

Negli ultimi mesi, sul panorama nazionale, si sono verificati diversi casi di frode collegati alla clonazione dei documenti di identità, documenti che sono stati utilizzati per l'attivazione di SPID fraudolenti e l'apertura conti correnti. Le conseguenze sono state anche severe, con furto di identità, accesso non autorizzato ai servizi online dei Fondi pensione, modifica dei contatti di riferimento (numeri di telefono e indirizzi e-mail), effettuazione di richieste di prestazioni attraverso la produzione di documentazione, anche sanitaria, falsificata.

Al fine di proteggersi il più possibile dalla creazione di SPID non autorizzati e dal furto d'identità, si raccomanda di:

- Non condividere mai immagini dei propri documenti sui social media e di non inviarli attraverso messaggi privati.
- Controllare sempre l'indirizzo ricevuto prima di accedere ai siti attraverso link diretti.
- Utilizzare solo e sempre i canali ufficiali per attivare o gestire l'utenza SPID, ad esempio in caso di richiesta di cambio della password dello SPID o di rinnovo dello stesso.
- Utilizzare password complesse, che non contengano riferimenti facili da individuare, come, ad esempio, date di nascita proprie o di familiari.
- Cambiare le password con costanza.
- Attivare l'autenticazione a più fattori, quando possibile.
- Controllare sempre le notifiche dei provider SPID, che normalmente avvisano di un accesso o di una modifica.

Al fine di proteggersi il più possibile dall'accesso non autorizzato alla propria area personale del Fondo, si raccomanda di:

- Accedere con una certa frequenza alla posizione personale sul Fondo per monitorare lo stato del proprio patrimonio e delle richieste effettuate.
- Verificare, nella sezione apposita dell'Area Riservata, l'eventuale presenza di operazioni non autorizzate.
- Tenere sempre aggiornati i propri contatti di riferimento (numeri di telefono e indirizzi e-mail), provvedendo a modificarli qualora gli stessi subiscano cambiamenti o siano diventati obsoleti (anche, ad esempio, in caso di cessazione del rapporto di lavoro, inserendo i contatti personali e non più aziendali, se necessario).
- Controllare le notifiche e gli avvisi che possono arrivare da parte del Fondo e verificare sempre l'autenticità delle comunicazioni pervenute dallo stesso.

- Accedere alla pagina web del Fondo digitando l'indirizzo completo (<https://www.fipdaf.it>) e non effettuare l'accesso cliccando su un link ricevuto via mail, sms o altri mezzi di comunicazione.

Nel caso si sospetti un accesso non autorizzato all'Area Riservata del Fondo:

- Contattare immediatamente il Fondo utilizzando i canali ufficiali dello stesso, ad esempio via e-mail, all'indirizzo fipdaf@stellantis.com, o telefonando allo 011 0058106 / 011 0056980.

Nel caso si sospetti un accesso non autorizzato o un furto d'identità:

- Modificare le credenziali dello SPID presso il gestore dell'identità digitale e, nel caso se ne venga a conoscenza, bloccare le identità digitali attivate presso altri provider.
- Presentare immediata denuncia alle Autorità competenti, come la Polizia Postale nei casi di furto di identità digitale.