



Prot. n., *vedi segnatura*

Civitanova M., 17 settembre 2024

Al Personale Docente

Interno ed Esterno

Agli Assistenti Amministrativi e Tecnici

Al DSGA

Al Sito Web

Amministrazione Trasparente:

Disposizioni Generali

Privacy

Oggetto: Raccomandazioni ai docenti, al DSGA, al personale Assistente Amministrativo e Tecnico per l'uso dei sistemi informatici nello svolgimento della propria 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, sono particolarmente rilevanti 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=oggknseErEU&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 informatici si rappresentano le seguenti raccomandazioni rivolte al DSGA, al personale amministrativo, tecnico e docente che utilizza le dotazioni dell'istituto per svolgere le attività didattiche in presenza o da remoto utilizzando le dotazioni fornite dalla scuola o quelle personali (BYOD).

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 postazione fornita dalla scuola, 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;
- 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.

Firmato digitalmente da EDOARDO IACUCCI

MCIC83500T - A7C46D6 - REGISTRO PROTOCOLLO - 0010039 - 18/09/2024 - I.4 - I



- Evitare di usare la casella di posta istituzionale (anche quella personale sul dominio *civitanovatacito.edu.it* o *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);

Regole nella scelta delle password:

- Aggiornare regolarmente le credenziali di accesso alle caselle e-mail, al registro elettronico, ai gestionali di segreteria e ad altri servizi eventualmente utilizzati adottando requisiti di complessità;
- 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;
- Al manifestarsi di una sospetta anomalia o attività legata ad accessi non autorizzati in una casella, provvedere subito a cambiare la password del servizio.

Raccomandazioni uso dotazioni informatiche a scuola

1. Non installare senza autorizzazione alcun software sulle postazioni utilizzate per il registro elettronico o per l'attività didattica/lavorativa;
2. Se colleghi dispositivi mobili (pen-drive, hdd-esterno, etc) alle dotazioni della scuola fai prima di tutto una scansione antivirus ad individuare la presenza di eventuale software malevolo;
3. Effettua sempre il log-out dai servizi/portali utilizzati (ad esempio *posta*, *registro elettronico* o *aree riservate di siti*) quando ti allontani, anche temporaneamente, dalla postazione;
4. Non memorizzare sui dispositivi le password di accesso alle piattaforme ed ai sistemi utilizzati per il lavoro a distanza;
5. Non memorizzare sul client di posta elettronica le credenziali di accesso alle caselle di posta elettronica (istituzionali o personali);
6. Accertati di aver scelto le tue password attenendoti alle regole fissate nella sezione precedente;
7. Non lasciare mai a nessuno e per nessun motivo le tue credenziali di accesso ai sistemi ed ai servizi;
8. Conserva con cura la parola chiave evitando di trascriverla dove può essere carpita dagli studenti o da chiunque altro;
9. Nell'uso della rete wi-fi dell'istituto non condividere né rendere visibile la password di accesso;
10. Non memorizzare sui dispositivi della scuola documenti contenenti dati personali (di alunni o di altre persone) che potrebbero subire una violazione in caso di furto o di accesso da parte di persone non autorizzate.

Raccomandazioni per lo svolgimento dell'attività lavorativa da casa (didattica o no)

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 XP o 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 o ai servizi con i quali svolgi l'attività lavorativa (il registro elettronico o i gestionali di segreteria, per esempio);
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 wi-fi, accertati di adottare una password sicura per il suo accesso (mai lasciare accessi liberi alla rete wi-fi).

* * *

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.

Si precisa che il Titolare è responsabile della mancata esecuzione degli adempimenti previsti dal D.lgs. n.196/2003 e del Regolamento UE 2016/679, fermo restando che le responsabilità per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili riguardano anche gli incaricati che non rispettino o non adottino le misure necessarie.

* * *

L'Ufficio del Personale avrà cura di verificare e documentare con data certa l'avvenuta sottoscrizione per presa visione della determina dirigenziale di designazione dell'unità organizzativa di riferimento e delle presenti *Raccomandazioni* da parte del personale in indirizzo; del pari, per i supplenti in servizio durante l'anno scolastico dovrà essere predisposta per la firma la seguente dichiarazione: *"Dichiaro di aver preso visione della determina dirigenziale di designazione dell'unità organizzativa Docenti/Assistenti Amministrativi/Assistente Tecnico cui vengo a far parte e delle specifiche linee guida e Raccomandazioni relative alla sicurezza"*.

Il Dirigente Scolastico

Edoardo Iacucci

(Documento firmato digitalmente)