GUIDA ALLA SICUREZZA

Servizio di Gestione Sistema Pubblico dell'Identità Digitale (SPID)

Stato delle Revisioni del Documento

REV.	CAP.	DESCRIZIONE MOTIVO	DATA
00	TUTTI	EMISSIONE BOZZA IN CONFORMITÀ AL COMMA 3 REGOLAMENTO PER L'ACCREDITAMENTO E VIGILANZA GESTORI DELL'IDENTITA' DIGITALE SPID	15/03/2021
01	TUTTI	REVISIONE AZIONI CORRETTIVE	15/11/2021
02	TUTTI	FORMATTAZIONE E AGGIORNAMENTO LINK	30/06/2022

Sommario

Guida alla sicurezza dell'identità digitale

EtnaID è il servizio offerto da Etna Hitech S.c.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 Etna Hitech 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 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 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.

Se devi cambiare il numero di cellulare e/o l'e-mail ricordati di aggiornarli sul tuo profilo personale EtnaID, prima di procedere con la dismissione 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", è presente la voce "codice SPID". Conservalo accuratamente, potrebbe essere utile nel caso in cui dovessi recuperare la tua Identità Digitale. Non comunicarlo a terzi e non divulgarlo in alcun modo durante il periodo di validità della tua Identità Digitale.

Conserva i codici di revoca, di sospensione e di sblocco

I codici dispositivi di sblocco, revoca e sospensione vengono inviati nella e-mail di attivazione. Conservali accuratamente, perché ti serviranno se vorrai revocare o sospendere la tua Identità Digitale.

Proteggi la tua password

1. Utilizza password non facili da indovinare

Quando imposti la tua password, evita di utilizzare riferimenti personali facili da indovinare. EtnaID 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.

2. Non riutilizzare la tua password

Utilizza password diverse per ogni tuo account, ad esempio una per l'account e-mail ed una per la tua Identità EtnaID. 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 violare anche tua Identità Digitale.

Inoltre, assicurati di non utilizzare password già utilizzate in passato.

3. 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. EtnaID ti obbligherà a farlo almeno ogni 6 mesi, al primo utilizzo della password successivo alla scadenza.

4. Custodisci in modo sicuro la tua password

Non scrivere mai le tue password su biglietti che poi magari conservi nel portafoglio o indosso, o che puoi distrattamente lasciare in giro, oppure in file non protetti sui tuoi dispositivi personali (computer, smartphone o tablet).

Evita di immettere la password in luoghi pubblici e di condividerla anche con conosciuti, in quanto le credenziali potrebbero essere diffuse involontariamente a terzi o rubate da malintenzionati. Ricorda che la password ti sarà chiesta solo sul sito EtnaID. Non inserirla su siti diversi da quello di Etna Hitech S.c.p.A.

Verifica e aggiorna la tua identità digitale spesso

1. Verifica la tua e-mail

Se selezionerai l'apposita opzione, Etna Hitech 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...

Nel caso in cui avessi il sospetto che la tua Identità EtnaID possa essere stata violata, richiedine rapidamente la sospensione online sul sito https://etnaid.eht.eu o contatta il nostro Contact Center per ricevere assistenza. Trovi i numeri di contatto all'interno dei documenti EtnaID e sul sito ww.etnaid.it nella sezione Contatti.

Proteggi il tuo dispositivo cellulare

1. Blocca lo schermo del tuo smartphone

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.

2. 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.

3. 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.

4. 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

1. Conserva accuratamente la tua smart card

Conserva la tua smart card in luoghi sicuri, evita di conservarla nello stesso luogo dove si conserva il relativo codice PIN.

2. 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

1. 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.

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 Etna Hitech 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.