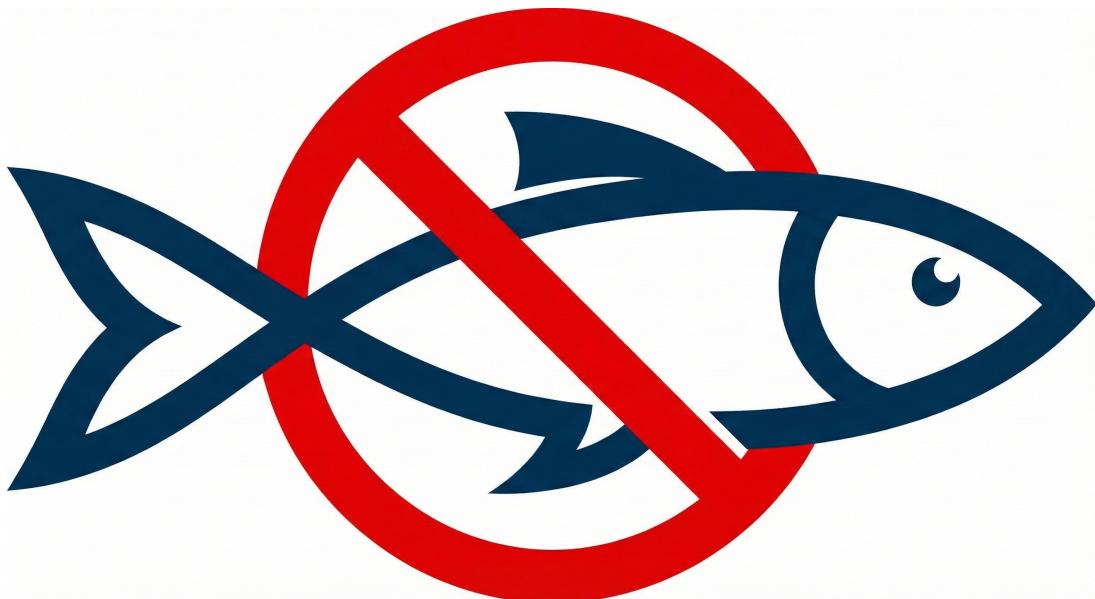


Manuale Utente: BlockDaFish Analizzatore Anti-Phishing

Guida Operativa all'Uso del Software

Autore: Josh Van Edward Abanico

Progetto: <https://github.com/joshvanedwardabanico/BlockDaFish>



Indice

1	Introduzione	2
2	Preparazione e Avvio dell'Applicativo	2
3	Fase 1: Estrazione del Sorgente Email	3
3.1	Recupero dati da ambiente Gmail	3
4	Fase 2: Esecuzione dell'Analisi	4
4.1	Inserimento dei Dati in BlockDaFish	4
4.2	Elaborazione tramite AI	4
5	Fase 3: Interpretazione dell'Esito	7
5.1	Esito Critico: Possibile Phishing	7
5.2	Esito Negativo: Email Sicura	7

1 Introduzione

Il presente documento costituisce il manuale d'uso ufficiale per **BlockDaFish**, un software di analisi automatizzata ideato per mitigare il rischio di attacchi Phishing. L'applicativo sfrutta l'integrazione con l'intelligenza artificiale (modello Gemini) per esaminare il codice HTML e gli header di posta elettronica, fornendo un responso immediato sulla legittimità della comunicazione.

2 Preparazione e Avvio dell'Applicativo

Per iniziare, avviare lo script Python dell'interfaccia grafica `BlockDaFishGUI.py` dall'ambiente virtuale preconfigurato. Una volta lanciato, si aprirà la dashboard principale dell'Analizzatore Anti-Phishing.

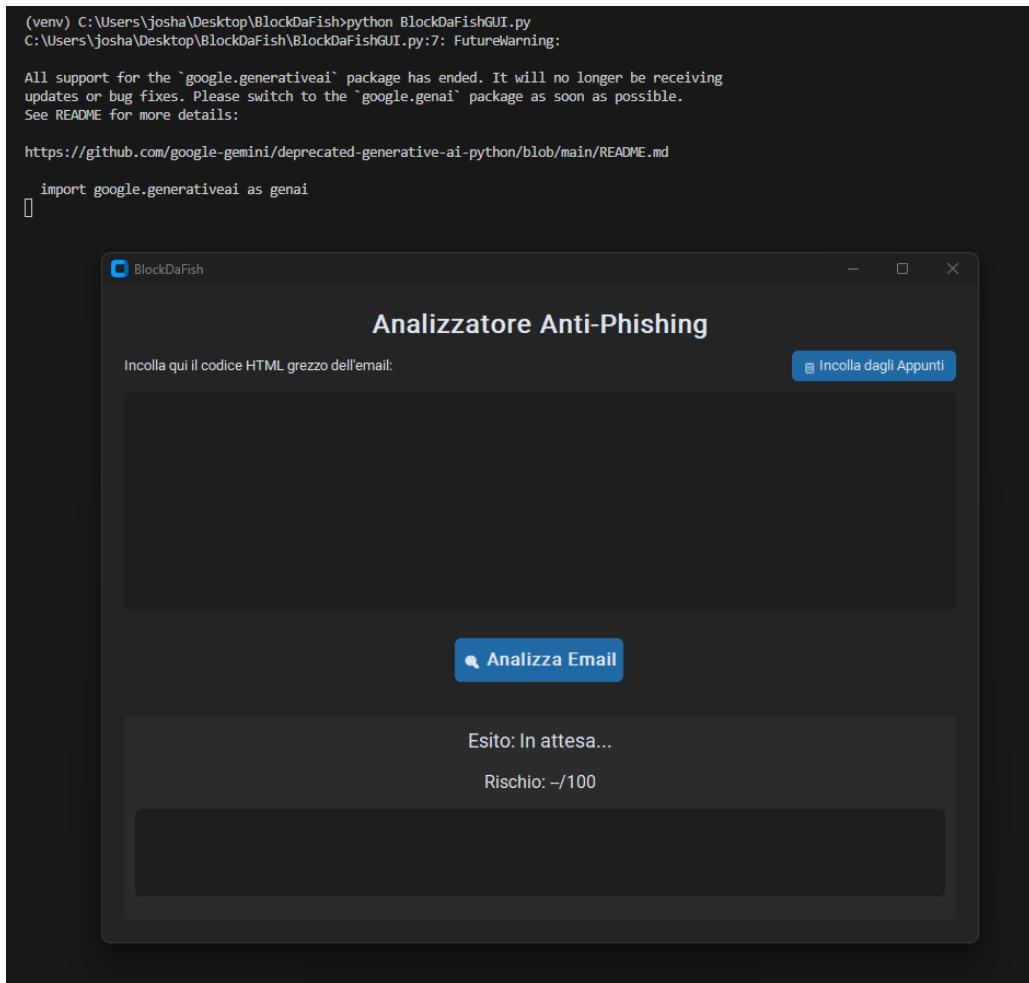


Figura 1: Terminale in esecuzione e interfaccia principale di BlockDaFish in attesa di input.

3 Fase 1: Estrazione del Sorgente Email

Per consentire al sistema di analizzare parametri tecnici vitali come firme DKIM, record SPF e DMARC, è fondamentale acquisire il messaggio in formato "grezzo" (originale).

3.1 Recupero dati da ambiente Gmail

Accedere alla propria casella di posta e aprire l'email classificata come sospetta.

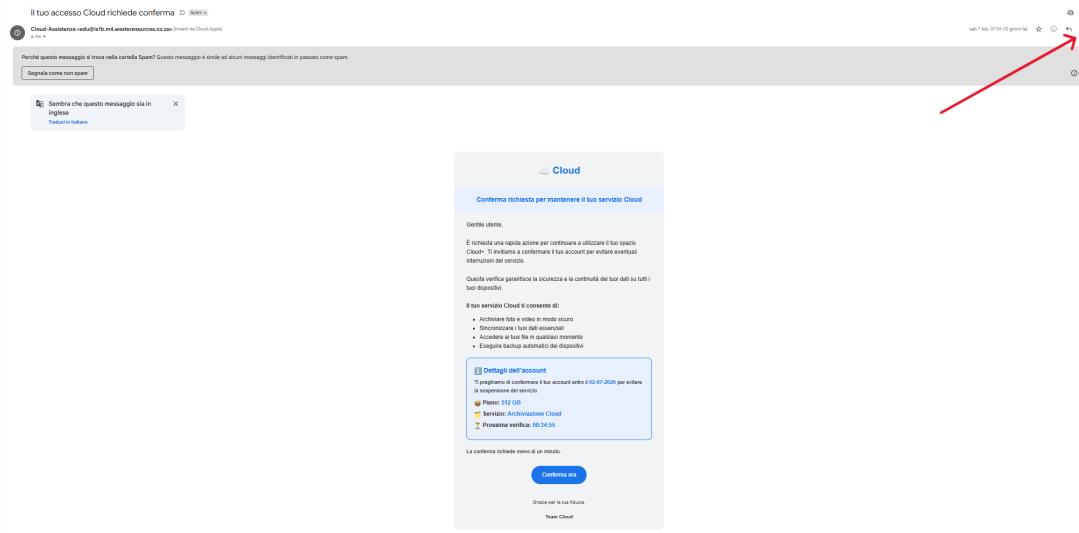


Figura 2: Individuazione dell'email sospetta all'interno del client di posta.

Fare clic sul menu delle opzioni contestuali (rappresentato dai tre puntini verticali in alto a destra) e selezionare la voce "**Mostra originale**".

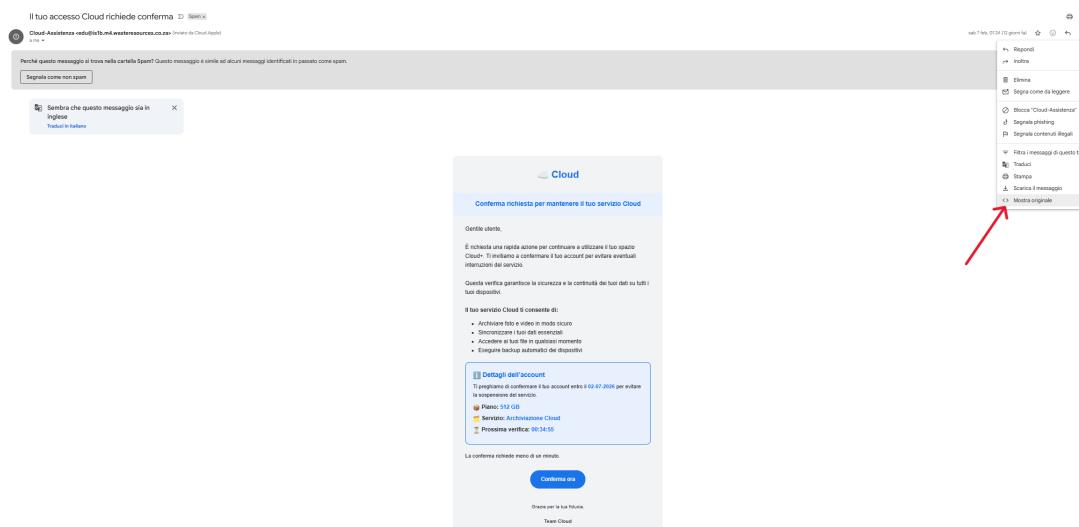


Figura 3: Selezione della funzione per l'esposizione degli header di rete.

Il browser aprirà una nuova scheda contenente l'ID del messaggio, i log di recapito e il corpo del testo grezzo. Cliccare sul pulsante blu "**Copia negli appunti**" per acquisire l'intero blocco di dati.

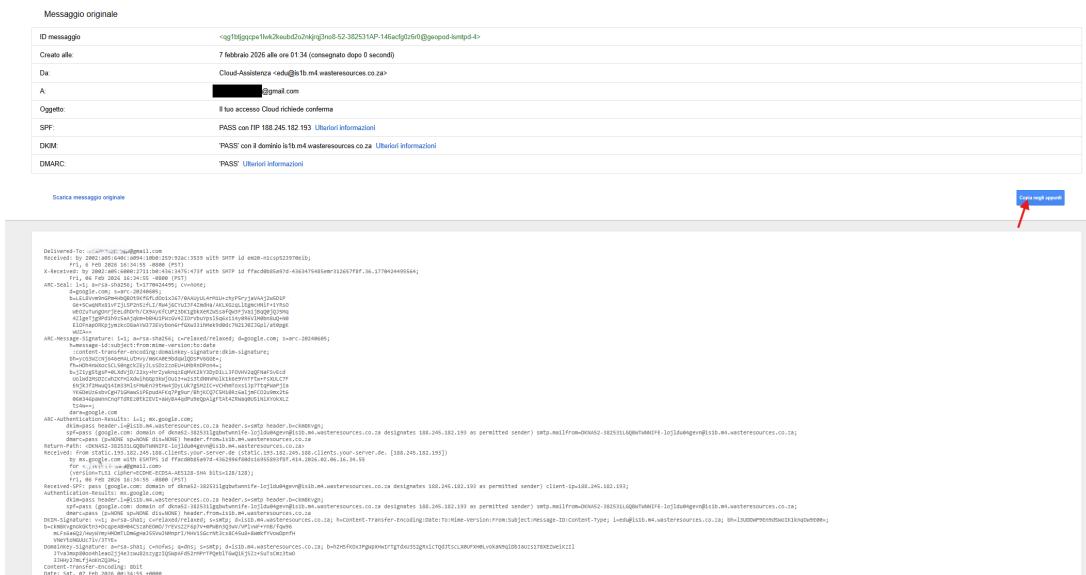


Figura 4: Acquisizione del payload email tramite appunti di sistema.

4 Fase 2: Esecuzione dell'Analisi

4.1 Inserimento dei Dati in BlockDaFish

Ritornare alla finestra dell'applicativo BlockDaFish e cliccare sul pulsante "**Incolla dagli Appunti**". Il testo sorgente popolerà automaticamente l'area di testo centrale.

4.2 Elaborazione tramite AI

Avviare la routine diagnostica cliccando su "**Analizza Email**". L'interfaccia si aggiornerrà bloccando ulteriori input e mostrando il caricamento "Analizzando i dati tramite Gemini...". In questa fase, il sistema sta valutando le discrepanze semantiche e strutturali della mail.

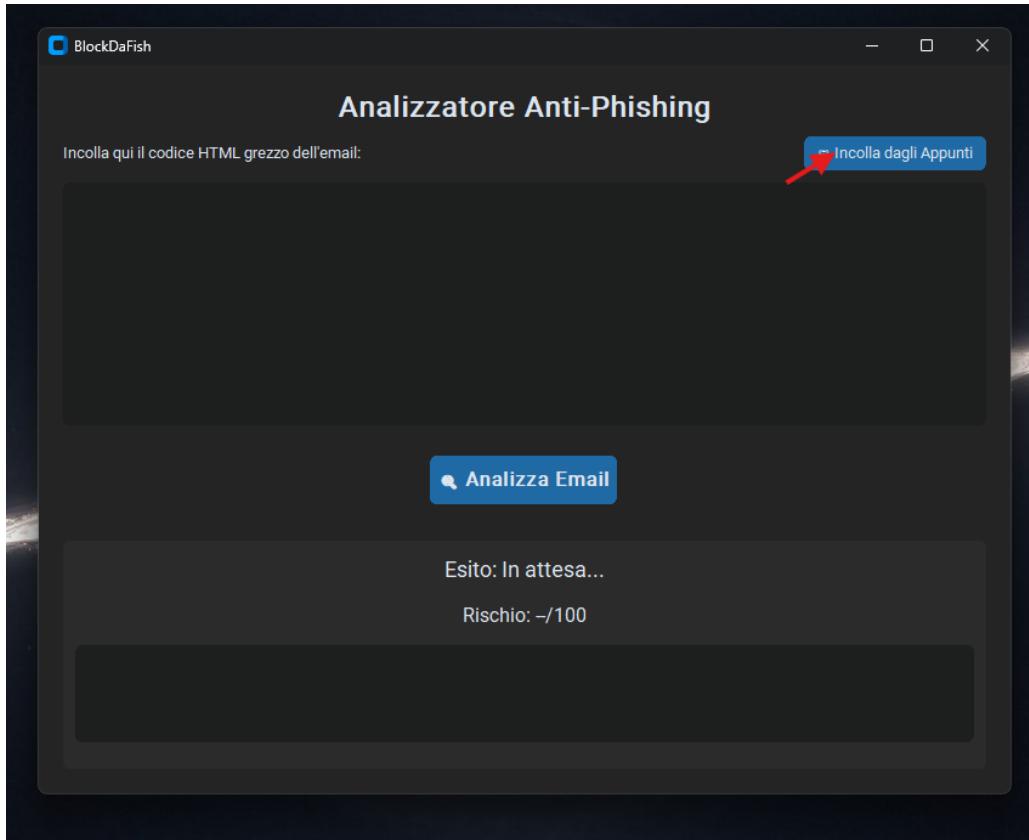


Figura 5: Inserimento rapido tramite il pulsante apposito.

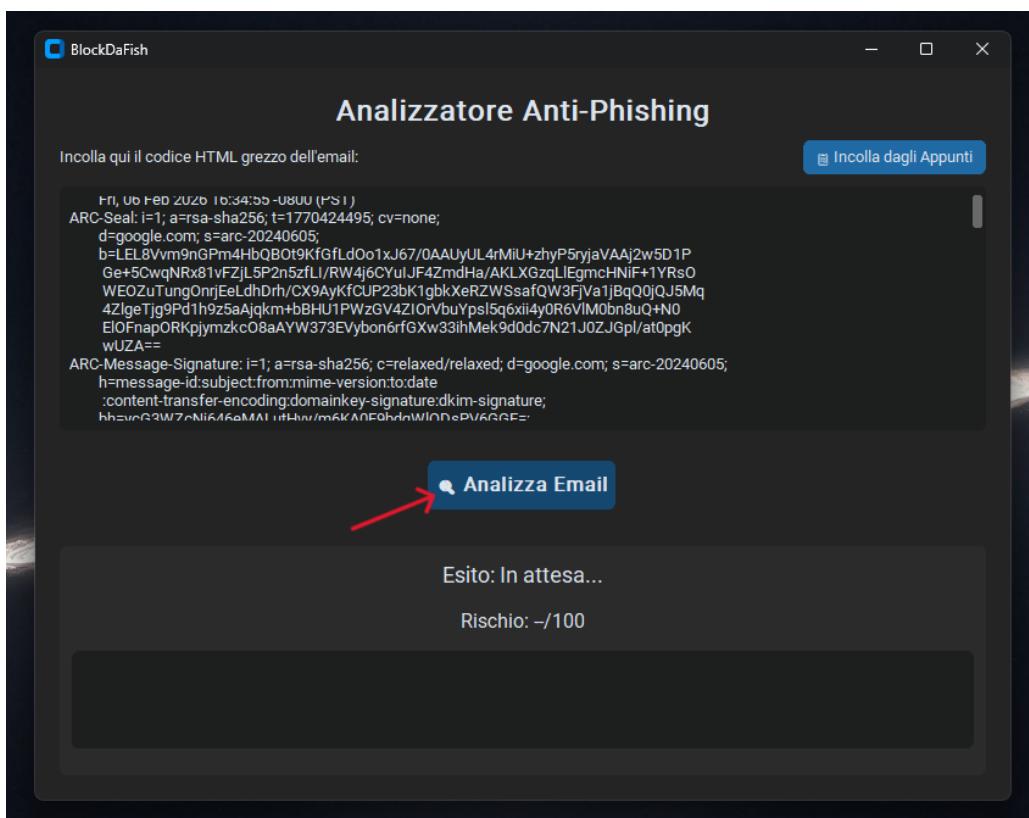


Figura 6: Avvio dell'analisi del codice HTML e Header.

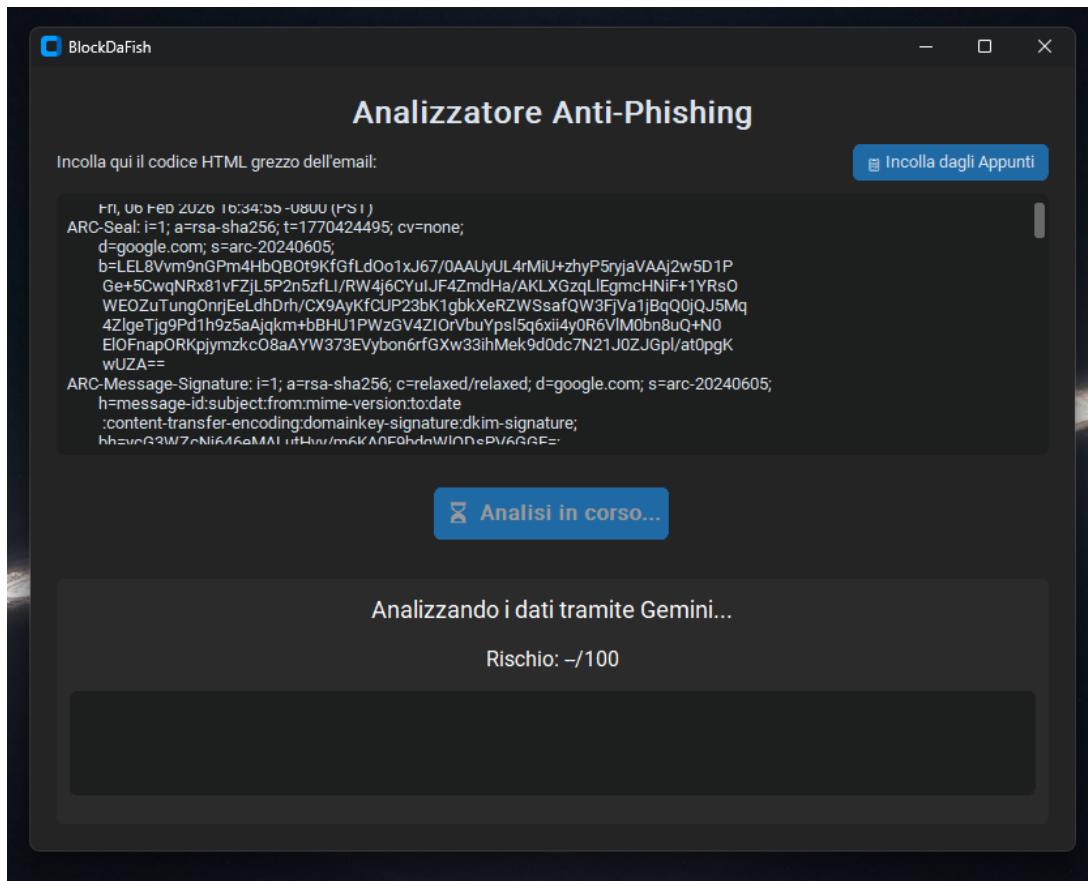


Figura 7: Stato di attesa durante la consultazione del modello Gemini.

5 Fase 3: Interpretazione dell'Esito

Al termine dell'analisi, BlockDaFish emetterà un verdetto quantificabile con un indicatore di rischio e una dettagliata motivazione testuale.

5.1 Esito Critico: Possibile Phishing

Nel caso in cui l'email presenti segnali di compromissione, l'interfaccia si colorerà di rosso. L'esempio riportato mostra un **Rischio: 100/100**. La motivazione tecnica generata indicherà le tecniche rilevate, come domini mittenti non correlati ai servizi citati, tecniche di offuscamento "word salad" o link fraudolenti rivolti a bucket di archiviazione generici.

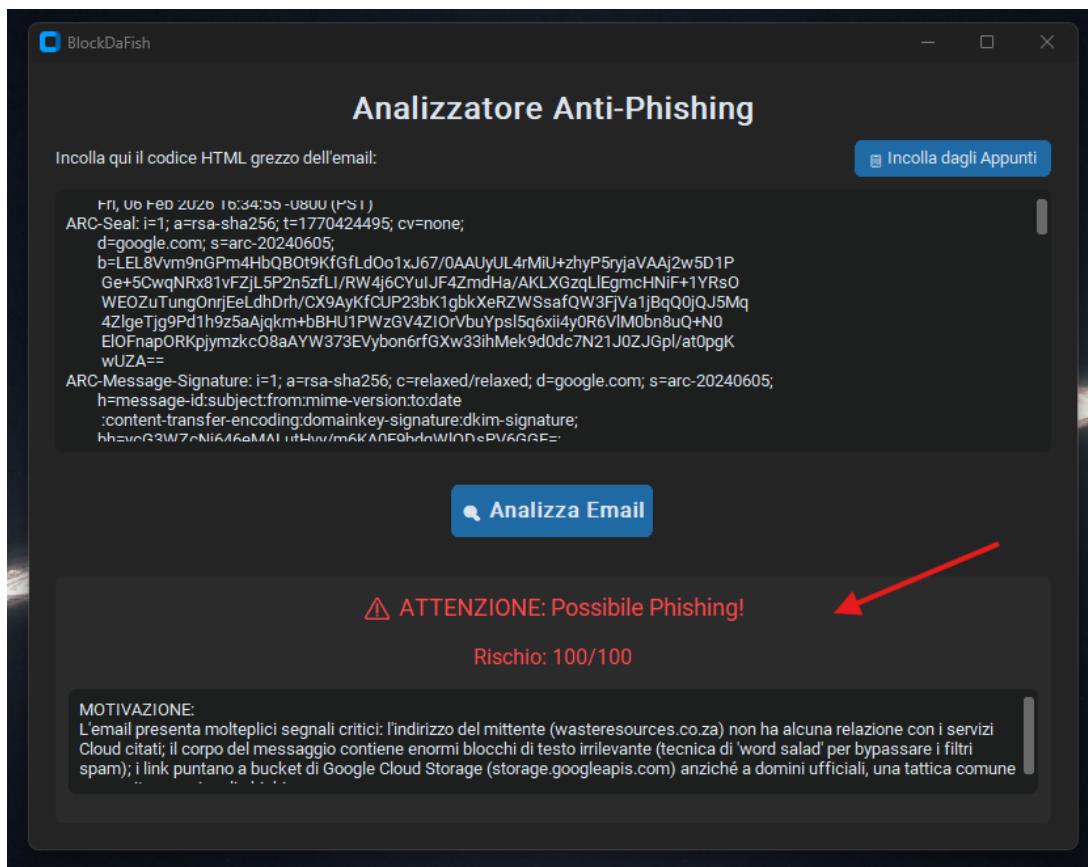


Figura 8: Riscontro positivo a una minaccia: Alert rosso e motivazione dettagliata.

5.2 Esito Negativo: Email Sicura

Se l'analisi attesta l'autenticità del messaggio, l'interfaccia restituirà un alert verde. L'esempio mostra un **Rischio: 5/100**. La motivazione confermerà la validità dei record SPF, DKIM e DMARC e verificherà che l'invio tramite server accreditati sia una pratica standard e sicura per quel dominio.

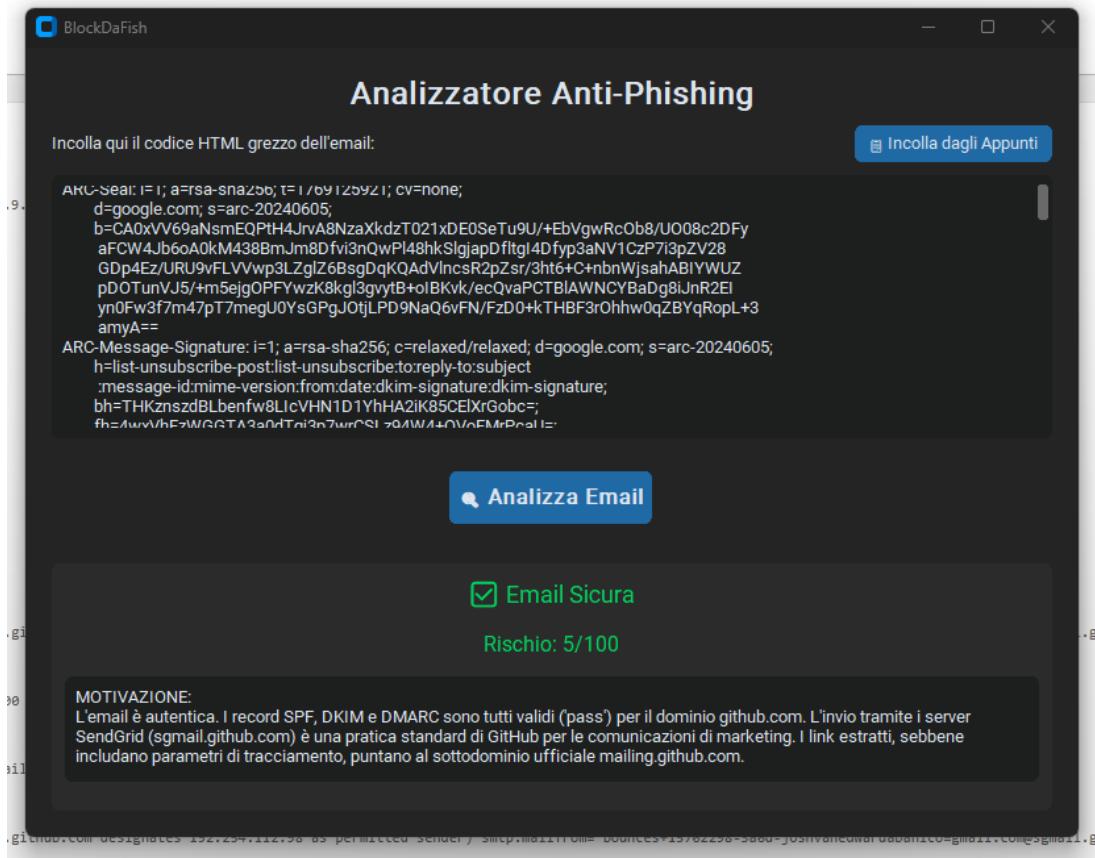


Figura 9: Riscontro di email legittima con validazione dei protocolli di sicurezza.