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

Scenario 1
Tecnologia e IT (ad es. materiali, processi, organizzazione della produzione, IT)

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nome del partner: Foro de Formación y Ediciones

Open Educational Resources

Questo materiale è stato creato nell'ambito del progetto BRAIN "BringING STEM into Active AgING" (GRANT AGREEMENT 2020-1-PL01-KA204-081805). Questo progetto è stato finanziato con il supporto della Commissione Europea. L'autore è il solo responsabile di questa pubblicazione e la Commissione declina ogni responsabilità sull'uso che potrà essere fatto delle informazioni in essa contenute.

Akademia WSEI LUBLIN

Mine Vaganti NGO

FFE Foro de Formación y Ediciones S.L.

HORIZONT X PROCONSULT

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

Perdita di dati personali, creazione di password forti, organizzatori di password

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nome del partner: Foro de Formación y Ediciones

Questo materiale è stato creato nell'ambito del progetto BRAIN "BringING STEM into Active AgING" (GRANT AGREEMENT 2020-1-PL01-KA204-081805). Questo progetto è stato finanziato con il supporto della Commissione Europea. L'autore è il solo responsabile di questa pubblicazione e la Commissione declina ogni responsabilità sull'uso che potrà essere fatto delle informazioni in essa contenute.

Akademia WSEI LUBLIN

Mine Vaganti NGO

FFE Foro de Formación y Ediciones S.L.

HORIZONT X PROCONSULT

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

Rompighiaccio

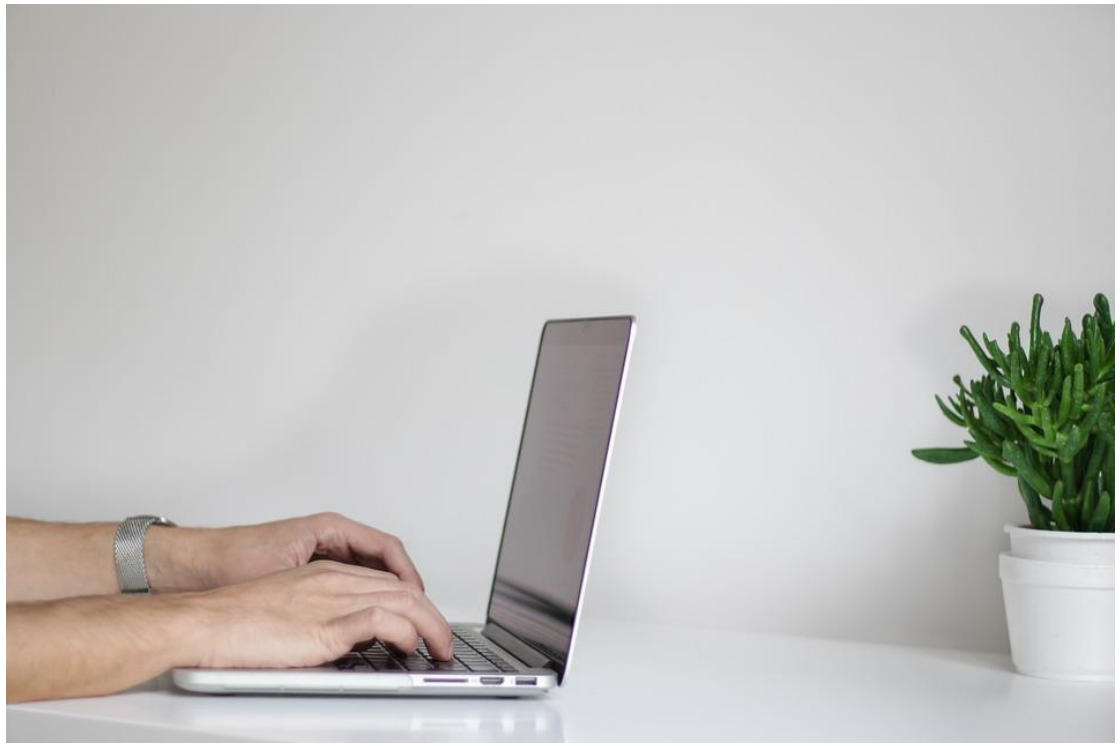
Mettiamoci in cerchio. Iniziate dicendo il vostro nome e una parola relativa all'informatica che inizia con la stessa lettera. Ad esempio, Adam Application, Bartek Banner, Celine Cookies, Darek Domain, ecc....

Poi la persona successiva fa il suo, più il vostro. Poi la terza persona fa il suo, quello della seconda e il nome della prima e una parola relativa all'informatica. Si procede poi in ordine sparso, in modo che l'ultima persona debba fare il nome di tutti i membri del gruppo. Si possono fare diverse varianti di questo gioco, ma è ottimo per far conoscere al gruppo gli altri e i nomi.

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

Introduzione

Internet è diventato un fattore determinante per lo sviluppo della società odierna. È stato utilizzato come mezzo principale per l'interazione tra persone e computer, per lo scambio di informazioni e per promuovere la rapida trasmissione di esperienze e conoscenze indipendentemente dalla posizione geografica.



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

Introduzione

Dagli inizi negli anni '60 a oggi, Internet è stato un ingrediente fondamentale per lo sviluppo tecnologico, l'istruzione, le comunicazioni, la medicina, la scienza, l'arte e praticamente tutte le discipline e le professioni. in un mondo globalizzato. Sebbene inizialmente fosse destinato all'uso militare, i suoi vantaggi sono stati radicalmente estesi praticamente a qualsiasi campo.

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

Introduzione

Il commercio è un altro ambito in cui Internet è riuscito ad avere un impatto positivo, sia per il venditore che per l'acquirente. I grandi supermercati e le catene di negozi, oltre ad avere i loro punti vendita, hanno sviluppato piattaforme per le vendite online, riuscendo ad abbassare alcuni costi come il personale di vendita e le sedi, ad esempio. Il commercio elettronico consente alle aziende di attraversare i confini senza la necessità di essere fisicamente in un luogo. Questo ha portato a un'efficienza commerciale e ha aperto nuove strade per il commercio.

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

Introduzione

Inoltre, il commercio elettronico non è più un'esclusiva dei grandi marchi. La versatilità del business ha permesso anche alle piccole e medie imprese di avventurarsi in questo settore, e i social network hanno dato un contributo interessante a questa dinamica.

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

Introduzione

Internet è quindi oggi un mezzo di comunicazione globale che ci permette di interagire in spazi diversi. Dalla comunicazione attraverso una videochiamata o una chat con un'altra persona a migliaia di chilometri di distanza, all'accesso a un'istruzione di qualità in istituti e università di diverse parti del mondo, all'acquisto di prodotti o servizi online, alla lettura di giornali, riviste o libri, all'ascolto di musica, alla visione di film o all'interazione sui social network. Questo, per citare solo alcune delle tante possibilità che ci offre.

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

Introduzione

È nelle nostre mani l'uso razionale e oggettivo di uno strumento tanto potente quanto vorremmo che fosse.

Il modo in cui Internet si è evoluto dalla sua invenzione è fantastico e ci ha fatto capire che continuerà a evolversi così velocemente da non smettere di stupirci.

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.
Lavagna a fogli mobili sulle fake news

I materiali

telefoni/tablet/laptop con accesso a Internet, lavagna luminosa, penne, pennarelli, lavagna a fogli mobili, foglietti adesivi, fogli A4.

Indicazioni stradali

Il conduttore scrive il termine "FAKE NEWS" al centro della lavagna a fogli mobili. Distribuisce 3 post-it ai partecipanti e chiede loro di scrivere le loro associazioni con il termine e di incollarli sulla lavagna a fogli mobili. Leggete le associazioni scritte, raggruppandole se possibile. Discutete ogni associazione e confrontatela con la definizione di fake news (appendice sotto).

Appendice

Il termine "Fake news"

Le fake news sono "notizie false e non veritiere, solitamente diffuse dai tabloid per suscitare scalpore o diffamare qualcuno (di solito un politico)". Il Cambridge Dictionary dice che si tratta (tradotto) di "storie false che sembrano notizie, diffuse su Internet o attraverso altri media, di solito create per influenzare le opinioni politiche o per scherzo".

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.
Lavagna a fogli mobili sulle fake news

Il termine "fake news" è un neologismo ed è difficile da collocare in un quadro definitorio. Denota una notizia mediatica che non è né vera né falsa allo stesso tempo e si basa sulla disinformazione, spesso includendo parti vere. Le fake news sono solitamente basate sulla disinformazione o su uno scherzo, spesso contenenti elementi veri. Le fake news possono fingere di essere informazioni reali, articoli, post sui social media, meme, ecc. Possono essere create con diverse intenzioni, dall'inganno, a strumenti di propaganda, a creare sensazionalismo, a uno scherzo.
Le fake news sono "una manipolazione dei fatti, utilizzata con foga dai giornalisti il cui scopo, durante la preparazione di una pubblicazione, è quello di suscitare il maggior interesse possibile per l'argomento, e non la sua conformità con la realtà".
Internet è attualmente la fonte di comunicazione più diffusa. Tuttavia, i contenuti pubblicati su di esso devono essere affrontati con cautela. Lo studio IAB "Disinformazione nel Web. Analysis of the credibility of information channels" mostra che i social media sono i leader nella diffusione di fake news. Al secondo posto ci sono i portali internet.

Tipi di fake news:
totale falsità - le informazioni fornite sono inventate, contraddittorie,
la verità è contestabile - i fatti sono presentati in modo selettivo o nel giusto contesto, con il risultato di ingannare il destinatario,
manipolazione della citazione - l'affermazione viene collocata nel contesto appropriato o le frasi o i loro frammenti vengono rimossi, il che cambia il senso dell'affermazione e di conseguenza sostiene la tesi specifica.

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.
Video di notizie false

I materiali

telefoni/tablet/laptop con accesso a Internet, lavagna luminosa, penne, pennarelli, lavagna a fogli mobili, foglietti adesivi, fogli A4.

Indicazioni stradali

Utilizzando una lavagna luminosa, il presentatore mostra brevi filmati su cosa sono le fake news e come riconoscerle.
Come si diffondono le notizie false - Noah Tavlin (inglese, sottotitoli disponibili in altre lingue)
https://www.youtube.com/watch?v=cSKGa_7XJkg
Come scegliere le notizie - Damon Brown (inglese, sottotitoli disponibili in altre lingue)
https://www.youtube.com/watch?v=q-Y-z6HmRgI
Presentare al gruppo gli elementi grazie ai quali si possono riconoscere le fake news, distinguendole dalle informazioni reali (appendice sotto).

Appendice

INTERPRETAZIONE DEL MATERIALE DI PARTENZA:
- prestare attenzione al linguaggio emotivo, alle descrizioni brutali
- essere consapevoli dei propri pregiudizi
- porre domande sul materiale (chi è l'autore? il messaggio è coerente? altre fonti confermano le informazioni? ecc.)

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.
Video di notizie false

- prestare attenzione al fatto che le immagini utilizzate siano inserite in un contesto reale
verificare la credibilità del sito web - l'URL è corretto e conduce al sito web corretto e autentico
- controllare la data e la tempestività delle informazioni
- verificare l'autore - se è credibile, quali sono i suoi obiettivi e le sue intenzioni, se ha già pubblicato altri materiali online
- verificare che le immagini non abbiano un aspetto strano o non siano state manipolate - questo può essere fatto, ad esempio, utilizzando l'opzione di ricerca inversa delle immagini disponibile nei motori di ricerca

FAKE NEWS - REGOLE GENERALI:
Sono dominati da immagini/foto e testi brevi.
Il messaggio è fortemente emotivo: usa parole d'odio, mostra scene e immagini violente e commoventi.
Spesso finge di essere di prima mano.
Utilizzano verità e credenze generalmente conosciute.
Spesso mostrano mezze verità, travisano i fatti in modo tale che è impossibile sapere dove iniziano e dove finiscono le informazioni verificate. Si basano sul presupposto che una verità parziale confermi la verità dell'insieme.
A volte descrivono eventi veri ma cambiano il contesto.
Quasi sempre includono immagini o video per contribuire ad aumentare rapidamente la copertura.
Non comunicano che le informazioni fornite potrebbero non essere certe.
Evitano le sfumature e i diversi punti di vista.

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

È il momento delle domande...

Cosa mi può dire sulla privacy online?

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

È ora di rispondere...

La definizione di privacy online è il livello di protezione della privacy di un individuo quando è connesso a Internet. Copre la quantità di sicurezza online disponibile per i dati personali e finanziari, le comunicazioni e le preferenze. La privacy su Internet è importante perché consente di controllare la propria identità e le proprie informazioni personali. Senza questo controllo, chiunque abbia l'intenzione e i mezzi per farlo può manipolare la vostra identità per raggiungere i propri obiettivi, che si tratti di vendervi una vacanza più costosa o di rubare i vostri risparmi.

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

L'importanza delle password

Le password sono la chiave che apre la porta all'utilizzo di tutti i nostri servizi. Se le nostre password vengono esposte, i criminali informatici potrebbero essere in grado di utilizzarle per entrare e impersonare noi, effettuare pagamenti a nostro nome, modificare o accedere ad altri tipi di informazioni o ad altre persone, tra le altre cose, quindi è consigliabile adottare una serie di misure per la nostra protezione.

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

L'importanza delle password

Una password deve essere forte, con un minimo di 8 caratteri e composta da:

-Maiuscolo (A, B, C...)

-Numeri (1, 2, 3...)

-Minuscole (a, b, c...)

-Caratteri speciali ($, &, #...)

È importante utilizzare password non facili da indovinare. Ad esempio: "123456789", "qwerty", "aaaaa", nomi propri, compleanni, ecc...

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

L'importanza delle password

Le password non devono essere condivise con nessuno, una password deve appartenere esclusivamente all'utente che la crea e deve essere utilizzata solo dall'utente stesso. Condividerla ci rende vulnerabili e lo è ancora di più se il modo in cui la condividiamo è una rete di messaggistica come (WhatsApp, Telegram, Facebook), poiché le informazioni vengono memorizzate sui server di questi servizi.

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

L'importanza delle password

Cercate di evitare assolutamente di utilizzare la stessa password per tutti i servizi, poiché se un criminale informatico entra in possesso di tale password, sarà in grado di accedere a tutti i servizi.

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

L'importanza delle password

Cambiate le password periodicamente e non una permanente per sempre. Un buon modo per ricordare quando dovremmo cambiare le nostre password è tenere a mente le stagioni dell'anno. Una password viene cambiata per ogni stazione, in modo da essere sempre aggiornata ogni 3 mesi.

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

L'importanza delle password

Per ovviare al gran numero di password che si dovrebbero gestire nel caso in cui se ne avesse una per servizio, esistono dei gestori di password che semplificano la vita quando si tratta di ricordarle tutte.

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

Autenticazione in 2 fasi

A volte, avere una password non è sufficiente, per quanto forte possa essere, o dopo aver seguito tutti i passaggi precedenti.

I criminali informatici potrebbero entrarne in possesso attraverso diverse tecniche, come il "phishing" o alcuni virus progettati per questo scopo che vedremo più avanti.

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

Autenticazione in 2 fasi

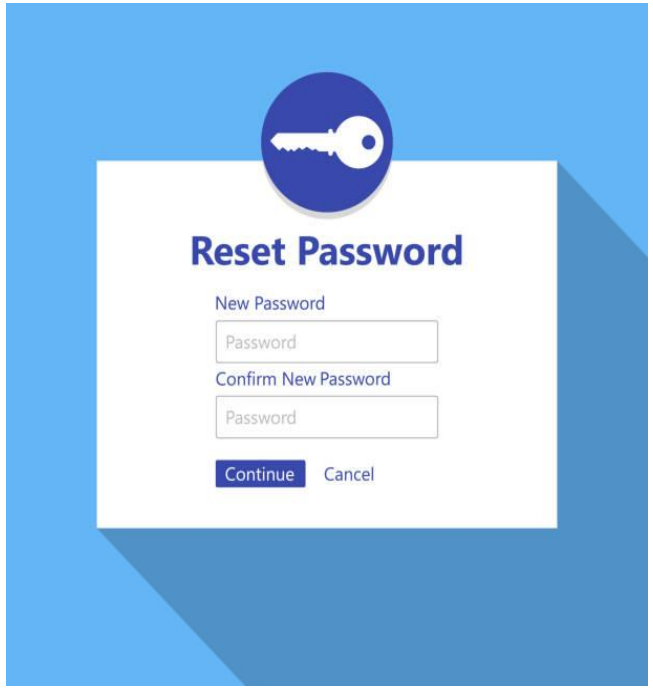
Per questo motivo molti servizi offrono già l'autenticazione in due passaggi. Con questo metodo utilizzeremo la password del servizio in modo normale e poi ci verrà chiesto di aggiungere un secondo codice.

Il modo più comune per ricevere questo codice è riceverlo come SMS sul nostro smartphone, anche se può essere una telefonata attraverso un apparecchio o un'applicazione di servizio che cambia attivamente i codici ogni 5 minuti.

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

Autenticazione in 2 fasi

È chiaro che il servizio deve essere precedentemente configurato per collegarvi il nostro smartphone e ricevere i codici. In questo modo, anche se il criminale informatico riesce a ottenere la vostra password, non potrà accedere al servizio perché avrà bisogno di questo secondo codice per entrare.



Se in qualsiasi momento vi trovate di fronte a un tentativo di accesso al vostro account perché avete ricevuto il doppio codice di autenticazione e non siete stati voi, dovreste prendere in considerazione la possibilità di cambiare la password perché è molto probabile che non sia più una chiave sicura.

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

È il momento delle domande...

Che cos'è lo spionaggio?

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

È ora di rispondere...

Quando siete online, siete spiati da numerosi tracker per vari scopi. I tracker tengono traccia della vostra cronologia di ricerca e di tutte le vostre attività online attraverso vari mezzi. Questo fornisce loro un quadro chiaro di chi siete e dei vostri interessi, il che costituisce una violazione delle norme sulla privacy online e vi rende una proprietà pubblica. Nella maggior parte dei casi, questo tracciamento è finalizzato esclusivamente a scopi pubblicitari e consente agli inserzionisti di mostrare annunci in base ai vostri gusti e interessi. Ma a volte queste informazioni vengono utilizzate dai criminali informatici per svolgere attività non autorizzate e illegali, mettendo a rischio la vostra esistenza online.

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

Dati personali

Prima di fornire i vostri dati personali, dovete analizzare chi ve li chiede e a cosa vi servono queste informazioni.

Le informazioni che dovrete fornire, ad esempio, per contrattare un conto bancario, non sono le stesse che dovrete fornire per iscrivervi a un sito di shopping online. Nel primo caso, le informazioni richieste saranno sostanzialmente ampie, mentre nel secondo saranno sufficienti nome, cognome, indirizzo di consegna, dati di fatturazione e modalità di pagamento.

Se qualcuno richiede i vostri dati personali, dovete informarvi sullo scopo, sull'uso che ne farà, sul trattamento e sulla durata della conservazione dei vostri dati.

È utile sapere come esercitare i propri diritti (Accesso, Rettifica, Opposizione, Limitazione del trattamento e Portabilità).

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

Phishing

Il phishing è il furto di identità di un servizio o di un'azienda per cercare di truffare le persone. Ad esempio, potreste ricevere un'e-mail che vi chiede di aggiornare i vostri dati bancari perché la vostra carta di credito sta per scadere. In questa e-mail viene fornito un link per accedere a questo servizio. Quando lo si apre, appare una pagina web che è una copia dell'originale, l'utente aggiorna i dati del suo conto bancario e a quel punto è caduto nell'inganno.

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

Phishing

Suggerimenti per evitare di essere una vittima

1. Diffidate delle e-mail che sembrano provenire da enti bancari o da servizi noti con messaggi del tipo:

a. Problemi tecnici dell'entità

b. Problemi di sicurezza nell'account utente.

c. Raccomandazioni di sicurezza per evitare le frodi.

d. Modifiche alla politica di sicurezza dell'entità

e. Promozione di nuovi prodotti

f. Buoni sconto, premi o regali

g. Imminente cessazione o disattivazione del servizio.

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

Phishing

2. Diffidate degli errori grammaticali presenti nel testo.

3. Se ricevete comunicazioni anonime indirizzate a "Gentile cliente" o "Notifica utente", è un'indicazione che deve mettervi in guardia.

4. Se il messaggio vi obbliga a prendere una decisione in poche ore, è un brutto segno. Si tratta di un contrasto diretto tra l'urgenza reale o meno e il servizio offerto da altri canali.

5. Verificare che il testo del link corrisponda all'indirizzo a cui punta.

6. Un servizio affidabile utilizzerà i propri domini per gli indirizzi e-mail aziendali. Se si ricevono le comunicazioni da una casella di posta elettronica del tipo @gmail.com o @hotmail.com, non è un buon segno.

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

Phishing

Cosa fare in caso di rilevamento di un caso di phishing

1. Non rispondete a queste e-mail in nessun caso. Se avete dubbi, chiedete direttamente all'azienda o al servizio che rappresenta.

2. Non accedete ai link forniti nel messaggio e non scaricate alcun documento allegato.

3. Eliminate il messaggio e avvisate i vostri contatti della frode.

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

È il momento delle domande...

Che cosa sapete della gestione scorretta delle informazioni?

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

È ora di rispondere...

Su Internet ci sono diversi siti che hanno bisogno delle vostre informazioni personali per accedere ai loro servizi. Spesso questi siti memorizzano i cookie e salvano le informazioni personali dell'utente per poi utilizzarle per vari scopi. Nella maggior parte dei casi queste informazioni non sono criptate e possono essere accessibili a chiunque. Questa gestione scorretta delle informazioni personali può portare a gravi conseguenze. La tendenza moderna dell'e-banking e dei portali di e-business ha moltiplicato i rischi associati alla privacy online. Condividendo i vostri dati bancari e i file più importanti su Internet, aprite la strada ai ladri e vi rendete vulnerabili ai criminali informatici.

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

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Due verità e una bugia

I materiali

Telefoni/tablet/laptop con accesso a Internet, proiettore, fogli di carta, penne, cartoncini.

Indicazioni stradali

Gioco Due verità e una bugia. Ai partecipanti vengono date tre affermazioni. Due saranno vere, una sarà una bugia. I partecipanti devono identificare la bugia.

Appendice

Ai partecipanti vengono date tre affermazioni. Due saranno vere, una sarà una bugia. I partecipanti devono identificare la bugia. Tutte le affermazioni saranno legate ad argomenti di Internet.

Shopping online:

1. La carta di credito è uno dei modi più pericolosi per pagare le merci online
2. Non dovreste mai inserire i vostri dati di pagamento in una pagina a meno che non ci sia una S dopo l'HTTP.
3. Se non si dispone di una carta di credito o di debito, PayPal è una buona alternativa per pagare i prodotti online.

Malware:

1. Il malware è un tipo di virus informatico
2. Un worm informatico sfrutta spesso i computer che utilizzano software non aggiornati
3. Un passo importante per proteggersi dal ransomware è la realizzazione di backup regolari.

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

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Due verità e una bugia

Phishing:

1. Se un'e-mail si rivolge a voi come "cliente", dovreste essere particolarmente cauti.
2. Una truffa di phishing che conosce dettagli personali pertinenti al destinatario è chiamata attacco di spear-phishing.
3. Fare clic su un link in un'e-mail va bene se l'e-mail proviene da una banca con cui si ha un conto.

Privacy sui social media:

1. L'unico livello di privacy predefinito consigliato è SOLO amici e familiari.
2. L'installazione di applicazioni di social media (Facebook, Instagram, Twitter...) può dare accesso a determinate informazioni su di voi a perfetti sconosciuti.
3. Se blocco qualcuno su Facebook o Twitter, questa persona non potrà vedere nulla di ciò che faccio o pubblico sul mio account.

Truffa su Facebook:

1. Aggiungere uno sconosciuto su Facebook gli consente di accedere al mio computer
2. Aggiungere uno sconosciuto su Facebook potrebbe mettere a rischio i miei amici
3. Aggiungere uno sconosciuto su Facebook potrebbe portare al furto d'identità

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

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Due verità e una bugia

Truffe via e-mail:

1. Le truffe via e-mail con commissioni anticipate si basano sull'inganno della vittima, che viene spinta a inviare denaro con la promessa di un ritorno molto più consistente.
2. Un allegato di posta elettronica che contiene un documento di Word può comunque essere pericoloso da aprire.
3. La cosa migliore da fare se ricevo un'email truffaldina del "principe nigeriano" è rispondere e dire loro di smettere di inviarmi email.

Ransomware

1. Se il ransomware infetta il mio computer, un programma antivirus affidabile e rispettabile può rimuoverlo.
2. L'antivirus può annullare gli effetti del ransomware
3. Il ransomware è una delle minacce online più prolifiche del 2017 e del 2018

Dopo questi esempi, i partecipanti dovranno pensarne almeno un altro. Poi cercheranno di scoprire quale affermazione è sbagliata.

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

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Due verità e una bugia

Risposte:

1

3

3

1

1

3

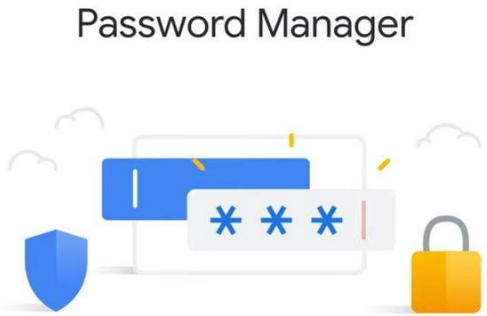
2

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

Gestori di password

Avere una versione gratuita di un ottimo gestore di password

è sempre meglio che non averne affatto.



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

Gestori di password

1Password: grande opzione per le famiglie ➞ https://cnews.link/get-1password_7/

==========

Piano gratuito contro:

Controlla le password compromesse

Assistenza via e-mail 24/7

Utenti illimitati per un account

Opzione di archiviazione locale

Limitazioni del piano gratuito:

❌ Nessun supporto di chat dal vivo

❌ Nessun aggiornamento della password con un solo clic

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

Gestori di password

NordPass: il gestore di password più versatile ➞ https://cnews.link/get-nordpass_46/

==========

Piano gratuito pro:

Crittografia di nuova generazione

Memorizzazione illimitata del caveau delle password

Autenticazione a più fattori

Trasferimenti facili del caveau

Assistenza clienti via chat

Limitazioni del piano gratuito:

La maggior parte delle funzioni sono a pagamento.

❌ Mancano i componenti aggiuntivi per altri browser

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

Gestori di password

Dashlane: un'esperienza sicura e semplificata ➞ https://cnews.link/get-dashlane_39/

==========

Piano gratuito:

Condivisione della password con 5 utenti

Ottima reputazione

Supporto 2FA

Memorizzare fino a 50 password

Limitazioni del piano gratuito:

Il numero massimo di password memorizzate è 50.

La versione iOS è carente

Limita l'utente a un solo dispositivo.

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

Gestori di password

Keeper: eccezionale strumento di gestione delle password ➞ https://cnews.link/get-keeper_10/

==========

Piano gratuito contro:

Grande compatibilità

Opzioni 2FA multiple

App di messaggistica privata

Limitazioni del piano gratuito:

❌ Poche opzioni di esportazione

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

Gestori di password

RoboForm ➞ https://cnews.link/get-roboform_10/

==========

Piano gratuito contro:

Memorizzazione illimitata del caveau delle password

Aggiornamento comodo delle password più deboli

Condivisione della password via e-mail

Monitoraggio del dark web

RoboForm

Limitazioni del piano gratuito:

❌ Potrebbe essere più facile da usare

❌ Chat in diretta solo per gli utenti a pagamento

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

È il momento delle domande...

Potete dirmi che cos'è il furto d'identità e alcuni dei modi in cui viene perpetrato? (phishing, malware, pharming, computer e telefoni abbandonati...)

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

È ora di rispondere...

Il furto d'identità e la frode d'identità sono termini utilizzati per riferirsi a tutti i tipi di reato in cui qualcuno ottiene e utilizza indebitamente i dati personali di un'altra persona in qualche modo che implica frode o inganno, tipicamente per un guadagno economico.

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

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Con chi stai parlando?

I materiali

Telefoni/tablet/laptop con accesso a Internet, proiettore, fogli di carta, penne, cartoncini.

Indicazioni stradali

Questo gioco dovrebbe simulare quando si parla con qualcuno su Internet e non si sa chi c'è dall'altra parte dello schermo, se sta dicendo la verità o meno, o se sta fingendo di essere qualcun altro per uno scopo nascosto.

A ogni partecipante viene assegnato un personaggio e gli altri devono scoprire chi sono. Ma alcuni di loro non corrisponderanno alla verità. Coloro che non hanno un personaggio, in coppia o in gruppo (a seconda dei partecipanti), devono indovinare attraverso delle domande chi è la persona con cui stanno parlando (quella che ha il ruolo assegnato). È pensato per un gruppo di 15 persone, dove 5 hanno un personaggio e 10 a coppie cercheranno di scoprire chi è il personaggio degli altri 5 e se è reale o meno. Il gioco si svolgerà in due gruppi di 15 partecipanti ciascuno.

Le persone con i personaggi assegnati devono rispondere alle domande come se fossero i personaggi stessi. Le coppie sapranno che è possibile che alcuni dei personaggi non siano chi dicono di essere. Le 5 coppie si faranno domande a vicenda per qualche minuto e si alterneranno. Dopo aver finito con tutti, ogni coppia deve dire chi pensa che sia ogni personaggio e se è davvero chi dice di essere.

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

Perdita di dati personali, creazione di password forti, organizzatori di password

Gioco: Con chi stai parlando?

Personaggio 1:

Ragazzo di 20 anni. Gli piace il calcio, uscire con gli amici e andare ai concerti.

Personaggio 2:

Ragazza di 25 anni. Gioca in una squadra di rugby e le piacciono gli sport di montagna. Le piacciono gli animali e ha un cane.

Personaggio 3: (Personaggio falso)

Risposte come: Ragazza di 18 anni. Partecipante a Biologia. Le piacciono la natura e le piante. È una fan di Rosalia.

In realtà lo è: Un uomo di 39 anni.

Personaggio 4: (Personaggio falso)

Risposte come: Ragazzo di 23 anni. Gli piace la musica rock e il surf. Di solito gioca ai videogiochi.

In realtà lo è: Un uomo di 47 anni.

Personaggio 5:

Ragazzo di 27 anni. Gioca a paddle tennis. Gli piacciono gli animali e ha due gatti. Lavora come grafico.

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

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Con chi stai parlando?

Cosa sta succedendo?

Questo gioco dovrebbe simulare quando si parla con qualcuno su Internet e non si sa chi c'è dall'altra parte dello schermo, se sta dicendo la verità o meno, o se sta fingendo di essere qualcun altro per uno scopo nascosto.

A ogni partecipante viene assegnato un personaggio e gli altri devono scoprire chi sono. Ma alcuni di loro non corrisponderanno alla verità.

Le persone con i personaggi assegnati devono rispondere alle domande come se fossero loro stessi i personaggi.

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

Scenario 2
Tecnologia e IT (ad es. materiali, processi, organizzazione della produzione, IT)

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nome del partner: Foro de Formación y Ediciones

Open Educational Resources

Questo materiale è stato creato nell'ambito del progetto BRAIN "BringING STEM into Active AgING" (GRANT AGREEMENT 2020-1-PL01-KA204-081805). Questo progetto è stato finanziato con il supporto della Commissione Europea. L'autore è il solo responsabile di questa pubblicazione e la Commissione declina ogni responsabilità sull'uso che potrà essere fatto delle informazioni in essa contenute.

Akademia WSEI LUBLIN

Mine Vaganti NGO

FFE Foro de Formación y Ediciones S.L.

HORIZONT X PROCONSULT

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

Problemi con gli acquisti e i trasferimenti di denaro online

BRinging STEM into Active agINg – BRAIN

Erasmus+ 2020-1-PL01-KA204-081805

Nome del partner: Foro de Formación y Ediciones

Questo materiale è stato creato nell'ambito del progetto BRAIN "BringING STEM into Active AgING" (GRANT AGREEMENT 2020-1-PL01-KA204-081805). Questo progetto è stato finanziato con il supporto della Commissione Europea. L'autore è il solo responsabile di questa pubblicazione e la Commissione declina ogni responsabilità sull'uso che potrà essere fatto delle informazioni in essa contenute.

Akademia WSEI LUBLIN

Mine Vaganti NGO

FFE Foro de Formación y Ediciones S.L.

HORIZONT X PROCONSULT

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

Rompighiaccio

Il gruppo forma un cerchio. I partecipanti si lanciano una palla. Ognuno dà un'associazione alla parola precedente pronunciata dalla persona da cui riceve la palla. L'attività viene ripetuta.

Cosa sta succedendo?

I rompighiaccio sono attività divertenti che aiutano le persone a conoscersi. Gli istruttori possono usarli per far conoscere ai partecipanti i contenuti e le aspettative del corso. I rompighiaccio possono anche servire a riscaldare gli spazi di apprendimento online e a orientare i partecipanti all'ambiente online.

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

Pagamenti mobili

I portafogli digitali sono un mezzo per memorizzare più carte di credito o di debito fisiche.

App bancaria che può essere utilizzata per l'autenticazione, come richiesto quando si effettuano transazioni o si accede ai servizi bancari. Di solito, ogni banca ha la propria applicazione.

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

Vantaggi di pagamenti mobili

Il Touch ID, sotto forma di scansione delle impronte digitali o di inserimento del PIN, li rende più sicuri delle carte di credito o di debito fisiche,

Eliminazione del portafoglio fisico

Le persone non sono in grado di vedere quale carta avete (alcune carte sono fornite per i clienti con bassi limiti di punteggio di credito. Alcune persone si vergognano di mostrarla agli altri).

Funge da fornitore di pagamenti di terze parti più semplice quando si paga su siti web di e-commerce.

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

È il momento delle domande...

Cosa sono i biscotti? A cosa servono?

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

È ora di rispondere...

I cookie sono piccole parti di testo che i siti web visitati inviano al browser dell'utente. Consentono ai siti web di ricordare le informazioni relative alla visita dell'utente, facilitando così la rivisitazione dei siti e rendendoli più utili per l'utente. Sono file temporanei che possono durare per un periodo di tempo più o meno lungo. Possiamo configurarli, utilizzare strumenti per bloccarli, cancellarli quando vogliamo... Il problema può sorgere soprattutto quando raccolgono dati personali senza avvisare l'utente.

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

Problemi con gli acquisti online, con le carte e con i trasferimenti di denaro.

Acquisti online sicuri

I materiali

Telefoni/tablet/laptop con accesso a Internet, proiettore, fogli di carta, penne, cartoncini.

Indicazioni stradali

I partecipanti saranno seduti in cerchio. Il formatore scriverà sulla lavagna a fogli mobili le domande guida per i partecipanti, aiutandoli a definire le regole per acquistare online in modo sicuro (appendice sotto).

Appendice

- utilizzare un sito web familiare
- utilizzare lo strumento di valutazione della sicurezza dei siti web per i nuovi siti
- cercare la serratura
- non condividete i vostri dati sensibili con tutti
- Utilizzare il Wi-Fi privato
- Creare password forti
- Non acquistate con la carta in luoghi pubblici

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

Portafogli digitali

- **Esempi:**
- Apple Pay, Google Pay e Samsung Pay sono probabilmente i tre portafogli digitali più popolari, ma ne esistono molti altri. Tra gli altri portafogli digitali più diffusi ci sono PayPal e Venmo, che hanno entrambi un carattere sociale unico, in quanto consentono di inviare facilmente denaro a rivenditori e amici.

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

Problemi con gli acquisti online, con le carte e con i trasferimenti di denaro.

I pericoli dell'uso del denaro nello spazio digitale

I materiali

Telefoni/tablet/laptop con accesso a Internet, proiettore, fogli di carta, penne, cartoncini.

Indicazioni stradali

Il relatore scrive al centro della lavagna a fogli mobili il termine "Pericoli dell'uso del denaro nello spazio digitale". Distribuisce ai partecipanti dei post-it adesivi (di colori diversi) e chiede loro di scrivere le loro associazioni con il termine e di incollarli sulla lavagna a fogli mobili. Leggete le associazioni scritte, raggruppandole se possibile. Discutete ogni associazione e cercate di conoscere i pericoli online legati al denaro (appendice sotto).

Appendice

I pericoli dell'uso del denaro nello spazio digitale

1. I dati della carta possono essere rubati (IBAN, CVC, data di scadenza).

I vostri dati personali possono essere rubati (nome e cognome, codice ID, data di nascita, numero di telefono, password).

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

I PORTAFOGLI DIGITALI SONO SICURI?

I portafogli digitali sono in realtà più sicuri delle carte fisiche, perché i pagamenti mobili sono fortemente criptati e tokenizzati, il che significa che nessun numero di carta o di conto corrente viene memorizzato all'interno del portafoglio digitale.

I portafogli digitali fanno un ulteriore passo avanti aggiungendo la tokenizzazione, che prende i dati sensibili criptati e li sostituisce con un equivalente digitale non sensibile, noto come token. Questi token unici vengono generati in modo casuale ogni volta che un utente effettua un pagamento e solo il gateway di pagamento dell'esercente può abbinare il token per accettare il pagamento.

Non solo le informazioni sono più sicure grazie a questa tecnologia, ma anche grazie alla verifica dell'utente. Questo ulteriore livello di sicurezza viene solitamente effettuato tramite impronta digitale, riconoscimento facciale o PIN.

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

Apple e Google pagano la somiglianza

Entrambi i sistemi utilizzano la tecnologia NFC

Sia Google Pay che Apple Pay possono effettuare acquisti online direttamente da un'app o da un sito web, gestendo automaticamente l'intero processo di checkout con impostazioni predefinite e richiedendo solo la verifica del PIN o del Touch ID per completare la transazione.

Entrambe sono più sicure delle carte di debito e di credito fisiche, perché il sistema non rivela al venditore i dati della carta dell'utente.

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

Differenze tra Apple e Google Pay

Apple pay consente l'autenticazione con Touch ID o Face ID, ma è compatibile solo con i nuovi gadget hardware.

Google, invece, opta per un sistema di autenticazione più tradizionale basato sul PIN. Questo permette di funzionare anche su hardware più vecchi.

È possibile aggiungere qualsiasi carta di credito o di debito a google pay. In apple pay è possibile aggiungere solo carte di credito o di debito che la società Apple ha in contatto con le banche che emettono carte fisiche.

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

È il momento delle domande...

Sapete cosa sono i dati del cloud?

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

È ora di rispondere...

Il cloud storage è un modello di cloud computing che prevede l'archiviazione dei dati su Internet tramite un provider di cloud computing che gestisce e opera l'archiviazione dei dati come servizio. Viene fornito su richiesta con capacità e costi just-in-time ed elimina l'acquisto e la gestione della propria infrastruttura di archiviazione dati.

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

Sicurezza di Google? Come funziona?

1. I dati della carta dell'utente vengono forniti una sola volta, durante la configurazione iniziale sui server di Google. (Google memorizza i dati della carta sui propri server).

2. Google salva i dati della carta sui suoi server.

3. La carta virtuale viene emessa sul vostro dispositivo con la crittografia dei dati sensibili.

4. Al momento del pagamento il venditore non vede mai i dati reali della carta, che sono protetti dai server di Google.

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

Sicurezza Apple? Come funziona?

- Apple utilizza un sistema di tokenizzazione.
  Passi;
- Quando i dati della carta vengono forniti al dispositivo, questo contatta direttamente la banca emittente. (Apple non memorizza i dati della carta)
- Quando la carta viene confermata, la banca riceve un token specifico del dispositivo e della carta (correlato), chiamato Device Account Number (DAN), che viene memorizzato su un chip sicuro del dispositivo.
- Il DAN assomiglia strutturalmente a un numero di carta di credito e viene trasmesso all'esercente quando viene effettuato un pagamento prima di essere autorizzato dalla banca.
- Apple pay spiegato in dettaglio:
  https://www.youtube.com/watch?v=mt5FEvoEHEk

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

Portafogli di criptovalute

Un portafoglio sicuro per le criptovalute funziona come un normale portafoglio, ma le valute e il contenuto del portafoglio possono essere violati attraverso mezzi digitali. Inoltre, un portafoglio può consentire agli utenti di effettuare diverse transazioni tenendo sotto controllo il proprio saldo.

Alcune banche online come Revolut, Wirex, Cryptopay ecc. permettono di prelevare gratuitamente le monete crittografiche dagli ATM in euro/dollari fino a un certo limite.

Revolut

wirex

CRYPTOPAY

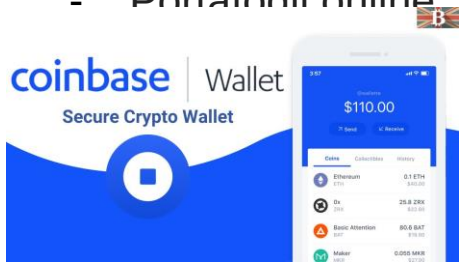
Co-funded by the
Erasmus+ Programme
of the European Union

Tipi di portafogli di criptovalute

Portafogli software

I portafogli software sono portafogli caldi in quanto spesso sono collegati a Internet. Si tratta di portafogli che funzionano con un programma specifico che consente un facile accesso. Alcuni esempi di portafogli software sono:

- Portafogli da tavolo
- Portafogli mobili
- Portafogli online



Portafogli hardware

I portafogli hardware si differenziano dai portafogli software in quanto memorizzano le chiavi private dell'utente in un dispositivo hardware come una chiavetta. Il loro scopo principale è quello di memorizzare i dati offline per evitare la violazione della privacy. Il loro scopo principale è quello di memorizzare i dati offline per evitare l'invasione della privacy.

Portafogli di carta

Questi tipi di portafogli includono un software particolare che può essere utilizzato per generare le chiavi e stamparle. Le altre funzioni comprendono il trasferimento dei fondi all'indirizzo e lo spostamento delle attività nel proprio portafoglio desktop. Per quest'ultima operazione, gli utenti dovranno inserire manualmente le chiavi o scansionare il codice incluso nel portafoglio.

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

È il momento delle domande...

Qualcuno potrebbe dirmi cos'è la cybersecurity?

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

È ora di rispondere...

La cybersecurity è la pratica di proteggere sistemi, reti e programmi dagli attacchi digitali. Questi attacchi informatici sono solitamente finalizzati all'accesso, alla modifica o alla distruzione di informazioni sensibili, all'estorsione di denaro agli utenti o all'interruzione dei normali processi aziendali.

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

Vantaggi dei diversi tipi di portafogli per criptovalute

Portafogli caldi/online/software

- Finalità di spesa;
- Non sono disposto a pagare per un portafoglio.

Portafogli freddi/offline/Hardware

- Finalità di investimento;
- Se state immagazzinando più criptovalute, allora state utilizzando.

Problemi con gli acquisti online, con le carte e con i trasferimenti di denaro.

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

Truffe negli acquisti online - video

I materiali

Telefoni/tablet/laptop con accesso a Internet, proiettore, fogli di carta, penne, cartoncini.

Indicazioni stradali

ELEMENTI DI CREDIBILITÀ DEL SITO WEB

Come individuare ed evitare un sito web truffa (inglese):

https://www.youtube.com/watch?v=3oEI0FCnI_Y

Consigli per acquistare online in modo sicuro (inglese):

https://www.youtube.com/watch?v=cWcNQgPiqhc

Passi:

1. Prima di riprodurre i video di cui sopra, i partecipanti sono invitati a seguirli e a notare che non tutti gli elementi di credibilità sono stati presi in considerazione.
2. Dopo aver visto i video, i partecipanti seduti in cerchio sono invitati a scrivere sulla lavagna a fogli mobili gli elementi per verificare la credibilità di un sito web.
3. Ogni scritto viene discusso subito dal partecipante e dal formatore (appendice sotto).

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

Problemi con gli acquisti online, con le carte e con i trasferimenti di denaro.

Truffe negli acquisti online - video

Appendice

Come verificare la credibilità di un sito web:
Annunci a pagamento - alcuni truffatori utilizzano gli annunci a pagamento di Google per apparire in cima alle ricerche su Google.
Recensioni positive false degli utenti - i siti web falsi creano recensioni positive per aumentare la credibilità. recensioni di utenti decisamente falsi.
URL falso - alcuni siti web falsi utilizzano lettere di diversi alfabeti per imitare siti web legittimi.
PadLock e HTTPS - indicano che i dati inseriti nel sito web sono criptati. (I terzi non possono vedere le vostre password, e-mail ecc.).
Certificato - controllare la data di scadenza del certificato del sito web e chi lo ha rilasciato.
Indirizzo dell'azienda. diritti d'autore e contatti - l'indirizzo dell'azienda non si trova su google maps o è in un posto strano (foresta, deserto ecc.)
Diritti d'autore, statuto di funzionamento/lavoro - devono essere aggiornati.
E-mail false - meglio inserire i link dal browser che dalle e-mail, perché possono contenere dati spyware per raccogliere dati sensibili.

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

Carta di debito

Le carte di debito sono **emesse dalla vostra banca e funzionano come una combinazione di carta bancomat e carta di credito**. Tuttavia, a differenza di una carta di credito, una carta di debito si collega direttamente al vostro conto bancario, utilizzando il denaro che avete in deposito per pagare i vostri acquisti o per effettuare il prelievo al bancomat in modo digitale.

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

Carte di debito

Pro

- Prevenire il debito
- Nessuna tassa annuale
- Ottimo per acquisti di piccole dimensioni
- Facile da ottenere

Contro

- Hanno fondi limitati
- Hanno commissioni di scoperto
- Complicato per gli articoli di grande valore

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

È il momento delle domande...

Qualcuno sa come creare una password forte?

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

È ora di rispondere...

Le chiavi principali per creare una password forte sono che deve essere lunga almeno 12 caratteri, mescolando lettere maiuscole e minuscole, numeri e un simbolo. È inoltre necessario utilizzare password diverse per ogni sito e cambiarle di tanto in tanto.

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

Carte di credito

Le carte di credito offrono una linea di credito che può essere utilizzata **per effettuare acquisti, trasferimenti di saldo e/o anticipi di contante**, con l'obbligo di restituire l'importo del prestito in futuro. Quando si utilizza una carta di credito, è necessario effettuare almeno il pagamento minimo ogni mese entro la data di scadenza del saldo.

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

Carte di credito

Pro

- Tempo per notare gli errori
- Può costruire il credito
- Offerta di premi
- Hanno limiti elevati

Contro

- Può perdere non molto denaro
- Può danneggiare il credito
- Potenziale di spesa eccessiva

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

È il momento delle domande...

Che cos'è una VPN?

Akademia WSEI
Mine Vaganti NGO
FFE Foro de Formación y Ediciones S.L.
Horizont X Proconsult

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

È ora di rispondere...

VPN è l'acronimo di "virtual private network", un servizio che vi aiuta a mantenere la privacy online. Una VPN stabilisce una connessione sicura e crittografata tra il vostro computer e Internet, fornendo un tunnel privato per i vostri dati e le vostre comunicazioni mentre utilizzate le reti pubbliche.

Come rimanere al sicuro usando la carta di debito o di credito online

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

Cercate il lucchetto: Assicuratevi di fare acquisti su un sito web sicuro, soprattutto quando è il momento di inserire il numero della carta. Cercate l'icona del lucchetto bloccato nel vostro browser e prestate attenzione agli avvisi di sicurezza che compaiono.

Monitorate il vostro conto: È sempre una buona idea tenere sotto controllo il proprio denaro, ed è particolarmente importante se si condividono informazioni sul conto online. Controllate regolarmente i vostri conti: come minimo una volta al mese, anche se è meglio una frequenza maggiore. E impostate degli avvisi sul vostro conto in modo da sapere quando il denaro esce.

Utilizzate connessioni sicure: I dispositivi mobili e la connessione Wi-Fi gratuita facilitano le cose da fare. Ma non si può mai sapere quanto sia sicuro un hotspot pubblico. Se dovete accedere a conti finanziari o digitare numeri di carte di credito, conservate queste operazioni per quando siete a casa o al lavoro e sapete che il vostro traffico è sicuro.

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

Utilizzate siti web familiari

- Iniziate da un sito affidabile. I risultati della ricerca possono essere truccati per portarvi fuori strada, soprattutto quando superate le prime pagine di link. Se conoscete il sito, è probabile che sia meno probabile che si tratti di una fregatura. Sappiamo tutti che Amazon.com offre tutto quello che c'è sotto il sole; allo stesso modo, quasi tutti i principali punti vendita hanno un negozio online, da Target a Best Buy a Home Depot. Attenzione agli errori di scrittura o ai siti che utilizzano un dominio di primo livello diverso (ad esempio, .net invece di .com): questi sono i trucchi più vecchi del mondo. Sì, le vendite su questi siti possono sembrare allettanti, ma è così che vi ingannano per farvi dare i vostri dati.

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

È il momento delle domande...

Sapete come vengono tracciati gli utenti nei motori di ricerca (cronologia delle ricerche, cookie, indirizzi IP, cronologia dei clic)?

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

È ora di rispondere...

Un motore di ricerca può tracciare l'utente attraverso i siti web se i siti visitati contengono script di tracciamento del motore di ricerca come parte della pagina. Ciò che cercate lascia una traccia di informazioni su di voi. Queste informazioni rivelano ciò che vi interessa, ciò che vi incuriosisce e persino ciò che pensate di queste cose.

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

Cercare il lucchetto

- Non acquistate mai nulla online con la vostra carta di credito da un sito che non abbia installato almeno la crittografia SSL (secure sockets layer).
- Saprete se il sito è dotato di SSL perché l'URL del sito inizierà con HTTPS, invece che con HTTP. Apparirà l'icona di un lucchetto chiuso, in genere a sinistra dell'URL nella barra degli indirizzi o nella barra di stato in basso; dipende dal browser.
- L'HTTPS è ormai uno standard anche per i siti non commerciali, tanto che Google Chrome segnala come "non sicura" qualsiasi pagina senza la S aggiuntiva. Quindi un sito che ne è sprovvisto dovrebbe risaltare ancora di più.

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

Social media - gestione sicura delle immagini e delle informazioni online
La nostra sicurezza online e la protezione della nostra privacy

I materiali

Laptop con accesso a Internet per il relatore, lavagna luminosa, penne, pennarelli, lavagna a fogli mobili, foglietti adesivi, fogli A4, pallina da tennis.

Indicazioni stradali

Il relatore divide i partecipanti in gruppi di 4-5 persone e chiede loro di pensare e scrivere su dei cartoncini le risposte alla domanda: cosa possiamo fare per prenderci cura della nostra sicurezza online e proteggere la nostra privacy? Chiede poi ai rappresentanti dei gruppi di leggere le risposte e di scriverle sulla lavagna/flipchart. Dopo aver scritto tutte le risposte, il conduttore chiede ai partecipanti di scegliere la regola che sembra più importante per loro. I volontari dicono agli altri partecipanti perché l'hanno scelta. Vedi sotto:

Inoltre: Riassunto da parte dell'istruttore della classe, discussione sull'impatto dei social media su di noi, sulle opportunità e i rischi di un uso sbagliato dei social media, su cosa possiamo fare per aumentare la nostra sicurezza.
Visione congiunta di tutto o parte del video di You Tube "La verità sui social media"
https://www.youtube.com/watch?v=DU3655oQexw

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

Social media - gestione sicura delle immagini e delle informazioni online
La nostra sicurezza online e la protezione della nostra privacy

Appendice

- Se non siete sicuri dell'interlocutore, non date alcuna informazione su di voi.
- Non rivelate le vostre password ad altri. Organizzatene una che sia difficile da indovinare (non può essere la vostra data di nascita o il vostro nome!). La password non deve contenere meno di 8 caratteri, compresi numeri e lettere maiuscole. Utilizzate password diverse per servizi diversi.
- Non permettete al vostro browser di ricordare le password per le e-mail e i servizi che utilizzate. Effettuate il logout quando avete finito.
- Se utilizzate i social network, assicuratevi di avere le giuste impostazioni sulla privacy. Meno informazioni condividete con gli estranei, meglio è.
- Sui forum di discussione o sui blog, utilizzate un nickname (pseudonimo), non il vostro nome. Evitate di pubblicare online informazioni su di voi.
- Non utilizzate la possibilità di "etichettarvi" automaticamente dove vi trovate.
- Prestate attenzione ai messaggi che compaiono durante il download di giochi e applicazioni per telefoni cellulari e smartphone. Da essi potete apprendere quali sono i vostri dati a cui il servizio scaricato chiede di accedere. Fate attenzione a ciò che accettate.
- Fornite solo i dati necessari per creare un account.
- Invece di seguire Facebook, utilizzate le newsletter e i feed RSS.

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

Non condividere troppo

- Nessun rivenditore online ha bisogno del vostro numero di previdenza sociale o della vostra data di nascita per fare affari.
- Tuttavia, se i truffatori li ottengono, insieme al numero della carta di credito, possono fare molti danni. Più i truffatori sanno, più è facile rubare la vostra identità.
- Quando è possibile, è consigliabile fornire il minor numero possibile di dati personali. I siti più importanti vengono violati di continuo.

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

È il momento delle domande...

Conoscete qualche trucco per evitare che le vostre informazioni vengano tracciate?

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

È ora di rispondere...

Modificate le impostazioni per bloccare i tracker, utilizzare la modalità in incognito, utilizzare una VPN, utilizzare browser privati. Search Encrypt utilizza la crittografia per nascondere la cronologia delle ricerche da altri che potrebbero utilizzare il dispositivo dopo le ricerche.

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

Problemi con gli acquisti online, con le carte e con i trasferimenti di denaro.

Utilizzo sicuro di carte di credito e di debito

I materiali

Telefoni/tablet/laptop con accesso a Internet, proiettore, fogli di carta, penne, cartoncini.

Indicazioni stradali

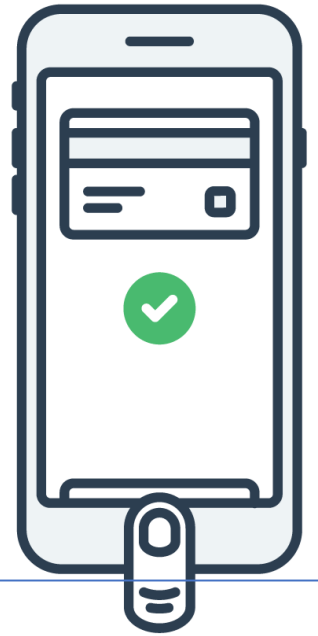
I partecipanti saranno seduti in cerchio. Il formatore scriverà sulla lavagna a fogli mobili le domande guida per i partecipanti, aiutandoli a definire le regole per un uso sicuro delle carte di credito e di debito (appendice sotto).

Appendice

- Utilizzare meglio l'applicazione di pagamento mobile
- Utilizzare le funzioni di sicurezza fornite dall'emittente della carta.
- In caso di smarrimento della carta, informare immediatamente la banca.
- Non mostrate la carta in pubblico.

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

Non usare la carta, usa il telefono



Il pagamento degli articoli con lo smartphone è ormai una consuetudine nei negozi e nei negozi commerciali ed è ancora più sicuro dell'uso della carta di credito.

L'utilizzo di un'applicazione di pagamento mobile come Apple Pay genera un codice di autenticazione per l'acquisto, utilizzabile una sola volta, che nessun altro potrebbe mai rubare e utilizzare.

Inoltre, si evitano gli skimmer di carte di credito e non c'è nemmeno bisogno di portare con sé la carta di credito se si frequentano solo posti che accettano pagamenti via telefono.

Che importanza ha se si fanno acquisti online? Molte applicazioni telefoniche accettano ora i pagamenti con Apple Pay e Google Pay. È sufficiente l'impronta digitale, il volto o il codice di accesso per effettuare il pagamento all'istante.

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

Creare password forti

- Assicurarsi di utilizzare password non decifrabili. Non è mai così importante come quando si fanno operazioni bancarie e acquisti online. I nostri vecchi consigli per creare una password unica possono tornare utili in un periodo dell'anno in cui fare acquisti significa probabilmente creare nuovi account sui siti di e-commerce.
- Anche la vostra password perfetta non è perfetta. La mossa più intelligente è utilizzare un gestore di password che crei per voi password non craccabili. Ne terrà traccia e le inserirà, in modo che voi non dobbiate pensarci.

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Non ho mai...

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

I materiali

Telefoni/tablet/laptop con accesso a Internet, proiettore, fogli di carta, penne, cartoncini.

Indicazioni stradali

- Tutti i partecipanti si dispongono in cerchio. Vengono pronunciate le frasi che iniziano con "Non ho mai..." e i partecipanti che hanno fatto questa affermazione devono fare un passo avanti. Poi tornano al loro posto. Qui ci sono alcuni esempi, ma i partecipanti possono anche dire qualsiasi affermazione vogliano.
- Non ho mai fatto acquisti online
- Non sono mai stato truffato su internet.
- Non ho mai parlato con qualcuno online senza conoscerlo.
- Non ho mai dimenticato le mie password
- Non ho mai ricevuto un'e-mail di spam
- Non sono mai stato attaccato da un malware
- Non ho mai ricevuto un'e-mail che mi chiedesse tutte le mie informazioni personali.
- Non ho mai cercato di scoprire la password di qualcuno.
- Non ho mai sospettato che qualcuno si fosse introdotto in uno dei miei account.
- Non ho mai trovato sul mio telefono una pubblicità di qualcosa che avevo appena cercato.
- Non ho mai sospettato di essere spiato via Internet.
- Non ho mai perseguitato nessuno
- Non ho mai subito cyberbullismo

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Non ho mai...

- Non ho mai fatto cyberbullismo su nessuno
- Non ho mai avuto accesso a siti web sospetti
- Non ho mai scaricato un virus mentre cercavo di scaricare qualcos'altro.
- Non ho mai dovuto cambiare tutte le mie password.
- Non ho mai dovuto cambiare la mia carta di credito perché i suoi dati erano stati divulgati.
- Non ho mai fatto finta di essere qualcun altro su Internet.
- Non ho mai ignorato le regole per mantenere una password sicura.
- Non ho mai partecipato a una finta lotteria su Internet.
- Non ho mai perso tutto il mio lavoro o qualcosa di importante perché non avevo una copia di backup.
- Non ho mai cliccato su un banner che diceva che avevo vinto un premio.
- Non ho mai navigato nel Deep Web
- Non ho mai condiviso informazioni private sui social media.
- Non ho mai condiviso immagini imbarazzanti su Internet.
- Non ho mai postato commenti offensivi su Internet.
- Non ho mai ricevuto commenti offensivi su Internet.
- Non ho mai cercato di scoprire le informazioni private di qualcuno.
- Non ho mai usato l'autenticazione in due fasi.
- Non ho mai usato una VPN
- Non mi sono mai sentita insicura su Internet.

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

Perdita di dati personali, creazione di password forti, organizzatori di password
Gioco: Non ho mai...

Cosa sta succedendo?

Gioco Non ho mai. Sui temi di Internet.
Tutti i partecipanti si dispongono in cerchio. Vengono pronunciate le frasi che iniziano con "Non ho mai..." e i partecipanti che hanno fatto questa affermazione devono fare un passo avanti. Poi tornano al loro posto. Ci sono alcuni esempi, ma possono anche dire qualsiasi affermazione venga loro in mente.

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

Privatizzate il vostro Wi-Fi

- Se fate acquisti tramite un hotspot pubblico, limitatevi alle reti conosciute, anche se gratuite, come quelle presenti nei negozi Starbucks o Barnes & Noble.
- In genere ci si può fidare di tutti i provider presenti nella nostra raccolta dei Wi-Fi gratuiti più veloci a livello nazionale, ma per sicurezza è consigliabile utilizzare anche una rete privata virtuale (VPN) (ecco perché).

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.

Test CRAAP - Presentazione

I materiali

telefoni/tablet/laptop con accesso a Internet, lavagna luminosa, penne, pennarelli, lavagna a fogli mobili, foglietti adesivi, fogli A4.

Indicazioni stradali

Presentazione dello strumento di verifica delle informazioni (test CRAAP), a cosa serve e come si usa (allegato sotto) insieme alla presentazione.

Appendice

Il test CRAAP è un test sull'affidabilità oggettiva delle fonti di informazione in varie discipline scientifiche. CRAAP è un acronimo che sta per currency, relevance, authority, accuracy e purpose. Il test CRAAP è stato ideato per aiutare gli insegnanti e i partecipanti a determinare se le loro fonti possono essere attendibili. Utilizzando il test nella valutazione delle fonti, il ricercatore può ridurre la probabilità di utilizzare informazioni inaffidabili. Il test CRAAP, sviluppato da Sarah Blakeslee e dal suo team di bibliotecari della California State University, Chico (CSU Chico), è utilizzato principalmente dai bibliotecari dell'istruzione superiore. È uno dei vari approcci alla critica delle fonti.

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.

Test CRAAP - Presentazione

Si può essere tentati di utilizzare nel proprio articolo qualsiasi fonte che sembri essere d'accordo con la propria tesi, ma ricordate che non tutte le informazioni sono buone informazioni, soprattutto in un ambiente online.
Sviluppato dai bibliotecari della California State University-Chico, il test CRAAP è un'utile lista di controllo da utilizzare per valutare una risorsa online (o qualsiasi altra risorsa). Il test fornisce un elenco di domande da porsi per decidere se una risorsa è sufficientemente affidabile e degna di fiducia per essere utilizzata in un documento di ricerca.
Il test CRAAP è l'acronimo di: Valuta, Rilevanza, Autorità, Accuratezza e Scopo.
Non è facile stabilire se una fonte è affidabile e può essere utilizzata come strumento di ricerca. Il test consente di risparmiare il tempo e l'energia necessari per valutare i contenuti disponibili su Internet.

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.

Test CRAAP - Presentazione

Le risorse devono passare attraverso cinque fasi di verifica.
Valuta - tempestività delle informazioni
L'ora in cui le informazioni sono state pubblicate o postate, se le informazioni sono state aggiornate o corrette e se il link funziona o meno.
Rilevanza - la rilevanza delle informazioni
Verifica se le informazioni sono correlate all'argomento, se la risorsa è rilevante e se può essere utilizzata nel lavoro accademico.
Autorità
Crea fiducia fornendo dettagli sull'autore e sull'editore prima di fidarsi delle informazioni e del sito web.
Precisione
Prestate attenzione all'accuratezza del contenuto. Le informazioni devono essere basate su prove presentate al pubblico. È necessario controllare il tono della lingua, gli errori grammaticali e altri errori tipografici.
Scopo delle informazioni
Determinare gli scopi dell'informazione: informare, insegnare, vendere, intrattenere o persuadere.

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.

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

Test CRAAP - Quiz

I materiali

telefoni/tablet/laptop con accesso a Internet, lavagna luminosa, penne, pennarelli, lavagna a fogli mobili, foglietti adesivi, fogli A4.

Indicazioni stradali

Dividete il gruppo in squadre di circa 4 persone. Chiedete a ogni squadra di trovare un articolo su un argomento a scelta. Scegliete un argomento adatto al gruppo (appendice sotto). Distribuite i test craap stampati (appendice sotto) e consegnateli a ogni persona. Chiedete ai partecipanti di leggere l'articolo, poi fateli analizzare l'intero testo alla luce delle domande incluse nel test. Sul lato destro hanno a disposizione uno spazio per pensieri/conclusioni/risposte. In base al test, determineranno l'attendibilità dell'articolo. Non c'è una scala di valutazione o un numero di punti.

Le persone lavorano "online" sul materiale ricevuto, il che significa che possono condurre un'analisi approfondita del materiale - conoscere l'intero articolo, esaminare la fonte in modo più dettagliato, verificare i dati utilizzati, imparare qualcosa sull'autore, ecc. È importante che verifichino, utilizzando i criteri indicati nel craap test, se il materiale è credibile, quali elementi indicano la credibilità e quali la compromettono. I partecipanti possono anche scrivere i loro pensieri, il che faciliterà la discussione. Chiedete a ogni gruppo di presentare brevemente i risultati della loro analisi.

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.

Test CRAAP - Quiz

Appendice

Argomenti per i gruppi:
Il clima
Coronavirus
Rifugiati
Vaccini
Celebrità
Sport
Unione Europea

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.

Test CRAAP - Quiz

		Note / risposte
Valuta tempestività informazioni	Quando sono state pubblicate le informazioni?	
	Le informazioni (se non nuove) sono state aggiornate?	
	Il caso per il quale state esaminando queste informazioni richiede dati più recenti e aggiornati o potete fare affidamento su materiale più vecchio?	
	I link (se presenti) postati nelle informazioni funzionano?	
Rilevanza materialità delle informazioni in relazione a le vostre esigenze	Le informazioni si riferiscono all'argomento che state trattando o rispondono a una domanda importante per voi?	
	Per chi sono state preparate le informazioni? Per quale gruppo target?	
	Le informazioni sono di livello adeguato alle vostre esigenze? Sono troppo basilari e generiche o troppo avanzate e dettagliate?	
	Avete controllato altre fonti di informazione prima di decidere di usare solo questa?	

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.

Test CRAAP - Quiz

Autorità origine delle informazioni	**Chi è l'autore, l'editore, la fonte o lo sponsor delle informazioni?**	
	Quali sono le credenziali dell'autore delle informazioni? A quale organizzazione, ente o istituzione è affiliato?	
	L'autore è qualificato per scrivere su questo argomento?	
	È possibile trovare informazioni di contatto, ad esempio il nome dell'editore, l'indirizzo e-mail e così via, accanto alle informazioni?	
	L'indirizzo del sito Web in cui sono apparse le informazioni dice qualcosa sull'autore o sul mittente (ad esempio, l'URL termina con .com, .edu, .gov)?	
Precisione affidabilità, veridicità e accuratezza delle informazioni	Da dove provengono le informazioni?	
	Le informazioni fornite sono supportate da prove?	
	Le informazioni sono state sottoposte a revisione paritaria o citate (si applica principalmente agli articoli scientifici)?	
	Siete in grado di confermare almeno alcune delle informazioni fornite da un'altra fonte o utilizzando le vostre conoscenze?	
	Il linguaggio o la pronuncia di tutte le informazioni indicano imparzialità e sono privi di coloriture emotive?	
	Ci sono errori ortografici, grammaticali o stilistici nella situazione?	

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

Fake news - ovvero ricerca su Internet, verifica delle informazioni fornite dai media.

Test CRAAP - Quiz

Scopo scopo di le informazioni, il motivo per cui sono state create	Per cosa sono state create le informazioni? Per educare, informare, intrattenere, persuadere?
	L'autore o la persona che finanzia la creazione delle informazioni ha chiarito lo scopo delle stesse?
	L'informazione è una citazione o una descrizione di fatti, presenta un'opinione o ha un carattere propagandistico?
	Il punto di vista presentato nelle informazioni dà l'impressione di imparzialità e obiettività?
	Vedete nelle informazioni elementi che indicano pregiudizi, prese di posizione particolari su questioni legate alla politica, alla religione, alla visione del mondo o, per esempio, la presentazione della prospettiva di una sola istituzione o persona?