



I.I.S.S. "LUIGI EINAUDI"



ISTITUTO TECNICO STATALE COMMERCIALE, TURISTICO E PER GEOMETRI
Viale Paolo Borsellino, 20 – 74024 Manduria (TA) Centralino: Tel./Fax 099/9711152
ISTITUTO PROFESSIONALE STATALE SERVIZI PER L'AGRICOLTURA E LO SVILUPPO RURALE
Via per Maruggio Km. 2 – 74024 Manduria (TA) Tel.Fax 099/9712679

C.F.90214640733

www.einaudimanduria.gov.it

TAIS02600R@ISTRUZIONE.IT

Circolare n. 68/ATA del 05.06.2020

PERSONALE ATA
SEDE

p.c. **Dirigente Scolastico**

**OGGETTO: MIUR – Computer Security Incident Response Team- ATTENZIONE A PHISHING
E MALSPAM**

Al fine della sicurezza informatica si allega alla presente nota mail del MIUR del 20.05.2020 contenente le raccomandazioni per la difesa da virus e minacce informatiche affinché siano seguite dalle SS.VV.

Si raccomanda di prestare particolare attenzione e la puntuale osservanza di quanto nella stessa prescritto.

IL D.S.G.A.

(Dott.ssa Tecla Famà)

Firma autografa sostituita a mezzo stampa

ai sensi dell'articolo 3, comma 2, del D.lgs n. 39 del 1993

Da: noreply@istruzione.it
Oggetto: MI - Computer Security Incident Response Team - ATTENZIONE A PHISHING E MALSPAM
Data: 20/05/2020 10:08:06

I.I.S.S. - "L. EINAUDI" - MANDURIA
Prot. 0003225 del 20/05/2020
C19 (Entrata)

OSK A J.

Gentile utente,

si segnala in questi giorni:

- l'arrivo di mail di spam massivo a indirizzi di posta elettronica istituzionali, con messaggi temporalmente ravvicinati;
- l'occorrenza di situazioni per le quali gli Utenti ricevono messaggi da mittenti 'verosimili' e rispetto ai quali nelle mail si richiedono azioni di accesso a pagine web/download file potenzialmente malevoli.

Allo scopo di limitare l'occorrenza di incidenti di sicurezza, rispetto ai suddetti scenari si ribadiscono pertanto le seguenti raccomandazioni.

- non dare seguito all'apertura di file non attesi dalla dubbia provenienza o che giungono da caselle non note;
- non installare software soprattutto se a seguito di sollecitazioni via e-mail. Non date seguito alle richieste di mail sospette;
- nel caso in cui la richiesta provenga da parte del personale tecnico della nostra 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?

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

Raccomandiamo inoltre, per quanto concerne il proprio PC di casa usato in telelavoro, di assicurarsi periodicamente:

- 1) - che il sistema operativo del proprio PC sia aggiornato;
- 2) - che il proprio PC sia dotato di antivirus e che questo sia aggiornato;
- 3) - che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per ser distinti e che afferiscono a sfera lavorativa e personale. Al momento della modifica delle password evitare di 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.

Grazie per la collaborazione

Ministero dell'Istruzione

D.G.S.I.S.