

AVVISO DI SICUREZZA DEL 15.7.19– CAMPAGNA DI EMAIL PHISHING “WELCOME TO UNIVERSITÀ DEGLI STUDI DI MILANO - ONLINE SERVICES”

Gentilissimi Utenti,

vi inviamo la presente per avvisarvi del fatto che sono in atto **nuove campagne di email phishing**.

Veicolate attraverso il servizio di posta elettronica di Ateneo ed indirizzate, tra gli altri, ai possessori di un account istituzionale, hanno quale **obiettivo quello di sottrarre ai loro destinatari le credenziali di accesso ai servizi di Ateneo**.

Premesso tutto quanto sopra, con la presente comunicazione l'Ufficio di Staff Sicurezza ICT di Ateneo invita i destinatari della campagna di email phishing in esame a:

- **non cliccare sul collegamento al web form** sviluppato con finalità fraudolente e riportato nel testo dell'email malevola;
- **non inserire le proprie credenziali di accesso ai servizi di Ateneo** nei campi di input del web form di cui al punto precedente.

Attenzione!

NON devono compiere operazioni particolari, compreso l'invio di apposita segnalazione all'ufficio scrivente, coloro i quali NON avessero cliccato sul collegamento malevolo e NON avessero inserito le credenziali di accesso ai servizi @unimi utilizzando il web form.

Raccomandiamo a tutti voi di consultare frequentemente la sezione del portale di Ateneo dedicata alla sicurezza ICT e protezione dati e in particolare:

- **gli avvisi di sicurezza delle campagne malevole (tra cui quelle odierne) 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

Si invitano gli utenti a **consultare il file in allegato per proteggersi dalle campagne malevole di phishing veicolate tramite posta elettronica**.

Le email in esame, il cui **oggetto** è WELCOME TO UNIVERSITÀ DEGLI STUDI DI MILANO - ONLINE SERVICES, riportano un testo analogo al seguente:

Da: SA***** <s*****@uni*i.it>

Data: 15/lug/2019 09.41.35

Oggetto: WELCOME TO UNIVERSITÀ DEGLI STUDI DI MILANO - ONLINE SERVICES

Avviso generale,

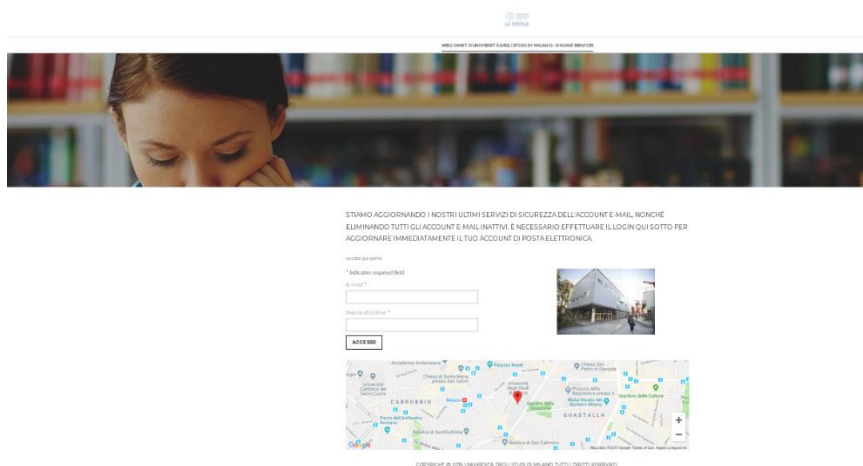
Stiamo aggiornando i nostri ultimi servizi di sicurezza dell'account e-mail, oltre all'eliminazione di tutti gli account e-mail inattivi. Ti chiediamo di fare clic sul link di aggiornamento qui sotto o copiare il link al browser del tuo dispositivo per aggiornare l'account della tua casella di posta.

https://u***f*milan-o*lineser*****s.weeb***.com/

Elaboreremo la tua richiesta una volta ricevute le tue informazioni.

Gestione.

Pagina web di destinazione del link malevolo:



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

L'Ufficio di Staff Sicurezza ICT, venuto a conoscenza della campagna di phishing in esame, ha attuato tutte le misure tecnologiche utili ad impedire dall'interno della rete di Ateneo la raggiungibilità del web form creato per scopi fraudolenti e linkato dall'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) o precedentemente all'azione di blocco.

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;
- verificare che sistema operativo e antivirus in uso siano aggiornati.

COSA FARE SOLO SE HAI INSERITO LE TUE CREDENZIALI DI ACCESSO AI SERVIZI @UNIMI (e non unimi)

Chiunque abbia inserito le credenziali di Ateneo nel web form dopo aver ricevuto l'email deve:

- **effettuare un cambio repentino della password** dell'account di Posta di Unimi, tramite il link <https://auth.unimi.it/password/>
- **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.

Ulteriori raccomandazioni

Si approfitta dell'occasione per ricordare altresì agli utenti quanto segue:

- 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.

Cordialmente

Ufficio di Staff Sicurezza ICT - Direzione Generale