Istituto di Istruzione Secondaria Superiore
"Archimede"
Via Sipione, 147 - 96019 Rosolini (SR)
Tel.0931/502286 – Fax: 0931/850007
e-mail: sris017003@istruzione.it - sris017003@pec.istruzione.it
C.F. 83001030895 - Cod. Mecc. SRIS017003
Codice Univoco Ufficio: UF5C1Y
www.istitutosuperiorearchimede.edu.it

CIRCOLARE n. 135 del 09/01/2020

Al personale docente e ATA
Agli Studenti e Alle Studentesse
Alle Famiglie
Al DSGA

OGGETTO: Sicurezza informatica – Azioni di phishing verso mail istituzionali

Nell'ultimo periodo si stanno rilevando numerose mail di phishing indirizzate al personale ministeriale; tali messaggi sono indirizzati a caselle di posta elettronica istituzionali (@posta.istruzione.it), 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 Ministero dell'Istruzione.
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 dell'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 di questi fenomeni è da imputarsi sia ad attacchi informatici di eventuali hacker, sia dall'imprudente comportamento di molti utenti e dal non rispetto delle buone prassi e indicazioni da parte dell'Amministrazione.

Dato che i criteri per la creazione dell'username sono noti, se si usa una password facile da indovinare, risulterà semplice per un malintenzionato appropriarsi della casella di posta elettronica per usi illeciti, pertanto si consiglia fortemente la verifica dei canoni di sicurezza appresso indicati:

- scansionare periodicamente per la ricerca virus le postazioni di lavoro ed i dispositivi utilizzati per lavoro;
- nel caso di utilizzo del P.C. 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.

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?*

Maggiori dettagli sulle campagne phishing in atto sono rinvenibili all'indirizzo internet: *https://csirt.gov.it/*

La Dirigente Scolastica
dott.ssa Maria Teresa Cirmena