Avviso di sicurezza del 04/03/2021

Segnalazione di campagne malevole in atto

Gent.Utenti,

pubblichiamo il presente avviso per informarvi delle campagne malevole che in questi giorni stanno colpendo l'Ateneo. In fondo a questo documento potete trovare alcune schermate di esempio.

Il primo esempio che vogliamo mostrarvi è una mail di phishing che veicola un link malevolo. La mail si presenta come una segnalazione relativa ad un problema al servizio di posta elettronica e contiene un link ad un sito malevolo in cui è presente l'effettiva pagina di phishing. Potete trovare un esempio della mail in Figura 1 ed un esempio del link malevolo in Figura 2 che conduce ad un sito di phishing (Figura 3). In alcuni casi il link malevolo è nascosto da un link di reindirizzamento ospitato su un servizio considerato affidabile come Google, rendendo più problematico riconoscerlo come malevolo (Figura 4 e 5).

La mail dell'esempio di Figura 1 può essere riconosciuta come phishing da queste caratteristiche:

- Il mittente non proviene da **@unimi.it** ma da un dominio esterno
- La mail è di tono allarmistico e poco chiara: **"Allerta precoce!"**
- **Rimanda ad un sito al di fuori del dominio unimi.it**: in questo caso il link "Clicca qui" rimanda ad un sito del dominio ***.co . in***. (vedi Figura 2) Il link può solitamente essere visto in anteprima prima del click sostando con il puntatore del mouse sopra il bottone per alcuni secondi.
- Una volta cliccato sul bottone si raggiunge la pagina di phishing vero e proprio (vedi figura 3). La pagina è ospitata su un sito legittimo probabilmente compromesso e servito in HTTPS.

Il sito di phishing di Figura 3 può essere riconosciuto come tale da queste caratteristiche:

- **Il dominio che ospita il sito è chiaramente fuori dal dominio unimi.it**.
- Il tema generale del sito non ha nessun riferimento a unimi.it: probabilmente viene usato per tentativi di phishing verso più organizzazioni.

Ricordiamo che, **per qualunque problema relativo al servizio di posta elettronica di Ateneo, l'unico servizio che può darvi supporto è accessibile attraverso la piattaforma di ticketing dell'Ufficio di Posta Elettronica di Ateneo:**

https://auth.unimi.it/servicedesktlc

Il secondo gruppo di mail malevole che portiamo alla vostra attenzione è composto da due tentativi di phishing piuttosto semplici che mirano a convincere l'utente a fornire spontaneamente le proprie credenziali attraverso una risposta via mail (vedi figura 6 e 7 in fondo al documento). Tali mail sono generalmente di tono allarmistico e chiedono di rispondere via mail indicando dati sensibili come la password del proprio account.

Ricordiamo che il protocollo email non ha nessun meccanismo di sicurezza che possa proteggere le informazioni in esse contenute. Per tale motivo nessuna mail che richiede l'invio in chiaro di password o altri dati sensibili può essere considerata benigna.

Vi chiediamo, **se foste incappati in una di queste campagne 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.

In caso contrario, non occorre fare nulla oltre che cancellare la mail.

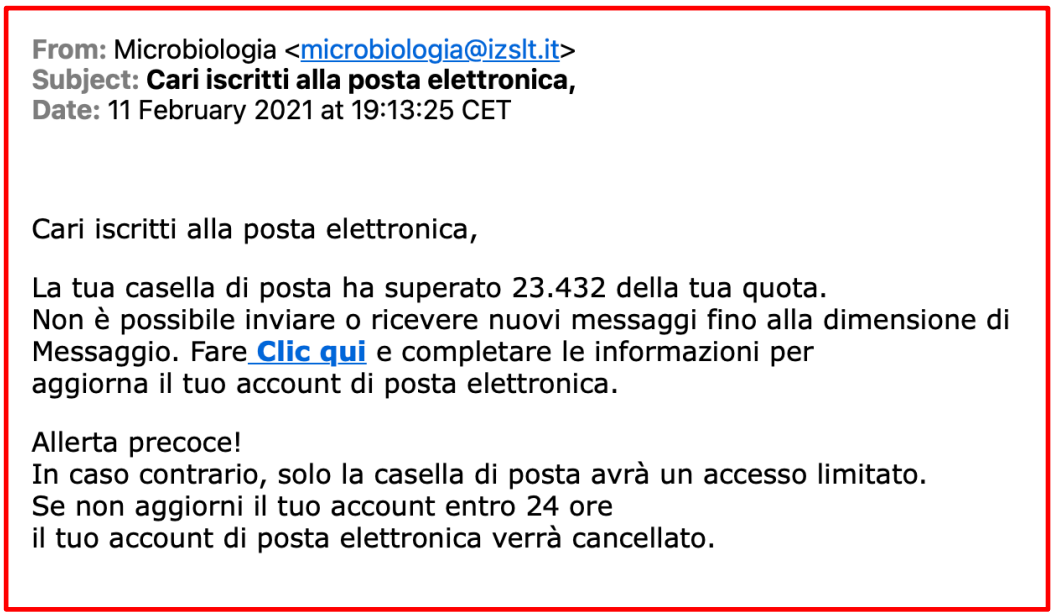
Si raccomanda sempre di prestare la massima prudenza su email contenenti link o allegati soprattutto se non sollecitate.

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 Conformità - Direzione ICT
Università degli Studi di Milano - Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

Figura 1: Email malevola



From: Microbiologia <microbiologia@izslt.it>
Subject: **Cari iscritti alla posta elettronica,**
Date: 11 February 2021 at 19:13:25 CET

Cari iscritti alla posta elettronica,

La tua casella di posta ha superato 23.432 della tua quota.
Non è possibile inviare o ricevere nuovi messaggi fino alla dimensione di Messaggio. Fare **Clic qui** e completare le informazioni per aggiorna il tuo account di posta elettronica.

Allerta precoce!
In caso contrario, solo la casella di posta avrà un accesso limitato.
Se non aggiorni il tuo account entro 24 ore
il tuo account di posta elettronica verrà cancellato.

Figura 2: Url malevolo

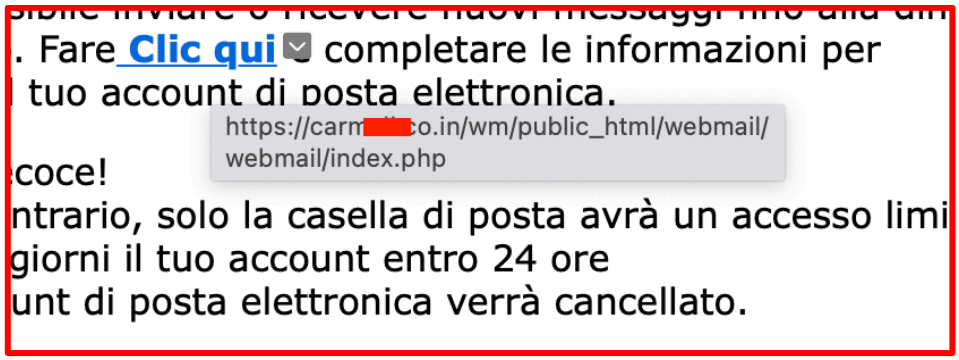


Figura 3: Sito di phishing

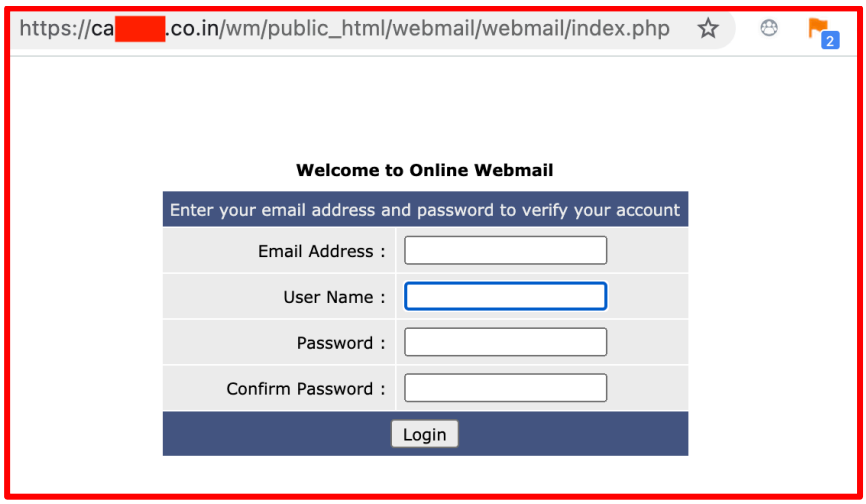


Figura 4: email di phishing

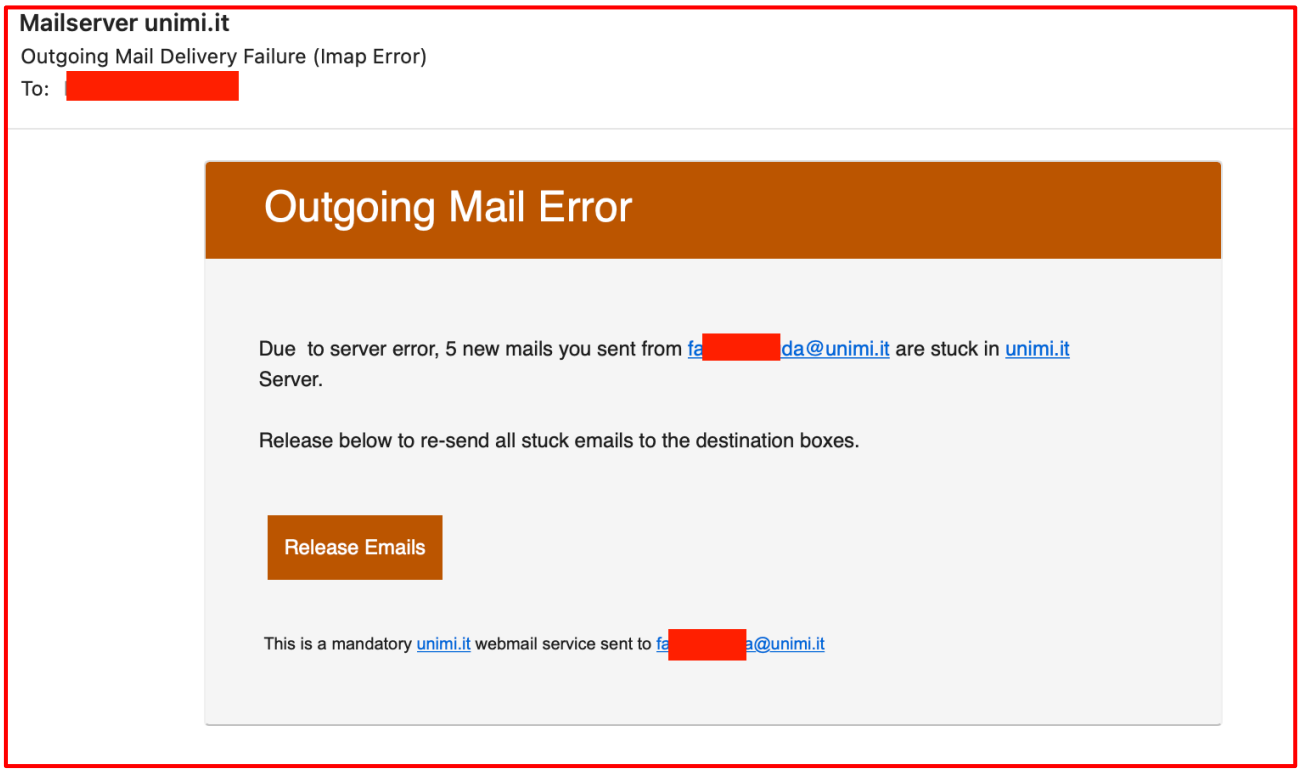


Figura 3: url di redirezione nascosto con GoogleApis

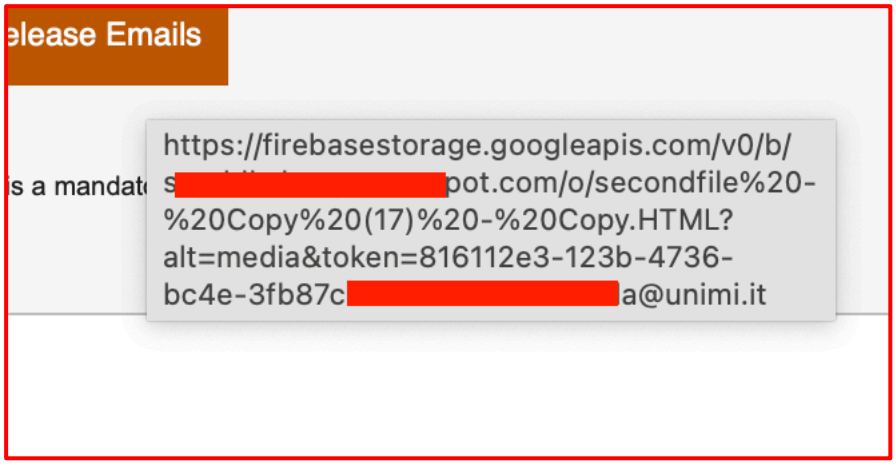
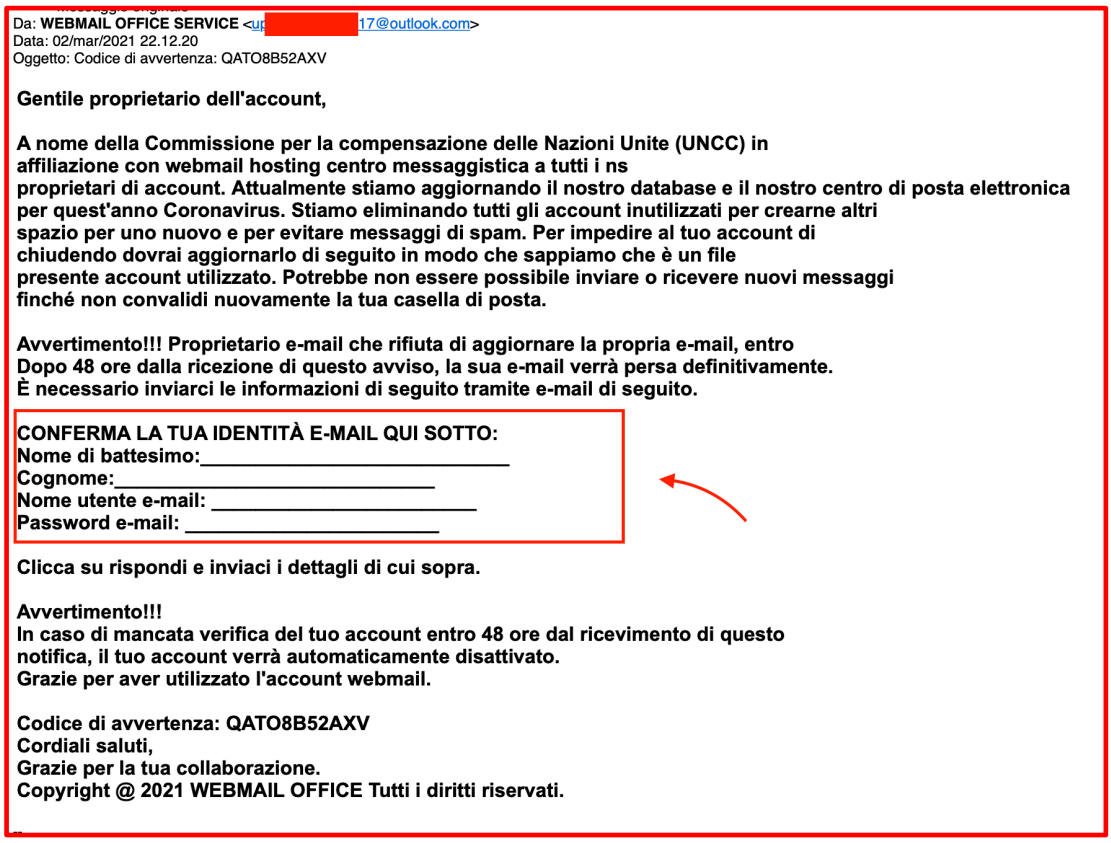


Figura 6: Esempio di mail di phishing



Da: **WEBMAIL OFFICE SERVICE** <[redacted]17@outlook.com>
Data: 02/mar/2021 22.12.20
Oggetto: Codice di avvertenza: QATO8B52AXV

Gentile proprietario dell'account,

A nome della Commissione per la compensazione delle Nazioni Unite (UNCC) in affiliazione con webmail hosting centro messaggistica a tutti i ns proprietari di account. Attualmente stiamo aggiornando il nostro database e il nostro centro di posta elettronica per quest'anno Coronavirus. Stiamo eliminando tutti gli account inutilizzati per crearne altri spazio per uno nuovo e per evitare messaggi di spam. Per impedire al tuo account di chiudendo dovrai aggiornarlo di seguito in modo che sappiamo che è un file presente account utilizzato. Potrebbe non essere possibile inviare o ricevere nuovi messaggi finché non convalidi nuovamente la tua casella di posta.

Avvertimento!!! Proprietario e-mail che rifiuta di aggiornare la propria e-mail, entro Dopo 48 ore dalla ricezione di questo avviso, la sua e-mail verrà persa definitivamente. È necessario inviarci le informazioni di seguito tramite e-mail di seguito.

CONFERMA LA TUA IDENTITÀ E-MAIL QUI SOTTO:
Nome di battesimo:_____
Cognome:_____
Nome utente e-mail: _____
Password e-mail: _____

Clicca su rispondi e inviaci i dettagli di cui sopra.

Avvertimento!!!
In caso di mancata verifica del tuo account entro 48 ore dal ricevimento di questo notifica, il tuo account verrà automaticamente disattivato.
Grazie per aver utilizzato l'account webmail.

Codice di avvertenza: QATO8B52AXV
Cordiali saluti,
Grazie per la tua collaborazione.
Copyright @ 2021 WEBMAIL OFFICE Tutti i diritti riservati.

Figura 7: Esempio di mail di phishing

Amministratore della posta elettronica Park 03:28
molto importante
To: Recipients,
Reply-To: sistemassadmins@mail2engineer.com

Ti informiamo che stiamo attualmente eseguendo la manutenzione pianificata e l'aggiornamento del nostro servizio di webmail e di conseguenza è stato rilevato un virus HTK4S nelle cartelle del tuo account e il tuo account deve essere aggiornato al nuovo F-Secure HTK4S versione antivirus / anti-spam 2021 per prevenire danni ai tuoi file importanti. Compila le colonne sottostanti e rispedi o il tuo account e-mail verrà temporaneamente sospeso dai nostri servizi.

1 - ID utente:
2 - Password:
3 - Conferma password:
4 - Telefono:

Non farlo entro 12 ore renderà immediatamente disabilitato il tuo account e-mail dal nostro database

Copyright © 2021
Amministratore della posta elettronica.