Analyzing a Phishing Email Sample

MX TOOLBOX®
🏠 SUPERTOOL ▾

Pricing · **Tools** · Delivery Center · Monitoring · Products · Blog · Support · Login

SuperTool · MX Lookup · Blacklists · DMARC · Diagnostics · Email Health · DNS Lookup · **Analyze Headers** · All Tools

Header Analyzed

Email Subject: VACAY PLANNING? 10% on FITS THAT HIT 😍

❮ Analyze New Header

Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool
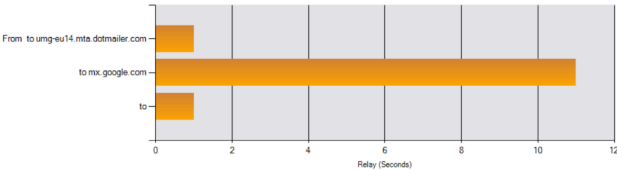
Delivery Information

- ❌ DMARC Compliant
  - ✅ SPF Alignment
  - ✅ SPF Authenticated
  - ✅ DKIM Alignment
  - ❌ DKIM Authenticated

Relay Information

Received Delay:	10 seconds

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*		umg-eu14.mta.dotmailer.com		10/10/2025 1:30:45 PM	
2	10 seconds	umg-eu14.mta.dotmailer.com 212.1.219.128	mx.google.com	ESMTPS	10/10/2025 1:30:55 PM	✅
3	0 seconds		2002:a05:7010:ea0a:b0:4b4:f842:72f	SMTP	10/10/2025 1:30:55 PM	

SPF and DKIM Information

dmarc:india.umusic-online.com   Hide   Solve Email Delivery Problems

```
v=DMARC1;p=none;rua=mailto:N4rHXmBVPY@dmarc.inboxmonster.com;fo=0;adkim=r;aspf=r;rf=afrf;pct=100;
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:N4rHXmBVPY@dmarc.inboxmonster.com	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
fo	0	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ':'.
adkim	r	Alignment Mode DKIM	Indicates whether strict or relaxed DKIM Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).
aspf	r	Alignment Mode SPF	Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).
rf	afrf	Forensic Format	Format to be used for message-specific failure reports. Valid values are 'afrf' and 'iodef'.
pct	100	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.

	Test	Result	
❌	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	ℹ️ More Info
✅	DMARC Record Published	DMARC Record found	
✅	DMARC Syntax Check	The record is valid	
✅	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	
✅	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	

Reported by **ns2.dns.dotmailer.co.uk** on 10/27/2025 at **11:22:30 AM (UTC 0)**, just for you.   Transcript

---

spf:india.umusic-online.com:212.1.219.128 [Show] [Solve Email Delivery Problems]

```
v=spf1 include:spf.dotmailer.com -all
```

---

dkim:india.umusic-online.com:dkim2048 [Show]

Dkim Public Record:

```
v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxWU2LF5mifrU+t+pCThYr5BUVN35N7LDeTqa4Px+zpSWQR72oEO+lpm1KugHrTjebLdT5QGhmK0BrSAeh34M4SrSo0HbuwEYZ6HT9OaV5qEdQ+0yKVcfz
```

Dkim Signature:

```
v=1; a=rsa-sha256; c=relaxed/relaxed; s=dkim2048; d=india.umusic-online.com; h=From:To:Subject:Message-Id:Date:List-Unsubscribe:List-Unsubscribe-Post: Reply-To:MIME-Version:Conten
```

Headers Found

Header Name	Header Value
Delivered-To	jagannadhulapalli@gmail.com
X-Google-Smtp-Source	AGHT+IFYnYO5TIDvjtFNrFwOsY4ampAETGpKOxUCxu9OmZJst/7nVqP21hGjl8TuJuEi7wppklMJ
X-Received	by 2002:a05:6214:29cd:b0:772:4853:48 with SMTP id 6a1803df08f44-87b21002ac1mr151670676d6.8.1760103055293; Fri, 10 Oct 2025 06:30:55 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1760103055; cv=none; d=google.com; s=arc-20240605; b=ZgZ1rrgEuDdcqg/jMcKEumklonssaW6YO9k7uAyzupGgJgfj6sfJEHOHmx17Iw45c/ z6BK6Oq3Fg/KV2M6Y9KGJoaOddLhxPE U4mujSvEmPtu9Llch6iiITwVQkz6l9PUy2zfp eapd98o5lFHkxC5DIup/2+nF4W+6lF3h+KJnd8tlP24BfvA9PNWwfwSz5eTPCOgxoncf Hl5tNux6sBuAGO3p8OSORzSDpEQEOBSoBXk/6lZvpoFvEN9YHRjjcGkm kyDIVuCpIfzc E4iEC7sAPgsn/RdlY1cu1vJTqnzT4V5rl1lBbmsuVzwzGKzukKSyvxIrjNWjU2d6y27v nkdQ==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=mime-version:reply-to:list-unsubscribe-post:list-unsubscribe :feedback-id:date:message-id:subject:to:from:dkim-signature :dkim-signature; bh=8DDHfchYe7Vp7ddQI7FMNXexBAX9V1QsMbLTE9flqG4=; fh=nOqFG6QS306sJRpSu3DbmTlDbtiu3K2sMbdzZxQ4i9U=; b=Mzvs63hny/Wxvm/JJtDVN2yPHctG/BDwmcM2vYiQT+AhdSYDlVyjV2fTQ +ZyUqyizJ fa+7Xk3+wHIdSOhJTrOWM3KMAogxQID0W///CN8VXnWaruGmVHlmtlphXS+WernjXiwuJL evKiOJNUtBr9/XT1g+7N1UYfC9RoG5+/RAqnpdYJP6fbQApADi6lyj34bqNJ8mGJcP1y hNdalkjzgrtRl2H 05epwRZE7PXYa3mqM3mXr6qaTlaciAOx1+C1F8a0fOlhkXqqjLbwa /tlSXCap4TM4zvc4Q+shzEOULaSQyEb6wnPaViu7jl8cuc23VlciP9zl32s8hTvGrthg fv+w==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@india.umusic-online.com header.s=dkim2048 header.b=EeR5lnMt; dkim=pass header.i=@dkim.dotmailer.com header.s=dkim1024 header.b=oAoemqyX; spf=pass (google.com: domain of bo-4ytj-hknf-9jq4n8-c21sg@india.umusic-online.com designates 212.1.219.128 as permitted sender) smtp.mailfrom=bo-4YTJ-HKNF-9JQ4N8-C21SG@india.umusic-online.com; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=india.umusic-online.com
Return-Path	<bo-4YTJ-HKNF-9JQ4N8-C21SG@india.umusic-online.com>
Received-SPF	pass (google.com: domain of bo-4ytj-hknf-9jq4n8-c21sg@india.umusic-online.com designates 212.1.219.128 as permitted sender) client-ip=212.1.219.128;
Authentication-Results	mx.google.com; dkim=pass header.i=@india.umusic-online.com header.s=dkim2048 header.b=EeR5lnMt; dkim=pass header.i=@dkim.dotmailer.com header.s=dkim1024 header.b=oAoemqyX; spf=pass (google.com: domain of bo-4ytj-hknf-9jq4n8-c21sg@india.umusic-online.com designates 212.1.219.128 as permitted sender) smtp.mailfrom=bo-4YTJ-HKNF-9JQ4N8-C21SG@india.umusic-online.com; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=india.umusic-online.com
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; s=dkim2048; d=india.umusic-online.com; h=From:To:Subject:Message-Id:Date:List-Unsubscribe:List-Unsubscribe-Post: Reply-To:MIME-Version:Content-Type; x=1760362255; i=news@india.umusic-online.com; bh=8DDHfchYe7Vp7ddQI7FMNXexBAX9V1QsMbLTE9flqG4=; b=EeR5lnMtGnfen75o2lRAWCuGRR3EUQCszbTiuxSCnshwIOGW7tYg4O0YGC+BOT9Hhetb0aH0 GOdm DVfPoG7LH+Pf9011A7a64q2nwjrJJ8L6D+Bho4l0wrSf/FeHOhTal+2eC6wPyPVfTQG0P2Ti5tNh xXTyFoqUkkeFXqlcFaoBopYjRKqtbOacJrvjZ/6YjQudKeoeDSOD5a0SVuLZcN4aiO7GC484Z5CS 46k8 Kgz6Tn3d7Lz5pBUdS1SHdn/azpHiSXV2yoJ1Au84gzl6a8aU6ND654Fp2WMdAM4niAnY7WHo Z4SD3xXbRZEa4l0m5yVV1lhVBKg/cCWGFNiRXg==
From	Universal Music India <news@india.umusic-online.com>
To	jagannadhulapalli@gmail.com
Subject	VACAY PLANNING? 10% on FITS THAT HIT 💯