Analizza il mittente

Controlla sempre l'indirizzo email completo, non solo il nome visualizzato. I truffatori spesso usano indirizzi simili a quelli legittimi (ad esempio "paypa1.com" invece di "paypal.com"). Se il mittente è sospetto o non ti aspettavi un'email da quella fonte, diffida.

Nei sorgenti della mail (Ctrl-U) verificare l'intestazione "Received:"

```
Return-Path: <Admin@verlata.it>
X-Original-To: gbarichello@verlata.it
Delivered-To: gbarichello@verlata.it
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=verlata.it;
    s=default; t=1758010243;
    bh=WFinekvhbbXS5x2kSf4ZqWJf0aVHDqew9Y4uUYH2Ah4=;
    h=From:To:Subject:Date:From;
    b=lu0iMPcb7dM8HA+CmXIGjqYGek2DPIExaAnQVr3avZMLfcirs73NYv5cXF0HARGfE
     qIa8aLyma+xEWqPLbrnF41oUvH/ollMqKo5+2qZFL7pJPWulF9wBBp3gfVsSP1FR7Q
     F70pbp/hwoQFa32chRoJukBCZlJEbt3uad+Jlfwo7LuR7IkIwl7lsV6mRQE00JAroG
     XhpIbtiGjO7wQ4KxjOXgDDvxaBIuBYz30bB5vRioTCH4XpzwHvBvuVhfrw1PtOPb7v
     ClHycjU1oI5pKIdIMDzl8MPq7GwiKU6z93VAdT/tFBcf7ur6KqBix2eJ/tP4+0WJIY
     V9vyIxjyRZqRA==
Received: from localhost (localhost [127.0.0.1])
    by mail1.verlata.it (Postfix) with ESMTP id 0A95CA064E
    for <gbarichello@verlata.it>; Tue, 16 Sep 2025 10:10:43 +0200 (CEST)
X-Virus-Scanned: Debian amavis at verlata.it
Received: from mail1.verlata.it ([127.0.0.1])
 by localhost (takanuwa.verlata.it [127.0.0.1]) (amavis, port 10024)
 with ESMTP id 5PJlxj5HINkz for <gbarichello@verlata.it>;
 Tue, 16 Sep 2025 10:10:42 +0200 (CEST)
Received-SPF: Softfail (mailfrom) identity=mailfrom; client-ip=94.156.175.82; helo=light.kolsea.com; envelope-from=admin@verlata.it; receiver=verlata.it
Received: from light.kolsea.com (light.kolsea.com [94.156.175.82])
    by mail1.verlata.it (Postfix) with ESMTPS id 71466A0643
    for <gbarichello@verlata.it>; Tue, 16 Sep 2025 10:10:42 +0200 (CEST)
From: Admin@verlata.it
To: gbarichello@verlata.it
Subject: =?UTF-8?B?Tm90aWZpY2EgSGVscERlc2s6IFNjYWRlbnphIGRlbGxhIHBhc3N3b3JkIG9nZ2kg4oCTIEF6aW9uZSByaWNoaWVzdGEgfHwg?=verlata.it || HelpDesk IT
Date: 16 Sep 2025 07:31:14 +0300
Message-ID: <20250916073114.4E75FA0715E148CF@verlata.it>
MIME-Version: 1.0
Content-Type: text/html;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

Cerca segni di urgenza artificiale

Le email fraudolente spesso creano **pressione psicologica** con frasi come:

- "Verifica il tuo account entro 24 ore"
- "Azione richiesta immediatamente"
- "Il tuo account verrà bloccato"
- "Confermami i dati entro oggi"

I servizi legittimi raramente richiedono azioni urgenti via email.

Esamina i link e gli allegati

- **Non cliccare su link direttamente**. Passa il mouse sopra per vedere l'URL effettivo (spesso non corrisponde al testo visibile)
- I link legittimi dovrebbero portare a domini ufficiali (es. "amazon.it", non "amaz0n-verify.com")
- **Non aprire allegati da mittenti sconosciuti** o inaspettati
- I file .exe, .zip, .scr, .img sono particolarmente rischiosi
- Verifica gli allegati e i link su https://www.virustotal.com

---

Riconosci errori linguistici e di formattazione

Le email di phishing spesso contengono:

- **Errori di grammatica e ortografia** (soprattutto se la lingua non è quella del servizio)

- Loghi sfocati, pixelati o mal formattati
- Layout disordinato o strano
- Font incoerenti

Le aziende serie controllano la qualità prima di inviare.

Attenzione alle richieste di dati personali

Nessun servizio legittimo ti chiederà mai via email:

- Password
- Numero di carta di credito
- Codice PIN o OTP
- Dati bancari
- Numero di conto

Se ricevi una richiesta simile, è **sempre una truffa**.

Verifica l'autenticità in modo indipendente

Se ricevi un'email da un servizio che usi:

1. **Non cliccare i link nell'email**
2. Accedi al sito direttamente dal browser (digitando l'URL o cercandolo su Google)
3. Contatta il servizio tramite i numeri ufficiali nel loro sito
4. Verifica se hanno effettivamente inviato comunicazioni

Proteggi il tuo account

- **Attiva l'autenticazione a due fattori (2FA)** quando disponibile
- Usa **password uniche e complesse (= lunghe)** per ogni account
- Mantieni **aggiornato il software** antivirus
- Configura **filtri anti-spam** nella tua casella di posta

Cosa fare se sospetti una truffa

- **Non rispondere** all'email
- **Non cliccare link** né aprire allegati
- **Segnala come spam/phishing** nel tuo programma di posta.
- Se hai cliccato un link, segnala all’Amministratore di Sistema e **cambia le password** dei tuoi account importanti
- Se hai condiviso dati sensibili, **contatta immediatamente il servizio** interessato