Guida alla sicurezza dell'identità digitale

SielteID è il servizio offerto da Sielte S.p.A. per abilitare 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 noi 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 chi la possiede. Con alcuni 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.

Memorizza e conserva i tuoi dati di contatto

Il numero di cellulare e l'indirizzo mail devono essere personali essendo associati alla tua identità digitale e lo smarrimento di uno di questi potrebbe comportare l'inutilizzo della tua identità.

Nel caso in cui devi cambiare indirizzo mail o numero di cellulare ricordati di aggiornarli sul tuo profilo personale SielteID prima di procedere con la disattivazione definitiva dei vecchi dati di contatto.

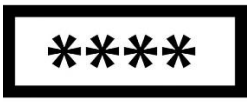
Conserva il tuo codice SPID

Il codice SPID è un dato che ti identifica in maniera univoca. Lo trovi all'interno della tua area personale nella sezione "il tuo profilo" nella scheda "dati SPID" c'è la voce "codice SPID". Conservalo accuratamente potrebbe essere utile in caso di recupera della tua identità digitale.

Conserva i codici di sblocco revoca e sospensione

I codici di sblocco revoca e sospensione vengono inviati nella mail di attivazione. Conservali accuratamente perché ti serviranno nel caso in cui vorrai revocare o sospendere la tua identità digitale.

Proteggi la tua password



Utilizza password non facili da indovinare

Quando imposti la tua password, non utilizzare informazioni personali che possano renderla facile da indovinare. SielteID 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 "xyz123". 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 "LaM1aPassw0rd!"). Troverai sulla Guida Utente il dettaglio delle regole minime per la composizione di una password.

Non riutilizzare la tua password

Ricordati sempre di utilizzare una password diversa per ogni tuo account, ad esempio una per l'account e-mail ed una per la tua Identità SielteID. Riutilizzare le stesse password è molto rischioso. Nel caso in cui qualcuno riuscisse a indovinare la password della tua casella di posta elettronica, potrebbe tentare di riutilizzarla per avere accesso alla tua Identità Digitale.

Ricordati di cambiare regolarmente la tua password

Ricordati di cambiare regolarmente la tua password ogni volta che sospetti che qualcuno possa esserne venuto a conoscenza. SielteID ti obbligherà a farlo almeno ogni 6 mesi.

Custodisci in modo sicuro 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". Ricorda che la password ti sarà chiesta solo sul sito SielteID. Non inserirla su siti diversi da quello di Sielte S.p.A.

Verifica periodicamente la tua identità

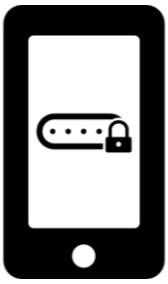
Verifica la tua e-mail

Se selezionerai l'apposita opzione, Sielte 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.

Se sospetti una violazione….

Nel caso in cui avessi il sospetto che la tua Identità Sielte ID possa essere stata violata, procedi rapidamente alla richiesta di sospensione online sul sito http://www.sielteid.it o contatta il nostro Service Desk per ricevere assistenza. Trovi i numeri di contatto sul Manuale Operativo e sul sito di Sielte nella sezione Contatti.

Progetti il tuo dispositivo cellulare



Blocca lo schermo del tuo telefono

È 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.

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.

Disattiva l'anteprima degli SMS

Questo tipo di configurazione impedisce a chi ci è attorno a noi di osservare il nostro schermo e visualizzare il codice di accesso a SPID.

Mantieni aggiornato il tuo dispositivo

Mantieni sempre aggiornati il sistema operativo dei tuoi dispositivi e i relativi aggiornamenti delle applicazioni. Gli aggiornamenti sono importanti per tener lontani i malintenzionati dai nostri dispositivi.

Proteggi il tuo PC

Utilizza software antivirus e 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.

Usa software sempre aggiornato

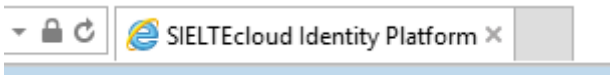
Procedi regolarmente all'aggiornamento del tuo sistema operativo, accertandoti che sia attiva la funzionalità di aggiornamento automatico affinché la tua postazione sia sempre protetta. Una postazione sempre aggiornata riduce la possibilità di intrusione da parte di malintenzionati.

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.

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 Sielte 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.