Finanziato dall'Unione europea NextGenerationEU

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

ARPAC CAMPANIA

Cybersecurity & Data Protection

Newsletter mensile: Settembre 2025

Questo mese parliamo di...

SOCIAL MEDIA: USO SICURO

I **social media**, pur essendo utili strumenti di comunicazione, possono **esporre l'Agenzia a rischi** significativi. In questa newsletter, esploreremo le principali minacce digitali a cui i dipendenti dell'Agenzia possono essere esposti sui social e i comportamenti da adottare per ridurre tali rischi.

PRINCIPALI RISCHI

CONDIVISIONI RISCHIOSE

Anche una semplice foto della postazione di lavoro può rivelare **dettagli sensibili** sull'Agenzia, come documenti visibili sulla scrivania o informazioni riservate condivise in post pubblici. Questi contenuti, se diffusi online, possono compromettere la **sicurezza** e la **riservatezza** delle attività istituzionali.

SOCIAL ENGINEERING

Comprende tecniche di manipolazione psicologica usate dai criminali per **ottenere informazioni sensibili fingendosi colleghi, fornitori o enti istituzionali**. Induce la vittima a rivelare dati riservati, aprire link dannosi o compiere azioni che possono compromettere la sicurezza Agenziale. I rischi includono installazione di malware, sottrazione/ alterazione di dati su sopralluoghi e ispezioni, esiti analitici e segnalazioni, furto di credenziali, piani di emergenza e dati personali.

ATTENZIONE A COSA PUBBLICHI

Evita di condividere immagini o testi che mostrino **ambienti di lavoro**, documenti, schermi o riferimenti a progetti riservati. Prima di pubblicare, chiediti sempre se il contenuto potrebbe esporre l'Agenzia a **rischi di sicurezza o violazioni di privacy**.

MANTIENI UN PENSIERO CRITICO

Per difendersi è importante mantenere un **atteggiamento vigile**, soprattutto di fronte a **richieste inusuali**, **urgenti** o provenienti da contatti poco noti. Non accettare collegamenti a cuor leggero e non fornire mai **password** o **codici** tramite chat o messaggi. In caso di dubbio, **verifica sempre l'identità** attraverso un canale ufficiale e sicuro.

COME DIFENDERSI

STAI DAVVERO USANDO I SOCIAL MEDIA IN MODO SICURO?

- Non accettare richieste di collegamento da profili sospetti o sconosciuti;
- Non condividere dettagli sulle attività aziendali, progetti o colleghi senza autorizzazione;
- Attenzione ai messaggi o commenti che potrebbero essere usati per raccogliere informazioni personali o aziendali;
- Non cliccare su link non verificati ricevuti tramite social o messaggistica;
- Ricorda che anche un post apparentemente innocuo può compromettere la sicurezza o la reputazione dell'Agenzia.

Proteggi ARPAC: segui la Politica di utilizzo sicuro degli asset e delle informazioni aziendali