Istituto di Istruzione Secondaria Superiore "Giuseppe Colasanto" Andria

I.I.S.S. "Giuseppe Colasanto" – Via Niccolò Paganini snc 76123 Andria (BT) – Tel.: 0883/563206 – Fax: 0883/564236 – Sito: http://www.istitutocolasanto.edu.it – PEO: btis04400a@istruzione.it – PEC: btis04400a@pec.istruzione.it – Codice fiscale: 90005000725 – Codice meccanografico: BTIS04400A – Codice univoco: UF4MQ6

CIRCOLARE INTERNA N. 182
A.S. 2025/2026

Al personale ATA
Al DSGA

Oggetto: Raccomandazione al personale ATA per l'uso dei sistemi informatici nello svolgimento dell'attività lavorativa.

I sistemi informatici delle pubbliche amministrazioni sono sempre più oggetto di attacchi con gravi conseguenze sulla riservatezza e l'integrità dei dati trattati e sulla continuità dei servizi prestati. Secondo le segnalazioni del CSIRT MI, particolarmente rilevanti sono, in questo ultimo periodo, i tentativi di phishing indirizzati alle caselle istituzionali degli istituti scolastici e a quelle personali dei suoi dipendenti. 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 (o personale del dipendente) e, a cascata, all'infrastruttura tecnologica del MI. Per ulteriori informazioni sul phishing si invita a visionare il video curato da CSIRT-MI e presente al link https://www.youtube.com/watch?v=oqgknseErEU&t=23s

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.

Allo scopo di limitare l'occorrenza di incidenti di sicurezza si rappresentano le seguenti raccomandazioni rivolte prioritariamente al personale che utilizza le dotazioni dell'istituto per svolgere la propria attività e a quello che usa dotazioni personali per attività di telelavoro, smartworking o BYOD (Bring Your Own Device) ma che è importante sia osservato anche nell'uso delle dotazioni personali per scopi personali da parte di tutti i dipendenti dell'amministrazione scolastica.

Raccomandazioni uso della posta elettronica:

- 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;
- scansionare periodicamente per la ricerca malware le postazioni di lavoro ed i dispositivi che accedono alla Posta Elettronica;
- nel caso in cui la richiesta provenga da parte del personale tecnico del Ministero dell'Istruzione o dagli amministratori dei nostri sistemi informatici, 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.

- Evitare di usare la casella di posta istituzionale (anche quella personale sul dominio istruzione.it) per iscriversi a servizi o siti non riconducibili alla sfera lavorativa.
- Evitare di cliccare su un link quando punta su destinazioni non note (posizionando il puntatore del mouse sul link senza cliccare dà in genere la possibilità di vedere l'indirizzo contenuto nel link stesso);

Raccomandazioni per attività in telelavoro e smartworking o svolte da casa con propri dispositivi personali:

1. Nel caso in cui utilizzi un PC personale per svolgere l'attività lavorativa, prima del suo primo utilizzo, installa un buon antivirus e fai una accurata scansione preventiva per rimuovere qualunque software malevolo
2. Utilizza i sistemi operativi per i quali attualmente è garantito il supporto (non utilizzare, ad esempio, macchine con sistema operativo windows 7 di cui microsoft ha terminato il supporto)
3. Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo ed accertati che siano abilitati
4. Non installare software proveniente da fonti/repository non ufficiali
5. Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
6. Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette
7. Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza
8. Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.
9. Non memorizzare sui dispositivi le password di accesso alle piattaforme ed ai sistemi utilizzati per il lavoro a distanza
10. Non memorizzare sul client di posta elettronica le credenziali di accesso alle caselle istituzionali
11. Accertati di aver impostato una password sicura sul router utilizzato per l'accesso ad Internet (accertati di non aver lasciato la password di default proposta dal costruttore e nota a qualunque malintenzionato)
12. Se utilizzi una connessione wifi, accertati di adottare una password sicura per il suo accesso (mai lasciare accessi liberi alla rete wifi)

Regole nella scelta delle password:

- Modificare le credenziali delle caselle, con cadenza trimestrale, adottando requisiti di complessità;
- Al manifestarsi di una sospetta anomalia o attività legata ad accessi non autorizzati in una casella, provvedere subito a cambiare la password del servizio;
- Usare una parola chiave di almeno nove caratteri
- Non usare le stesse password per l'accesso a servizi differenti
- La parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato (come per esempio nome, cognome, data di nascita, numeri di telefono, etc. propri o dei propri familiari)
- Usare una combinazione di caratteri alfabetici e numerici, meglio se contenente almeno un segno di interpunzione o un carattere speciale;

- Conservare con cura la parola chiave evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio

Ricordiamo che una violazione dei sistemi informatici comporta spesso anche una violazione dei dati personali trattati (data breach) che deve essere tempestivamente segnalato al Dirigente Scolastico.

Andria, 29/12/2025

IL DIRIGENTE SCOLASTICO
Prof. Cosimo Antonino Strazzeri