PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 16 - numero 3283 di martedì 25 marzo 2014

SISTRI: Messaggi di posta fraudolenti

In rete transitano messaggi di posta elettronica che sembrano provenire dal dominio di posta del SISTRI ma che in realtà si dimostrano essere messaggi inviati da malintenzionati: come si realizza la truffa informatica?

Sulla rete Internet transitano messaggi di posta elettronica che sembrano provenire dal dominio di posta del SISTRI ma che in realtà si dimostrano essere messaggi "civetta" inviati da malintenzionati per attuare delle truffe informatiche.

Tale problematica non è riconducibile al SISTRI e non è in alcun modo possibile impedirne il perpetrarsi.

Questo fenomeno è riconducibile al cd. phishing, una tipologia di truffa informatica che viene implementata senza la violazione dei sistemi appartenenti al dominio utilizzato in cui i messaggi non vengono veicolati attraverso l'infrastruttura di connettività.

Al fine di prevenire e proteggersi da eventuali attacchi di phishing si raccomanda di considerare che le procedure operative del SISTRI non prevedono, in alcun caso, l'invio di mail per mezzo delle quali si invitano gli Utenti a fornire o confermare i dati di accesso o eseguire pagamenti.

Tramite le tecniche di phishing i suddetti messaggi vengono appositamente preparati ed inviati per impossessarsi, in modo fraudolento, di informazioni riservate dell'utente (es. codici di accesso ai Servizi via internet).

La truffa si realizza attraverso i seguenti passi:

· il truffatore (phisher) prepara una mail con un testo "civetta" che simula, nella grafica e nel contenuto, un'istituzione o un'azienda (es: un istituto bancario o portale di carta di credito);
· il phisher invia a migliaia di indirizzi email la falsa comunicazione, spacciandosi per l'istituzione/azienda suddetta e consigliando al destinatario di fornire, per ragioni riconducibili a controlli o risoluzione di problemi, le informazioni di cui intende entrare in possesso;
· a tal fine il destinatario viene invitato a collegarsi ad uno specifico indirizzo internet mediante un link inserito nel testo della mail stessa;
· l'utente, inconsapevole del tentativo di truffa, può cadere nel tranello e cliccare sul link indicato nella mail, anche in considerazione del fatto che tali link sono appositamente generati per nascondere/offuscare il reale indirizzo al quale ci si collega;
· nel momento in cui l'utente clicca sul collegamento viene indirizzato al sito civetta controllato dal phisher (del tutto simile a quello originale) per immettere le informazioni richieste;
· le informazioni riservate vengono registrate dal phisher per essere successivamente riutilizzate per accedere al relativo servizio e perpetuare la truffa.

Fonte: sistri.it

www.puntosicuro.it