Avviso di sicurezza del 25/05/2022

Segnalazione di campagne malevole in atto veicolata attraverso un allegato Excel contenente macro

Gentili Utenti,
pubblichiamo questo avviso per segnalarvi una campagna malevola in atto in queste ore che ha raggiunto gli account di posta elettronica di Ateneo. La mail contiene un allegato malevolo in formato Excel contenente macro.

Di seguito trovate la descrizione dettagliata della campagna.

Ricordiamo di prestare sempre la massima attenzione agli allegati e ai link presenti nelle mail inaspettate; scansionate sempre gli allegati prima di aprirli con un antivirus aggiornato.

Per ulteriori informazioni e segnalazioni di mail sospette, scrivete all'indirizzo di posta sicurezza@unimi.it , eventualmente inoltrando le mail sospette come allegato.

Settore Cybersecurity, Protezione Dati e Conformità - Direzione ICT
Università degli Studi di Milano
Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

UNIMI-SOC-202205230000000004 Per favore, usate questo riferimento per ulteriori comunicazioni su questa segnalazione

Campagna malevola veicolata attraverso un allegato Excel contenente macro

Gent. Utenti,
pubblichiamo questo avviso per segnalarvi una campagna malevola in atto in queste ore che ha raggiunto il vostro account di posta. Di seguito a questo documento potete trovare un esempio.
La mail malevola si può presentare in vari modi e generalmente è estremamente stringata e di contenuto incerto. Allegato alla mail è presente un file malevolo in formato Excel macro. Il mittente, un account probabilmente compromesso, è solitamente di un dominio anonimo spesso mascherato per sembrare proveniente da UniMi. Qui trovate una guida per analizzare in autonomia l'header nascosto delle mail sospette:

https://work.unimi.it/filepub/sicurezza_ict/DICT_IO_GuidaPraticaAnalisiMail_rev.3del16062021.pdf

La mail può essere riconosciuta come phishing da queste caratteristiche:

- L'effettivo mittente non proviene da un dominio riferibile all'Ateneo.
- La mail contiene un file in formato *xls* che può contenere codice malevolo. Una volta aperto, viene richiesto di eseguire macro.

Il Settore Cybersecurity, Protezione dati e Conformità della direzione ICT ha attuato le operazioni necessarie a contrastare le campagne in atto.

Se non avete aperto il file *xls* e non avete attivato le macro, non occorre fare nulla oltre che cancellare la mail.
Se avete aperto il file *xls* e avete attivato le macro occorre:

- Cambiare immediatamente la password attraverso il sito istituzionale:
  https://auth.unimi.it/password
- Effettuare una scansione completa del dispositivo con un antivirus aggiornato.
- Darne rapida comunicazione, sicurezza@unimi.it avendo cura di specificare l'orario indicativo in cui si è aperto il file malevolo e l'orario in cui è stato effettuato il cambio della password.

Si raccomanda sempre di prestare la massima prudenza su e-mail contenenti link o allegati soprattutto se non sollecitate.

Altre informazioni su come migliorare la sicurezza dell'Ateneo possono essere trovate sul portale istituzionale al link: https://work.unimi.it/servizi/security_gdpr/118546.htm

-------- Messaggio originale --------
Da: [redacted] <commerciale@dedaloass.it>
Data: 20/mag/2022 17.52.55
Oggetto: Re:
A: [redacted]

spiacente, ma non è possibile.

mittente non unimi

[redacted]

La Statale per il futuro
Salute, transizione digitale, sostenibilità
Il tuo 5xmille ai nuovi progetti di ricerca dell'Università degli Studi di Milano
Codice fiscale: 80012650158

file malevolo xls

Nuovo
docum....20.xls