



**I.P.S.S.E.O.A "FRANCESCO PAOLO CASCINO"  
PALERMO**

I.P.S.S.A.R. "F.P. CASCINO" - PALERMO  
Prot. 0011243 del 19/04/2021  
(Uscita)

**CIRCOLARE**

**Al Sito Web della scuola  
Ai Sigg. Docenti**

**OGGETTO: sicurezza informatica – Raccomandazioni da parte della Presidenza del Consiglio dei Ministri**

A seguito della comunicazione inviata da CSIRT MI (CSIRT Computer Security Incident Response Team - Italia: istituito presso il Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri) avente come oggetto: CSIRT MI - Alert PYSA-CONTI si riportano, in allegato:

1. Raccomandazioni di sicurezza per l'utente;
2. CSIRT-MI Raccomandazioni di Sicurezza Posta Elettronica.

Il personale docente è tenuto ad attenersi a quanto indicato al punto n. 1 quando usufruisce di un dispositivo di proprietà della scuola e alle raccomandazioni al punto n. 2 quando utilizza la propria mail ministeriale (@istruzione.it) o quella istituzionale (@alberghierocascino.edu.it).

Per qualsiasi problematica si prega di rivolgersi al prof. Lillo Zagarro, animatore digitale della scuola.

**Si raccomanda il massimo rispetto delle indicazioni sopra elencate.**

**IL DIRIGENTE SCOLASTICO**  
**Prof.ssa Lucia Assunta Ievolella**  
(documento firmato digitalmente)

## **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.

## **CSIRT-MI**

### ***Raccomandazioni di Sicurezza Posta Elettronica***

Allo scopo di limitare l'occorrenza di incidenti di sicurezza sulla casella di Posta Elettronica si rappresentano le seguenti raccomandazioni:

1. non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle di posta non note;
2. non installare software sulla propria postazione, soprattutto se a seguito di sollecitazioni via e-mail che presentino link di accesso ad altre pagine o di esecuzione file.
3. non dare seguito alle richieste di e-mail sospette;
4. 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'email puntino a siti conosciuti, se il mittente fosse noto e/o corretto;
5. di scansionare periodicamente per la ricerca malware le postazioni di lavoro ed i dispositivi che accedono alla Posta Elettronica;

nel caso di utilizzo del PC personale (telelavoro/smart working) si raccomanda di assicurarsi periodicamente:

6. che il sistema operativo della propria workstation sia aggiornato;
7. che la propria workstation sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;
8. che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale.
9. al momento della modifica delle password evitare di fare solo piccole modifiche come ad esempio numerazioni progressive ecc...;
10. di eseguire il backup periodico dei dati elaborati 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.