Sono in corso **nuove campagne malevole veicolate attraverso il servizio di posta elettronica.**

La campagna odierna risulta particolarmente insidiosa perché, col pretesto di richiedere un falso aggiornamento del certificato webmail unimi scaduto, induce gli utenti a compilare con le proprie credenziali Unimi un web form corredato del logo di Ateneo.

Le email in esame, di cui riportiamo un esempio, **presentano le seguenti caratteristiche:**

Oggetto: **Aggiorna il tuo certificato di posta elettronica**

Mittente: **UNIMI Amministratore**

Testo:

Gentile utente della webmail,

Il tuo certificato webmail unimi è scaduto e sta bloccando la configurazione del recapito della posta elettronica e delle impostazioni dell'account POP.

Devi aggiornare il tuo certificato webmail per non perdere email importanti. Per fare ciò, si prega di aggiornare le informazioni, seguendo il seguente link:

<link malevolo>
Quando le informazioni fornite corrispondono a quelle che abbiamo nel nostro database, il certificato webmail verrà aggiornato e funzionerà normalmente dopo il processo di verifica.

Cordiali saluti,
UNIMI Amministratore

Si fa presente che sia l'oggetto, che il testo dell'email potrebbero riportare delle variazioni.

Invitiamo gli utenti che interessati a:

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

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

Cosa fare

L'Ufficio di Staff Sicurezza ICT, venuto a conoscenza delle campagne di phishing 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, ed ha contattato il gestore della piattaforma per la rimozione immediata del form.

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) o precedentemente all'azione di blocco.

Chiunque abbia ricevuto la mail e abbia inserito le credenziali di Ateneo deve:

- effettuare un cambio repentino della password dell'account di Posta di Unimi
- segnalarlo all'Ufficio di Staff Sicurezza ICT tramite mail a sicurezza@unimi.it specificando a che ora è stata fornita la password (collegata a servizi Unimi) e ora di cambio password

Nel caso in cui la password fosse utilizzata anche su altri sistemi (interni o esterni al dominio Unimi) si richiede di cambiarla immediatamente su tutti i sistemi interessati, utilizzando un PC diverso da quello con cui si è acceduto al link.

Per coloro i quali abbiano riconosciuto la mail fraudolenta come sospetta e dunque non abbiano ceduto alcun dato sul sito segnalato, 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);
- attivare la domanda di controllo per il recupero della password
- 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;**
- **di non scaricare / aprire eventuali allegati.**

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**

Cordialmente

Ufficio di Staff Sicurezza ICT - Direzione Generale