In atto una nuova pericolosa campagna di phishing

La Ragioneria Generale dello Stato informa che è in atto una nuova pericolosa campagna di phishing relativa ad un finto aggiornamento del "certificato webmail MEF".

Secondo tale mail truffa, che contiene al suo interno il logo RGS, il destinatario viene invitato a fornire le informazioni di accesso alla mail istituzionale per poter continuare a ricevere mail importanti di lavoro.
Al fine di prevenire furti di identità e, più in generale, per evitare di condividere involontariamente informazioni riservate, si fa presente che non è in corso nessuna raccolta di dati personali e nessun aggiornamento di certificati webmail.
Si raccomanda, pertanto, a tutti gli utenti RGS:
• di controllare sempre con la massima attenzione le mail ricevute, verificando l'attendibilità del mittente (nel caso di specie chiaramente fraudolenta), dell'oggetto e del testo del messaggio;
• di non inviare, in nessun caso, dati personali o credenziali di accesso, compilando form ricevuti via posta

elettronica o seguendo link di accesso a siti esterni.
In caso di dubbio, si invita a segnalare prontamente al Nucleo Informatico e Supporto Tecnologico (NISuT) dell'IGICS la ricezione di contenuti sospetti. (Così , comunicato pubblicato nel sito http://www.rgs.mef.gov.it/ il 30 gennaio 2019)

Contatti (segnalati nel sito della Ragioneria Generale dello Stato)

Nisut (rgs.nisut@mef.gov.it)