Gentilissimi utenti,

In queste ore è in corso una nuova campagna malevola di **phishing**, veicolata dal servizio di posta elettronica di UniMi, diretta a carpire credenziali di autenticazione al sistema di posta elettronica dell'Ateneo.

La mail in questione è così strutturata:


venerdì 28/12/2018 08:48

UNIMI MAIL <accounts@hear.to>

Re: Estremamente urgente

A

L'attività del tuo account di posta viola di recente i termini di servizio di unimi.it. Ci vorranno almeno 24 ore per controllare i termini e le condizioni di unimi.it La tua email verrà invalidata dal servizio senza fare nulla. Effettua il login con il tuo indirizzo e-mail e password per confermare la tua e-mail Conferma login, Clicca qui Oppure copia il link sottostante al browser e accedi http://transfertoyou.org/unimi.it/webmail/ GrazieGrazie milleIl team di unimi.it

Si fa presente che sia l'oggetto che il testo della mail potrebbe presentarsi con alcune varianti

L'Ufficio Sicurezza appena ne è venuto a conoscenza, ha provveduto a bloccare la raggiungibilità del sito dall'interno dell'Ateneo; tuttavia non è possibile escludere che, tra gli utenti a cui è stata consegnata la mail fraudolenta nella INBOX, ve ne sia qualcuno che abbia cliccato sul link malevolo da una rete esterna ad Unimi (ad es. reti cellulari/domestiche o reti di altri enti o fornitori di connettività a Internet).

Con la presente mail, l'ufficio Sicurezza intende avvisare gli utenti della campagna in atto e richiedere agli utenti di **non cliccare sui link**.

COSA FARE:
COSA FARE PER CHI AVESSE RICEVUTO LA MAIL MALEVOLA

Se avete ricevuto la mail fraudolenta e **avete cliccato sul LINK malevolo** dovete:

· Disconnettere il dispositivo dalla rete (scollegando il cavo di rete oppure spegnendo l'interfaccia wi-fi)

· Effettuare una scansione antivirus, e salvare lo screenshot del risultato

· **Da un pc non infetto** 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.

· Inviare tempestivamente una mail all'Ufficio di Sicurezza ICT tramite mail 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

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.**

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.