IVASS
ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI

INFORMATIVA SURVEY IPER

Gestione e conservazione credenziali

Tutti gli utenti coinvolti nella survey IPER sono identificati e autenticati. L'utente viene identificato tramite un'utenza e autenticato, tramite password che deve essere mantenuta segreta. Nel caso di autenticazione a due fattori (c.d. strong authentication), sarà richiesto l'utilizzo di dispositivi One Time Password (OTP).

Agli utenti si richiede di:

- Non condividere o rivelare ad alcuno, le utenze e le password.
- Cambiare immediatamente la password se si sospetta che essa sia stata rivelata a una terza parte non autorizzata.
- Non annotare le password e lasciarle in luoghi dove persone non autorizzate possano facilmente scoprirle.
- Cambiare la password con regolarità.

In ogni caso, l'utente rimane responsabile di tutte le attività effettuate con la propria utenza e la propria password.

Comunicazioni e notifiche via mail

I messaggi di posta elettronica, inviati non hanno caratteristiche di sicurezza, poiché su Internet soggetti con le opportune abilità possono leggerli, memorizzarli, duplicarli, alterarli nel mittente e nel destinatario e persino modificarli nei contenuti. La posta elettronica è infatti utilizzata anche per veicolare codice malevolo o catturare informazioni, come ad esempio gli indirizzi di posta degli utenti o i codici di accesso, tramite tecniche di raggiro che sfruttano l'ingenuità delle persone (c.d. "Phishing").

Al riguardo, per la survey IPER, si fa presente che:

- Non saranno mai richiesti via e-mail dati riservati.
- Non cliccare mai *link* o *URL* presenti su e-mail inerenti la survey.
- Non sarà mai richiesta la conferma di dati riservati.
- Non saranno mai presenti *link* o *URL* che rinviano a siti web, all'interno delle mail inviate dalla survey IPER, per la notifica di specifiche attività.