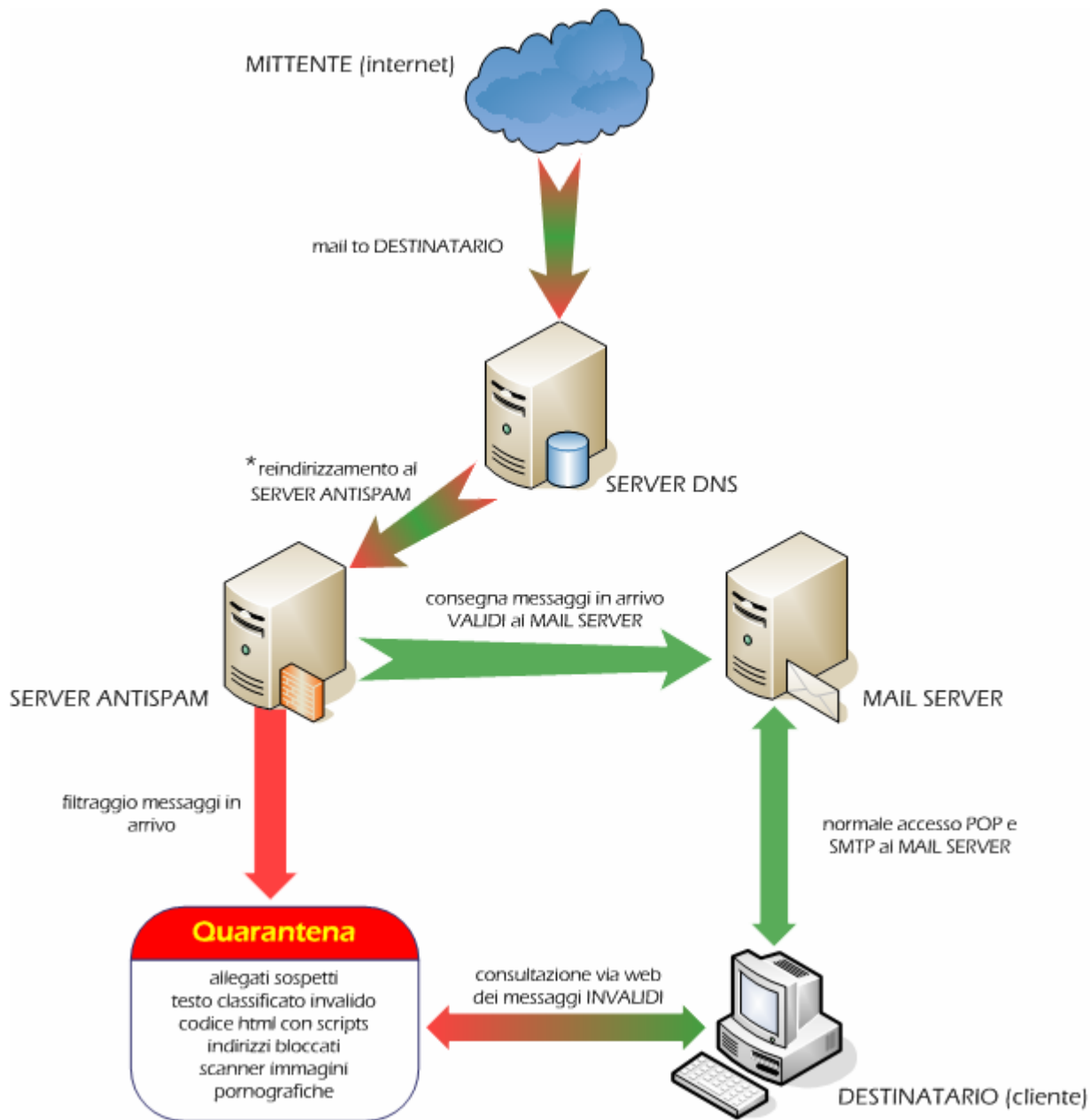


COME FUNZIONA



*Per attivare il servizio di spam e virus filtering è necessario modificare il record MX (mail exchange) del dominio del cliente in modo che tutti i messaggi indirizzati a casella@dominiocliente.it vengano dirottati verso il Server Antispam, il quale a sua volta consegnerà solo i messaggi ritenuti validi al Mail Server del cliente. Proprio per questo non sono necessarie altre configurazioni aggiuntive, soprattutto per il client di posta elettronica dell'utente finale che continua ad usare lo stesso server di posta in entrata POP3 e posta in uscita SMTP.

Come rappresentato nello schema precedente **Onyx Systems Messaging Security Suite** è una soluzione di spam e virus filtering sever side, quindi basata sul passaggio della posta elettronica del cliente presso il Server Antispam. Quest'ultimo processa ogni singolo messaggio e lo sottopone alle seguenti verifiche per stabilire se è da considerarsi VALIDO o INVALIDO:

- **Attachment Filter:** ovvero filtro degli allegati, questo filtro rileva gli allegati con estensioni sospette (.bat, .cmd, .com, .cpl, .dll, .drv, .exe, .hta, .js, .pif, .src, .vbs) che costituiscono il veicolo più usato per la diffusione di mass mailing worm e quindi virus.
- **Bayesian Text Classifier:** questo filtro classifica i messaggi in base al teorema bayesiano di probabilità condizionale. Si avvale di circa due milioni di record archiviati in un database, che contengono le parole più usate dagli spammers ed i relativi pesi statistici di utilizzo in mail "promozionali". Confrontando le frasi presenti nel messaggio con tali record assegna un punteggio che decreta se il messaggio è da considerarsi valido o invalido.
- **HTML Cleaner:** questo filtro è in grado di analizzare il codice HTML delle mail inviate in tale formato e di rilevare eventuali scripts che nella maggior parte dei casi sono di origine maligna.
- **Text Pattern Analyzer:** questo filtro riesce ad interpretare eventuali messaggi inviati sotto forma di immagini e confrontare il testo visualizzato con una serie di parole o combinazioni alfanumeriche considerate invalide.
- **Pornographic Image Analyzer:** questo filtro riesce a scansionare i messaggi inviati sotto forma di immagini ed a rilevare le varie tonalità di colore della pelle che frequentemente rappresentano messaggi spam di siti pornografici.

Al termine di tali verifiche se il messaggio risulta ancora classificato come VALIDO viene consegnato al Mail Server del cliente per poter essere scaricato normalmente, al contrario, se viene ritenuto INVALIDO rimane in **quarantena 7 giorni** presso il Server Antispam, dopodichè verrà automaticamente eliminato. Per tale periodo di tempo i messaggi rimangono comunque consultabili via web all'indirizzo <http://spam.onyxsystems.it> :



APLEXA
ARCHEOMETRA GROUP

Free your box!

Libera la tua casella di posta!

Aplexa Messaging Security Suite è la soluzione server side di spam e virus filtering. Grazie ad un potente classificatore bayesiano, un virus scanner ed uno skin scanner riconosce la stragrande maggioranza dei messaggi indesiderati e li mette in quarantena presso i nostri server. Tali messaggi rimangono consultabili via web e recapitabili a vostra discrezione.

MEMBER LOGIN

Mail address:

Password:

Login

Scopri i vantaggi di un sistema antispam

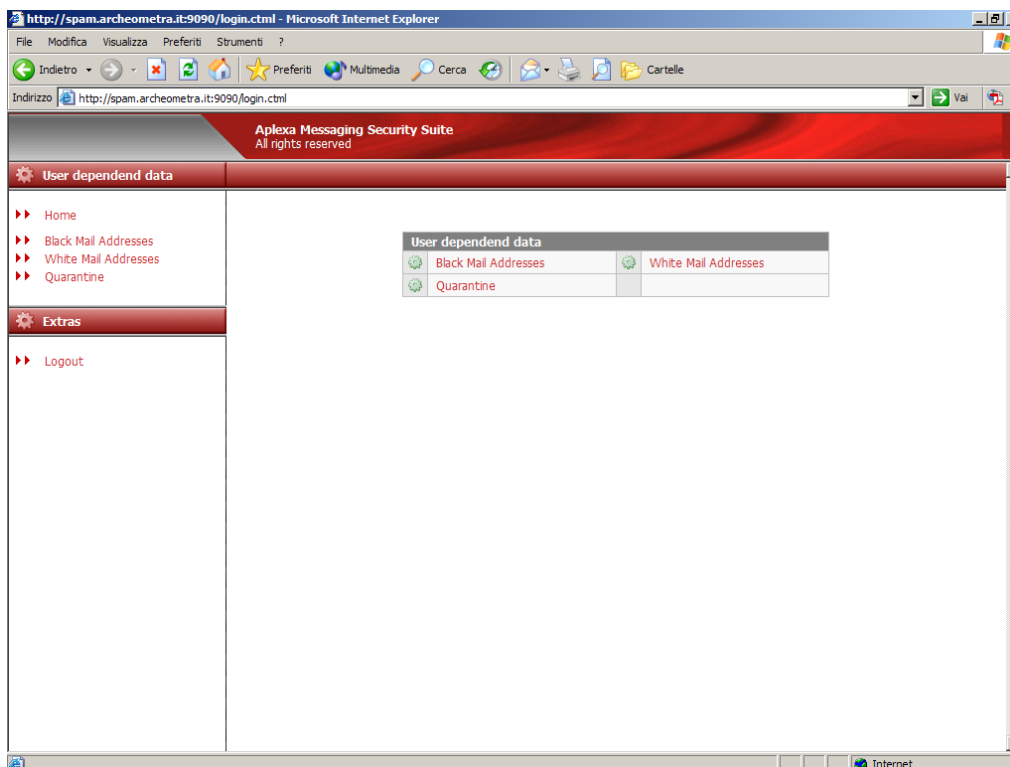
Come Funziona

Copyright © 2004 Aplexa. All rights reserved.
NOTICE: We collect personal information on this site.

Operazione completata

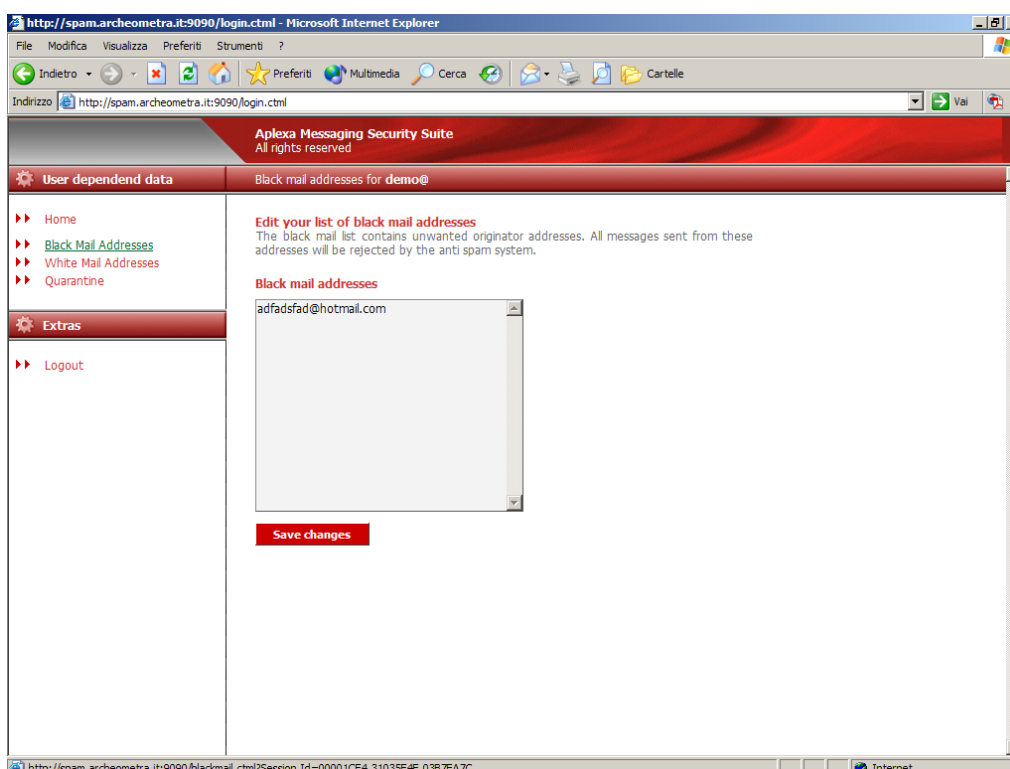
Internet

Dopo aver effettuato l'accesso con la coppia di credenziali fornite (indirizzo mail e password), la schermata che si presenta è la seguente:

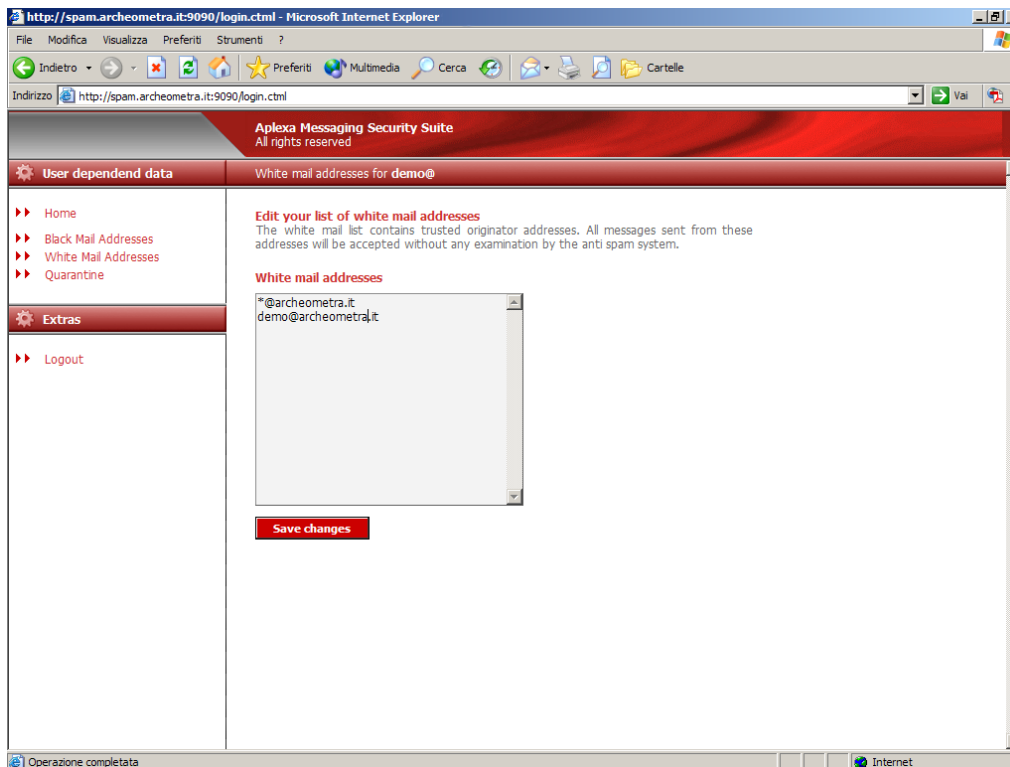


Come si può notare è possibile accedere a tre diverse aree, e rispettivamente:

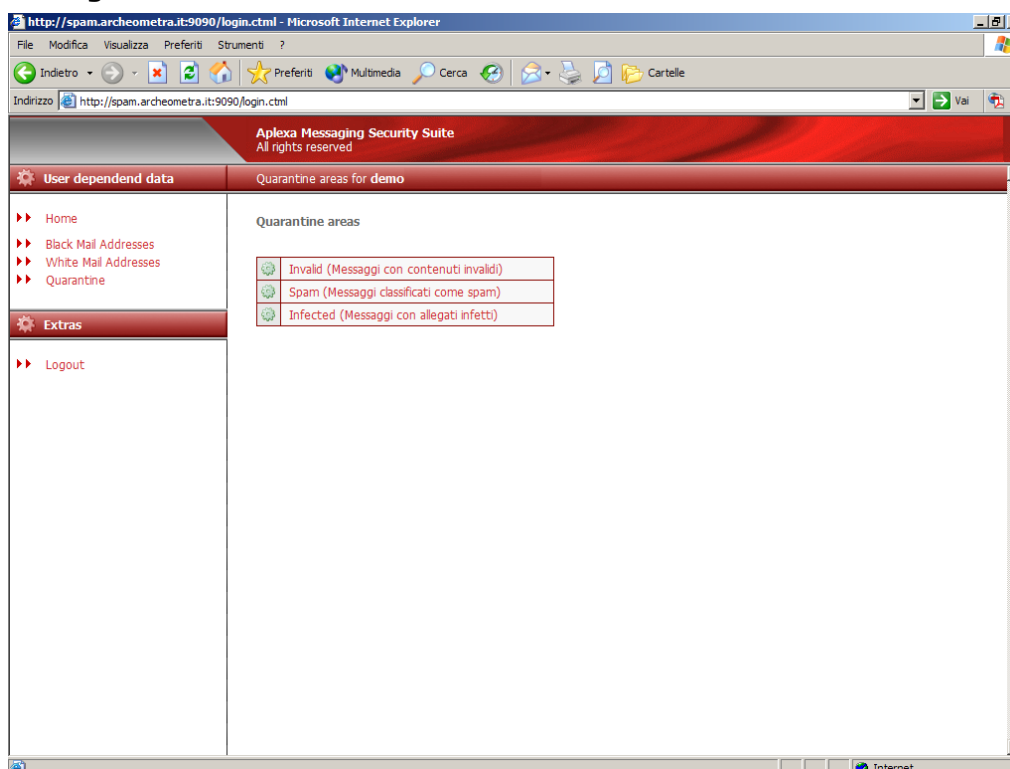
Black Mail Addresses: ovvero indirizzi mail bloccati dall'utente, in quest'area è possibile memorizzare indirizzi mail o interi domini (usando il carattere jolly: *@dominio.it) dai quali non si vuole più ricevere nessun messaggio. Attenzione che i messaggi provenienti da questi indirizzi/domini verranno direttamente rifiutati dal sever (Remote host said: 553 Address not accepted; Originator address is blocked by user) senza passare per la quarantena. Quindi si consiglia di usarlo per indirizzi "reali" (newsletter o simpaticoni invadenti) e non per limitare lo spam in quanto sarebbe inutile visto che gli spammers utilizzano indirizzi fittizi e li cambiano di frequente.



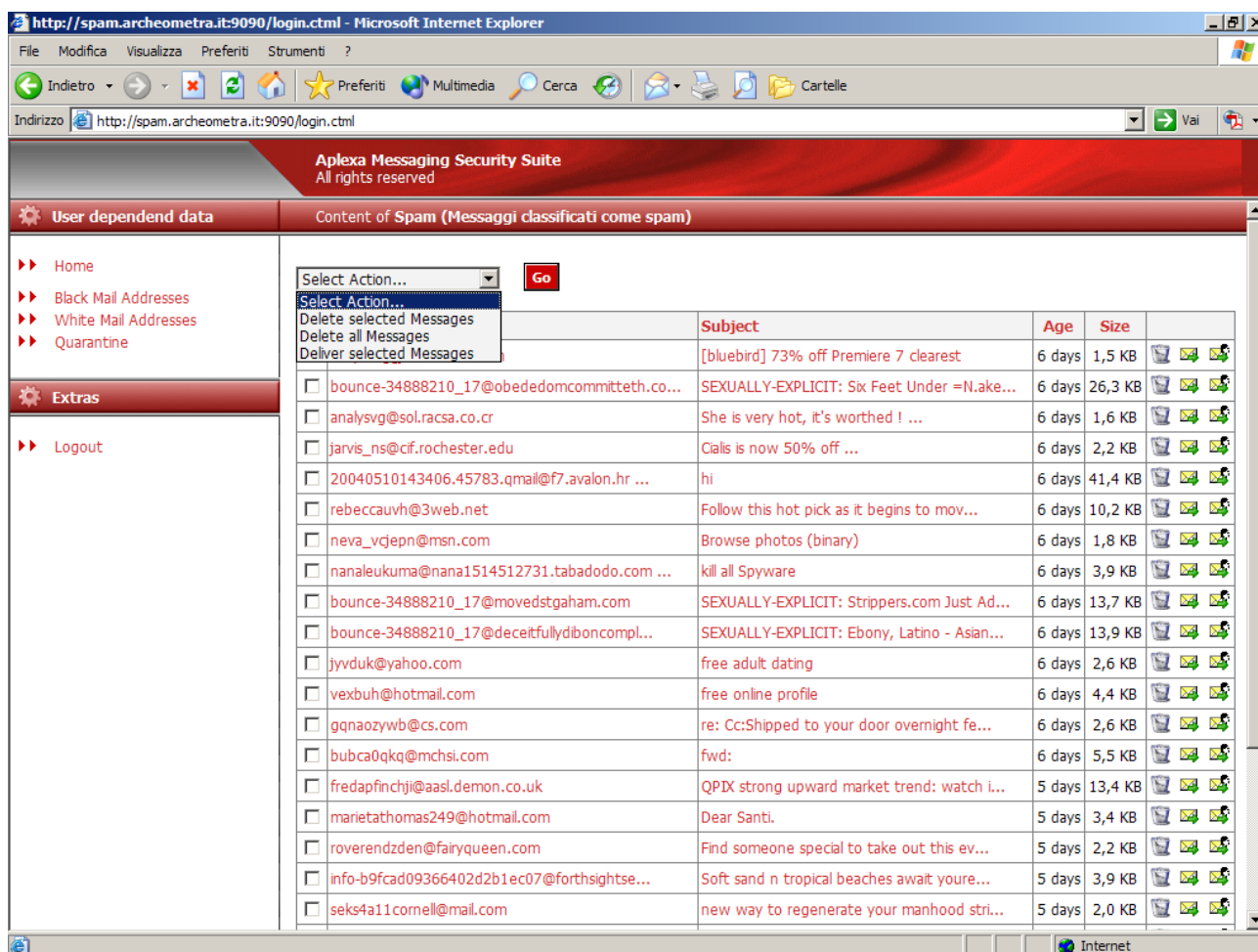
White Mail Addresses: ossia indirizzi sicuri, in quest'area è possibile salvare tutti quegli indirizzi o interi domini (usando il carattere jolly: `*@dominio.it`) di comprovata affidabilità (clienti/fornitori, amici ecc..). Così facendo si evita di sottoporre questi messaggi a tutte le verifiche e quindi si esclude la possibilità che erroneamente finiscano in quarantena.






Quarantine: l'area quarantena è a sua volta suddivisa in altre tre diverse zone, **Invalid** (messaggi con contenuti invalidi) include tutti i messaggi che sono risultati invalidi dopo il filtro html o il text pattern analyzer; **Spam** (messaggi classificati come spam) qui sono raccolti tutti i messaggi che non hanno superato il classificatore bayesiano o lo skin scanner; **Infected** (messaggi con allegati infetti) contiene tutti i messaggi con allegati sospetti intercettati dal filtro allegati.



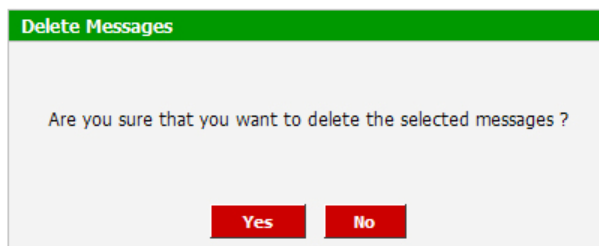
Entrando in ognuna delle suddette aree di quarantena, la schermata che si presenta è la seguente:



Mostra tutti i messaggi relegati nella rispettiva area visualizzando mittente, soggetto, tempo di permanenza, dimensione. Cliccando sulle intestazioni di colonna si possono ordinare i messaggi in senso crescente o decrescente rispetto ai vari criteri. Il menu a tendina permette di effettuare varie operazioni in modo rapido: **Delete selected messages** (cancella i messaggi selezionati spuntando la check box sulla prima colonna); **Delete all messages** (cancella tutti i messaggi all'interno dell'area senza bisogno di selezionarne alcuno); **Deliver selected messages** (recapita i messaggi validi selezionati, finiti erroneamente in questa zona). Inoltre nell'ultima colonna è possibile specificare un'azione per ogni singolo messaggio ed in particolare:

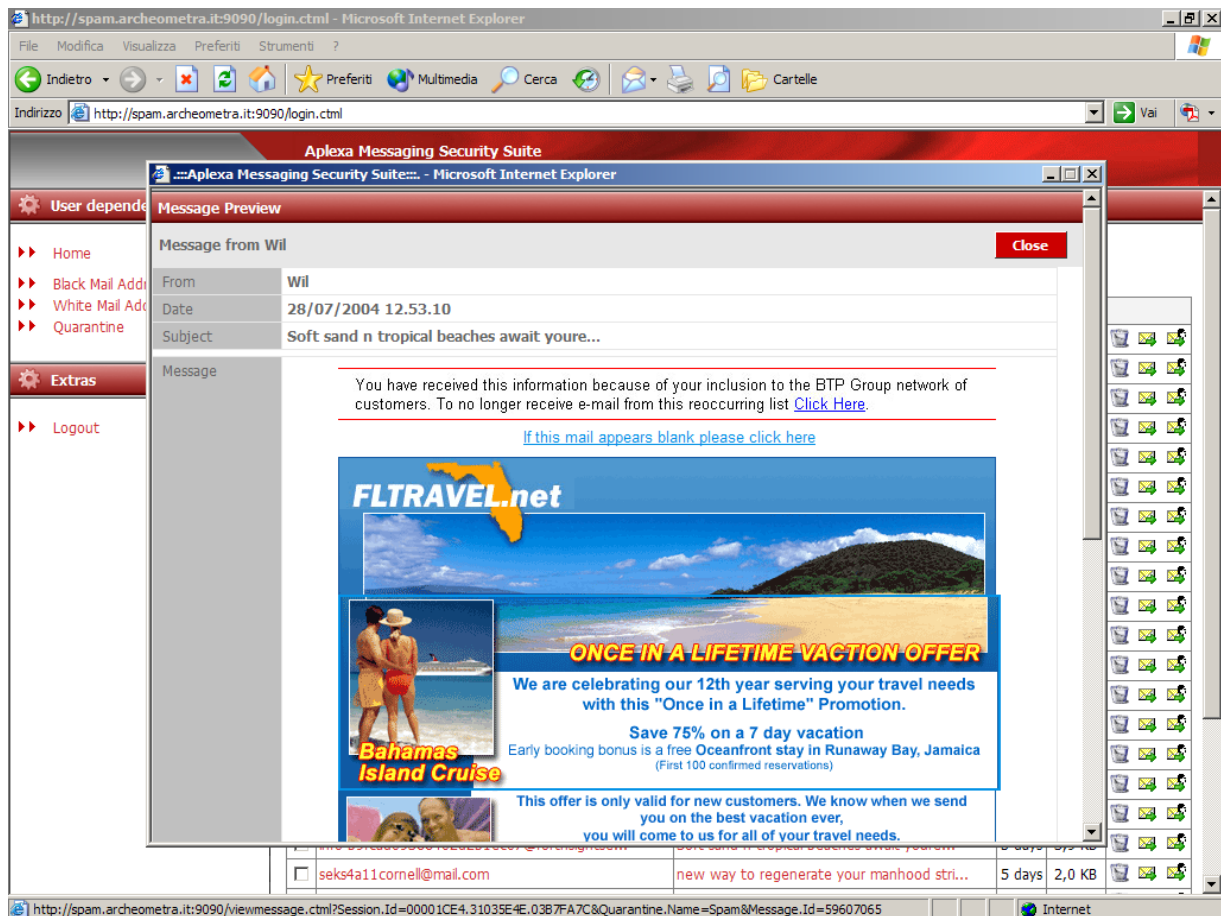
-  Cancella il messaggio corrispondente
-  Consegna/recapita il messaggio corrispondente all'indirizzo mail associato
-  Inoltra il messaggio corrispondente ad un indirizzo mail diverso da quello associato

Si ricorda che a seguito di qualsiasi azione di eliminazione messaggi comparirà una finestra di conferma per dare la possibilità di rimediare ad eventuali click involontari.



Questo non avviene per la consegna dei messaggi validi all'indirizzo mail associato  , pertanto è necessario prestare maggiore attenzione quando si rilevano messaggi validi nelle zone della quarantena.

Quindi prima di eliminare un messaggio è necessario accertarsi della provenienza attraverso l'indirizzo del mittente e, nei casi dubbi, visualizzarne l'anteprima cliccando indifferentemente sull'indirizzo del mittente o sull'oggetto corrispondenti:



Infine proponiamo una serie di accorgimenti da seguire per limitare la mail spazzatura e migliorare il servizio antispam:

1. Limitare al massimo la diffusione del proprio indirizzo di posta sul web, per esempio non inviare il proprio indirizzo mail attraverso form su siti non affidabili o che propongono servizi "FREE" senza una chiara privacy policy;
2. Non rispondere mai a mail indesiderate ne tantomeno seguire le procedure di unsubscribe/remove, così facendo si confermerebbe l'esistenza dell'indirizzo già in possesso dello spammer;
3. Evitare di rispondere alle cosiddette "Catene di Sant'Antonio", queste storie strazianti sono create ad hoc per accrescere il database di indirizzi degli spammers recuperando le intestazioni Fw:, R:, dei messaggi precedenti, dove possibile usare l'inoltro tramite Copia Carbone nascosta (Ccn:);
4. Non aprire il messaggio e possibilmente disabilitare la visualizzazione di immagini e l'anteprima automatica, il codice html contenuto nel messaggio riesce a comunicare al mittente che l'indirizzo esiste anche senza effettivamente rispondere al messaggio;
5. Eventualmente individuare il mittente attraverso la lettura degli header e segnalarlo al provider o denunciarlo direttamente al Garante della Privacy. Per maggiori informazioni <http://www.collinelli.net/antispam>;
6. Se dopo l'attivazione del servizio dovessero pervenire comunque mail indesiderate prima di cancellarle, inoltrarle a spam@dominiocliente.it, tale procedura permette al sistema antispam di apprendere nuove combinazioni di parole e quindi intercettare tali messaggi in futuro;
7. Come già detto in precedenza accedere almeno ogni **7 giorni** a <http://spam.onyxsystems.it> per recuperare eventuali messaggi validi ed eliminare quelli invalidi;
8. Se si necessita di file nei formati sospetti bloccati dal filtro sugli allegati richiedere esplicitamente al mittente di inviarli in formato compresso (.zip, .rar).