



## Città di Reggio Calabria

U.P.I. COMUNICAZIONE, PARTECIPAZIONE,  
TRANSIZIONE DIGITALE E QUALITÀ DEI  
PROCESSI E SERVIZI FONDI SIE E PNRR - PON  
METRO E POC METRO



Via Michele Barillaro s.n.c.  
Palazzo CE.DIR. Corpo I  
Reggio Calabria



0965 3622621



E-Mail: [protocollo@pec.reggiocal.it](mailto:protocollo@pec.reggiocal.it)

Ai dipendenti del Comune di Reggio Calabria

**Oggetto:** Progetto “ReggioCyber” -PNRR M1C1 Investimento 1.5 “Cybersecurity. Attivazione percorso formativo per i dipendenti dal 31 luglio p.v. al 30 settembre p.v

Nell’ambito del progetto in oggetto, di cui questa UPI è soggetto attuatore, attraverso la piattaforma di e-learning Cyber Guru è stato avviato un percorso formativo e di addestramento dedicato al tema della Cyber Security Awareness che consentirà a ciascun dipendente dell’Ente di essere custode dei dati che vengono trattati ogni giorno e, quindi, di proteggere se stesso e l’organizzazione dai possibili attacchi informatici.

La suddetta formazione, in modalità e-learning ed asincrona, è fruibile dal 31 luglio p.v. e sino al 30 settembre p.v. Essa è articolata in 12 moduli formativi, 36 lezioni, ciascuno dei quali è dedicato ad uno specifico argomento.

Considerato che il metodo di fruizione è sequenziale, per accedere dal 2° al 12° modulo è necessario, quindi, completare il modulo precedente previo superamento del relativo test di apprendimento costituito da 4 domande a risposta multipla. Il test è superato rispondendo correttamente ad almeno 3 domande e, ove necessario, può essere ripetuto, ancorché venga registrato il punteggio ottenuto al primo tentativo.

Ciascun modulo è formato da 3 brevi lezioni, ognuno dei quali è costituito da un video di circa 15 minuti che, in ausilio, si completa con un documento contenente la riassunta trascrizione dei medesimi contenuti.

Le 3 lezioni costituenti ciascuno dei 12 moduli formativi, sono così organizzate:

- La prima lezione è quella della conoscenza di base per fornire gli elementi cognitivi che consentono la comprensione del rischio;
- La seconda lezione è quella dell’approfondimento per stimolare la “prontezza”, creando le condizioni per riconoscere le minacce anche quando queste si presentano in forma insolita e/o sofisticata;
- La terza lezione è quella delle best practice per acquisire le “buone pratiche” di comportamento, stimolando la “reattività” e, quindi, la capacità di agire in modo consapevole.

Ogni dipendente riceverà sul proprio indirizzo email istituzionale una comunicazione dalla piattaforma di e-learning Cyber Guru Awareness, con la quale saranno trasmesse individualmente le relative credenziali di accesso.

La fruizione della formazione è monitorata sia con riguardo agli accessi sia con riferimento ai relativi avanzamenti.

È garantito un servizio di supporto con casella di posta dedicata [supporto@cyberguru.it](mailto:supporto@cyberguru.it).

La presente informativa è pubblicata nella sezione "House Organ" del sito web istituzionale.

Il Dirigente  
Giuseppe Quartuccio