

- **Oggetto:** MIUR - Sicurezza Informatica - Accorgimenti per il Telelavoro e attenzione a campagne che sfruttano l'emergenza CODIV-19
- **Data ricezione email:** 18/03/2020 15:30
- **Mittenti:** Alert Fatturazione Elettronica - Gest. doc. - Email: noreply@istruzione.it
- **Indirizzi nel campo email 'A':** <noreply@istruzione.it>
- **Indirizzi nel campo email 'CC':**
- **Indirizzo nel campo 'Rispondi A':** <noreply@istruzione.it>

Testo email

Gentile utente,

il CERT-PA ci mette in guardia da e-mail e PEC che circolano in questi giorni e che, facendo leva sull'emergenza [COVID-19](#), promuovono prodotti dalle dubbie funzionalità da utilizzare in regime di telelavoro.

In alcuni casi si tratta di veri e propri malware molto dannosi il cui intento è quello di raccogliere in maniera fraudolenta dati e password degli utenti.

Soprattutto in questo momento, la necessità del telelavoro ci espone ad una maggiore responsabilità per la sicurezza del nostro computer di casa.

Dobbiamo evitare di incorrere in errori che potrebbero mettere a repentaglio la sicurezza dei dati e dei servizi dell'Amministrazione.

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. 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.

Raccomandiamo inoltre di assicurarsi:

- 1) che il sistema operativo del proprio PC sia aggiornato
- 2) che il proprio PC sia dotato di antivirus e che questo sia aggiornato
- 3) 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

4) di eseguire il backup periodico dei dati elaborati sul proprio PC nell'ambito della sfera lavorativa.

E' possibile trovare ulteriori informazioni ai seguenti indirizzi:

<https://www.cert-pa.it/notizie/coronavirus-attenzione-agli-sciacalli/>

<https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/17/smart-working-vademecum-lavorare-online-sicurezza>

Grazie per la collaborazione

Ministero dell'Istruzione, dell'Università e della Ricerca

D.G. Contratti, Acquisti, Sistemi Informativi e Statistica