UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

"Supporto all'operatività della riforma in materia di semplificazione"
CUP J59J16000760006

Webinar 21 luglio 2020

Una lezione dal Covid-19: resilienza, intelligenza collettiva e tecnologie nelle nuove azioni formative a distanza

Risposte alle domande poste in chat

a cura di
Luca Diracca, Giacomo Re, Lamberto Savino

FormezPA

Domande & Risposte

1. Pensate che questo tipo di formazione è possibile mantenerla a distanza anche dopo questo periodo di resilienza, quindi di adattabilità?

Il patrimonio d'esperienza non sarà sicuramente buttato, anzi, riteniamo che molti partecipanti chiederanno ancora attività formative a distanza anche di fronte alla possibilità di svolgerle in presenza.

La formazione a distanza presente diversi punti di forza (azzera gli spostamenti fisici, permette maggiore flessibilità, …) ma anche diversi punti di debolezza (problemi di connessione, difficoltà nelle interazioni, …), esattamente come la formazione in presenza (seppure in maniera diversa).

Sarà fondamentale quindi trovare il giusto mix e la corretta alternanza fra questi strumenti cercando di utilizzare la modalità più consona al tipo di attività che proponiamo e al pubblico con cui ci confrontiamo. La parola d'ordine sarà "equilibrio", per minimizzare i limiti di queste due modalità ed esaltarne invece tutti gli aspetti positivi.

2. Prima che si concluda il webinar vorrei dire a tutti grazie mi avete aiutato attraverso la narrazione e la vostra esperienza a far ordine nei miei pensieri, si capisce molto chiaramente che il progetto incontra le persone. vorrei capire se il manuale come essere splendidi nella formazione on - line può essere disponibile per imparare. grazie molte.

Sì, il manuale sarà disponibile fra i materiali del corso.

3. L'utente come si può accorgere dei furti dati o intromissioni non autorizzate nella rete/piattaforme?

Purtroppo non è facile rispondere perché dipende moltissimo dal tipo di attacco portato. Possono esserci (elenco non esaustivo):

1. Una persona che riesce ad "intrufolarsi" nei meeting (e quindi lo si vede apparire, accendere telecamera e microfono, dire improperi, condividere immagini o video "poco opportuni" e in sintesi disturbare lo svolgimento dell'incontro)
2. Una persona che riesce ad intercettare lo streaming video e/o la registrazione e vedere il webinar anche se non autorizzato (e questo è invisibile in generale a noi e può essere scoperto solo da chi produce e gestisce la piattaforma: Microsoft, Alphabet, Zoom etc)
3. Una vera e propria installazione di malware sul pc (qui gli strumenti antivirus sono quelli in grado di avvertirci e/o impedire che avvenga – fondamentale la prevenzione con strumenti antivirus adeguati e con l'aggiornamento costante della applicazione di videoconferenza utilizzata)
4. Un "furto di credenziali" (di cui è molto difficile accorgersi e per questo è fondamentale cambiare spesso le proprie password e soprattutto non utilizzare la stessa password per sistemi diversi: se mi rubano le credenziali di zoom il problema può essere limitato a patto che

la stessa password non la possano usare per accedere alla mia posta elettronica o al conto corrente…).

Va notato però che malware e furto di credenziali (3. e 4.) in genere sono possibili solo da persone che partecipano al nostro stesso incontro (che per esempio possono mandarci una “emoticon con sorpresa” sulla chat) e quindi nei corsi chiusi il rischio è molto ridotto.