Istituto di Istruzione Superiore "Segato"
Via Jacopo Tasso, 11 – 32100 Belluno - C.F. 80001970252
Sez. ITIS "Segato" Tel. 0437 940159 – Fax 0437 940973
Sez. IPSIA "Brustolon" Tel. 0437 950033 – Fax 0437 950177
Sito: www.segatobrustolon.edu.it
E-mail: blis011002@istruzione.it blis011002@pec.istruzione.it

COMUNICATO N. 334

- **Ai docenti**
- **Al personale ATA**
- **Agli studenti**

Oggetto: Sicurezza informatica. Comunicazione da CERT-PA

Il CERT-PA (Computer Emergency Response Team – Pubblica Amministrazione), che opera all'interno di AgID (Agenzia per l'Italia Digitale), ha il compito di supportare le pubbliche amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica.
Si segnalano diverse tipologie di nuove minacce informatiche in essere in questi giorni.

1) Nuova campagna di malspam volta a veicolare il malware Ursnif.
   (https://www.cert-pa.it/notizie/campanga-malspam-ursnif-veicolata-in-italia-sfrutta-emergenza-coronavirus/)
2) Nuove campagne di diffusione di malware sfruttano il crescente uso delle piattaforme come ZOOM e TEAMS.
   (https://www.cert-pa.it/notizie/la-piattaforma-zoom-sfruttata-per-veicolare-malware/)
3) Falsi aggiornamenti di Google Chrome.
   (https://www.cert-pa.it/notizie/campagna-malware-utilizza-falso-aggiornamento-google-chrome/)
4) Campagne di phishing.
   (https://www.cert-pa.it/notizie/campagne-di-phishing-ai-danni-di-utenti-di-supermercati-e-corrieri/)

Raccomandazioni

- Si raccomanda di non dare seguito all'apertura di file non attesi dalla dubbia provenienza o che giungono da caselle non note.
- Non installate software soprattutto se a seguito di sollecitazioni via e-mail. Non date seguito alle richieste di e-mail sospette.
- Nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, verificate 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? In caso di dubbio chiedete conferma ai vostri referenti.

Raccomandazioni per il proprio PC usato in telelavoro

- Tenere aggiornato il sistema operativo del proprio PC.
- Assicurarsi che il proprio PC sia dotato di antivirus e che questo sia aggiornato.
- Assicurarsi che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale. Al momento della modifica delle password evitare di fare solo piccole modifiche come ad esempio numerazioni progressive ecc…
- Eseguire il backup periodico dei dati elaborati sul proprio PC nell'ambito della sfera lavorativa.

Belluno, 2 aprile 2020

Il dirigente scolastico
F.to Prof.ssa Ilaria Chiarusi