Allegato c)

Indicazioni riassuntive per mantenere il livello di sicurezza nell'uso di sistemi informatici

Password

Evitare di lasciare biglietti con le password di accesso alle procedure informatiche o postazioni di lavoro ben visibili sulla scrivania o in prossimità della stessa.

Ove possibile effettuare l'accesso ai programmi tramite SPID, in altri casi si consiglia di scegliere sempre la password con una sequenza minima di 8 caratteri alfanumerici utilizzando caratteri maiuscoli, minuscoli, numeri, utilizzando caratteri speciali, come @ # $ % ^ & alternando maiuscole a minuscole.

Nel creare una password sicura è altresì buona norma non usare parole comuni per la password come ad esempio: la data di compleanno, il proprio nome utente (User-ID), così che non sia riconducibile all'incaricato.

Al fine di aumentare il grado di sicurezza è consigliabile creare password diverse per tipologie diverse di utilizzo.

Tool per verificare la sicurezza della password: https://www.security.org/how-secure-is-my-password/

Uso del PC

Il computer deve essere protetto da password; in caso di breve e temporaneo inutilizzo, la postazione deve essere bloccata tramite la combinazione dei tasti WINDOWS + L o in alternativa deve essere fatta la disconnessione del proprio utente in maniera tale da impedirne l'utilizzo a personale non autorizzato.

E' buona pratica effettuare, almeno una volta a settimana, un riavvio del PC (oltre allo spegnimento), per l'applicazione degli aggiornamenti, o comunque ogniqualvolta venga richiesto dal sistema.

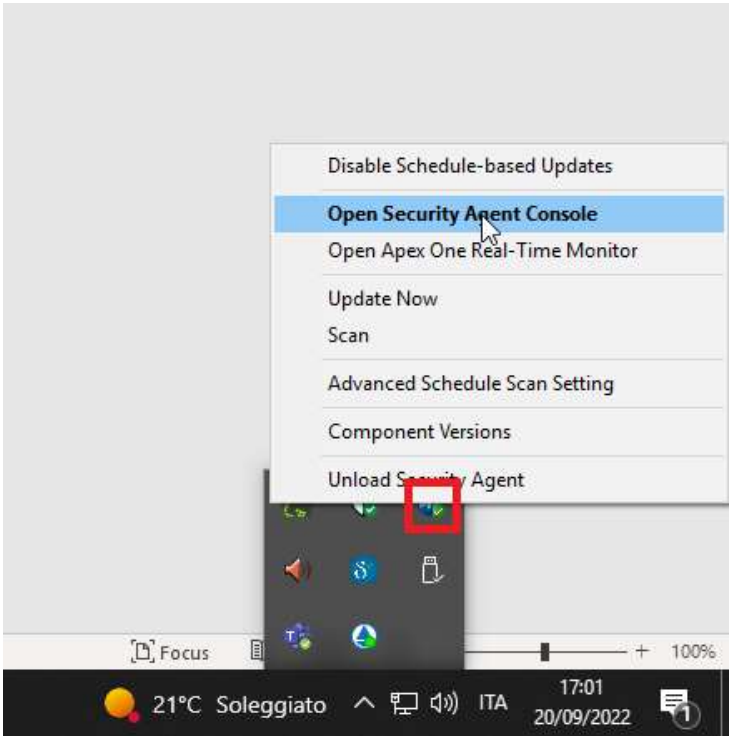
E' severamente vietato l'uso o l'installazione di programmi diversi da quelli distribuiti ed installati ufficialmente dall'Ufficio Informatica.

E' sconsigliato il collegamento di chiavette personali, dischi esterni o qualunque dispositivo non fornito dall'Ente; anche in presenza di dispositivi forniti dall'Ente è vietato memorizzare su di essi eventuali dati sensibili riconducibili a fatti e/o persone.

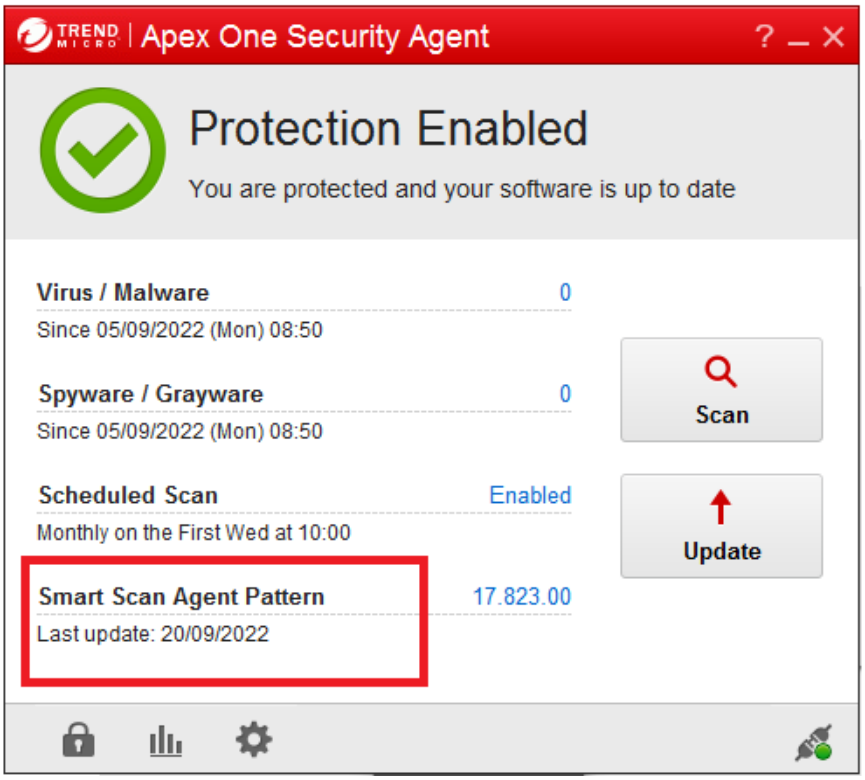
Si ricorda che i file salvati su PC **NON** sono soggetti a backup pertanto in caso di guasto al sistema il recupero dei dati non è garantito.

E' buona norma controllare che l'antivirus sia aggiornato ed eventualmente segnalare all'ufficio informatica eventuali mancati aggiornamenti. A tale scopo basta aprire l'agent antivirus

- ➔ Icone nascoste → Pallino blu con linea verde → Open Security Agent Console



e controllare l'ultima riga, accertandosi che la data sia il più recente possibile



Rete

Navigare sempre su siti noti e che utilizzano il protocollo https. In caso di problemi su un sito che normalmente funziona, contattare l'ufficio informatica per le valutazioni del caso.

Non scaricare programmi o file con estensione .exe, .docx, .zip, senza previo consulto dell'ufficio informatica; prestare particolare attenzione allo scambio di files tramite programmi di condivisione (Wetransfer, Dropbox,..) . Per l'invio di file di grandi dimensioni, il sistema GIFRA ne permette la spedizione previa abilitazione. In caso di necessità chiedere all'ufficio informatica.

E' vietato l'utilizzo di siti online per la conversione di file in formati diversi dall'originale (es .. PDF to Word, I love PDF..)

Phishing

Linee guida per l'autotutela

- ➔ Non utilizzare il proprio account e-mail fornito dal Titolare per usi personali
- ➔ Non inviare risposte ad e-mail che richiedano dati ovvero credenziali di accesso
- ➔ Non aprire incondizionatamente allegati anche se provengono da mittenti noti, soprattutto se hanno le estensioni (.zip, .docx, .exe)
- ➔ Verificare sempre ortografia e sintassi nel testo delle e-mail ricevute
- ➔ Diffidare di e-mail che mettono urgenza, che minacciano sanzioni, che promettono premi e vincite o che contengono richieste di aiuto
- ➔ Non cliccare su link contenuti sul corpo delle e-mail

Eventuali email contenti richieste di rinnovi contratti, fatture (anche se di cortesia), tracking di spedizioni o segnalazioni di credenziali compromesse vanno sempre considerate in primis come fraudolente e vanno quindi analizzate caso per caso col supporto dell'ufficio informatica.

Sospetto incidente

In caso di apertura di e-mail / link / allegati sospetti il dipendente deve informare subito, in maniera circostanziata, l'Ufficio Informatica della avvenuta fuoriuscita di dati all'esterno. Se il dipendente sospetta di aver comunicato le credenziali ad un sito truffaldino è necessario che egli cambi immediatamente la password utilizzando un dispositivo diverso, avvisando immediatamente l'Ufficio Informatica.