Gentilissimi,

è attualmente in corso una campagna di **malspam** il cui obiettivo è quello **di compromettere il dispositivo** utilizzato dai suoi destinatari **attraverso l'invio di un allegato malevolo (pseudofattura in formato Ms Excel \ Ms Word \ Pdf).**

Caratteristiche delle email

Le email in esame, **il cui testo potrebbe variare di volta in volta al pari del mittente**,

- riportano nell'oggetto un riferimento alla "**Fatturazione Elettronica**"
- sono state inviate insieme con **un allegato**
- hanno quale mittente, in **apparenza**, una **persona nota** ai loro destinatari o sembrano apparentemente inviate da una persona da essi conosciuta.

Ne riportiamo, di seguito, un esempio:

Oggetto: Fatturazione elettronica

```
Buongiorno,

in allegato la fattura di settembre.


Grazie e Saluti,
G**** ******
m*********.g****@unimi.it
```

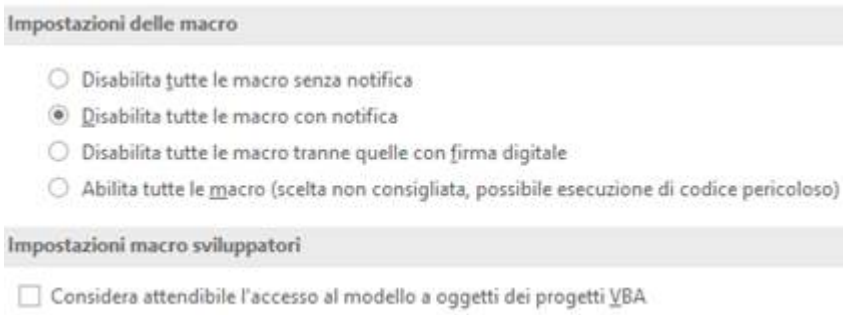
Cosa fare

In linea generale, l'Ufficio di Sicurezza ICT invita gli utenti destinatari della presente campagna di malspam a:

- **non aprire eventuali allegati**
- **non rispondere all'email ricevuta**
- **non compiere alcune delle operazioni suggerite** attraverso il messaggio di posta elettronica.

Si fa presente, altresì, che l'attivazione delle macro (una serie di comandi che possono essere utilizzati per automatizzare operazioni ricorrenti**)** nei file di **MS Office e simili potrebbe rappresentare un rischio per la sicurezza dei dispositivi** utilizzati per aprire gli allegati ricevuti tramite email**.**

Si consiglia, pertanto, di verificare che l'Opzione "Disabilita tutte le macro con notifica" (utilizzando Ms Word o Excel: File -> Opzioni -> Centro di Protezione -> Impostazioni Centro di Protezione) **sia attiva o di effettuare la loro disattivazione.**



Si specifica che, una volta **acquisita la certezza dell'affidabilità della fonte delle macro**, è possibile riabilitarle.

Per ulteriori informazioni, si consiglia di consultare la documentazione ufficiale delle applicazioni utilizzabili per aprire i file ricevuti (Ms Office: cfr. https://support.office.com/it-it/article/attivazione-o-disattivazione-di-macro-nei-file-di-office-12b036fd-d140-4e74-b45e-16fed1a7e5c6).

Non è richiesto il compimento di alcuna azione a coloro i quali avessero riconosciuto l'email di cui scriviamo come sospetta e, di conseguenza, l'abbiano ignorata e non abbiano aperto o scaricato l'allegato.

Chiunque avesse erroneamente cliccato e aperto / scaricato l'allegato e/o risposto all'email è invitato a:

- **Non proseguire la conversazione**

- **Disconnettere il dispostivo dalla rete**
- **Effettuare una scansione antivirus**, e salvare lo screen del risultato
  - **Inviare una email all'Ufficio di Sicurezza ICT** (email: sicurezza@unimi.it) **tramite un pc non infetto,** precisando nell'oggetto un riferimento alla campagna malevola ed indicando le seguenti informazioni:

    - IP del dispositivo in uso
    - 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 Sicurezza ICT – Direzione Generale