E' nuovamente in corso **una campagna di email phishing** il cui obiettivo è quello di **sottrarre agli utenti del servizio di posta elettronica le credenziali** utilizzabili per autenticarvisi e/o per autenticarsi tramite esse a qualunque altro servizio di Ateneo.

Ne **riportiamo il testo** di seguito, facendo presente che **potrebbe presentare alcune differenz**e rispetto a quello utilizzato per comporre il messaggio effettivamente ricevuto nella casella INBOX:

Oggetto: Aggiornamento dell'account

"Gentile utente

La tua quota di posta ha raggiunto il tuo limite. Non puoi inviare o ricevere nuovi messaggi finché non controlli di nuovo la tua casella di posta.

CLICCA QUI per controllare di nuovo la tua casella di posta

Supporto tecnico"

Attenzione! Ci troviamo di fronte ad un tentativo di truffa informatica per cui invitiamo gli utenti che abbiano ricevuto l'email in esame a:

- **non cliccare sul link** riportato nell'email ricevuta!
- **non inserire** le proprie **credenziali!**
- **non rispondere** al messaggio!

Cosa fare

L'Ufficio Sicurezza ICT di Ateneo ha attuato tutte le misure tecnologiche utili ad **impedire che dall'interno della rete di Ateneo sia possibile raggiungere la pagina web** che ospita il web form da compilare inserendo le proprie credenziali.

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).

Coloro i quali abbiano riconosciuto l'email fraudolenta come sospetta e dunque non abbiano cliccato sul link in essa riportato e inserito le credenziali sul sito malevolo, **non devono compiere alcuna azione**.

Solamente coloro che, ricevuta l'email fraudolenta, **abbiano inserito le proprie credenziali** sul sito malevolo devono:

- **segnalarlo all'Ufficio Sicurezza ICT di Ateneo** inviando un'email a: **sicurezza@unimi.it**
- **effettuare un cambio repentino della password** dell'account di posta di Ateneo accedendo a: 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.

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

1. **IP del dispositivo** utilizzato per navigare in rete
2. **Sistema operativo** installato sul dispositivo in uso
3. **Nome / tipo di antivirus** in possesso
4. **Screenshot del risultato della scansione** eseguita attraverso l'antivirus

Indicazioni di sicurezza sempre valide

In linea generale, raccomandiamo 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);
- **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**.

Al fine di poter gestire al meglio i tentativi di phishing e di malspam, chiediamo agli utenti che ricevono email sospette di:

- non cliccare sui link presenti nel testo;
- non rispondere;
- non scaricare / aprire eventuali allegati.

Inoltre, si invitano gli utenti ad inviare le future segnalazioni di spam a spam@unimi.it, mettendo in copia sicurezza@unimi.it solo nel caso in cui si ricevano email che possano rappresentare rischi di sicurezza, e quindi afferenti al nostro ufficio (alcuni esempi sono disponibili al link https://work.unimi.it/servizi/security_gdpr/118606.htm).

Cordialmente

Ufficio Sicurezza ICT di Ateneo- Direzione Generale