
# Technology - Digital Literacy

TIM

OSSERVATORIO PERMANENTE GIOVANI-EDITORI

Si ringraziano per i contributi portati
alla presente pubblicazione:

Carlo Sorrentino, *Professore Ordinario di Sociologia dei Processi culturali dell'Università degli Studi di Firenze*
Anna Gatti, *Angel Investor e Founder, Associate Professor of Practice, Digital Transformation, SDA Bocconi*
Lapo Cecconi, *Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
Ester Macrì, *Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*


Curatore dell'editing: Headline Giornalisti
Progetto grafico e copertina: Essedicom

# i 15 temi dell'alfabetizzazione tecnologica digitale

# INTRODUZIONE

## di Carlo Sorrentino

*Professore Ordinario di Sociologia dei Processi culturali dell'Università degli Studi di Firenze*

Nessuno girerebbe per una qualsiasi città - soprattutto in auto o in moto - senza la minima conoscenza del codice della strada, perché saprebbe di essere esposto a un pericolo continuo.
Ma nessuno deciderebbe di restarsene chiuso in casa perché non conosce il codice della strada.
Tutti, piuttosto, ed è quanto accaduto, si sono impegnati a imparare i principi basilari per poter circolare come pedone, oppure ad acquisire conoscenze più approfondite per guidare un qualsiasi mezzo di locomozione.
Per lo stesso motivo, sarebbe assurdo pensare che non sia necessario un analogo addestramento per abitare il mondo digitale. Anzi, un migliore addestramento, visto che il mondo digitale è molto più vasto e complesso, caratterizzato da varie dimensioni e sfaccettature.
È quando si cerca di fare in questo volume, segnalando una serie di rischi che la rete presenta. Ma non con spirito luddistico, per scoraggiarne la frequentazione; quanto, piuttosto, per favorire un uso più consapevole.
A leggere i titoli delle varie schede presenti in questo volume si potrebbe restare spiazzati: la maggior parte fa riferimento a pericoli e degenerazioni della rete.
Per questo motivo, si potrebbe essere tentati di soprassedere, nella colpevole considerazione che l'ignoranza possa attenuare l'apprensione. Oppure, ci si potrebbe spaventare, fino a essere indotti a "dimettersi" dalla rete.
Ma l'unico atteggiamento adeguato e opportuno, invece, è migliorare le conoscenze adeguate per frequentare la rete in modo consapevole.
Infatti, l'ambiente digitale ha come precipua caratteristica la sua enorme, sconfinata vastità; appare naturale, quindi, che per frequentarla siano necessarie delle mappe di viaggio particolarmente accurate e informate. Peraltro, in rete inevitabilmente ci esponiamo – attraverso la presenza sui social, attraverso le foto e i commenti che postiamo oppure attraverso le informazioni che forniamo - senza nemmeno accorgercene. Quando accettiamo i cookies - semplicemente navigando - lasciamo dappertutto nostre tracce. Per cui si potrebbe dire che se non conosciamo la rete, la rete ci conosce molto bene.
L'importanza della conoscenza non è l'unico comun denominatore delle schede che leggerete. C'è anche la condivisione. A guardar bene, infatti, molto spesso la soluzione migliore davanti all'immensità della rete e, quindi, alle ineludibili insidie che pone è

appoggiarsi alle competenze degli altri, condividere con amici, colleghi, conoscenti le modalità opportune per ottenere informazioni più ponderate, dialogare per assicurarsi dell'affidabilità di quanto letto o visto; ma anche - se dovesse succedere - per confidarsi in merito alla possibile soluzione di uno spiacevole coinvolgimento in casi di insulti o minacce.
L'aspetto positivo dell'immensità della rete consiste proprio nella possibilità di condividere ogni informazione o situazione con chi riteniamo più opportuno farlo, senza farsi intimorire da imbarazzi o vergogne.
Bisogna iniziare a considerare l'ambiente digitale come parte del nostro mondo quotidiano e, proprio per questo, gestirla insieme agli altri. Riconoscendo, con modestia, capacità e competenze di chi può aiutarci nella gestione delle tante situazioni in cui possiamo trovarci.
La rete, infatti, si basa su connessioni, sulla moltiplicazione delle connessioni – non a caso si parla di intelligenza connettiva - e, quindi, dalla rete dobbiamo prendere la forza propria dell'unione, piuttosto che la solitudine a cui induce la prevalente forma di fruizione, che avviene tramite *device* del tutto personali - il proprio smartphone, il proprio iPad, i propri profili - a cui accediamo attraverso password che conosciamo soltanto noi e dai luoghi più intimi e privati della nostra quotidianità.
La rete è un luogo pubblico. Non bisogna mai scordarselo, sia per assumere l'adeguato comportamento che di solito assumiamo nei contesti pubblici, sia per non sentirsi mai soli se dovessimo trovarci a disagio o in difficoltà.
Le schede si soffermano anche sugli eccessi prodotti dalla rete. Infatti, la sconfinata immensità dell'ambiente digitale può indurci all'eccesso oppure a esporci agli eccessi altrui. Per questo motivo, abbiamo pensato a fornire informazioni per gestire opportunamente tali eccessi.
Qual è una delle insidie maggiori della rete? L'estrema semplicità d'accesso.
Abbiamo in mano, come ci capita molto di frequente, il nostro smartphone, non sappiamo che fare, siamo in attesa di qualcuno o di qualcosa, ci stiamo annoiando nel posto dove ci troviamo, oppure semplicemente vogliamo distrarci dall'impegno del momento: clicchiamo… e siamo in rete!
Propria tale facilità può condurci nei posti più insoliti e, soprattutto, farci abbassare il livello d'attenzione; proprio come talvolta succede quando girovaghiamo in città senza meta. Dunque, non bisogna abbassare mai la guardia, restare sempre vigili su dove si sta andando e perché.
Ancora meglio sarebbe, soprattutto per i più giovani, se si definissero in anticipo i perimetri d'interesse e, quindi, si indicassero gli obiettivi della propria "navigazione".
In tal modo, ci si muoverebbe sempre con cognizione di causa.
Non si azzererebbero deviazioni di percorso e "perdite di posizione"; ma si avrebbe sempre cognizione di ciò che si sta facendo.
Non si tratta di individuare dei limiti quantitativi (non navigare per più di tot tempo)

oppure qualitativi (farlo soltanto per cause che valgano la pena); sebbene - come segnalato nelle schede - un po' di digital detox, cioè di allontanamento dalla rete temporaneo e deciso autonomamente, possa essere una preziosa valvola di sfogo. Ciò di cui parliamo è, molto più semplicemente, darsi delle priorità, porsi dei limiti.
È pertanto necessario, se si è superata l'infanzia e si è già nell'adolescenza, che questi limiti siano autoimposti e non vengano visti come odiosi divieti. Infatti, ancora una volta, l'immensità dell'ambiente digitale rende molto semplice aggirare tali divieti; quindi, meglio favorire un consumo consapevole piuttosto che imposto.
Un'ultima annotazione, prima di lasciarvi alla lettura delle schede: non avere - nei confronti dell'ambiente digitale - un atteggiamento di distacco e diffidenza. Temendone la competizione sul campo educativo e relazionale. Perché l'inevitabile conseguenza sarebbe la sconfitta, con relativo senso di frustrazione. È troppo più grande di ciascuno di noi.
Meglio, pertanto, muoversi secondo una logica di alleanza. E' una risorsa e non un problema. Come ogni risorsa può diventare un problema, soprattutto se non se ne conoscono le potenzialità, per cui - come già detto - non si gestisce tale risorsa, ma si viene gestiti da tale risorsa.
Mai come in questi ultimi mesi si sta parlando, in merito agli sviluppi dell'ambiente digitale, di intelligenza artificiale.
Con posizioni prevalentemente di timore e preoccupazione. Il principale dei quali è che richiamo di diventare vittime di tali intelligenze. Tuttavia, l'evoluzione della rete, la moltiplicazione degli algoritmi e la loro crescente efficienza non hanno niente a che vedere con l'intelligenza, quanto piuttosto con una profondissima trasformazione nelle forme comunicative che siamo chiamati a gestire. Molto opportunamente Elena Esposito, in un suo interessante libro, preferisce parlare di comunicazione artificiale, piuttosto che di intelligenza artificiale.
Dunque, capire come funziona è indispensabile per acquisire una propria autonoma capacità di gestione di tali nuove forme di comunicazione; per coglierne i rischi - che certamente non mancano; ma senza alcun pregiudizio.
Come già dicevano gli antichi, conoscere e conoscere insieme, connettendo le nostre intelligenze umane (le uniche per adesso esistenti), prima di darci delle risposte ci permette di porci le domande giuste. L'unica strada per arrivare, poi, alle risposte.

# COME DIVENTARE UN CITTADINO DIGITALE RESPONSABILE

di Anna Gatti
*Angel Investor e Founder*
*Associate Professor of Practice, Digital Transformation, SDA Bocconi*

Sono nata quando internet non era un servizio disponibile, anzi necessario, per tutti.
Il telefono fisso a casa era quel servizio.
Quando sono nata io, internet era un'idea a cui lavoravano gli scienziati e la cui diffusione commerciale sembrava ancora lontana.
Sono andata a scuola quando in classe non si usavano ancora i computer. In verità, quando ho iniziato la scuola io, i computer non si usavano neppure a casa.
Mi ricordo ancora quando mi venne regalato il Commodore 64. Avevo dieci anni. Tutti gli amici si riunivano a casa mia per vedere cosa si poteva fare con quel video e quella tastiera.
Avevo già la patente quando è stato lanciato il primo smartphone, il che implica che ho iniziato a guidare quando si sfogliavano ancora le mappe stradali per andare da un posto ad un altro. Ora uso il mio telefono cellulare che si collega automaticamente alla mia macchina elettrica quando mi avvicino alla vettura.
Avevo dieci anni quando fu lanciato il primo telefono cellulare e ne avevo diciotto quando mi fu regalato il mio primo cellulare: era grande quasi come un asciugacapelli.
Nel mio telefono oggi c'è più intelligenza artificiale di quanto potessi immaginare quando negli anni '90 lessi per la prima volta il libro "The Age of Intelligent Machines" scritto da Ray Kurzweil.

Il mondo è cambiato in modo importante durante la mia vita. Questi cambiamenti sono avvenuti in un periodo di tempo relativamente breve. Il fattore principale che ha consentito questi cambiamenti è stata la tecnologia.
La tecnologia ha cambiato profondamente le nostre vite, consentendo miglioramenti importanti in tanti ambiti, ma portando con sè anche nuovi rischi, nuovi pericoli, nuovi quesiti, nuove opportunità e nuove abitudini che dobbiamo imparare a gestire.
Quando ero studente non avrei neppure potuto immaginare le soluzioni a cui avrei lavorato anni dopo a Google, YouTube e Microsoft.
Quando ero studente non avrei potuto immaginare che un giorno avrei finanziato startup che sviluppano profilazioni avanzate dei gusti di una persona in tempo reale e suggeriscono acquisti prima ancora che la persona abbia iniziato a pensare di comperare qualcosa.

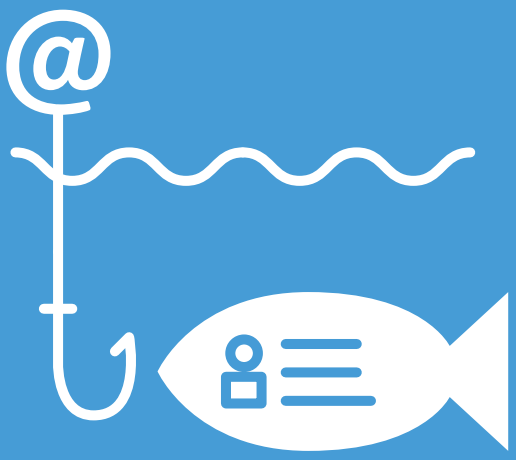
Quando ero studente non avrei potuto immaginare che avrei fondato una società che misura in pochi minuti come funzionano i circuiti cerebrali di un individuo e che fa un check up della tua salute mentale come facciamo un check up della nostra salute fisica.
Quando io ero studente non esistevano ChatGPT ed i suoi concorrenti.
Quando ero studente si andava in banca a ritirare i soldi e si pagava con i contanti o la carta di credito. Ora abbiamo accesso alla banca dal nostro smartphone. Paghiamo tirando fuori il telefono. Entriamo in metropolitana appoggiando il telefono ai tornelli. Investiamo e gestiamo il nostro patrimonio con un app scaricata sul nostro telefonino.
Quando io ero studente pensavo che ciò che leggevo sui libri fosse "vero". Pensavo che i miei amici fossero "reali", che quello che vedevo e ascoltavo fosse "reale", ovvero un sistema contrapposto al sogno e all'invenzione.
Quando io ero piccola veniva insegnato a "non parlare con gli sconosciuti".
Veniva insegnata l'educazione civica a scuola.
Veniva insegnato a chiedere permesso quando si entra in casa di altri e a non toccare le cose altrui.
Oggi le cose sono anche cose virtuali. Gli amici sono virtuali. Si gioca in ambienti di realtà virtuale immersiva, si consumano notizie, informazioni ed emozioni in formati virtuali. Abbiamo bisogno di insegnare come ci si comporta in questi ambienti virtuali, perché le conseguenze di non saperlo sono profondamente reali. E per lo piu' negative.
Il modello di realtà in cui sono cresciuta io è stato profondamente modificato dalle soluzioni tecnologiche che negli ultimi anni sono state lanciate sul mercato e adottate velocemente da masse di persone in ogni parte del mondo. Soprattutto giovani. Giovanissimi.
Imparare ad essere cittadini consapevoli e responsabili in questo nuovo modello ibrido di realtà è fondamentale per continuare a progredire come società.
L'innovazione, ovvero ciò che è nuovo, non è necessariamente progresso.
Secondo la Treccani, "progresso" viene definito come "lo sviluppo verso forme di vita più elevate e più complesse, perseguito attraverso l'avanzamento della cultura, delle conoscenze scientifiche e tecnologiche, dell'organizzazione sociale, il raggiungimento delle libertà politiche e del benessere economico, al fine di procurare all'umanità un miglioramento generale del tenore di vita, e un grado maggiore di liberazione dai disagi".
La straordinaria innovazione tecnologica che ha caratterizzato gli ultimi decenni è stata spesso celebrata come 'progresso' prima che gli impatti sulla nostra società e soprattutto sui giovani si potessero pienamente capire.
Imparare a capire (o quantomeno a farsi domande su) gli impatti di lungo periodo delle innovazioni tecnologiche sulla nostra società è a mio parere fondamentale per diventare cittadini attivi e responsabili. L'etica dell'innovazione è una materia che oggi merita maggiore attenzione.

Avere una cultura digitale di base è importante come sapere leggere e scrivere.
Cultura digitale non vuole dire sapere scrivere un programma in phyton (per quanto utile possa essere). Cultura digitale per me vuole dire avere un framework etico e civico per approcciare le innovazioni tecnologiche.
Io credo che sia importante insegnare questo framework e discuterlo nelle scuole, perché' è dove ci formiamo come cittadini attivi e responsabili. Le scuole sono la più importante sede di incubazione del futuro.
Come si potrebbe insegnare ai bambini e ragazzi di oggi ad essere buoni cittadini di internet?
Partendo dalla realtà (non quella virtuale) per poi traslare l'esperienza al mondo digitale. Insegnando che su internet ci si deve comportare come ci si aspetta che ci si comporti nei luoghi pubblici: presentarsi con il decoro con cui si cammina per strada, comunicare come si dovrebbe comunicare tra persone civili (anche se siamo nascosti dietro le sembianze di un personaggio in un videogioco o di un avatar), non rubare cose altrui (anche se queste "cose" sono in forma di dati digitali, password, musica o video), bandire e condannare il bullismo (che su internet prende la forma di cyberbulling), chiudere la porta per evitare che i ladri entrino (anche se la chiave su internet si chiama password e la vogliamo sicura come la serratura di casa), non dire falsità (che su internet si chiamano fake news), non promuovere l'odio e chi lo diffonde (che su internet si chiamano haters). Potrei continuare questo elenco di regole di base della cittadinanza attiva digitale perché', avendo passato la maggior parte della mia carriera a capire come influenzare i comportamenti degli utenti su internet, ho avuto molto tempo per riflettere su come non lasciarsi travolgere da queste tecniche di influenza digitale. è, forse, però piu' interessante soffermarsi a riflettere non tanto sulla lista di cose pratiche che i giovani dovrebbero imparare, ma sul framework, ovvero sulle dimensioni fondamentali con cui guardare all'innovazione tecnologica e al mondo digitale per cercare di avere una bussola che ci consenta di trovare la direzione giusta in un mondo per noi ancora relativamente nuovo ed in constante divenire.
Credo che sia importante insegnare la distinzione tra tecnologia ed applicazione.
Spesso una tecnologia di per sé non è né buona né cattiva. Ciò che ne fa una innovazione che contribuisce o meno al progresso della società è la sua applicazione.
La mia esperienza professionale mi ha portato a pensare che le dimensioni fondamentali, i punti cardinali della bussola che ci serve per orientarci nel mondo digitale siano sostanzialmente quelli che ci riportano alla definizione di progresso. La domanda fondamentale per me è la seguente: l'applicazione tecnologica "x" (dove potete sostituire ad 'x' l'ultima applicazione tecnologica di moda) porta ad un miglioramento sostenibile della condizione umana non di pochi eletti, ma dell'insieme degli individui che costituiscono la società? Se applichiamo questo framework logico, per esempio, è difficile pensare che i social network, così come oggi sono usati e diffusi, abbiano

costituito una fase positiva nello sviluppo della società. I dati offerti da numerosi studi fatti in prestigiose università ci indicano che negli ultimi anni, insieme ad una spinta adozione dei social networks da parte di giovani e giovanissimi (ad oggi non è stato ancora introdotto a scala un modo efficace di evitare che i ragazzi al di sotto dei 13 anni usino i social network), c'è stato anche un importante aumento della depressione e dei disturbi alimentari tra pre-adolescenti ed adolescenti. L'Organizzazione Mondiale della Sanità da anni si occupa delle implicazioni sulla salute pubbliche dell'uso eccessivo dei social media. I risultati a cui sono giunti sinora non sono rassicuranti.
I social networks sono diventati piattaforme ideali per predators che cercano di adescare minori. Nel corso degli anni le forze dell'ordine hanno sviluppato task force specializzate nel combattere questo tipo di crimine, facilitato dalla mancanza di una educazione digitale di base. è importante, tuttavia, che anche le famiglie e gli educatori insegnino i pericoli associati a navigare da soli su internet.

Oggi si parla molto (e a mio parere in modo troppo confuso) di intelligenza artificiale.
Il termine è ampio e si riferisce a un insieme complesso di tecniche computazionali e algoritmi che consentono di processare dati. All'interno della famiglia dell'intelligenza artificiale ci sono moltissime tecniche di calcolo che vanno dal machine learning al natural language processing.  Lasciando agli studiosi di computer science i dettagli di queste tecniche e come continuare a svilupparle per consentire modellizzazioni sempre più complesse e precise, la cosa certa è che di per sè questi algoritmi non sono nè buoni nè cattivi. Sono come studi avanzati di matematica o di fisica.
Ciò che ne fa una innovazione che contribuisce al progresso o al peggioramento della nostra società sono le applicazioni di queste tecniche di intelligenza artificiale.
Quando devo spiegare a mia figlia Athena di 13 anni l'intelligenza artificiale uso l'esempio della plastica. La plastica è stata inventata il secolo scorso ed è valsa anche un Nobel all'Italia, con il chimico Giulio Natta. Molti chimici si sono impegnati a sviluppare tecniche per la produzione della plastica, contribuendo a importanti innovazioni nell'ambito della chimica. Fino a qui tutto bene.
Nel corso degli anni la plastica è stata usato per innumerevoli applicazioni, senza farsi tante domande sulla reale necessità o beneficio di lungo periodo di tali applicazioni, che hanno portato all'attuale produzione di 380 milioni di tonnellate di plastica all'anno. Questo immenso ammontare di plastica rimane attivo sul nostro pianeta per centinaia di anni e oggi contribuisce alla primaria fonte di inquinamento degli oceani.
La diffusione non ragionata, tattica o opportunistica della plastica ha fatto diventare una innovazione tecnologica uno dei maggiori problemi dell'inquinamento del nostro pianeta. L'innovazione chimica di per sé non era negativa. Tutt'altro.
L'uso non ragionato di tale innovazione, le sue innumerevoli applicazioni sono state il problema.

Quando il danno ambientale era già serio, i governi sono intervenuti con regolamentazioni e leggi. Per i governi è complicato regolamentare ciò che non esiste ancora.
La regolamentazione è spesso la risposta a un problema esistente.
L'intelligenza artificiale è un pò come la plastica. Di per sé lo sviluppo di tecniche computazionali complesse è buono e ha la potenzialità di risolvere problemi complessi, oltre a rendere la nostra quotidianità più organizzata (grazie alle molte applicazioni che già oggi usiamo integrate nei nostri cellulari e in altri dispositivi nelle nostre case). Occorre riflettere sulle conseguenze delle molte applicazioni che si possono lanciare sul mercato.
Auspicare qualche forma di regolamentazione sembra utile, ma non ci si può aspettare che la legge possa regolamentare applicazioni che ancora non sono state pensate.
Per questo insegnare ai giovani a pensare alle conseguenze di lungo periodo delle nostre azioni e dare un framework di base per navigare il mondo digitale e la sua velocità di innovazione mi sembra un passo fondamentale per il progresso della nostra società.
La scuola e gli insegnanti devono essere tenuti al centro dell'educazione dei nostri figli, assicurandogli la necessaria formazione ed il necessario rispetto professionale affinché' possano continuare ad esercitare efficacemente il ruolo di formatori dei cittadini di domani.



# 1

# Phishing

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

ARTICOLO

Il Sole 24 ORE

# Le banche non rispondono per il phishing ai clienti se hanno sistemi di sicurezza efficaci

**di Patrizia Maciocchi** **11 aprile 2023**

L'istituto non paga per le frodi informatiche, quando è lo stesso cliente a fornire codici segreti che solo lui conosce. L'Abi rilancia la sentenza con una circolare

La banca che adotta un sistema di sicurezza efficace per le operazioni online non risponde del phishing ai clienti se sono proprio questi ultimi a fornire ai truffatori le loro credenziali. La Corte di cassazione respinge così il ricorso di una coppia di correntisti che avevano chiesto a Poste Italiane di essere risarciti dei 6mila euro spariti dal loro conto corrente, dopo un bonifico eseguito per via telematica da un soggetto terzo. Una richiesta accolta dal Tribunale di primo grado, secondo il quale le Poste non avevano adottato «tutte le misure di sicurezza tecnicamente idonee» a prevenire il danno che i clienti avevano subìto. La Corte d'Appello aveva però ribaltato il verdetto, con una sentenza che la Suprema corte, considera corretta.
I giudici di legittimità dettano dunque un principio che rappresenta uno scudo per gli istituti di credito nel caso di richieste di risarcimento avanzate da correntisti truffati on line.

Nel caso esaminato la sicurezza del servizio Bancoposta on line era garantita da sistemi informati certificati da enti appositi, secondo rigorosi standard internazionali. L'utilizzo del servizio può avvenire, infatti, solo inserendo codici segreti in possesso dell'utente che neppure il personale dell'istituto conosce. Nell'operazione "incriminata" dunque solo il cliente poteva avere fornito i codici, user id, password e pin, poi utilizzati dall'hacker per il giroconto di 6mila euro.
In più le banche sono a posto quando, come avvenuto nella controversia esaminata, mettono in guardia i clienti avvertendoli della loro diretta responsabilità nella custodia di identificativi, parola chiave, codice di attivazione ecc.
E ancora nei siti degli istituti di credito esiste in genere uno spazio dedicato alle informazioni per evitare le frodi informatiche, in particolare il phishing, nel quale i correntisti vengono avvertiti che gli istituti, non richiedono mai, mai attraverso

posta elettronica, lettere o telefonate di fornire codici personali.
Per queste ragioni l'acquisizione fraudolenta non basta ad escludere la condotta colposa dei danneggiati.

## La Circolare Abi

L'Abi con una circolare ha fatto rinvio ai contenuti della decisione della Suprema corte, segnalando alcuni aspetti agli associati, in relazione al comportamento da considerare "imprudente e negligente" da parte dei correntisti.
Con riferimento all'onere probatorio, conclude nella circolare l'Abi, la Corte di Cassazione ha deciso che l'intermediario non era tenuto a provare che l'addebito fosse stato approvato dai correntisti, in quanto dalle «caratteristiche di sicurezza proprie del sistema informatico (dell'intermediario) per l'esecuzione di operazioni bancarie per via telematica, vi era la prova, derivata da presunzioni, che tali username, pin e password, che i ricorrenti affermavano di non avere utilizzato per impartire tale ordine, vennero utilizzati da un terzo, previa loro illecita captazione».

# SCHEDA
# Phishing

di Ester Macrì e Lapo Cecconi

Il phishing rappresenta una delle più comuni minacce informatiche nel mondo digitale. Si tratta di una pratica fraudolenta in cui i criminali cercano di ottenere informazioni personali sensibili, come password, dati finanziari o informazioni di accesso, fingendosi una fonte affidabile. È, infatti, una vera e propria forma di frode online in cui aggressori si spacciano per entità o organizzazioni legittime, come banche, società di carte di credito o servizi online, al fine di indurre le persone a condividere informazioni personali o finanziarie e sensibili. Questa truffa avviene solitamente attraverso e-mail, messaggi di testo, chiamate telefoniche o siti web contraffatti che sembrano autentici. Sono davvero molte le persone che nella loro vita rimangono vittime di phishing almeno una volta.

Ma quali sono i principali rischi per gli individui e le organizzazioni del fenomeno del phishing? I più comuni sono:

- Furto di identità: i criminali possono utilizzare le informazioni personali trovate per rubare le identità della vittima e commettere frode finanziarie o attività illegali a suo nome.
- Frodi finanziarie: le informazioni finanziarie ottenute tramite phishing possono

essere utilizzate per effettuare transazioni non autorizzate, accedere ai conti bancari o aprire le carte di credito, causando danni finanziari significativi.
- Violazione della privacy: i dati personali rubati tramite phishing possono compromettere la privacy dell'individuo, mettendo a rischio la sicurezza personale e aprendo la porta al ricatto o allo stalking.
- Danneggiamento della reputazione: se le informazioni ottenute tramite phishing vengono utilizzate per condurre attività illegali o dannose, la reputazione dell'individuo o dell'organizzazione coinvolta può essere gravemente danneggiata.

Per non cadere in questi rischi è necessario che gli individui e le aziende portino avanti alcuni atteggiamenti concreti per prevenire il fenomeno. Nel dettaglio, gli atteggiamenti possono essere così riassunti:

1. È necessario porre attenzione alle e-mail e ai messaggi che chiedono informazioni personali o finanziarie. Inoltre, è importante verificare attentamente l'indirizzo e-mail del mittente, controllare la grammatica o gli errori di ortografia e fare attenzione ai link o agli allegati sospetti.
2. È essenziale non condividere informazioni sensibili, personali o finanziarie tramite e-mail o messaggi, specialmente se la richiesta sembra sospetta. Le istituzioni finanziarie o i servizi online affidabili non chiederanno mai credenziali tramite questa modalità.
3. È importante verificare la fonte e la legittimità dell'ente o dell'organizzazione coinvolta al momento della richiesta di informazioni o di azioni. Utilizzare canali ufficiali, come siti web autentici o numeri di telefono verificati, per contattare direttamente l'organizzazione e confermare le richieste, sarà fondamentale per evitare il fenomeno del phishing.
4. Come ultima azione, è importante mantenere il software, il sistema operativo, i programmi antivirus, e i browser web aggiornati. Tali aggiornamenti spesso includono patch di sicurezza che correggono vulnerabilità che possono essere sfruttate dai truffatori.

Anche la tecnologia può rivelarsi utile per contrastare il phishing. In primis ciò potrebbe avvenire attraverso l'utilizzo del filtro antispam per bloccare e identificare e-mail sospette o potenzialmente pericolose. Sono stati inventati, inoltre, recentemente dei veri e propri strumenti di rilevamento del phishing ovvero browser web moderni che spesso avvertono gli utenti quando visitano siti web sospetti o non sicuri.
L'intelligenza artificiale, in più, ha contribuito molto, tramite i suoi algoritmi, a migliorare la situazione: il contenuto delle e-mail o dei messaggi possono essere in brevissimo tempo analizzati per identificare segnali di phishing e avvisare gli utenti.
Inoltre, il potere delle tecnologie è grandissimo per quanto riguarda l'educazione sulla sicurezza informatica: la tecnologia può essere utilizzata per fornire informazioni e

programmi di formazione sulla sicurezza informatica, educando le persone sulle tattiche di phishing e sui metodi per riconoscerle e evitarle.
In conclusione, il phishing rappresenta una minaccia costante nel mondo digitale. Per proteggersi dal phishing è necessario adottare atteggiamenti consapevoli come l'attenzione alle e-mail sospette, la verifica delle fonti e la non condivisione di informazioni sensibili. La tecnologia offre anche strumenti di sicurezza avanzati come filtri antispam e rilevamento automatico del phishing, che possono aiutare a contrastare questa minaccia. La consapevolezza e l'educazione sulla sicurezza informatica sono fondamentali per proteggere gli individui e le loro informazioni dagli attacchi di phishing.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

Ogni studente dovrà intervistare 3 familiari o amici adulti chiedendo:

- Sei mai stato vittima di phishing?
- Se sì: come mai sei caduto nella trappola? Cosa è successo? Sei riuscito a riavere i soldi perduti?
- Se no: hai comunque ricevuto messaggi con tentativi di phising? Come li hai riconosciuti?

In aula confrontiamo le risposte e discutiamo.

- È frequente essere vittime di phishing? Perché?
- Quali sono le categorie più a rischio? Perché?

# TEST

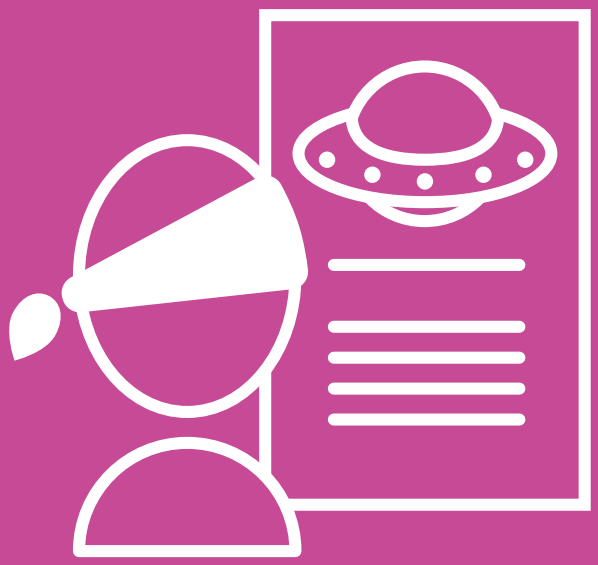
**1. Cosa è il phishing?**
**a.** Una pratica di pesca sportiva
**b.** Un metodo di catturare pesci usando esche speciali
**c.** Un tipo di attacco informatico che mira a rubare informazioni sensibili
**d.** Un gioco online basato sulla pesca

**2. Quali sono i rischi del phishing?**
**a.** Miglioramento della sicurezza online
**b.** Diffusione di informazioni accurate e verificate
**c.** Possibilità di furto di dati personali, password e informazioni finanziarie
**d.** Promozione della condivisione responsabile delle informazioni online

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare il phishing?**
**a.** Fare clic sul link sospetti nelle mail o sui social media
**b.** Condividere liberamente informazioni personali online
**c.** Verificare attentamente l'autenticità delle e-mail e dei siti web
**d.** Ignorare le avvertenze di sicurezza sui dispositivi

**4. Come può la tecnologia aiutare a contrastare il phishing?**
**a.** Diffondendo link sospetti ed e-mail di phishing in modo più efficace
**b.** Implementando filtri antiphishing e rilevamento delle minacce
**c.** Facilitando l'accesso a siti web non sicuri
**d.** Creando nuovi account online senza autenticazione

Soluzioni: 1c, 2c, 3c, 4b



# 2

# Fake news

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

QN il Resto del Carlino

# Fake news sull'alluvione

**Redazionale** **9 marzo 2022**

Fake news sull'alluvione in Emilia-Romagna: video e foto rimbalzano senza controllo
In queste ore drammatiche continua la diffusione di immagini vecchie o decontestualizzate. A cominciare dal bacio dei fidanzati nel fango: un problema che alimenta panico e confusione.
Bologna, 19 maggio 2023 - In queste ore drammatiche in cui si contano ancora le vittime, i dispersi e i danni quasi infiniti provocati dall'alluvione continuano a circolare diverse notizie e video falsi. O meglio, filmati reali e veritieri, ma decontestualizzati o risalenti a diverso tempo fa.

## Nei supermercati mancano cibo e acqua

Un problema non di poco conto, che alimenta confusione e disperazione, in un momento già tragico, con le fake news che impazzano di telefonino in telefonino e spingono tanti cittadini verso la disinformazione generando panico e preoccupazione. Per fortuna ci sono anche esempi contrari: come la foto della poliziotta che salva il bimbo in mezzo all'acqua che sta commuovendo il web.

## I fidanzati nel fango... a Senigallia

In primis è tornata in auge una foto che ritrae due ragazzi giovanissimi, abbracciati mentre si lasciano andare a un bacio, con tanto di vanga in mano, scarponi e fango fino alle ginocchia: lo scatto risale in realtà allo scorso anno, durante l'alluvione che ha colpito le Marche, e in particolar modo la zona di Senigallia, a settembre. Ed è proprio qui che la foto è stata scattata, in quei giorni.

## Bologna, il video falso della stazione allagata

Un'altra fake news che ha preso piede è quella di un presunto (e massiccio) allagamento della stazione dell'alta velocità bolognese: il filmato, invece, riprende chiaramente un altro snodo ferroviario. I più attenti potranno già essersi accorti osservando con accuratezza, ma lo stesso video potrebbe mandare invece in tilt quei viaggiatori che per necessità si trovano a dover transitare in stazione. Anche le Ferrovie, infatti, hanno emanato un comunicato per chiarire la questione.

## La strada crolla: il video girato a Cesena e non a Bologna

Disinformazione anche per quanto riguarda i Colli: un video girato a Tezzo di Sarsina (in provincia di Forlì-Cesena) in cui si vede una collina franare completamente sulla strada fino a spazzarla via (con tanto di terra e alberi in movimento) è invece rimbalzato sulle app di messaggistica istantanea indicando che la devastante voragine si è aperta sui colli Bolognesi, ma non è vero.

## Piazza Maggiore come un fiume: è un vecchio filmato

L'ultimo episodio riguarda un altro filmato, questa volta girato in una piazza Maggiore completamente allagata: l'acqua scorre a fiumi ai bordi dei marciapiedi davanti a San Petronio, ma la ripresa - anche in questo caso - non è di questi giorni, bensì di anni addietro.

Tutte le fake news, purtroppo, hanno avuto un effetto quasi virale raggiungendo una grande visibilità e diverse condivisioni, a discapito della chiarezza e della corretta informazione.

# SCHEDA
# Fake news
## di Ester Macrì e Lapo Cecconi

Nell'era digitale in cui viviamo, le fake news sono diventate un fenomeno attuale, sempre più diffuso e pericoloso. Con la rapida diffusione delle informazioni attraverso i social media e le piattaforme online che caratterizzano l'odierna istantaneità della comunicazione, le notizie false possono propagarsi velocemente, influenzando l'opinione pubblica, distorcendo la realtà e minando la fiducia nelle fonti di informazione tradizionali.
Ma cosa è una fake news? Le fake news, o notizie false, sono informazioni o storie inventate o mal divulgate che vengono presentate come se fossero vere.
Esistono due tipi di fake news: la prima è la disinformazione, ovvero la diffusione di notizie false create intenzionalmente per manipolare l'opinione pubblica e creare confusione informativa; ma le informazioni false possono anche essere divulgate senza nessun intento malevolo e in quel caso si tratterà di "misinformazione".
Le fake news possono riguardare qualsiasi argomento come politica, salute, scienza, economia e persino questioni sociali. Spesso sono progettate e architettate intenzionalmente per attirare l'attenzione e generare clic, aumentando il traffico sui siti web o alimentando scopi malevoli.

Le fake news rappresentano una minaccia significativa per la società e anche per ciascuno di noi. Infatti, i rischi che le fake news si portano dietro sono molteplici e di varia natura:

- Manipolazione dell'opinione pubblica: le fake news possono influenzare le opinioni delle persone su questioni importanti come elezioni, politiche pubbliche o movimenti sociali. La manipolazione dell'opinione pubblica mina la democrazia e ostacola il processo decisionale informato.
- Diffusione di disinformazione: le fake news possono diffondere informazioni errate su argomenti come salute, medicina o ambiente, mettendo a rischio la vita delle persone. Ad esempio, notizie false sulla sicurezza dei vaccini (e durante la pandemia sono stati molteplici gli episodi a riguardo) possono portare alla diffusione di malattie evitabili.
- Polarizzazione e conflitti: le fake news possono alimentare la polarizzazione e il conflitto all'interno della società. La disinformazione deliberata, infatti, può intenzionalmente creare divisioni tra gruppi di persone, generando tensioni sociali dannose.

Come contrastare allora l'impatto delle fake news?
Di seguito, alcuni atteggiamenti concreti da adottare per prevenire o contrastare il fenomeno:

1. Verificare le fonti: prima di condividere notizie, assicurarsi sempre di verificare la loro autenticità. Controllare le fonti, cercare conferme da altre fonti attendibili e fare attenzione alle notizie con titoli sensazionalistici o con contenuti eccessivamente emozionali. Nel mondo giornalistico questa fase è la fase del fact-checking.
2. Sviluppare pensiero critico: tutte le notizie vanno sempre analizzate in modo obiettivo e senza pregiudizi. Sarà necessario, allora, valutare la credibilità dell'autore, cercare le evidenze e considerare prospettive diverse prima di accettare una notizia come vera.
3. Educazione mediatica: sarà sempre più necessario promuovere un'educazione mediatica nelle scuole e nella società al fine di informare sempre più sull'esistenza e sulla pericolosità del fenomeno.

Fortunatamente le stesse tecnologie che hanno contribuito alla diffusione delle fake news possono anche offrire soluzioni per contrastarle. Ecco alcune modalità in cui la tecnologia può aiutare, ad esempio tramite algoritmi di rilevamento delle fake news. Le piattaforme digitali possono utilizzare algoritmi avanzati per identificare automaticamente le potenziali fake news: questi algoritmi analizzano il contenuto e le notizie, verificano le fonti e identificano segnale di manipolazione o disinformazione. Tali sistemi possono essere integrati nelle piattaforme social media per segnalare le notizie dubbia agli utenti o limitarne la diffusione.
Altro sistema per contrastare le fake news attraverso la tecnologia è la verifica dei fatti automatizzata. Esistono strumenti di verifica dei fatti basati sull'intelligenza artificiale che aiutano a rilevare e contraddire le fake news. Questi strumenti analizzano le affermazioni presentate nelle notizie e confrontano i dati con fonti attendibili. attraverso l'automazione, la verifica dei fatti può essere accelerata e resa più accessibile a un pubblico più ampio.
Inoltre, le piattaforme di social media possono introdurre etichette o avvisi per identificare le notizie che sono state segnalate come potenziali fake news.
Queste etichette possono fornire agli utenti informazioni aggiuntive sulla veridicità del contenuto e incoraggiarli a fare una valutazione critica prima di condividerle.
È importante ricordare che nonostante il contributo della tecnologia, combattere le fake news richiede uno sforzo collettivo. La responsabilità di condividere solo notizie verificate e combattere la disinformazione spetta sia alle piattaforme digitali che agli utenti stessi. solo attraverso una combinazione di tecnologia, educazione e impegno individuale possiamo affrontare efficacemente il problema delle fake news nella società digitale di oggi.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Vero o falso?"

La classe si divide in coppie. Ogni coppia deve trovare online una notizia vera e inventare una notizia falsa. A turno, ciascuna coppia presenterà alla classe le due notizie e le altre coppie dovranno indovinare quale delle due è la notizia vera e quale la falsa. Vince la coppia che, alla fine, avrà individuato il maggior numero di fake news. Dopo il gioco si potrà condurre una breve discussione:

- Come avete riconosciuto le notizie false?
- È stato facile o difficile?
- Come avete inventato le notizie false?

# TEST

**1. Cosa sono le fake news?**
**a.** Notizie verificate e accurate;
**b.** Informazioni non verificate o deliberate in modo errato;
**c.** Articoli di opinione basati su fatti verificati;
**d.** Contenuti ironici o satirici.

**2. Quali sono i rischi delle fake news?**
**a.** Diffusione di informazioni accurate e verificate;
**b.** Promozione di un dibattito sano e costruttivo;
**c.** Manipolazione dell'opinione pubblica e creazione di confusione;
**d.** Miglioramento della fiducia nell'informazione.

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare le fake news?**
**a.** Condividere indiscriminatamente ogni notizia trovata online;
**b.** Verificare la fonte e la veridicità delle informazioni prima di condividerle;
**c.** Credere ciecamente a tutto ciò che viene pubblicato sui social media;
**d.** Diffondere notizie senza verificare i fatti.

**4. Come può la tecnologia aiutare a contrastare le fake news?**
**a.** Diffondendo informazioni senza alcun controllo;
**b.** Implementando algoritmi di riconoscimento delle fake news;
**c.** Facilitando la creazione e la diffusione di notizie false;
**d.** Bloccando l'accesso a internet per evitare la diffusione delle fake news.

Soluzioni: 1b ,2c ,3b ,4b

# 3

# Troll e haters

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

la Repubblica

# Haters, Carlotta Perego solidale con Benedetta Rossi: "Io mi sono difesa col metodo Ferragni”

**di Nicoletta Moncalero** **8 maggio 2023**

L'influencer: "Mi hanno attaccato per un glicine fritto... Quando l'odio ha colpito me ho lasciato che la polemica si smorzasse da sola. Nel web ci sono mele marce, è incredibile che anche una persona genuina come Benedetta possa attirarle"

Non solo Benedetta Rossi, anche Carlotta Perego (Cucina Botanica) nei giorni scorsi è finita nella mira degli haters se non addirittura dei cospiratori per una ricetta in cui ha fritto e mangiato il glicine. Per questo oggi, c'è anche lei tra chi sostiene il video di sfogo della cuoca più amata d'Italia, con i suoi 4 milioni e mezzo di follower.

Carlotta, cosa ha pensato quando ha visto il video di Benedetta Rossi?
"Secondo me ha fatto benissimo a fare quel video. I commenti che ha citato facevano passare le persone che la seguono in cucina come persone senza gusto, senza piacere per il cibo. Come se chi non ha la possibilità di comprare un ingrediente di top qualità allora non sia in grado di fare una ricetta. Trovo sia una cosa molto triste e molto brutta, che rende i social un posto meno bello da frequentare".

Però questo è anche il vostro posto, siete voi ad aprire la porta
"Lo so, purtroppo è come darsi la zappa sui piedi. Sui social pubblichiamo le nostre ricette, le nostre idee, condividiamo parte della nostra vita e allo stesso tempo però inneschiamo questo meccanismo di commenti, di like.
Un meccanismo che può diventare tossico. Ho visto molte volte questa parola nei commenti al post di Benedetta e trovo che sia molto giusta per descrivere la situazione che si sta creando, negli ultimi tempi specialmente. Secondo me dopo il Covid, tutto è un pò peggiorato".

Eppure, il Covid non doveva farci diventare tutti più buoni?
"Nel mio piccolo, io ho iniziato quasi 5 anni fa e ho notato come questo fenomeno

stia aumentando nell'ultimo periodo. In parte forse anche perché anche i miei profili crescono ed esponendomi sempre a più persone ovviamente tra tanti la mela marcia la trovi, la trovi meno in un gruppo più ristretto. Però vedo che anche persone tranquille, pacifiche, genuine come Benedetta attirano un odio ingiustificato.
Mi chiedo sempre che frustrazione debbano avere per esprimere tutta questa cattiveria in risposta a video che non sono su argomenti così divisivi. Parliamo di ricette di una torta salata con la pasta sfoglia. Davvero non capisco tutto questo rancore".

La scorsa settimana è stata lei al centro dell'attenzione per un glicine fritto. Ci racconta cosa è successo?
"Spero che questa parentesi si sia chiusa, sono stata malissimo in questi giorni perché mi sono sentita impotente di fronte a quello che stava succedendo.
Ci tengo a dire come è andata. Una sera della scorsa settimana sono stata molto male e con tutta la tranquillità del mondo l'ho raccontato ai miei follower, come racconto tante altre cose. Dopo poco alcune persone mi hanno fatto sapere che su Twitter, piattaforma che non frequento assolutamente perché mi mette l'ansia, alcuni stavano cospirando sul fatto che il malessere potesse essere legato al glicine. Inizialmente credo che fosse anche in maniera scherzosa. Io ho subito fatto una story per chiarire: per dire che il video del glicine era stato registrato una decina di giorni prima e comunque la ricetta non me la ero inventata. Che non mangio cose a caso, come una pazza.
Pensavo di aver messo un punto sulla questione, la ritenevo comunque una piccolezza. Poi però la storia è stata ripresa da alcuni giornali, con titoli del tipo influencer intossicata dal glicine... si sono inventati che sono addirittura finita in ospedale.
Non era vero nulla, ma da lì è partito tutto".

Cosa ha mangiato quella sera?
"Adesso vi faccio ridere: ho mangiato ceci con fagiolini al pesto. Forse col senno di poi avrei dovuto specificarlo".

Però non è più tornata sull'argomento, come mai da deciso di lasciar perdere?
"Ho adottato il metodo Ferragni: ho lasciato e sperato che la polemica si spegnesse da sola. Ne ho parlato anche con un amico che fa il coach ed è molto bravo nella gestione di queste cose. E mi ha consigliato di lasciare che la cosa si smorzasse. Se non fosse successo avrei messo i miei limiti. Però questa seconda opzione non l'ho dovuta applicare, non è stata necessaria.

# SCHEDA
# Troll e haters
## di Ester Macrì e Lapo Cecconi

Gli haters e i troll sono personaggi comuni nel mondo del digitale che possono avere un impatto significativo sulla nostra esperienza online. Gli haters sono persone che diffondono odio e negatività online. Criticano distruttivamente, prendono di mira persone, gruppi o idee, diffondendo commenti offensivi o contenuti dannosi.
I troll, invece, sono individui che si impegnano di proposito in comportamenti provocatori o offensivi. Cercano di suscitare reazioni emotive e provocare conflitti online attraverso commenti disturbanti, insulti o comportamenti scorretti. Inoltre, spesso si godono la reazione delle persone e cercano di creare discordia e disarmonia.

Il fenomeno degli haters può portare a due rischi significativi:

- Impatto emozionale: gli haters possono causare danni emotivi significativi alle vittime dei loro attacchi. Le loro parole possono ferire e avere conseguenze negative sulla salute mentale e il benessere delle persone coinvolte.
- Cyberbullismo: gli haters possono perpetrare bullismo online e discriminazione, prendendo di mira persone in base alla loro razza, religione, genere e orientamento sessuale. Questo comportamento può avere conseguenze devastanti sulla vittima e alimentare l'odio nella società.

Anche il fenomeno del Troll non è da meno nei rischi che può portare dietro di sé:

- Creazione di conflitti: i troll cercano di alimentare il conflitto e la discordia online. Il loro comportamento può scatenare discussioni infuocate, aumentando la tensione e l'aggressività nell'ambiente digitale.
- Diffusione di disinformazione: i troll possono diffondere notizie false o fuorvianti, alimentando la confusione e minando la fiducia nella verità. Questo può portare a divisioni sociali e politiche.

Come affrontare attivamente il fenomeno degli haters e dei Troll attraverso alcuni semplici atteggiamenti?

1. Non alimentare le provocazioni: non rispondere agli haters o ai troll con rabbia o risposte emotive dato che il loro intento spesso è proprio la voglia di una reazione. È quindi necessario ignorare i commenti negativi per far sì che il loro impatto sia sminuito.
2. Bloccare o segnalare: è necessario utilizzare le funzionalità di blocco e segnalazione disponibili sulle piattaforme di social media per ridurre l'interazione con gli haters

e i troll. Questo può aiutare a limitare la loro influenza sul proprio ambiente online.
3. Focalizzarsi sulla positività: è necessario concentrarsi su contenuti positivi, costruttivi e significativi nelle proprie interazioni online. È importante, infatti promuovere sempre più una cultura dell'empatia, della gentilezza e del rispetto.

La tecnologia può svolgere un ruolo importante nel cercare di contrastare queste due figure del mondo digitale attraverso numerosi strumenti. In primo luogo, si possono bloccare questi comportamenti scorretti attraverso i filtri e gli strumenti di moderazione contenuti sulle piattaforme di social media e i forum online per individuare e bloccare contenuti offensivi o dannosi. Questi strumenti aiutano a creare un ambiente online più sicuro e positivo. La tecnologia può essere utilizzata anche per fornire programmi di educazione e sensibilizzazione sulla consapevolezza digitale, promuovendo la comprensione dei rischi degli haters e dei troll e fornendo strumenti per affrontarli in modo efficace. Gli algoritmi di intelligenza artificiale, inoltre, possono essere utilizzati per identificare automaticamente comportamenti di trolling e hate speech, consentendo una risposta più rapida ed efficace per contrastarli. Quel che, infine, le nuove tecnologie possono offrire se usate nel giusto modo, sono comunità online sicure e rispettose, in cui gli utenti si sentono protetti e possano segnalare comportamenti inappropriati. La moderazione attiva e la collaborazione tra utenti possono contribuire a ridurre l'influenza degli haters e dei troll.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Haters o troll?"

Chiediamo ai ragazzi di cercare post molto commentati sui social network (Facebook e Instagram). Tra i commenti dovranno individuare quali sono attribuibili a hater e quali a troll.
Discutiamo:

- Sono più frequenti i commenti degli hater o dei troll? Perché?
- Quali si identificano meglio? Perché?
- A voi è mai successo di ricevere commenti di questo tipo? Raccontate
- Come comportarsi in questi casi?

# TEST

**1. Cosa sono gli haters?**
**a.** Persone che amano e supportano gli altri online
**b.** Persone che diffondono amore e gentilezza sui social media
**c.** Individui che criticano, insultano o diffamano gli altri online
**d.** Sostenitori di cause sociali su internet

**2. Cosa sono i troll?**
**a.** Creature leggendarie delle fiabe e delle leggende
**b.** Persone che condividono informazioni accurate e verificate sui social media
**c.** Individui che provocano, infastidiscono o creano conflitti online
**d.** Appassionati di giochi di ruolo su internet

**3. Quali sono i rischi dovuti agli haters?**
**a.** Promozione di un dialogo costruttivo e rispettoso online
**b.** Diffusione di amore e comprensione su internet
**c.** Mancanza di fiducia nelle interazioni online e danni emotivi agli individui presi di mira
**d.** Sviluppo di una comunità online positiva e inclusiva

**4. Quali potrebbero essere gli atteggiamenti concreti per evitare gli haters e i troll?**
**a.** Rispondere e alimentare le provocazioni o gli insulti online
**b.** Ignorare completamente gli attacchi e non rispondere
**c.** Diffondere odio e negatività come risposta agli haters
**d.** Condividere informazioni personali online con gli haters

Soluzioni: 1c, 2c, 3c, 4b


YOU WIN €

# 4

# Clickbaiting

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

la Repubblica

# Post acchiappa click, ecco la comunità che spoilera la disinformazione su Facebook

**di Cristina Cuciniello** **22 gennaio 2015**

"IL VIDEO che ha commosso il web, una mamma e il suo bambino che...". "Perdi fino a tre chili in una settimana, con questo ingrediente segreto: è...". "Lutto nel mondo dello spettacolo: l'Italia in lacrime per...": titoli così - allarmistici, ingannevoli, incompleti nel veicolare una notizia, vera o presunta che sia - impestano le bacheche di Facebook di ogni utente, ogni giorno.
I post acchiappa-click. In larga parte si tratta di sponsored post, inserzioni a pagamento che un committente diffonde al fine di veicolare traffico verso il proprio sito web, contando sulla curiosità che muove l'utente a cliccare sul link proposto per recuperare la parte mancante di un'informazione apparentemente ghiotta.

È il clickbaiting: una pratica così molesta da aver attirato le ire di Mark Zuckergerg che - da diversi mesi - combatte il fenomeno dei link acchiappa-click a colpi di algoritmi.
La comunità che combatte il clickbaiting. Ma dove non arriva l'algoritmo, arriva l'ingegno umano, o forse l'esasperazione: è così che è nata la comunità di utenti Facebook "Spoilerare post che lasciano informazioni a metà".

Circa 20.000 utenti, nel momento in cui scriviamo, un'impostazione goliardica e spiritosa: cosa fa "Spoilerare post"? Utilizza il meccanismo dello spoiler, cioè l'anticipazione di un contenuto, per boicottare i post acchiappa-click. In pratica, sotto ogni post incompleto c'è un utente che commenta anticipando cosa si troverà una volta aperto il link. Il risultato è esilarante: sotto promesse di diete miracolose, cure per ogni male, video imperdibili, si scopre la spesso banalissima verità. Ovvero: che di mirabolante c'è poco. Un'idea nata quasi per gioco. "L'idea della pagina è nata durante una riunione fra amici, per parlare del futuro del nostro blog", racconta Ilario, 21 anni, studente universitario di Bergamo. "Curo insieme ad alcuni amici un blog il cui intento è stimolare i nostri coetanei a informarsi, partecipare e discutere dei temi d'attualità. Accanto al blog, con il quale cerchiamo di proporre un'informazione corretta e approfondita, abbiamo pensato di creare una pagina goliardica che avesse l'obiettivo di distruggere la disinformazione

che spesso viene diffusa tramite Facebook".
Non solo contenuti a metà, dunque, la comunità di utenti che si raccoglie su "Spoilerare post" cerca anche di smascherare le bufale, altra piaga delle nostre bacheche, verso la quale Facebook ha appena lanciato l'offensiva.
Dal gioco alla guerriglia social. "All'inizio sembrava un gioco", commenta Ilario, "poi tantissimi utenti hanno iniziato a postare sulla nostra pagina i fermi immagine dei loro spoiler. Pensavamo di non dare fastidio a nessuno, ma man mano sono arrivati anche i primi ban. Tutto questo mi ha spinto a proseguire in questa piccola guerriglia social, anche stilando e condividendo una black list di siti che fanno pessima informazione".
Non a tutti, insomma, piace che la disinformazione venga smascherata: ma gli utenti si organizzano in modi sempre più creativi per contrastarla.

# SCHEDA
# Clickbaiting
## di Ester Macrì e Lapo Cecconi

Il clickbaiting è una pratica comune nell'ambiente digitale in cui titoli o contenuti ingannevoli vengono utilizzati per attirare l'attenzione degli utenti fino a spingerli a cliccare su un determinato link. Questa tecnica mira a generare traffico e visualizzazioni, ma può creare aspettative false o fuorvianti. Nello specifico, il clickbaiting è una strategia utilizzata per attirare l'attenzione degli utenti online mediante l'utilizzo di titoli accattivanti, sensazionali o ambigui. L'obiettivo principale è proprio quello di indurre le persone a fare clic sul link per generare traffico verso un sito web o una piattaforma online. Tuttavia, spesso i contenuti effettivi non corrispondono alle promesse fatte nel titolo, deludendo gli utenti.

Tre sono i rischi che questa pratica di “acchiappa click” può riversare sugli utenti online:
- Disinformazione: il clickbaiting può diffondere informazioni false o fuorvianti, creando confusione e minando la fiducia delle persone nelle notizie e nei contenuti online.
- Perdita di tempo e frustrazione: questa pratica può portare gli utenti a cliccare su contenuti che non soddisfano le aspettative o che non sono rilevanti per loro. Ciò può comportare la perdita di tempo e generare frustrazione.
- Sicurezza online compromessa: i link di questo tipo possono essere utilizzati per indirizzare gli utenti a siti web dannosi o contenenti malware. Ciò mette a rischio la sicurezza dei dispositivi e delle informazioni personali degli utenti.


Delle semplici mosse che gli utenti online possono seguire per evitare di cascare nella trappola del clickbaiting possono essere:

1. Leggere oltre il titolo: prima di fare clic su un link, è necessario leggere l'intero contenuto dell'articolo o della pagina e cercare informazioni affidabili confrontando più fonti per valutare l'attendibilità delle notizie o dei contenuti.
2. Senso critico: è importante fare domande e analizzare attentamente il titolo o le promesse fatte chiedendosi se questi sembrino troppo sensazionali, se siano presenti promesse irrealistiche o se sia troppo bello per essere vero.
3. Verificare la fonte: è importante controllare la credibilità della Fonte del contenuto e cercare informazioni sull'autore, l'organizzazione o il sito web per valutare la sua reputazione e l'attendibilità delle informazioni fornite.
4. Utilizzare strumenti di blocco e filtro: è importante conoscere anche alcuni strumenti quali l'estensione del browser o le app che bloccano e filtrano i contenuti di clickbaiting, riducendo così la possibilità di visualizzare titoli fuorvianti.

Come appena accennato, la tecnologia può fare molto se utilizzata in modo positivo per cercare di contrastare tale fenomeno. Nello specifico la tecnologia, i motori di ricerca, le piattaforme social, tramite gli algoritmi di rilevamento, possono identificare il clickbaiting e ridurre la sua visibilità. Questi algoritmi possono analizzare i titoli, i contenuti e il comportamento degli utenti per fornire i risultati più rilevanti e autentici. Inoltre, le piattaforme online possono offrire strumenti di segnalazione che consentono agli utenti di segnalare contenuti di clickbaiting. Questi rapporti possono aiutare a identificare e rimuovere i contenuti fuorvianti. La tecnologia può essere utilizzata anche per fornire programmi di formazione sulla consapevolezza digitale, educando gli utenti e fornendo loro strumenti per identificare ed evitare situazioni acchiappa click. Infine, alcune piattaforme online consentono agli utenti di personalizzare le loro preferenze di visualizzazione dei contenuti.

In conclusione, il clickbaiting può essere un'esperienza frustrante e fuorviante nell'ambiente digitale. Per evitarlo, è importante adottare atteggiamenti critici come leggere oltre il titolo, verificare le fonti e valutare l'attendibilità dei contenuti.

La tecnologia può svolgere un ruolo significativo nel contrastare il fenomeno attraverso l'utilizzo di algoritmi di rilevamento, strumenti di segnalazione, educazione sulla consapevolezza digitale e filtri personalizzati dei contenuti. Utilizzando la tecnologia in modo responsabile e consapevole, possiamo proteggerci meglio dalle pratiche di clickbaiting e promuovere una cultura online basata sulla verità e sulla rilevanza dei contenuti.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Titoli acchiappa click"

La classe viene divisa in quattro gruppi. Tre gruppi sono le testate giornalistiche, un gruppo invece interpreta i lettori. Le testate giornalistiche dovranno produrre 5 titoli ciascuna. Ogni titolo sarà scritto su un foglio di carta e appeso in aula. Una volta appesi tutti i titoli, il gruppo dei lettori girerà per l'aula e ogni lettore potrà scegliere un solo titolo sul quale cliccare per leggerlo per intero. Se lo sceglie farà sul foglio una piccola x. Vince la squadra i cui articoli saranno i più scelti (i cui fogli avranno totalizzato più x). Discutiamo insieme:

- Come mai hanno vinto questi titoli?
- Cosa avevano di accattivante?
- Come si scrive un titolo acchiappa click?
- Come si capisce che un titolo è acchiappa click?


# TEST

**1. Cosa è il clickbaiting?**

**a.** Un tipo di pesca sportiva specializzato nella cattura di pesci che abboccano facilmente

**b.** Un metodo di attrarre l'attenzione degli utenti online con titoli ingannevoli o sensazionalistici

**c.** Una forma di marketing digitale che promuove prodotti innovativi

**d.** Un gioco online basato sulla velocità di click sullo schermo

**2. Quali sono i rischi del clickbaiting?**

**a.** Promozione di contenuti accurati e informativi

**b.** Generazione di interesse e coinvolgimento degli utenti online

**c.** Diffusione di informazioni ingannevoli o poco rilevanti

**d.** Miglioramento dell'esperienza di navigazione online

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare il clickbaiting?**

**a.** Cliccare su tutti i titoli sensazionalistici o ingannevoli che si incontrano online

**b.** Verificare attentamente il contenuto prima di cliccare su un titolo

**c.** Condividere liberamente contenuti senza valutarne l'attendibilità

**d.** Ignorare completamente i titoli dei contenuti online

**4. Come può la tecnologia aiutare a contrastare il clickbaiting?**

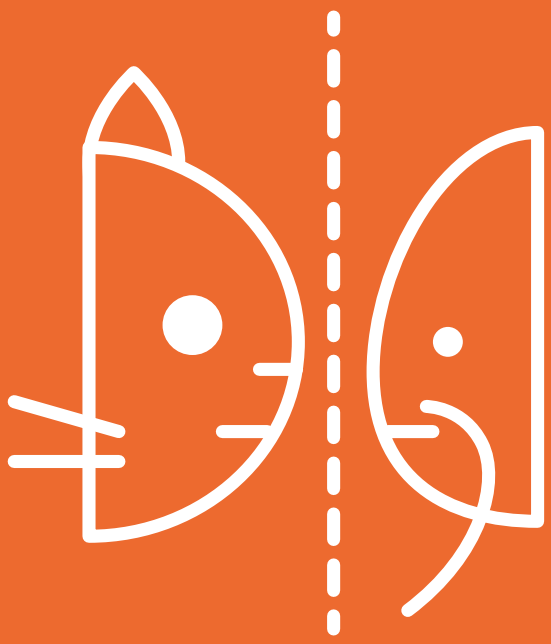
**a.** Diffondendo titoli ingannevoli in modo più efficace

**b.** Implementando algoritmi di rilevamento per identificare e ridurre il clickbaiting

**c.** Creando più contenuti sensazionalistici per attirare l'attenzione degli utenti

**d.** Facilitando la condivisione indiscriminata di contenuti online

Soluzioni: 1b, 2c, 3b, 4b



# 5

# Catfishing

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

QN IL GIORNO

# Finta fidanzata per 13 anni, truffato il pallavolista azzurro Roberto Cazzaniga

**Redazionale** **25 novembre 2021**

In inglese si definisce "catfish", ovvero "pesce gatto", ed è un fenomeno ben preciso: fingersi qualcuno che non si è e prendere in giro una persona, già nota o conosciuta in quel momento, utilizzando i social network. In italiano, però, il caso di cui è stato vittima Roberto Cazzaniga si definisce una vera truffa. Il pallavolista milanese, noto per aver vestito anche la maglia della Nazionale italiana di volley, per ben 13 anni è stato convinto di essere fidanzato con una ragazza che in realtà non esiste. E le ha anche fatto regali e dato soldi per un totale di 700mila euro. Altro che il "mi sono sentita sposata" di Eliana Michelazzo ai tempi dell'affaire Mark Caltagirone con Pamela Prati e Pamela Perricciolo.

## La storia

Nel 2008 Roberto Cazzaniga, opposto che ora gioca in serie B a Gioia del Colle, conosce una ragazza di nome Maya. Come? Tramite un'amica. Piccola "red flag", ovvero bandierina rossa che in criminologia segnala qualcosa di poco logico: Maya sui social network utilizzava le foto di Alessandra Ambrosio, ovvero modella di fama mondiale nonché angelo di Victoriàs Secret per diversi anni. Il pallavolista però non coglie il segnale e continua a conoscere Maya sino a innamorarsene. Senza mai incontrarla. Le fa regali, anche costosi come un'auto. E le dà soldi, tanti soldi. Centinaia di migliaia di euro. E continua non incontrarla. Così come continua a non avere il minimo sospetto sulla reale esistenza di Maya.

## La scoperta

Spinto da amici e parenti, Cazzaniga dopo 13 anni di "relazione" si rivolge alla trasmissione tv Le Iene e sporge denuncia alla Guardia di finanza. La scoperta è delle più amare: Maya non solo non esiste, ma Roberto Cazzaniga è vittima anche di un raggiro da parte di un'amica e del suo fidanzato. I bonifici del pallavolista - la "fidanzata" sosteneva di doversi pagare cure sanitarie per problemi di salute - non arrivavano a

Maya, bensì a una donna che viveva in Sardegna. Che ha prosciugato il conto corrente dell'innamorato. Ora la giustizia farà il proprio corso e ad occuparsi di questa vicenda sarà la magistratura.

# SCHEDA
## Catfishing
### di Ester Macrì e Lapo Cecconi

Il catfishing è una pratica ingannevole che si verifica quando una persona crea una falsa identità online per ingannare gli altri. Questa forma di frode può causare danni emotivi, finanziari e psicologici alle vittime coinvolte. Nello specifico il catfishing si verifica quando qualcuno crea un profilo falso sui social media o su altre piattaforme on line, fingendo di essere una persona diversa da quella che realmente è. Il catfish (colui che crea il falso profilo) può utilizzare foto, informazioni personali e storie inventate per ingannare gli altri e instaurare relazioni online.

Ma quali sono i principali rischi del fenomeno del catfishing?

- Danno emotivo: le persone coinvolte nel catfishing possono sviluppare legami emotivi con il catfish, credendo di avere una connessione autentica. Una volta scoperta la verità, possono sperimentare dolore, rabbia, vergogna e senso di tradimento.
- Truffe finanziarie: il catfish può cercare di ottenere denaro o informazioni finanziarie delle sue vittime attraverso inganni o false promesse. Questo può portare a gravi perdite finanziarie per le persone coinvolte.
- Violazione della privacy: le vittime del catfishing possono subire una violazione della loro privacy, condividendo informazioni personali con il catfish che possono essere utilizzate in modo dannoso.
- Rischio per la sicurezza personale: in alcuni casi, il catfish può raccogliere informazioni personali sensibili o conoscere dettagli intimi della vita della vittima. Questo può mettere a rischio la sicurezza fisica e la privacy delle persone coinvolte.

Come evitare di cadere vittima di un catfish? Quali atteggiamenti concreti è necessario seguire?

1. Verificare l'identità online: è importante cercare di verificare sempre l'identità delle persone con cui si interagisce online. Controllando le informazioni fornite, confrontandole con altre fonti o chiedendo incontri video per confermare che la persona corrisponda alla propria identità dichiarata, permette di prevenire i fenomeni

di catfishing.

2. Non condividere informazioni personali sensibili: è necessario evitare di condividere informazioni personali sensibili, come indirizzi, numeri di telefono o dettagli finanziari, con persone sconosciute o di cui si hanno sospetti.
3. Fare ricerche online: un'altra strada è quella di utilizzare strumenti di ricerca online per cercare informazioni sulle persone con cui si interagisce. In questo caso, si controllano i loro profili sui social media e si verifica se ci sono state segnalazioni di truffe o identità false associate al loro nome.
4. Fidarsi del proprio istinto: se qualcosa sembra sospetto o troppo bello per essere vero, è necessario fare attenzione e ascoltare il proprio istinto. Alcuni segnali del catfishing sono proprio la sensazione che qualcuno tenga nascoste le informazioni o che si comporti in modo incoerente.

La tecnologia, oggi, possiede strumenti avanzati per cercare di controllare, governare e contrastare il fenomeno del catfishing. Senza dubbio il riconoscimento automatizzato delle immagini consente di individuare l'utilizzo di foto di profili false o rubate. Questi strumenti possono essere utilizzati per verificare l'autenticità delle immagini utilizzate dai potenziali catfish. Inoltre, alcune piattaforme online stanno introducendo funzionalità di verifica dell'identità, come budget di verifica o sistemi di autenticazione a due fattori per aiutare a identificare e prevenire il carpfishing. La tecnologia può anche essere utilizzata per fornire programmi di formazione sulla consapevolezza digitale, educando le persone sui rischi del catfishing e fornendo strumenti per riconoscere i segnali di un possibile catfish. Infine, le piattaforme online forniscono i meccanismi di segnalazione per scovare ed evidenziare potenziali catfish e comportamenti sospetti per contribuire a ridurre il rischio di catfishing.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Controllo di identità"

Ogni studente dovrà scrivere una lista di accorgimenti per riuscire a capire se una persona conosciuta online è realmente chi dice di essere.
Confrontiamo le liste e discutiamo:

- È facile o difficile capire se una persona sta mentendo sulla sua identità?
- Quali di questi accorgimenti sono i più utili?
- Vi è mai capitato di capire che una persona con cui parlavate online non era chi diceva di essere? Come ve ne siete accorti? Cosa è successo?

# TEST

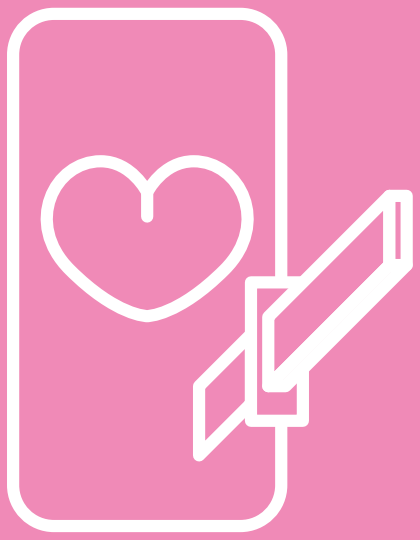
**1. Cos'è il catfishing?**
**a.** Un tipo di pesca sportiva
**b.** Un metodo per catturare gatti selvatici
**c.** Una pratica in cui una persona si finge qualcun altro online
**d.** Un gioco di ruolo basato sui gatti

**2. Quali sono i rischi del catfishing?**
**a.** Miglioramento delle relazioni online
**b.** Creazione di connessioni autentiche e significative
**c.** Inganno, manipolazione emotiva e potenziale pericolo per le vittime
**d.** Promozione della trasparenza e della fiducia online

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare il catfishing?**
**a.** Credere ciecamente a tutto ciò che viene presentato online
**b.** Condividere liberamente informazioni personali con sconosciuti online
**c.** Essere cauti e verificare l'autenticità delle persone online
**d.** Ignorare i segnali di potenziale catfishing

**4. Come può la tecnologia aiutare a contrastare il catfishing?**
**a.** Creando piattaforme online che consentono di nascondere l'identità degli utenti
**b.** Implementando algoritmi di rilevamento per identificare profili falsi o sospetti
**c.** Facilitando la creazione di identità false online
**d.** Diffondendo informazioni false per promuovere il catfishing

Soluzioni: 1c, 2c, 3c, 4b



# 6

# Revenge porn

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*

ARTICOLO

Il Sole 24 ORE

# Revenge porn, la tecnologia può aiutare ad arginare il fenomeno

**Redazionale** **3 novembre 2021**

C'è ancora molto da fare sul fronte della prevenzione e repressione del cosiddetto reato di revenge porn. Oggi le vittime hanno a disposizione strumenti di tutela penali e amministrativi che però non sempre sono sufficienti a evitare la viralità dei contenuti. Sul fronte penale si può sporgere querela entro 6 mesi dalla conoscenza del fatto (termine doppio rispetto a quello ordinario). Il reato è procedibile d'ufficio se commesso ai danni di una persona in condizione di inferiorità fisica o psichica o di una donna in gravidanza. Non è invece prevista un'aggravante specifica a tutela dei minorenni.

## I meandri del web

La condivisione dei materiali può, però, avvenire attraverso un numero talmente ampio di piattaforme - applicazioni di messaggistica crittografati, social network, siti hard, peer to peer, mailing list - che tali strumenti da soli non bastano a bloccare i contenuti. Il progetto pilota del Garante dello scorso marzo per ora riguarda soltanto Facebook e Instagram e non le piattaforme di messaggistica come WhatsApp o Telegram, il che di fatto ne riduce notevolmente la portata, anche se va nella giusta direzione.
La condivisione in modalità compressa e la criptografia end to end, poi, non agevolano la scansione e il blocco preventivo dei contenuti. Inoltre, non esiste ancora la possibilità di una deindicizzazione preventiva da parte dei motori di ricerca.

## Il ricorso all'intelligenza artificiale

Eppure la tecnologia consente di scansionare i contenuti in forma massiva. Non è un caso che quest'estate Apple abbia annunciato di volerlo fare per evitare la condivisione dei contenuti pedopornografici. A parte le giuste osservazioni sugli eventuali abusi dello strumento in termini di violazione della privacy, ciò dimostra che l'intelligenza artificiale è in grado di confrontare le immagini con quelle segnalate evitando il caricamento dei contenuti, cosa che avviene già in molti casi per le violazioni del diritto d'autore.
Spesso poi la condivisione del materiale avviene anche con sconosciuti, di cui può diventare difficile l'identificazione. Oppure la condivisione con terze persone non è ancora avvenuta, ma la vittima vive col timore che possa succedere.

Tutti motivi per rafforzare gli strumenti preventivi, non solo penali. In caso di cyberbullismo i minorenni hanno a disposizione anche lo strumento dell'ammonimento del questore, che può essere attivato pure per fatti legati al cosiddetto sexting. Ogni Stato però continua a legiferare in maniera diversa e questo non agevola la rimozione dei contenuti e la collaborazione tra le autorità e le piattaforme coinvolte.

## Un filtro agli hosting

La Corte di giustizia Ue ha, però, stabilito che i singoli Paesi dell'Unione possono imporre ai social network e agli hosting in generale di cancellare o disabilitare l'accesso a contenuti illeciti in tutto il mondo (sentenza del 3 ottobre 2019 nella causa C-18/18).
La questione dei filtri preventivi degli hosting era già arrivata del 2011 davanti ai giudici del Lussemburgo, che nel caso delle violazioni del diritto d'autore avevano considerato però troppo oneroso per i social network prevedere un sistema di monitoraggio costante (sentenza del 24 novembre 2011 nella causa C-70/10).
A diverse considerazioni potrebbero giungere nel caso di contenuti intimi, visto che il giudizio di bilanciamento potrebbe propendere a favore degli utenti che chiedono ormai da tempo maggiori tutele.

# SCHEDA

## Revenge porn

di Ester Macrì e Lapo Cecconi

Il Revenge porn, che si potrebbe tradurre in italiano come "pornografia di vendetta", è una forma di abuso digitale in cui immagini o video sessuali privati vengono diffusi senza il consenso della persona coinvolta. Questo atto malizioso può causare gravi danni emotivi, psicologici e sociali alle vittime coinvolte.
Nel dettaglio, si verifica il Revenge porn quando immagini o video intimi di una persona vengono condivisi o diffusi senza il suo consenso. Spesso queste immagini sono detenute da ex partner o da terze persone con l'intento di umiliare, ricattare o diffamare la vittima. Il Revenge porn rappresenta una grave violazione della privacy e dei diritti delle persone coinvolte oltre che un vero e proprio reato. Infatti, in Italia, secondo l'articolo 612-bis, chiunque diffonde, tramite qualsiasi mezzo di comunicazione, immagini o video con contenuti sessuali di una persona senza il suo consenso, al fine di ledere la reputazione o la dignità della persona stessa, è soggetto a sanzioni penali.
La pena prevista per chi commette Revenge porn in Italia può variare a seconda delle circostanze specifiche del caso. In generale, il reato è punibile con la reclusione da 6 mesi a 5 anni.

Se la vittima è minorenne o se il reato è commesso da parte di un ex partner o coniuge, la pena può essere aumentata.

Ma quali sono i maggiori rischi che le vittime del Revenge porn devono subire?

- Danneggiamento della reputazione: il Revenge porn può danneggiare gravemente la reputazione e l'immagine di una persona, con conseguenze a lungo termine sulla sua vita personale, professionale e sociale.
- Danno emotivo e psicologico: le vittime del Revenge porn spesso sperimentano ansia, depressione, vergogna, isolamento sociale e altri effetti negativi sulla salute mentale. Questo abuso digitale può causare gravi traumi emotivi.
- Estorsione e ricatto: gli autori del Revenge porn possono tentare di ricattare o estorcere le vittime, minacciando di diffondere ulteriormente il materiale compromettente a meno che non accettano le loro richieste.
- Diffusione non controllata: una volta che le immagini o i video sono condivisi online, è difficile controllare o rimuovere completamente il materiale, aumentando così il rischio di ulteriore diffusione e danni continui alla vittima.

Come evitare di cadere vittime di pratiche di Revenge porn? Ecco alcuni atteggiamenti concreti da adottare:

1. Consenso informato: è necessario assicurarsi di avere un consenso chiaro e informato da parte di tutte le persone coinvolte prima di condividere o scattare immagini o video intimi.
2. Protezione dei dispositivi: è importante mantenere i propri dispositivi digitali, come telefoni o computer, protetti da password robuste e aggiornamenti regolari del software. Inoltre, è importante evitare di salvare immagini o video intimi sul cloud o su dispositivi non sicuri.
3. Condivisione selettiva: è necessario fare attenzione a chi e come condividere immagini o video personali; la selezione della scelta delle persone a cui inviare del materiale deve essere accurata e le piattaforme o le app di condivisione di contenuti sensibili devono essere sicure.
4. Educazione sulla privacy digitale: è necessario partecipare a programmi di formazione sulla privacy digitale, in modo da conoscere i propri diritti e come proteggersi da situazioni di Revenge porn. È importante, infatti, imparare a gestire le impostazioni di privacy sui social media e a riconoscere i segnali di potenziale abusi.

La tecnologia, con le sue potenti mezzi e strumenti, può aiutare a prevenire e a contrastare il fenomeno del Revenge porn nei seguenti modi:

- Strumenti di segnalazione e rimozione: le piattaforme di social media e gli operatori di servizi online possono fornire strumenti di segnalazione per consentire alle

vittime o agli utenti di segnalare contenuti di Revenge porn punto e piattaforme possono poi agire rapidamente per rimuovere tale materiale abusivo.

- Software di riconoscimento delle immagini: la tecnologia può essere utilizzata per sviluppare software di riconoscimento delle immagini che aiuta a identificare e segnalare i Revenge porn. Questi strumenti possono facilitare il rilevamento e la rimozione del materiale dannoso.
- Leggi e politiche: i governi possono promuovere leggi specifiche per affrontare il Revenge porn, consentendo alle vittime di denunciare l'abuso e perseguire legalmente gli autori. Le piattaforme online, invece, possono adottare politiche rigorose contro il Revenge porn e fornire supporto alle vittime.
- Supporto e consulenza: La tecnologia può essere utilizzata per offrire supporto e consulenza alle vittime di Revenge porn, fornendo risorse, linee guida e servizi di assistenza online per aiutare le persone a gestire la situazione e ottenere sostegno legale ed emotivo.

Il Revenge porn rappresenta una grave violazione della privacy e dei diritti delle persone coinvolte e un vero e proprio reato perseguibile penalmente.
La tecnologia può svolgere un ruolo significativo nel contrastare il fenomeno attraverso strumenti di segnalazione e rimozione, software di riconoscimento delle immagini, legge e politiche adeguate e offerta di supporto e consulenza alle vittime.
Promuovendo l'educazione, la consapevolezza e l'uso responsabile della tecnologia, possiamo contribuire a proteggere l'intimità digitale e combattere il Revenge porn.

# TRACCIA PER L'ATTIVITA' IN CLASSE

## "Come comportarsi in caso di Revenge porn"

La classe viene divisa in due gruppi.
Un gruppo impersona la vittima di Revenge porn e un gruppo i compagni di classe.
Il primo gruppo dovrà scrivere come si deve comportare la vittima e il secondo gruppo come si comportano i compagni di classe. Quali azioni compiono? Come si sentono?
I due gruppi si confrontano su quanto hanno scritto.

# TEST

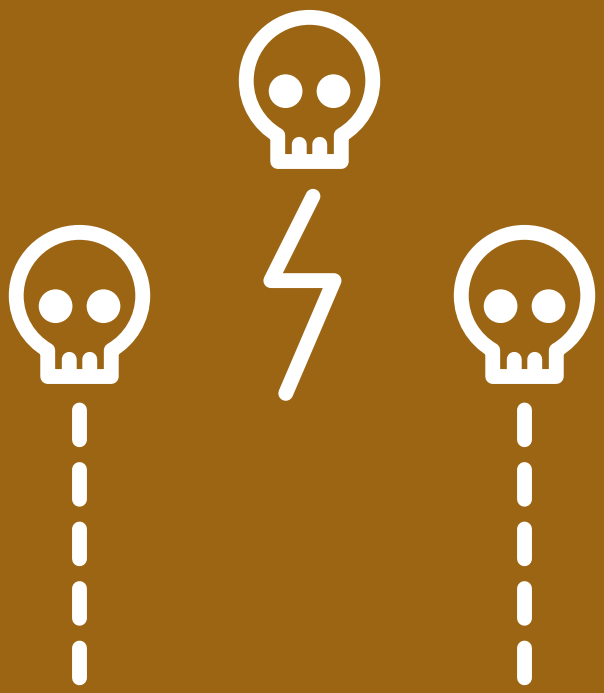
**1. Cos'è il Revenge porn?**
**a.** Una forma di intrattenimento legale online
**b.** La diffusione consensuale di contenuti intimi online
**c.** La divulgazione non consensuale di materiale sessualmente esplicito di una persona
**d.** Un gioco di ruolo online incentrato sulla vendetta

**2. Quali sono i rischi del Revenge porn?**
**a.** Creazione di una sana consapevolezza dell'intimità digitale
**b.** Protezione dei diritti delle persone coinvolte
**c.** Danneggiamento della reputazione, trauma emotivo e violazione della privacy
**d.** Promozione di una cultura del rispetto e dell'empatia online

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare Revenge porn?**
**a.** Condividili liberamente contenuti intimi online
**b.** Mantenere la consapevolezza della propria Intimità e limitare la condivisione di contenuti sensibili
**c.** Ignorare rischi e le conseguenze dell'invio di materiale intimo da altre persone
**d.** Non cercare supporto o assistenza in caso di Revenge porn

**4. Come può la tecnologia aiutare a contrastare il Revenge porn?**
**a.** Diffondendo il Revenge porn in modo più rapido ed efficace
**b.** Implementando strumenti di segnalazione e rimozione per contenuti di Revenge porn
**c.** Facilitando la condivisione non consensuale di materiale intimo
**d.** Creando nuove piattaforme online per la diffusione dei Revenge porn

Soluzioni: 1c, 2c, 3b, 4b



# 7

# Shitstorm

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

Il Messaggero

# Perché l'odio online è una forma di censura

**di Andrea Andrei** **16 Luglio 2020**

In gergo internettiano si chiama "shitstorm" (letteralmente, "tempesta di merda"), ed è un fenomeno tipico - e per la verità molto diffuso - sui social network. Consiste nel riversare su una persona ogni tipo di insulto e di minaccia, con tutti i mezzi possibili, che siano messaggi pubblici o privati, con la classica logica del branco, in cui tutti si sentono legittimati dalle azioni altrui e si muovono in un sostanziale anonimato.

È un fenomeno che colpisce soprattutto personaggi pubblici e giornalisti, ma che spesso diventa una micidiale arma per i bulli nelle scuole. Di solito, a meno che non si tratti di un vero e proprio fenomeno persecutorio ai danni di un singolo, la tempesta dura poco, al massimo qualche giorno, anche se è di elevata intensità.
Comunque, di sicuro rientra in quelle esperienze che sarebbe meglio evitare.

Perché la shitstorm è, a tutti gli effetti, una forma di violenza. Un'arma, appunto, che spesso viene sfruttata da personaggi famosi o gruppi d'interesse (che siano i tifosi di una squadra di calcio o i fan di una cantante) per reprimere le voci scomode o contrarie. Una sorta di spedizione punitiva 2.0 e quindi, quando fatta contro i giornalisti, una forma di censura a tutti gli effetti. Per questo forse sarebbe ora di cominciare a prevedere delle sanzioni non tanto per i "picchiatori", quanto per i mandanti.
Anche per quelli che usano la violenza fatta contro di loro come scusa per scatenarne dell'altra.

# SCHEDA
# Shitstorm
## di Ester Macrì e Lapo Cecconi

La "shitstorm" è un fenomeno sempre più diffuso nell'era digitale e si verifica nel caso in cui una persona o un'azienda venga bersagliata da una valanga di critiche, insulti e commenti negativi su piattaforme online. Una shitstorm è una vera e propria tempesta di commenti negativi, spesso di natura offensiva e aggressiva, che si scatena contro una persona o un'organizzazione su internet. Può essere innescata da una controversia, un'opinione impopolare o anche solo un errore commesso pubblicamente.
Due possibili esempi di shitstorm sono il caso di una celebrità che pubblica un commento insensibile sui social media e viene attaccata da migliaia di utenti arrabbiati, oppure un'azienda che lancia una campagna pubblicitaria controversa e si trova sommersa da una marea di critiche e insulti.
La shitstorm può avere conseguenze negative significative per le persone coinvolte. Può causare stress emotivo, ansia e persino danneggiare la reputazione di un individuo o di un'azienda. Inoltre, può portare a un clima di odio e intolleranza online, in cui le persone si sentono incoraggiate a insultare e aggredire gli altri anonimamente.

Se ci si trova vittime di una shitstorm, è importante mantenere la calma e adottare le seguenti misure:

- Non rispondere con rabbia: è fondamentale evitare di rispondere con insulti o provocazioni, poiché ciò potrebbe alimentare ulteriormente la shitstorm. Mantenere un tono calmo e rispettoso, se si sceglie di rispondere.
- Bloccare o filtrare i commenti: utilizzare le funzionalità di blocco o filtraggio disponibili sulle piattaforme social per evitare di vedere i commenti negativi o offensivi. Questo permetterà di proteggere la propria salute mentale e limitare l'impatto negativo della shitstorm.
- Cercare supporto: rivolgersi a persone fidate come amici, familiari o professionisti per ottenere sostegno emotivo durante questo periodo difficile. Condividere le proprie esperienze può aiutare a superare gli effetti negativi della shitstorm.

Per evitare di finire in una shitstorm, si possono adottare alcune precauzioni:

- Pensare prima di postare: riflettere attentamente prima di condividere commenti o opinioni online. Considerare le possibili conseguenze e il modo in cui il proprio messaggio potrebbe essere interpretato da diverse persone.
- Essere rispettosi e empatici: mantenere un approccio rispettoso nei confronti degli altri, anche se si è in disaccordo. Evitare di attaccare o insultare gli altri in modo

gratuito.

- Essere consapevoli delle implicazioni: comprendere che ciò che si pubblica online può avere un impatto duraturo sulla propria reputazione e sull'immagine che gli altri hanno di noi. Prendere il tempo necessario per valutare se ciò che si sta condividendo è appropriato e coerente con i propri valori.

La shitstorm è un fenomeno pericoloso e sgradevole che può colpire chiunque sia attivo online. È importante conoscere le strategie per affrontarla se si è vittime e prendere precauzioni per evitarla. Mantenere il rispetto reciproco, la calma e la consapevolezza delle proprie azioni online possono contribuire a creare un ambiente digitale più sano e costruttivo.

La tecnologia potrebbe svolgere un ruolo significativo nel contrastare il fenomeno delle shitstorm. Una delle possibili soluzioni potrebbe essere l'implementazione di filtri avanzati da parte delle piattaforme di social media e dei siti web. Questi filtri utilizzerebbero algoritmi di intelligenza artificiale per individuare automaticamente i commenti offensivi e insultanti, limitando così l'impatto delle shitstorm. Inoltre, le piattaforme online potrebbero dedicare maggiori risorse alla moderazione dei contenuti, impiegando team appositi per monitorare e rimuovere i commenti inappropriati. Questo aiuterebbe a creare un ambiente digitale più sicuro e contrasterebbe la diffusione delle shitstorm.

Oltre ai filtri e alla moderazione attiva, la tecnologia potrebbe essere utilizzata per sviluppare programmi di educazione digitale. Questi programmi avrebbero l'obiettivo di insegnare agli utenti come comportarsi responsabilmente e rispettosamente online. Attraverso l'educazione digitale, le persone potrebbero apprendere come gestire le critiche e i conflitti in modo costruttivo, promuovendo un dialogo sano e civile. Questo tipo di formazione potrebbe contribuire a ridurre l'incidenza delle shitstorm fornendo agli utenti le competenze necessarie per interagire in modo positivo e responsabile su internet.

Un'altra possibile soluzione potrebbe essere l'implementazione di meccanismi per tracciare gli autori di commenti offensivi anonimi. Pur rispettando la privacy degli utenti, potrebbe essere importante sviluppare strumenti che consentano di individuare le persone che si nascondono dietro commenti negativi e offensivi. Questo potrebbe aumentare la responsabilità degli utenti e dissuadere comportamenti dannosi, contribuendo a ridurre l'incidenza delle shitstorm.

Inoltre, le piattaforme online potrebbero incentivare la promozione del feedback positivo e costruttivo. Creare spazi in cui gli utenti possano evidenziare contenuti di valore e esprimere apprezzamento verso le buone pratiche potrebbe favorire un ambiente virtuale più equilibrato. In questo modo, si potrebbe creare un clima di sostegno reciproco e incoraggiare una cultura digitale basata sulla gentilezza e sulla condivisione di contenuti di qualità.

È importante sottolineare, tuttavia, che la tecnologia da sola non risolverà completamente il problema delle shitstorm. È necessario adottare un approccio olistico che comprenda anche l'educazione degli utenti e la promozione di comportamenti rispettosi e costruttivi online. L'individuo deve assumersi la responsabilità di come si comporta e interagisce su internet, ricordando di trattare gli altri con gentilezza e rispetto.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Storia di una shitstorm"

Agli studenti viene chiesto di cercare un caso famoso di shitstorm (possono scegliere anche uno che conoscono già) e raccontarlo seguendo questa traccia:

- Chi è la vittima della shitstorm?
- Cosa ha scatenato la shitstorm?
- Quali sono state le accuse?
- Chi sono stati i più feroci accusatori?
- Come si è difesa la vittima?
- Come è andata a finire?
- Ci sono state conseguenze?
- Cosa possiamo imparare da questa situazione?

# TEST

**1. Che cos'è una shitstorm?**
**a.** Una tempesta di commenti positivi su piattaforme online
**b.** Una serie di critiche costruttive verso una persona o un'azienda
**c.** Una valanga di commenti negativi offensivi su internet
**d.** Una campagna pubblicitaria di successo

**2. Quali sono alcuni rischi associati a una shitstorm?**
**a.** Aumento della reputazione e dell'immagine di un individuo o un'azienda
**b.** Isolamento sociale e il ritiro dai social media
**c.** Maggiore fiducia nel dialogo e nella condivisione di opinioni
**d.** Sensazioni di gratitudine e soddisfazione personale

**3. Quali sono alcune misure che si possono adottare per affrontare una shitstorm?**
**a.** Rispondere con rabbia e insultare gli aggressori
**b.** Bloccare o filtrare commenti negativi
**c.** Ignorare completamente la situazione
**d.** Evitare di cercare supporto da persone fidate

**4. Come potrebbe la tecnologia aiutare a contrastare la shitstorm?**
**a.** Incentivando la diffusione di commenti offensivi e negativi
**b.** Implementando filtri e moderazione dei contenuti per limitare i commenti offensivi
**c.** Promuovendo una cultura di odio e intolleranza online
**d.** Monitorando e incentivando l'anonimato per gli autori di commenti negativi

Soluzioni: 1c, 2b, 3b, 4b

8

# Furto di identità digitale

di Ester Macrì

*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

e Lapo Cecconi

*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

ARTICOLO

Il Sole 24 ORE

# Identità digitale a rischio? Dalla start up insurtech arriva l'app per tutelarla

**di Gianni Rusconi** **20 aprile 2023**

Oltre un terzo degli italiani ha dichiarato di essere stato vittima di un crimine digitale: lo dice una recente ricerca condotta da Ipsos per conto di Wallife. E non è certo l'unica indagine a confermare una tendenza che vede le violazioni degli account social, la clonazione delle carte di pagamento e la diffusione non autorizzata di immagini e video personali essere tra i reati che riguardano l'identità digitale più diffusi.
L'esempio più ricorrente è quello degli strumenti (impiegati anche in ambito professionale) che richiedono l'accesso biometrico per essere riconosciuti, come il Face ID e il Touch ID di Apple, e quindi soluzioni pensate per sbloccare in sicurezza il proprio dispositivo mobile, autenticare gli acquisti perfezionati online o accedere alle applicazioni. Sebbene la diffusione crescente di questi strumenti si porti inevitabilmente dietro maggiori possibilità di attacco da parte dei cybercriminali e conseguenti maggiori occasioni per i furti di identità digitale, la percezione dei rischi a cui gli individui sono esposti è ancora molto limitata.
Nasce quindi da questi presupposti il lancio dell'app Wallife, soluzione che la start up insurtech romana fondata nel 2020 (fra i suoi investitori vi sono i fondi di venture capital United Ventures, Azimut Digitech e Gellify) ha presentato ufficialmente e che promette di proteggere, per l'appunto, l'identità digitale delle persone mitigando il rischio di furto dei dati personali dallo smartphone.
Il plus dichiarato dell'app è una tecnologia proprietaria che sfrutta avanzati algoritmi di machine learning per intercettare e rilevare più di sessanta minacce di sicurezza che possono compromettere il dispositivo e le app installate. Grazie a un sistema di rilevazione anti-phishing, inoltre, la soluzione consente di verificare l'affidabilità di link, messaggi Sms e documenti che potrebbero nascondere possibili tentativi di phishing.

Direttamente dall'app, infine, gli utenti potranno gestire in totale autonomia la propria polizza Biometrics ID, servizio lanciato lo scorso a settembre 2022 con l'intento di assicurare l'identità digitale dei clienti proteggendone l'accesso ai propri conti correnti bancari, ai sistemi di pagamento online e ai social media. Come ha confermato anche

Maria Enrica Angelone, la Ceo di Wallife, la nuova app sarà disponibile gratuitamente per 90 giorni per tutti e sarà liberamente acquistabile unitamente alla copertura assicurativa al termine del periodo di prova.

# SCHEDA
# Furto di identità digitale
## di Ester Macrì e Lapo Cecconi

Il furto di identità digitale è un crimine che si verifica quando vengono rubate informazioni personali sensibili per assumere un'identità altrui e commettere frodi finanziarie o altre attività illegali.
Si verifica quando dei criminali ottengono e utilizzano illegalmente informazioni personali con nome, indirizzo, numero di previdenza sociale, informazioni finanziarie o di carte di credito al fine di commettere frodi. Queste informazioni possono essere ottenute attraverso attacchi informatici, phishing, hacking o forti fisici di dispositivi.

I principali rischi per gli individui legati al furto di identità digitale sono:

- Frodi finanziarie: i criminali possono utilizzare le informazioni personali rubate per effettuare transazioni finanziarie fraudolente, accedere ai conti bancari, aprire carte di credito o fare acquisti online, causando danni finanziari significativi alla vittima.
- Danneggiamento della reputazione: gli hacker possono utilizzare le identità di una persona per commettere attività illegali online, lasciando la vittima a fronteggiare le conseguenze legali o danneggiando la sua reputazione online.
- Violazione della privacy: il furto d'identità digitale può compromettere la privacy personale, consentendo ai criminali di accedere a informazioni personali, messaggi privati o fotografie, che possono essere utilizzate per ricattare o molestare la vittima.
- Impatto emozionale: essere vittima di furto di identità digitale può causare stress, ansia e preoccupazione costante per la sicurezza personale e finanziaria.
- Nel mondo digitale in cui viviamo, proteggere la nostra identità online è di fondamentale importanza.

Per evitare il furto di identità digitale, è importante essere consapevoli della problematica e adottare alcuni atteggiamenti semplici ma concreti:

1. Protezione delle informazioni personali: è necessario mantenere le informazioni personali al sicuro, evitando di condividerle con sconosciuti o su siti web non affidabili. Due consigli per la protezione dei dati possono essere quello di utilizzare

password complesse e spesso aggiornate e quello di evitare di inserire i dati sensibili su siti non sicuri o collegati a link sospetti.
2. Attenzione a e-mail e messaggi: è necessario non solo essere cauti riguardo a e-mail e messaggi che richiedono informazioni personali o finanziarie ma anche evitare di cliccare sul link sospetti o scaricare legati provenienti da fonti non attendibili.
3. Utilizzo di software di sicurezza: installare e mantenere aggiornato un software antivirus e antimalware affidabile sul proprio dispositivo può contribuire a prevenire il furto di identità digitale; questi programmi, infatti, possono rilevare e bloccare minacce online, fornendo una maggiore sicurezza.
4. Monitoraggio delle attività finanziarie: è necessario controllare regolarmente i propri conti finanziari e le transazioni e segnalare tempestivamente qualsiasi attività sospetta alle società competenti e alle istituzioni finanziarie.

Le nuove tecnologie svolgeranno un ruolo fondamentale nella prevenzione e nel contrasto del furto identità digitale, un fenomeno purtroppo sempre più attuale. Molti sono gli strumenti di sicurezza informatica, sotto forma di software sempre più avanzati, che offrono funzionalità come il rilevamento di malware, il blocco di siti web dannosi e la protezione dei dati personali. Inoltre, le nuove tecnologie offrono la possibilità di autenticazione a due fattori: questo metodo, richiede l'uso di una seconda forma di verifica, come un codice inviato al proprio telefono, per accedere proprio account, rendendo più difficile per i criminali accedere alle proprie informazioni personali. Quello che le nuove tecnologie offrono, inoltre, sono strumenti e applicazioni con crittografia dei dati, specialmente quando si tratta di comunicazioni sensibili o di archiviazione di informazioni personali. Per finire, la tecnologia può essere utilizzata per educare le persone sui rischi del furto identità digitale, fornendo informazioni sulle migliori pratiche di sicurezza e sensibilizzando sulle tattiche utilizzate dai criminali informatici.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Identificazione a due fattori"

Agli studenti viene chiesto di controllare su quali dei loro canali hanno attivato l'identificazione a due fattori.

- Chi ha attivato l'identificazione a due fattori? Su quali piattaforme? Perché?
- Chi non l'ha attivata come mai non lo ha fatto?
- Quali sono i rischi di non attivare l'identificazione a due fattori?

# TEST

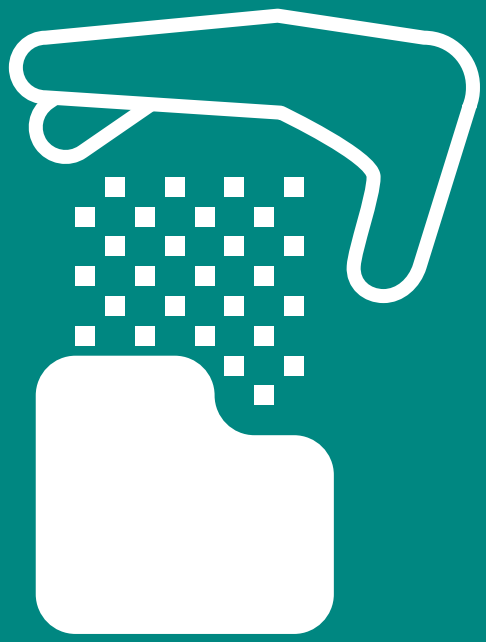
**1. Cos'è il furto di identità digitale?**
**a.** Utilizzo legale delle informazioni personali di qualcun altro
**b.** Protezione dei dati personali su internet
**c.** Acquisizione e utilizzo non autorizzato delle informazioni personali di un'altra persona
**d.** Scambio di identità tra due individui online

**2. Quali sono i rischi del furto di identità digitale?**
**a.** Miglioramento della sicurezza online
**b.** Utilizzo improprio delle informazioni personali per scopi finanziari o fraudolenti
**c.** Protezione dei dati personali
**d.** Condivisione responsabile delle informazioni online

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare il furto di identità digitale?**
**a.** Condividere liberamente informazioni personali su siti web non sicuri
**b.** Utilizzare password complesse e aggiornare regolarmente gli account online
**c.** Fare clic su link sospetti nelle e-mail o sui social media
**d.** Connettersi a Reti wi-fi pubbliche senza precauzioni

**4. Come può la tecnologia aiutare a contrastare il furto di identità digitale?**
**a.** Facilitando l'accesso e la condivisione delle informazioni personali
**b.** Crittografando i dati e proteggendo le transazioni online
**c.** Diffondendo informazioni personali in modo indiscriminato
**d.** Creando nuovi account online con facilità

Soluzioni: 1c, 2b, 3b, 4b



# 9

# Furto di dati

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione,*
*Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

QN LA NAZIONE

# Occhio alle insidie della vita social in aumento le truffe telematiche

**Redazionale** **17 febbraio 2023**

La campagna di educazione al buon uso del mondo dei social e di sensibilizzazione alle trappole che possono trovarsi navigando in rete arriva oggi a Sarzana. L'iniziativa itinerante promossa da Polizia postale e delle comunicazioni in collaborazione con il Ministero della pubblica istruzione e la Questura della Spezia stamanI fa tappa in piazza Matteotti unica data fissata nella nostra provincia.

Un tema di stretta attualità considerato che negli ultimi tempi anche il commissariato di Sarzana ha fatto fronte a un sensibile aumento di denunce da parte di utenti della rete che si sono fidati di siti non sicuri o sono stati vittime del furto dei dati personali e di quelli delle carte di credito. Gli uffici hanno già proceduto in pochi mesi a denunciare 12 persone, italiane e straniere, per contraffazione di carte di credito. Ben 23 "navigatori" si sono affidati a fantomatici siti specializzati nella vendita delle macchine usate a prezzi vantaggiosi ma hanno perso soltanto tempo e soldi; 22 utenti si sono visti rubare i dati della carta di credito o del bancomat utilizzato per gli acquisti su siti non protetti. Sono state 9 le frodi informatiche: falsi profili Facebook e di altre piattaforme violati e utilizzati da altri. Insomma, un'attività criminosa che sta prendendo campo e obbliga anche le forze dell'ordine a continui aggiornamenti per tenere il passo di hacker e esperti "ladri" di identità.

Oggi, dunque, arriverà il camper 'Una vita da social', aperto agli incontri con scuole e cittadinanza alla presenza degli esperti del settore informatico della Polizia di Stato. In mattinata saranno presenti anche la sindaca Cristina Ponzanelli, il questore Lilia Fredella, la vice questore dirigente del commissariato cittadino Annamaria Ciccariello. Gli operatori della Polizia Postale spiegheranno le tecnologie di ultima generazione, utilissime per affrontare le principali insidie del web. Le lezioni con le scolaresche si svolgono dalle 9 alle 13 mentre nel pomeriggio il truck sarà aperto a associazioni e cittadinanza fino alle 16.30.

# SCHEDA
# Furto di dati
di Ester Macrì e Lapo Cecconi

Il furto di dati è una minaccia sempre crescente nell'era digitale in cui viviamo.
Si verifica quando informazioni sensibili o riservate vengono illegalmente acquisite o diventano accessibili da parte di terze parti non autorizzate. Si verifica, inoltre, quando informazioni personali o riservate, come nome, indirizzo, numeri di telefono, dati finanziari o dati di accesso, vengono compromessi da attacchi informatici, frodi o violazioni della sicurezza. Coloro che hanno rubato i dati, possono utilizzare queste informazioni per commettere frodi finanziarie, durante la privacy o compiere attività illegali.

Il furto dei dati sta diventando qualcosa di sempre più attuale sia per i singoli individui che per le grandi aziende e i rischi che possono verificarsi, sono di molteplice natura:

- Frodi finanziarie: i dati finanziari compromessi possono essere utilizzati per effettuare transazioni non autorizzate, aprire carte di credito o accedere a conti bancari, causando danni finanziari significativi alle vittime.
- Violazione della privacy: il furto di dati può compromettere la privacy personale, consentendo a terze parti non autorizzate di accedere a informazioni personali, foto, messaggi privati o altre informazioni sensibili. ciò può portare a ricatti, estorsioni o molestie.
- Furto di identità: i dati rubati possono essere utilizzati per creare identità false o impersonale delle vittime, aprendo la strada a frodi o attività illegali al loro nome.
- Danneggiamento della reputazione: la divulgazione di dati sensibili può danneggiare la reputazione di individuo e organizzazioni, compromettendo la fiducia dei clienti o dei partner commerciali.

È importante imparare a proteggersi da questo fenomeno maligno e sempre più attuale.
Questo può essere fatto iniziando a mettere in atto alcuni semplici comportamenti:

1. Utilizzare password sicure, lunghe, complesse e uniche per i propri account online è il primo passo per proteggersi dal furto dei dati. Inoltre, sarà necessario evitare di utilizzare informazioni personali facilmente deducibili e cambiare le password regolarmente utilizzando l'autenticazione a due fattori quando disponibile.
2. Come secondo consiglio, vi è l'attenzione e la cautela da riporre sulle mail o sui messaggi sospetti che richiedono informazioni personali o finanziarie. è essenziale evitare di cliccare sul link o allegati provenienti da mittenti sconosciuti o non

attendibili.

3. Sarà, inoltre, necessario mantenere sempre aggiornato il software del dispositivo, inclusi il sistema operativo, i programmi antivirus e gli aggiornamenti di sicurezza. Le facce di sicurezza, Inoltre, spesso correggono vulnerabilità che possono essere sfruttate dai criminali informatici.
4. Altro consiglio è quello di utilizzare strumenti di crittografia per proteggere i dati sensibili memorizzati sui propri dispositivi o durante le comunicazioni online. Il consiglio è, inoltre, quello di utilizzare connessioni sicure (https) Per accedere a siti web sensibili o effettuare transazioni online.

Come può la tecnologia aiutare a prevenire e contrastare questo fenomeno?
Le nuove tecnologie offrono molteplici opportunità partendo da soluzioni di sicurezza informatica come software antivirus e anti-malware affidabili per proteggere i propri dispositivi da attacchi informatici, malware e virus dannosi. Inoltre, firewall e filtri di sicurezza possono essere utilizzati per proteggere la rete da intrusioni indesiderate o da siti web dannosi. Con la crittografia si possono proteggere i dati più sensibili salvati sui propri dispositivi o durante le comunicazioni, rendendoli inaccessibili a terze parti non autorizzate. Infine, la consapevolezza e la formazione fornite dalle nuove tecnologie rendono gli individui sempre più consapevoli delle ultime minacce informatiche e contribuiscono a migliorare le pratiche di protezione dei dati.
In conclusione, il furto di dati rappresenta una minaccia reale nella nostra società digitale punto per proteggere le nostre informazioni personali e prevenire il furto di dati, è fondamentale adottare atteggiamenti consapevoli, come l'utilizzo di password sicuri, l'attenzione alle comunicazioni sospette e l'aggiornamento regolare del software. La tecnologia può anche fornire strumenti avanzati, come soluzione di sicurezza informatica e crittografia dei dati, per contrastare il furto di dati e proteggere la nostra informazione digitale.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Password inviolabili"

La classe è divisa a coppie. In ogni coppia una persona deve inventare una password con questi criteri: almeno un carattere maiuscolo, almeno un carattere speciale, almeno un numero, 6 caratteri in tutto. È importante che sia una password che riesce a ricordare. L'altro avrà 10 tentativi per indovinarla. Ad ogni tentativo se un carattere è giusto ma in una posizione sbagliata verrà evidenziato in giallo, se è giusto e nella posizione giusta verrà segnato in verde. Se quel carattere non è presente nella password sarà segnato in rosso.

Le coppie si possono poi scambiare.

Discutiamo insieme:

- È facile o difficile inventare una password sicura?
- Le nostre password sono sicure?
- Come potremmo migliorarle?

# TEST

**1. Cosa è il furto di dati?**
**a.** Acquisizione legale di informazioni personali da parte di aziende
**b.** Protezione dei dati personali su internet
**c.** Ottenimento non autorizzato di informazioni personali o riservate
**d.** Condivisione responsabile dei dati sensibili online

**2. Quali sono i rischi del furto di dati?**
**a.** Utilizzo responsabile delle informazioni personali
**b.** Protezione dei dati personali su internet
**c.** Possibilità di frode finanziaria, identità rubate o danni alla reputazione
**d.** Promozione della condivisione aperta dei dati online

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare il furto di dati?**
**a.** Condividere liberamente dati personali su siti web non sicuri
**b.** Utilizzare password complesse e autenticazione a due fattori per gli account online
**c.** Fare clic sul link sospetti nelle e-mail o sui social media
**d.** Connettersi a reti wi-fi pubbliche senza precauzioni

**4. Come può la tecnologia aiutare a contrastare il furto di dati?**
**a.** Facilitando la condivisione indiscriminata dei dati personali
**b.** Crittografando i dati e fornendo protocolli di sicurezza avanzati
**c.** Diffondendo informazioni personali su siti web non sicuri
**d.** Creando nuovi account online senza protezioni

Soluzioni: 1c, 2c, 3b, 4b

# 10

# Stalking online

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

IL GAZZETTINO

# Trentenne condannato per “stalking online”: vittima un'amica di 35 anni

**Redazionale** **16 Febbraio 2018**

PIACENZA/CORNEDO - Un giovane di 30 anni di Cornedo Vicentino ieri dal tribunale di Piacenza è stato condannato con il rito abbreviato a 1 anno di reclusione per “stalking online” nei confronti di una manager piacentina di 35 anni, la pena è stata sospesa. Il cornedense nel maggio 2016 aveva iniziato a molestare la giovane donna, minacciandola di morte assieme al compagno e alle figlie per una mancata risposta dell’agenzia di ricerca lavoro dove la donna riveste il ruolo di direttore commerciale. Attraverso i social media il 30enne ha offeso a ripetizione e minacciato di morte la 35enne, con la possibilità di tirarle addosso un secchio di acido. Con la denuncia presentata dalla donna è scattata un’indagine da parte della polizia postale servita a rilevare che il cornedense aveva creato undici profili Facebook per attaccare violentemente la donna e il suo compagno. Inoltre, aveva scaricato alcune foto della 35enne per aprire un aprire falso profilo su un sito pornografico con nome, cognome e numero di telefono. Al condannato che è ospite in una struttura per seguire una terapia psicologica sono stati revocati gli arresti domiciliari, sostituiti con la libertà vigilata: una perizia psichiatrica ha messo in luce che è affetto dalla sindrome di Asperger (disturbo pervasivo dello sviluppo imparentato con l'autismo, che non presenta compromissione dell'intelligenza, della comprensione e dell'autonomia, a differenza delle altre patologie classificate in tale gruppo).

# SCHEDA
# Stalking online
di Ester Macrì e Lapo Cecconi

La rivoluzione digitale ha aperto nuovi orizzonti di comunicazione e connessione, consentendoci di interagire con il mondo in modi mai visti prima.
Tuttavia, con le opportunità offerte dalla tecnologia emergono anche nuovi rischi, come ad esempio lo stalking online.
Ma che cos'è precisamente lo stalking online? Lo stalking online si verifica quando una persona utilizza internet e le sue piattaforme per perseguire, minacciare o molestarne un'altra. Questo comportamento può includere l'invio di messaggi indesiderati, la monitorizzazione costante dei profili social, l'accesso non autorizzato agli account online, la raccolta e la divulgazione di informazioni personali senza consenso.

Lo stalking online può avere gravi conseguenze per la vittima, sia dal punto di vista emotivo che fisico. I rischi includono:

- Violazione della privacy: Lo stalking online invade la privacy della vittima, creando un senso di paura e insicurezza costante.
- Molestie e minacce: Gli stalker online possono inviare messaggi minatori, insultanti o minacciosi, causando ansia e stress significativi.
- Diffamazione e cyberbullismo: L'abuso online può includere diffamazione, pubblicazione di contenuti imbarazzanti o umilianti e situazioni di cyberbullismo.
- Perdita di reputazione: Gli stalker online possono cercare di danneggiare la reputazione della vittima diffondendo informazioni personali o false accuse online.
- Pericolo fisico: In alcuni casi estremi, lo stalking online può sfociare in minacce e comportamenti fisicamente pericolosi.

Come è possibile proteggersi dallo stalking online? Sebbene la prevenzione totale dello stalking online possa essere difficile, ci sono alcune misure che si possono adottare per ridurre i rischi:

- Mantieni la privacy online: limita le informazioni personali che condividi sui social media e imposta le impostazioni di privacy in modo da controllare chi può accedere ai tuoi dati.
- Utilizza password sicure: crea password complesse e uniche per i tuoi account online, evitando di utilizzare informazioni facilmente accessibili o indovinabili.
- Non accettare richieste da estranei: evita di accettare richieste di amicizia o connessione da persone sconosciute sui social media e altre piattaforme online.

- Monitora la tua presenza online: controlla regolarmente i risultati delle ricerche sul tuo nome per individuare eventuali segni di stalking online e prendere provvedimenti tempestivi.
- Segnala e documenta: se pensi di essere vittima di stalking online, segnala immediatamente l'incidente alle autorità competenti e raccogli prove come screenshot, messaggi o registrazioni audio.

Il fenomeno dello stalking online è quindi un problema serio. Con l'avanzamento della tecnologia e la sempre maggiore dipendenza dalla connettività digitale, è probabile che il fenomeno dello stalking online continui a crescere e a adattarsi alle nuove piattaforme e modalità di comunicazione.
Nel futuro, potremmo assistere a sviluppi tecnologici che rendono ancora più facile per gli stalker individuare, monitorare e molestare le loro vittime.
Ad esempio, l'uso di intelligenza artificiale potrebbe consentire agli stalker di raccogliere e analizzare grandi quantità di dati personali per creare profili dettagliati delle loro vittime. Inoltre, l'espansione di Internet delle Cose potrebbe offrire agli stalker accesso a dispositivi connessi, come telefoni cellulari o dispositivi domestici intelligenti, che potrebbero essere utilizzati per spiare o invadere la privacy delle persone.
Tuttavia, è importante sottolineare che le misure di protezione e la consapevolezza del problema saranno anche rafforzate nel tempo. Gli sviluppatori di tecnologia e le autorità competenti stanno lavorando per implementare soluzioni innovative che possano prevenire e contrastare lo stalking online. Inoltre, una maggiore sensibilizzazione pubblica sul tema potrebbe portare a una cultura di rispetto della privacy e della sicurezza online.
Lo stalking online rappresenta in definitiva un grave rischio per la privacy e la sicurezza delle persone. È fondamentale essere consapevoli dei pericoli associati e adottare misure preventive per proteggersi. Mantenere la privacy online, utilizzare password sicure, limitare le connessioni con estranei e segnalare tempestivamente gli incidenti sono solo alcune delle azioni che possono contribuire a contrastare il fenomeno.
Solo attraverso una combinazione di misure di protezione individuali, di educazione continua e di sviluppo tecnologico responsabile possiamo sperare di mitigare il problema dello stalking online e garantire un ambiente digitale più sicuro per tutti.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Automonitoraggio"

A ciascuno studente viene chiesto di auto monitorarsi online cercando il proprio nome e cognome sui principali motori di ricerca e osservando i propri profili social.
Ognuno dovrà quindi rispondere alle domande:

- È possibile risalire a informazioni sensibili su di me (indirizzo, numero di telefono, abitudini)?
- È possibile riuscire a contattarmi? Su quali canali? In che modo?
- In generale la mia vita online è privata o pubblica?

# TEST

**1. Cosa è lo stalking online?**
**a.** Una forma di pesca sportiva praticata online
**b.** Un metodo per migliorare la propria reputazione online
**c.** L'uso di internet per perseguire, minacciare o molestare qualcuno
**d.** Un gioco di ruolo virtuale basato sulla sorveglianza

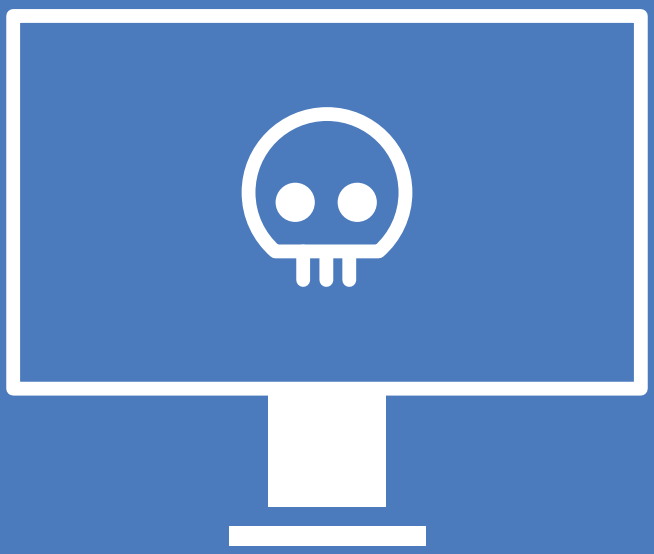
**2. Quali sono i rischi dello stalking online?**
**a.** Aumento della privacy e della sicurezza online
**b.** Creazione di una comunità on-line positiva
**c.** Violazione della privacy, molestie, diffamazione e pericolo fisico
**d.** Promozioni di relazioni sane e rispettose online

**3. Quali potrebbero essere gli atteggiamenti concreti per proteggersi dallo stalking online?**
**a.** Condividere liberamente e informazioni personali su piattaforme online
**b.** Utilizzare password facili da indovinare per gli account online
**c.** Accettare richieste di amicizia da persone sconosciute sui social media
**d.** Mantenere la privacy online, utilizzare password sicura, non accettare richieste da estranei e segnalare eventuali incidenti

**4. Come potrebbe la tecnologia aiutare a contrastare lo stalking online?**
**a.** Facilitando l'accesso a informazioni personali delle vittime
**b.** Implementando strumenti di sicurezza e privacy avanzati su piattaforme online
**c.** Creando nuove piattaforme per lo stalking online
**d.** Diffondendo informazioni sensibili online

Soluzioni: 1c, 2c, 3d, 4b

# 10



# 11

# Virus informatici

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

LA STAMPA

# TIM Cybersecurity Made in Italy Challenge

**Redazionale** **16 maggio 2023**

Prende il via la 'TIM Cybersecurity Made in Italy Challenge', la sfida rivolta ad aziende, PMI, startup e scaleup italiane e internazionali per individuare soluzioni innovative da integrare nell'offerta di servizi cyber di Telsy, la società del Gruppo focalizzata nel settore della cybersecurity, che opera nell'ambito di TIM Enterprise.

La Challenge rientra tra le attività previste nell'ambito del programma di Open Innovation TIM Growth Platform, il nuovo modello di innovazione che punta sulla collaborazione industriale con società ad alto potenziale con l'obiettivo di accelerarne la crescita. L'iniziativa intende favorire lo sviluppo del settore Cyber al fine di accrescere il livello di sicurezza di Istituzioni, grandi aziende e PMI italiane.

"L'iniziativa - ha dichiarato Eugenio Santagata, Chief Public Affairs & Security Officer di TIM e Amministratore Delegato di Telsy - ha il duplice obiettivo di sviluppare nuove soluzioni volte a contrastare il crescente fenomeno legato ai rischi informatici e arricchire il nostro portafoglio di servizi e prodotti che fanno uso di tecnologie innovative e proprietarie per una sicurezza made in Italy. Il mercato della sicurezza cibernetica in Italia sta crescendo in maniera significativa con un valore che oggi supera i 2 miliardi di euro. Siamo convinti che questo settore rappresenti una delle maggiori priorità di investimento digitale per il nostro Paese e confidiamo che anche grazie a questo tipo di iniziative si possa sensibilizzare l'attenzione di Pubbliche amministrazioni e imprese verso la transizione digitale".

Saranno individuate le migliori soluzioni innovative di cybersecurity basate su tecnologie emergenti (Artificial Intelligence, Big Data ecc.). Ai vincitori verrà offerta una partnership tecnologica e commerciale con TIM Enterprise e Telsy. Le società selezionate avranno infatti un accesso privilegiato al mercato della cybersecurity e la possibilità di crescere ulteriormente.

# SCHEDA
# Virus informatici
di Ester Macrì e Lapo Cecconi

I virus informatici sono una delle principali minacce nel mondo digitale moderno. Questi software dannosi possono infettare computer e compromettere la sicurezza dei dati personali e aziendali.
Un virus informatico è un tipo di software malevolo progettato per replicarsi e diffondersi da un computer a un altro, infettando file e programmi lungo il percorso. Una volta che il virus ha infettato un sistema, può danneggiare, alterare o distruggere i dati, rallentare il funzionamento del computer o consentire agli hacker di accedere al dispositivo infetto.

Molti sono i rischi che i virus informatici possono provocare ad utenti ed organizzazioni:
- Perdita di dati: i virus possono corrompere o cancellare dati importanti, causando gravi perdite per gli individui e le aziende. Questo può portare problemi finanziari ma anche reputazionali.
- Furto di informazioni personali: alcuni virus sono progettati per raccogliere informazioni personali, come password, dati bancari e informazioni sensibili. queste informazioni possono essere utilizzate per frodi.
- Interruzione delle attività aziendali: le aziende possono subire interruzioni significative a causa di attacchi di virus informatici, con conseguenti perdite di produttività e di entrate.
- Diffusione tramite e-mail e social media: i virus informatici possono propagarsi attraverso e-mail di phishing o link dannosi sui social media, mettendo a rischio gli utenti non informati.

Nonostante tutti questi rischi molto può essere fatto per proteggersi dai virus informatici adottando alcuni atteggiamenti semplici ma concreti:
1. Installare software antivirus e anti-malware: è necessario utilizzare software antivirus e anti-malware affidabili e mantenere sempre aggiornate le definizioni delle minacce. Questi programmi, infatti, possono individuare e rimuovere virus prima che possano causare danni.
2. Aggiornare regolarmente il sistema operativo e le applicazioni: le patch di sicurezza rilasciate dai produttori possono correggere le vulnerabilità nei software. Mantenere il sistema e le applicazioni aggiornate aiuterà a ridurre i punti deboli esposti ai virus informatici.
3. Fare attenzione agli allegati e ai link: è necessario evitare di aprire allegati o cliccare

sul link sospetti presenti nelle mail o sui social media. Verificare sempre la fonte prima di interagire con qualsiasi contenuto sconosciuto dovrà essere la base per approcciarsi ad un corretto utilizzo delle nuove tecnologie.

4. Esercitare la prudenza online: evitare di scaricare software da fonti non attendibili o di visitare siti web sospetti. Sarà necessario prestare attenzione quando si scaricano file da internet e assicurarsi di utilizzare solo siti web sicuri e certificati.

Le nuove tecnologie hanno sicuramente esasperato il fenomeno del virus informatico. Ma, paradossalmente, possono aiutare molto proprio nel contrastare tali virus attraverso metodi avanzati di protezione di vario tipo. In primis attraverso i software di rilevamento avanzato, ovvero algoritmi sofisticati per identificare i virus informatici e bloccarli in tempo reale. Questi strumenti possono scansionare in modo proattivo i file e i programmi alla ricerca di segni di infezione. Ancora, firewall e strumenti di sicurezza di rete possono aiutare a proteggere i sistemi da attacchi esterni. Questi strumenti possono rilevare e bloccare tentativi di intrusione da parte di un virus informatico o di un hacker. Il monitoraggio del comportamento dei programmi, inoltre, permette di identificare attività sospette o dannose consentendo di rilevare i virus informatici che possono evadere le firme di riconoscimento tradizionali. Le nuove tecnologie, infine, possono essere utilizzate per fornire programmi di formazione sulla sicurezza informatica, con programmi che educano gli utenti sugli atteggiamenti sicuri da adottare online e informano sugli ultimi tipi di minacce informatiche.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Attenti al virus!"

Viene chiesto agli studenti (tutta la classe insieme o divisi a gruppi) di girare un piccolo video-tutorial su come difendersi dai virus informatici, seguendo i consigli riportati nella scheda o altri che possono derivare dalla loro esperienza diretta. Il video potrà essere inviato poi ai genitori e/o essere pubblicato sul sito della scuola.

# TEST

**1. Cosa sono i virus informatici?**
**a.** Programmi che proseguono il computer da minacce esterne
**b.** Software che Velocizza il funzionamento del computer
**c.** Codici malevoli che infettano e danneggiano i computer
**d.** Applicazioni per navigare in sicurezza su internet

**2. Quali sono i rischi dei virus informatici?**
**a.** Miglioramento delle prestazioni del computer
**b.** Protezione dei dati personali
**c.** Perdita di dati, furto di informazioni sensibili e danni al sistema
**d.** Ottimizzazione delle risorse Hardware

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare virus informatici?**
**a.** Scaricare file da fonti non attendibili
**b.** Fare clic sul link sospetti nelle mail
**c.** Mantenere il sistema operativo e gli antivirus aggiornati
**d.** Condividere liberamente informazioni personali online

**4. Come può la tecnologia aiutare a contrastare i virus informatici?**
**a.** Diffondendo virus informatici in modo più efficace
**b.** Identificando e bloccando minacce potenziali
**c.** Facilitando l'accesso ai dati personali
**d.** Creando nuovi tipi di virus informatici

Soluzioni: 1c, 2c, 3c, 4b

# 12

# Information overload

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

ARTICOLO

Il Sole 24 ORE

# Il disaccordo che accresce la conoscenza

**Redazionale** **4 novembre 2012**

I media e le conoscenze formano un intreccio nel quale ci si perde o ci si trova.
La struttura mutante della prima influenza le seconde. E viceversa.
Si può soffocare per mancanza di accesso all'informazione come per eccesso di dati. Mail, social network, web, giornali, televisione, radio, cartelloni stradali, telefonate, sms, assediano di messaggi le vite quotidiane degli occidentali e inducono a lamentare l'information overload, il sovraccarico informativo, motivo di disattenzione o addirittura ignoranza. Ma d'altra parte i critici più socialmente avvertiti non cessano di combattere le varie forme contemporanee di esclusione, dal digital divide all'analfabetismo funzionale. «La conoscenza non è più quella di una volta» sorride David Weinberger, filosofo della rete, nel suo ultimo libro, "La stanza intelligente. La conoscenza come proprietà della rete", appena tradotto da Codice Edizioni.
In che cosa è cambiata la conoscenza? «Era un insieme di contenuti; ora è la stessa rete». Weinberger risponde gentile alle domande via mail, mentre il suo viaggio di ritorno a Boston dall'Italia, dove era stato per il Festival della Scienza di Genova, è dirottato a Londra per l'uragano Sandy. «La conoscenza era un insieme di "affermazioni" che ritenevamo vere, scegliendole tra tutte le affermazioni in competizione. Era un sistema che funzionava in modo da rispondere alle domande. Era immensamente efficiente. Queste proprietà della conoscenza erano anche le proprietà del mezzo che consentiva l'accesso: carta, libri, biblioteche. I vecchi media limitavano la dimensione della conoscenza. Il che era ragionevole perché fin dall'origine il nostro scopo era comprendere un vastissimo universo con i nostri piccolissimi cervelli». E la stessa gerarchia del sapere, dai dati alle informazioni, dalle interpretazioni alla saggezza, era un percorso nel quale agivano in parallelo le autorità garanti della correttezza delle conoscenze e i mezzi di registrazione e comunicazione.
«Ma oggi il nuovo medium della conoscenza è internet. E la conoscenza sta assorbendo le proprietà della rete. Ora la conoscenza può crescere senza limiti di dimensioni - perché non dobbiamo fare posto a una nuova informazione togliendone una precedente, come avveniva sugli scaffali delle biblioteche - e tutte le conoscenze

possono essere linkate tra loro. Il che significa che non solo si pubblica ogni dato e qualunque idea, ma ciascun elemento è collegato a molti altri, in reti di discussioni e commenti. Sicché la conoscenza non è più un percorso lineare di domande e risposte, ma diventa una complessa galassia di link che inducono nella tentazione di cliccare in ogni direzione per non fermarsi mai».

Esempi? «Quando è nato, il knowledge management era un sistema per filtrare e comunicare le informazioni aziendali di maggior valore ed eliminare il rumore. Il successo del web ha trasformato il knowledge management in un sistema di servizi che connettono le persone in reti nelle quali le discussioni sono vivaci e le conoscenze acquisite sono messe costantemente in discussione».

Ma che cosa succede alle autorità che un tempo incarnavano la conoscenza o almeno la distinzione tra la conoscenza attendibile e il resto? «Il ruolo degli esperti sta cambiando a sua volta. Un tempo ci si rivolgeva alle autorità accreditate per ottenere risposte. Ora si va sul web per trovare esperti più o meno accreditati che sono impegnati in accese discussioni tra loro. Nella migliore delle ipotesi queste discussioni producono diversi punti di vista che si illuminano a vicenda e che allargano la qualità delle risposte. Nella peggiore delle ipotesi quelle discussioni diventano battaglie selvagge tra opinioni incompatibili. O peggio ancora, si trasformano in cori di voci perfettamente omogenee nei quali tutti sono d'accordo». Cioè? «Sarebbe bello un mondo in cui tutti sono in armonia. Ma si scopre che il disaccordo accresce la conoscenza».

Bene. Ma come funziona la generazione della conoscenza nelle organizzazioni non gerarchiche ma basate sulla struttura della rete? «L'esempio è Wikipedia. Oppure il sistema operativo Linux. Le organizzazioni basate sulla rete hanno dimostrato di poter arrivare a risultati che le strutture gerarchiche non potevano realizzare».

Ma che cosa vuol dire che la stanza è intelligente? «Gli esperti sono persone di grande valore. Ma gli individui possono avere solo conoscenze limitate. Per consentire alla conoscenza di crescere abbiamo bisogno di esperti che conversano attraverso una delle molteplici forme di interazione che il web rende possibili. Una rete di conoscenze genera una conoscenza più grande della conoscenza di ciascuna persona connessa. La persona più intelligente che c'è in una stanza è la stanza stessa».

Ma se la rete consente la pubblicazione di qualunque cosa, se i filtri vengono applicati dopo la pubblicazione - e non più prima - qual è la strategia emergente per scegliere la conoscenza di qualità? «Abbiamo bisogno dei filtri tradizionali applicati da curatori professionali. E abbiamo bisogno anche di filtri che usano algoritmi e reti sociali per trovare quello che giudicheremo utile e interessante. Abbiamo bisogno di nuove università che funzionino non solo in base alla presenza fisica in un campus ma anche attraverso la rete. Abbiamo bisogno di generare conoscenza con nuove istituzioni inclusive e non più soltanto esclusive».

# SCHEDA
# Information overload
di Ester Macrì e Lapo Cecconi

Nell'era digitale in cui viviamo, siamo costantemente bombardati da un'enorme quantità di informazioni provenienti da diverse fonti. Questo fenomeno è noto come information overload o sovraccarico di informazioni e si verifica quando siamo esposti a un'eccessiva quantità di informazioni, superando la nostra capacità di elaborarle e assimilarle in modo efficace. Questo si traduce in una sensazione di sopraffazione e difficoltà nel selezionare le informazioni rilevanti, concentrandoci su ciò che è importante.

L'Information Overload può avere diversi effetti negativi sul nostro benessere e sulla nostra produttività. I danni includono:

- Stress e ansia: l'eccesso di informazioni può causare un aumento dello stress
- e dell'ansia, poiché ci sentiamo costantemente sopraffatti e preoccupati di non
- riuscire a tenere il passo.
- Ridotta capacità di concentrazione: l'abuso di informazioni può ridurre la
- nostra capacità di concentrazione e di focalizzarci sulle attività importanti,
- compromettendo la nostra produttività.
- Affaticamento cognitivo: l'elaborazione continua di informazioni può affaticare il nostro cervello, portando a una diminuzione della capacità di pensare in modo chiaro e di prendere decisioni efficaci.
- Scarsa memorizzazione: quando siamo sovraccarichi di informazioni, la nostra capacità di memorizzare e recuperare le informazioni importanti può essere compromessa.

Fortunatamente, ci sono azioni concrete che possiamo intraprendere per limitare l'Information Overload e migliorare la nostra gestione delle informazioni anche nella nostra vita quotidiana:

- Stabilisci priorità: definisci i tuoi obiettivi e le tue priorità in modo chiaro. Concentrati solo sulle informazioni che sono rilevanti per raggiungere quegli obiettivi.
- Filtra le fonti di informazione: scegli con cura le fonti di informazione affidabili e pertinenti alle tue necessità. Limita l'esposizione a notizie e contenuti superflui.
- Imposta limiti di tempo: dedica periodi specifici alla consultazione delle informazioni, evitando di lasciare che distruggano l'intera giornata. Stabilisci delle pause dedicate alla disconnessione digitale.
- Organizza le informazioni: utilizza strumenti di organizzazione, come app per

prendere appunti o elenchi di cose da fare, per tenere traccia delle informazioni importanti e ridurre il disordine mentale.
- Pratica il "Digital Detox": di tanto in tanto, disconnettiti completamente dalla tecnologia.

L'Information Overload rappresenta una sfida significativa nell'era digitale in cui viviamo, ma il progresso tecnologico potrebbe anche fornirci strumenti per affrontare questo problema in modo più efficace.
Nel futuro, potremmo vedere lo sviluppo di tecnologie intelligenti che aiutano a filtrare e selezionare le informazioni in base alle nostre preferenze e obiettivi.
Ad esempio, l'intelligenza artificiale potrebbe essere utilizzata per personalizzare i feed di notizie e i contenuti online, offrendoci solo ciò che è rilevante e di interesse per noi.
Inoltre, l'avanzamento delle tecnologie di analisi dei dati potrebbe fornire strumenti più potenti per gestire l'Information Overload. Algoritmi sofisticati potrebbero essere in grado di riconoscere i modelli nelle nostre abitudini di consumo di informazioni e fornirci suggerimenti e sintesi automatiche per semplificare il processo di ricerca e apprendimento.
D'altro canto, spetta anche a noi come individui adottare comportamenti consapevoli e responsabili nell'utilizzo delle tecnologie. Dobbiamo essere selettivi nella scelta delle fonti di informazione, stabilire priorità chiare e imparare a gestire il nostro tempo in modo efficiente.
In conclusione, sebbene limitare e gestire l'Information Overload sia una sfida complessa, il progresso tecnologico potrebbe offrire soluzioni innovative per aiutarci. Tuttavia, è fondamentale mantenere un equilibrio saggio tra l'utilizzo della tecnologia e le nostre capacità individuali di filtrare, organizzare e selezionare le informazioni che ci servono. Solo attraverso una combinazione di progresso tecnologico e una mentalità consapevole possiamo sperare di affrontare in modo efficace l'Information Overload e trarre il massimo beneficio dalle risorse informative che ci sono disponibili.

# TRACCIA PER L'ATTIVITA' IN CLASSE

## "Un mare di informazioni"

Agli studenti viene chiesto di cercare online articoli su alcune tematiche (es. vaccini, guerra in Ucraina, riscaldamento globale). Ad uno studente vengono letti quindi ad alta voce 10 articoli diversi sullo stesso tema (possibilmente con visioni diverse). Lo studente dovrà tentare di riassumere e, alla fine, provare a dire quale posizione è per lui più attendibile tra quelle ascoltate.

Discutiamo insieme:

- È facile o difficile orientarsi tra tante informazioni?
- Come riuscire a valutare le fonti migliori?

# TEST

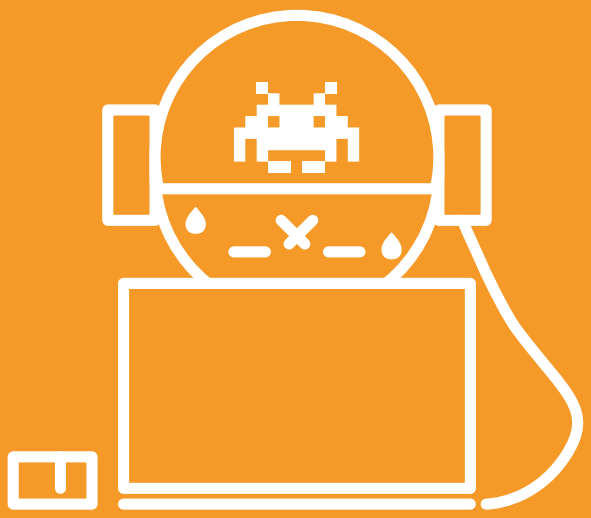
**1. Quali sono i rischi dell'information Overload?**
**a.** Aumento della produttività e della creatività
**b.** Affaticamento cognitivo e difficoltà di concentrazione
**c.** Miglioramento della memoria e delle capacità decisionali
**d.** Aumento della capacità di gestire grandi quantità di informazioni

**2. Come possiamo limitare l'information Overload?**
**a.** Esposizione continua notizie e contenuti online
**b.** Filtraggio delle fonti di informazione e limitazione delle esposizioni a contenuti non rilevanti
**c.** Assorbimento passivo di tutte le informazioni disponibili
**d.** Ignorare la pianificazione delle priorità e la gestione del tempo

**3. Quali sono alcune strategie per gestire l'information Overload nella vita quotidiana?**
**a.** Dedicare tutto il tempo disponibile alla consultazione delle informazioni
**b.** Utilizzare app per la gestione delle informazioni solo occasionalmente
**c.** Stabilire priorità chiare e fissare limiti di tempo per la consultazione delle informazioni
**d.** Ignorare completamente l'organizzazione delle informazioni

**4. Come potrebbe la tecnologia aiutare a gestire l'information Overload?**
**a.** Aumentando la quantità di informazioni disponibili senza filtri
**b.** Utilizzando intelligenza artificiale per personalizzare contenuti in base alle preferenze individuali
**c.** Creando più distrazioni digitali per gestire le information Overload
**d.** Facilitando l'accesso indiscriminato a tutte le fonti di informazioni disponibili

Soluzioni: 1b, 2b, 3c, 4b



# 13

# Internet gaming disorders

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

ARTICOLO

la Repubblica

# Cos'è la "Internet addiction", la malattia di cui molti soffrono senza neanche saperlo: in Italia seguiti 3.600 malati di gioco e social

**di Alessandra Corica** **15 aprile 2019**

C'è chi salta la scuola o gli esami universitari, chi chiede permessi su permessi al lavoro. Chi passa le notti in bianco, sveglio, davanti alla luce del monitor. Fino a quando quelle ore passate online diventano vera e propria "malattia". Sono i pazienti che presentano la Internet addiction, uno dei nuovi fenomeni osservati negli ambulatori che si occupano di dipendenze: "Nel corso degli ultimi anni è stato registrato un incremento, anche a causa di situazioni che hanno incentivato il rapporto con la Rete, come per esempio il lockdown della primavera del 2020 - spiega Roberto Truzoli, dirigente psicologo dell'Asst Fatebenefratelli-Sacco e professore associato alla Statale - . Ma non solo: grazie agli screening nei servizi territoriali oggi c'è maggiore contezza del fenomeno, e questo aiuta a farlo emergere".

Secondo una ricognizione fatta dall'Istituto superiore di sanità, in Italia sono un centinaio - con oltre 3.600 persone prese in carico - gli ambulatori che si occupano di Internet addiction: a Milano si tratta del Serd che dipende dall'ospedale Sacco e di quello di via Boifava che fa capo all'Asst Santi Paolo e Carlo.

I numeri degli assistiti sono ancora limitati, vista anche la poca conoscenza del fenomeno: nell'ambulatorio di via Boifava hanno in carico una ventina di persone, in quello in zona Forze Armate è stato effettuato uno screening su 175 pazienti già in cura presso i centri psicosociali e il Ctdd (Centro per il trattamento dei disturbi depressivi) del Sacco, e tra loro 54 hanno mostrato un rapporto problematico con la Rete.

"La maggior parte delle volte - spiega Claudio Nicolai, che guida i servizi per le dipendenze dell'Asst Santi Paolo e Carlo - osserviamo il disturbo associato ad altre patologie psichiatriche o dipendenze: si tratta quindi di un fenomeno secondario, e finora raramente abbiamo avuto pazienti con la dipendenza dalla Rete come disturbo primario. Chi ne soffre, difficilmente ha la consapevolezza di avere questo problema".

Che, nei casi più estremi, può arrivare al fenomeno degli "Hikikomori", che vivono murati in casa, con un monitor e una connessione quale unico, flebile, legame con il mondo.
"Per capire se c'è un rapporto problematico con la Rete viene somministrato un test, che prevede due step - spiega Truzoli del Sacco - . Il primo può evidenziare la presenza, nel rapporto del paziente con Internet, di alcune criticità che iniziano a influenzarne la quotidianità, per esempio con la riduzione delle ore di sonno o la sottrazione del tempo da dedicare allo studio o al lavoro per restare connessi online. Il secondo step, invece, indica la cosiddetta Internet addiction, con una dipendenza dalla Rete più marcata".
Secondo uno studio (in attesa di review) condotto dal docente della Statale su 1.032 studenti lombardi tra i 12 e i 25 anni (con età media di 18 anni), il 47,6 per cento supera questo primo step e presenta quindi un rapporto con la Rete caratterizzato da alcune criticità (quali, per esempio, il trascurare lo studio o lo sport) mentre l'1,5 per cento arriva al secondo step, delineando quindi un quadro compatibile con la dipendenza dalla Rete. Con una leggerissima prevalenza del fenomeno tra i maschi, per i quali è preponderante l'uso patologico dei videogiochi online, rispetto alle femmine, maggiormente "addicted" ai social network.
"Ovviamente, la diagnosi non si fa soltanto somministrando un test - ribadisce Truzoli - . Va fatto anche un colloquio di valutazione, con cui si fa un'anamnesi psicologica. L'obiettivo è costruire un profilo psicologico individuale e quindi, sulla base di questo, un percorso di trattamento". Che può prevedere, a seconda di altre patologie psichiatriche o dipendenze associate, sia l'utilizzo di farmaci per curare il problema "primario", sia la terapia comportamentale e cognitiva.

Ma quali sono i segnali che le famiglie non devono trascurare?
"Le spie di un eventuale rapporto problematico con la Rete, da parte di un ragazzo giovane, possono essere diverse - dice Truzoli - . I genitori, per esempio, possono notare un peggioramento della carriera scolastica, oppure una progressiva tendenza a isolarsi e ridurre la vita sociale: questi possono essere degli indicatori da tenere sotto controllo".
E se è vero che il fenomeno è particolarmente diffuso tra i più giovani, non è detto che anche persone di altre fasce d'età non possano soffrirne: "Da noi l'età media dei pazienti che hanno questo tipo di problema è intorno ai 35 anni in associazione ad altre problematiche, e 45 anni per quei pochissimi che invece presentano l'Internet addiction come disturbo primario - dice Nicolai dei Santi Paolo e Carlo - . Certo, stiamo parlando di un campione abbastanza ridotto. Ma può essere considerato indicativo, considerando anche che la Internet addiction spesso si associa ad altre dipendenze quale, per esempio, quella dal gioco d'azzardo, in virtù del gaming online".

# SCHEDA

# Internet gaming disorder

di Ester Macrì e Lapo Cecconi

L'internet gaming disorder (IGD), noto anche come disturbo da gioco su internet, è un problema crescente nel mondo digitale. Questa condizione è caratterizzata da un'eccessiva e incontrollabile partecipazione ai giochi online, che può portare a gravi conseguenze per la salute fisica, mentale e sociale degli individui.
L'internet gaming disorder è un disturbo comportamentale che si manifesta con un'ossessione e un'incapacità di controllare il tempo trascorso sui giochi online.
Le persone affette da IGD dedicano sempre più tempo al gioco, trascurando gli impegni personali, sociali e educativi. questa dipendenza può avere gravi ripercussioni sulla salute e sul benessere generale.

Diversi sono i rischi che l'internet gaming disorder può presentare per la salute individuale e per le relazioni sociali:

- Problemi di salute mentale: l'IGD può aumentare il rischio di sviluppare dei disturbi dell'umore, come l'ansia e la depressione. il senso di isolamento sociale e l'immersione costante nel mondo virtuale possono influire negativamente sul benessere psicologico.
- Problemi fisici: il tempo prolungato trascorso davanti allo schermo può portare una vita sedentaria, problemi posturali, disturbi del sonno e aumento del rischio di obesità.
- Isolamento sociale: l'eccessiva partecipazione ai giochi online può portare alla perdita di contatti sociali nel mondo reale. Le relazioni personali possono essere danneggiate, il che può portare a sentimenti di solitudine e isolamento.
- Problemi accademici e professionali: il tempo e l'energia dedicati al gioco possono influire negativamente sulle performance scolastiche e professionali. la mancanza di concentrazione e la scarsa gestione del tempo possono compromettere le opportunità educative e lavorative.

Per evitare che l'internet gaming disorder diventi un problema sempre più generalizzato, è importante adottare alcuni atteggiamenti concreti e insegnargli a partire già dalle scuole:

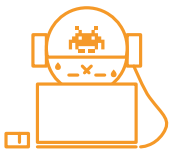
1. Stabilire limiti di tempo: È necessario impostare limiti di tempo per il gioco online e rispettarli. Fissare delle regole chiare su quando e per quanto tempo sarà possibile dedicarsi ai giochi online è essenziale per un corretto uso del tempo libero.
2. Promuovere un equilibrio tra vita virtuale e vita reale: sarà necessario dedicare del

tempo alle attività fuori dal mondo dei giochi, come l'esercizio fisico, gli hobby, le relazioni sociali, lo studio o il lavoro. questo, infatti, aiuterà a mantenere un equilibrio tra le diverse sfere della vita e sarà fondamentale per il benessere generale della persona.

3. Coinvolgimento sociale: per non cadere nel rischio dell'IGD sarà necessario partecipare attivamente alle attività sociali e coltivare relazioni significative nel mondo reale. La partenza può essere quella di cercare di trascorrere del tempo con amici e familiari, partecipando a esperienze che non coinvolgano i giochi online.
4. Consapevolezza dei segnali di dipendenza: è necessario monitorare i comportamenti di gioco e prestare attenzione a segnali di dipendenza, come l'incapacità di smettere di giocare nonostante le conseguenze negative o l'irritabilità quando si allontani dai giochi. Se tali segnali saranno notati, sarà essenziale cercare il supporto da parte di professionisti o gruppi di sostegno specializzati.

Come può la tecnologia aiutarci a contrastare l'Internet Gaming Disorder?
Le nuove tecnologie forniscono strumenti di controllo del tempo: alcune piattaforme di gioco, infatti, offrono funzionalità di controllo del tempo, che consentono agli utenti di impostare limiti di gioco e di ricevere avvisi quando si superano determinati limiti stabiliti. Inoltre, sono nate sempre nuove app di monitoraggio e gestione che aiutano proprio a monitorare e gestire il tempo trascorso sui giochi online. Queste app, infatti, possono fornire statistiche dettagliate sull'utilizzo del tempo e inviare notifiche per avvisare quando si raggiungono limiti predefiniti. Ma la tecnologia può essere utilizzata anche per fornire informazioni e risorse sulla consapevolezza dei rischi legati all'IGD. Siti web, forum online e applicazioni possono diffondere consigli, guide o storie di esperienze per aiutare le persone a comprendere meglio il problema e adottare comportamenti più sani.

L'Internet Gaming Disorder rappresenta sicuramente una sfida significativa nel mondo digitale odierno. Per prevenire e affrontare questo disturbo, è necessario adottare atteggiamenti consapevoli, come l'impostazione dei limiti di tempo, il mantenimento di un equilibrio tra vita reale e virtuale e il coinvolgimento sociale. La tecnologia, quando utilizzata in modo appropriato, può offrire strumenti e risorse utili per monitorare e gestire il tempo trascorso sui giochi online, nonché per educare e sensibilizzare sulle conseguenze dell'Internet Gaming Disorder.



# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Il peso del gioco"

Viene proiettato in aula il video: https://www.youtube.com/watch?v=**_-KV0l6o5FE**
Si discute:

- Qual è il significato di questo video?
- Perché il ragazzo cade sotto il peso del joystick?
- Come ci si può accorgere che i videogiochi stanno diventando per noi un problema?
- Quali altre cose possono essere un peso che schiaccia?

# TEST

**1. Cos'è l'Internet Gaming Disorder?**
**a.** Un disturbo mentale causato dall'utilizzo eccessivo di social media
**b.** Una condizione in cui le persone giocano online in modo moderato e bilanciato
**c.** Un disturbo caratterizzato da un'ossessione eccessiva per i giochi online
**d.** Una dipendenza da internet che coinvolge esclusivamente giochi di ruolo

**2. Quali sono i rischi dell'Internet Gaming disorder?**
**a.** Aumento della socializzazione e delle abilità cognitive
**b.** Isolamento sociale, problemi di salute mentale e riduzione delle prestazioni accademiche
**c.** Miglioramento della coordinazione e della concentrazione
**d.** Promozione della creatività e dell'immaginazione

**3. Quali potrebbero essere gli atteggiamenti concreti per evitare l'Internet Gaming Disorder?**
**a.** Impostare limiti di tempo per il gioco online
**b.** Passare la maggior parte del tempo libero a giocare online
**c.** Ignorare gli impegni scolastici e sociali per giocare online
**d.** Non cercare supporto consulenza in caso di problematiche legate al gioco online

**4. Come può la tecnologia aiutare a contrastare l'Internet Gaming disorder?**
**a.** Promuovendo giochi online più coinvolgenti e stimolanti
**b.** Monitorando e fornendo statistiche dettagliate sull'uso del tempo di gioco
**c.** Incentivando l'uso eccessivo di giochi online
**d.** Facilitando l'accesso a contenuti di gioco sempre disponibili

Soluzioni: 1c, 2b, 3a, 4b

14

# Online shopping addiction

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

la Repubblica

# Nettuno, fa shopping compulsivo per 170 mila euro e minaccia i genitori per avere i soldi

**di Clemente Pistilli** **15 febbraio 2020**

L'uomo, 40 anni, ha sottoposto il padre e la madre a una serie di violenze fisiche e psicologiche e li ha fatti finire sul lastrico. Il gip ha disposto per lui il divieto di avvicinamento e il braccialetto elettronico

Colto da shopping compulsivo, un 40enne di Nettuno ha mandato sul lastrico gli anziani genitori, spendendo circa 170mila euro e sottoponendo il padre e la madre a una serie di violenze fisiche e psicologiche per ottenere in continuazione denaro. Questo il quadro emerso dalle indagini svolte dal commissariato di Anzio e sfociate ora nel divieto di avvicinamento alle vittime disposto dal gip del Tribunale di Velletri, che ha anche fatto applicare al 40enne il braccialetto elettronico, affinché la polizia possa monitorarlo costantemente e intervenire subito se dovesse tornare a bussare alla porta dei familiari.

Dagli accertamenti compiuti dal pool costituito nel commissariato di Anzio per contrastare la violenza di genere, è inoltre venuto fuori che gli anziani genitori dell'indagato, per far fronte alle richieste del figlio, erano stati costretti a stipulare prestiti con cui ripianare i debiti accumulati, che venivano picchiati ogni volta che cercavano di resistere alle continue richieste di denaro e persino costretti ad accompagnare il 40enne a fare acquisti di ogni tipo.

Il gip ha così ordinato all'indagato di lasciare la casa del padre e della madre, di andare a vivere in un altro appartamento che i genitori gli hanno messo a disposizione e di non avvicinarsi appunto ai due anziani.

SCHEDA

# Online shopping adiction

di Ester Macrì e Lapo Cecconi

Lo shopping online ha rivoluzionato il modo in cui facciamo acquisti, offrendoci una vasta gamma di prodotti e la comodità di acquistare da casa. Tuttavia, per alcune persone, questa pratica può sfociare in una dipendenza nota come "online shopping addiction" o dipendenza da shopping online.
Che cos'è dunque la dipendenza da shopping online? La dipendenza da shopping online è un disturbo comportamentale caratterizzato da un'ossessione per gli acquisti online e la perdita di controllo sulla spesa. Le persone affette da questa dipendenza trascorrono una quantità eccessiva di tempo a navigare e fare acquisti online, spesso incorrendo in debiti e compromettendo il benessere personale, finanziario e relazionale.

Molteplici sono i rischi di questo comportamento che può avere effetti negativi su diverse aree della vita. I rischi associati includono:

- Problemi finanziari: la spesa eccessiva può portare a gravi problemi finanziari, indebitamento e difficoltà nel soddisfare le necessità di base.
- Disturbi emotivi: la dipendenza da shopping online può causare sensazioni di colpa, ansia e depressione, specialmente quando si accumulano debiti o si acquistano oggetti inutili.
- Isolamento sociale: le persone affette da questa dipendenza possono isolarsi socialmente, preferendo trascorrere il tempo a fare acquisti online anziché partecipare ad attività sociali o sviluppare relazioni significative.
- Problemi di salute mentale: la dipendenza da shopping online può contribuire allo sviluppo o all'aggravarsi di disturbi come l'ansia, la depressione o il disturbo da accumulo.

Per evitare di cadere nella dipendenza da shopping online, è possibile adottare alcuni comportamenti quotidiani:

- Stabilire un budget: fissa un limite di spesa mensile e mantieniti fedele ad esso. Evita di acquistare impulsivamente o di superare il tuo budget senza una valida ragione.
- Praticare lo shopping consapevole: prima di effettuare un acquisto, poni domande critiche su ciò che stai comprando. Chiediti se ne hai davvero bisogno, se sarà utile e se è un acquisto ragionevole.
- Limitare le notifiche: riduci le notifiche delle app di shopping o disabilitale del tutto

per evitare di essere costantemente tentato a fare acquisti.
- Cercare alternative salutari: trova attività alternative per trascorrere il tempo libero che non coinvolgano lo shopping online, come l'esercizio fisico, la lettura e altre attività non virtuali.

La dipendenza da shopping online rappresenta sicuramente un problema per molte persone, ma al contempo, il progresso tecnologico può offrire soluzioni per contrastare questo fenomeno.
Nel futuro, potremmo assistere allo sviluppo di tecnologie che aiutano a monitorare e limitare l'accesso a siti di shopping online in modo controllato.
Ad esempio, potrebbero essere introdotti strumenti di gestione del tempo e del controllo degli acquisti, che consentono agli utenti di impostare limiti di tempo di navigazione e di spesa, contribuendo così a prevenire la dipendenza.
Inoltre, l'intelligenza artificiale potrebbe essere utilizzata per analizzare i pattern di acquisto e riconoscere segnali di comportamenti compulsivi. Ciò consentirebbe di fornire avvisi e suggerimenti personalizzati agli utenti, aiutandoli a prendere decisioni più consapevoli e limitando gli acquisti impulsivi.
D'altra parte, è fondamentale sottolineare che la responsabilità individuale gioca un ruolo cruciale nella prevenzione della dipendenza da shopping online.
È importante sviluppare una consapevolezza critica dei propri comportamenti di spesa, stabilire limiti personali e ricercare un equilibrio sano tra l'uso della tecnologia e il benessere personale.
Mentre la tecnologia può offrire strumenti e soluzioni per contrastare la dipendenza da shopping online, è essenziale anche un impegno personale nel gestire consapevolmente i nostri comportamenti di acquisto. Come visto per altri rischi legati al mondo digitale, solo la combinazione di progresso tecnologico e consapevolezza individuale ci aiuterà a mitigare i rischi della dipendenza da shopping online, consentendoci di godere dei vantaggi dello shopping online in modo equilibrato e responsabile.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "Occhio al carrello"

Viene chiesto agli studenti di fare un giro online su alcune piattaforme di vendita e di rispondere a queste domande:
- Quali strategie possiamo individuare in queste piattaforme per spingere le persone a comprare sempre di più?
- Cosa hanno di accattivante queste piattaforme?
- Come possiamo porci un freno negli acquisti online?

# TEST

**1. Che cos'è la dipendenza da shopping online?**
**a.** Una forma di intrattenimento online basata sugli acquisti
**b.** Un disturbo comportamentale caratterizzato da un'ossessione per gli acquisti online
**c.** Un metodo per risparmiare denaro attraverso lo shopping onlinea
**d.** Un gioco virtuale in cui si simula un acquisto online

**2. Quali sono i rischi della dipendenza da shopping online?**
**a.** Aumento della consapevolezza finanziaria e dei Risparmi
**b.** Disturbi emotivi come ansia e depressione
**c.** Miglioramento delle relazioni sociali attraverso lo shopping online
**d.** Promozione di comportamenti di spesa consapevole

**3. Quale potrebbero essere gli atteggiamenti concreti per evitare la dipendenza da shopping online?**
**a.** Spendersi senza limiti e senza un budget
**b.** Fare acquisti in modo consapevole e stabilire un limite di spesa mensile
**c.** Attivare le notifiche delle app di shopping per essere costantemente aggiornati sulle offerte
**d.** Dipendere esclusivamente dallo shopping online come attività di svago

**4. Come potrebbe la tecnologia aiutare a contrastare la dipendenza da shopping online?**
**a.** Promuovendo l'accesso illimitato a Siti di shopping online
**b.** Utilizzando l'intelligenza artificiale per riconoscere i comportamenti compulsivi e fornire suggerimenti personalizzati
**c.** Creando più app e piattaforme per lo shopping online
**d.** Diffondendo informazioni sulle ultime tendenze di moda e sconti online

Soluzioni: 1b, 2b, 3b, 4b

# 15

# Binge watching

di Ester Macrì
*Presidente di ReteSviluppo, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*
e Lapo Cecconi
*Fondatore di Kinoa srl, docente di Progettare l'innovazione, Master in Digital Transformation, Università degli Studi di Firenze*

# ARTICOLO

Il Sole 24 ORE

# I millennials amano “abbuffarsi” di serie tv: cos'è il binge watching?

**di Michela Piccoli** **15 ottobre 2017**

Letteralmente “maratona di visione”, il binge watching è una nuova pratica di consumo di contenuti in streaming che consiste nel guardare diversi episodi di una serie televisiva consecutivamente, senza soste. Come? Grazie ai servizi di streaming in abbonamento (Netflix, Hulu, Amazon Prime e tanti altri).

Fondato nel 1997 come “home entertainment company”, entrato nel mercato del video streaming dieci anni fa e diventato da quel momento il leader nel settore dell’on demand con 104 milioni di abbonamenti (dato aggiornato a giugno 2017), Netflix è stato il motore propulsore di una vera e propria rivoluzione nelle abitudini di consumo di film e serie tv.

Il fenomeno della maratona televisiva è sempre esistito, ma negli ultimi anni – con la diffusione di piattaforme di streaming in abbonamento – ha assunto nuove caratteristiche andando a modificare radicalmente le diete di contenuti di intrattenimento delle nuove generazioni.

Netflix mette infatti a disposizione un pacchetto di episodi, eliminando l’attesa della nuova puntata di settimana in settimana.

Secondo la ricerca condotta da YouGov, il 58% degli americani ha praticato binge-watching almeno una volta nella vita e di questi il 72% dichiara di preferire questa modalità di fruizione dei contenuti rispetto a quella tradizionale.

Il “binging” sta riscuotendo un grande successo in particolare tra i più giovani: il 68% dei rispondenti tra i 18 e i 34 anni hanno espresso la propria preferenza per il “Netflix way”, mentre solo il 17% continua a scegliere la scansione “normale”. Diverse le percentuali tra gli over55, più attaccati alle vecchie abitudini.

E le motivazioni? Sei americani su dieci preferiscono vedere tutta la storia in una volta sola, per non perdere il filo logico della narrazione. Il 48% invece dice di non tollerare la suspense che accompagna inevitabilmente l’attesa di un nuovo episodio. Insomma, una scelta di comodità e flessibilità.

# SCHEDA
# Binge watching
## di Ester Macrì e Lapo Cecconi

Il binge watching, ovvero una vera e propria abbuffata di episodi di serie TV o film, è diventato una pratica molto diffusa grazie alla disponibilità di piattaforme di streaming online. Tuttavia, mentre vedere tanti episodi di una serie tv di fila può essere un modo divertente per godersi i nostri contenuti preferiti, può anche sfociare in una dipendenza problematica. Quando si può parlare di binge watching? Il binge watching in senso stretto si riferisce alla pratica di guardare consecutivamente diversi episodi di una serie TV o film, spesso in una sola sessione. Grazie alla facilità di accesso ai contenuti on-demand attraverso le piattaforme di streaming, sempre più persone si trovano ad essere coinvolte in questa pratica. Nonostante il binge watching possa sembrare un comportamento innocuo e sia estremamente diffuso, esso può comportare alcuni rischi per la nostra salute e benessere.

Alcuni rischi molto comuni associati a questa pratica possono essere:
- Problemi di sonno: questo comportamento può causare disturbi del sonno, poiché spesso ci porta a restare svegli fino a tarda notte per finire una serie o un film.
- Sedentarietà e inattività fisica: il passare lunghe ore seduti a guardare episodi consecutivi può portare a uno stile di vita sedentario e alla mancanza di attività fisica.
- Isolamento sociale: il binge watching può portare a un ritiro sociale, poiché preferiamo trascorrere il tempo davanti allo schermo piuttosto che impegnarci in attività sociali o interazioni con gli altri.
- Ridotta produttività: il tempo trascorso nel binge watching può interferire con la nostra capacità di concentrarci sul lavoro, sugli studi o sulle attività quotidiane, riducendo la nostra produttività complessiva.

Per evitare di cadere in una dipendenza da binge watching, è possibile adottare alcuni comportamenti sani:
- Imposta limiti di tempo: fissa limiti di tempo giornalieri o settimanali per il binge watching. Ad esempio, stabilisci di guardare solo un certo numero di episodi o limita il tempo totale trascorso di fronte allo schermo.
- Pratica l'autodisciplina: sii consapevole dei tuoi limiti e pratica l'autodisciplina nel rispettare i limiti che hai stabilito. Resistere alla tentazione di continuare a guardare quando hai raggiunto il tuo limite previsto.
- Diversifica le attività: trova un equilibrio tra il tempo trascorso a guardare contenuti

e il coinvolgimento in altre attività. Dedica tempo all'esercizio fisico, alla lettura, alle interazioni sociali o a hobby che ti interessano.

- Crea una routine di sonno sana: assicurati di mantenere una routine regolare di sonno e di evitare di guardare episodi fino a tarda notte. Il riposo adeguato è fondamentale per il benessere generale.

Il binge watching può essere un modo divertente per godersi i nostri contenuti preferiti, ma è importante adottare comportamenti sani per evitare una dipendenza da binge watching. Mentre il progresso tecnologico ci offre un facile accesso a una vasta gamma di contenuti, è fondamentale trovare un equilibrio tra l'intrattenimento digitale e uno stile di vita sano. Con una consapevolezza critica e l'adozione di comportamenti sani, possiamo godere del binge watching senza cadere nella trappola della dipendenza e preservare il nostro benessere complessivo.

Nel futuro, il progresso tecnologico potrebbe offrire soluzioni per contrastare la dipendenza da binge watching. Ad esempio, le piattaforme di streaming potrebbero integrare strumenti di monitoraggio e limitazione del tempo di visione. Questi strumenti consentirebbero agli utenti di impostare limiti di tempo giornalieri o settimanali e ricevere avvisi quando stanno superando tali limiti. Inoltre, l'intelligenza artificiale potrebbe analizzare i modelli di visione degli utenti per offrire raccomandazioni personalizzate che incoraggiano una varietà di contenuti, evitando così il ciclo ripetitivo di binge watching.

Inoltre, potrebbero essere sviluppate applicazioni o strumenti di gestione del tempo specificamente dedicati al controllo del binge watching. Questi strumenti aiuterebbero gli utenti a pianificare le loro attività quotidiane in modo più equilibrato, fornendo promemoria e allarmi per prendere pause e dedicarsi ad altre attività al di fuori dello schermo.

La tecnologia potrebbe anche analizzare i pattern di visione e i comportamenti degli utenti per rilevare segnali di dipendenza da binge watching. In caso di utilizzo eccessivo o problematico, potrebbero essere forniti avvisi o suggerimenti per aiutare le persone a gestire meglio il loro consumo di contenuti.

Tuttavia, nonostante questi sviluppi tecnologici, rimane fondamentale l'assunzione di responsabilità individuale nella gestione del binge watching. Anche con l'assistenza della tecnologia, sarà essenziale coltivare una consapevolezza critica e stabilire limiti personali. Trovare un equilibrio tra intrattenimento digitale e benessere generale sarà sempre una responsabilità personale che va esercitata.

# TRACCIA PER L'ATTIVITÀ IN CLASSE

## "A piccole dosi"

Per un'intera settimana vengono dedicati alcuni minuti alla lettura di un racconto di paura o giallo (es. un racconto di Edgar Allan Poe). Il racconto non viene letto tutto insieme ma diviso in cinque parti, uno per ogni giorno di scuola nella settimana, cercando di creare suspense sul finale.

Discutiamo insieme:

- Sarebbe stata la stessa cosa leggere il racconto tutto di fila?
- Sarebbe stata la stessa cosa leggere un intero libro di racconti tutti di fila?
- Quali vantaggi porta dividere in piccole parti qualcosa invece di abbuffarsi?
- Potremmo fare così anche per le serie tv?

# TEST

**1. Che cos'è il binge watching?**
**a.** La pratica di guardare episodi di una serie TV o film consecutivamente
**b.** La pratica di guardare contenuti online occasionalmente
**c.** La pratica di guardare la televisione tradizionale
**d.** La pratica di guardare film solo al cinema

**2. Quali sono i rischi associati al binge watching?**
**a.** Aumento dell'attività fisica e dello sviluppo sociale
**b.** Problemi di sonno e disturbi del sonno
**c.** Aumento della produttività e della concentrazione
**d.** Miglioramento delle abilità di gestione del tempo

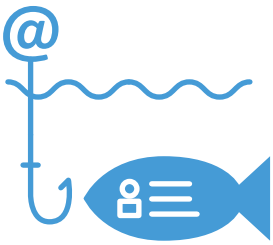
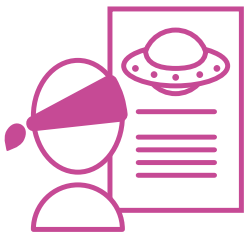
**3. Quali sono alcune misure che si possono adottare per evitare la dipendenza da binge watching?**
**a.** Impostare limiti di tempo e praticare l'autodisciplina
**b.** Guardare episodi di serie tv fino a tarda notte
**c.** Concentrarsi solo Sul binge watching e trascurare alcune attività
**d.** Non preoccuparsi di creare una routine di sonno sana

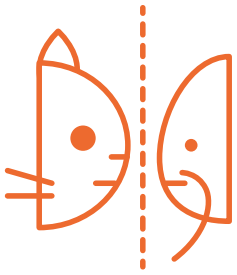
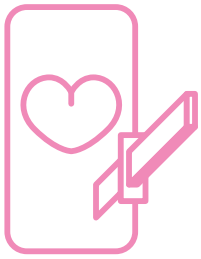
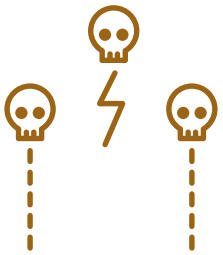
**4. Come potrebbe la tecnologia aiutare a contrastare le dipendenze da binge watching?**
**a.** Aumentando l'accesso illimitato a contenuti online
**b.** Integrando strumenti di monitoraggio e limitazione del tempo di visione nelle piattaforme di streaming
**c.** Promuovendo Il binge watching come pratica salutare
**d.** Creando più piattaforme di streaming per incentivare una varietà di contenuti

Soluzioni: 1a, 2b, 3a, 4b

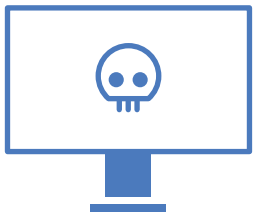
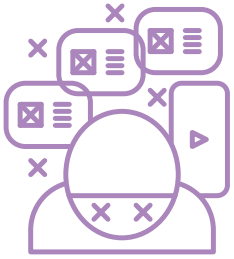
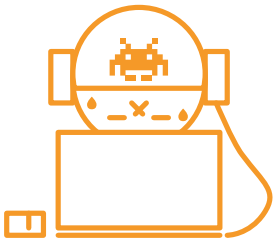
# 15

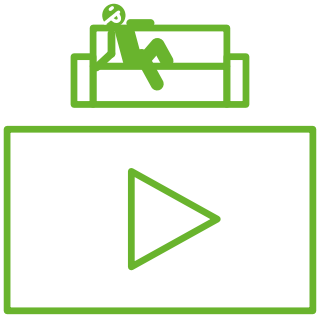
# Appunti





osservatorionline.it