- **Oggetto:** CSIRT-MI - Campagna phishing Emotet del 07/03/2022
- **Data ricezione email:** 07/03/2022 12:54
- **Mittenti:** Alert Fatturazione Elettronica - 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 Utente,

a seguito di analisi di questo CSIRT, si è rilevato che nella giornata di oggi Lei potrebbe aver ricevuto nella sua casella postale mail con oggetto che può variare come nelle seguenti formulazioni 'Re:[nome mail destinatario]', 'fw:[nome mail destinatario]', 'RE:[nome mail destinatario]', 'FW:[nome mail destinatario]', 'POSTA CERTIFICATA: I: ANOMALIA MESSAGGIO: RV:', 'Re: Lista delle Direzioni Regionali', 'Fw:', 'FW:', 'Tr:', 'RE:', 'Re:', '@istruzione.it', 'Fwd:' con allegati file di diversa nomenclatura e con estensione xlsm o zip.

Si tratta di una campagna di phishing molto aggressiva.
Le chiediamo di non ritenere attendibili tali mail e quindi eliminarle.

L'uso della funzionalità di inoltro automatico non è consigliato in quanto rappresenta un rischio sia per la sicurezza dei suoi dati sia di quelli di soggetti terzi, con ripercussioni possibili anche sull'intero patrimonio informativo del Ministero dell'Istruzione nel caso in cui queste fossero divulgate o utilizzate da soggetti malintenzionati.

Nel caso in cui lei abbia proceduto per errore ad aprire l'allegato, le chiediamo di eseguire 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 -> nella barra superiore di ricerca inserire "Cancella dati di navigazione" -> Cancella dati di navigazione -> Selezionare "Cronologia di navigazione", "Cookie e altri dati dei siti", "Immagini e file memorizzati nella cache" -> Cliccare su "Cancella dati");
• 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

Si ringrazia della collaborazione.

CSIRT MI