Guida alla sicurezza dell'identità digitale

SielteID è il servizio offerto da Sielte S.p.A. per abilitare tutti i cittadini che fanno richiesta di un'Identità Digitale e consentire tramite quest'ultima l'accesso 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 Sielte la sicurezza ha un'importanza rilevante e giornalmente si impegna 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 propria 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 e 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 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.

Se 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.

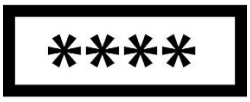
Conserva il tuo indirizzo mail e il tuo numero cellulare

Custodisci, in modo da ricordarli sempre, i tuoi recapiti mail e cellulare forniti in fase di registrazione. All'interno dell'area personale del tuo profilo è inoltre possibile rintracciare il tuo codice SPID che ti identifica in maniera univoca. Nella sezione *il tuo profilo*, nella scheda *dati SPID*, è presente la voce *codice SPID*.

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 se 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, perché possono essere facilmente sottratti da persone che ti sono vicine. Non conservare la password in luoghi facilmente accessibili da parte di terzi ed in ogni caso mai nelle vicinanze del computer. Quando salvi le tue password in un file sul computer, non assegnare al file un nome che consenta ad altri di riconoscerne facilmente il contenuto, come 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.

Non comunicare a nessuno la tua password. Ricordati che lo scopo principale per cui si utilizza una password è quello di assicurare che nessun altro possa utilizzare le tue risorse. Quando immetti la password assicurati che nessuno la stia osservando.

Altre informazioni e buone pratiche utili da conoscere

Non utilizzare come password parole di uso comune o riconducibili a te. Questo perché tramite un attacco denominato *a dizionario*, un malintenzionato potrebbe facilmente scovare la tua password. Questo metodo, infatti, fa leva sulla poca esperienza e competenza in ambito informatico dell'utente, il quale, per comodità, tipicamente inserisce parole semplici di linguaggio comune che è in grado di ricordare a memoria, piuttosto che più o meno complesse combinazioni, a volte anche non di senso compiuto, di lettere e numeri. A questo punto il malintenzionato dovrà soltanto attingere ad un normale dizionario e provare, tramite più tentativi e utilizzando un sistema automatico, a scovare la tua password. Nonostante esistano efficaci contromisure informatiche per prevenire questi attacchi, ad esempio il blocco temporaneo delle credenziali dopo diversi tentativi, è sempre meglio seguire la regola sopradescritta. Non credere che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.

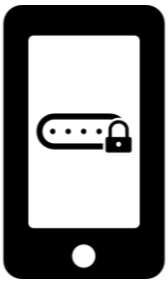
Un altro attacco estremamente diffuso nell'ambito del furto delle credenziali è quello denominato "di forza bruta", che al contrario dell'attacco *a dizionario* utilizza risorse computazionali e tempistiche molto maggiori per provare a scovare la password provando tutte le combinazioni alfanumeriche possibili. Ne consegue che il miglior modo per proteggersi da questo attacco, e ovviamente anche da quello *a dizionario*, è quello di utilizzare password di elevata complessità (almeno 10 caratteri, maiuscole, minuscole e caratteri speciali), possibilmente utilizzando dei termini non presenti sul dizionario. In questo caso, infatti, le risorse computazionali e i tempi che ci vorrebbero per provare un numero così elevato di combinazioni sarebbero proibitivi e controproducenti per l'attaccante.

Verifica periodicamente la tua identità

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 Contact Center per ricevere assistenza. Trovi i numeri di contatto all'interno dei documenti SielteID e sul sito di Sielte nella sezione Contatti.

Proteggi 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 ad utilizzare Wi-Fi pubbliche ed aperte per evitare che eventuali malintenzionati possano 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 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 le applicazioni. Gli aggiornamenti sono importanti per tener lontani i malintenzionati dai nostri dispositivi.

Proteggi la tua smartcard

Conserva accuratamente la tua smart card

Custodisci la tua smart card in luoghi sicuri, evita di conservarla nello stesso luogo dove tieni anche il relativo codice PIN.

Custodisci in modo sicuro il tuo PIN

Non lasciare post-it con scritto il tuo PIN sul computer, sulla scrivania o vicino alla smart card.

Evita di re-impostare il PIN della smart card ad un nuovo valore basato su schemi prevedibili come numeri di telefono e date.

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, accertandoti che questi siano sempre attivi e sia attiva anche la tipica funzionalità di aggiornamento automatico. Questi strumenti consentono di impedire l'installazione anche involontaria di software pericolosi 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.

Usa soltanto programmi provenienti da fonti fidate

Se devi scaricare un programma, utilizza sempre il sito del produttore. Se scarichi un software da una fonte non attendibile, potresti incorrere in virus o keylogger.

Diffida da messaggi o e-mail di dubbia provenienza

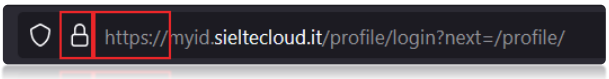
Se hai qualche dubbio in merito all'attendibilità di un messaggio o di una e-mail, non aprire eventuali allegati o link all'interno di essa, potrebbe facilmente contenere dei virus di vario tipo.

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 che 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.