

Guida alla sicurezza per l'utilizzo dell'Identità Digitale SpidItalia by Register

Di seguito alcuni consigli per evitare che altri possano illecitamente utilizzare la tua **Identità Digitale SpidItalia** ed avere accesso ai tuoi dati o operare per tuo conto.

Register ha un sistema di monitoraggio evoluto, ma le buone pratiche personali permettono di ridurre i rischi di violazione ed abusi. La sicurezza della tua Identità Digitale dipende anche da te, potrai migliorarla mediante piccoli accorgimenti, aiutandoci così ad evitare abusi ed usi illeciti.

Ecco una serie di consigli e buone pratiche.

Protezione della Password

1. Crea password non facili da indovinare: evita di utilizzare informazioni personali, di inserire parole semplici o frasi come "password" o serie di tasti come "qwerty" o "qazwsx" o sequenze come "abcd1234". Register renderà evidente la robustezza della password mentre la inserirai.
2. Non lasciare appunti scritti con le tue password su computer o scrivania; se salvi la password su file, nominalo con un nome che non sia facilmente riconducibile al contenuto.
3. Cambia regolarmente la tua password anche ogni volta che sospetti che qualcuno possa esserne venuto a conoscenza.

Protezione dello Smartphone

1. Proteggi il tuo Smartphone attivando le funzioni di blocco tramite password, PIN (numerico) o disegni o impronta digitale.
2. Disattiva l'opzione di connessione Wi-Fi automatica e fai attenzione alle Wi-Fi pubbliche ed aperte.
3. Utilizza market ufficiali per il download delle app. L'installazione di programmi risulta spesso il principale mezzo per veicolare software potenzialmente pericolosi (malware, virus).
4. Mantieni aggiornato il tuo dispositivo
5. Mantieni aggiornati sistema operativo ed app.
6. Resetta il tuo smartphone/computer se e quando lo dai via, cancellando tutto il contenuto trasferendo su altro supporto se si intende conservarlo.

Protezione il tuo PC e la tua postazione

1. Utilizza software antivirus e personal firewall, disponibili online anche gratuitamente. Questi strumenti consentono di impedire l'installazione anche involontaria di software pericoloso.
2. Aggiorna regolarmente il tuo sistema operativo, attiva la funzionalità di aggiornamento automatico affinché la tua postazione sia sempre protetta. Riduci così la possibilità di intrusione.
3. Se utilizzi la tua Identità Digitale tramite un computer diverso dal tuo o pubblico, ricordati di non salvare password e di effettuare il logout ed utilizzare le funzionalità del browser per cancellare dati, password, cache e cookie.
4. Quando utilizzi la tua Identità Digitale verifica sempre che la pagina di login sia quella di Register e sia presente l'icona 'lucchetto chiuso' sulla barra degli indirizzi ed il prefisso https.
 - a. Non immettere mai i tuoi codici su altri siti, specialmente se raggiungibili tramite link inviati via e-mail.
5. Se sospetti una violazione, richiedi subito la sospensione della tua Identità Digitale.