Avviso di sicurezza del 21.10.19

Gentilissimi Utenti,

vi inviamo la presente per avvisarvi del fatto che **sono attualmente in corso due tentativi di frode informatica a cui prestare la massima attenzione** , invitandovi a **sensibilizzare colleghi e collaborator**i in merito ai possibili rischi di esserne vittima**.** Nello specifico:

1) una **Campagna di social engineering** il cui obiettivo è quello di **sfruttare l'identità di un utente noto** al suo destinatario (es. direttore o segretario di dipartimento Unimi) **per carpire informazioni e/o sottrargli denaro;**.

2) una **Campagna di email phishing** i cui destinatari sono invitati ad inserire lo proprie credenziali di autenticazione ai servizi Unimi utilizzando, a tal proposito, una **finta pagina di login** alla piattaforma web **Unimia.**

Per ulteriori approfondimenti e per ricevere indicazioni utili, **vi invitiamo a leggere nella sua interezza il presente messaggio** di posta elettronica.

Campagna di social engineering "Sei disponibile?"

Caratteristiche della campagna in corso

La **campagna di social engineering** in esame sfrutta **il legame di colleganza** o di semplice conoscenza instaurato con una persona (normalmente il direttore o il segretario di un dipartimento o un suo collaboratore) al fine **carpire al suo destinatario informazioni o di sottrargli denaro .**

Generalmente, tali tentativi di frode informatica sono caratterizzati da:

- **una prima fase in cui si ricerca un contatto** con la vittima, solitamente un segretario di dipartimento o un Suo collaboratore, **impersonificandoLa, attraverso un alias**, utilizzando un indirizzo mittente che potrebbe richiamare quello istituzionale e utilizzando la Sua firma. **Tipicamente questo contatto richiede una risposta alla mail con urgenza.**
- una seconda fase in cui il malintenzionato richiede un pagamento o informazioni riservate, fornendo delle scuse apparentemente plausibili

La buona riuscita di tale attacco informatico si basa sull'autorevolezza del finto mittente e sul panico, creato dall'urgenza della richiesta. Suggeriamo perciò di verificare sempre l'indirizzo email del mittente e, se persiste anche un minimo dubbio, di contattare il mittente su un altro canale ad esempio telefonicamente o inviando una *nuova* mail senza rispondere a quella sospetta.

Riportiamo, di seguito, un esempio di email thread, facendovi presente che sia l'oggetto, che il testo, che il mittente dell'email potrebbero variare:

Email n.1

From: **********
To: **********
Subject: URGENTE

Ciao xxxx! Sei disponibile ?
****
Professore e direttore di dipartimento
Dipartimento di **********
Università degli Studi di Milano
Via **********
20***** MILANO (MI)

(…)

Email n.2

Ho bisogno che tu mi aiuti a ottenere buoni regalo da qualsiasi negozio fuori dal campus, ti rimborserò quando arrivo in ufficio.? Devo inviarlo a un collega ed è molto importante perché sono ancora alla conferenza inaugurale e devo farlo spedire al più presto.? Puoi farlo per me, per favore?

****
Professore e direttore di dipartimento
Dipartimento di **********
Università degli Studi di Milano
Via **********
20***** MILANO (MI)

(…)

Email n.3
Aiutami gentilmente a ottenere quattro buoni regalo Amazon da EUR 100 da qualsiasi negozio.? Quello in totale, sarà di EUR 400.? Ti rimborserò non appena arrivo in ufficio.? Ho bisogno di carte fisiche, quindi mi aiuterai a prenderle dal negozio.? Quando li ottieni, basta grattare, scattare una foto delle carte con ricevuta, allegare all'e-mail e inviarla alla sua posta XXXXXXXXXXXX@gmail.com.? Grazie

****
Professore e direttore di dipartimento
Dipartimento di **********
Università degli Studi di Milano
Via **********
20***** MILANO (MI)

Cosa fare

Raccomandiamo di **non rispondere a questo tipo di email affrettatamente**, di **segnalare tempestivamente l'accaduto ai referenti informatici** del dipartimento, i quali inoltreranno le mail sospette all'Ufficio Sicurezza ICT (sicurezza@unimi.it), di avvisare **immediatamente i collaboratori della campagna in atto.**

Nel caso non siano presenti i referenti informatici nel dipartimento, si invita ad inoltrare le mail sospette all'Ufficio di Sicurezza ICT.

Campagna di email phishing "Messaggio in sospeso"

Caratteristiche della campagna in corso

La campagna di email phishing odierna mira alla **sottrazione delle credenziali di accesso ai servizi web istituzionali utilizzate** normalmente dagli **utenti Unimi.**

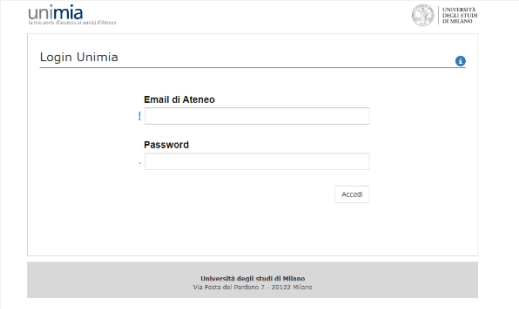
Le email in esame, il cui **oggetto è "unimi.it"** , sono apparentemente inviate dall'**Amministratore della web mail di Ateneo** e riportano un testo analogo al seguente**:**

Oggetto: unimi.it

Mittente: Admin <**********>

Hai un nuovo messaggio in sospeso; Clicca sul link qui sotto per leggere: http[:]//cas-uni**i-it[.]esy.***

Al clic sul link si atterrerà su una pagina web creata per finalità fraudolente (sottrazione di credenziali ai servizi Unimi) avente le caratteristiche illustrate dall'immagine seguente:



Cosa fare

SOLO SE HAI INSERITO LE TUE CREDENZIALI DI ACCESSO AI SERVIZI @UNIMI e non Unimi **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 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 a partire dal link.**

Attenzione! NON deve compiere alcuna operazione particolare, compreso l'invio di apposita segnalazione all' ufficio scrivente **chi non abbia cliccato sul collegamento malevolo e NON abbia inserito le credenziali di** accesso ai servizi @unimi utilizzando il web form.

Indicazioni valide in tutti i casi

L'Ufficio di Staff Sicurezza ICT, venuto a conoscenza della due campagne malevole 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 o che abbia effettuato un pagamento. Invitiamo gli utenti che interessati a:

- **non cliccare sul link riportato nell'email ricevute;**
- **non rispondere al messaggio e non continuare la conversazione via email**
- **non compiere alcuna delle azioni suggerite nell'email ricevuta; (es pagamento \ acquisto ecc.)**

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**.

Raccomandiamo a tutti voi, infine, 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 al link https://work.unimi.it/servizi/security_gdpr/118582.htm (tra cui quelle per proteggersi dal Phishing, che alleghiamo alla presente)**

Cordialmente

Ufficio Sicurezza ICT - Direzione Generale