Gentilissimi /e,

in queste ore è nuovamente in corso in Italia **una campagna di malspam con allegati malevoli** veicolata attraverso la posta elettronica di Ateneo.

Le email presentano caratteristiche analoghe alle seguenti:

Oggetto: Relazione di notifica decreto N.616******** Del 13/07/2019

Contenuto:

Io sottoscritto Avvocato ********** con studio a Agrigento situato in ********** AGOSTINO , 9*4 P. IV A:83**********55 nella mia qu al ita di di fensore e domici liatario del Sig. Paolo **********, res. a Agrigento indirizzo ********** , 515

COMUNICO
Ad ogni valid ita di leg ge l'a sent enza Numero 83**********9 in originale digitale

Che lo po visua liz zare al seg uente link: Decreto (ovvero) i n copia digitale conf orme all'originale digitale da me pre disposto nel giudizio civile dinanzi al Trib unale di Agrig ento , mediante i nvio di messa ggio d i posta ele ttronica dalla mia ca sella, e con ricevuta completa, alla tua email Attesto infine che il messaggio , oltre all a presente relata di notifica sot toscritta digitalmente, contiene il seguente Se ntenza ch e lo po sca ricare al se guente link: Doc umenti anch'essi sottoscritti d igitalmente: – copia info rmatica della atto.

Si fa presente che sia l'oggetto che il testo dell' email potrebbe presentarsi con alcune varianti

L'Ufficio Sicurezza appena ne è venuto a conoscenza, ha provveduto a bloccare la raggiungibilità del sito dall'interno dell'Ateneo; tuttavia non è possibile escludere che, tra gli utenti a cui è stata consegnata la mail fraudolenta nella INBOX, ve ne sia qualcuno che abbia cliccato sul link malevolo da una rete esterna ad Unimi (ad es. reti cellulari/domestiche o reti di altri enti o fornitori di connettività a Internet).

Con la presente mail, l'ufficio Sicurezza intende avvisare gli utenti della campagna in atto e richiedere agli utenti di **non cliccare sul link**

COSA FARE
Chiunque abbia ricevuto la mail fraudolenta e abbia cliccato sul link al sito malevolo deve:

- Disconnettere il dispositivo dalla rete (scollegando il cavo di rete oppure spegnendo l'interfaccia wi-fi)
- Contattare il Referente della struttura di afferenza per avere un opportuno supporto informatico.
- Effettuare una scansione antivirus, e salvare lo screen del risultato

- **Da un pc non infetto** effettuare un cambio repentino della password dell'account di posta di Ateneo all'indirizzo https://auth.unimi.it/password/newpwd.php e di qualunque altro servizio (anche esterno all'Ateneo) per il quale sono state utilizzate le stesse credenziali di accesso.
- Inviare una mail all'Ufficio di Sicurezza ICT tramite mail a sicurezza@unimi.it con le seguenti informazioni:

    1. Ip del dispositivo
    2. Sistema operativo del dispositivo
    3. Tipo di antivirus in possesso
    4. Screenshot del risultato della scansione antivirus

Si raccomanda in generale a tutti gli utenti di utilizzare:

- password per ciascun account univoche e robuste (almeno 8 caratteri, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente);
- di impostare come domanda di controllo per il cambio password, una domanda la cui risposta non sia facilmente indovinabile o desumibile da informazioni disponibili in rete;
- cambiare le password regolarmente e con frequenza almeno ogni 6 mesi;
- non riutilizzare la stessa password a breve distanza di tempo.

Ulteriori informazioni saranno reperibili sul portale notizie Unimi
http://www.unimi.it/personale/122020.htm

Cordialmente
Ufficio Sicurezza ICT - Direzione Generale