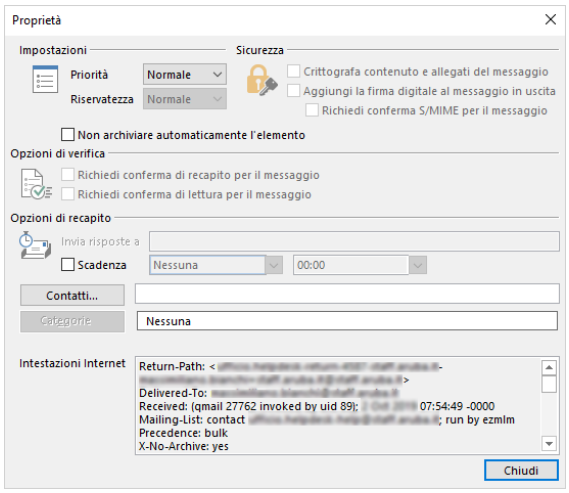
ANALISI DELLE E-MAIL

Quando si sospetta la ricezione di messaggi contraffatti, il modo migliore di verificarne la reale identità è quello di leggere le informazioni di autenticazione, una procedura comunemente conosciuta come “Autenticazione mail”.

Questo tipo di operazione consiste nel rintracciare il reale mittente (indirizzo IP) del messaggio di posta, analizzando gli header dell’email ricevuta.
Per visualizzare gli header è necessario accedere alle proprietà della mail ricevuta, operazione fattibile da ogni programma (client) di posta elettronica.

Ora vediamo come fare:

Visualizzazione degli header mediante Microsoft Outlook

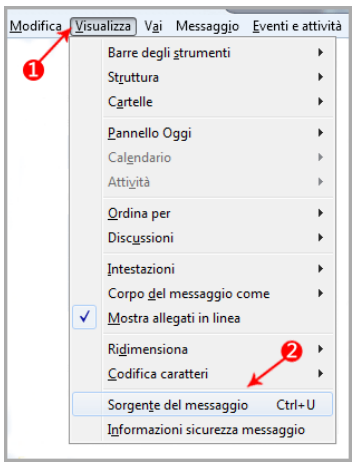


Per visualizzare gli Header con il Client di posta di Microsoft Outlook fare doppio clic su un messaggio di posta elettronica per aprirlo all'esterno del riquadro di lettura, poi cliccare il menu File e poi su Proprietà.

Le informazioni di intestazione vengono visualizzate nel box Intestazioni Internet

Visualizzazione degli header mediante Thunderbird

Per visualizzare gli Header di un messaggio tramite il Client di posta Mozilla Thunderbird, selezionare il messaggio e poi selezionare la voce di menu Visualizza, poi fare click su Sorgente del messaggio.
Si apre quindi una finestra con gli header del messaggio.



Altri client di posta

AOL

- Accedi al tuo account AOL.
- Apri l'email di cui vuoi visualizzare le intestazioni.
- Nel menu "Action" (Azione), seleziona View Message Source (visualizza origine messaggio).

Le intestazioni verranno visualizzate in una nuova finestra.

Webmail di Excite

- Accedi al tuo account Excite.
- Apri l'email di cui vuoi visualizzare le intestazioni.
- Fai clic su View poi su Full Headers (visualizza intestazioni complete).

Le intestazioni verranno visualizzate in una nuova finestra.

Hotmail

- Accedi al tuo account Hotmail.
- Fai clic su Inbox (posta in arrivo).
- Fai clic con il pulsante destro del mouse sull'email di cui vuoi visualizzare le intestazioni.
- Fai clic su View Message Source (visualizza origine messaggio).

Le intestazioni verranno visualizzate in una nuova finestra.

Yahoo! Mail

- Accedi al tuo account Yahoo! Mail.
- Seleziona l'email di cui vuoi visualizzare le intestazioni.
- Fai clic su More (Altro) poi View Raw Message (visualizza messaggio non elaborato).

Le intestazioni verranno visualizzate in una nuova finestra.

Mail di Apple

- Apri Mail di Apple.
- Apri l'email di cui vuoi visualizzare le intestazioni.
- Fai clic su View (Visualizza) poi Message (Messaggio) a seguire All Headers (tutte le intestazioni).

Le intestazioni verranno visualizzate nella finestra sotto la Posta in arrivo.

Mozilla

- Apri Mozilla.
- Apri l'email della quale si vogliono visualizzare le intestazioni.
- Fai clic su View (visualizza) poi Message Source (sorgente messaggio).

Le intestazioni verranno visualizzate in una nuova finestra.

Opera

- Apri Opera.
- Fai clic sull'email di cui vuoi visualizzare le intestazioni per fare in modo che si apra nella finestra sotto la posta in arrivo.
- Fai clic con il pulsante destro del mouse sul corpo dell'email.
- Fai clic su View All Headers and Message (mostra tutte le intestazioni del messaggio).

Le intestazioni verranno visualizzate nella finestra sottostante.

Outlook

- Apri Outlook.
- Apri l'email di cui vuoi visualizzare le intestazioni.
- Fai clic su File Proprietà.

Le intestazioni verranno visualizzate nella casella Intestazioni Internet.

Outlook Express

- Apri Outlook Express.
- Fai clic con il pulsante destro del mouse sull'email di cui vuoi visualizzare le intestazioni.
- Fai clic su Properties (proprietà).
- Fai clic sulla scheda Details (dettagli), le intestazioni verranno visualizzate in una casella.

A seguire la definizione di header, le modalità per visualizzarli e per leggerli.

Queste header o intestazioni sono dati che vengono aggiunti, da ogni server in grado di ricevere e spedire posta elettronica, nel quale transita il messaggio; ad ogni passaggio viene quindi inserito un ulteriore record sopra al precedente.
Per questo motivo, gli header devono essere letti dal basso verso l'alto.

Esempio:

Return-Path	<nomecasella@nomedominio.ext>
Delivered-To	casella_destinatario@nomedominio.ext
Received	(qmail 11111 invoked by uid 11); 14 Jun 2016 10:02:22 -0000
Received	from unknown (HELO mx.xx.aruba.it) (11.11.11.111) by mx.aruba.it with SMTP; 14 Jun 2016 10:02:22 -0000
Received	from smtp.aruba.it ([22.22.22.22]) by mx.aruba.it with bizsmtp id 6a2L1t00X21B1vA01a2Lpy; Tue, 14 Jun 2016 12:02:22 +0200
Received	from nomedominio.ext ([33.33.33.33]) by smtp.aruba.it with bizsmtp id 6a2L1t00S1xJdJu01a2LV7; Tue, 14 Jun 2016 12:02:20 +0200
Date	Tue, 14 Jun 2016 12:02:20 +0200
Message-Id	<O8RAJW$84901134BDC7C45F58E8272C7AAAED58@nomedominio.ext>
Subject	Header
MIME-Version	1.0
X-Sensitivity	3
Content-Type	multipart/alternative; boundary="_=__=_XaM3_.1465898540.2A.469743.42.2397.52.42.007.568922602"
Reply-To	nomecasella@nomedominio.ext
From	"Mario Rossi" <casella_mittente@nomedominio.ext>
To	casella_destinatario@nomedominio.ext
X-XaM3-API-Version	V3(R2)
X-SenderIP	95.110.221.50
X-Spam-Rating	mx.aruba.it 1.6.2 0/1000/N

Molte delle informazioni contenute nell'header possono essere falsificate, mentre le linee Received, almeno in parte, possono essere ritenute affidabili.

Ad esempio per quanto riguarda il dettaglio: Received: from indirizzo (IndirizzoIP) By nome_server_mail …. Il campo indirizzo è il nome con cui si identifica il mittente al destinatario e può essere falsificato; mentre IndirizzoIP è effettivamente il reale mittente.

I campi che solitamente compongono l'header di una mail sono:

- Return-Path: indica l'indirizzo mail a cui torneranno eventuali errori di recapito del messaggio;
- Delivered-To: indica l' indirizzo e-mail a cui è destinato il messaggio;
- Received: fornisce informazioni sull'accettazione della mail da parte dei server in cui è transitata, come la data l'ora e i dati del server;
- Date: data di trasmissione della mail;
- Message-Id: è formato da una stringa alfanumerica seguita da @nomedominio_mittente.ext che identifica in modo univoco la mail ed è generato dal client da cui parte il messaggio;
- Subject: oggetto dell'email;
- MIME-Version: definisce la versione del protocollo MIME (Multipurpose Internet Mail Extensions, letteralmente Estensioni multifunzione alla posta di Internet, è uno standard di Internet che estende la definizione del formato dei messaggi di posta elettronica, originariamente definito dall'SMTP, il protocollo di trasmissione delle email) utilizzato dal mittente;
- X-stringa: non esiste uno standard per i campi che iniziano con X-, vengono inseriti a discrezione del Client di posta;
- Reply-To: vi può essere indicato un indirizzo email, generalmente diverso dal mittente, a cui inviare eventuali risposte;

- From: indica l'indirizzo mittente;
- To: indica l'indirizzo destinatario.

Nell'esempio riportato il primo received partendo dal basso, è quello che identifica la postazione mittente; in particolare, la parte del From indica il server mittente, mentre To (o For) indica il destinatario dell'email.

Gli ultimi Received, cioè quelli più in alto, mostrano il passaggio dell'email dai server che ne hanno gestito l'invio ai server che ne hanno gestito la ricezione.
È comunque possibile aggiungere righe di Received falsificate.
Eventuali righe di Received falsificate possono essere inserite solo all'inizio dell'header, quindi più in basso, poiché la lettura di un header deve essere sempre fatta dal basso verso l'alto.
Gli orari indicati fanno sempre riferimento al GMT (Greenwich).
In Italia l'orario è pari a GTM+1 ora con l'ora solare o GTM+2 ore con l'ora legale.

In genere, l'utilizzo dell'ora locale sulla base del fuso con Greenwich, o l'inserimento diretto dell'orario di Greenwich è una opzione inserita dal server che la imposta in automatico.