FONDO PENSIONE
CRÉDIT AGRICOLE ITALIA

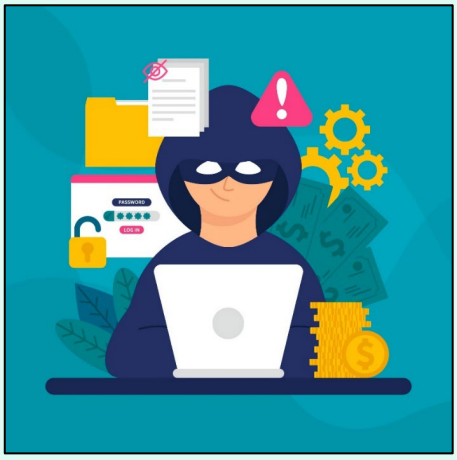
FURTO DI IDENTITA' DIGITALE

Conoscere per proteggersi

Ogni giorno utilizziamo strumenti digitali per accedere a servizi, consultare informazioni e gestire anche dati personali e previdenziali.

Per questo è importante prestare attenzione alla sicurezza delle proprie credenziali e delle informazioni condivise online.

Un utilizzo consapevole degli strumenti digitali aiuta a proteggere la propria identità e a prevenire tentativi di frode o accessi non autorizzati.



COS'E' IL FURTO DI IDENTITA' DIGITALE?

È quando qualcuno entra in possesso dei tuoi dati personali e li utilizza senza il tuo permesso per **compiere azioni a tuo nome** (*come ad esempio aprire conti, fare acquisti, richiedere servizi, accedere ai tuoi risparmi o alla tua posizione previdenziale*).

La Cassazione (*sent. n. 13559/2024, confermata da Cass. n. 34362/2024*) ha chiarito che la nozione di «**Identità Digitale**» che integra l'aggravante di cui all'art. 640-ter, comma terzo, c.p., non presuppone una procedura di validazione adottata dalla Pubblica amministrazione, ma **trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati,** quindi non solo SPID/CIE/firma digitale, ma anche le credenziali **dell'area riservata di un fondo pensione,** di una banca o di un portale privato.

Un fenomeno in crescita

Almeno **559,4 milioni di euro** sono stati **sottratti tramite frodi digitali** in Italia nel triennio **2022-2024.**

PERCHE' E' IMPORTANTE ESSERNE A CONOSCENZA?

Ci possono essere conseguenze ***economiche***, ***burocratiche, legali, reputazionali.***

I tuoi **dati personali** hanno valore per i criminali informatici.

Intervenire subito è più facile se sai come riconoscere il **rischio.**

Con semplici attenzioni puoi **ridurre il rischio** in modo efficace.

FONDO PENSIONE
CRÉDIT AGRICOLE ITALIA

2

LE REGOLE D'ORO

*per proteggere la tua **Identità Digitale***

1

Usa password forti e diverse

Scegli password lunghe, con lettere, numeri e simboli.
Usa una password diversa per ogni servizio online.

2

Attiva sempre la verifica in due passaggi

Aggiunge un livello di sicurezza in più ai tuoi accessi online ed un ostacolo ulteriore per i malintenzionati.

3

Fai attenzione alle e-mail e ai messaggi sospetti

Non cliccare su link o allegati sospetti inviati da mittenti che non conosci.

4

Usa reti sicure

Evita di accedere ai tuoi servizi personali da reti WI-FI pubbliche e/o non protette.

5

Mantieni aggiornati i tuoi dispositivi

Aggiornamenti e antivirus aiutano a proteggerti dalle minacce più recenti.

6

Controlla regolarmente i tuoi account

Verifica spesso movimenti e attività sui tuoi conti e/o servizi online.

COSE DA EVITARE

- **Condividere password** o **codici di accesso** con altri
- **Cliccare su link sospetti** ricevuti via e-mail o SMS
- **Accedere** da dispositivi di **terzi** o **condivisi**
- Rispondere a **richieste di dati personali** via e-mail, SMS o telefono
- **Salvare password in modo non sicuro** o lasciarle scritte in luoghi visibili
- Credere a promesse di **beni** o **servizi fuori mercato**

COME PUO' AVVENIRE

I principali modi con cui i malintenzionati possono rubare i tuoi dati

Phishing

Tentativo di truffa tramite **e-mail o messaggi** che **sembrano provenire** da enti affidabili e invitano l'aderente a cliccare su link per inserire i suoi dati.

Smishing (SMS fraudolenti)

Tentativo di truffa tramite **SMS** che spingono l'aderente ad agire in fretta, minacciando blocchi o problemi per **indurre a fornire credenziali** di accesso o dati personali.

Vishing (telefonate ingannevoli)

Tentativo di truffa tramite **telefono** che, suscitando un clima di fiducia correlato ad un'urgenza di agire, cerca di **ottenere dati riservati e personali** degli aderenti.

Malware

Software dannosi che si installano sul dispositivo personale e **rubano informazioni** senza che il titolare se ne accorga.

Social Engineering

Tecniche di **manipolazione psicologica** utilizzate per ingannare gli aderenti ed indurli a rivelare informazioni riservate.

Dati esposti o condivisi

Dati personali pubblicati online, persi o condivisi in modo incauto possono essere **raccolti ed usati** dai malintenzionati per prendere possesso di **credenziali riservate**.

COSA FARE SE SOSPETTI UN FURTO DI IDENTITA'

Agisci subito cambiando le password dei servizi coinvolti

Contatta il Fondo Pensione per ottenere supporto
fondopensione@credit-agricole.it

Monitora i tuoi account e conserva le prove utili di quanto accaduto