Chat/forum

Compito	Gli scolari discutono sulla base di un articolo di giornale dei pericoli dei social network. Gli scolari inventano un gioco di ruolo nel quale prendono la parola diverse persone tratte dall'articolo. Gli scolari riflettono sulla discussione, scrivendo delle istruzioni su come comportarsi in una chat/un social network e su quali informazioni è opportuno rivelare e quali invece è meglio non comunicare.
Obiettivi	• Gli scolari conoscono i pericoli e i rischi dei social network. • Gli scolari sono in grado di immedesimarsi in diverse persone tratte dall'articolo di giornale e formulare le loro riflessioni. • Gli scolari sono in grado di riflettere sulle proprie conclusioni sulla base di un testo formulato autonomamente e riassumendole a parole.
Riferimenti al programma d'insegnamento	• Gli scolari sono in grado di comunicare tramite i media seguendo regole di sicurezza e di comportamento. (MI.1.4c)
Materiale	• Articolo di giornale «Su Facebook ci sono falsi amici» • Scheda «Chat/forum»
Forma sociale	Discussione plenaria/lavoro individuale
Durata	45 minuti

Informazioni aggiuntive

- Articolo di approfondimento: http://www.ilroma.net/news/cronaca/razzismo-contro-medico-su-fb-presidente-ordine-napoli-con-faccia-nera
- Articolo di approfondimento: https://www.skppsc.ch/it/temi/internet/sextortion/

Social network

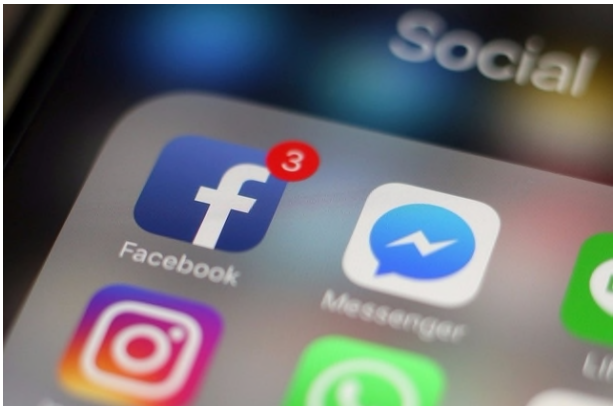
Discussione

Leggi l'articolo di giornale riportato qui sotto e poi discuti con il tuo compagno /la tua compagna di banco degli altri pericoli ai quali ci si può esporre sui social network.
Scrivete le vostre conclusioni sotto forma di concetti chiave nelle righe riportate dopo l'articolo.
Svolgi quindi i due compiti successivi sui pericoli e i rischi dei social network.

https://www.tagesanzeiger.ch/zuerich/verbrechen-und-unfaelle/auf-facebook-sind-falsche-freunde-aktiv/story/10875168 (in tedesco)

Su Facebook ci sono falsi amici

Truffatori utilizzano il social network per spillare denaro. Si moltiplicano le denunce alla polizia di Zurigo.



Gli hacker copiano i profili Facebook e inviano nuove richieste di amicizia.

Foto: Keystone

Stefan Hohler
Reporter di polizia @tagesanzeiger09.05.2017

«Se vi capita di ricevere richieste di amicizia da qualcuno che si chiama come me e che vuole avere il vostro numero di telefono in chat: non sono io!» Ormai non passa giorno senza che un utente di Facebook invii avvisi simili a questo.

Gli hacker copiano i profili esistenti e inviano richieste di amicizia ai conoscenti del titolare originario. In una seconda fase, alle vittime vengono chiesti il numero di cellulare e un codice per SMS mediante il quale gli hacker possono poi fare acquisti che vengono addebitati direttamente sulla fattura telefonica della vittima.

Forte aumento dei casi

Secondo Michael Walker, portavoce della polizia urbana, il fenomeno si è manifestato per la prima volta nell'autunno 2015. All'inizio le truffe erano ancora casi isolati, ma ora hanno subito un forte aumento. Solo nei primi due mesi di quest'anno sono state presentate circa 50 denunce, con tendenza in crescita.

Le somme truffate sono in generale modeste. Via Internet, i truffatori aprono presso fornitori online conti che permettono di pagare le fatture tramite numeri di cellulare. La fattura viene addebitata solo se viene confermata attivamente mediante il codice inviato o il numero di cellulare.
Anche la polizia cantonale deve occuparsi sempre più spesso di casi di questo tipo. «Attualmente ne riceviamo due-tre al giorno», spiega Carmen Suber, portavoce della polizia cantonale. Ci sono indagini in corso ma non si è arrivati ancora a nessun arresto. La difficoltà consiste nel fatto che gli autori agiscono anche dall'estero oppure potrebbero essere attivi a livello internazionale.

Verificare ogni richiesta di amicizia

Carmen Suber raccomanda di non comunicare il numero del proprio cellulare. Inoltre, non bisogna inoltrare codici PIN ricevuti per SMS e/o confermare SMS di sconosciuti.
Come misure di sicurezza preventive è possibile proteggere la propria sfera privata tramite le impostazioni della propria pagina Facebook, consentendo l'accesso solo agli amici. «Ogni richiesta di amicizia deve essere verificata attentamente, in particolare se non si ha ancora un rapporto di amicizia con la persona in questione», spiega la portavoce della polizia.
Anche un giornalista dei giornali locali e di quartiere zurighesi «Lokalinfo» ha fatto conoscenza con gli hacker. Ha accettato una richiesta di amicizia e poco dopo ha ricevuto un messaggio tramite il messenger di Facebook. «Dammi un attimo il tuo numero di cellulare.» Una volta comunicato il numero è arrivata la nuova richiesta: «Tra poco riceverai un codice per SMS, me lo puoi comunicare?» Il giornalista non ha esitato a comunicare alla presunta collega di redazione anche il suddetto codice,
accorgendosi solo più tardi che gli hacker avevano addebitato sulla sua fattura telefonica una console per giochi acquistata in un online shop straniero al costo di 100 franchi. «L'importo è stato addebitato sulla mia fattura del cellulare tramite un cosiddetto operatore terzo.» Il giornalista ha presentato denuncia alla polizia e informato **Swisscom**, che gli è venuta incontro non effettuando l'addebito.
«Se un caso di questo genere riguarda una fattura Swisscom, consigliamo al cliente di contattarci», spiega la portavoce dell'azienda Sabrina Hubacher rispondendo alla nostra richiesta. Swisscom infatti, in caso di truffa, non procede al pagamento a operatori terzi, i quali devono poi provvedere direttamente a richiedere gli importi in questione. Hubacher consiglia comunque di effettuare una comunicazione a **Facebook** in merito al profilo hackerato e una denuncia alla polizia.

(Tages-Anzeiger)
Creato: il 09.05.2017, alle 14:51

1. **Pericoli e rischi dei social network:**

.....

.....

.....

.....

.....

2. **Rifletti su ciò che direbbero in un'intervista le persone coinvolte nell'articolo. Perché si sono venute a trovare in quella situazione? Per quali motivi hanno agito così? Che cosa ne pensano a posteriori? Come si sentono dopo il «fatto»? Quali conseguenze si devono attendere?**

La vittima:

Gli autori:

La polizia:

Ulteriori informazioni sui pericoli dei social network sono disponibili alle voci:

Giovani e media, Media sociali, Opportunità e rischi
http://www.giovaniemedia.ch/it/opportunita-e-rischi/media-sociali.html

3. **Scrivi delle istruzioni per spiegare a un giovane come ci si deve comportare sui social network, quali informazioni si devono rivelare e quali invece non vanno comunicate.**
   Come aiuto puoi utilizzare il seguente link:
   https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/servizi-online/media-sociali/informazioni-inerenti-alle-reti-sociali.html
   (Incaricato federale della protezione dei dati e della trasparenza, Media sociali, «Raccomandazioni agli utenti»)

Così puoi utilizzare i social network in modo sicuro:

.....

.....

.....

.....

.....

.....

.....

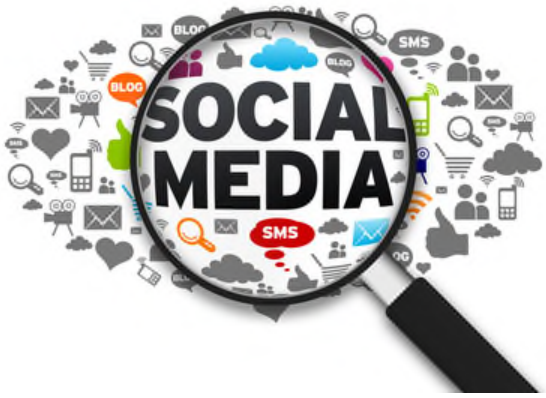
.....

.....

.....

.....

.....



Fonte immagini: Handwerk-Magazin.de
https://img.handwerk-magazin.de/files/smthumbnaildata/392x/5/1/4/6/3/1/Fotolia_44298834_kbuntuFotolia.com_social_media.jpg

Proposte di soluzione:

1. **Pericoli e rischi dei social network:**

- *Mancanza di consapevolezza riguardo alla possibilità per altre persone di accedere a commenti, foto ecc., nonché al relativo rischio di abuso dei dati. Una volta caricate in rete, le foto non possono praticamente più essere cancellate.*
- *Dipendenza da Internet*
- *Distrazione dai compiti a casa se i giovani li fanno al computer e al contempo sono loggati in un social network.*
- *Contatti indesiderati e molestie sessuali: I pedofili possono utilizzare i social network per contattare potenziali vittime.*
- *Rischio di essere presi in giro pubblicamente, offesi o molestati da altri «utenti» (cybermobbing)*

(Fonte: http://www.giovaniemedia.ch/it/opportunita-e-rischi/media-sociali.html)

Altre possibilità:

- *ottenimento di dati con l'inganno o furto di dati che poi possono essere utilizzati per abusi o pubblicati;*
- *ricatti sulla base di informazioni, immagini, video che vengono messi in rete dalla vittima oppure sono stati rubati dal ricattatore (con o senza la consapevolezza della vittima);*
- *le informazioni tratte dai social network possono essere utilizzate per attacchi di phishing.*

2. **Rifletti su ciò che direbbero in un'intervista le persone coinvolte nell'articolo. Perché si sono venute a trovare in quella situazione? Per quali motivi hanno agito così? Che cosa ne pensano a posteriori? Come si sentono dopo il «fatto»? Quali conseguenze si devono attendere?**

Soluzioni individuali degli scolari

Possibili riflessioni
Vittima: non pensava alle possibili conseguenze, è stata ingenua. A posteriori può provare delusione, vergogna, rabbia ecc. I dati caricati in rete o rubati saranno probabilmente presenti in rete anche dopo molto tempo. Conseguenze successive non sono pertanto escluse se i dati vengono inoltrati o venduti.
Autori: i motivi possono essere svariati (povertà, avidità, sadismo ecc.), dopo il fatto ci si può sentire in un primo tempo forti e superiori poi può eventualmente subentrare il pentimento, anche perché magari non si è riflettuto sulle possibili conseguenze. Se il reato viene scoperto sono previste conseguenze penali.

Poliziotto: si attiva non appena viene presentata una querela. Probabilmente è in grado di immedesimarsi nella persona danneggiata. Deve cercare di indagare i fatti e individuare i responsabili (autori). Può sentirsi frustrato se vengono denunciati spesso casi di questo tipo e le indagini non portano i risultati sperati.

3. **Scrivi delle istruzioni per spiegare a un giovane come ci si deve comportare sui social network, quali informazioni si devono rivelare e quali invece non vanno comunicate.**

Soluzioni individuali degli scolari
Possono essere confrontate con le regole di comportamento disponibili sul sito
https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/servizi-online/media-sociali/informazioni-inerenti-alle-reti-sociali.html
(Incaricato federale della protezione dei dati e della trasparenza, Media sociali, «Raccomandazioni agli utenti»)