Campagna di phishing “Notifica in sospeso”

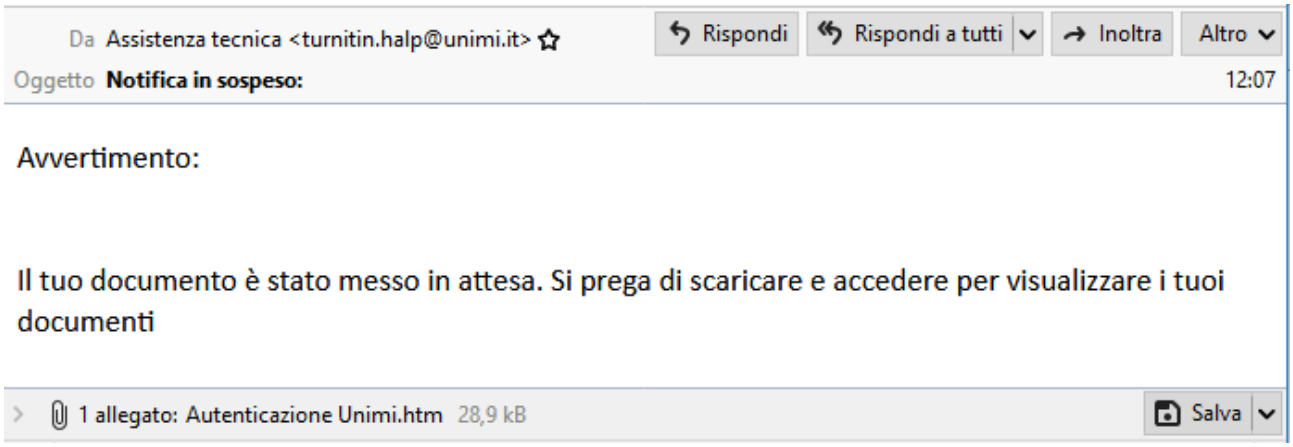
Gentilissimi utenti,

E’ attualmente in corso una nuova campagna di phishing, veicolata attraverso la posta elettronica con l’obiettivo di rubare le credenziali della posta di Ateneo e veicolare virus.

La campagna odierna risulta particolarmente insidiosa perché contiene in allegato una pagina html che riproduce la pagina web di accesso alla posta elettronica di Ateneo.

Le email in esame **vengono apparentemente inviate da un indirizzo di posta del dominio @unimi.it e hanno come oggetto “Notifica in sospeso”.**

Ecco un esempio di mail:



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 aprire l’allegato**
- **non rispondere all’email ricevuta;**
- **non compiere alcuna delle azioni suggerite nell’email ricevuta.**

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.

Chiunque avesse erroneamente cliccato e aperto l'allegato è invitato a:

- Disconnettere il dispostivo dalla rete
- Effettuare una scansione antivirus, e salvare lo screen del risultato
- Inviare una email all'Ufficio di Staff Sicurezza ICT all'indirizzo sicurezza@unimi.it, **tramite un pc non infetto,** precisando nell'oggetto la campagna malevola, ed indicando le seguenti informazioni:
    - IP del dispositivo
    - sistema operativo del dispositivo
    - tipo di antivirus in possesso
    - screenshot del risultato della scansione antivirus

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.

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