**Scheda formativa**

|  |  |
| --- | --- |
| Titolo  | Cybersecurity e protezione dei dati per gli operatori dell'IFP |
| Rif. DigCompEdu  | Area 6: Facilitare le competenze digitali degli studenti |
| Parole chiave (meta tag) | Cybersecurity, crimine informatico, antivirus, protezione dei dati, phishing, spam, Internet |
| Lingua | Italiano |
| Obiettivi / Finalità / Risultati di apprendimento | * Conoscere i pericoli di Internet.
* Imparare a navigare in modo sicuro e ad evitare la criminalità informatica.
* Proteggere i nostri dati da potenziali attacchi informatici.
* Capire gli antivirus: criteri, tipi e opzioni gratuite.
 |
| Descrizione | Il mondo online offre un numero incommensurabile di risorse e informazioni che possono aiutarci sia nell'apprendimento sia nella vita quotidiana. Tuttavia, presenta anche diversi pericoli che possono compromettere la nostra sicurezza. In questo corso imparerete come identificare queste minacce informatiche e come evitarle, proteggendo la vostra identità e garantendo la vostra sicurezza su Internet. |
| Contenuti organizzati su 2 livelli: | **Cybersecurity e protezione dei dati per gli operatori dell'IFP****1. La sicurezza informatica**1.1. Cos'è la cybersecurity1.2. I pericoli di Internet 1.3. Consigli per stare al sicuro online**2. La protezione dei dati**2.1 Cos'è la protezione dei dati?2.2 Consigli per la protezione dei dati2.3 Come scegliere un antivirus. |
| Autovalutazione (domande e risposte a scelta multipla) | **1. Quale tra questi è un crimine informatico?**a. VPNb. Avirac. Phishing**2. Cosa bisogna considerare quando si cerca un antivirus?**a. Compatibilità b. Affidabilitàc. Entrambi**3. Che cosa si deve fare se si riceve un link da un mittente sconosciuto?**a. Aprirlo e verificare di cosa si trattab. Non aprirlo e segnalare il messaggioc. Riportare un altro link**4. Come possiamo proteggere i nostri dati?**a. Pubblicando frequentemente contenutib. Inviando mail con le nostre informazioni ai nostri conoscenti c. Mantenendo il software aggiornato**5. Cosa deve includere una password sicura?**a. Informazioni sull'utenteb. Maiuscole, minuscole, numeri e caratteri specialic. Parole credibili |
| Toolkit (linee guida, buone pratiche, liste di controllo, lezioni apprese…) | Nome  | Cheklist Cybersecurity  |
| Descrizione | Una lista di controllo progettata per garantire la sicurezza digitale della vostra azienda da potenziali attacchi e minacce informatiche. |
| Nome File |  |
| Risorse (video, link di riferimento)  |  |
| Material correlato |  |
| PPT correlato |  |
| Bibliografia | <https://www.incibe.es/protege-tu-empresa/blog/el-ataque-del-man-middle-empresa-riesgos-y-formas-evitarlo> <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security> <https://www.ncsc.gov.uk/section/board-toolkit/home> <https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices> <https://blog.malwarebytes.com/cybercrime/2018/08/under-the-hoodie-why-money-power-and-ego-drive-hackers-to-cybercrime/> <https://protecciondatos-lopd.com/empresas/suplantacion-de-identidad/>  |
| Fornito da  | Internet Web Solutions |