- **Oggetto:** CSIRT MI - Raccomandazioni e Indicazioni per la Sicurezza rispetto a Campagna Phishing
- **Data ricezione email:** 21/10/2021 13:25
- **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,

si segnala che da attività di monitoraggio dello CSIRT MI, si è analizzata una campagna phishing globale che è stata puntualmente bloccata dai sistemi di sicurezza perimetrali in uso.
Qualora si dovessero ricevere mail sospette e/o appartenenti a conversazioni passate, che non sono state intercettate dai sistemi di sicurezza, si raccomanda di:
• verificare sempre il mittente della comunicazione;
• non aprire eventuali file allegati sospetti;
• non cliccare su link presenti nel corpo della mail.

Si raccomanda pertanto di seguire sempre in modo scrupoloso le politiche di sicurezza e le indicazioni ministeriali per la sicurezza informatica e per l'utilizzo consapevole degli asset di lavoro, in particolare prestando sempre la massima attenzione a possibili messaggi mail malevoli ed ad eseguire regolarmente scansioni antivirus delle proprie postazioni di lavoro.

Per approfondimenti sulla sopra citata minaccia informatica si consiglia la visualizzazione del video tutorial "Il Phishing" sull'area intranet:
https://iam.pubblica.istruzione.it/iam-areariservata-web/contenuto/pagina/video-tutorial

Grazie per la collaborazione.

CSIRT MI