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. 50/ATA del 24.04.2020

PERSONALE ATA
SEDE

p.c. **Dirigente Scolastico**

OGGETTO: MIUR - Sicurezza Informatica- ATTENZIONE A NUOVE CAMPAGNE DI PHISHING E MALSPAM

Al fine della sicurezza informatica si allega alla presente nota mail del MIUR del 22.04.2020 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: MIUR - Sicurezza Informatica - ATTENZIONE A NUOVE CAMPAGNE DI PHISHING E MALSPAM
Data: 22/04/2020 10:06:43

Gentile utente,

Il CERT-PA ci segnala le seguenti nuove minacce in essere in questi giorni.

1) Campagna di phishing.

E' stata rilevata una consistente campagna di phishing, veicolata attraverso una e-mail con oggetto "Avvertimento Aggiornamento Necessario", volta alla sottrazione delle credenziali degli utenti Outlook

NON DATE SEGUITO A COMUNICAZIONI DI QUESTO TIPO

2) Nuova campagna di malspam volta a veicolare il malware sLoad.

Al fine di rendere credibile la notifica di un *documento contabile*, la e-mail riporta il **codice fiscale** d nell'oggetto, nel corpo del messaggio e nel nome dell'allegato.

L'allegato compresso, denominato "*fattura-cf-***CODICEFISCALE***.zip*", contiene due file malevoli tra

NON APRITE GLI ALLEGATI DI QUESTA TIPOLOGIA DI EMAIL

E' possibile trovare ulteriori informazioni ai seguenti indirizzi:

https://www.cert-pa.it/notizie/campagna-di-phishing-ai-danni-di-utenti-outlook/

https://www.cert-pa.it/notizie/campagna-malspam-sload-veicolata-in-italia-via-pec/

Ribadiamo le seguenti raccomandazioni.

Si raccomanda di non dare seguito all'apertura di file non attesi dalla dubbia provenienza o ch caselle non note.

Non installate software soprattutto se a seguito di sollecitazioni via e-mail. Non date seguito sospette.

Nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministra attentamente il contesto: l'e-mail era attesa? Le frasi sono scritte con grammatica corretta installare ha un fine specifico? Eventuali link nell'e-mail puntano a siti conosciuti? Il mittente

In caso di dubbio chiedete conferma ai vostri referenti.

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

) che il sistema operativo del proprio PC sia aggiornato

) che il proprio PC sia dotato di antivirus e che questo sia aggiornato

che le proprie password siano sicure, ovvero complesse, non facilmente individu stinti e che afferiscono a sfera lavorativa e personale. Al momento della modifica dell lo piccole modifiche come ad esempio numerazioni progressive ecc...

di eseguire il backup periodico dei dati elaborati sul proprio PC nell'ambito della s

azie per la collaborazione