Anno 61 N° 7/10
LUGLIO-OTTOBRE 2024

IL TELESPETTATORE

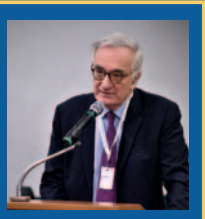
EDITORIALE
Giovanni Baggio
RITROVARE IL SENSO DEL CAMMINO

SPECIALE

BAMBINI AL CENTRO

Si moltiplicano i rischi nel mondo virtuale e l'Aiart a 70 anni dalla sua fondazione rinnova il suo impegno per la tutela dei minori. Obiettivo: essere parte attiva del bisogno di interazione tra istituzioni e cittadini mediali

'Serve il coinvolgimento attivo di bambini e adolescenti nei processi decisionali... '. Il presidente Ernesto Caffo racconta Telefono Azzurro: 38 anni di cambiamenti e la forte sinergia con Aiart.



Ernesto Caffo, presidente e fondatore di Telefono Azzurro

Social media: "Ci è chiesto un impegno rigoroso come esperti di cura...". Lo racconta Stefano Benzoni

Stefano Benzoni, Specialista in neuropsichiatria infantile

L'economia della comunicazione tra costi e investimenti

Intervista a Vincenzo Corrado, direttore Ufficio Comunicazioni sociali della Cei

Identità bugiarde: il lato oscuro delle social Botnets

IL TELE SPETTATORE

7/10/2024

in questo numero

News Aiart

I precedenti numeri de Il Telespettatore sono visitabili sul sito **www.aiart.org**. La rivista è disponibile solo su richiesta da inviare via email all'indirizzo aiart@aiart.org oppure telefonando la Segreteria nazionale al numero 06.66048450 nelle mattine del martedì, mercoledì e giovedì.

COME ADERIRE AD AIART
Le quote annuali di iscrizione sono:

Soci ordinari	**25 euro**
Soci sostenitori, associazioni, scuole e soci collettivi	**40 euro**
Soci studenti	**6 euro**

I versamenti possono essere effettuati sul
– C/C postale n. 45032000
– C/C bancario, IBAN: IT 42 U 05387 10807 000003343247

Intestati a:
Sede nazionale AIART, Via Aurelia, 468 – 00165 Roma
PayPal: aiart@aiart.org

Donazioni detraibili

Puoi sostenere l'Aiart in forma di donazione volontaria e potrai usufruire della detrazione pari al 26% della donazione oppure della deduzione del 100% della donazione effettuata.

PER FAR SENTIRE LA TUA VOCE
DONA IL 5x1000 ALL'AIART
CODICE FISCALE 02436700583

aiart associazione cittadini mediali

IL TELE SPETTATORE
Direttore responsabile:
Maria Elisa Scarcello
Mobile 333 1133942

Bimestrale dell'Aiart - Associazione Cittadini Mediali
Via Aurelia 468, 00165 Roma - Tel. 06 66048450
www.aiart.org - aiart@aiart.org
C/C Postale n. 45032000 distribuzione gratuita ai soci Poste Italiane SpA
Spedizione in Abbonamento Postale D.L. 353/2003 (conv. in L. 27/02/2004 n. 46)
art. 1, comma 2 - DCB Roma - Filiale di Roma - Abbonamento annuo € 25,00
Registrazione Tribunale di Roma n. 10108 del 5/12/64
Grafica, Impaginazione e Stampa a cura di STILGRAFICA Srl Roma

Identità bugiarde: il lato oscuro delle social botnets

Cosa sono le botnet sociali e cosa nascondono? Come influenzano le discussioni online e le percezioni; in che modo possono facilitare attività fraudolente e quale il loro scopo quando vengono assemblate con i cyberattacchi? Dalle principali concause 'sociali' del successo di tali software, alle difficoltà nel riconoscerli e proteggersi.

Ashley Madison è un sito di appuntamenti con milioni di partecipanti che mette in connessione persone sposate alla ricerca di avventure extra coniugali. Nel 2015, *The Impact Team*, un gruppo di hacker informatici si impossessa illegalmente dei dati sensibili degli iscritti al sito pubblicando tutto online. Ciò fece scalpore, perché tra i nomi dei frequentatori della piattaforma vi erano anche parecchi politici, giornalisti e personaggi di spicco. Tuttavia, il motivo per cui si è parlato molto di questa vicenda è un altro. Analizzando meglio i dati dei soggetti registrati si scoprì che 9 su 10 erano uomini. Eppure, ognuno di loro era convinto di chattare con un numero corrispondente di donne. L'indagine sui profili femminili rivelò, al contrario, che questi erano quasi tutti falsi e che a fornire risposte e generare chissà quali illusioni, non fossero esseri umani, ma *bot*, ossia software in grado di creare relazioni e selezionare informazioni in totale autonomia.

Software in relazione

Macchine senza corpo. Mettono *mi piace*, commentano, *ripostano*, provocano, coinvolgono altri utenti in conversazioni, discussioni finanche relazioni. Robot che si inseriscono nelle discussioni "umane" all'interno dei social networks, così vengono presentati i **social botnet.**

I social botnet, da ro**bot** + **net**work, sono reti composte da software automatizzati su piattaforme di social media. Essi sono progettati per imitare il comportamento umano mediante la simulazione della comunicazione e l'analisi dei dati e dei contenuti della rete nascosti dal *web crawler*. Non si tratta, quindi, né di *bot autodichiarati* che offrono risposte automatiche alle domande più frequenti né di *spambot* che distribuiscono pubblicità indesiderata. I social botnet impersonano un account simulando un utente umano.

Monete relazionali

Per l'apparenza di "normalità", per l'indipendenza, la discrezionalità e la credibilità che si cerca di costruire attorno a questa tipologia di profilo in rete ne emerge un lato, sempre più, oscuro, "bugiardo". Nell'attiva-

Sito web: https://eithos.eu

zione di un dialogo naturale, oltre alla possibilità di pubblicazione di un messaggio o di invio di una richiesta di connessione, i social botnets possono celare anche intenti disinformativi, persuasivi, manipolatori o legati al furto delle identità altrui. È facile, dunque, se i social botnet "bugiardi" raggiungono una posizione influente all'interno dei social network che incidano sulla "salute" del suo ecosistema minandone l'integrità delle conversazioni online.

Nell'incontro con il furto di identità online, in particolare, i social botnet possono costituire da soli un attacco oppure fare da tramite per attuare truffe secondarie e cybercrimini su vasta scala. Quando i social botnet vengono assemblati per i cyberattacchi hanno lo scopo di espandere, automatizzare e accelerare le possibilità di guadagno economico e personale sferrando attacchi su larga scala con costi limitati ed efficienza operativa anche psico-emotiva. "Monete relazionali" li chiama il giurista Ziccardi (2019), infrastrutture destinate a creare engagement. L'intento, solitamente, è quello di acquisire dati e informazioni dell'ignaro utente per la rivendita a terzi o per l'estorsione di denaro talvolta inducendolo a cliccare su link malevoli talaltra imitandone le biografie. In quest'ultimo caso, le informazioni biografiche vengono accuratamente selezionate, prima di iniziare una fase di dialogo, in base all'obiettivo criminale e all'audience di riferimento. Alcuni studi dimostrano, infatti, che le persone tendono a rispondere positivamente alle informazioni con cui hanno dimestichezza a causa di pregiudizi cognitivi come il *bias* di familiarità o di simpatia. Pertanto, la persona connessa potrebbe essere più propensa a comunicare con un social botnet se l'auto-presentazione di quest'ultimo corrisponde perfettamente a livello identitario e ideologico. Un'altra tendenza degli ultimi anni, poi, vede i social botnet trasformarsi in *dissenter* per acquisire consensi e seguaci da parte degli utenti reali della rete. Si tratta di una strategia molto sottile: l'account botnet interviene in un dibattito, ad esempio, su Facebook per sostenere alcune parti e andare contro il proprio committente. In realtà, l'obiettivo è quello di ottenere traffico, polarizzazione, viralità e fidelizzazione verso l'account che rappresenta da parte. In questo modo, i social botnet provano anche a stimolare determinate emozioni, facendo agire l'utente "di pancia" sull'onda di paure, pregiudizi, crisi, dissenso, sfiducia e far leva sulla perdita di pensiero critico, dovuta a sua volta all'accumulo di troppe informazioni, al poco tempo a disposizione che porta a leggere in modo "sbrigativo", all'incapacità di approfondire una tematica, alla brevità dei dialoghi, alla progressiva tendenza a non ascoltare e valutare opinioni differenti dalla propria enfatizzata dalla perdita di contatto con la realtà che il dialogo online inevitabilmente comporta.

Il contributo di EITHOS

Attirare e/o affrancare l'utente sul suo stesso terreno di conoscenza è una delle principali concause "sociali" del successo di tali software. Essi, oltre a essere in grado di (ri)produrre o riutilizzare messaggi in modo autonomo, tendono anche ad infiltrarsi in grandi gruppi di utenti sfruttando la sottovalutazione del rischio, il sentirsi a proprio agio e l'eccessiva fiducia nelle proprie competenze digitali da parte degli utenti reali della rete. E proprio come emerge dalla ricerca empirica sul furto di identità che sta conducendo l'Università di Bologna all'interno del Progetto EITHOS, queste dimensioni hanno poi un impatto sugli utenti-vittime soprattutto in termini di danneggiamento della reputazione, di auto-biasimo e vergogna per non aver captato in tempo il realizzarsi di un evento negativo, per essere fidati ed affidati a qualcuno di cui conoscevano solo qualche riga della biografia digitale. Anzi più elevata è l'esperienza, l'alfabetizzazione digitale e la sicurezza di Sé all'interno del contesto online più il danno subito è percepito come disabilitante e stigmatizzante.

Se dal punto di vista della cybersicurezza molte sono ancora le difficoltà nel riconoscere e proteggersi dalle Social Botnet con intenti criminosi, l'Osservatorio di EITHOS si sta attivando su due fronti. Per le autorità di polizia, sta costruendo una serie di tecnologie innovative basate sull'intelligenza artificiale per rilevare i falsi botnet sui social networks. Per i cittadini-utenti suggerisce di fare particolare attenzione a: (1) foto utente di fantasia o inverosimili; (2) contenuti testuali e linguistici preconfezionati, con sintassi e grammatica scadenti, mono-espressivi (3) pubblicazione seriale e scarsa variabilità dei post (4) rapporto follower-amici e tasso di coinvolgimento (like/follower) disequilibrato.

Annalisa Plava