Reporting Handbook

This is a compressed summary. For full explanations, please refer to PhishFort's Guide to Effective Takedowns and Evidence Collection

Case	Case Evidence Required
Website impersonation	Original website Statements / clear abuse that the site is maliciously targeting the brand in question
Social Media Accounts	The real and/or legitimate account as a reference point, Letter of Authorization, and/or Statement of Impersonation of the company or person. Requires 2 from: - impersonating logo - impersonating name - post with affiliation claim/impersonation
Messaging Platforms	Specify Messenger on the platform or submit as a URL, screen, or text where visible: - Username - Date - Infringing text. - It's best if also provided with a summary of the malicious activity
Phone scams	Both numbers involved in the call + TZ description of what was said / sms text (should be impersonation statement)
TM/Copyright infringement	Proof of ownership of specific material (TM reg, link to photo on official website, etc.) Proof of unfair use LoA must match the TM

APK websites	link to the original App.
Email attack	email headers from the email attack, malicious or impersonating content in the email.
Similar/Typo squat domain	In general, takedown requests for typosquat domains are not pursued. However, there is a higher chance of success if the domain is not composed of generic words, but malformed/improper wording, takedown not accepted if the website under the domain looks legit and has a historic footprint on the internet.
Parked page	Clear TM in the link; that is not a generic word. There is no legal reason to take down parked pages, so such takedown attempts are performed only when possible.
Redirect source	Submit the target domain as a separate incident with a comment about the redirect. The source custom domain should have a clear TM in the link, which is not a generic word. Link shortener requires a phishing target domain. There is no legal reason to take down redirects, so such takedown attempts are performed only when possible.
Scams	Case-specific, but usually court-level: - Service promised. - Proof of transaction. - Proof of no service delivered
Suspicious / not malicious	Research is possible as part of the detection package.
Other	Please explain in detail how to reproduce the case, and what the scam or threat is.

*Takedown times will vary depending on the specifics of each takedown

WHAT MAKES EVIDENCE STRONGER, AND WHAT IS NOT ACTIONABLE:

Brand Impersonation

Brand impersonation, or brand spoofing, is a phishing tactic that involves cybercriminals falsely representing themselves as your organization or one of your organization's employees.

Evidence	**Not / counter evidence**
Usage of the victim logo as its own logo	Having own logo / using victim logo somewhere in content
Use client name as own in page title, main header, footer (c)	Mention brand as category or subpage related to service provided
Clearly state to be official support / helpdesk / other department of victim brand	Say that they can help with something, without pretending to be official Representative
Account use name/photo/position of official employee.	Former worker; Same name, but not related
	Competitors or similar businesses, especially when brand name is very generic

Trademark and copyright infringements

TM/CR infringements are not part of brand impersonation (as impersonation is malicious and more powerful evidence). In summary, it is all uses that are not "fair" or "nominative". https://www.trademarklawy erfirm.com/what-is-trademark-fairuse/#:~:text=“Fair use” is a term,rather%2C for its descriptive meaning.

Fair Trademark usage:

- The use of the plaintiff's mark is necessary to describe their goods or services.

- They use only as much of the mark as is necessary to describe the product. Their conduct reflects the accurate relationship they have with the plaintiff

For nominative Trademark usage, the following elements must be present:

- The use must accurately refer to the owner of the trademark or the goods or services sold under the trademark it cannot be misleading or defamatory;
- The use must not imply any endorsement or sponsorship by the trademark owner;
- There should be no easier way to refer to the owner or its products; and
- Only so much of the trademark can be used as is needed to identify the trademark owner and no more.

Similar domains not covered by TM, exact TM often only through UDRP

Evidence	Not / counter evidence
Claims to be an official partner/distributor/sponsored	Service connected with product / TM; Identifying customers
Fake news if evidence of the opposite can be presented	News reporting and commentary; Parody Critics
Assets that can be proven to be copyright-protected	Product reviews, Comparative advertising, Compatibility claims
	Typosquat only domains
	Guides and other informational content

PhishFort's Guide to Effective Takedowns and Evidence Collection

INDEX:

WHY IS THE FIRST REPORT SO IMPORTANT?
WHAT CAN AND CANNOT BE TAKEN DOWN?
WHAT CANNOT BE TAKEN DOWN?
WHAT CAN BE TAKEN DOWN?
DOMAIN INCIDENTS:
QUICK SUMMARY OF MINIMUM EVIDENCE FOR ALL DOMAIN-RELATED CASES:
ICANN CONSIDERATIONS AND ESCALATIONS
UDRP (Uniform Domain-Name Dispute Resolution Policy)
EMAIL ATTACKS:
SOCIAL MEDIA PLATFORMS:
- FACEBOOK:
- X/TWITTER:
- TIKTOK:
- LINKEDIN:
- YOUTUBE:

PHONE-RELATED ATTACKS:
- SMISHING:
- PHONE SCAMS:

MESSAGING APPLICATIONS:
- WHATSAPP:
- TELEGRAM:
- DISCORD:

IP REPORTING
OTHER PLATFORMS
- GITHUB:
- GITBOOK:
- SCRIBD:

APK CASES:
BROWSER EXTENSIONS:
SEARCH ENGINES:

TRADEMARK & COPYRIGHT INFRINGEMENT AND FAIR USE DOCTRINE:
- Trademark and Copyright Definitions:
- What is a DMCA?
- What is the Fair Use Doctrine?
- What is TM or CR infringement?
- Trademark Infringement: most frequent cases and evidence required:
- Fake News:

SCAMS:

At PhishFort, we are committed to protecting your brand against phishing attacks and trademark or brand infringements. We aim to ensure your brand and your customers' safety online. With that, we created this guide that outlines the evidence required for different incident types. Your collaboration is invaluable in helping us build strong cases and submit effective takedown reports. By providing detailed evidence and context, you enable us to act swiftly and decisively against the threats posed by these incidents. Additionally, having this information will help us submit a complete first report quickly and limit any back-and-forth communication or unnecessary delays due to a lack of context.

WHY IS THE FIRST REPORT SO IMPORTANT?

Submitting a complete and detailed first report is critical to the success of any takedown request. A strong report with the necessary evidence increases the likelihood of resolving the issue on the first attempt, impeding scammers from benefiting from unnecessary delays and preventing business losses or reputation damage. On the other hand, incomplete or unclear reports can lead to rejections, delays, or the need to resubmit the case, prolonging the resolution process. However, it is important to note that in some instances—especially with complex phishing attacks—additional back-and-forth may be unavoidable to fully understand the context of the incident. By ensuring the initial report is thorough, we can streamline the process and achieve better outcomes. Together, we can safeguard your brand's reputation and minimize the impact of malicious activities.

WHAT CAN AND CANNOT BE TAKEN DOWN?

Before jumping into the evidence we need, let's review what can and cannot be taken down.

WHAT CANNOT BE TAKEN DOWN?

Although our mission is to protect brands and customers from cyberattacks, it is important to know that not all content can be taken down from the internet. Certain types of content are protected from takedowns, depending on jurisdiction and specific legal frameworks. Generally, we cannot perform takedowns of content that does not involve illegal activities or is considered trademark fair use. For that reason, before proceeding with a takedown, even if it is reported by the customer, our analysts need to determine whether it is a phishing case or a trademark/copyright infringement incident.

Here is a quick guide on common cases that cannot be taken down without additional signs of malicious activity:

- Empty websites with no typosquat.
- Parked domains with typosquat, as it is not being used for fraudulent activities or trademark infringement. Nevertheless, PhishFort can monitor these domains to act accordingly if content is uploaded to the website. Also, we have a list of registrars that agree to turn off even parked pages if asked, and typosquat is not generic
- Tutorial websites that clearly state they are not related to the customer providing guides to earn from ads is considered legal activity on the internet.
- Websites selling our clients' products that are genuine/original and do not counterfeit the First Sale Doctrine.
- All content in social media and websites that falls under the Fair Use doctrine. At the end of this playbook, you will find a section exclusively dedicated to Fair Use.
- Content that does not violate social media platform policies, even if the content is somehow harmful to the brand. For these cases, the more evidence you can provide, the better. That will allow us to analyze the case from different angles and find a possible platform policy violation that leads to content removal.
- Legit businesses with Trademark or Copyright disputes.
- Doxxing cases.
- Public Information or Information that is considered to be in the public domain.

- No typosquatting domains in which content is violating the Trademark. For these cases, we can get the content removed, but not always take down the website.

WHAT CAN BE TAKEN DOWN?

As you may know, a takedown is a request issued to an ISP, web host, social media company, domain registrar, or mobile app store operator to remove malicious or fraudulent content or domains abusing your company's brand. We will perform a takedown for a malicious domain using your brand (e.g., a phishing site), someone impersonating your brand, or an unauthorized mobile app mimicking one of your apps in an App Store or posted as a downloadable file on a website. Additionally, we can try to take down any content that targets your brand and violates specific platform rules.

Specific takedown types that we will cover in this guide:

- Domains: All domains with phishing content are susceptible to being taken down. However, domains with typosquatting alone are usually not taken down by Registrars as the website must contain malicious content or brand abuse to qualify for a takedown.
- Emails: We can facilitate the takedown of email addresses involved in any type of cyber attack or malicious activity, effectively disrupting their use and mitigating potential harm to our clients and their digital assets.
- Social media and messaging platforms: We can report and take down accounts with different types of infringements, such as Trademark violation, Copyright Abuse, or Impersonation. Each platform's policies will restrain what can or cannot be taken down in these incidents. However, our analysts are specialists in social media policies and will decide on the better approach for each case.
- Phone Numbers: We can execute takedowns of phone numbers involved in smishing/phishing over SMS cases.
- IP: We execute takedowns of infrastructure that hosts infringing content, diligently working to remove unauthorized material and safeguard intellectual property while ensuring compliance with legal and regulatory standards.
- Third-Party Apps: We can remove copies of legitimate apps, adware, mobile malware, or mobile app brand abuse.

- Other Platforms in general: anything that violates the policies of the specific platform and related to protecting the brand can be attempted as part of a takedown.

BULK REPORTING:

For certain social media platforms, we offer bulk reporting functionality, as long as the following criteria are met:

- They are using the same platform.
- They are targeting the same brand or person.
- The attack pattern should be similar or the same. For example, all of them are fake customer support.

Clients may submit up to 10 URLs in the same report. Some of the supported platforms are:

- Facebook
- Instagram
- Scribd
- GitBook
- Teachable
- Telegram

This list is not exhaustive. If you are unsure whether bulk reporting is supported for a specific platform, please contact PhishFort Support.

How to submit incidents in bulk:

When submitting an incident, you may include up to 10 URLs: one primary URL in the incident form plus up to nine additional URLs in the incident comments.

When creating the incident, select the incident type as social to ensure the report is processed under the correct workflow.

Please provide all available supporting evidence for the reported cases.

How we evaluate success:

- If at least one URL in the bulk submission is successfully actioned (takedown), the incident will be marked successful.

- If none of the URLs are successful, the incident will not be marked successful.

Our Operations team will notify you of any failed URLs. Failed URLs should be resubmitted in a new incident for another takedown attempt. Failed URLs cannot be reported in bulk again.

⚠️ **IMPORTANT:** Bulk reporting of domains is not available at this time. Do not include domain-level takedown requests in bulk social submissions.

DOMAIN INCIDENTS:

Attacks using malicious or deceitful domains are a great portion of what we deal with in the brand protection environment. For that reason, the first thing to consider when handling malicious or infringing domains is that a single domain can host multiple types of violations. Depending on the violation, the required evidence might change. In this guide, we aim to cover the minimum evidence that is generally required. This means that the analysts can contact you about a specific case, asking for further context or evidence. When reporting a domain incident, the most important thing you can provide is the steps to reproduce the attack (Live Proof), so our analysts can easily access the domain and gather further information if needed. For this, clients should provide:

1. Direct links with evidence of the infringement, such as a payment tracking number leading to a page with violations.
2. Screenshots showing phishing forms or other harmful content, including the full URL and visible date/time.
3. Context about the case, such as how it was discovered, where it was found, device, location and any other relevant details.
4. If there is suspicion that the attack is geo-fenced, please also provide the browser, location, and device from which the attack was observed.

Types of Domain-Related Incidents

1. **Website Brand Impersonation:**
    a. This occurs when the domain pretends to be the victim's brand, for example, by claiming to be the "official" website.
    b. Evidence required:
        i. Screenshots of the webpage showing brand assets and the full URL.
        ii. Screenshots of any statements from the attacker claiming to represent the brand.
2. **Email Attacks Using Similar Domains:**
    a. It’s crucial to differentiate between:

i. Malicious domains registered specifically for attacks. i.e., sup port@exampleattack.com - takedown will be performed against the domain rather than through the Registrar.
ii. Attacks that are carried out through legitimate mail service (e.g., sup portbrand@gmail.com). - takedown will be performed against the account through the platform (e.g., Gmail)

b. Evidence required:
i. Email headers (mandatory). Please refer to the email section of the guide for further information.
ii. Screenshots of the email (optional).

3. **Typosquats or Similar Domains Only:**
a. Typosquats (domains that mimic legitimate ones to gain legitimacy) are an aggravating factor in impersonation cases, but typosquats alone are not enough to execute a takedown.

QUICK SUMMARY OF MINIMUM EVIDENCE FOR ALL DOMAIN-RELATED CASES:

1. Full URL. i.e.: www.example.com/attack1/brand2
2. Screenshots showing (preferable): The infringement (ideally phishing forms or harmful content). Date, time, and full URL.
3. Case description (context, how it was found, any other relevant details).
4. Location, device, and browser used to observe the attack.

Once submitted, an analyst may contact you for additional details if necessary.

ICANN CONSIDERATIONS AND ESCALATIONS

ICANN (Internet Corporation for Assigned Names and Numbers) is a regulatory body for many of the most common Top-Level Domains (TLDs), such as .com, .org, .net. However, ICANN does not cover country code TLDs (ccTLDs) such as .sa, .ru, .fr, .io. and some of TLDs. It is possible to escalate a regulated Registrar that is being unresponsive to ICANN.

ICANN Considerations and Timeline:

To escalate a case to ICANN

- The domain must involve any type of clear infringement that violates Registrar policies, with evidence of phishing or clear impersonation (e.g., screenshots, URLs, or other relevant details).
- The case must have been reported through the corresponding methods assigned by each Registrar.
- A minimum waiting period of at least 72 hours must have passed since the initial report.

Once escalated, ICANN will attempt to contact the registrar up to three times, waiting 15 days for a response after each communication, before issuing a Notice of Breach.

For ICANN escalations, the average resolution time is approximately one month. ICANN is treated as the last resort in domain-related escalations. If ICANN is unable to resolve the issue, alternative measures such as UDRP (Uniform Domain-Name Dispute Resolution Policy) or legal action may need to be pursued.

UDRP (Uniform Domain-Name Dispute Resolution Policy)

https://www.wipo.int/amc/en/domains/guide/#What_is_the

The UDRP is a legal framework for resolving disputes between domain name registrants and third-party trademark owners over abusive registration and use of Internet domain names. A UDRP has an additional cost, and the official procedures involved require specific information about TM disputes over domains. Key factors:

- No money back on failure.
- It takes significant effort to fill submissions and maintain communication compared to regular takedowns.
- The procedure takes time, between 14-30 days.
- Requires TM registration.
- It requires that the domain include TM, requires proof of unfair usage of the domain, or at least unfair intent.

EMAIL ATTACKS:

To execute takedowns of phishing emails or malicious email addresses, we need the original email headers. Every single Internet e-mail message is made up of two parts: the header and the body of the email. Every single email you send or receive on the Internet contains an Internet Header, a full and valid e-mail header provides a detailed log of the network path taken by the message between the mail sender and the mail receiver(s) (email servers).

Your email client program will usually hide the full header or display only lines, such as From, To, Date, and Subject. But that's not the only important information contained in email headers. Additionally, every time you forward an email, email headers are replaced with new ones. Please for more information on how to obtain them, follow this Email Headers Guide.

SOCIAL MEDIA PLATFORMS:

Social media platforms can vary significantly in their level of cooperation when handling takedown requests. While some may act swiftly on clear evidence of phishing or malicious activity, others may require extensive documentation and context to act. We would like to stress that our requests for specific evidence are not arbitrary but rather the result of carefully tested approaches aimed at increasing the likelihood of success. Our ultimate goal is to take down every reported case, and this requires building strong, well-supported reports. As a general rule, we execute takedowns for all social media platforms available. However, if you report a very specific platform that we are not able to support you with, we will let you know and provide optional courses of action. In this guide, you will find the minimum evidence required for virtually all social media platforms and some specifications for the most popular social media platforms: Facebook, X/Twitter, TikTok, Instagram, and LinkedIn.

KEY EVIDENCE FOR ALL SOCIAL MEDIA PLATFORMS:

- Letter of Authorization (LOA): It is the document that allows PhishFort to act on behalf of the client and proceed with Trademark / Copyright / DMCA infringement cases. This document is often requested by authorities, especially by social media platforms, to ensure that someone is not trying to take down legitimate accounts or domains trying to harm a brand/business. We will ask for the original URLs protected by us, the company registration number and jurisdiction, and registration numbers and jurisdictions of copyrights and trademarks. If we are protecting associated brands, we encourage them to be included in the LOA. The more complete the document is, the better chances we have to achieve a successful takedown.
- Detailed Explanation of the Infringement: Context is crucial to report the correct type of infringement. For that reason, having a good understanding of the case is of utmost importance for our analysts, so they can evaluate the case and submit a compelling report. Sending just a link or an image without explanation will not suffice.

- The original brand or executive profile on the reported social media platform: (if available). It is useful as it helps us prove which is the real profile being impersonated. If we have this profile, the takedown time is expected to be shorter and the success rate higher.

FACEBOOK:

When dealing with Facebook cases, it's important to consider the option of obtaining a direct link to the infringement. This can be highly beneficial depending on the situation at hand. For instance, if you're reporting impersonation, the URL of the fake profile may be sufficient. For reporting comments or posts, providing a direct link is advisable. In cases involving comments, it is particularly useful to hide the reported comments and share the link instead of deleting them, as this makes the evidence more accessible to the platform's authorities. If obtaining a link isn't possible, please ensure that you provide a screenshot that clearly shows the infringement.

Key evidence for Facebook incidents includes:

- Letter of Authorization (LOA).
- A legitimate profile for impersonation cases (optional).
- The URL of the profile, post, or comment, or a screenshot of the infringement.
- Context related to the case

IMPORTANT! *Unofficial, automatically generated Facebook business location pages are not infringements, as they are clearly marked as unofficial and are not used for malicious activity. Therefore, they cannot be taken down.*

X/TWITTER:

Choosing the right form for X/Twitter cases is crucial. To evaluate the situation effectively and select the form with the best chance of success, we need your help in explaining the details of the case. A thorough description can make a significant difference and expedite the takedown process by minimizing back- and forth communication.

Note for Impersonation Cases: X/Twitter has a clear and strict definition of impersonation that must meet at least two of the following criteria:

- Display name (the username is not taken into consideration)
- Profile description
- impersonating post (please provide a link to the message when reporting).

If these criteria are not met, they will reject the takedown.

Key Evidence for X/Twitter Incidents Includes:

- Letter of Authorization (LOA).
- A legitimate profile (optional for impersonation cases), Context, and a brief description of the case
- Screenshots or proof of impersonation if the logo is not visible on the fake account (only for impersonation cases without the brand's logo).

TIKTOK:

For TikTok, it is important to know that they will not act on reports for profiles with a brand's name. They will only act on accounts with an infringing post that does not fall under the Fair Use doctrine. Without a post, takedowns cannot be executed.

Key Evidence for TikTok Incidents Includes:

- Letter of Authorization (LOA).
- A legitimate profile (mandatory). If that profile doesn't exist, please let us know. We can execute the takedown but with a different process and escalation system.
- Link to the infringing TikTok post.

LINKEDIN:

LinkedIn takedown cases often require detailed evidence and context to ensure a successful resolution.

Types of Violations: Cases generally fall into two categories:

1. False Information: Incorrect details in the "Experience" section, such as false employment claims.

2. Scams: Individuals impersonating someone else or fraudulently associating themselves with a company.

Key Evidence for LinkedIn Incidents Includes:

- Location of the Infringement: Identify where the violation occurs (e.g., a specific section of the profile or company page).
- Nature of the Harm: Explain who is affected and how the content is causing damage.
- Reason for the Report: Provide a concise explanation of why the content affects your brand so we can link it with a violation of LinkedIn's policies (e.g., impersonation, fraudulent claims).
- Letter of Authorization (LOA).
- Direct Link to the Profile/Page: Include the exact URL of the content being reported.
- Impersonation Proof: Indicate who the individual is impersonating. Ideally, link to the real profile or page of the person or company being mimicked.
- If the impersonation involves a client employee, we might need proof of employment.

Specific Cases Important to Consider:

1. Pre-Made Pages: The platform rejects takedown attempts of pre-made pages. So, we advise that instead of reporting a pre-made company page, claim ownership through LinkedIn's process for associating a page with the primary company profile.
2. False Information: LinkedIn allows the removal of false details in the "Experience" section, such as fraudulent claims of employment. Important Note: Descriptions in profiles cannot typically be removed.
3. Individual posts: These are not typically taken down unless explicit violation of LinkedIn's content guidelines (e.g., phishing or malicious content).
4. Scam or Impersonation: Highlight how the profile or page is pretending to be someone or falsely claiming association with a company.

YOUTUBE:

For YouTube cases, you must take into account that the evidence required will vary depending on the type of attack you are facing.

Key Evidence for YouTube Incidents According to the Type of Attack Includes:

1. Phishing:
    a. Link to the legitimate account being impersonated, if possible.,
    b. URLs with videos showing the impersonation (if possible). In case there are too many videos, posting just some examples will help as well.,
2. Scams:
    a. Link to the videos performing the scams.,
    b. Explanation on how the scam scheme works and how it is affecting your brand (if applicable).
3. DMCA:
    a. Link to the video infringing the DMCA.
    b. If the infringement is a specific part of the video, the timestamp of the part of the video showing the infringement.,
    c. An explanation of how the video infringes your copyrights.
    d. Letter of Authorization to act on behalf of the brand being impersonated.
4. Trademark infringement:
    a. Link to the video or account infringing your trademarks.,
    b. If the infringement is a specific part of the video, the timestamp of the part of the video showing the infringement.,
    c. Trademark registration for the word being infringed.,
    d. Letter of Authorization to act on behalf of the brand being impersonated.

PHONE-RELATED ATTACKS:

SMISHING:

Key Evidence for Smishing Incidents Includes:

- Sender number (preferable).
- Receiver number.
- Date, time of the SMS. Time zone.
- The text or screenshot of the SMS.
- Brief description of the attack (if possible).

PHONE SCAMS:

Key Evidence for Phone Scam Incidents Includes:

- Caller number.
- Receiver number.
- Screenshot of the phone call with the date and time.
- Time zone.
- Brief description of the call/attack.

MESSAGING APPLICATIONS:

To ensure we can assist you effectively with reporting messengers, please include a clear statement indicating your intention. For example, specify if you would like to take down a WhatsApp account or provide the URL of the account. This helps us avoid any confusion and act efficiently.

These should be reported as “Social” incidents.

WHATSAPP:

Key Evidence for WhatsApp Incidents Includes:

- Letter of Authorization (LOA).
- Phone Number: Provide the phone number involved in the infringement in the format wa.me/phone_number.
- Important: Sharing the contact directly (e.g., via a vCard or "Share Contact" option) is not sufficient for reporting.
- Screenshots with Evidence: clear screenshots that capture the infringement (e.g., messages impersonating the client or malicious activity).

IMPORTANT! *Screenshots showing group member lists or participant details do not necessarily strengthen the case if the rest of the evidence is not provided.*

TELEGRAM:

Telegram presents some unique challenges when performing takedowns, as it often ignores standard infringement reports. In general, the platform only takes quick action in cases involving severe violations, such as illegal content. We execute Telegram takedowns and we analyze the specific cases from all angles, looking for a positive resolution. However, brand impersonation or phishing reports are generally low-priority unless overwhelming evidence is provided.

Key Evidence for Telegram Incidents Includes:

<u>Message:</u>

- Link to the message.
- Screenshots: Provide screenshots showing undeniable evidence of the violation. If possible, ensure the messages include timestamps and dates to contextualize the infringement.
- Context about it.
- Legitimate account being impersonated (if possible).
- LOA.

Channel:

- Link to the Channel.
- Context about it.
- Legitimate account being impersonated (if possible).
- LOA.

Group:

- Link to the group.
- Context about it.
- Legitimate account being impersonated (if possible).
- LOA.

IMPORTANT: Overall success rates for Telegram vary depending on the type of infringement, quality of evidence, and how the reported infringement violates Telegram's fair use policies. Telegram operates with a very loose enforcement mandate, which our team continuously manages and files escalations for on behalf of our customers.

DISCORD:

Discord presents unique requirements for takedown cases due to its structure, where users, messages, and servers all have distinct identifiers.

Key Evidence for Discord Incidents Includes:

- User, Message, and Server Information:

- User ID: Obtain the User ID by right-clicking on the user's profile, selecting the three dots, and choosing "Copy ID."
- Message Link: Provide the direct link to the specific message causing harm. To copy the link, right-click the message and select "Copy Link."
- Server ID: Copy the Server ID by logging into the infringing server. Screenshots: Include screenshots of the infringing content. If possible, ensure the screenshots include visible timestamps, usernames, and the context of the infringement. Context Explanation: Describe how the reported activity causes harm.

How to Obtain Relevant IDs and Links:

- Go to the specific user, message, or server causing the issue.
- Right-click on the element (e.g., user profile or message), then select the three dots and click "Copy Link".
- This is an example of how a message ID would look like: https://discord.com/channels/XXXXXXX/YYYYYYY/ZZZZZZZ 1. XXXXXXX is the Server ID. 2. YYYYYYY is the Channel ID. 3. ZZZZZZZ is the Message ID.

IMPORTANT! *You must be part of the server to collect the necessary details. Ensure your access is active to retrieve the message links and IDs.*

IP REPORTING

Reporting IPs requires extra care and detailed evidence due to the complexities of their use. Many IP addresses host multiple websites, and not all of them may be malicious. For this reason, domain-level takedowns are usually more effective than targeting entire IPs, as entire IP takedowns are challenging and often result in rejection due to the collateral impact on unrelated websites.

Key Evidence for IP Incidents Includes:

- Specific URL Evidence: If possible, always provide a specific URL associated with the malicious activity hosted on the IP address.

- Detailed Explanation of the Issue: Describe how the reported content is harmful or infringing and include proof of malicious activity, such as phishing, malware, or impersonation attempts.
- Entire IP reporting: Avoid reporting entire IPs unless absolutely necessary, as they often host multiple unrelated and legitimate websites.

Domain vs. IP Considerations: If the same domain is used across multiple IPs, prioritize reporting the domain rather than the IPs, as when a TLD is taken down, it cannot change IPs to be up again.

IMPORTANT! *Cases involving malware or sensitive content (e.g., NSFW material) demand heightened attention and should be flagged clearly. Please, let our analysts know when you are reporting such cases.*

OTHER PLATFORMS

GITHUB:

Key Evidence for GitHub Incidents Includes:

- Type of Attack: Specify the nature of the attack (e.g., phishing, exposure of credentials, or other brand infringement).
- File Containing the Infringement: Provide the exact file name where the infringing content is located.
- Location of the Evidence: Include the repository path and file location (e.g., repository name and folder structure). This is for brand infringement cases, as maybe not the whole repository is infringing.
- Lines of Code: Specify the exact lines of code or content within the file that contain the infringement. This is for brand infringement cases, as maybe not the whole file/code is infringing.
- Context/Incident Explanation: Briefly explain why the identified content is infringing on your brand or intellectual property.

GITBOOK:

Key Evidence for GitBook Incidents Includes:

- Full URL
- A brief explanation of the context of the attack.

SCRIBD:

Key Evidence for Scribd Incidents Includes:

- The name of the company that's being impersonated.
- The suspicious URLs: these are of utmost importance.
- Files titles, meaning, according to Scribd articles, "Enter titles of copyrighted material being infringed upon and, if possible, additional identifying information such as

ISBNs, publication dates, etc — or, if the material is a web page, the URL where the original can be found."

- TM registration numbers and/or documents would also be helpful, especially when sub-brands are targeted.

APK CASES:

An APK is an app hosted outside official distribution platforms like the Google Play Store or Apple App Store. These apps are typically hosted on third-party websites, but there are instances where malicious apps may appear on official platforms as well. We can take down APK incidents from official distribution platforms and third-party websites. It is important to note that, regardless of where the app is hosted, APK cases are treated as DMCA takedowns. This means we do not require trademark registrations as evidence. Instead, we need proof of copyright violation and verification of the relationship between the client and the brand being infringed. APK takedowns often require more back-and-forth communication, as these apps are not always inherently malicious. In some cases, they are distributed to provide compatibility for older devices and may not directly violate any policies. This makes proving infringement more challenging and highlights the importance of showing a clear relationship between the client and the reported brand.

Key Evidence for APK Incidents Includes:

- Letter of Authorization (LOA).
- Proof of Copyright Violation: Evidence that the client's copyright is being infringed.
- Client Relationship Evidence:
    - If the case involves a sub-client of a PhishFort partner, we need additional proof of a legal relationship between our partner and the end customer. This is because the platform hosting the app must confirm we are authorized to act on our reseller and their customer's behalf.
    - If we have to proceed with a case involving a sub-brand of a global/parent company, a single reference to the parent company is sufficient. For example, the mention of the parent company somewhere in their website/official app.
- Malicious APKs: for these cases, we must demonstrate that the APK is malicious. For example, if there is a phishing behavior, we need screenshots of instances where the app asks for sensitive information, such as cryptocurrency wallet credentials or banking details.

- If screenshots are unavailable, please provide the link to the original APK for investigation.

We work with you to protect your intellectual property and remove harmful APKs quickly and effectively. Your support in providing detailed evidence, authorizations, and context is critical for building strong cases.

IMPORTANT: *In general, for these cases, the takedown is performed on the file itself by removing it. However, the informational page might not be taken down and may remain active.*

BROWSER EXTENSIONS:

Key Evidence required for Browser Extension Incidents includes:

- Clear evidence of copyright infringement using proprietary code without authorization, such as:
    - Screenshots showing brand misuse (logo, brand name).
    - Screenshots of the extension in action (e.g., login form, phishing behavior).
    - Link to the extension in the Chrome/Edge/Firefox store.

GOOGLE ADS IMPERSONATIONS AND MALICIOUS LANDING PAGES:

PhishFort can carry out takedowns for malicious ads and landing pages.

To proceed, they have to be submitted as two separate incidents: one for the ad and another for the landing page.

Key evidence for malicious ads and landing pages includes:

- Ad URL
- Landing page URL
- A screenshot of the search results showing impersonation

Additional evidence that helps strengthen the case includes:

- The date and time the ad appeared
- GCLID values or IP addresses associated with the attack.

SEARCH ENGINES:

Reporting Search Engine Cache Incidents

When unwanted or malicious content continues to appear in search results—even in a cached form—you can request removal of those cached versions as an extra mitigation. Cached data is a stored version of a webpage that loads faster, but may show outdated or removed content, as it's not consulting online data to show it.

How Cached Removal Works

Before a search engine will remove a cached page, the content must actually be unavailable on the live site (for example, the original page returns a 404 or has been previously taken down/deleted).

Search engines like Google use bots (called crawlers) to discover and index content across the web. When a page is updated, deleted, or fixed, the crawler may recrawl it to refresh its data. This process isn't instant—it can take days or even a week depending on the site's popularity, crawl frequency, and other factors. Recrawling is especially important when trying to remove outdated or malicious cached content from search results.

Some browsers or search engines offer a way to "speed up" cache removal by submitting a cache-specific report.

Key evidence for search engine incidents

- The exact URL as it appears in the search results.
- The search engine name (e.g., Google, Bing).
- The cached-page URL (if available).

Important: Please report each cached link as a separate incident (one URL = one incident), even if the same search term appears across multiple engines.

TRADEMARK & COPYRIGHT INFRINGEMENT AND FAIR USE DOCTRINE:

At PhishFort, we protect your brand not only from malicious activity but also from TM and CR infringements. To better understand the scope of our services on these matters, let's go through some concepts together ;)

Trademark and Copyright Definitions:

A trademark is a distinctive symbol, phrase, or word that identifies a particular product or service. It serves to legally distinguish one offering from others in the marketplace while also acknowledging the ownership of the brand by the respective company. This differentiation is important for both consumers and businesses, as it helps ensure quality and brand integrity. The trademark registration protects your brand to selling products or services.

On the other hand, Copyright "is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings." (Source: https://www.wipo.int/en/web/copyright).

To summarize, a copyright protects creative expressions, while trademarks protect brand identity. For DMCA takedowns, only copyright-related claims are applicable.

What is a DMCA?

The Digital Millennium Copyright Act (DMCA) is a U.S. law enacted in 1998 to address copyright protection in the digital age. It provides a framework for copyright holders to request the removal of infringing content from websites, platforms, or digital services. It also protects service providers from liability if they promptly respond to such requests. While the DMCA is specific to the U.S., many countries have adopted similar laws under the WIPO Copyright Treaty (for more information, please refer to

https://www.wipo.int/treaties/en/ip/wct/), which the DMCA implements in the U.S. One example of this would be the European Union, with the EU Copyright Directive regulating digital copyright and providing guidelines for handling infringing content.

These laws may differ in procedures and enforcement, but share the goal of balancing copyright protection with innovation and user rights.

What is the Fair Use Doctrine?

The fair use doctrine allows limited use of copyrighted material without permission for purposes such as criticism, commentary, news reporting, education, or research. It balances the rights of copyright holders with the public interest by considering factors like the purpose, nature, amount used, and impact on the market value of the original work. The fundamental consideration of Fair Use is that it shouldn't cause any confusion to the users/customers, meaning, there isn't brand impersonation involved.

Following "Trademark Lawyer Firm"'s definition, "Fair use" is a term in trademark law that means using a mark in such a way that it will not infringe upon the owner's rights. A common defense in trademark infringement litigation, fair use provides that a party may use a protected mark not as an actual trademark, but rather, for its descriptive meaning. Specifically, there are two types of fair use: classic fair use and nominative fair use.

Classic Fair Use involves using a trademark to describe goods or services without indicating their source. This is done with the intent to help prevent monopolies on descriptive terms, making it easier for others to use such words that describe products or services.

Nominative Fair Use allows the use of another's mark to identify their goods or services when they cannot be easily identified otherwise. For example, media outlets may refer to a trademarked name for reporting purposes, provided there's no false affiliation suggested. This type of Fair Use is the most common.

When Does Trademark Fair Use Apply?

Fair use applies when the mark is used in good faith without causing consumer confusion. Common scenarios include:

- News Reporting: Referring to a trademark in news stories or commentary is allowed, as long as the information provided is accurate.
- Product Reviews: Mentioning a brand name is necessary to identify a product for review, even if it is a criticism of the product/service.
- Parody: Parody uses of trademarks are protected by the US law and many other countries' legislation, as they typically don't confuse consumers.
- Comparative Advertising: Ads that compare products can include trademarks as long as they are non-deceptive.
- Compatibility Claims: Stating a product's compatibility with another brand qualifies as nominative fair use.
- Identifying Customers: Using a partners logo in marketing is allowed if only as much of the logo as necessary is used.

(Source: Trademark Lawyers Firm).

As a general guide, follow the following:

Fair Trademark Usage:

To qualify as Fair Trademark Usage, it is necessary that:

- The use of the plaintiff's trademark must be necessary to accurately describe their goods or services.
- Only the amount of the trademark that is essential for description should be used.
- How the trademark is used must reflect the true relationship between the user and the plaintiff.

Nominative Trademark Usage:

To qualify as a nominative trademark usage, the following elements must be present

- The usage must accurately refer to the trademark owner or the goods/services sold under the trademark, and it cannot be misleading or defamatory.
- The usage must not suggest that there is any endorsement or sponsorship by the trademark owner.

- There must be no alternative way to refer to the owner or their products that is easier than using the trademark.
- Only the amount of the trademark necessary to identify the owner should be used, and no more.

What is TM or CR infringement?

Copyright Infringement occurs when a copyrighted work is used, reproduced, or distributed without permission. These types of infringement are addressed under the DMCA or equivalent laws.

Trademark Infringement occurs when a trademark is used without permission in a way that causes confusion about the source of goods or services. These cases usually require evidence of consumer confusion and are not typically covered under the DMCA. These infringements are all uses of Trademark that are not "Fair" or "Nominative" use nor are brand impersonation.

Trademark Infringement: most frequent cases and evidence required:

To recap, TM infringement occurs when a party uses a mark or symbol in a way that is likely to confuse consumers about the source, sponsorship, or affiliation of goods or services. Apart from Brand Impersonation, the following are common types of TM infringement:

- Counterfeiting: The unauthorized use of a trademark on identical or nearly identical goods to deceive consumers into believing they are purchasing genuine products.
- Dilution: Using a famous trademark in a way that weakens its uniqueness, even if there is no direct competition or confusion. Unauthorized Use in Advertising or
- Marketing: Using a trademark without permission to promote a product or service, often creating a false endorsement. Infringing Use of a Trademark on Goods or
- Services: Using a similar mark on related goods or services to confuse consumers about their origin.

Key Evidence for TM Infringement cases includes:

1. Ownership of a Valid Trademark: Provide TM registration documents.
2. Likelihood of Confusion: We need to prove how the unauthorized use of the mark is likely to mislead consumers.
3. Harm Caused by the Infringement: Evidence of reputational damage, financial loss, or consumer complaints.

We want to help you protect your Trademark, that's why our SOC team may reach out to build proper documentation and clear explanations together, as they are crucial for successfully addressing trademark infringement cases.

FAKE NEWS:

In cases involving suspected fake news, it is important to note that such material is often hosted on legitimate news platforms and distributed across multiple credible sources. Based on prior experience, requests to remove this type of content are generally declined by hosting providers and authorities unless supported by compelling legal documentation.

Takedown efforts for news articles and editorial content are typically only successful when one of the following conditions is met:

- Verifiable evidence demonstrating that the content is clearly false or misleading.,
- A court order issued by a competent legal authority mandating the removal of the content.,

Due to the sensitive nature of press freedom and editorial standards, hosting providers and platforms tend to reject takedown requests that do not meet these criteria. While we aim to assist to the fullest extent possible, prior attempts to remove similar content without sufficient legal backing have not yielded positive outcomes.

We advise clients to consult with their legal teams to assess the possibility of pursuing a court order. This approach offers the most reliable path to achieving content removal in fake news cases.

Key Evidence for Fake News or Misleading Editorial Content Includes:

- Fact-based rebuttal or correction from a credible source, demonstrating that the claims in the article are false or misleading.
- Official statements or press releases from the client or relevant authorities disproving the reported information.
- Screenshots or archives of the article, including timestamps, to preserve the version in question.
- Evidence of harm or damage caused by the article, such as reputational damage, financial loss, or legal consequences.
- Statements from affected individuals (e.g., company representatives) refuting the content.

- Court order or legal opinion stating that the content constitutes defamation or misinformation under applicable law.,

Copyright Infringement:

Most frequent cases and evidence required:

Summarizing, Copyright Infringement occurs when someone uses copyrighted material without the owner's permission or legal justification. There are several types of infringements, and they might require different evidence.

Please find the most common below:

- Unauthorized Reproduction or Distribution: Copying, sharing, or distributing copyrighted material without permission.
- Plagiarism or Verbatim Copying: Using copyrighted text, images, or other creative works without attribution or authorization.
- Unauthorized Public Performance or Display: Performing or displaying copyrighted material without permission.
- Derivative Works Without Permission: Creating and distributing a modified version of copyrighted material.
- Software Piracy: Copying, distributing, or using software without proper licensing.
- Unauthorized Use of Online Content: Using copyrighted content on websites, blogs, or social media without permission.
- Copyright Infringement in Visual Media: Using photos, designs, or other visual content without permission.

Key Evidence for Copyright Infringement cases includes:

- Ownership of the Copyrighted Material: Registration certificate or other proof of authorship.
- Proof of Infringing Material: Evidence of unauthorized use, reproduction, or distribution.
- Substantial Similarity: Demonstrate how the infringing work is substantially similar to the original.
- Absence of Authorization: Show that the infringer had no license or permission to use the material.

IMPORTANT! *We can take action against any infringements as long as they do not fall under the Fair Use Doctrine. Understanding what is or isn't covered by the Fair Use Doctrine is a collaborative process between our analysts and you. We will always strive to act on your requests. However, if there is no evidence of infringement in the materials you provide, we will explain why we cannot take action and ask if you have any additional evidence.*

We want to help you protect your Copyright, which is why our SOC team may reach out to build proper documentation and clear explanations together, as they are crucial for improving our chances of successful enforcement.

SCAMS:

A scam incident occurs when a website or its content appears legitimate, but the advertised service is not. Simply put, if you pay for a coffee but receive only water or nothing at all, that is a scam. In general, scams do not target our customers directly, but they can still be affected by them. To take action against a scam, we require proof or evidence of the purchase of a service or goods, along with documentation showing that it was not delivered as promised. We understand that obtaining this proof can be challenging, which limits our possible courses of action and might affect our ability to take those down.

Key evidence for Scam incidents includes:

- Context describing the scam.
- Evidence of the purchased services or goods. Specifically, the text used to scam contains a clear payment ask.
- Proof that the agreement was not completed.

Cyber threats are constantly evolving, and so are we. This playbook is a work in progress, and we will periodically share updates to help you protect your brand and ensure a smooth, collaborative takedown process. We hope you find this information useful.