Guida pratica per analizzare le mail

Identificare un tentativo di truffa o phishing veicolato attraverso email standard è un'operazione difficile poiché non c'è modo di garantire in automatico e senza dubbi la veridicità del contenuto di una mail. In questo ambito, l'attenzione ad alcuni dettagli contenuti nelle mail ricevute può essere determinante per evitare problemi. Questo breve documento riassume alcuni semplici passi da compiere per controllare eventuali mail sospette. Ulteriori elementi per definire se una mail è malevola o meno sono da trovare nel "decalogo per proteggersi dal phishing".

A cosa occorre prestare attenzione

Generalmente (ma non è garantito) le mail contenenti un tentativo di truffa o phishing sono caratterizzate da alcuni di questi aspetti:

- **tono allarmistico**: se non si reagisce immediatamente, si viene minacciati di subire qualche tipo di danno;
- **testo sgrammaticato o con parti in lingue diverse**: spesso i testi delle mail malevole vengono prodotti usando convertitori di lingua automatici che producono testi di cattiva qualità;
- **mittente proveniente da un dominio non coerente con il contenuto della mail**: ad esempio, una mail che richiede un cambio di password per le credenziali di Ateneo proveniente da un account ***@live.com***;
- **presenza di caratteri strani nel oggetto della mail o nel campo from**: per sfuggire agli scanner della posta a volte vengono usate traslitterazioni con caratteri non latini che assomigliano graficamente a caratteri latini, ad esempio, ***ĀCCOЦNT*** al posto di ***ACCOUNT****;*
- **rimando ad un link esterno per il download delle informazioni necessarie:** in alcuni casi è accaduto che un virus sia stato veicolato attraverso link considerati affidabili, Google Drive o simili, per cui occorre prestare la massima attenzione prima di cliccare su un link all'interno di una mail o scaricare un allegato specie la mail non è stata sollecitata dal ricevente.

Analizzare una mail sospetta

Allo scopo di rendere più semplice la spiegazione viene preso in esempio la mail della campagna "Avviso finale per aggiornare il tuo account" (giugno 2019) descrivendo alcuni passi da compiere per analizzare la mail.

Le email sono composte da due parti:

- **header:** contenente informazioni di servizio, generalmente nascosto dal client di posta; questa parte spesso viene nascosta dal client di posta che mostra solo versioni riassunte del campi **From, To, Reply To, Subject**;
- **body:** composto da varie parti, contenente il testo della mail, a volte in vari formati, per poter essere visualizzato da vari client di posta, e gli eventuali allegati; i moderni client di posta supportano il formato HTML che permette di scrivere mail fortemente formattate, al pari dei siti web; questo crea qualche problema nella verifica dei link all'interno delle mail, che nelle mail malevole viene spesso offuscato in vari modi.

La mail malevola portata come esempio si presenta come l'immagine in Figura 1: il mittente è apparentemente un utente unimi e il testo della mail sembra riportare un avviso da parte della Divisione Telecomunicazioni di aggiornamento account della posta.

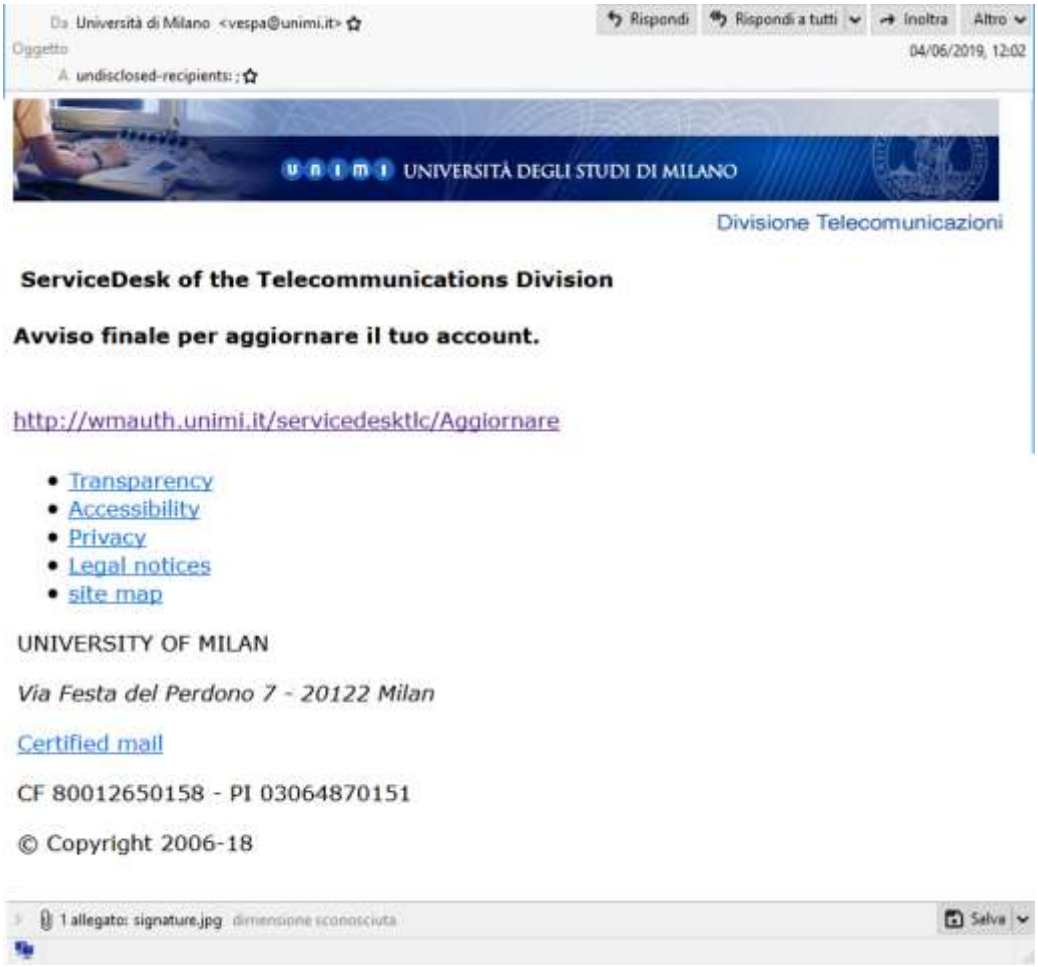


Figura 1: Mail di phishing analizzata

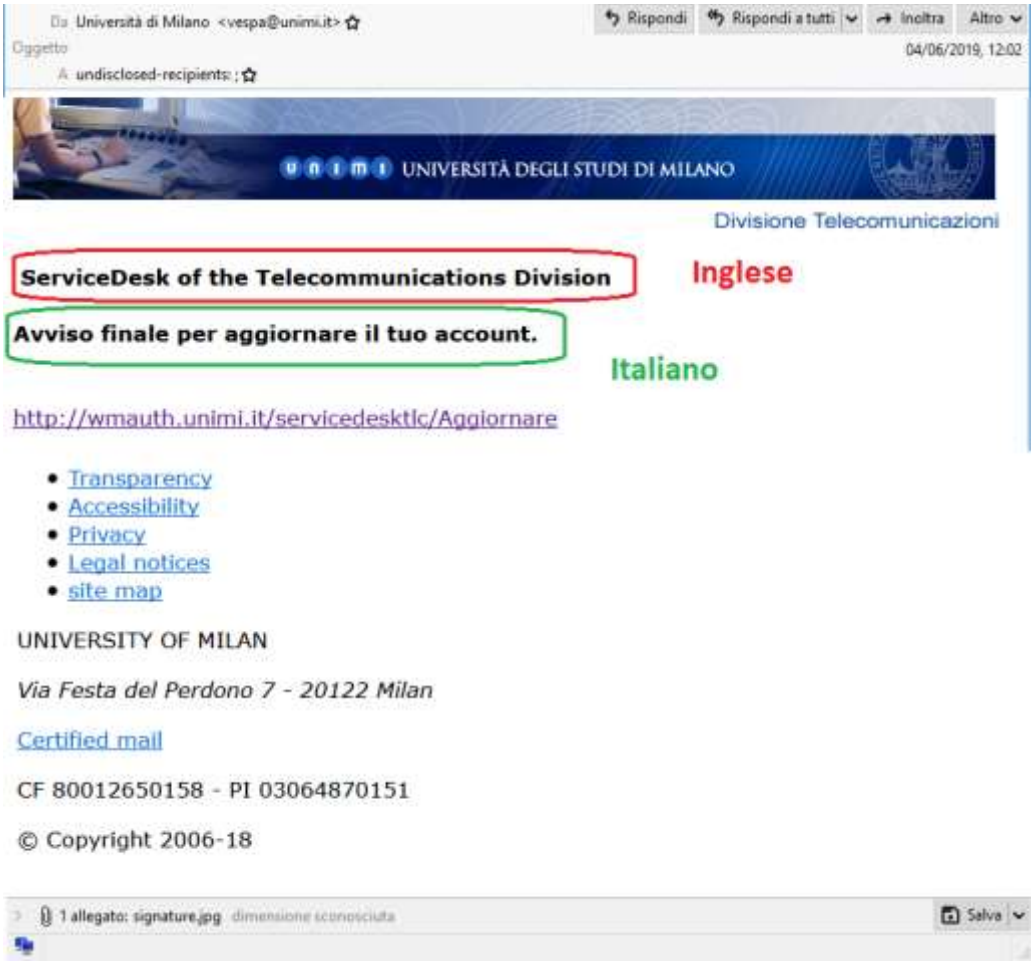
Analisi del testo della mail

Nonostante la mail sembri genuina, ci sono degli elementi che mettono in allarme:

- **Testo misto italiano/inglese**: si parte con "ServiceDesk of the Telecommunications Division" e poi segue "Avviso Finale per aggiornare il tuo account"
- **Tono allarmistico:** "Avviso finale"
- **Allarme del client di posta:**
  I client di posta elettronica moderni, come ad esempio Thunderbird, contengono controlli che possono rivelare contenuti anomali; nell'esempio indicato il client Thunderbird presenta un avviso di sicurezza "questo messaggio potrebbe essere un tentativo di frode" (Figura 2)

Figura 2: avviso di tentativo di frode da parte del client di posta Thunderbird

Il corpo della mail riporta il logo dell'Università degli Studi di Milano con riferimento alla Divisione Telecomunicazioni, ma leggendo il testo si nota che è scritto sia in lingua italiana che in inglese, apparentemente tradotto attraverso un tool automatico. La firma finale, in particolare, riporta University of Milan, e alcuni link alle sezioni del sito riportate in lingua inglese. La firma dell'Ateneo, come riportato nel sito, sia nella versione italiana che inglese, è sempre in italiano. A queste incongruenze nella lingua si aggiunge il tono allarmistico della mail: "Avviso finale".



Analisi dei link della mail

I collegamenti della mail riportano al sito dell'Ateneo, tranne il testo relativo al link principale (Figura 3) dove cliccare per l'eventuale aggiornamento dell'account. La verifica che il testo del link coincida con il collegamento effettivo può essere fatta in uno dei seguenti modi:

- passando sopra il testo del link il mouse: il collegamento effettivo apparirà nella parte inferiore della mail (Figura 3);
- cliccando con il tasto destro del mouse e scegliendo l'opzione "copia link", incollare il link in un file di testo (Figura 4).

Nel caso in esempio i due link non coincidono!!

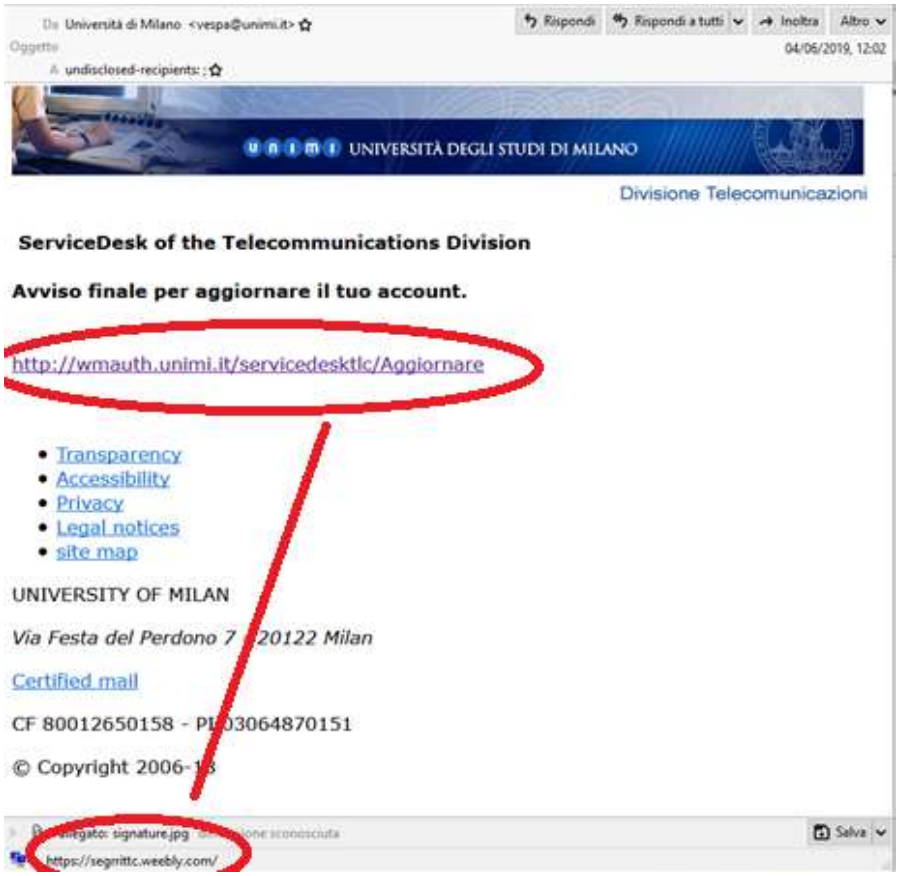


Figura 3 Analisi dei link della mail

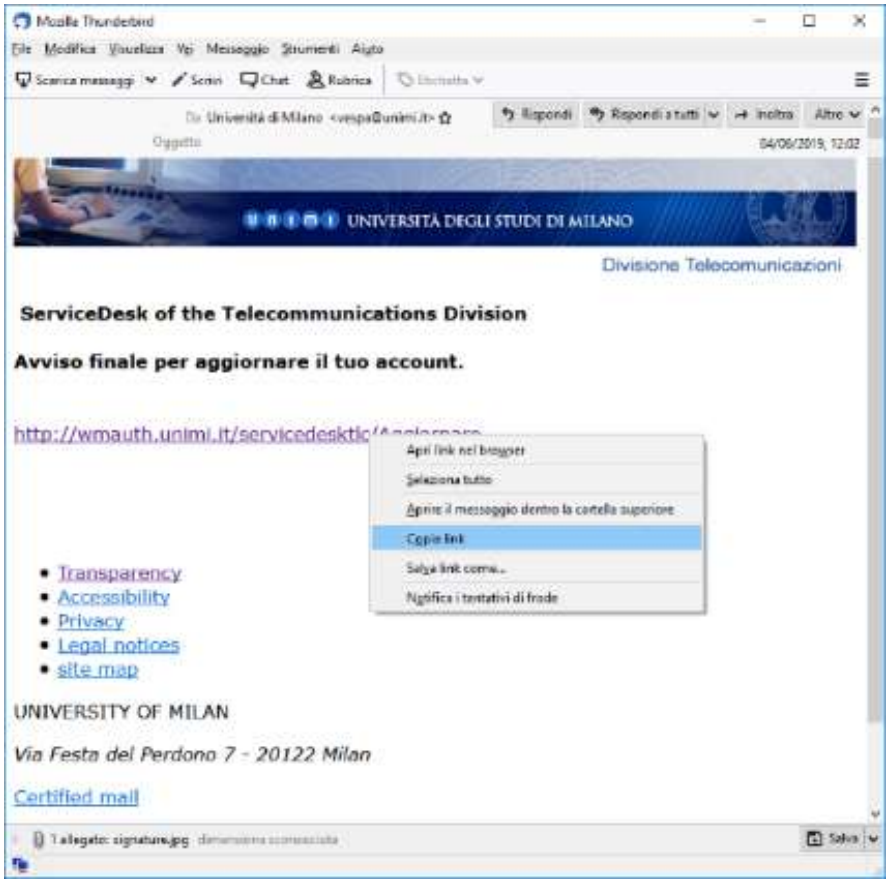


Figura 4: copiare il link della mail

Analisi dell'header

Apparentemente la mail sembra arrivare da un indirizzo del dominio *@unimi.it*. Ciò che appare però dipende dal client di posta che spesso nasconde le parti più tecniche dell'indirizzo. L'analisi dell'header permette di identificare il reale mittente della comunicazione ed avere qualche informazione in più per poter prendere una decisione sulla bontà della mail. Poiché però il protocollo di posta non implementa nativamente nessun meccanismo di autenticazione anche il reale indirizzo va considerato inaffidabile (vedi *Email spoofing*).

Estendiamo la visibilità delle intestazioni (header), come in Figura 5, esaminando alcuni i campi in Figura 6 :

- **"*From*"**: mittente apparente, può essere falsificato.
- ***"envelope from"***: serve per verificare il mittente reale, che potrebbe non coincidere con quello apparente indicato dal campo *from*. Se i due campi non coincidono potrebbe essere indice di mail malevola.
- ***"Received"*:** fornisce informazioni sui server di posta coinvolti durante la trasmissione. Tale campo presenta almeno due righe: una relativa al server di invio e una a quello di ricezione. Leggendo le informazioni dal basso verso l'alto si osserva che il server di posta del mittente è *posti.itea.ntnu.no* con IP 129.241.56.174.

Figura 5: visualizzazione degli header della mail

```
Received: from mailgw01.it.ntnu.no (mailgw01.it.ntnu.no [129.241.56.174])
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
    (No client certificate requested)   by unimix1.unimi.it (Postfix)
 with ESMTPS id D88E5400C8; Tue,  4 Jun 2019 13:20:50 +0200 (CEST)
Received: from localhost (localhost [127.0.0.1])
    by mailgw01.it.ntnu.no (Postfix) with ESMTP id 4A942244658; Tue,
 4 Jun 2019 13:19:57 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at mailgw01.it.ntnu.no
Received: from mailgw01.it.ntnu.no ([127.0.0.1])
    by localhost (mailgw01.it.ntnu.no [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id hrSU5YUu0EiA; Tue,  4 Jun 2019 13:19:56 +0200 (CEST)
Received: from alumnimail01.it.ntnu.no
 (alumnimail01.it.ntnu.no [IPv6:2001:700:300:4::54])
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-SHA (256/256 bits))
    (No client certificate requested)   by mailgw01.it.ntnu.no (Postfix)
 with ESMTPS id EADC7244162;    Tue,  4 Jun 2019 13:19:55 +0200 (CEST)
Received: from webmail.alumni.ntnu.no (posti.itea.ntnu.no [129.241.56.163])
    (using TLSv1 with cipher ECDHE-RSA-AES256-SHA (256/256 bits))
    (No client certificate requested)   (Authenticated sender: akol)
    by alumnimail01.it.ntnu.no (Postfix) with ESMTPSA id 416D366229;    Tue,
 4 Jun 2019 12:02:56 +0200 (CEST)
Received: from BuyaQKI70vHt5pAVgWsPBsD0TSmehNZAHqNn8D2Vf1AVkzE6fG68Og==
 (r5M/HVIsmzu3o2lC/KeXhD1+GWb6vxrc) by webmail.alumni.ntnu.no with HTTP
 (HTTP/1.1 POST); Tue, 04 Jun 2019 12:02:55 +0200
```

Figura 6: campo Received nell'header esteso

Per ulteriori informazioni sulle tematiche di sicurezza informatica, per l'approfondimento di quanto descritto in questo documento e per le modalità tecniche di implementazione delle misure di sicurezza richieste fare riferimento alle linee guida e indicazioni dell'Ufficio di Staff Sicurezza ICT pubblicati sul portale di Ateneo a partire dalla URL: https://work.unimi.it/servizi/security_gdpr/118546.htm