ISTITUTO COMPRENSIVO STATALE DI VIALE LIBERTA'
Scuole dell' Infanzia "C. Corsico" - "S. Maria delle Vigne"
Scuole Primarie "E. De Amicis" - " A. Botto"
Scuola Secondaria di Primo Grado "G. Robecchi"
Viale Libertà, 32 – 27029 Vigevano (PV) Tel. 0381/42464 - Fax 0381/42474
e-mail pvic83100r@istruzione.it - Pec: pvic83100r@pec.istruzione.it
Sito internet: www.icvialelibertavigevano.edu.it
Codice Fiscale 94034000185
Codice Meccanografico: PVIC83100R

Circ. n. 175 Vigevano, 06 febbraio 2023

Ai docenti
Agli assistenti amministrativi
Atti
Sito web

OGGETTO: Sicurezza delle reti e dei sistemi informatici – Istruzioni operative

Gentilissimi,
in considerazione anche delle recenti seppur frammentarie notizie relative alla *cybersicurezza* nazionale, concernenti problematiche che, in ogni caso, potrebbero riguardare indirettamente anche piccole PA cui non si applica la direttiva NIS sulla sicurezza delle reti e dei sistemi informatici (che invece trova piena applicazione nei confronti di fornitori di servizi essenziali, ad es., nel contesto dei trasporti e dell'energia e, per quanto potrebbe interessare in modo più immediato, a taluni fornitori di servizi digitali), ricordo l'opportunità di prestare **crescente attenzione alla prevenzione** di attacchi *ransomware* e di quanto, più in generale, potrebbe derivare da una non corretta gestione di email di *phishing* (buone pratiche sempre al centro delle attività formative svolte).
Si ricorda la necessità di prestare particolare attenzione alle mail di *phishing* ed agli attacchi *ransomware*, che potrebbero derivare anche da una non corretta gestione delle medesime.
A tal proposito, si invita alla lettura integrale delle pagine https://www.garanteprivacy.it/documents/10160/0/Phishing+attenzione+ai+pescatori+di+dati+personali.+Infografica.pdf/4786aabd-facb-4fe7-aecf-c529a4887253?version=5.0 e soprattutto https://www.garanteprivacy.it/temi/cybersecurity/ransomware, con preghiera di attenersi, nei trattamenti svolti in relazione alle mansioni lavorative di ciascuno e per quanto di rispettiva competenza, a quanto in esse indicato. In particolare e per immediatezza:
*"**La prima e più importante forma di difesa è la prudenza**. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.) e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ignora il contenuto.*
Anche se i messaggi provengono da soggetti a noi noti, è comunque bene adottare alcune piccole accortezze. Ad esempio:
- non aprire mai allegati con estensioni "strane" (ad esempio, allegati con estensione ".exe" sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);
- non scaricare software da siti sospetti (ad esempio, quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento);
[…]
- se si usa un pc, si può passare la freccia del mouse su eventuali link o banner pubblicitari ricevuti via e-mail o presenti su siti web senza aprirli (così, in basso nella finestra del browser, si può vedere

l'anteprima del link da aprire e verificare se corrisponde al link che si vede scritto nel messaggio: in caso non corrispondano, c'è ovviamente un rischio).
È inoltre utile:
• *installare su tutti i dispositivi un antivirus con estensioni anti-malware;*
• *mantenere costantemente aggiornati il sistema operativo oltre che i software e le app che vengono utilizzati più spesso […]".*
Inoltre, si raccomanda di prestare molta attenzione ai link indicati nei messaggi di posta (e/o in sms / messaggi sospetti, per chi utilizza dispositivi personali ad es. per quanto concerne il registro elettronico) e di NON aprirli nei casi in cui non sia possibile verificare la veridicità della fonte di provenienza.
Prestare particolare attenzione anche a non aprire allegati compressi (ad es. file con estensione .zip) se di dimensioni manifestamente modeste e tali da non giustificare il ricorso alla compressione, così come, più in generale, a non inserire mai le proprie credenziali in pagine web sospette.
Tali indicazioni sono applicabili anche ai casi di utilizzo di dispositivi informatici personali per lo svolgimento delle attività lavorative.
In caso di dubbio, anche in relazione ad una potenziale violazione dei dati, occorrerà attenersi a quanto sopra indicato e comunque informare tempestivamente la Dirigenza.

Il Responsabile della Protezione Dati,
Dott. Riccardo Colangelo

IL DIRIGENTE SCOLASTICO,
Dott.ssa Giovanna Montagna (*)

(*) Il documento è firmato digitalmente ai sensi del D.Lgs. 82/2005 s.m.i. e norme collegate e sostituisce il documento cartaceo e la firma autografa.