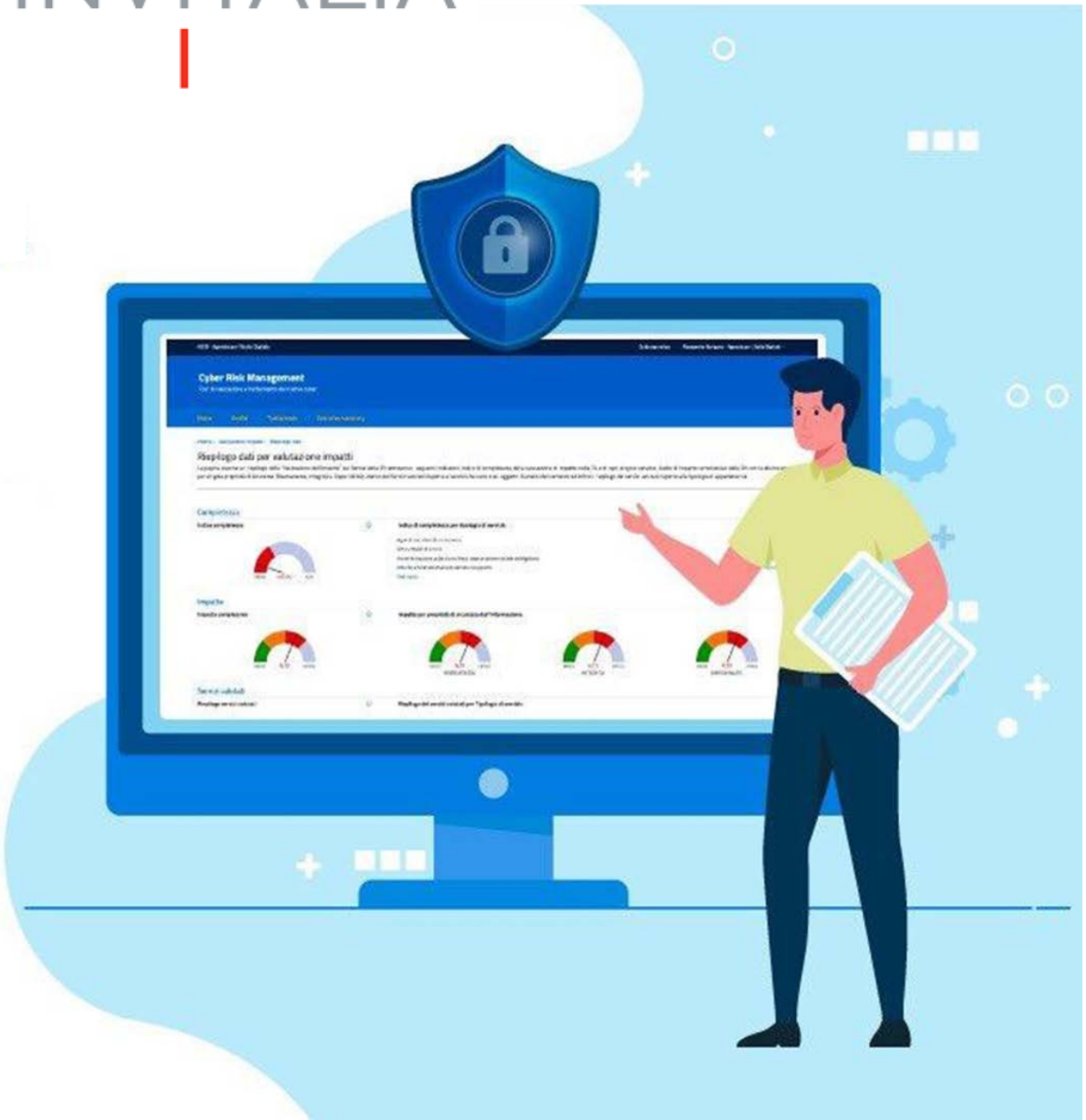
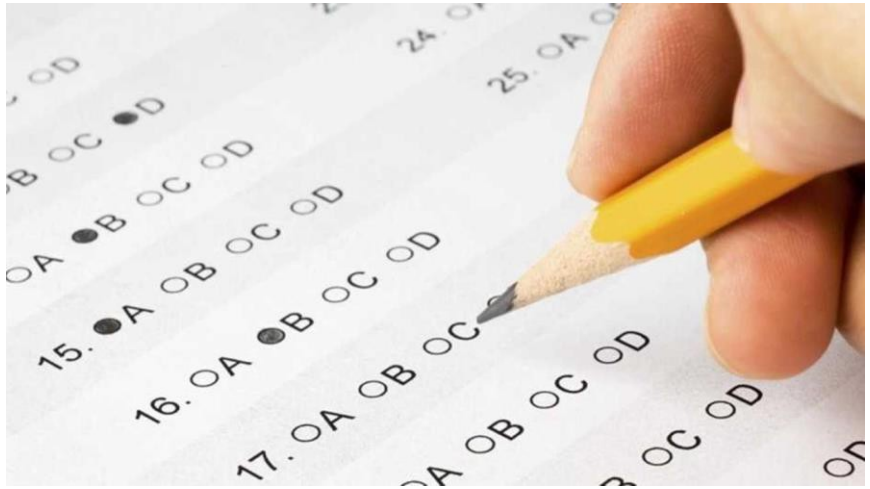
FORMAT S.R.L.
CENTRO STUDI RICERCHE E FORMAZIONE

INVITALIA

Proposta per il programma di
Cybersecurity Awareness



La proposta si articola in 5 steps:



1) verifica livello «*cybersecurity awareness*»:

- Test d'ingresso (test a risposte multiple);
- Campagna di phishing

2) Formazione asincrona, in modalità e-learning

Erogazione di uno o più video (da concordare) della durata di 2 ore che ha come obiettivo la «cybersecurity awareness», il programma, in accordo con il test di ingresso, potrebbe essere articolato come segue:

- Introduzione
- Definizioni (es: *informazione, sicurezza informatica, cybersecurity, attacco informatico, minaccia, rischio, etc.*)
- Perché si viene attaccati
- Dove si viene attaccati (*dati, servizi, piattaforme, infrastrutture, persone*)
- Chi viene attaccato
- Come si viene attaccati (*elenco dei principali metodi di attacco soffermandosi in particolare sul* ***Social Engineering***)

3) Formazione in video

2 ore con un docente che, approfondisce i temi legati alla sicurezza in ambito Smart Working e, in base al livello del gruppo, modula la lezione fornendo le best practices di riferimento.

Di seguito il programma:

- Rischi dello Smart Working
- Modelli di minaccia e modalità di attacco
- Contromisure per mitigare i rischi
- Esempi di attacchi e contromisure
- Best Practices

4) **Test finale**
5) **Review dei risultati e definizione di nuove azioni alla luce del *Piano Triennale* per le PA 2020-2022**