Tematiche e Soluzioni Metodologiche Trattate nelle Attività di Formazione

Il corso "Educare alla Sicurezza Informatica: comprendere le minacce online e apprendere come difendersi" ha coperto diverse tematiche cruciali, accompagnate da soluzioni metodologiche pratiche per garantire una formazione efficace e applicabile. Di seguito una descrizione delle principali tematiche trattate e delle metodologie adottate:

1. Rischi e Minacce Informatiche in Rete:

Introduzione alle varie tipologie di minacce informatiche, tra cui malware, phishing, ransomware, e altre tecniche di attacco.

Soluzioni Metodologiche:

Lezioni Teoriche: Presentazioni dettagliate e casi studio reali per illustrare le diverse minacce.

Simulazioni Pratiche: Esercitazioni che replicano scenari di attacco in un ambiente controllato per aiutare i partecipanti a riconoscere e rispondere a questi attacchi.

2. Soluzioni e Buone Pratiche:

Discussione delle principali soluzioni di sicurezza informatica e delle buone pratiche da adottare quotidianamente per proteggersi online.

Soluzioni Metodologiche:

Workshop Interattivi: Laboratori pratici per imparare a utilizzare strumenti di sicurezza come antivirus, firewall, software di crittografia e sistemi di autenticazione a due fattori.

Esercitazioni Pratiche: Attività hands-on per installare e configurare questi strumenti, gestendo le impostazioni di sicurezza sui dispositivi.

Metodologie Didattiche Applicate

Lezioni Frontali: Fornire una base teorica solida sulle minacce informatiche e le tecniche di difesa.

Casi Studio: Analisi di esempi concreti di attacchi informatici per comprendere le strategie dei cybercriminali.

Simulazioni: Riproduzione di scenari di attacco per esercitare il riconoscimento e la reazione a minacce in tempo reale.

Laboratori Pratici: Sessioni interattive per l'installazione, configurazione e gestione degli strumenti di sicurezza.