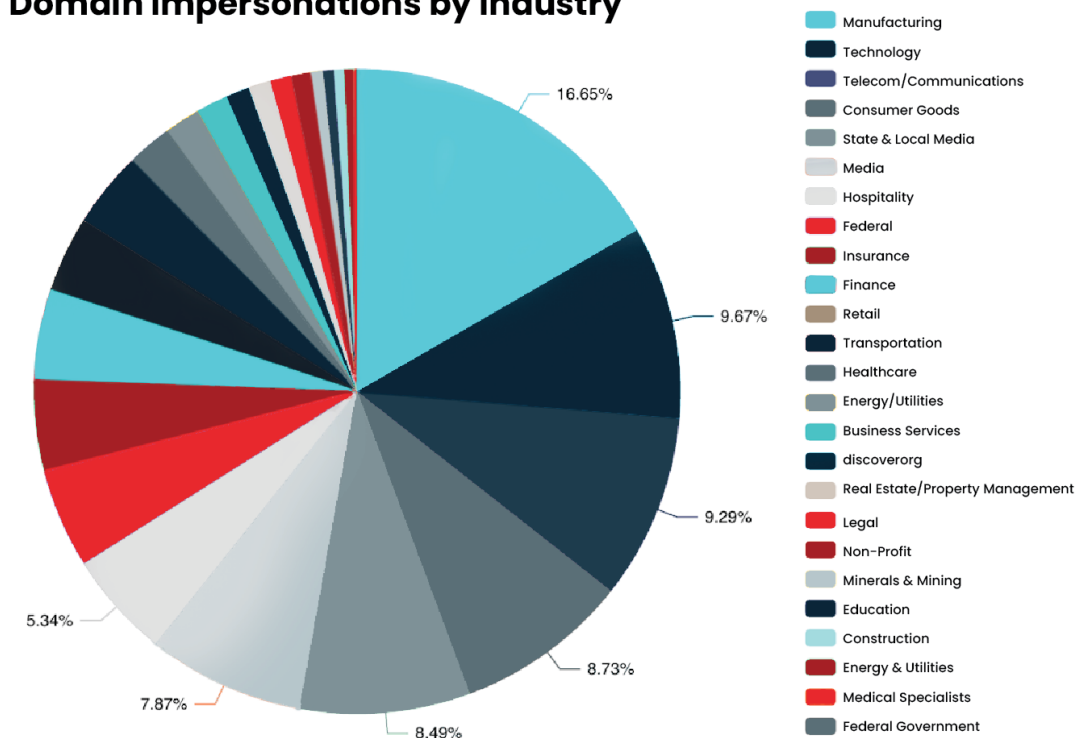
³ *Ibid.*

⁴

[hXXps://acleddata\[.\]com/2023/05/18/the-normalization-of-political-violence-and-the-2023-legislative-elections-in-greece/](https://acleddata.com/2023/05/18/the-normalization-of-political-violence-and-the-2023-legislative-elections-in-greece/)

From an industry perspective, the manufacturing sector saw the most marked increase in domain impersonations in the second quarter, with an 81 percent increase observed. While the technology industry also remained near the top of most-impacted industries on average by organization, it experienced a drop-off of two-thirds compared to the first quarter of 2023. Financial services remained the hardest-hit industry for domain impersonations; however, identified incidents quarter-over-quarter remained nearly level in the second quarter.⁵

Domain Impersonations by Industry

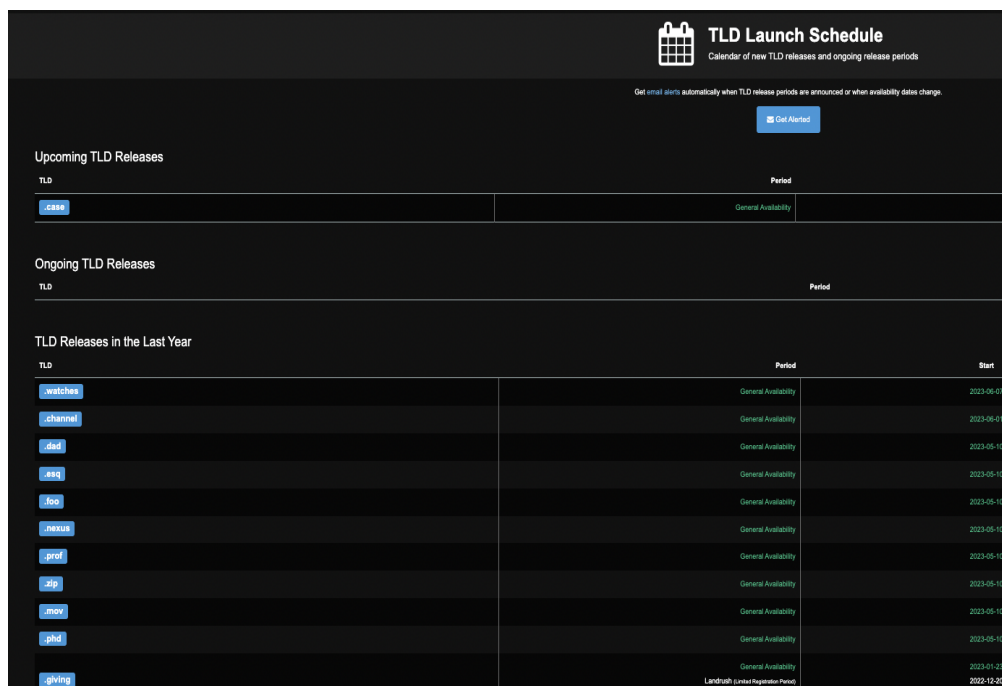


Source: ZeroFox Internal Collections

Compounding the issues inherent in defending a brand against impersonations is the fact that new Top Level Domains (TLDs) are released on a fairly regular basis. Some of these cause security researchers significant concern—not only because they expand the attack surface for threat actors but also because they have potential cybersecurity implications. For instance, the TLD .zip was released in May 2023 and raised concerns

⁵ ZeroFox Internal Collections

about the potential confusion of the TLD with the file designation, which has been leveraged by threat actors increasingly over the last few years in malware campaigns.⁶



TLD Launch Schedule
Calendar of new TLD releases and ongoing release periods

Get email alerts automatically when TLD release periods are announced or when availability dates change

[Get Alerts](#)

Upcoming TLD Releases

TLD	Period
.case	General Availability

Ongoing TLD Releases

TLD	Period
-----	--------

TLD Releases in the Last Year

TLD	Period	Start
.watche	General Availability	2023-08-07
.channel	General Availability	2023-08-01
.dad	General Availability	2023-05-10
.esq	General Availability	2023-05-10
.foo	General Availability	2023-05-10
.nexus	General Availability	2023-05-10
.prof	General Availability	2023-05-10
.rip	General Availability	2023-05-10
.zoo	General Availability	2023-05-10
.phd	General Availability	2023-05-10
.giving	General Availability	2023-01-23
	Launch (Last Registration Period)	2022-12-30

TLD Launch Schedule

Source: [hXXps://tld-list\[.\]com/launch-schedule](https://tld-list[.]com/launch-schedule)

> Forward Look:

- As new TLDs are rolled out, they can present additional vectors through which threat actors may leverage a brand name for malicious purposes. There is only one confirmed TLD release for the third quarter of 2023 thus far; additional TLDs will likely be added over the remainder of the year, but the amount will depend on the applications received as well as the outcomes of the review periods for each.⁷

Fraud

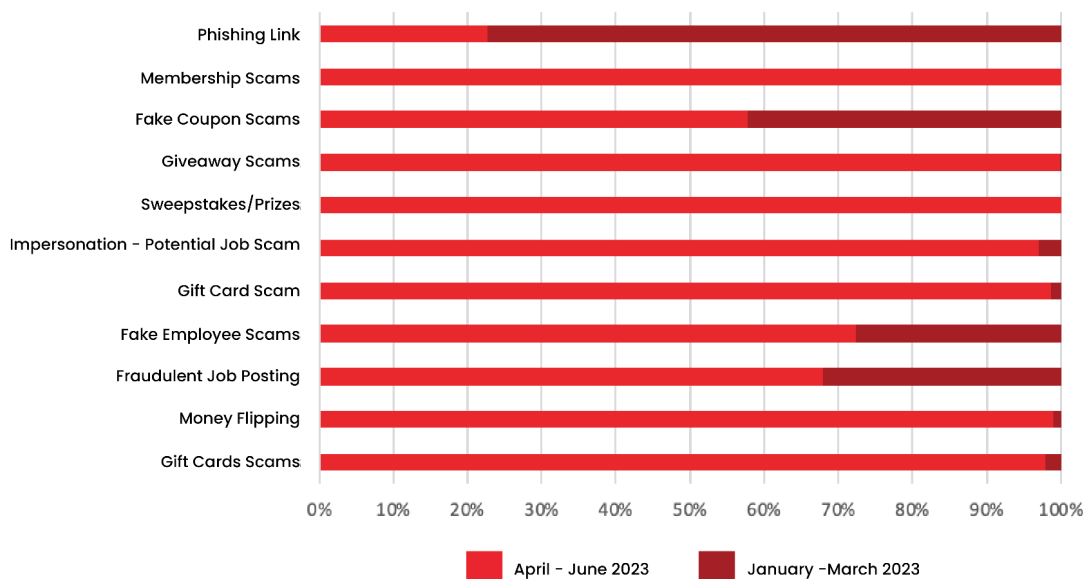
Different times of the year present various themes for threat actors to leverage in scam campaigns. At the end of the calendar year, the campaigns largely involve

⁶ [hXXps://www.malwarebytes\[.\]com/blog/news/2023/05/zip-domains](https://www.malwarebytes[.]com/blog/news/2023/05/zip-domains)

⁷ [hXXps://help.opensrs\[.\]com/hc/en-us/articles/203862546-New-TLD-Launch-Phases](https://help.opensrs[.]com/hc/en-us/articles/203862546-New-TLD-Launch-Phases)

holiday-themed lures; tax-themed lures are often used in the spring in the United States. Vacation-themed lures are typical in the summertime.⁸⁹¹⁰ In reality, any holiday, tragedy, or social event can present threat actors with opportunities for fraudulent activity, as indicated in ZeroFox Intelligence's 2023 Women's World Cup Event Assessment. Social engineering campaigns during the World Cup are almost certain to vary in complexity from low-level, rudimentary email and SMS-based scams targeting mass audiences to sophisticated spear phishing attacks directed at specific organizations and individuals associated with the tournament, such as diplomats, journalists, and high-profile executives.¹¹ In addition, scams can provide threat actors with a wealth of financially-lucrative information, including personal and financial data.

ZeroFox-Observed Fraudulent Activity



Source: ZeroFox Internal Collections

⁸ [hXXps://www.zerofox\[.\]com/blog/tax-scams-to-look-out-for-this-year/](https://www.zerofox.com/blog/tax-scams-to-look-out-for-this-year/)

⁹ ZeroFox Intelligence - [hXXps://cloud.zerofox\[.\]com/intelligence/advisories/18915](https://cloud.zerofox.com/intelligence/advisories/18915)

¹⁰

[hXXps://www.news24\[.\]com/news24/tech-and-trends/news/holidaymakers-beware-these-scams-are-used-to-target-people-booking-a-vacation-20230707](https://www.news24.com/news24/tech-and-trends/news/holidaymakers-beware-these-scams-are-used-to-target-people-booking-a-vacation-20230707)

¹¹ ZeroFox Intelligence - [hXXps://cloud.zerofox\[.\]com/intelligence/advisories/21226](https://cloud.zerofox.com/intelligence/advisories/21226)

ZeroFox tracks fraud and scams through its collection efforts in support of various client use cases, and several notable trends stood out in the second quarter of 2023. Overall, there was a 26 percent increase in the amount of fraudulent activity observed in this quarter compared to the last. Nearly 80 percent of this fraudulent activity was due to gift card scams, which plagued retailers and consumers. As Artificial Intelligence (AI) continues to evolve, cybercriminals continue to refine the use of botnets to brute force gift card websites in order to test card number/pin combinations, leading to better and quicker success in committing gift card fraud.¹² In addition, fraudulent job postings identified rose by over 50 percent, which leverages legitimate organizations to create fake job postings in order to solicit personal and financial information from victims. Furthermore, membership, giveaway, and sweepstakes/prizes scams saw marked increases compared to the previous quarter, as threat actors continue to prey on consumers using “too good to be true” lures. While not originating with a legitimate organization, victims frequently blame trademark owners for not better protecting their brands and keeping them from being leveraged in these scams.

Scammers also promote a variety of “money flipping” and other financial scams on social media, which can reflect poorly on a brand if it is tied to a money-flipping scheme which victims fall prey to. One of the most popular of these involves scammers alleging they can transfer “unclaimed funds” if a banking customer hands over their login information. Similarly, card-cracking scams involve convincing banking customers to provide a scammer with credit card and banking details. The scammer then deposits funds into the account using fraudulent checks and immediately withdraws the funds from an ATM.¹³ People tend to fall for these types of scams because they are promised a cut of the funds and that there will be no legal repercussions for their role in the scam since they are solely a temporary “middleman” in the transaction. The victims frequently blame the associated brand named in the scheme as the reason that they lost money. In Q2 of 2023, ZeroFox observed a nearly 100 percent increase in money-flipping incidents. In the last several months, money-flipping ads on social media have gained in

¹² <https://www.arkoselabs.com/explained/gift-card-fraud/>

¹³ <https://www.aba.com/Consumers/Pages/CardCracking.aspx>

popularity, with scammers promising to multiply victims' cryptocurrency investments—which are then unrecoverable.¹⁴

Also in May 2023, warnings were issued around threat actors with physical access to gift cards being able to tamper with them and gain access to the individual numbers and pins associated with each card.¹⁵ After consumers purchased the cards and went to use them, they found that the balances had been depleted as soon as they had been activated; the more sophisticated threat actors received notifications when the cards were activated.

> **Forward Look:**

- In June 2023, New York passed a law whereby retailers have to post signs near gift cards to warn consumers about possible scams. Should additional states implement similar legislation, this could have a marked increase in consumer awareness and make it more difficult for threat actors to prey on their victims, which would have an overall positive impact on brand sentiment.¹⁶
- As deepfake technology evolves rapidly, it will make it more challenging for potential victims to discern between real and deepfake-generated profiles. In addition, the wealth of data available on individuals online makes it much easier for deepfake technology to build robust, fraudulent profiles. Thus, organizations will have to be much more proactive in identifying impersonation profiles with ongoing monitoring when they appear, as well as remediating them when identified, in order to protect their organization's reputation.

Social Media-Based Threats

Both key personnel and organizations are frequently impersonated on social media by cybercriminals, who make fake accounts using their name, likeness, and other personal information. While these accounts may employ different tactics and have varied end goals, they can both lead to the same result: damage to an organization's brand. Pulling

¹⁴

[hXXps://www.wsocvtv\[.\]com/news/local/bbb-issues-warning-about-money-flipping-scam-gaining-popularity-tiktok/4BH7YBT7ZJF7PQQZYCY3HYRLE/](https://www.wsocvtv.com/news/local/bbb-issues-warning-about-money-flipping-scam-gaining-popularity-tiktok/4BH7YBT7ZJF7PQQZYCY3HYRLE/)

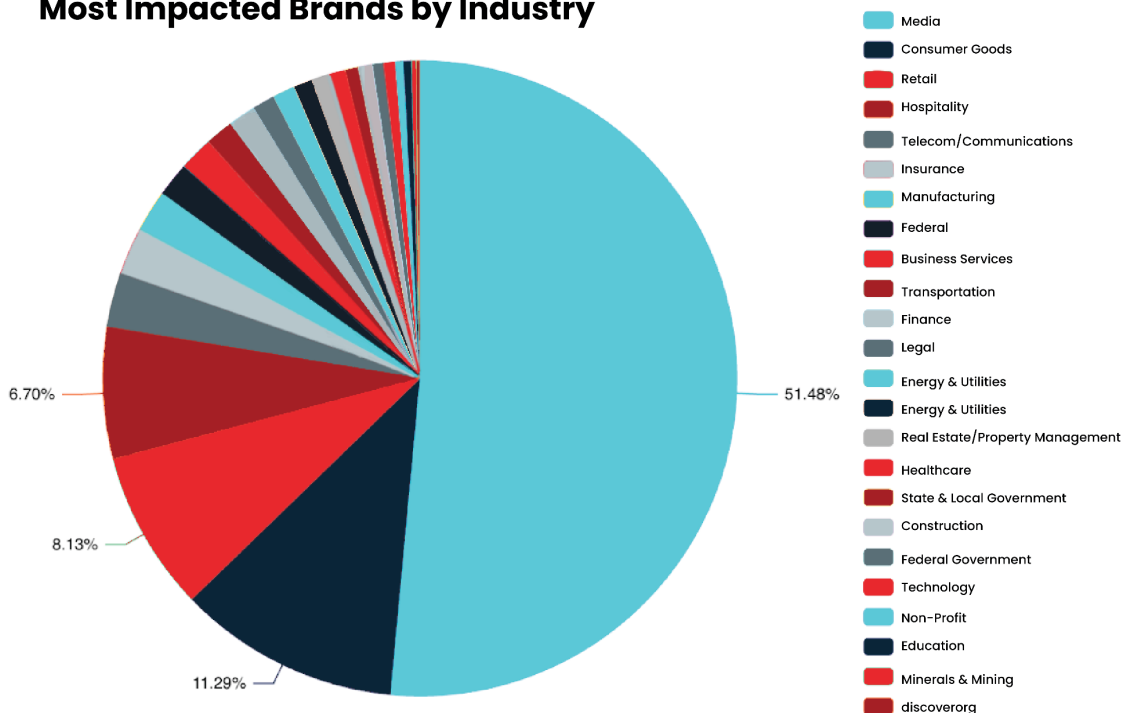
¹⁵ [hXXps://cbs4indy\[.\]com/news/4-your-money/beware-of-this-new-gift-card-scam-twist/](https://cbs4indy.com/news/4-your-money/beware-of-this-new-gift-card-scam-twist/)

¹⁶ [hXXps://www.nbcnewyork\[.\]com/news/local/new-ny-gift-card-law-to-protect-against-scams-goes-into-effect-what-to-know/4438121/](https://www.nbcnewyork.com/news/local/new-ny-gift-card-law-to-protect-against-scams-goes-into-effect-what-to-know/4438121/)

content together to populate an impersonation account typically has a very low barrier to entry; corporate websites and data aggregators can provide a wealth of information for threat actors to leverage to legitimize these brandjacked accounts.

Threat actors leverage social media impersonations in jobs, rewards, and other scam campaigns. These can be very lucrative because victims provide a host of personal and possibly even financial data when they believe they are pursuing an employment opportunity or that they will be receiving some sort of reward. Unfortunately for organizations, when victims realize they have fallen prey to an impersonation, they often blame the associated brand for it—even though the brand owner has no oversight into what threat actors create. Furthermore, threat actors can leverage a brand to create fake accounts that promote content against an organization's values. This type of content can land an organization in reputational trouble based on the content posted—whether it be offensive, political, or just taking specific social justice stances. The reputational backlash can include losing consumer loyalty, revenue, or investor confidence. Based on ZeroFox's research visualized in the chart below, over half of the impersonation accounts identified in the last quarter were in the media industry, which is logical given the number of personalities in that industry along with well-known executives. From there, a quarter of the impacted industries included consumer goods, retail, and hospitality.

Most Impacted Brands by Industry



Source: ZeroFox Intelligence

Key personnel social media impersonation accounts can also inflict significant damage on executives and their organizations. In Q2 of 2023, ZeroFox researchers observed no notable changes in the number of impersonation accounts utilizing only a name or a name and image together. However, impersonation accounts that also leveraged a biography with a name and image to legitimize these profiles saw a 22 percent increase, and those that used a biography with a name only increased by 35 percent. These biographies are typically quite easy for threat actors to find and utilize, as much of the content is available on corporate websites and/or professional social media profiles.

> Forward Look:

- Social media platforms actively roll out mechanisms to combat impersonation accounts. For instance, in the coming quarter, YouTube will begin cracking down on fan accounts that do not explicitly state their purpose—both to protect users from being misled by threat actor impersonation accounts created for nefarious purposes and to protect creators from having their likeness and brands used with malicious intent.¹⁷

¹⁷<https://support.google.com/youtube/thread/222141263/updates-to-youtube-policies-for-fan-channels>

- In addition, the Federal Trade Commission (FTC) has been working on new proposals for laws that would hold threat actors accountable for these impersonation accounts and give organizations more leverage to pursue them for financial and reputational damage resulting from these impersonations.¹⁸

| Conclusions

Organizations will continue to face challenges from threat actors utilizing their brands for financial gain; these brands present a lucrative financial opportunity for threat actors to leverage in their various fraud, scam, and otherwise malicious campaigns. Fairly or unfairly, how organizations proactively defend against these threats and protect their brands is tied directly to public sentiment towards them, as job seekers and consumers will continue to blame the organization itself when they fall victim to a campaign using that brand. Continually expanding attack surfaces through new TLDs and AI-generated impersonations will mean that organizations will need to have a robust monitoring program in place to maintain awareness of the threats and proactively address them.

¹⁸[https://gbhackers\[.\]com/the-brandjacking-threat-how-companies-can-avoid-losing-brand-equity/](https://gbhackers[.]com/the-brandjacking-threat-how-companies-can-avoid-losing-brand-equity/)

| Recommendations

While safeguarding an organization's brand requires a multi-faceted approach, ZeroFox researchers have identified several proactive steps that can be taken to protect a brand:

- Establish, monitor, and protect all digital and social media platforms in order to have an official presence, as well as identify any issues to the official accounts or to identify impersonation accounts.
- Organizations should proactively register domains leveraging their brand names based on the upcoming TLD release calendar to get ahead of threat actors registering and weaponizing these domains.
- Remove impersonating domains and social media accounts.
- Document and track executive exposure in open and closed sources and reduce digital footprints to minimize the availability of media that fuels impersonation.
- Establish a program for ongoing monitoring of brand mentions on the dark web.
- Configure ongoing domain monitoring with ZeroFox to proactively identify infringing domains that could cause reputational harm to your organization and your customers. From there, utilize ZeroFox Disruption services to take down the infringing content.
- Remain vigilant with texts and emails, and do not click on links from unknown senders.
- Integrate filtered or curated threat intelligence specific to your threat environment to better prioritize and surface relevant alerts.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%