Guida alla sicurezza per l'utilizzo dell'Identità Digitale PosteID

PosteID è la soluzione che offre Poste Italiane per dotare tutti i cittadini che ne fanno richiesta di una Identità Digitale e consentire tramite essa di accedere ai dati ed ai servizi online erogati dalle Pubbliche Amministrazioni e dai Fornitori di Servizi privati che aderiscono al Sistema Pubblico per la gestione dell'Identità Digitale (SPID).

Per Poste Italiane la sicurezza ha un'importanza rilevante e giornalmente è impegnata a valutare ed impiegare le misure migliori per proteggere le Identità Digitali dei propri utenti da violazioni e usi non autorizzati.

Naturalmente la sicurezza della tua Identità Digitale dipende anche da te. Con piccoli accorgimenti, puoi aiutarci ad evitare che malintenzionati possano entrare illecitamente in possesso della tua Identità ed avere accesso ai tuoi dati o operare online per tuo conto a tua insaputa.

Ecco una serie di consigli e buone pratiche da adottare per ridurre i rischi di violazione ed abusi relativi alla tua Identità Digitale.

Proteggi la tua password

1. Non riutilizzare le password

Utilizza una password diversa per ogni tuo account importante, ad esempio una per l'account e-mail ed una per la tua Identità PosteID. Riutilizzare le stesse password è rischioso. Se qualcuno indovina la password della tua posta elettronica, potrebbe tentare di riutilizzarla per avere accesso alla tua Identità Digitale.

2. Crea password non facili da indovinare

Quando crei la tua password, evita di utilizzare informazioni personali che possano renderla facile da indovinare. PosteID ti chiederà di comporre la tua password con alcuni accorgimenti, come previsto dalle regole di SPID, per impedire di generare password semplici. Non utilizzare comunque all'interno della tua password parole semplici o frasi come "password" o serie di tasti come "qwerty" o "qazwsx" o sequenze come "abcd1234". Ad esempio, per creare una password robusta, puoi utilizzare una frase e inserire lettere, segni e numeri all'inizio, al centro e alla fine (ad esempio "C3rcoUn@!Casa"). Troverai sulla Guida Utente il dettaglio delle regole minime per la composizione di una password.

3. Custodisci la tua password

Non lasciare post-it con le tue password sul computer o sulla scrivania, che possono essere facilmente sottratti da persone che ci sono vicine. Quando salvi le tue password in un file sul computer, assegna al file un nome che non consenta ad altri di riconoscerne facilmente il contenuto, ad esempio "password.txt". Per i più "esperti", sono disponibili gratuitamente online strumenti affidabili di gestione delle password.

Ricorda che la password ti sarà chiesta solo sul sito PosteID. Non inserirla su siti diversi da quello di Poste Italiane.

4. Cambia regolarmente la tua password

Ricordati di cambiare regolarmente la tua password ogni volta che sospetti che qualcuno possa esserne venuto a conoscenza.

PosteID ti obbligherà a farlo almeno ogni 6 mesi.

Proteggi il tuo Smartphone

1. Blocca lo schermo del tuo smartphone

E' consigliabile attivare le funzioni di blocco tramite password, PIN (numerico) o disegni dello smartphone. Anche se può sembrare noioso, questo accorgimento è una buona misura di protezione in caso di smarrimento del telefono per impedire ad un malintenzionato di accedere ai propri dati e contenuti.

2. Disattiva l'opzione di connessione Wi-Fi automatica.

Fai attenzione nell'utilizzo di Wi-Fi pubbliche ed aperte per evitare che eventuali malintenzionati possono intercettare le informazioni scambiate. Preferisci piuttosto le Wi-Fi che richiedono una registrazione per poter navigare.

3. Utilizza solo le applicazioni provenienti dai market ufficiali

Utilizza solo i market ufficiali per il download delle app. L'installazione di programmi di provenienza non fidata deve essere assolutamente evitata, in quanto principale mezzo per veicolare software potenzialmente pericolosi (malware, virus).

4. Disabilita l'anteprima degli Sms

Questo accorgimento impedisce a chi ci è attorno di sbirciare sul nostro schermo e, ad esempio, carpire un codice di accesso.

5. Mantieni aggiornato il tuo dispositivo

Mantieni sempre aggiornati il sistema operativo e le app. Gli aggiornamenti sono vitali per tener lontani i malintenzionati dai nostri dispositivi.

6. Usa solo le TUE impronte oppure il TUO volto

Sui dispositivi più moderni dotati di specifico sensore, potrai scegliere di non digitare ogni volta il tuo codice PosteID ma di associarlo alle tue impronte digitali o al riconoscimento del tuo volto (impronta facciale), attivando la funzionalità sul tuo smartphone o tablet e sull'App. In questo modo, usare la tua Identità Digitale sarà ancora più facile ma assicurati di registrare soltanto le tue impronte digitali e la tua impronta facciale: una volta abilitata la funzione tutte le impronte registrate potranno avere accesso al tuo codice PosteID. Se hai un gemello o un fratello/sorella somigliante ed utilizzare l'impronta facciale ti preoccupa, ti consigliamo di effettuare l'autenticazione tramite codice.

7. Resetta il tuo smartphone quando lo dai via

Una pratica importante da applicare quando si vende uno smartphone o un tablet è cancellarne tutto il contenuto, completamente, avendo cura di averlo trasferito su un altro dispositivo, se si intende conservarlo.

Questa misura evita che chi entrerà in possesso dello smartphone possa avere accesso a dati e codici privati.

Proteggi la postazione

1. Utilizza software antivirus e personal firewall

È molto importante proteggere la propria postazione con l'utilizzo di un software antivirus e personal firewall, disponibili online anche gratuitamente, accertandosi che questi siano sempre attivi e sia attiva la tipica funzionalità di aggiornamento automatico. Questi strumenti consentono di impedire l'installazione anche involontaria di software pericoloso e proteggono la tua navigazione in rete.

2. Usa software sempre aggiornato

Procedi regolarmente all'aggiornamento del tuo sistema operativo, accertandoti che sia attiva la funzionalità di aggiornamento automatico affinché la tua postazione sia sempre protetta. Una postazione sempre aggiornata riduce la possibilità di intrusione da parte di malintenzionati.

3. Cancella le tue tracce su computer pubblici

Se utilizzi la tua Identità Digitale tramite un computer pubblico, ricordati di effettuare sempre il logout prima di abbandonare il computer e di utilizzare le funzionalità del browser per cancellare i dati relativi a moduli, password, cache e cookie.

4. Verifica i siti quando utilizzi la tua Identità

Quando utilizzi la tua Identità Digitale tramite un browser, verifica sempre che la pagina di login sia quella di Poste Italiane e sulla barra degli indirizzi sia presente il prefisso https e l'icona "lucchetto chiuso".

Non immettere i tuoi codici su altri siti, specialmente se corrispondenti a link inviati via e-mail.

Controlla la tua identità

1. Verifica la tua posta elettronica

Se selezionerai l'apposita opzione, Poste Italiane ti invierà delle notifiche via e-mail ogni volta che utilizzerai la tua Identità, così che tu possa essere tempestivamente informato su usi impropri. Affinché questa misura sia efficace, quando usi uno smartphone, evita di configurare la tua e-mail di contatto su quest'ultimo: questo impedirà a chi entra in possesso del tuo smartphone di cancellare le nostre e-mail di notifica.

2. Se sospetti una violazione, richiedi la sospensione immediata della tua Identità

Qualora avessi il sospetto che la tua Identità PosteID possa essere stata violata, procedi rapidamente alla richiesta di sospensione online sul sito https://posteid.poste.it o tramite IVR o contatta il nostro Call Center per ricevere assistenza. Trovi i numeri di contatto sul Manuale Operativo e sul sito di Poste Italiane.

Ricorda…

- La tua Identità PosteID è strettamente personale e non deve essere ceduta né ne è consentito l'uso a nessuno al di fuori di te.
- Poste Italiane procederà alla sospensione immediata della tua Identità qualora i sistemi di monitoraggio rilevino usi anomali.
- Per assistenza, puoi contattare il nostro Call Center. Trovi i numeri di contatto sul Manuale Operativo e sul sito di Poste Italiane.