

Da: noreply@istruzione.it
Oggetto: Raccomandazioni per la Sicurezza della Posta Elettronica
Data: 31/12/2020 15:48:36

IIS "GUIDO MONACO DI POMPOSA" Prot. 0009056 del 31/12/2020 (Entrata)
--

Salve,

con la presente si rappresenta che, a seguito di rilevazione della possibile compromissione delle sue utenze istituzionali a fronte della campagna EMOTET in corso, è necessario effettuare le seguenti azioni

- eseguire approfondite scansioni antivirus di tutte le postazioni utilizzate dalla casella di posta;
- Scansione con software (per esempio AdwCleaner) 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 elettronica effettuata **successivamente** alla scansione antivirus nel caso in cui questa non abbia riscontrato minacce sul sistema

Qualora le indagini a cura dello CSIRT MI dovessero rivelare che le Sue credenziali fossero state illecitamente utilizzate prima del nostro intervento, ovvero comportando la violazione di dati personali Suoi o di Terzi, sarà prontamente informata.

Le ricordiamo inoltre di seguire sempre le raccomandazioni e le buone pratiche per la sicurezza suggerite dall'Amministrazione ed indirizzate da AgID (vedi allegato), di cui estratti ai file allegati alla presente comunicazione.

<https://www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2020/03/17/smart-working-vademecum-lavorare-online-sicurezza>

Grazie,

Auguri di Buone Feste

CSIRT MI