**Schulungsunterlagen**

|  |  |  |
| --- | --- | --- |
| Titel | Cybersicherheit und Datenschutz für Berufsbildungsbetreiber | |
| Ref. DigCompEdu | Bereich 6: Förderung der digitalen Kompetenz der Lernenden | |
| Schlüsselwörter (Meta-Tag) | Cybersicherheit, Cyberkriminalität, Virenschutz, Datenschutz, Phishing, Spam, Internet | |
| Sprache | Deutsch | |
| Ziele / Zweck / Lernergebnisse | * Um die Gefahren des Internets zu kennen. * Um zu lernen, wie man sicher surft und Cyberkriminalität vermeidet. * Um unsere Daten vor potenziellen Cyberangriffen zu schützen. * Antivirus verstehen: Kriterien, Typen und kostenlose Optionen. | |
| Beschreibung | Die Online-Welt bietet eine unermessliche Anzahl von Ressourcen und Informationen, die uns sowohl beim Lernen als auch in unserem täglichen Leben helfen können. Dennoch birgt es auch verschiedene Gefahren, die unsere Sicherheit gefährden können. In diesem Kurs lernen Sie, wie Sie diese Cyberbedrohungen erkennen und vermeiden können, um Ihre Identität zu schützen und Ihre Sicherheit im Internet zu gewährleisten. | |
| Inhalte in 3 Ebenen angeordnet | **Cybersicherheit und Datenschutz für Berufsbildungsbetreiber**   1. **Cybersicherheit**    1. Was ist Cybersicherheit    2. Gefahren im Internet    3. Tipps, um online sicher zu bleiben 2. **Datenschutz**    1. Was ist Datenschutz?    2. Tipps zum Datenschutz    3. Erfahren Sie, wie Sie ein Antivirenprogramm auswählen. | |
| Selbsteinschätzung (Multiple-Choice-Abfragen und -Antworten) | 1. Was ist eine Cyberkriminalität? 2. VPN 3. Avira 4. **Phishing** 5. Was sollten wir bei der Suche nach einem Antivirenprogramm beachten? 6. Kompatibilität 7. Zuverlässigkeit 8. **Beides ist richtig** 9. Was sollen wir tun, wenn wir einen Link von einem unbekannten Absender erhalten? 10. Öffnen Sie es und überprüfen Sie, was es ist 11. **Öffnen Sie es nicht und melden Sie die Nachricht** 12. Einen weiteren Link zurückgeben 13. Wie können wir unsere Daten schützen? 14. Häufiges Veröffentlichen von Inhalten 15. Versenden von E-Mails mit unseren Informationen an unsere Bekannten 16. **Die Software auf dem neuesten Stand halten** 17. Was sollte ein sicheres Passwort beinhalten? 18. Benutzerinformationen 19. **Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen** 20. Glaubwürdige Worte | |
| Toolkit (Leitfäden, Best Practices, Checkliste, Lessons Learned... ) | Name | Cybersicherheits-Checkliste |
| Beschreibung | Eine Checkliste, die entwickelt wurde, um die digitale Sicherheit Ihres Unternehmens vor potenziellen Cyberangriffen und Bedrohungen zu gewährleisten. |
| Dateiname |  |
| Ressourcen (Videos, Referenzlink) |  | |
| Zugehöriges Material |  | |
| Zugehörige PPT |  | |
| Bibliographie | <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/> | |
| Bereitgestellt von | Internet Web Solutions | |