

Ufficio di Staff Sicurezza ICT

# 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, *ACCOUNT* 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.



Ufficio di Staff Sicurezza ICT

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.

💷 Università di Milano 🛛 vespa@unimi.it> 😭	♦ Rispondi ♦ Rispondi a tutti    → Inoltra Altro
Oggetto	04/06/2019, 12:02
A undisclosed-recipients: ; 🏠	
the second se	
Unit mil Univers	ITÀ DEGLI STUDI DI MILANO
	Divisione Telecomunicazioni
ServiceDesk of the Telecommunicatio	ns Division
Avviso finale per aggiornare il tuo acc	ount.
http://wmauth.unimi.it/servicedesktlc/Agg	iornare
Transparency	
Accessibility	
Privacy	
I.egai notices     site map	
UNIVERSITY OF MILAN	
Via Festa del Perdono 7 - 20122 Milan	
Certified mail	
CF 80012650158 - PI 03064870151	
© Copyright 2006-18	
B 1 allegato: signature.jpg dimensione sconosciuta	🖬 Salva 🗸

#### 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)

D∎ Università di Milano ≺vespa⊕unimi.it> ✿	🕈 Rispondi	🄲 Rispondi a tutti 🗸	+ inoltra	Altro 🗸
Oggetto A undisclosed-recipients: ; 🏠			04/06/2	3019, 12:62
Questo messaggio potrebbe essere un tentativo di frode.			Qpzion	×



Ufficio di Staff Sicurezza ICT

#### 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).



Ufficio di Staff Sicurezza ICT

### Nel caso in esempio i due link non coincidono!!

Da Università di Milano «vespa@unimi.it» 🏠	★ Rispondi → Rispondi a tutti → → Inoltra Altro → 01/05/1000 13000
A undisclosed-recipients: :☆	WHORE BY S. TENE
and the second s	
Unit of UNIVER	SITA DEGLI STUDI DI MILANO
	Divisione Telecomunicazioni
Constant of the Talana martinetic	Philalan
ServiceDesk of the Telecommunicatio	ons Division
Avviso finale per aggiornare il tuo acc	ount.
the low suth union it loop is a desitte (A au	line and the second
http://wmauth.unimi.it/servicedesktic/Agg	pornare
• Transparency	
Accessibility	
Privacy	
Legal notices	
• site map	
UNIVERSITY OF MILAN	
Via Santa del Desdena 7 20122 Miles	
via resta del Perdono 7 20122 Milan	
Certified mall	
CE 80012650158 - PL03064870151	
© Copyright 2006-18	
Berenegato: signature.jpg	🖬 Salva 🛩
https://segnittc.weebly.com/	

Figura 3 Analisi dei link della mail



Ufficio di Staff Sicurezza ICT

Moste Thunderbird					-		×
Eit Medifica Yourkan Vei Messeggio St	iumenti Aiuto						
ØScanca massaggi ♥ /Scain QChat	& Rubrica	The increases w					Ξ
Die Universitä di M	lano «vespa@v	mitti it> 🖸	🤊 llispondi	🕈 Repondia tutti 🗸	+ incite	Altre	
Oygette		1010/00/054 1	10-111		64/06	(2019, 1)	2:02
Committee in the second		118/2	1225	HR.C.			
		ERSITÀ DEGLI	STUDI DI M		// Elai		
				Divisione Tele	comunic	azion	
			and the second se				
ServiceDesk of the Telecor	nmunica	tions Divis	ion				
A sector E and a sector sector							
Avviso finale per aggiornar	e il tuo a	ccount.					
http://wmauth.unimi.it/servic	edesktic/*	adarasta					
		Apri link nei br	eWett				
		Selaziona tutto					
		Aprine il messoggio dentro la cartella superiore					
		Copie ink					
<ul> <li>Transparency</li> </ul>		Salya link com	K				
<ul> <li>Accessibility</li> </ul>		Ngtifica i tavita	tivî di frade				
Privacy							
Legal honces							
- site inste							
UNIVERSITY OF MILAN							
Via Festa del Perdono 7 - 201.	22 Milan						
and the second se							
Certified mail							
👔 Talegete: cignature.jpg: climanosmi com	statistic .					E >	eter i v
n.							

Figura 4: copiare il link della mail



Ufficio di Staff Sicurezza ICT

### 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.

C) Mozilla Thun	nderbird							-	0	×
ile Modifice	Visualizza V	ji Messaggio	Strumenti	Aiuto						
Scarica mes	Barre de	gli strumenti		1	D Etichelta Y					- 2
Da Univer	Intestaz	oni	1		Iutte	* Rispondi	* Rispondi a tutti		Inoltra	Altro
	Corps g	jel messaggio ci	me		Normale				04/05/2	2019, 12
A undisc	Mostra	ellegati in linea								
	Ridimer	isiona								
	Codific	i del testo	2000	1						
	Sorgerd	e del messaggio	Ctrl=U							
	Informa	zioni sicurezza r	nessaggio							
1										
-	******				11//	110 118		W.B	TAK	<u>)</u>
	-	00		UNIN	ERSITÀ DEGL	STUDI DI MIL	ANO			
				-		111	Divisione Tel			alaat
							DAVISIONE TER	acon	numca	ZIONI
Avviso fin	nale per	aggiorn	are il ti	10 5	ccount.					
http://wm	auth.un	mi.it/serv	icedesk	tic//	Aggiornare					
• Transa	D D D D D D D D D									
Accos	parency									
Acces	SIDILLY									
• Local	natione									
Legar	I I U U U U U U U U U U U U U U U U U U									
CITA IT	nan									
• <u>site m</u>	nap									
	TY OF M	ILAN								
• <u>site m</u> UNIVERSI		ILAN								
• <u>site m</u> UNIVERSI Via Festa c	nap TY OF M del Perd	ILAN 2010 7 - 20	)122 Mil	an						
• <u>site m</u> UNIVERSI <i>Via Festa c</i>	nap TY OF M del Perde	ILAN 2010 7 - 20	122 Mil	ən						
• site m UNIVERSI Via Festa c Certified m	TY OF M del Perde nail	ILAN 2010 7 - 20	0122 Mil	ən						
• site m UNIVERSI Via Festa c Certified m CF 800126	nap TY OF M del Perdo nail 550158 -	ILAN 2010 7 - 20 - PI 03064	0 <i>122 Mil</i> 1870151	an						
• site m UNIVERSIT Via Festa o Certified m CF 800126	nap TY OF M del Perde nail 550158 -	ILAN ono 7 - 20 • PI 03064	0 <i>122 Mil</i> 1870151	an						
site m UNIVERSIT Via Festa c Certified m CF 800126 © Copyrig	TY OF M del Perd nail 550158 - ht 2006	ILAN ono 7 - 20 · PI 03064 -18	9 <i>122 Mil</i> 9870151	ən						
site m UNIVERSIT Via Festa c Certified m CF 800126 © Copyrig	nap TY OF M del Perd nall 550158 - ht 2006	ILAN ono 7 - 20 • PI 03064 -18	9 <i>122 Mil</i> 870151	ən						
SILE IT     UNIVERSIT     Via Festa c     Certified m     CF 800126     © Copyrig     1 allegate:	nap TY OF M del Perd nall 550158 - ht 2006	ILAN ono 7 - 20 · PI 03064 -18	0122 Mil 1870151	ən					E	) Salva

Figura 5: visualizzazione degli header della mail



Ufficio di Staff Sicurezza ICT

```
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 (Postfi
h ESMTPS id EADC7244162; Tue, 4 Jun 2019 13:19:55 +0200 (CEST)
                                        by mailgw01.it.ntnu.no (Postfix)
with ESMTPS id EADC7244162;
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 alumnimail@1.it.ntnu.no (Postfix) with ESMTPSA id 416D366229;
                                                                           Tue,
4 Jun 2019 12:02:56 +0200 (CEST)
<u>Beceived</u>: from BuyaQKI70vHt5pAVgWsPBsD0TSmehNZAHqNn8D2Vf1AVkzE6fG680g==
 (r5M/HVIsmzu3o21C/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