Ministero dell'Istruzione
ISTITUTO COMPRENSIVO *infanzia-primaria-sec. 1° grado*
Via Circonvallazione, 6 – **Mozzanica** (Bg) Tel: 0363 82109-Fax: 0363 828340e-mail
uffici: bgic85800C@istruzione.it - p.e.c.: bgic85800c@pec.istruzione.it
sito web:www.icmozzanica.edu.it - cod mecc. BGIC85800C - C.F. 83002250161

DISCIPLINARE INTERNO PER L'USO DI INTERNET E DELLA POSTA ELETTRONICA IN SEDE EI SMARTWORKING

Sommario

1. Premessa

L'uso degli strumenti informatici, della posta elettronica e l'accesso ad Internet da parte delle amministrazioni pubbliche si và sempre più diffondendo sotto l'impulso della nuova legislazione, con l'obiettivo di migliorare l'efficienza operativa, contenere i costi ed assicurare una maggiore qualità delle prestazioni.
I servizi informativi sono ormai diventati fondamentali anche per gli istituti scolastici che sempre più dovranno utilizzare strumenti come la posta elettronica ed Internet per fornire servizi all'utenza e per migliorare la propria efficienza.
In particolare, in seguito alle procedure di lavoro agile (c.d. smart working) adottate in seguito alla pandemia di COVID-19, l'utilizzo dei sistemi informatici da remoto tramite sistemi cloud è entrato a far parte delle modalità ordinarie di svolgimento del lavoro da parte dei dipendenti dell'amministrazione.

Pertanto è necessario che siano adottate adeguate ed opportune misure di sicurezza volte a proteggere la disponibilità e l'integrità delle risorse informative e a tutelare la riservatezza dei dati personali di tutti. A questo proposito si richiama quanto viene riportato anche nelle Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni del CNIPA (Comitato Nazionale per l'Informatica nella Pubblica Amministrazione):

"Tutti i dipendenti dell'Amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet, evitando eventi dannosi, anche al fine di non danneggiare l'immagine dell' Amministrazione".

Dall'esame di diversi reclami, segnalazioni e quesiti pervenuti, il Garante per la protezione dei dati personali ha preso atto dell'esigenza di prescrivere ai datori di lavoro pubblici e privati alcune misure, necessarie o opportune, per conformare alle vigenti disposizioni in materia di Privacy il trattamento di dati personali effettuato per verificare il corretto utilizzo, nel rapporto di lavoro, della Posta elettronica e di Internet.
A tale scopo è stato emanato il provvedimento generale pubblicato sul Bollettino n. 81 del Marzo 2007 e, successivamente, sulla Gazzetta Ufficiale – Serie generale n. 58 del 10.03.2007 (di seguito "il Provvedimento").
Con il presente disciplinare si fornisce concreto riscontro alle prescrizioni del Garante e si conforma a quanto previsto nelle conclusioni del Provvedimento, al punto 2), lett. a).

2. Principi

Il presente disciplinare viene predisposto nel rispetto della vigente disciplina in materia di Privacy, con riguardo, in particolare, alle norme del Reg. UE 679/2016 (GDPR) e del D. Lgs. 196/03 (Codice in materia di protezione dei dati personali) che disciplinano il trattamento effettuato dai soggetti pubblici.
L'Istituto Scolastico garantisce che il trattamento dei dati personali dei dipendenti relativo all'utilizzo da parte degli stessi di risorse informatiche proprie o dell'amministrazione, si conforma ai seguenti principi:

a) il principio di minimizzazione, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2 del Provvedimento);
b) il principio di trasparenza, secondo cui le caratteristiche dei trattamenti devono essere rese note agli interessati poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli

connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori

3. Utenti autorizzati all'uso di Internet

Per quanto riguarda l'uso delle dotazioni informatiche e l'accesso ad internet si individuano 3 tipologie di utenti:

1) Personale amministrativo: autorizzato all'uso per lo svolgimento dell'attività amministrativa
2) Personale docente: autorizzato all'uso per qualunque attività educativa, didattica e formativa.
3) Alunni: autorizzato limitatamente all'attività educativa, didattica e formativa programmata dai docenti

4. Ubicazione postazioni di lavoro

Per quanto riguarda il personale amministrativo, ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento della presa di servizio, ovvero in caso di cambiamento della propria posizione. L'uso di tale postazione non è tuttavia da ritenersi esclusivo e ciascun dipendente a seconda delle necessità potrà operare su altro PC non direttamente assegnato ***usando sempre la propria credenziale di accesso personale*** (nome utente e password).

L'accesso ad Internet da parte del personale tecnico, docente e degli alunni potrà avvenire nelle classi, nei laboratori ed in qualunque altro luogo a tale attività destinato.

5. Sistema di autenticazione

Al fine di ridurre al minimo il rischio di impieghi abusivi, l'accesso alle postazioni destinate all'attività amministrativa è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password. La gestione degli utenti è fatta in maniera centralizzata sul server di segreteria su cui è configurato un dominio in ambiente Windows server e nel quale potranno quindi essere conservate informazioni relative agli accessi dei singoli utenti.

6. Istruzione e formazione del personale

Il personale ha ricevuto specifiche istruzioni scritte in merito al comportamento da adottare nell'uso delle dotazioni informatiche messe a loro disposizione. In base alla criticità dei trattamenti effettuati da ciascuna componente, sono stati approntati specifici interventi di formazione.

7. Misure di tipo tecnologico connesse all'uso della posta elettronica

Ai fini dell'utilizzo corretto delle caselle di posta elettronica personali messe a disposizione del personale e degli alunni da parte dell'amministrazione, si mettono in evidenza i seguenti punti:

- *E' consentito l'utilizzo del proprio account a fini privati e personali, purché tale utilizzo non sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica dell'Amministrazione.*
- *Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure della Scuola e del Ministero della Pubblica Istruzione e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale*
- *E' fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del Ministero della Pubblica Istruzione.*
- *E' vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali.*
- *L'Amministrazione registra e conserva, in forma anonima, i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime: mittente del messaggio; destinatario/i; giorno ed ora dell'invio; esito dell'invio. L'amministrazione, inoltre, potrà procedere alla cancellazione*

dell'account qualora l'esistenza dello stesso non sia più compatibile con le condizioni e le finalità per cui era stato originariamente attivato (ad es. il dipendente non è più in servizio, l'alunno termina la propria permanenza nell'istituto).

Per evitare ogni interferenza con la sfera privata del personale docente e ATA, qualunque comunicazione di interesse amministrativo o di lavoro dovrà avvenire per mezzo delle caselle istituzionali.

La consultazione della posta elettronica da parte dei dipendenti può quindi riguardare:

- caselle personali
- caselle istituzionali di lavoro

UTILIZZO DELLE CASELLE PERSONALI

Il personale può consultare in orario di servizio caselle personali per motivi legati alla propria attività lavorativa. La gestione deve essere effettuata tramite servizi di "webmail": non è consentito configurare su computer dell'Istituto appositi programmi tipo Outlook o Thunderbird per gestire le proprie caselle personali (anche per garantire al dipendente la dovuta riservatezza).

Nell'uso di caselle personali all'interno della scuola, al dipendente non è comunque consentito:

- inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del MIUR;
- l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali;
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra lavorative o azioni equivalenti.

UTILIZZO DELLE CASELLE ISTITUZIONALI DI LAVORO

Le caselle istituzionali sono gestite dagli incaricati in base ai compiti loro assegnati. In caso di assenza dell'incaricato abituale, questo potrà essere sostituito da altro personale, in base all'organizzazione interna del lavoro disposta da D.S. o D.S.G.A.: quindi tali caselle devono essere utilizzate solo a scopo lavorativo e NON devono essere utilizzate come caselle personali.

Oltre alle disposizioni impartite per l'utilizzo delle caselle personali, si aggiungono le seguenti disposizioni:

- Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,....). In caso di dubbio consultare un tecnico.
- Nel caso in cui si debba inviare un documento all'esterno dell'Istituto, se non specificamente destinato alla modifica, è preferibile utilizzare il formato *.pdf.
- Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar,...)
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile. In caso di dubbio, è necessario contattare preventivamente il DS, il DSGA o un suo delegato, che definiranno l'effettiva sicurezza della stessa, consultandosi, se necessario, con l'amministratore di sistema e/o l'RPD dell'istituto.
- La casella di posta deve essere mantenuta in ordine.

8. Misure di tipo tecnologico connesse all'uso di Internet

L'Istituto Scolastico intende limitare nel maggior grado possibile i controlli sulla navigazione (che

potrebbero determinare il trattamento di informazioni personali o sensibili anche non pertinenti l'amministrazione).
Per tale motivo è fondamentale il rispetto delle disposizioni elencate, che hanno il fine di ridurre il rischio di usi impropri della "navigazione".

1. Al personale non è consentito, durante le ore di lavoro:
   - servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
   - utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting social network o similari (salvo specifiche attività espressamente autorizzate per le finalità istituzionali).
   - Utilizzare sistemi Social Network quali twitter, facebook, etc., salvo specifiche attività espressamente autorizzate per le finalità istituzionali.
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (attenzione nell'aprire mail e relativi allegati, non navigare su siti poco professionali, ecc..)
3. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus, segnalando ogni eventuale problema all'amministratore di sistema.

Si ricorda poi che scaricare file audio e video (o comunque grandi quantità di dati) è in grado di degradare le prestazioni offerte dal servizio agli altri utenti: per tale motivo ciò può avvenire solo se necessario e, possibilmente, al di fuori dei momenti "di punta" a livello di Istituto.

Per garantire la sicurezza informatica ed il controllo del corretto utilizzo dell'accesso ad Internet l'istituto si è dotato di strumenti specifici che consentono:

- La protezione da accessi non autorizzati provenienti da Internet
- Controlli antivirus centralizzati
- configurazione di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (quali a titolo esemplificativo e non esaustivo: l'accesso ai siti inseriti in black list individuati dall'Istituto, il download di file o software aventi particolari caratteristiche dimensionali o di tipologia di dato), anche in modo differenziato per le diverse postazioni o tipologie di accesso;
- la determinazione di informazioni sulla navigazione Internet che consentono la conservazione di informazioni relative ad utente, PC, ora di accesso, pagine accedute, etc.

Si precisa che ulteriori tracce dell'operato di ciascun utente, lasciate sui PC, sui server e sui programmi impiegati, potranno essere utilizzate per l'individuazione e la sanzione di eventuali comportamenti anomali.
La conservazione nel tempo dei dati relativi all'uso degli strumenti informatici verrà fatta per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in adempimento di obblighi previsti dalla legge;

9. Disposizioni per il lavoro da remoto (telelavoro)

Il personale che svolge la propria attività in modalità di lavoro agile deve attenersi alle raccomandazioni elaborate da Cert-PA di AgID per il rispetto delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare 17 marzo 2017, n. 1 che devono essere garantite anche dal personale che svolge la propria attività lavorativa da remoto e riportate di seguito:

1. segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione;
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;
4. assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc.) siano abilitati e costantemente aggiornati;
5. assicurati che gli accessi al sistema operativo siano protetti da una password sicura di almeno 8 caratteri contenente almeno una lettera maiuscola, un numero ed un carattere speciale;
6. non installare software proveniente da fonti/repository non ufficiali;
7. blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro;
8. non cliccare su link o allegati contenuti in email sospette;
9. utilizza l'accesso a connessioni Wi-Fi adeguatamente protette;
10. collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione);
11. effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Si coglie l'occasione per dare le seguenti ulteriori disposizioni:

- Utilizza esclusivamente servizi cloud certificati dall'amministrazione (tramite nomina a responsabile del trattamento) per il trattamento dei dati personali di cui l'amministrazione è titolare;
- 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;
- non memorizzare sui dispositivi le password di accesso alle piattaforme ed ai sistemi utilizzati per il lavoro a distanza;
- non memorizzare sul client di posta elettronica le credenziali di accesso alle caselle istituzionali;
- 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);
- se utilizzi una connessione wi-fi, accertati di adottare una password sicura per il suo accesso (mai lasciare accessi liberi alla rete wi-fi).

10. Trattamenti esclusi

L'Istituto Scolastico non effettua controlli prolungati, costanti o indiscriminati dell'uso di Internet e Posta elettronica da parte dei dipendenti.
L'Istituto Scolastico non effettua trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori attraverso:

- lettura e registrazione sistematica dei messaggi di posta elettronica personali dei dipendenti o dei relativi dati esteriori;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;

11. Gradualità dei controlli

1. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con

preventivi accorgimenti tecnici, il Dirigente Scolastico può adottare eventuali misure che consentano la verifica di comportamenti anomali.

2. Per quanto possibile, sarà preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti d'Istituto e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
3. La presenza di successive anomalie potrà comportare controlli su base individuale.
4. La rilevazione delle anomalie e delle verifiche tecniche è a cura dell'Amministratore di Sistema che potrà anche intervenire su richiesta del Dirigente Scolastico per la verifica di situazioni anomale o sospette.
5. Responsabile dei successivi e consequenziali provvedimenti è il Dirigente Scolastico.

12. Sanzioni

1. È fatto obbligo a tutti i Lavoratori di osservare le disposizioni del presente disciplinare e qualunque altra comunicata dall'Amministrazione in materia di sicurezza e gestione delle attrezzature informatiche.
2. Il mancato rispetto o la violazione delle regole contenute nel presente Disciplinare è perseguibile con tutte le azioni civili e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni normative e contrattuali vigenti per il personale o per l'area dirigenza del comparto Regioni ed Autonomie Locali. Rimane ferma ogni ulteriore forma di responsabilità civile e penale, quali ad es.:
   - Violazioni di dati personali e della tutela dell'immagine;
   - diffamazione;
   - accesso abusivo ad un sistema informatico e telematico;
   - violazione della legge sul copyright.
3. Il codice di comportamento ed il codice disciplinare sono consultabili nel sito internet dell'Ente

13. Disposizioni ulteriori

1. I dati personali inerenti i Lavoratori non possono essere portati a conoscenza di terzi non autorizzati. I colleghi di lavoro della persona interessata sono considerati terzi.
2. L'Amministrazione, nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. 11 del presente Disciplinare e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del Lavoratore, procede alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet e/o della Posta Elettronica e/o dei files delle telefonate e/o dei Fax e dei Fax mail, fino alla conclusione dei relativi procedimenti.
3. Il presente documento viene portato a conoscenza di tutti i Lavoratori, indicati all'art. 1 del presente Disciplinare, mediante pubblicazione nei sito internet.

14. Aggiornamento periodico

Il presente regolamento è aggiornato con cadenza almeno annuale o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali dei lavoratori, e portato a conoscenza di tutti i lavoratori mediante affissione all'albo dell'istituto e pubblicazione nell'intranet istituzionale.

Raccomandazioni Sicurezza Posta Elettronica

Allo scopo di limitare l'occorrenza di incidenti di sicurezza sulla casella di Posta Elettronica si rappresentano le seguenti raccomandazioni:

1. non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle di posta non note;
2. non installare software sulla propria postazione, soprattutto se a seguito di sollecitazioni via e-mail che presentino link di accesso ad altre pagine o di esecuzionefile.
3. non dare seguito alle richieste di e-mail sospette;
4. nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, 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 richiedel'installazione abbia un fine specifico, se eventuali link nell'email puntino a siti conosciuti, se il mittente fosse noto e/o corretto;
5. di scansionare periodicamente per la ricerca di virus e malware le postazioni di lavoro ed i dispositivi con cui si accede alla Posta Elettronica Istituzionale;

nel caso di utilizzo del PC personale (telelavoro/smart working) si raccomanda di assicurarsi periodicamente:

6. che il sistema operativo della propria workstation sia aggiornato;
7. che la propria workstation sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;
8. che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale.
9. al momento della modifica delle password evitare di fare solo piccole modifiche come ad esempio numerazioni progressive ecc…;
10. di utilizzare gli strumenti messi a disposizione dalla Amministrazione come ad esempio il Cloud Storage Microsoft OneDrive per dati elaborati nell'ambito della sfera lavorativa.

Si consiglia inoltra di evitare di iscriversi a siti internet non riconducibili alla sfera lavorativa, ovvero utilizzando la casella di posta istituzionale; tali siti potrebbero infatti essere poco sicuri nella protezione dei dati personali, con eventuali ripercussioni in violazioni all'interno della propria operatività lavorativa.

Raccomandazioni e Indicazioni per la Sicurezza

Gentile Utente,
anche in questo ultimo periodo stiamo rilevando il blocco di mail di phishing indirizzate al personale ministeriale da parte dei sistemi di sicurezza del MI; 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 postazionedi lavoro e, a cascata, all'infrastruttura tecnologica del MI.

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 del account, la cui compromissione il più delle volte è dovuta ad infezionida virus sulle postazioni di lavoro o sui dispositivi utilizzati per l'accesso.

La causa delle suddette situazioni risiede sicuramente in un'intensa e sempre più sofisticata attività da parte dei cyber attaccanti in internet, interessati a carpire informazioni riservate e sensibili, personali e/o dell'Organizzazione, ma anche e soprattutto in comportamenti da parte delle persone non sempre in linea con le buone prassi di sicurezza e le indicazioni in tal senso da parte dell'Amministrazione.

Si ribadisce allo scopo quindi di:

- scansionare periodicamente per la ricerca virus le postazioni di lavoro ed i dispositivi utilizzati per lavoro;
- nel caso di utilizzo del PC 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, almomento 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;
- si raccomanda l'uso di supporti removibili quali chiavette usb e/o hard disk esterni ecc. con molta cautela. Al momento della connessione di un supporto removibile, si consiglia di avviare una scansione completa dello stesso attraverso il software antivirus.

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?*

Si ricorda inoltre che nell'area riservata intranet allo CSIRT MI (dopo il login, sezione: *Area Riservata > Computer Security Incident Response Team > Security Awareness*) sono

presenti i contenuti relativi a campagne malevole di phishing in corso ed aggiornamenti su nuovi virus che potrebbero infettare le postazioni di lavoro del personale della Pubblica Amministrazione.

È fortemente consigliata la lettura dei suddetti contenuti, allo scopo di tenersi aggiornati sui rischi informatici incombenti sull'Amministrazione e proteggere sia la propria operatività sia il patrimonio informativo del Ministero da possibili attacchi.

Raccomandazioni di Sicurezza per l'utente

Allo scopo di limitare l'occorrenza di incidenti di sicurezza si rappresentano le seguenti raccomandazioni.

- 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;
- nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, 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.

In caso di dubbi rispetto a quanto sopra rivolgersi sempre conferma airispettivi referenti informatici.

Grazie della collaborazione

CSIRT MI

IL DIRIGENTE SCOLASTICO
Dott.ssa Teresa Patrizia Paradiso
Firmato digitalmente

Il Responsabile della Protezione dei Dati (RPD) è il Dott. COSIMO RIZZO – Tel. 3337199525 –
PEC: cosimorizzo.dpo@pec.it
(PEC abilitata alla ricezione di mail anche da PEO)

il Titolare del trattamento è: l' ISTITUTO COMPRENSIVO infanzia-primaria-sec. 1° grado -Via Circonvallazione, 6 – Mozzanica (Bg) Tel: 0363 82109 - e-mail uffici: bgic85800C@istruzione.it-P.E.C.bgic85800c@pec.istruzione.it rappresentato dal Dirigente scolastico Dott.ssa Teresa Patrizia Paradiso