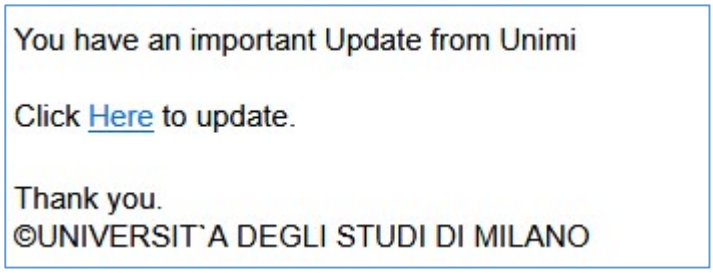
Gent.issimi utenti

Sono in corso **nuove campagne malevole veicolate attraverso il servizio di posta elettronica. La campagna odierna è un tentativo di furto di credenziali.**

Le email in esame, di cui alleghiamo un esempio, **hanno il seguente contenuto:**


You have an important Update from Unimi

Click Here to update.

Thank you.
©UNIVERSIT`A DEGLI STUDI DI MILANO

Si fa presente che sia l'oggetto che il testo delle email potrebbero presentarsi con alcune modifiche.

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.

Invitiamo gli utenti che interessati a:

- non rispondere all'email ricevuta;
- **non cliccare su eventuali link nell'email ricevuta;**
- non compiere alcuna delle azioni suggerite nell'email ricevuta;
- non scaricare / aprire eventuali allegati sospetti.

Ricordiamo infine che l'Ufficio Sicurezza ICT nella sezione dedicata del portale di Ateneo pubblica:

- **Gli avvisi di sicurezza della campagne malevoli in atto (tra cui l'attuale) 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**
- **In allegato le istruzioni per proteggersi dal phishing**

Sono inoltre disponibili dei test europei di autoapprendimento con l'obiettivo di promuovere la sicurezza informatica tra i cittadini e le organizzazioni; per sensibilizzare in modo semplice ed efficace **alle minacce informatiche** e ai **metodi** per contrastarle, attraverso l'**educazione** e la **condivisione di buone pratiche**.

Invitiamo caldamente a provare a rispondere ai suddetti questionari che potete trovare alla pagina: https://work.unimi.it/servizi/security_gdpr/118604.htm

Cordialmente

Ufficio di Staff Sicurezza ICT - Direzione Generale