

Federal Bureau of Investigation
Internet Crime Complaint Center (IC3)
www.ic3.gov

Subject: Phishing Complaint – USPTO Impersonation

Complaint Type: Phishing / Impersonation of U.S. Government Agency (USPTO)

I am submitting a report regarding a phishing email that impersonates the United States Patent and Trademark Office (USPTO) and attempts to induce recipient action under the pretense of a required verification process.

Email Details:

Date received: April 27, 2026

Recipient: llc@musclefitdynamic.com

Display name: "Uspto.gov"

Actual sender address: no-reply@teauspto.org

Reply-To address: teas@lawoffice105gov.us

Subject line: "Notice of Required Verification - USPTO Trademark Application"

Summary of Content:

The email claims that a USPTO trademark application requires immediate verification and instructs the recipient to initiate a call with an "Examining Officer" within a specified time window. It includes a reference number and uses formal language intended to appear official. The message is generic ("Dear Applicant") and does not reference any verifiable USPTO record or official communication channel.

Technical Analysis:

The sender domain "teauspto.org" is not affiliated with the USPTO (official domain: uspto.gov).

The Reply-To address uses a separate unrelated domain.

The email was transmitted using Zoho mail infrastructure (sender4-op-o16.zoho.com, IP 136.143.188.16).

SPF, DKIM, and DMARC checks passed for the domain, indicating the sender controls it.

The message identifies a bulk mailing system ("AxeMail Mail Engine").

Assessment:

This is a purpose-built phishing domain, not a compromised real USPTO system.

It was intentionally created to impersonate USPTO communications.

The sender is traceable to:

- a domain registration account
- a Zoho email account

However, the sender is not directly traceable to a real identity from header data alone without further investigation.

Indicators of Phishing:

- Lookalike domain impersonating a federal agency
- Mismatch between From and Reply-To domains
- Instruction to initiate contact via phone
- Generic salutation and lack of verifiable details
- Use of third-party mail infrastructure

User Impact:

No interaction was made. No links clicked. No data shared.

Attachments / Evidence:

Full email headers and PDF copy of the email.

Purpose of Report:

To document fraudulent impersonation of a U.S. government agency and assist in identifying patterns or infrastructure involved in similar campaigns.