Unione Europea
F.S.E
F.E.S.R.
P.O.N.

Istituto Comprensivo
"Santomasi Scacchi"

Corso Aldo Moro, 51 – 70024 Gravina in Puglia (BA)
Tel./Fax. 080.3267691
Cod. Mecc. BAIC811006 - Cod. Fisc. 82014400723
baic811006@istruzione.it - baic811006@pec.istruzione.it
www.icsantomasiscacchi.edu.it

Ministero dell'Istruzione
dell'Università
e della Ricerca

Gravina in Puglia, (Vedi protocollo)

Al DSGA pro-tempore
Agli Assistenti Amministrativi

Notifica Digitale (mail istituzionale)

E, p.c. Al DPO avv. Parisi Nicola
parisi@actioavvocati.it

***OGGETTO**: Smart working in relazione all'emergenza da COVID-19 – misure di sicurezza e protezione dei dati da adottare.*

Con l'attivazione del lavoro agile per tutto il personale, nelle more dell'emergenza COVID-19, fatti salvi eventuali successivi adeguamenti alle disposizioni nazionali e regionali, si ritiene dunque utile portare a conoscenza del personale che si avvale di tale modalità operativa in ambiente domestico alcuni aspetti inerenti alla sicurezza informatica delle proprie postazioni di lavoro. Fermo restando comunque l'obbligo di non divulgazione e di massima riservatezza riguardo ai dati personali e, in generale, alle informazioni trattate nella propria attività lavorativa, nel caso in cui tale attività venga svolta mediante dispositivi personali, si rammenta di:

- *Utilizzare i propri dispositivi in modo consono e adeguato, secondo criteri di diligenza professionale rispetto alla carica ricoperta o alla funzione/mansione svolta;*
- *Adibire tali dispositivi ad esclusivo uso lavorativo e personale evitando l'utilizzo condiviso con familiari e/o conviventi; se si dispone di un solo pc usato anche da altri famigliari, creare un account specifico per l'uso nei momenti di lavoro;*
- *Mantenere aggiornate le componenti software presenti sui dispositivi alle versioni più aggiornate;*
- *Installare e aggiornare l'antivirus e/o il firewall al fine di proteggere i dispositivi da attacchi malware e scongiurare eventuali data breach; effettuare una scansione completa dei dispositivi;*
- *Proteggere i dispositivi con password che devono essere di esclusiva conoscenza del dipendente e che non devono essere semplici da indovinare (es. date di nascita, nomi, etc.);*
- *Non salvare sul PC le password di accesso agli applicativi di lavoro;*
- *Nel caso ci si allontani dal PC durante il lavoro, bloccare il pc in modo che non sia utilizzabile da altri famigliari o conviventi;*
- *Settare un livello di protezione alto per le impostazioni privacy del browser e delle applicazioni utilizzate;*
- *Evitare la navigazione su siti web che possano compromettere la riservatezza dei dati e delle informazioni in essi contenute;*
- *Utilizzare gli strumenti per il lavoro agile messi a disposizione dall'Istituto;*
- *Connettere i propri dispositivi a reti sicure e protette da password;*
- *Evitare sui dispositivi utilizzati per il lavoro, l'accesso a social network o altre applicazioni facilmente hackerabili;*

- *Non stampare documenti se non nei casi in cui sia strettamente necessario e distruggere le stampe non appena la necessità sia conclusa;*
- *Non salvare documenti di ufficio sul PC personale se non temporaneamente e poi cancellarli immediatamente (specie se contengono informazioni personali).*

Si richiama inoltre l'attenzione del personale sui fenomeni di **phishing** inviati a mezzo mail o mediante siti web creati ad hoc per indurre le vittime a rivelare informazioni riservate o a scaricare malware sui propri dispositivi. Infatti in questo periodo si riscontra un aumento delle mail di phishing spesso legate a informazioni sull'emergenza da COVID-19, e inviate spesso da enti (o presumibilmente da essi) del Servizio Sanitario Nazionale o Regionale.
Si forniscono di seguito alcuni consigli per scongiurare tali attacchi informatici:

1. *Verificare con attenzione l'indirizzo del mittente: a volte l'indirizzo proviene da un sito non istituzionale o che SOMIGLIA a quello istituzionale (ad esempio può contenere piccoli errori nell'indirizzo). In molti casi i criminali informatici utilizzano indirizzi mail pubblici (es. @gmail.com) anziché quelli del dominio dell'ente mittente. In caso dubbio, prima di aprire la mail, e soprattutto gli allegati, si raccomanda di contattare direttamente il mittente (non rispondendo alla stessa mail!) e chiedere informazioni sulla mail ricevuta.*
2. *Non aprire le mail che provengono da mittenti sconosciuti e che invitano ad aprire l'allegato in esse presenti. Spesso tali mail conducono malware o, ancora peggio, ransomware che bloccano il dispositivo.*
3. *A volte le mail di phishing invitano a cliccare su un link nel testo della mail stessa (ad esempio può essere un link che richiama un sito istituzionale). Per visualizzare il vero indirizzo a cui tale link riporta, è sufficiente spostare il mouse sul link SENZA CLICCARLO e apparirà il link reale. In una mail di phishing tale link sarà un link sconosciuto e non quello indicato nella descrizione.*
4. *Controllare il modo in cui è scritta la mail, anche se proveniente da una persona che conosciamo. Spesso le mail di phishing contengono errori grammaticali ed ortografici. Anche lo stile di scrittura potrebbe essere diverso da quello che normalmente ci si aspetta dal mittente. Anche in questi casi è buona norma contattare direttamente il mittente e chiedere spiegazioni.*

Tanto per doverosa comunicazione.

Il Dirigente
Prof.ssa Rosa De Leo