MIG-DHL

Migrants Digital Health Literacy

Manuale

Modulo 6

Essere attivi nell'ambiente della salute digitale

Authors:

Josemar Alejandro Jimenez, Oxfam; Jenny Wielga, IAT

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

Il sostegno della Commissione europea alla realizzazione di questa pubblicazione non costituisce un'approvazione dei contenuti, che riflettono esclusivamente le opinioni degli autori. La Commissione non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in essa contenute. Numero del progetto: 2020-1-DE02-KA204-007679.

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

MIG-DHL
Migrants Digital Health Literacy

Questo manuale per il modulo 6 fa parte del programma MIG-DHL, che contiene 6 moduli di apprendimento in totale, sviluppati nell'ambito del partenariato strategico Erasmus+ **MIG-DHL- Migrants Digital Health Literacy.**

I contenuti della formazione in sintesi:

Programma MIG-DHL

- Modulo 1: Che cos'è la *Digital Health Literacy* (alfabetizzazione sanitaria digitale)?
- Modulo 2: I principali problemi di salute quando si arriva in un nuovo paese
- Modulo 3: I servizi sanitari
- Modulo 4: Diventare digitalmente alfabetizzati
- Modulo 5: Esplorazione degli strumenti per la salute digitale
- **Modulo 6: Essere attivi nell'ambiente della salute digitale**

Ulteriori informazioni sono disponibili sul sito web: https://mig-dhl.eu/

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

MIG-DHL Migrants Digital Health Literacy

Dichiarazione sul copyright:

Contenuto

6. Essere attivi nell'ambiente della salute digitale

Riteniamo che una delle principali competenze per essere attivi nell'ambiente digitale è quella relativa al sapere come proteggere i propri dati personali quando si naviga su Internet: abbiamo evidenziato nei precedenti moduli come la tutela della privacy contribuisca a proteggere la propria salute fisica e psicologica.

Pertanto questo modulo si concentra sull'analisi delle competenze necessarie alla tutela della privacy. Le informazioni contenute in questo modulo fanno seguito agli argomenti già trattati nel Modulo 4 e sono legate allo sviluppo di competenze in materia di sicurezza e privacy. Queste competenze si riferiscono alla capacità di proteggere dispositivi, contenuti, dati personali e privacy nell'ambiente digitale.

Questa parte è correlata all'area di competenza 4 "Sicurezza" di DigiComp, che è già stata introdotta nel modulo 4.

6.1 Protezione della privacy e dei dati personali nell'ambiente digitale

Esistono diversi fattori di rischio nell'ambiente digitale che riguardano la privacy e i dati personali. Riportiamo in questo paragrafo alcuni dei principali tra questi fattori, che sono evidenziati anche nei materiali di formazione.

6.1.1 Hacking

Con il termine "hacking" si fa riferimento ad attività mirate a compromettere dispositivi digitali, come computer, smartphone, tablet e persino intere reti. Sebbene le attività di "hacking" non sempre sono compiute a scopo malevolo, al giorno d'oggi la maggior parte dei riferimenti a questa e agli hacker la caratterizzano come un'attività illegale, in gran parte compiuta da criminali informatici e motivata da fattori quali il guadagno finanziario, la raccolta di informazioni (spionaggio) o anche solo per il "divertimento" della sfida alle istituzioni.

L'*hacking* è tipicamente di natura tecnica, ma gli hacker possono anche usare la psicologia per indurre l'utente a cliccare su un allegato dannoso o a fornire dati personali.

In effetti, è corretto definire l'*hacking* come un termine generale che racchiude le attività che stanno dietro alla maggior parte dei *malware* e gli attacchi informatici dannosi al pubblico informatico, alle aziende e ai governi. Le tecniche di *hacking* più comuni (i loro termini tecnici vengono riportati in inglese, ndr) includono:

- Botnets
- Browser hijacks
- Denial of service (DDoS) attacks
- Ransomware
- Rootkits
- Trojan
- Virus
- Worms

Tipologia di *hacking/hackers*

In linea di massima, si può dire che gli *hacker* tentano di introdursi nei computer e nelle reti principalmente per quattro motivi:

- Il guadagno economico criminale, ovvero il furto di numeri di carte di credito o la frode ai sistemi bancari.
- Il guadagno di credibilità e di reputazione all'interno della *sottocultura hacker* motiva alcuni hacker a lasciare il proprio marchio sui siti web che vengono vandalizzati come prova del fatto che hanno effettuato l'hacking.
- In ambito di spionaggio aziendale, quando gli hacker contrattati da un'azienda cercano di rubare informazioni sui prodotti e i servizi di un concorrente per ottenere un vantaggio sul mercato.

Misure di prevenzione da attività di *hacking*

- Protezione *anti-malware*: si può fare riferimento a prodotti (o applicazioni per il telefono) *anti-malware* affidabili, in grado di rilevare e neutralizzare il *malware* e di bloccare le connessioni a siti web di *phishing* dannosi.

- Attenzione alle app: si consiglia di scaricare le *app* del telefono solo dai mercati legittimi, come Google Play e Amazon Appstore, che hanno forti politiche di controllo sulle potenziali applicazioni portatrici di *malware* (si noti che la politica di Apple limita gli utenti di iPhone a scaricare solo dall'App Store). Tuttavia, ogni volta che scaricate un'applicazione, controllate prima le valutazioni e le recensioni. Se la valutazione è bassa e il numero di download è basso, è meglio evitarla.
- Proteggete le vostre informazioni: sappiate che nessuna banca o sistema di pagamento online vi chiederà mai le credenziali di accesso, il numero di previdenza sociale o il numero della carta di credito tramite e-mail.
- Aggiornate il vostro software: sia che usiate il telefono o il computer, assicuratevi che il vostro sistema operativo sia sempre aggiornato.
- Navigate con attenzione: Evitate di visitare siti web non sicuri e non scaricate mai allegati non verificati o cliccate su link in e-mail sconosciute.
- Sicurezza delle password: tutte le azioni sopra descritte rappresentano le misure di base di protezione, ma chi compie attività di hacking è sempre alla ricercar di nuove vie d'accesso di violazione dei sistemi altrui. Se un hacker scopre una delle vostre password che utilizzate per più servizi, ha a disposizione applicazioni che possono violare anche gli altri account a voi collegati. Per questo motivo le vostre password devono essere lunghe e complicate, evitate di usarne una uguale per diversi account e utilizzate un gestore di password (Malwarebytes, 2020).

6.1.2 Virus del Computer

Il virus informatico è una delle forme più comuni di *hacking*. In analogia ai meccanismi epidemiologici in biologia, il virus informatico è progettato per diffondersi da un dispositivo all'altro e ha la capacità di replicarsi. Allo stesso modo in cui i virus influenzali non possono riprodursi senza una cellula ospite, i virus informatici non possono riprodursi e diffondersi senza un elemento di programmazione, come ad esempio un file o un documento.

In termini più tecnici un virus informatico è un tipo di codice o programma dannoso scritto per alterare il funzionamento di un computer e progettato per diffondersi da un computer

all'altro. Un virus opera inserendosi o attaccandosi a un programma o documento legittimo che supporta le macro per eseguire il suo codice. Nel processo un virus può potenzialmente causare effetti imprevisti o dannosi, come danneggiare il software di sistema corrompendo o distruggendo i dati.

Come attacca un virus informatico? Una volta che un virus si è attaccato con successo a un programma, a un file o a un documento, il virus rimane inattivo finché le circostanze non fanno sì che il computer o il dispositivo esegua il suo codice. Affinché un virus colpisca il computer, è necessario eseguire il programma infetto, che a sua volta causa l'esecuzione del codice del virus. Ciò significa che un virus può rimanere inattivo sul computer, senza mostrare segni o sintomi importanti. Tuttavia, una volta infettato il computer, il virus può infettare altri computer collegati alla stessa rete. Rubare password o dati, registrare i tasti premuti, corrompere i file, inviare spam ai vostri contatti e-mail e persino prendere il controllo del vostro computer sono solo alcune delle cose devastanti che un virus può fare. Mentre alcuni virus possono essere giocosi nelle intenzioni e negli effetti, altri possono avere effetti profondi e dannosi. Ad esempio, possono cancellare i dati o causare danni permanenti al disco rigido. Peggio ancora, alcuni virus sono progettati con finalità di lucro.

Come si diffondono i virus informatici? In un mondo costantemente connesso è possibile contrarre un virus informatico in molti modi, alcuni più ovvi di altri.

I virus possono essere diffusi attraverso gli allegati di e-mail e messaggi di testo, i download di file da Internet e i link dei social media. I dispositivi mobili e gli smartphone possono essere infettati da virus mobili attraverso il download di applicazioni illegali. I virus possono nascondersi sotto forma di allegati di contenuti condivisibili sui social, come immagini divertenti, biglietti d'auguri o file audio e video. Per evitare di entrare in contatto con un virus, è importante prestare attenzione quando si naviga in rete, si scaricano file e si aprono link o allegati. Per essere sicuri non scaricate mai allegati di testo o e-mail da fonti non conosciute o file da siti web di cui non vi fidate.

Quali sono i segni principali relativi la presenza sul dispositivo di un virus informatico? L'attacco di un virus informatico può produrre una serie di sintomi. Eccone alcuni:

- Frequenti finestre pop-up. I pop-up possono incoraggiare l'utente a visitare siti insoliti. Oppure potrebbero invitare l'utente a scaricare programmi antivirus o altri software.
- Modifiche alla homepage. La vostra homepage abituale potrebbe venire modificata e rilanciare ad esempio un differente sito web. Inoltre potreste non essere in grado di reimpostarla.
- Invio massiccio di e-mail dal vostro account di posta elettronica. Un criminale informatico potrebbe prendere il controllo del vostro account o inviare e-mail a vostro nome da un altro computer infetto.
- Frequenti *crash*. Un virus può danneggiare gravemente il disco rigido. Ciò può causare il blocco o l'arresto del dispositivo. Può anche impedire al dispositivo di riaccendersi.
- Prestazioni del computer insolitamente lente. Un'improvvisa variazione della velocità di elaborazione potrebbe segnalare la presenza di un virus nel computer.
- Programmi sconosciuti che si avviano all'accensione del computer. Il programma sconosciuto può essere notato all'avvio del computer. Oppure potreste notarlo controllando l'elenco delle applicazioni attive del computer.
- Attività insolite come il cambio di password. Questo potrebbe impedire l'accesso al computer.

Come contribuire alla protezione dai virus informatici? Come potete contribuire a proteggere i vostri dispositivi dai virus informatici? Ecco alcune delle cose che potete fare per mantenere il vostro computer al sicuro.

- Utilizzate un prodotto antivirus affidabile e tenetelo aggiornato con le ultime definizioni di virus.
- Evitate di fare clic su qualsiasi pubblicità a comparsa.
- Esaminate sempre gli allegati di posta elettronica prima di aprirli.
- Eseguire sempre una scansione dei file scaricati con i programmi di condivisione dei file (Norton, 2020).

6.1.3 Furto di dati

(Si intendono inclusi: Furto di identità associata, informazioni sul conto della carta di credito, credenziali del cliente)

Il furto di dati rappresenta l'atto di rubare informazioni digitali memorizzate su computer, server o dispositivi elettronici di una vittima sconosciuta con l'intento di compromettere la privacy o ottenere informazioni riservate. Le informazioni possono includere qualsiasi cosa, dalle informazioni finanziarie, come i numeri delle carte di credito o i conti bancari, alle informazioni personali, come i numeri di previdenza sociale, i numeri di patente e i dati sanitari.

Come avviene il furto di dati? Il furto di dati può avvenire in diversi modi. Il più delle volte avviene perché qualcuno si è introdotto in un sistema informatico per rubare informazioni sensibili, come la carta di credito o i dati personali, oppure perché un dipendente di un'azienda ha gestito male le informazioni. In un mondo sempre più digitale, centinaia di aziende e organizzazioni diverse detengono i vostri dati personali, come il numero di previdenza sociale, l'indirizzo postale, la data di nascita e le informazioni sul conto bancario.

Come proteggersi? Il furto di dati è un problema reale e può capitare a chiunque. Anche se non c'è modo di prevenire completamente il furto di dati, ci sono diverse misure che potete adottare oggi per limitare il rischio.

- Utilizzate una carta di credito o di debito con tecnologia *pin-and-chip*.
- Proteggete il vostro computer da virus e *malware* installando, utilizzando e aggiornando software antivirus e *anti-spyware* su tutti i vostri computer e dispositivi elettronici.
- Mantenete aggiornati tutti i sistemi operativi e i programmi software installando regolarmente gli aggiornamenti per la sicurezza, i browser web, i sistemi operativi e i programmi software non appena sono disponibili.
- Non aprite e-mail o allegati di dubbia provenienza perché potrebbero essere e-mail di *phishing*.

- Controllate regolarmente gli estratti conto della carta di credito e il rapporto sul credito per verificare che non vi siano addebiti non autorizzati o nuove linee di credito.
- Utilizzate una password sicura e unica per tutti i siti web che richiedono il login. Cambiatela regolarmente, soprattutto se la password di un account è stata compromessa da una violazione dei dati.
- Utilizzate solo connessioni Wi-Fi sicure.
- Revisionare i documenti contenenti informazioni sensibili rimuovendo tutti i dati dai dispositivi elettronici (Michaud, 2021).

6.1.4 Spam-mail

A volte si ricevono e-mail indesiderate, pertanto è importante selezionare accuratamente quelle che si intendono leggere e che si valutano affidabili.

Le cosiddette e-mail di spam possono anche contenere pericoli come virus o programmi dannosi che si installano sul computer quando si apre l'e-mail e possono, ad esempio, spiare i dati di accesso. Anche il *phishing* è un tipo comune di truffa online in cui i criminali inviano e-mail dall'aspetto ufficiale nel tentativo di far rivelare all'utente dettagli che possono essere utilizzati per il furto di identità.

Pertanto:

- evitate di aprire gli allegati a meno che non siano stati sottoposti a un programma antivirus
- ricordarsi di disconnettersi, soprattutto quando si utilizza un computer pubblico condiviso
- cancellare tutte le e-mail provenienti da persone o enti sconosciuti
- non rispondere mai allo spam.

Come identificare le e-mail di spam?

- Errori grammaticali e di ortografia

- Messaggi in lingua straniera
- Nome del soggetto inviante mancante
- Richiesta urgente di azione, soprattutto se associata a una minaccia
- Richiesta di inserire dati personali (ad es. PIN)
- Richiesta di aprire un file
- Non si sono mai ricevute precedentemente email dal soggetto inviante (Verbraucherzentrale, 2021).

Riferimenti

Carretero, S.; Vuorikari, R. and Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. doi:10.2760/38842

Michaud, Katelyn. (2021). *What is Data Theft?* https://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft

MOZ (2022). *Google Search Operators.* https://moz.com/learn/seo/search-operators

Norman, C.; Skinner, H. (2006). eHealth Literacy: Essential Skills for Consumer Health in a Networked World. *J Med Internet Res* 8(2):e9. DOI: 10.2196/jmir.8.2.e9

Norton. (2020). *What is a computer virus?* https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

Malwarebytes. (2020). *Hacking definition: What is hacking?* https://www.malwarebytes.com/hacker

Verbraucherzentrale (2021). *Spam: E-Mail-Müll im Internet*. https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-emailmuell-im-internet-10757

WebsiteSetup (2021). https://websitesetup.org/evaluating-online-resources

World Health Organization [WHO]. 2017. *Digital Health Literacy*. https://www.who.int/global-coordination-mechanism/working-groups/digital_hl.pdf