



Regione Siciliana



Repubblica Italiana



Unione Europea

## ISTITUTO COMPRENSIVO "G. ALBO - GIOVANNI XXIII" - MODICA

Via F. Camillo, 40 - Tel.: 0932/1847426 Cell. 3387392936

C.F.: 90033440885

Codice Meccanografico: RGIC837007

Codice Univoco d'Ufficio: UF9JMY

E-Mail: [rgic837007@istruzione.it](mailto:rgic837007@istruzione.it)

Pec: [rgic837007@pec.istruzione.it](mailto:rgic837007@pec.istruzione.it)

Sito web: [www.scuolagiacomalobogiovannixiii.edu.it](http://www.scuolagiacomalobogiovannixiii.edu.it)

---

Circolare n.12

- Al D.S.G.A.
- A tutto il personale Docente e ATA
- Al sito web

### OGGETTO: CSIRT MI – Raccomandazioni e Indicazioni per la Sicurezza

In riferimento a quanto in oggetto, si porta a conoscenza tutto il personale scolastico della nota informativa allegata, con le indicazioni per la sicurezza informatica cui attenersi scrupolosamente per tutela dei dati sensibili.

- **"Sicurezza della Postazione di Lavoro utente"**
- **"Sicurezza posta elettronica"**

Si allega la nota pervenuta a questa Istituzione.

  
IL DIRIGENTE SCOLASTICO  
Prof.ssa *Fernanda Grana*



# Raccomandazioni e Indicazioni per la Sicurezza

13 Settembre, 2021

Gentile Utente,

anche in questo ultimo periodo stiamo rilevando il blocco di mail di phishing indirizzate al personale ministeriale da parte dei sistemi di sicurezza del MI; tali messaggi sono indirizzati a caselle di posta elettronica istituzionali, provenendo da mittenti 'verosimili' e rispetto ai quali nei testi si richiedono azioni di accesso a pagine web/download file che in realtà possono recare problemi alla postazione di lavoro e, a cascata, all'infrastruttura tecnologica del MI.

Con la stessa frequenza, inoltre si rileva anche attività anomala da parte di alcune caselle di posta istituzionali che inviano mail di spam all'insaputa dell'Utente titolare del account, la cui compromissione il più delle volte è dovuta ad infezioni da virus sulle postazioni di lavoro o sui dispositivi utilizzati per l'accesso.

La causa delle suddette situazioni risiede sicuramente in un'intensa e sempre più sofisticata attività da parte dei cyber attaccanti in internet, interessati a carpire informazioni riservate e sensibili, personali e/o dell'Organizzazione, ma anche e soprattutto in comportamenti da parte delle persone non sempre in linea con le buone prassi di sicurezza e le indicazioni in tal senso da parte dell'Amministrazione.

Si ribadisce allo scopo quindi di:

- **scansionare periodicamente per la ricerca virus le postazioni di lavoro ed i dispositivi utilizzati per lavoro;**
- **nel caso di utilizzo del PC personale (telelavoro/smart working) assicurarsi periodicamente:**
  - che il sistema operativo sia aggiornato;
  - che la propria postazione di lavoro sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;
  - che le proprie password di posta e strumenti di lavoro siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che, al momento della modifica, non siano apportate solo piccole modifiche (come ad esempio numerazioni progressive).
- **non usare l'account di lavoro per registrarsi in internet per fini non riconducibili alla sfera di lavoro ed evitare di salvare le password nel browser di navigazione Internet;**



- **si consiglia di non lasciare il PC portatile incustodito;**
- **si raccomanda l'uso di supporti removibili quali chiavette usb e/o hard disk esterni ecc. con molta cautela.** Al momento della connessione di un supporto removibile, si consiglia di avviare una scansione completa dello stesso attraverso il software antivirus.

Qualora doveste incorrere in messaggi mail di phishing, si ricorda quanto segue:

- **non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle non note;**
- **non installare software sulle proprie postazioni di lavoro, soprattutto se a seguito di sollecitazioni via e-mail;**
- **non dare seguito alle richieste incluse nei messaggi;**
- **nel caso in cui le richieste provengano da parte del personale tecnico dell'Amministrazione, verificare attentamente il contesto: l'e-mail era attesa? Le frasi sono scritte con grammatica corretta? Il software da installare ha un fine specifico? Eventuali link nell'e-mail puntano a siti conosciuti? Il mittente è corretto?**

Si ricorda inoltre che nell'area riservata intranet allo CSIRT MI (dopo il login, sezione: *Area Riservata > Computer Security Incident Response Team > Security Awareness*) sono presenti i contenuti relativi a campagne malevole di phishing in corso ed aggiornamenti su nuovi virus che potrebbero infettare le postazioni di lavoro del personale della Pubblica Amministrazione.

È fortemente consigliata la lettura dei suddetti contenuti, allo scopo di tenersi aggiornati sui rischi informatici incombenti sull'Amministrazione e proteggere sia la propria operatività sia il patrimonio informativo del Ministero da possibili attacchi.

Grazie della collaborazione

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'email 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.

