Gio 15 Gen, 2026

AVVISO IMPORTANTE: Campagna di mail fraudolente a nome di InfoCamere e Camere di Commercio

Si informano le imprese del territorio che è stata rilevata una campagna di e-mail fraudolente (phishing) che utilizza indebitamente il nome di “InfoCamere” e delle “Camere di Commercio” al fine di sottrarre illecitamente dati e credenziali.

Queste comunicazioni malevoli sono state inviate a diverse imprese e presentano le seguenti caratteristiche:

- **Oggetto:** L’oggetto dell’email è tipicamente “Servizio RIIT – Ricevuta REI-25313967” o formule simili.
- **Contenuto:** Il messaggio richiede di effettuare con urgenza una verifica dell’indirizzo email per “mantenere attivo il profilo InfoCamere”. Viene inoltre menzionata la necessità di ripetere la conferma ogni 90 giorni.
- **Tono minatorio:** Per indurre l’utente a compiere l’azione richiesta, l’email minaccia la “sospensione temporanea” dell’indirizzo email e un ripristino che potrebbe richiedere fino a 5 giorni lavorativi.
- **Link ingannevoli:** L’utente viene invitato a cliccare su un link per completare la verifica. Sebbene il testo del link possa sembrare simile all’indirizzo ufficiale del sistema camerale (es. https://login, infocamere, it/eacologin/login, action), esso in realtà indirizza a siti web malevoli, esterni e non sicuri, creati per rubare le informazioni dell’utente. Si noti come nell’esempio il link utilizzi virgole al posto dei punti.

Si sottolinea che il mittente di tali comunicazioni non è un canale ufficiale, ma un indirizzo fittizio (come ufficiogare@costruzionifacciolongo.it nell’esempio allegato).

La Camera di Commercio I.A.A. di Sassari, in coordinamento con InfoCamere, sta monitorando attentamente la situazione e procederà con la dovuta segnalazione all’autorità giudiziaria.

Tuttavia, cogliamo l’occasione per invitare tutte le imprese a prestare la massima attenzione.

RACCOMANDAZIONI

- **NON CLICCARE** sui link presenti in queste email.
- **NON FORNIRE** in nessun caso le proprie credenziali di accesso o altri dati personali.
- **VERIFICARE** sempre con attenzione l’indirizzo email completo del mittente.
- **ELIMINARE** immediatamente i messaggi sospetti.

ESEMPIO DI MESSAGGIO FRAUDOLENTO

In caso di dubbi sulla legittimità di una comunicazione ricevuta, si prega di contattare direttamente i canali di assistenza ufficiali di InfoCamere.

Stampa in PDF

PDF

Ultima modifica

Gio 15 Gen, 2026