Campagne di phishing "attenzione richiesta" e "Waiting for your reply"

In queste ore è stata registrata una nuova ondata di email, relativa alle campagne di phishing in oggetto, particolarmente insidiose, **scritte sia in lingua italiana che in altre lingue,** contenenti nell'oggetto la parola chiave "*Azione richiesta!*" (MAIL TIPO 1) o "*Waiting for your reply"* (MAIL TIPO 2) (in allegato alcuni esempi di email). Si fa presente che sia l'oggetto che il testo delle email potrebbero presentarsi con alcune modifiche.

L'Ufficio di Staff Sicurezza ICT di Ateneo chiede agli utenti di **non cliccare sui link, effettuare pagamenti, aprire eventuali allegati sospetti e non inserire credenziali di unimi su siti non affidabili**

Raccomandiamo, inoltre, di consultare frequentemente la sezione del portale di Ateneo dedicata alla sicurezza ICT e protezione dati. Sono reperibili al link https://work.unimi.it/servizi/security_gdpr/118606.htm gli avvisi di sicurezza delle campagne malevole in atto con le istruzioni dettagliate.

Invitiamo gli utenti a consultare le linee guida e indicazioni (tra cui quelle per proteggersi dal Phishing) al link https://work.unimi.it/servizi/security_gdpr/118582.htm. e aprendere visione del pdf con le relative istruzioni in allegato.

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**

Cosa fare se si è cliccato sui link

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 della 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).

MAIL DI TIPO 1

Chiunque abbia ricevuto la mail fraudolenta e **inserito le proprie credenziali o altre informazioni sul sito malevolo deve:**

- segnalarlo all'Ufficio di Staff Sicurezza ICT tramite mail a sicurezza@unimi.it
- 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 a sicurezza@unimi.it con le seguenti informazioni:
    - IP del dispositivo
    - Sistema operativo del dispositivo
    - Tipo di antivirus in possesso
    - Screenshot del risultato della scansione antivirus

MAIL DI TIPO 2

Chiunque abbia ricevuto la email fraudolenta e abbia cliccato sul link malevolo deve:

- disconnettere il dispositivo dalla rete (scollegando il cavo di rete oppure spegnendo l'interfaccia wi-fi)
- avvisare e chiedere assistenza al referente informatico della struttura di appartenenza se presente
- effettuare una scansione antivirus, e salvare lo screen 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 una email all'Ufficio di Staff Sicurezza ICT all'indirizzo sicurezza@unimi.it indicando le seguenti informazioni:

    - tipo di problema (indicazione della mail di spam ricevuta)
    - IP del dispositivo
    - sistema operativo del dispositivo
    - tipo di antivirus in possesso
    - screenshot del risultato della scansione antivirus

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;
- mantenere sistema operativo e antivirus aggiornati.

Cordialmente

Ufficio di Staff Sicurezza ICT - Direzione Generale