Liceo "Galilei - Vanoni"

con sezioni associate di
LICEO ARTISTICO - LICEO CLASSICO – LICEO LINGUISTICO
LICEO SCIENTIFICO – LICEO DELLE SCIENZE APPLICATE
LICEO DELLE SCIENZE APPLICATE QUADRIENNALE
LICEO DELLE SCIENZE UMANE

✉ via XX Settembre, 65 - 73048 NARDÒ (LE) – Ambito Territoriale 18 – C. F. 93173020756
C.M.: LEPS25000V – *E-mail*: leps25000v@istruzione.it – *P.e.c.*: leps25000v@pec.istruzione.it– *Tel.*: +39 0833 570542
Sito istituzionale: www.liceogalileinardo.edu.it

CIRCOLARE N. 125

Ai Docenti
Al personale ATA
Al DSGA
Al RE
Al SITO WEB

OGGETTO: Phishing attualmente in corso sul territorio nazionale, rivolta in modo specifico al settore dell'istruzione.

Si informa tutto il Personale scolastico che i sistemi di monitoraggio hanno rilevato una campagna di phishing attualmente in corso sul territorio nazionale, rivolta in modo specifico al settore dell'istruzione.

Modalità dell'attacco

Falsificazione del mittente (Email Spoofing)
I messaggi sembrano provenire da Ministeri, Enti Pubblici, Autorità di Controllo o fornitori di servizi qualificati, inducendo il destinatario a considerarli attendibili.

Esca del "File Riservato"
Le comunicazioni invitano a visualizzare o scaricare un presunto documento riservato tramite link o pulsanti presenti nel messaggio.

Obiettivo malevolo
Il collegamento conduce a siti fraudolenti progettati per sottrarre le credenziali di accesso degli utenti.

Regole fondamentali di prevenzione
• **Verificare sempre l'indirizzo reale del mittente**, controllando attentamente il dominio dell'indirizzo e-mail.
• **Diffidare di comunicazioni "Urgenti" o "Riservate"** che richiedano azioni immediate o l'apertura di documenti tramite link esterni.
• **Non cliccare su link o pulsanti sospetti** e verificare preventivamente l'effettiva destinazione del collegamento.
• **Non inserire mai le proprie credenziali su pagine raggiunte tramite e-mail** o su siti di cui non sia stata verificata l'autenticità.
• **In caso di dubbi, verificare la comunicazione tramite canali ufficiali** diversi da quelli indicati nel messaggio ricevuto.
• **Prestare attenzione a errori grammaticali, formule generiche o richieste inconsuete**, spesso indice di tentativi di frode.
• **Si raccomanda, a titolo precauzionale, di procedere al cambio delle password delle caselle istituzionali PEO e PEC**, adottando credenziali robuste e non riutilizzate su altri servizi.

Si invita tutto il personale scolastico a mantenere elevata l'attenzione e a segnalare tempestivamente eventuali comunicazioni sospette ai referenti informatici, evitando qualsiasi interazione con link, allegati o richieste di credenziali.

LA DIRIGENTE SCOLASTICA
Emilia Fracella
Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3 c. 2 del D.L. 39/93