Campagna di Social engineering / malspam con allegato malevolo

Gentilissimi,

è attualmente in corso una nuova campagna di **social engineering / malspam il cui obiettivo è quello di entrare il contatto con i suoi destinatari per compiere azioni malevole** di varia natura e/o **infettare il dispositivo** del loro destinatario **con un allegato malevolo.**

Caratteristiche dell'email

Le email in esame, il cui contenuto è variabile,

- potrebbero essere state inviate insieme con **un allegato malevolo (es. fattura in formato Excel)**
- potrebbero / sono **apparentemente inviate da persone note al loro destinatario**
- potrebbero aver assunto un tono allarmistico

Ne riportiamo, di seguito, due esempi:

Oggetto: **Invio documento rif.XXXXXXXXX del 25/09/2019 in formato elettronico**

Salve, posso parlarti via e-mail.

A presto

E*******a S****etti

Da: p********** <mrmolina@labomega.com.ar>

Oggetto: Invio documento rif.38835863 del 27/09/2019 in formato elettronico

Distinti saluti
P**********
p*****.******a@unimi.it

Si fa presente che il testo dell'email, il suo mittente ed il suo oggetto potrebbero variare.

L'Ufficio di Staff Sicurezza ICT invita gli utenti a:

- **non rispondere all'email ricevuta;**
- **non aprire eventuali allegati.**

Per coloro i quali abbiano riconosciuto la mail fraudolenta come sospetta, dunque abbiano ignorato l'email e non abbiano aperto l'allegato, **non è richiesta alcuna azione**.

Chiunque avesse erroneamente risposto all'email (e aperto un eventuale allegato) è invitato a:

- **Non proseguire la conversazione**
- **Non compiere alcuna delle azioni suggerite**

Chiunque avesse erroneamente cliccato e aperto l'allegato è invitato a:

- Disconnettere il dispostivo dalla rete
- Effettuare una scansione antivirus, e salvare lo screen del risultato
- Inviare una email all'Ufficio di Staff Sicurezza ICT all'indirizzo sicurezza@unimi.it, **tramite un pc non infetto,** precisando nell'oggetto la campagna malevola, ed indicando le seguenti informazioni:
  - IP del dispositivo
  - sistema operativo del dispositivo
  - tipo di antivirus in possesso
  - screenshot del risultato della scansione antivirus

Vi informiamo del fatto che gli avvisi di sicurezza relativi alle campagne malevoli in atto sono consultabili al seguente url: https://work.unimi.it/servizi/security_gdpr/118606.htm

Vi ringraziamo per la collaborazione.

Cordialmente,
Ufficio di Sicurezza ICT – Direzione Generale