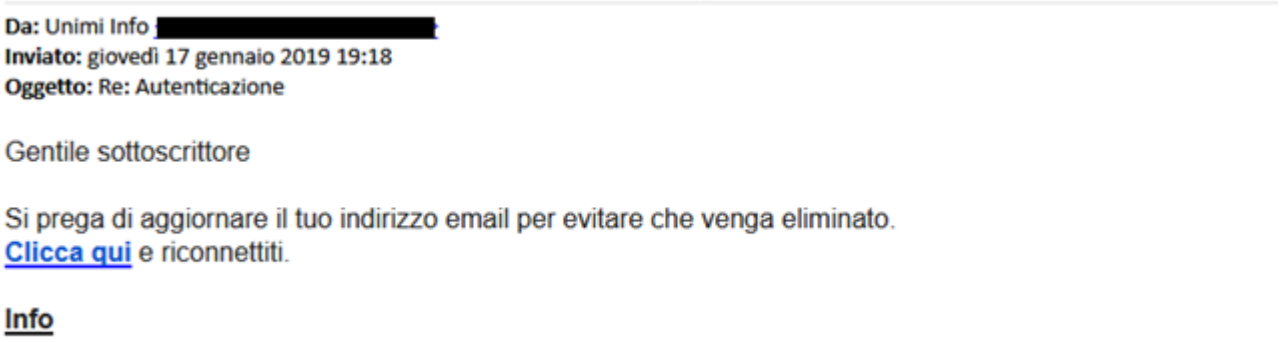
Avviso di sicurezza

Sono in corso nuove campagne di phishing malevolo veicolate attraverso il servizio di posta elettronica di Ateneo il cui obiettivo è carpire credenziali di autenticazione al sistema di posta elettronica dell'Ateneo e/o veicolare virus.

Le email in esame, di cui alleghiamo un esempio, richiede di cliccare su un link **con il falso scopo** di aggiornare la propria mail di ateneo.



Da: Unimi Info [redacted]
Inviato: giovedì 17 gennaio 2019 19:18
Oggetto: Re: Autenticazione

Gentile sottoscrittore

Si prega di aggiornare il tuo indirizzo email per evitare che venga eliminato.
Clicca qui e riconnettiti.

Info

Ci troviamo di fronte ad un tentativo di truffa informatica, per cui invitiamo gli utenti che interessati a:

- non cliccare sul link riportato nell'email ricevuta;
- non rispondere all'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 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).

Chiunque abbia ricevuto la mail fraudolenta e **inserito le proprie credenziali** 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:

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;
- 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;
- non scaricare / aprire eventuali allegati.

Inoltre, si invitano gli utenti ad inviare le future segnalazioni di spam a spam@unimi.it, mettendo in copia sicurezza@unimi.it solo nel caso in cui si ricevano email che possano rappresentare rischi di sicurezza, e quindi afferenti al nostro ufficio (alcuni esempi sono disponibili al link https://work.unimi.it/servizi/security_gdpr/118606.htm).

Cordialmente

Ufficio di Staff Sicurezza ICT - Direzione Generale