Avviso di sicurezza del 26/03/2021

Segnalazione di campagne malevole in atto

Gent.Utenti,

pubblichiamo il presente avviso per segnalarvi alcune campagne malevole in atto in queste ore. In fondo a questo documento potete trovare alcune schermate di esempio.

La prima campagna malevola che vi segnaliamo è un tentativo di phishing particolarmente insidioso poiché l'indirizzo malevolo è stato camuffato in modo da rendere difficile l'ispezione prima di aprire il link stesso. In fondo a questo documento potete trovare un esempio della mail in questione (Figura 1). Il link malevolo è stato mascherato in modo da non essere visualizzato su la maggior parte dei client di posta quando si sosta con il mouse sul link stesso. Potete vedere il risultato in Figura 2 e 3. In aggiunta, l'attaccante ha mascherato ulteriormente l'indirizzo reale di salto mettendolo dopo un servizio legittimo di Google, *googlefastweb,com* (Vedi Figura 3 in basso).

La mail può essere riconosciuta come phishing da queste caratteristiche:

- Il mittente non proviene da **@unimi.it** ma da un dominio esterno (Vedi Figura 1 in alto)
- La mail è di tono allarmistico e poco chiara: **"le tue email sono rifiutate!"**
- **Rimanda ad un sito al di fuori del dominio unimi.it**

Il Settore Cybersecurity, Protezione dati e Conformità della direzione ICT ha attuato le operazioni necessarie a contrastare le campagne in atto.

Con la presente vi chiediamo, **se aveste cliccato involontariamente sul link indicato ed aveste inserito le vostre credenziali** di:

- Cambiare immediatamente la password attraverso il sito istituzionale: https://auth.unimi.it/password/
- Darne rapida comunicazione, sicurezza@unimi.it avendo cura di specificare l'orario indicativo in cui si è cliccato sul link malevolo e l'orario in cui è stato effettuato il cambio della password.

Se non avete inserito le vostre credenziali, non occorre fare nulla oltre che cancellare la mail.

Si raccomanda sempre di prestare la massima prudenza su email contenenti link o allegati soprattutto se non sollecitate.

La seconda campagna malevola che portiamo alla vostra attenzione è un esempio di campagna di spam che differisce dalle usuali campagne di spam per la modalità di comunicazione. In questo caso il contenuto della mail è forgiato in modo da lasciare intendere all'interlocutore che esista già un contratto a suo nome in scadenza con il presumibile scopo di catturare l'attenzione e invogliare a seguire il link indicato nella mail (Vedi mail in allegato). Tali mail non costituiscono un reale problema di sicurezza. Qualora riceviate una di queste mail è sufficiente inoltrarle come allegato a spam@unimi.it in modo da contribuire al miglioramento del filtro anti-spam di Ateneo.

Altre informazioni su come migliorare la sicurezza dell'Ateneo possono essere trovate sul portale istituzionale al link: https://work.unimi.it/servizi/security_gdpr/118546.htm

I più cordiali saluti.

Nicla Diomede
Settore Cybersecurity, Protezione Dati e Conformita' - Direzione ICT
Universita' degli Studi di Milano - Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

Figura 1: esempio della mail di phishing

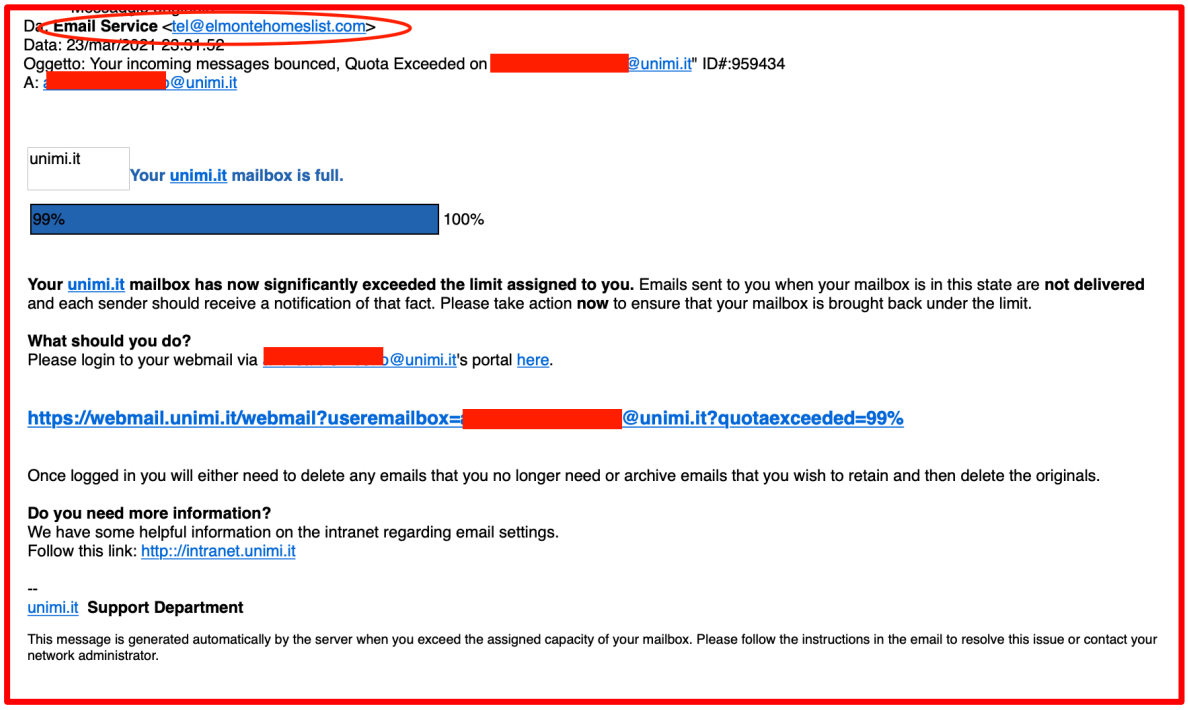

Figura 2: Url malevolo mascherato su Mail di Mac OSX

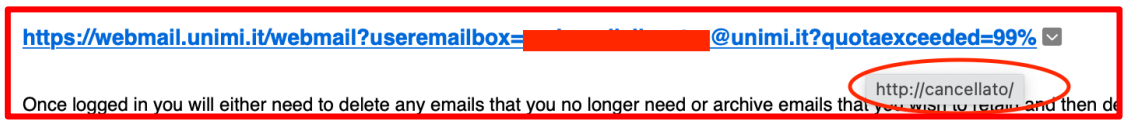

Figura 3: Url malevolo mascherato su Thunderbold

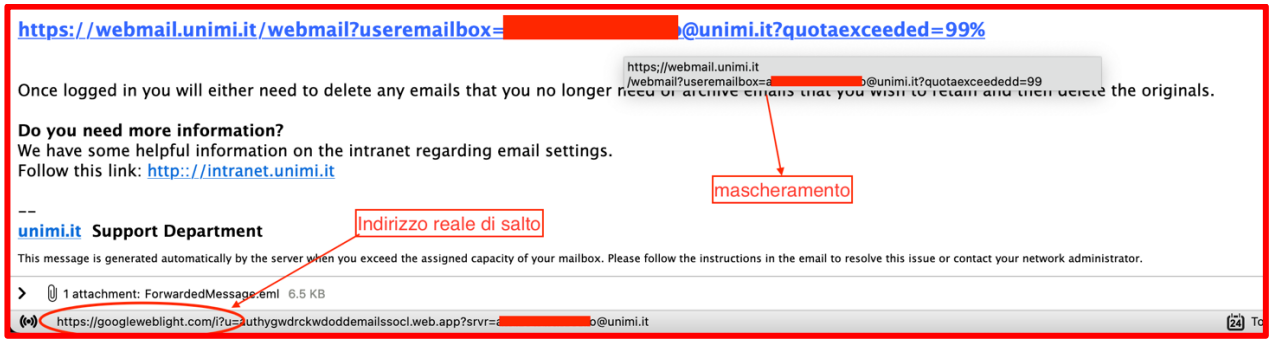

Figura 4: Alert in caso di click su Thunderbird

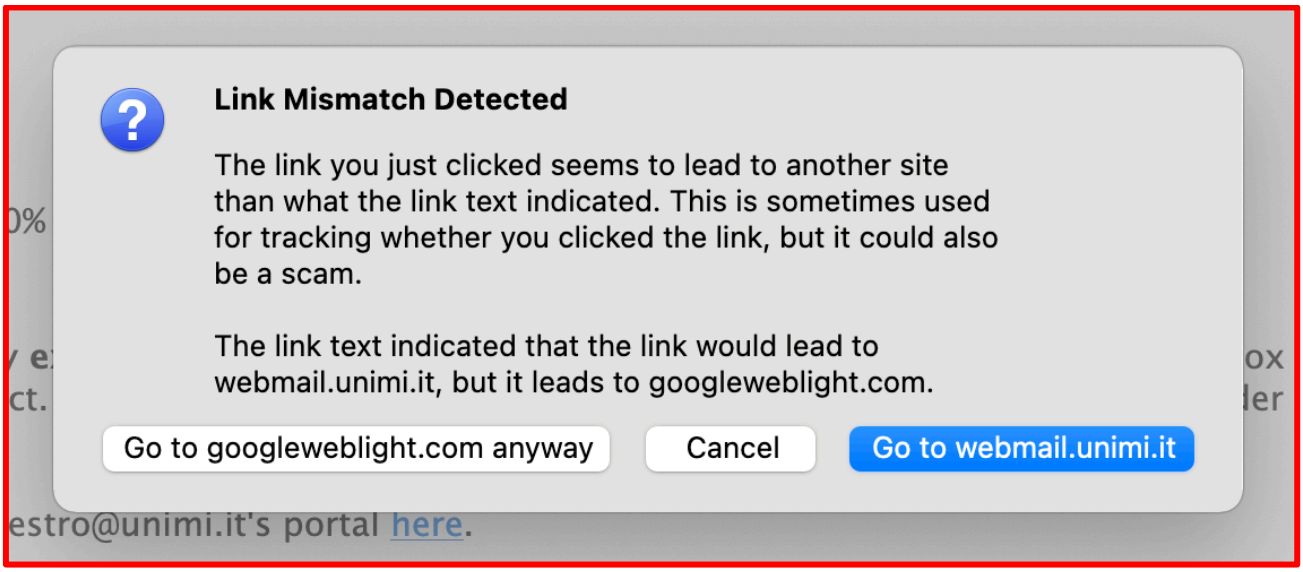

Figura 5: Email di spam

Da: **System Order** <sender@maya-med.[redacted]
Data: 23/mar/2021 17.50.44
Oggetto: Your free trial is about to end! CHT92[redacted]
A:[redacted]@unimi.it"[redacted]@unimi.it>

Dear Subscriber, # CHT9[redacted]

Unfortunately your free trial is ending in 2 days. But don't worry you will stay with us!You have provided a payment method which will be used to continue your membership. Your subscription will be continued using a payment method you mentioned. Selected plan will cost you $89.99 per month.

We are really excited that you with us, let's move to premium!
The new referral system is on! Every friend you brought will lower your monthly payment!

In the event that you want to change/drop the subcription, call us here: +1 323 [redacted]

The comment on our website will be highly appreciated! Thank you for choosing us!

Kind Regards,
Medical Reminder Service