



Istituto Professionale di Stato per i Servizi Alberghieri con Convitto annesso "Dea Persefone"

89044 LOCRI (RC) - Tel. Scuola 0964390572

Cod. Mecc. RCRH080001 - C.F. 81000650804 - Sito: www.ipssalocri.edu.it P.E.O.:

rcrh080001@istruzione.it - P.E.C.: rcrh080001@pec.istruzione.it

Prot. n. 2390/1.3

Locri, 13/03/2021

CIRCOLARE N. 130

A Tutto il Personale
Al DSGA
Atti
Sito Web

OGGETTO: Raccomandazioni di sicurezza per l'Utente

Per opportuna conoscenza e norma, si trasmette in allegato nota CSIRT MI del 12/03/2021.



Il Dirigente Scolastico

Prof.ssa Anna Maria Cama

La firma autografa è sostituita a mezzo stampa
in base ai sensi dell'art. 3 c. 2 del D. lgs. n. 39/93

CSIRT-MI

Raccomandazioni di sicurezza per l'Utente (smart working)

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 inoltre 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.

CSIRT-MI

Raccomandazioni di sicurezza per l'Utente

Allo scopo di limitare l'occorrenza di incidenti di sicurezza si rappresentano le seguenti raccomandazioni.

- non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungono da caselle di posta non note;
- non installare software sulla propria postazione di lavoro gestita, soprattutto se a seguito di sollecitazioni via e-mail che presentino link di accesso ad altre pagine o di esecuzione file.
- non dare seguito alle richieste di e-mail sospette;
- nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, verificare attentamente il contesto: ovvero se l'e-mail fosse attesa, le frasi siano scritte con grammatica e sintassi corretta, se il software di cui si richiede l'installazione abbia un fine specifico, se eventuali link nell'e-mail puntino a siti conosciuti, se il mittente fosse noto e/o corretto.

In caso di dubbi rispetto a quanto sopra rivolgersi sempre conferma ai rispettivi referenti informatici.