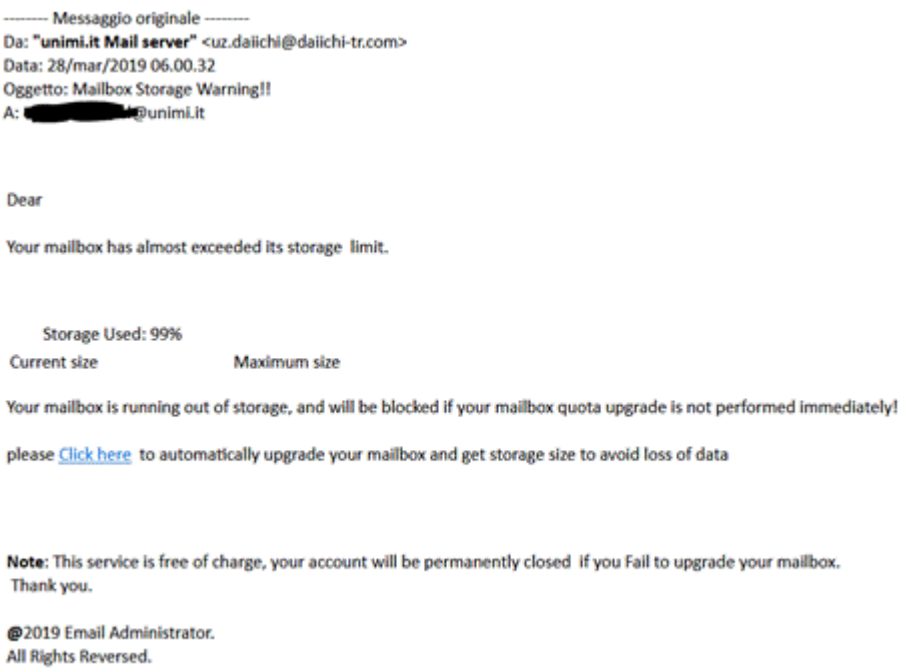
Campagna di phishing Mailbox Storage Warning!!

E’ attualmente in corso una nuova campagna di phishing, veicolata tramite la posta elettronica, il cui obiettivo è quello di **sottrarre ai loro destinatari le credenziali di Ateneo.**

Le email in esame **vengono apparentemente inviate da “unimi.it Mail server” e hanno come oggetto “Mailbox Storage Warning!!”.**

Ecco un esempio di mail:



-------- Messaggio originale --------
Da: **"unimi.it Mail server"** <uz.daiichi@daiichi-tr.com>
Data: 28/mar/2019 06.00.32
Oggetto: Mailbox Storage Warning!!
A: [redacted]@unimi.it

Dear

Your mailbox has almost exceeded its storage limit.

Storage Used: 99%
Current size Maximum size

Your mailbox is running out of storage, and will be blocked if your mailbox quota upgrade is not performed immediately!

please Click here to automatically upgrade your mailbox and get storage size to avoid loss of data

Note: This service is free of charge, your account will be permanently closed if you Fail to upgrade your mailbox.
Thank you.

@2019 Email Administrator.
All Rights Reversed.

Si fa presente che sia l'oggetto che il testo delle email potrebbero presentarsi con alcune modifiche.

Ci troviamo di fronte ad un tentativo di furto di credenziali, per cui invitiamo gli utenti interessati a:

- **non cliccare sul link riportato nell’email ricevuta;**
- **non rispondere all’email ricevuta;**
- **non compiere alcuna delle azioni suggerite nell’email ricevuta.**

L’Ufficio di Staff Sicurezza ICT, venuto a conoscenza della campagna in esame, ha attuato tutte le misure tecnologiche utili ad impedire dall'interno della rete di Ateneo la raggiungibilità del sito web malevolo linkato nel testo delle email in esame.

Tuttavia, **non è possibile escludere che, tra gli utenti a cui è stata consegnata la mail fraudolenta nella casella INBOX, ve ne sia qualcuno che abbia cliccato sul collegamento malevolo da una rete esterna ad Unimi** (ad es. reti cellulari/domestiche o reti di altri enti o fornitori di connettività a Internet).

Per coloro i quali abbiano riconosciuto la mail fraudolenta come sospetta e dunque non abbiano cliccato sul link in esse riportato e inserito le credenziali sul sito malevolo, **non è richiesta alcuna azione**.

Chiunque abbia ricevuto la mail fraudolenta e **inserito le proprie credenziali o altre informazioni** sul sito malevolo deve:

- effettuare un cambio repentino della password dell'account di posta di Ateneo all'indirizzo https://auth.unimi.it/password/newpwd.php e di qualunque altro servizio (anche esterno all'Ateneo) per il quale sono state utilizzate le stesse credenziali di accesso.

- segnalarlo all'Ufficio di Staff Sicurezza ICT tramite mail a sicurezza@unimi.it

- Inviare tempestivamente una mail all'Ufficio di Sicurezza ICT a sicurezza@unimi.it con le seguenti informazioni:

1. IP del dispositivo
2. Sistema operativo del dispositivo
3. Tipo di antivirus in possesso
4. Screenshot del risultato della scansione antivirus

Si raccomanda in generale a tutti gli utenti di utilizzare:

· **password per ciascun account univoche e robuste** (lunghezza idonea, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente);

· di impostare come domanda di controllo per il cambio password, una domanda la cui risposta non sia facilmente indovinabile o desumibile da informazioni disponibili in rete;

· cambiare le password regolarmente e con frequenza almeno ogni 6 mesi;

· non riutilizzare la stessa password a breve distanza di tempo;

· mantenere sistema operativo e antivirus aggiornati.

Ricordiamo infine che l'Ufficio Sicurezza ICT nella sezione dedicata del portale di Ateneo pubblica:

- **gli avvisi di sicurezza della campagne malevoli in atto al link https://work.unimi.it/servizi/security_gdpr/118606.htm**
- **le linee guida e indicazioni (tra cui quelle per proteggersi dal Phishing) al link https://work.unimi.it/servizi/security_gdpr/118582.htm**

Vi ringraziamo per la collaborazione.

Cordialmente,
Ufficio di Staff Sicurezza ICT

--