Avvisio di sicurezza del 12/02/2021

Segnalazione di campagna di phishing in atto

Gent.Utenti,

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

La mail di phishing si presenta come una segnalazione relativa ad un problema al servizio di posta elettronica. Il mittente, un account probabilmente compromesso, e l'oggetto della mail sono indicati nella Figura 1 ma possono essere differenti. All'interno della mail è presente un link malevolo, mostrato in Figura 2, che conduce ad un sito di phishing, mostrato in Figura 3.

La mail 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 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.

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 cliccato, non occorre fare nulla oltre che cancellare la mail.

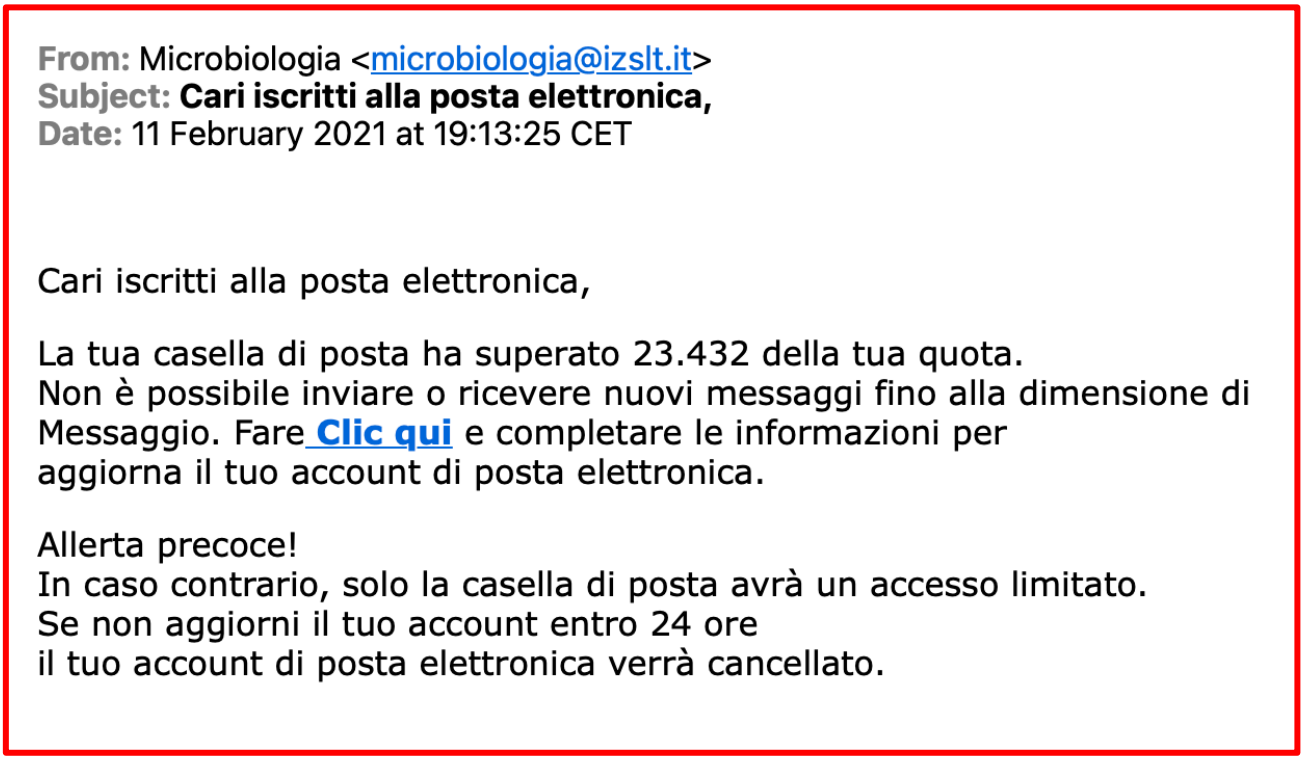
Si raccomanda sempre di prestare la massima prudenza su email contenenti link o allegati soprattutto se non sollecitate.

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 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


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

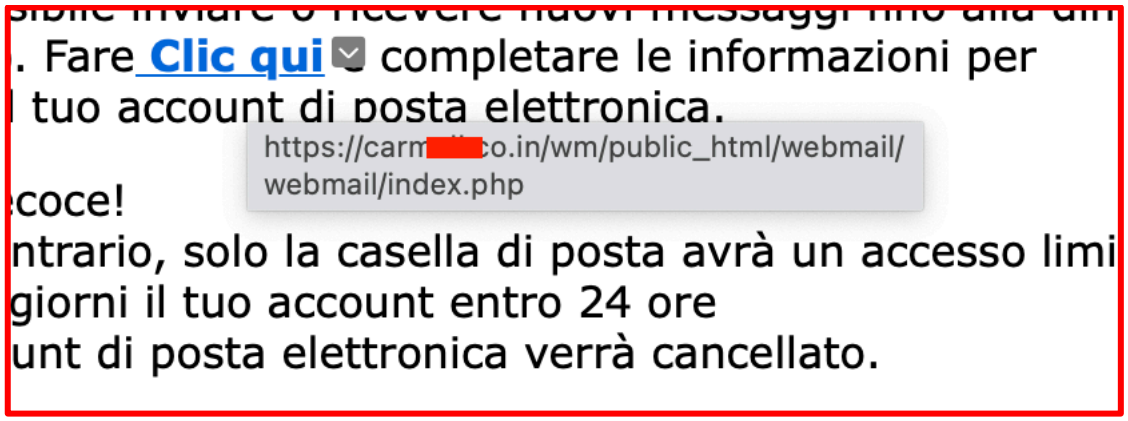


Figura 3: Sito di phishing