Sono in corso **nuove campagne malevole veicolate attraverso il servizio di posta elettronica di Ateneo il cui obiettivo è indurre i loro destinatari ad effettuare il possibile download sul dispositivo utilizzato di un allegato malevolo.**

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

Oggetto: (#2653) !!Mappa aggiornata delle uscite di emergenza

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

Vedere la mappa di uscita di emergenza nell'allegato.. (link malevolo)

Grazie,
**********,
Gestione Immobiliare

Si fa presente che sia l'oggetto, che il testo dell'email potrebbero riportare delle variazioni.

Cosa fare

L'Ufficio di Staff Sicurezza ICT, venuto a conoscenza delle campagne di malspam 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.**

Chiunque abbia ricevuto la mail, inoltre, deve segnalarlo all'Ufficio di Staff Sicurezza ICT tramite mail a sicurezza@unimi.it

Per coloro i quali abbiano riconosciuto la mail fraudolenta come sospetta e dunque abbiano ignorato l'email / non abbiano cliccato sul link non è richiesta alcuna azione.

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.**

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