RestartVET

RESTART VET:

An innovative approach to support VET teachers/trainers through the digital transformation of VET education

Digital Security (Italian)

Co-funded by the Erasmus+ Programme of the European Union

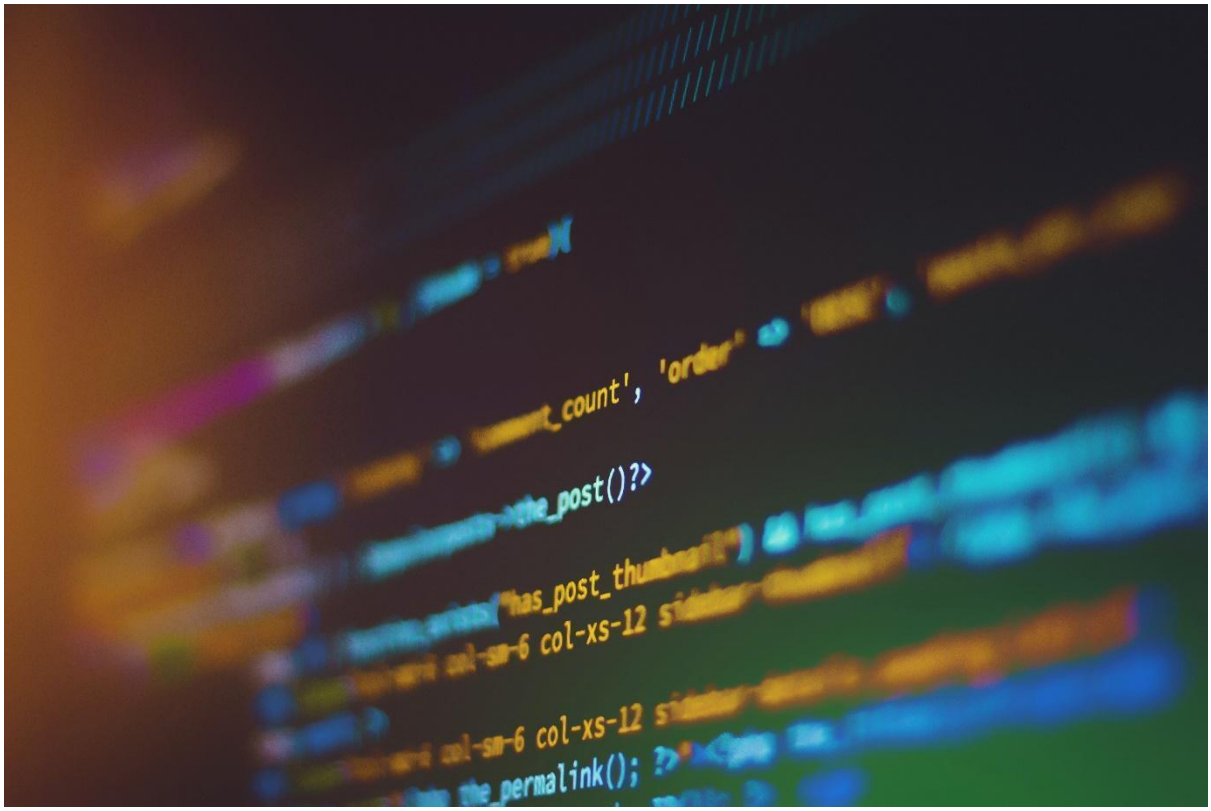
Sicurezza digitale

Introduzione:

Alcuni degli aspetti più comuni della nostra quotidianità sarebbero sembrati fantascienza solo un paio di decenni fa! L'uso di dispositivi mobili per quasi tutte le nostre esigenze tecnologiche, la velocità e la portata di internet, la ricchezza di applicazioni e soluzioni IT, hanno rimodellato la nostra esperienza quotidiana, il commercio, l'istruzione, l'intrattenimento, la ricerca e persino la nostra vita interpersonale.

Si stima che ci siano attualmente 4,66 miliardi di utenti attivi di Internet nel mondo su 7,83 miliardi di popolazione globale, il che significa che il 92,6% delle persone sul pianeta ha accesso al World Wide Web attraverso una varietà di dispositivi. Oltre a ciò, il 56,8% della popolazione globale usa regolarmente le applicazioni dei social media nella sua vita personale e professionale.

Con una tale diffusione della tecnologia, non c'è da meravigliarsi che ci siano diversi rischi che possono avere un impatto negativo sull'esperienza e minacce che possono compromettere la sicurezza degli utenti nel mondo digitale. In questo modulo, esamineremo e presenteremo i principali aspetti della sicurezza digitale sia per l'uso generale degli strumenti online che per l'aspetto dell'apprendimento / insegnamento all'interno del settore VET.



Co-funded by the
Erasmus+ Programme
of the European Union

Obiettivi di formazione:

Alla fine di questo modulo saprai:

- avere una comprensione dei rischi associati all'uso di strumenti digitali e online
- avere una maggiore consapevolezza della sicurezza digitale
- aver acquisito competenze di base per affrontare le vostre esigenze di sicurezza digitale
- aver acquisito competenze che ti permetteranno di mantenere un'esperienza di apprendimento online sicura e protetta per i tuoi studenti
- avere il potere e la motivazione per salvaguardare la sicurezza digitale e adottare le ultime best practice e soluzioni.

Consigli generali per il formatore:

Assicurati che ci sia una comprensione comune dei termini usati in questo modulo per assicurare una consegna agevole del contenuto; potrebbe essere utile passare un po' di tempo a distinguere tra parole diverse e strumenti diversi.

Chiedi agli studenti di pensare al proprio uso degli strumenti digitali e online e a quanto è esteso; magari chiedi loro come sarebbe diversa o più difficile o anche migliore la loro vita se per le prossime 24 ore non ci fosse internet disponibile.

Co-funded by the Erasmus+ Programme of the European Union

Sollecita gli studenti a condividere le loro esperienze o preoccupazioni riguardo alla sicurezza digitale, prendere nota di questi problemi e collegarli al contenuto del modulo, dove possibile. Se ci sono questioni che non sono trattate, cerca di offrire ulteriori risorse esterne.

1. Quali sono le principali minacce/rischi che esistono online?

Adware

Adware è un software indesiderato progettato per lanciare pubblicità sul tuo schermo, chiamato anche pop-up.

Ecco alcuni tipici segni rivelatori del fatto che hai un adware sul tuo sistema:

- Le pubblicità appaiono in posti dove non dovrebbero essere.
- La homepage del tuo browser è misteriosamente cambiata senza il tuo permesso.
- Le pagine web che visiti di solito non vengono visualizzate correttamente.
- I link del sito web reindirizza a siti diversi da quelli che ti aspettavi.
- Il tuo browser web rallenta fino a fermarsi.
- Nuove barre degli strumenti, estensioni o plugin popolano improvvisamente il tuo browser.
- Il tuo computer inizia a installare automaticamente applicazioni software indesiderate.

Malvertising

Il malvertising - o pubblicità dannosa - è una tecnica di cyberattacco che inietta un codice dannoso all'interno degli annunci digitali. Difficile da rilevare sia dagli utenti di Internet che dagli editori, questi annunci infetti sono di solito serviti ai consumatori attraverso reti pubblicitarie legittime. Poiché gli annunci vengono visualizzati a tutti i visitatori del sito web, praticamente ogni visitatore della pagina è a rischio di infezione.

Phishing

Il phishing è l'attacco solitamente inviato via e-mail che invoglia gli utenti finali a cliccare su un link o un allegato dannoso. Gli aggressori possono usare il phishing per guadagnare un punto d'appoggio in un'organizzazione, spesso distribuendo malware.

Co-funded by the Erasmus+ Programme of the European Union

Spear phishing

Lo spear phishing è un metodo di phishing che prende di mira individui o gruppi specifici all'interno di un'organizzazione. Si tratta di una potente variante del phishing, una tattica dannosa che utilizza e-mail, social media, messaggistica istantanea e altre piattaforme per indurre gli utenti a divulgare informazioni personali o eseguire azioni che causano la compromissione della rete, perdita di dati o perdite finanziarie. Un tipico attacco di spear phishing comprende un'e-mail e un allegato. L'email include informazioni specifiche per l'obiettivo, tra cui il nome del bersaglio e il suo grado all'interno dell'azienda. Questa tattica di ingegneria sociale aumenta le possibilità che la vittima compia tutte le azioni necessarie per l'infezione, compresa l'apertura dell'email e dell'allegato incluso

Cybersquatting (domain squatting)

Il cybersquatting è la registrazione e l'uso non autorizzato di nomi di dominio Internet che sono identici o simili a marchi, marchi di servizio, nomi di società o nomi personali al fine di creare confusione, o per attirare maliziosamente gli utenti o condurre truffe.

Spyware

Lo spyware è un software con un funzionamento malevolo che mira a raccogliere informazioni su una persona o un'organizzazione e a inviarle a un'altra entità in un modo che danneggia l'utente.

Smishing

Gli attacchi di smishing utilizzano il servizio di messaggi brevi o SMS, più comunemente noti come messaggi di testo.

Lo smishing comprende il furto di dati personali da te, fingendosi un rappresentante della tua banca, facendoti cliccare su un link nel messaggio di testo per connetterti alla pagina web della tua banca e verificare un recente addebito sospetto, chiedendo di chiamare il loro numero di servizio clienti, convenientemente incluso nel messaggio di testo, per parlare con loro di un recente addebito sospetto o di un conto compromesso.

Quanto sopra rappresenta solo una selezione limitata delle minacce online che sono attualmente prevalenti, prendendo di mira milioni di utenti ogni giorno in questo momento. Si consiglia agli utenti di rimanere informati sugli sviluppi e le nuove minacce monitorando regolarmente i siti web come quelli inclusi sotto la voce "Ulteriori risorse":

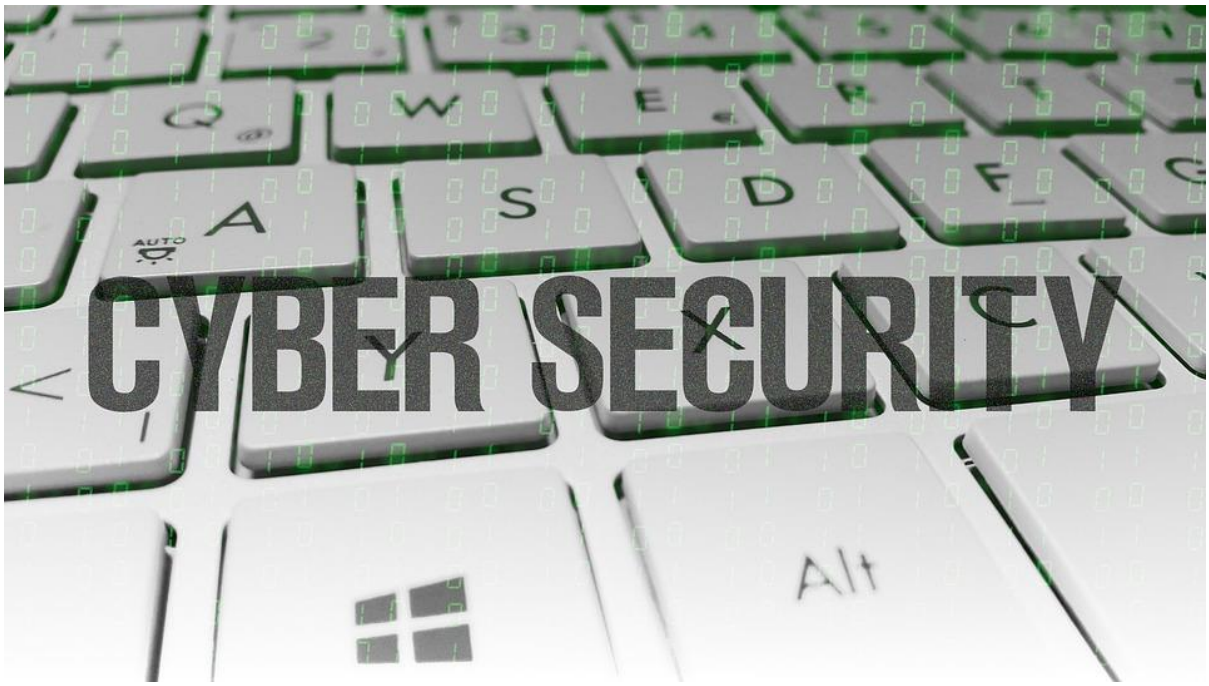
Ulteriori risorse

ENISA (europa.eu)

Cybersecurity Risks | NIST

Co-funded by the Erasmus+ Programme of the European Union

Si consiglia ai formatori di arricchire l'elenco di ulteriori risorse con materiali nella propria lingua e/o materiali pertinenti al paese/area. Una buona fonte di informazioni può anche essere trovata su articoli online e pubblicazioni di esperti e ricercatori di sicurezza informatica.



2. Misure di sicurezza digitale

Creare password e renderle forti.

Un gran numero di utenti non usa la funzione password su almeno uno dei propri dispositivi abilitati a internet, lasciandolo aperto a chiunque possa prenderlo. Blocca tutti i tuoi dispositivi, compresi computer, tablet e smartphone, con password sicure. Questo terrà fuori occhi indiscreti e aggiungerà una linea di difesa nel caso in cui i tuoi dispositivi vengano persi, spostati o rubati. Una password forte è lunga almeno 12 caratteri. I consigli per una password forte includono l'uso di un mix di lettere minuscole e maiuscole, numeri e simboli, evitando di usare informazioni personali che possano essere facilmente identificate (nome del coniuge, nome dell'animale domestico, compleanni, ecc). Una password debole sarebbe qualcosa che chiunque potrebbe facilmente scoprire, come il nome di un amato animale domestico "KittkyCat"; una password forte potrebbe essere come "1Kitty234Cat!

Quanto spesso è necessario cambiare le password?

Co-funded by the Erasmus+ Programme of the European Union

A meno che non si venga a conoscenza di una violazione delle password, non c'è bisogno di cambiare le password regolarmente se ognuna è forte e unica. Questo è ancora più vero se si utilizza l'autenticazione a due fattori.
Ogni volta che è possibile, utilizza una forma di autenticazione a due fattori in modo che una password violata non comprometta il tuo account. Combinando l'autenticazione a due fattori con password generate da macchine, la maggior parte degli account utente diventa praticamente inattaccabile.

Cos'è una password unica?

Una password unica è:

1. Mai utilizzata. Una volta che usi una password, non puoi mai usarla per un altro account.
2. Abbastanza lunga. Una password forte è lunga almeno 12 caratteri. I consigli per una password forte includono l'uso di un mix di lettere, numeri e simboli.
3. Niente che si riferisca a te. Questo significa che non devi usare il nome di un bambino o di un animale domestico nella tua password o altre informazioni che possono essere facilmente ricondotte a te.

Poiché al giorno d'oggi gli utenti utilizzano più applicazioni e dispositivi, può essere molto allettante usare una sola password per la maggior parte dei tuoi dispositivi e applicazioni. Per quanto conveniente, questa pratica può causare una grande vulnerabilità, in quanto un attacco dannoso può colpire la maggior parte dei tuoi account e persino compromettere l'online banking o le soluzioni di cloud storage. Si consiglia quindi vivamente di utilizzare diverse password uniche per i diversi dispositivi e applicazioni e di prestare attenzione quando si condividono o si digitano tali password su reti pubbliche.

Come funziona l'autenticazione a due fattori?

Puoi attivare un'autenticazione a due fattori nelle impostazioni del tuo account di social media, e-mail o altri profili. L'autenticazione a due fattori sarà effettuata con l'aiuto del tuo numero di telefono o attraverso un'app di autenticazione sul tuo smartphone. Dopo aver attivato l'autenticazione a due fattori, ogni volta che accederai al tuo account da un nuovo dispositivo o browser, il codice di sicurezza verrà inviato al tuo telefono o alla tua app di autenticazione. È necessario inserire questo codice e vi sarà permesso di accedere. Se un cybercriminale cerca di entrare nel tuo account non sarà in grado di farlo se non ha accesso al tuo telefono cellulare. Potrai anche accorgerti di un tentativo di accesso al tuo account, perché riceverai una notifica con un codice. Non condividere mai questo codice con altre persone! Un hacker cercherà di ottenerlo. Se hai ricevuto il codice ma non hai tentato l'accesso, cancella il messaggio del codice e cambia la tua password il prima possibile.

Co-funded by the
Erasmus+ Programme
of the European Union

Impostazioni della privacy nei social media

Quando si creano post sui social media, è possibile scegliere le impostazioni di privacy. Per esempio, puoi scegliere quale pubblico vedrà il tuo post. Potrebbe essere solo i tuoi amici che hai aggiunto sul social network, potrebbe essere un post pubblico per chiunque, o potrebbe essere un post privato solo per te. Puoi anche specificare o non specificare la tua posizione. Assicurati che le tue informazioni private non siano condivise. Per esempio, le tue password, il numero di telefono, l'e-mail, ecc.

Regole di sicurezza nei social media, messenger e e-mail

Nella comunicazione attraverso le reti sociali, i messenger e posta elettronica devi stare attento a non essere danneggiato da pretexting, malvertising o diversi tipi di phishing. Non cliccare sui link che ti vengono inviati da una persona sconosciuta. Fai attenzione - i cyber criminali possono fingere di essere, per esempio, dipendenti di Facebook o del servizio di sicurezza di Instagram. Non fidarti di quei messaggi, se li ricevi attraverso una normale chat, un post o da una normale pagina di Facebook. I messaggi di sicurezza ti saranno consegnati attraverso le notifiche o saranno disponibili nelle impostazioni. Gli impiegati dei social media non ti chiederanno mai la tua password o informazioni private.

Qualcuno ti chiede dei soldi?

Se amici o familiari ti chiedono di aiutarli in caso di emergenza, chiama sempre per parlare con loro personalmente e confermare che il messaggio sia partito da loro. Altrimenti quei messaggi possono essere di cyber criminali. Possono creare un profilo identico a quello di un membro della tua famiglia o di un amico e cercare di ottenere denaro da te.

Sicurezza del dispositivo

Usa il software di sicurezza. Installa un software di sicurezza sui tuoi dispositivi da una fonte affidabile e tienilo aggiornato. È meglio eseguire regolarmente il software antivirus e antispyware. Diffida degli aggiornamenti di sicurezza provenienti da annunci pop-up o e-mail. Potrebbero essere in realtà malware che potrebbero infettare il tuo computer.

Utilizza la protezione di sicurezza predefinita del firewall sul tuo computer.

Il tuo sistema operativo (OS) ha probabilmente delle impostazioni firewall predefinite che proteggono il tuo computer senza bisogno di adattamenti. Se il tuo software antivirus include una protezione firewall aggiuntiva che puoi regolare separatamente, considera di contattare un professionista del computer per avere assistenza e

Co-funded by the
Erasmus+ Programme
of the European Union

assicurarti di essere protetto in modo sicuro senza bloccare troppo i siti e i programmi che usi regolarmente.

Log out. Ricordati di fare il logout da app e siti web quando hai finito di usarli. Lasciarli aperti sullo schermo del computer potrebbe renderti vulnerabile ai rischi per la sicurezza e la privacy.

10 consigli per tenerti al sicuro online

1. Crea password e rendile forti.

2. Accesso sicuro ai tuoi account. Dato che le password possono essere rubate, aggiungere l'autenticazione in due fasi agli account fornisce un secondo livello di protezione. Molti servizi online, tra cui app e siti web, offrono opzioni gratuite che potrebbero aiutarti a proteggere le tue informazioni e a garantire che sia davvero tu a cercare di accedere al tuo account e non qualcuno con la tua password.

3.Pensa prima di agire. Le e-mail e le comunicazioni che creano un senso di urgenza, come un problema con il tuo conto bancario o con le tasse, sono probabilmente una truffa. Considera di contattare direttamente l'azienda per telefono per determinare se l'e-mail è legittima o no.

4. 4. In caso di dubbio, cestinala. Cliccare sui link nelle e-mail è spesso il modo in cui i truffatori hanno accesso alle informazioni personali. Se un'e-mail sembra insolita, anche se conosci la persona che l'ha inviata, è meglio cancellarla. Ricorda che i truffatori possono impossessarsi degli indirizzi e-mail degli amici e inviarti messaggi spacciandosi per loro. Attiva i filtri antispam per il tuo account di posta elettronica per aiutarti a filtrare i messaggi sospetti.

5. Condividi con cura. Fai attenzione a ciò che condividi pubblicamente su siti di social media come Facebook. Regola le impostazioni della privacy per limitare chi può vedere le tue informazioni. Evita di condividere la tua posizione.

6. Usare software di sicurezza. Installa un software di sicurezza sui tuoi dispositivi da una fonte affidabile e tienilo aggiornato. È meglio eseguire regolarmente il software antivirus e antispyware. Diffida degli aggiornamenti di sicurezza provenienti da annunci pop-up o e-mail. Potrebbero essere in realtà malware che potrebbero infettare il tuo computer.

7.Regola le impostazioni di sicurezza del browser. Probabilmente cerchi notizie, informazioni e prodotti utilizzando un browser internet come Firefox, Google Chrome, Internet Explorer e Safari. Regola le tue impostazioni in ognuno di questi browser per impostare le tue opzioni per una sicurezza ottimale. Questi menu si trovano spesso nell'angolo in alto a destra del tuo browser. Considera di cancellare la tua cronologia di navigazione alla fine della tua sessione in modo da non lasciare una traccia di dati sensibili.

Co-funded by the Erasmus+ Programme of the European Union

8. Utilizza la protezione di sicurezza predefinita del firewall sul tuo computer. Il tuo sistema operativo (OS) ha probabilmente delle impostazioni firewall predefinite che proteggono il tuo computer senza bisogno di regolazioni. Se il tuo software antivirus include una protezione firewall aggiuntiva che puoi regolare separatamente, considera di contattare un professionista del computer per avere assistenza e assicurarti di essere protetto in modo sicuro senza bloccare troppo i siti e i programmi che usi regolarmente.

9. Esci. Ricordati di uscire dalle app e dai siti web quando hai finito di usarli. Lasciarli aperti sullo schermo del tuo computer potrebbe renderti vulnerabile ai rischi per la sicurezza e la privacy.

Considera il supporto. Se sei preoccupato per la sicurezza digitale, rivolgiti a un professionista di fiducia o chiedi supporto e approfondimenti al dipartimento IT della tua organizzazione.

AUTOVALUTAZIONE:

- Rifletti sulle tue abitudini e pratiche quotidiane, credi che potresti essere vulnerabile in termini di sicurezza digitale?
- Quanti dei 10 consigli proposti stai attuando attualmente?
- Quali sono i consigli o le idee che hai intenzione di utilizzare?
- Quali sono 3 consigli che offriresti agli studenti per quanto riguarda la sicurezza digitale?

Co-funded by the
Erasmus+ Programme
of the European Union