Erasmus+

GoDIGITAL

Testo epanso

SPOŁECZNA AKADEMIA NAUK
UNIVERSITY OF SOCIAL SCIENCES
EUnipartners
PUBLICA FIDES
Emphasys CENTRE

2.2.1 ARGOMENTO 1: SICUREZZA INTERNET

2.2.1 ARGOMENTO 1: SICUREZZA INTERNET

Internet potrebbe essere paragonato all'oceano. L'oceano può essere un posto molto pericoloso: le persone possono essere perse o affogate cercando di godersi il mare o esplorare la sua incantevole immensità. Ma la madre nella fotografia non proibisce il contatto dei suoi figli con il mare. Invece, li tiene in contatto con lei e insegna loro a godersela spiegando alcune regole per un "uso" sicuro del mare. All'inizio si trova accanto a loro e li consiglia in modo che acquisiscano gradualmente l'autonomia e possano godersi il mare in un secondo momento.

Questo è il modo in cui dovremmo pensare all'uso di Internet. Dobbiamo identificare i potenziali pericoli di Internet diffusa e acquisire conoscenze e modi per evitare tutti i possibili rischi. È quindi necessario introdurre i giovani studenti all'adozione di buone pratiche in relazione all'uso sicuro di Internet.

I rischi su Internet sono di molti tipi. Delineiamo dieci (10) dei rischi più importanti:

1. Dipendenza da Internet e alienazione degli utenti dal mondo reale

2. Contenuti inappropriati e offensivi del sito web

Erasmus+

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

3. Messaggi indesiderati (spam)

4. Bullismo su Internet

5. Seduzione elettronica degli utenti - Segnalazione di pedopornografia, gioco d'azzardo online, giochi violenti e altri comportamenti dannosi

6. Violazione della privacy dell'utente

7. Disinformazione diffusa su Internet (notizie false, miti urbani, scherzi digitali)

8. Intercettazione di dati personali tramite "phishing" e "pharming"

9. Software dannoso che infetta i PC

10. Condizioni fisiche derivanti dall'uso prolungato di computer.

Crediamo che oggigiorno la conoscenza teorica di quanto sopra non sia sufficiente per un insegnante. Richiede familiarità e conoscenza pratica. Per questo motivo, nei paragrafi seguenti verranno sviluppati alcuni problemi tecnici, in modo che gli utenti e gli insegnanti, in particolare, possano essere sensibili, ma anche reagire, ai possibili rischi online e possono essere in grado di proteggere ed educare i loro studenti di conseguenza fin dalla giovane età.

2.2.1.1 Come evitare i siti danneggiati

Prima di iniziare a introdurre modi per evitare i siti Web "cattivi", dobbiamo rispondere alla domanda: cosa è considerato un sito "cattivo"? Un sito "cattivo" è generalmente considerato come qualsiasi sito web contenente materiale che rientri nelle categorie da 1 a 8 presentate nell'introduzione sopra.

Alcuni dei modi per evitare questo tipo di siti Web sono i seguenti:

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

• **Utilizzare i filtri Internet**

Esistono molti filtri Internet che si può acquistare o scaricare, che impediscono a lui / lei o ai membri della sua famiglia di aprire siti discutibili. Questi filtri funzionano nel impedire l'accesso dell'utente a siti ritenuti discutibili dal punto di vista della sicurezza o che presentano contenuti inappropriati o **NSFW**(non sicuri per il lavoro). Molti genitori usano questi filtri per assicurarsi che i loro figli stiano usando solo siti adatti all'età, ma persone di tutte le età, così come insegnanti, possono usarli per assicurarsi che le loro ricerche sul web siano sempre al sicuro.

• **Approfittare dei filtri integrati dei motori di ricerca**

Molti motori di ricerca offrono agli utenti di Internet la possibilità di scegliere una ricerca "più sicura" quando utilizzano i loro servizi. Ad esempio, Google offre "filtro di ricerca sicuro". Questo vale per tutte le ricerche di immagini e video, nonché per le notizie e i contenuti di ricerca generali.

• **Non indovinare l'indirizzo di un sito Web**

Questo è probabilmente il primo modo in cui le persone si mettono nei guai. Esistono molti siti che utilizzano indirizzi Web simili ai siti Web legittimi in modo che quando le persone cercano di ricordare quale sito visitare, finiscono per visitare il sito sbagliato per errore.

• **Non cliccare mai su siti che sembrano discutibili**

Quando qualcuno è in dubbio, puo decidere di non non fare clic. Se la descrizione del sito, il titolo o l'URL sembrano in qualche modo "sbagliato" a lui / lei, lui / lei può trovare un altro sito che è più stimabile, specialmente quando usa quel sito in una capacità di ricerca.

2.2.1.2 Introduzione al malware: come evitare

Il rischio numero 9 nell'introduzione parla del malware. Il malware è un termine utilizzato per software dannoso progettato per fare danni o azioni indesiderate a un sistema informatico. Esempi di malware includono: virus, worm, trojan, spyware e software di sicurezza corrotto.

Ecco una breve descrizione di ciascuno di questi tipi di software dannoso in modo che l'insegnante abbia familiarità con la terminologia e in particolare con il modo in cui funziona ciascuno di questi software.

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

• Virus informatici

Un virus informatico è un piccolo programma software che si diffonde da un computer a un altro e interferisce con il funzionamento del computer. Un virus informatico potrebbe corrompere o eliminare dati su un computer, utilizzare un programma di posta elettronica per diffondere il virus su altri computer o persino eliminare tutto sul disco rigido.

I virus informatici sono spesso diffusi dagli allegati nei messaggi di posta elettronica o dai messaggi di messaggistica istantanea. Pertanto, l'utente non deve mai aprire un allegato a meno che non sappia chi ha inviato il messaggio. I virus possono essere mascherati come allegati di immagini divertenti, biglietti di auguri o file audio e video. I virus informatici si diffondono anche attraverso il download su Internet. Possono essere nascosti in software piratati o in altri file o programmi che qualcuno potrebbe scaricare.

- **Computer worms**

A worm is computer code that spreads without user interaction. Most worms begin as email attachments that infect a computer when they're opened. The worm scans the infected computer for files, such as address books or temporary webpages, that contain email addresses. The worm uses the addresses to send infected email messages, and frequently mimics (or spoofs) the "From" addresses in later email messages so that those infected messages seem to be from someone you know. Worms then spread automatically through email messages, networks, or operating system vulnerabilities, frequently overwhelming those systems before the cause is known. Worms aren't always destructive to computers, but they usually cause computer and network performance and stability problems.

• I Trojan horse

Un Trojan Horse è un programma software dannoso che si nasconde all'interno di una pagina altri programmi. Entra in un computer nascosto all'interno di un programma legittimo, come uno screen saver. Quindi inserisce il codice nel sistema operativo che consente a un hacker di accedere al computer infetto. I cavalli di Troia di solito non si diffondono da soli. Sono diffuse da virus, worm o software scaricato.

• Spyware

Gli spyware possono essere installati su un computer senza che gli utenti ne siano a conoscenza. Questi programmi possono modificare la configurazione del computer o raccogliere dati pubblicitari

Erasmus+

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

e informazioni personali. Lo spyware può tracciare le abitudini di ricerca su Internet e può anche reindirizzare il browser web a un sito Web diverso da quello su cui l'utente intende navigare.

• Software di sicurezza corrotta

Un programma software di sicurezza corrotta cerca di far credere all'utente che il suo computer sia stato infettato da un virus e di solito spinge lui/ lei a scaricare o acquistare un prodotto che rimuove il virus. I nomi di questi prodotti contengono spesso termini come Antivirus, Shield, Security, Protection o Fixer. Questo li fa sembrare legittimi. Spesso vengono eseguiti subito dopo che qualcuno li ha scaricati o la volta successiva che il computer viene avviato. Il software di sicurezza non autorizzato può impedire l'apertura di applicazioni come Internet Explorer. Il software di sicurezza corrotta potrebbe anche fare passare come infezioni i file di Windows che sono legittimi e importanti.

Per evitare tutti questi tipi di malware, l'utente dovrebbe familiarizzare con alcune tecniche come:

• Installare programmi antivirus di qualità

• Installare la protezione anti-spyware in tempo reale

• Tenere aggiornate le applicazioni anti-malware

• Esegui scansioni quotidiane

• Disabilitare l'esecuzione automatica

• Disabilitare le anteprime delle immagini in Outlook

• Evitare di fare clic sui collegamenti e-mail o sugli allegati

• Navigare in modo intelligente

• Utilizzare un firewall basato su hardware

• Distribuire la protezione DNS

Tuttavia, il malware può essere prevenuto con un comportamento intelligente. Il singolo più grande fattore nel prevenire un'infezione da malware su un PC è l'utente stesso. Gli utenti di PC non hanno bisogno di conoscenze specialistiche o di formazione specifica. Devono solo essere vigilanti per evitare di scaricare e installare qualsiasi cosa che non capiscono o di cui non si fidano, non importa quanto allettanti, dalle seguenti fonti:

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

• **Da un sito Web:** se non si è sicuri, lasciare il sito e ricercare il software che si sta chiedendo di installare. Se va bene, puoi sempre tornare al sito e installarlo. Se non va bene, eviterai un mal di testa da malware.

• **Da e-mail:**non fidarti di nulla associato a una e-mail di spam. Avvicinarsi con cautela alle e-mail da persone che conosci quando il messaggio contiene collegamenti o allegati. Se sei sospettoso di ciò che ti viene chiesto di visualizzare o installare, non farlo.

• **Dai mezzi fisici:**i tuoi amici, familiari e associati potrebbero inconsapevolmente fornirti un disco o un'unità flash con un file infetto. Non accettare inconsciamente questi file; scannerizzali con un software di sicurezza. Se non sei ancora sicuro, non accettare i file.

• **Da una finestra pop-up:**alcune finestre o finestre a comparsa tenteranno di indirizzarti verso il download di software o l'accettazione di una "scansione di sistema" gratuita di qualche tipo. Spesso questi pop-up impiegano tattiche intimidatorie per farti credere che hai bisogno di ciò che stanno offrendo per essere al sicuro. Chiudi il pop-up senza fare clic su alcun elemento al suo interno (inclusa la X nell'angolo). Chiudi la finestra tramite Task Manager di Windows (premi Ctrl-Alt-Canc).

• **Da un altro elemento di software:**alcuni programmi tentano di installare malware come parte del loro processo di installazione. Quando si installa il software, prestare molta attenzione alle finestre di messaggi prima di fare clic su Avanti, OK o Accetto. Esegui la scansione del contratto utente per qualsiasi cosa che suggerisca che il malware possa far parte dell'installazione. In caso di dubbi, annullare l'installazione, controllare il programma ed eseguire nuovamente l'installazione se si è certi che sia sicuro.

• **Da servizi di condivisione di file illegali:** sei da solo se entri in questo reame. Non c'è controllo di qualità nel mondo del software illegale, ed è facile per un utente malintenzionato nominare un pezzo di malware dopo un film, un album o un programma popolare per tentart a scaricarlo.

2.2.1.3. Come rimuovere il malware

Se qualcuno sospetta un malware o se vuole solo stare attento, ci sono alcuni passi da fare.

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

Come rimuovere il malware

Se qualcuno sospetta un malware o se vuole solo stare attento, ci sono alcuni passi da fare.

a) Eseguire il backup di tutti i file e altri dati

File e dati sono fondamentali. Pertanto, nel momento in cui qualcuno si rende conto che il suo computer è infetto da malware, deve eseguire il backup di tutti i file e altri dati, prima che il malware raggiunga quei file e altri dati e li corrompa. Inoltre, tale backup aiuterà a tornare rapidamente in pista.

b) Disconnettersi da Internet

La cosa migliore da fare è disconnettere il PC da Internet per prevenire ulteriori danni, visto che Internet è il terreno fertile del malware. E ogni momento in cui l'utente rimane connesso, specialmente dopo un'infezione da malware, peggiorerà la sua situazione.

c) Fare la scansione del computer in modalità provvisoria

Passare alla modalità provvisoria e scansionare il computer. Senza essere troppo tecnico, la modalità sicura è una modalità limitata che consente solo l'esecuzione di applicazioni sane, riducendo il rischio di diffusione di malware ad altre parti del PC. Nel migliore dei casi, una tale pulizia può migliorare le prestazioni del PC. Un'altra misura semplice ma efficace sarebbe quella di ripulire il file temporaneo e scaricati.

d) Utilizzare lo strumento di rimozione malware

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

Se non ce n'è già uno, scarica un legittimo programma anti-malware. Quindi, installalo ed eseguilo. Programmi come questi sono progettati per cercare ed eliminare qualsiasi malware su un dispositivo.

Una volta che il dispositivo è pulito, è una buona idea cambiare le password, non solo per il PC o dispositivo mobile, ma anche per e-mail, per account di social media, per i siti di shopping preferiti e per le operazioni bancarie online e le fatturazione online.

Rimuovere malware non è né un compito semplice né piacevole. Quindi è meglio lasciare che gli esperti gestiscano la situazione se qualcuno pensa di non poter risolvere il problema da solo.

2.2.1.4 Protezione degli account Internet

Le password sono come le chiavi della nostra casa personale online. Dovremmo fare tutto ciò che possiamo per impedire alle persone di accedere alla nostra password. Possiamo proteggere ulteriormente i nostri account utilizzando metodi di autenticazione aggiuntivi. Alcuni suggerimenti principali sono:

- Chiudi gli account che non stai utilizzando da molto tempo
- Crea una password sicura (ad esempio, imposta la password come frase)
- Account unico - password unica
- Annotarlo e tenerlo al sicuro
- Cambia le tue password regolarmente
- Blocca accesso (autenticazione forte)
- Controlla l'attività del tuo account
- Tieni aggiornato il tuo software
- Specifica i tuoi contatti fidati

Altre idee sulla sicurezza in Internet sono disponibili nella letteratura aggiuntiva proposta.

2.2.1.5 GDPR

Un altro importante problema che gli insegnanti dovrebbero conoscere è il GDPR. Il regolamento generale sulla protezione dei dati ("GDPR") è un regolamento nella legislazione dell'UE sulla

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543

protezione dei dati e sulla privacy per tutti gli individui all'interno dell'Unione europea (UE) e dello Spazio economico europeo (SEE). Affronta anche l'esportazione di dati personali al di fuori delle aree UE e SEE. Il GDPR mira principalmente a dare il controllo alle persone sui loro dati personali e a semplificare il contesto normativo per gli affari internazionali unificando il regolamento all'interno dell'UE. Il regolamento contiene disposizioni e requisiti relativi al trattamento dei dati personali degli individui (formalmente denominati soggetti dei dati nel GDPR) all'interno del SEE e si applica a un'impresa stabilita nel SEE o - indipendentemente dalla sua ubicazione e dalla cittadinanza degli interessati - che sta elaborando le informazioni personali degli interessati all'interno del SEE.

I responsabili dei dati personali devono adottare misure tecniche e organizzative adeguate per attuare i principi di protezione dei dati. I processi aziendali che gestiscono i dati personali devono essere progettati e costruiti tenendo conto dei principi e fornire salvaguardie per proteggere i dati (ad esempio utilizzando la pseudonimizzazione o la completa anonimizzazione, ove appropriato) e utilizzare le impostazioni di privacy più elevate possibile per impostazione predefinita, in modo che i dati non siano disponibili pubblicamente senza il consenso esplicito e informato e non possono essere utilizzato per identificare un argomento senza ulteriori informazioni memorizzate separatamente. Nessun dati personali possono essere elaborati a meno che non sia fatto secondo una base legale specificata dal regolamento, o a meno che il responsabile del trattamento non abbia ricevuto un'affermazione univoca e individualizzata del consenso dell'interessato. L'interessato ha il diritto di revocare questo consenso in qualsiasi momento. (Da Wikipedia, l'enciclopedia libera)

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.
Submission Number: 2017-1-PL01-KA201-038543