Awareness azioni di Sicurezza

Raccomandazioni di Sicurezza per l'Utente - Smart Working

Ottobre, 2021

Tabella delle versioni

Versione	Data	Note
1.0	29/10/2021	Nuovo formato documento

Si fa raccomandazione agli Utenti, per quanto concerne il proprio PC di casa usato in telelavoro, di assicurarsi periodicamente:

1. che il sistema operativo della propria workstation sia aggiornato;
2. che la propria workstation sia dotata di antivirus e che questo sia aggiornato;
3. che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale. Al momento della modifica delle password evitare di fare solo piccole modifiche come, ad esempio, numerazioni progressive ecc…;
4. di eseguire il backup periodico dei dati elaborati sul proprio PC nell'ambito della sfera lavorativa;

Si consiglia inoltra di evitare di iscriversi a siti internet non riconducibili alla sfera lavorativa, ovvero utilizzando la casella di posta istituzionale; tali siti potrebbero infatti essere poco sicuri nella protezione dei dati personali, con eventuali ripercussioni in violazioni all'interno della propria operatività lavorativa.

Si ricorda che infezioni a pc personali usati per lavoro possono recare danni alla sicurezza dei dati di lavoro, con ripercussioni sull'intero patrimonio informativo del Ministero dell'Istruzione.
Si raccomanda l'uso di supporti removibili quali chiavette usb e/o hard disk esterni ecc. con molta cautela, ovvero verificarne sempre la pulizia da virus prima di utilizzarli sulle postazioni istituzionali.

A tal fine si consiglia quindi:

- usare gli strumenti messi a sua disposizione dal Ministero quali Posta Elettronica e OneDrive;
- al momento della connessione di un supporto removibile, avviare una scansione completa dello stesso attraverso il software antivirus.

Grazie per la collaborazione,

CSIRT MI