

27.08.2026

Spesso la più grande falla nella sicurezza è l'essere umano

Oggi i criminali informatici ricorrono sempre più a stratagemmi psicologici per ottenere informazioni riservate. Invece di sfruttare le vulnerabilità tecniche, manipolano le persone in modo mirato tramite e-mail, telefonate o messaggi falsi.

Con storie avvincenti e pressioni psicologiche, i truffatori di Internet inducono le loro vittime a rivelare password, fare clic su link dannosi o condividere dati sensibili. Questa forma di attacco manipolativo è nota come social engineering.

I metodi utilizzati si fanno sempre più raffinati. Grazie all'intelligenza artificiale, i messaggi e le telefonate sembrano più autentici che mai, e si moltiplicano anche i casi di voci, foto, video e identità contraffatte.

La sensibilizzazione e una sana dose di sfiducia sono fondamentali per riconoscere tempestivamente gli attacchi di social engineering e reagire correttamente.

Volete saperne di più sui metodi di attacco più in uso e sulle misure di sicurezza? Allora seguite il nostro webinar «Social engineering – riconoscere le truffe e agire in modo sicuro». Il nostro personale esperto vi mostrerà con esempi pratici come potete proteggere efficacemente voi stessi, i vostri dati e il vostro patrimonio dai più arditi tentativi di frode:

- **Martedì 20 ottobre, ore 13:00** (<https://events.teams.microsoft.com/event/1071392a-6e09-4c1a-bcea-13e520e64d77@75a34008-d7d1-4924-8e78-31fea86f6e68>)
- **Mercoledì 21 ottobre, ore 19:00** (<https://events.teams.microsoft.com/event/545297b9-ae92-45bc-ac13-5238eaa06794@75a34008-d7d1-4924-8e78-31fea86f6e68>)

Iscrivetevi subito e consolidate le vostre competenze in materia di sicurezza!