Avviso di sicurezza del 6.3.19

Sono attualmente in corso nuove campagne di malspam **il cui obiettivo è quello di infettare con un malware il dispositivo utilizzato dai loro destinatari**. Le email in esame **utilizzano il riferimento ad un documento di fatturazione elettronica che si è invitati a consultare.** Riportiamo, di seguito, il testo delle email in esame:

Oggetto: Fv: fatture emessa U***53*1
A: ****@unimi.it

Salve Gentile Cliente,

In allegato Vi inviamo come da Voi richiesto il documento U***53*1 del 11.10.2018 Documento disponibile qui

D**** R********
Cordiali Saluti

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

L'Ufficio di Staff Sicurezza ICT di Ateneo intende:

- avvisare gli utenti delle campagne in atto
- richiedere agli utenti di **non cliccare sul link / non aprire eventuali allegati sospetti / non inserire credenziali se richieste**
- **richiedere di non rispondere all' email**
- **raccomandare agli utenti di consultare regolarmente la sezione Avvisi dell'Ufficio di Staff Sicurezza ICT** presente sul portale di Ateneo, sempre aggiornato sulle nuove campagne malevoli http://www.unimi.it/personale/122020.htm

Cosa fare

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).

Solo chi avesse cliccato sul link e/o scaricato il file malevolo è invitato a:

- **isolare il pc dalla rete**
- **effettuare la scansione del dispositivo con un antivirus aggiornato e a salvare lo screenshot** del risultato ottenuto
- **contattare repentinamente l'Ufficio Sicurezza ICT per ricevere istruzioni in merito a come operare, inviando un' email a: sicurezza@unimi.it** (specificando

possibilmente come suo oggetto " Nuova campagna di malspam con link a finti documenti di fatturazione")

In tutti gli altri casi non è richiesto lo svolgimento di alcuna operazione.

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

Vi ringraziamo per la collaborazione.

Cordialmente,
Ufficio di Staff Sicurezza ICT