Sono in corso **nuove campagne malevole** veicolate attraverso il servizio di posta elettronica di Ateneo, il cui obiettivo è indurre i loro destinatari ad inserire credenziali di Ateneo o scaricare malware.

L'Ufficio di Staff Sicurezza ICT di Ateneo intende:

- avvisare gli utenti delle campagne in atto
- richiedere agli utenti di **non cliccare sul link, effettuare pagamenti, inserire credenziali o aprire eventuali allegati sospetti**

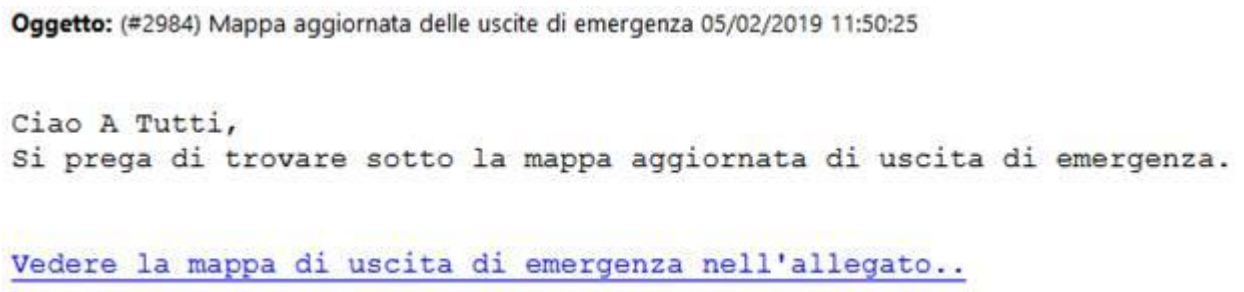
Raccomandiamo agli utenti di consultare frequentemente la sezione del portale di Ateneo dedicata alla sicurezza ICT e protezione dati e in particolare:

- **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 veicolate tramite posta elettronica.

Le email in esame, di cui riportiamo un esempio, **presentano le seguenti caratteristiche:**

MAIL DI TIPO 1



Oggetto: (#2984) Mappa aggiornata delle uscite di emergenza 05/02/2019 11:50:25

Ciao A Tutti,
Si prega di trovare sotto la mappa aggiornata di uscita di emergenza.

Vedere la mappa di uscita di emergenza nell'allegato..

MAIL DI TIPO 2

Oggetto: Fw: fattura emessa HJB 598716

Salve Gentile Cliente,

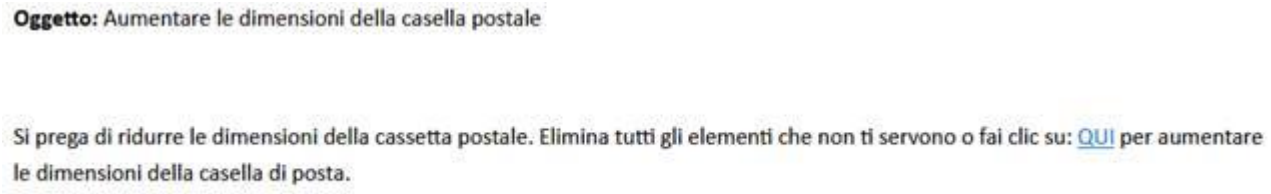
Come da voi desiderato Come concordato allego alla presente fattura N.ĩ‹ HJB 598716 del 04.10.2018 rimasta in sospeso. Fattura disponibile

---

[redacted]
Cordiali Saluti

Vi ricordiamo che siete tenuti a stampare e conservare la fattura allegata come da art. 90 -- SFO 618/07, succ. modifiche e da risoluzione Ministero delle Finanze R.M. 18.11.1990 Nessuna copia verra' inviata a mezzo servizio postale.

MAIL DI TIPO 3



Oggetto: Aumentare le dimensioni della casella postale

Si prega di ridurre le dimensioni della cassetta postale. Elimina tutti gli elementi che non ti servono o fai clic su: QUI per aumentare le dimensioni della casella di posta.

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 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 delle 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 siano aggiornati.**

Per coloro i quali abbiano riconosciuto la mail fraudolenta come sospetta e dunque abbiano ignorato l'email e non abbiano cliccato sul link **non è richiesta alcuna azione,** si prega quindi di non rispondere alla presente comunicazione.

COSA FARE IN CASO DI MAIL DI TIPO 1 o 2

Chiunque avesse erroneamente cliccato sul link o aperto un allegato è invitato a:

- effettuare una scansione antivirus, e salvare lo screen del risultato
- inviare una email all'Ufficio di Staff Sicurezza ICT all'indirizzo sicurezza@unimi.it indicando le seguenti informazioni:

    1. tipo di problema (indicazione della mail di spam ricevuta)

2. IP del dispositivo
3. sistema operativo del dispositivo
4. tipo di antivirus in possesso
5. screenshot del risultato della scansione antivirus

COSA FARE IN CASO DI MAIL DI TIPO 3

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, 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.

Ufficio di Staff Sicurezza ICT - Direzione Generale