

- **Oggetto:** CSIRT-MIM - Campagna phishing Emotet del 10/03/2023
- **Data ricezione email:** 10/03/2023 11:59
- **Mittenti:** noreply@istruzione.it - Gest. doc. - Email: noreply@istruzione.it
- **Indirizzi nel campo email 'A':** <noreply@istruzione.it>
- **Indirizzi nel campo email 'CC':**
- **Indirizzo nel campo 'Rispondi A':** <noreply@istruzione.it>

## Testo email

---

Gentile Collega,

il CSIRT MIM ha evidenza di campagne malspam in corso che attenzionano questo Ministero e raccomanda di prestare maggiore attenzione alle e-mail ricevute.

Tali mail hanno allegato un file \*zip con all'interno un file \*doc o \*xlsx, sembrano provenire da un determinato account (mentre invece il mittente reale è un altro) e riportano nel corpo della mail riferimenti a possibili conversazioni reali avvenute e carpite in precedenza tramite altre attività malevole.

Anche gli oggetti sono tali da indurre nell'utente un senso di sicurezza e spingerlo ad aprire il file allegato e a dare seguito a quanto richiesto nella mail.

Esempi di Oggetto della mail sono:

-Fw: Re: RE: Tr: Fwd: RE:[testo di mail recuperato da precedente Leak]

Si tratta di una campagna di phishing a tema EMOTET molto aggressiva.

Le chiediamo di non ritenere attendibili tali mail e quindi eliminarle.

Nel caso in cui lei abbia proceduto per errore ad aprire l'allegato, le chiediamo di eseguire quanto prima le seguenti azioni nell'ordine riportato:

- Scansione antivirus completa ed approfondita;
- Scansione con software (per esempio AdwCleaner o RogueKiller) per l'individuazione di eventuali Adware, Toolbars, Potentially Unwanted Programs (PUP);
- Pulizia della cache del browser (su Chrome: impostazioni -> "Privacy e Sicurezza" -> "Cancella dati di navigazione" -> Cliccare su "Cancella Dati" per confermare l'operazione);
- Controllo delle estensioni del browser per rilevare che non siano presenti estensioni non personalmente installate;
- Reset e cambio password della casella di posta istituzionale successivamente ai passi sopra menzionati.

Le ricordiamo di prendere visione e di seguire sempre le regole relative le Politiche di Sicurezza adottate dal Ministero raggiungibili nell'apposita sezione dell'area riservata del portale istituzionale <https://miur.gov.it>

Cordiali saluti,

CSIRT MIM