fcri
Fundació Catalana per a la Recerca i la Innovació

10 TIPUS DE DESINFORMACIÓ UTILITZATS A LES XARXES SOCIALS

Material informatiu per al professorat de Secundària

Chryssanthopoulou, K., Gotsi, I., López, B., Miras, M., Neuvonen, M., Ražinskaitė, R., Salo, M., Varanauskas, A., Zinkevičiūtė, G.

Check or Cheat

European Commission

This project is co-funded by the European Commission under the preparatory action "Media Literacy for All 2018".

Índex

INTRODUCCIÓ

L'objectiu d'aquest document és que el professorat es familiaritzi amb deu tipus de desinformació que solen trobar-se a les xarxes socials. S'hi presenten nocions sobre cada un dels tipus de desinformació escollits, incloent-hi el grau d'engany, el principi de funcionament, exemples, mètodes de comprovació i altra informació rellevant.

Aquests continguts proporcionen només informació essencial relacionada amb el tipus concret de desinformació, ja que el document pretén ser un primer pas per als docents en el camí cap a l'alfabetització en matèria de mitjans de comunicació i informació. Després de cada tipus de desinformació o al final del document, es poden trobar enllaços a altres materials útils que, com aquest, animem categòricament a llegir i a utilitzar.

Es van seleccionar deu tipus de desinformació presents a les xarxes socials mitjançant un procés iteratiu. Al principi, es va analitzar el material i els estudis d'investigació existents i es va elaborar una llarga llista dels diferents tipus de desinformació. Tot seguit, experts de cada col·laborador, mitjançant activitats de catalogació i triatge, van seleccionar 15 tipus de desinformació sobre els quals es va seguir treballant. En l'últim pas, es van recollir els comentaris de professors i estudiants i es va poder reduir la llista a exactament deu tipus de desinformació emprats a les xarxes socials.

Aquest recurs educatiu es pot utilitzar com a material autosuficient (juntament amb diapositives preparades i complements visuals com pòsters o similars). Tanmateix, també hi ha disponibles de manera gratuïta mitjans excel·lents d'altres organitzacions. Per això, com a col·laboradors del consorci, en recomanem encaridament l'ús per tal que cada estudiant obtingui la millor experiència. Especialment, recomanem la infografia de la *European Association for Viewers Interest* (EAVI), en la qual es presenten deu tipus de notícies enganyoses (https://eavi.eu/beyond-fake-news-10-types-misleading-info/), així com els tipus d'informació errònia i desinformació definits per First Draft: https://firstdraftnews.org/fake-news-complicated/. Es poden trobar més fonts d'inspiració al final del document.

A més, dins d'aquest projecte (gaMEdia, cofinançat per la Comissió Europea en virtut de l'acció preparatòria *Media Literacy for All*, 2018, LC-01234900), es crearà un joc de cartes per a estudiants de 12 a 15 anys que s'hauria de fer servir com a eina complementària per a l'alfabetització mediàtica. A www.checkorcheat.eu es pot accedir a més informació i materials del projecte.

Abans de procedir a llegir la informació sobre els deu tipus de desinformació seleccionats, cal aclarir uns quants conceptes, ja que a vegades, actors diferents els utilitzen de manera diferent. En aquest projecte, fem servir les definicions següents per distingir els termes informació errònia, desinformació i malinformació:

- Informació errònia: Quan es difon informació falsa, però sense la intenció de fer mal.
- Desinformació: Quan es difon informació falsa a posta per fer mal.

- Malinformació: Quan es difon informació verdadera per fer mal.

Alguns temes d'aquest document no es presenten amb la profunditat que seria necessària. Tot i així, no s'exclouen per falta d'importància; tot al contrari, degut a la seva rellevància, requeririen una publicació apart. Una d'aquestes qüestions és el contingut de YouTube enganyós. Els infants de totes les edats miren nombrosos vídeos i, a causa dels algorismes de suggeriment, estan molt exposats a teories de la conspiració fora de mida, idees marginals o límit, al·legacions saludables paranoiques i contingut radicalitzat (discurs de l'odi). En aquest document es tracten els temes esmentats anteriorment, però no es presta cap atenció a l'ús de les seccions de comentaris com a armes, normalment per grups de la dreta alternativa. Una altra qüestió que no s'exposa aquí és la de les operacions psicològiques, que són operacions militars dirigides habitualment a influir en l'estat d'ànim de l'enemic a través de mitjans no combatius (com ara la distribució de tríptics); són molt complexes i requeririen fer una investigació extensa i centrar-se en tecnicismes. L'últim tema que creiem que cal esmentar és el ciberassetjament escolar (*cyberbullying*), ja que és un problema molt estès i molts estudiants s'hi enfronten en l'entorn d'Internet. Moltes de les tècniques emprades s'assemblen molt a les utilitzades en la desinformació (capacitat de difondre rumors, imatges i vídeos manipulats, nus, ús de mems divertits). Considerem que el tema del ciberassetjament escolar s'ha tractat de forma àmplia en els debats de l'educació contemporània i que molts autors ho han fet més bé del que podríem fer-ho nosaltres.

Abans de començar a llegir sobre els diversos tipus de desinformació, fem un petit recordatori sobre com cadascun de nosaltres pot contribuir a no difondre informació falsa o pensada per fer mal.

1. No llegeixis només el titular. Llegeix el text sencer abans de difondre'l, inclòs el nom de l'autor i la data de publicació. Si el relat és fals, aquí és on trobaràs les primeres pistes, especialment si el titular no coincideix amb el contingut.

2. Comprova si altres mitjans de comunicació informen sobre la mateixa història. Si només un mitjà informa d'una notícia concreta, darrere podria haver-hi una bona raó: podria tractar-se d'una exclusiva o basar-se en informació filtrada o procedent de fonts que volen romandre en l'anonimat. En aquests casos, altres mitjans d'informació acostumen a ser ràpids en intentar verificar la història o cobrir-ne la reacció, la qual cosa dona més confiança sobre la veracitat del relat. Però si cap dels mitjans de comunicació més coneguts no ha recollit la notícia i només la podeu trobar en blocs o mitjans minoritaris, espereu-vos abans de difondre la història o el vídeo.

3. Fes una cerca ràpida a Google. És possible que trobis més informació; o bé que descobreixis que la notícia es va publicar, per exemple, cinc anys abans, o que el titular és fals.

4. Quan algú et digui o passi alguna cosa que pugui semblar falsa, pregunta-li on l'ha sentida, vista o llegida.

En cas de dubte, no la difonguis. Deixar de difondre un contingut no fa mai mal; en canvi, sí que pot ser perjudicial compartir quelcom que no és cert.

Hipertrucatge (*deepfake)*

Qui ho pot fer:

Professional - **Aficionat** - Qualsevol.

No obstant, l'avenç de la tecnologia és incontrolable i, en un futur proper, es preveu que qualsevol podria fer-ho: https://www.theverge.com/2019/6/10/18659432/deepfake-ai-fakes-tech-edit-video-by-typing-new-words.

Ja existeixen aplicacions (https://www.malavida.com/en/soft/fakeapp/#gref) que els usuaris es poden descarregar per començar a experimentar.

Grau d'engany:

Baix - Mitjà - Alt - **Molt alt**.

La detecció d'un hipertrucatge és tot un repte. Els hipertrucatges fets per aficionats de vegades es poden detectar a simple vista, però cada cop són millors i aviat haurem de dependre de les anàlisis forenses digitals per detectar-los, si és que podem.

Descripció breu:

L'hipertrucatge és una tecnologia basada en la intel·ligència artificial (AI) que s'empra per crear o alterar el contingut d'un vídeo mitjançant la modificació de les cares (intercanvi de cares o creació de noves expressions facials). Els primers hipertrucatges es van obtenir canviant les cares de persones que sortien en vídeos per cares de celebritats, concretament en vídeos pornogràfics. Va ser el desembre de 2017 i ho va fer l'usuari de Reddit conegut com "deepfakes" (acrònim dels termes anglesos *deep learning* [aprenentatge profund] i *fake* [falsificació], encunyat després per designar aquest tipus de desinformació), que va utilitzar la tecnologia d'aprenentatge profund per editar les cares. Amb la finalitat de difondre informació falsa, es fa servir la tecnologia d'aprenentatge profund per crear una nova expressió facial en persones famoses que simula moviments musculars facials que acompanyen un text inventat, mai dit per aquesta persona.

Principi de funcionament (què fa i com):

L'hipertrucatge de vídeo s'aconsegueix mitjançant l'ús de dos sistemes d'AI que competeixen l'un amb l'altre: el que s'anomena generador i el denominat discriminador. El generador crea un vídeo fals i, a continuació, demana al discriminador que determini si és real o fals. Cada vegada que el discriminador precisa que un vídeo és fals, dona al generador una pista sobre què no fer quan creï el següent vídeo.

A mesura que el generador millora a l'hora de crear vídeos falsos, el discriminador millora a l'hora de detectar-los. Per contra, a mesura que el discriminador cada cop és més bo detectant vídeos falsos, el generador cada cop és més bo creant-los.

Junts, el generador i el discriminador formen el que s'anomena *xarxa generativa antagònica (GAN)*. El primer pas per establir una GAN és determinar-ne el resultat desitjat i crear un conjunt de dades d'entrenament per al generador. Quan el generador comença a obtenir resultats d'un nivell acceptable, els vídeos poden enviar-se al discriminador.

Font: https://whatis.techtarget.com/definition/deepfake.

Exemples:

Al canal de YouTube TheFakening es poden trobar molts exemples (alguns d'ells, aplicables a l'educació): https://www.youtube.com/c/TheFakening/videos.

Article de Gizmodo sobre l'hipertrucatge: https://gizmodo.com/insanely-accurate-lip-synching-tech-could-turn-fake-new-1796843610.

Vídeo "Synthesizing Obama": https://www.youtube.com/watch?time_continue=62&v=MVBe6_o4cMI&feature=emb_logo.

Mètode de comprovació:

Si l'hipertrucatge no és professional, és fàcil veure que les ombres no quadren o que la persona no pestanyeja. Però si és de més qualitat, no hi ha manera d'apreciar-ho a simple vista. Moltes empreses estan tractant de desenvolupar programari que pugui ajudar a identificar hipertrucatges: https://techcrunch.com/2020/09/14/sentinel-loads-up-with-1-35m-in-the-deepfake-detection-arms-race/. L'exèrcit nord-americà també està finançant un projecte per descobrir hipertrucatges: https://www.technologyreview.com/s/611146/the-us-military-is-funding-an-effort-to-catch-deepfakes-and-other-ai-trickery/.

Pseudociència

Qui ho pot fer:

Professional - Aficionat - **Qualsevol.**

És molt fàcil difondre pseudociència i no requereix cap tipus d'habilitat. Però l'elaboració de la teoria de la pseudociència és molt més difícil del que un s'espera.

Grau d'engany:

Baix - Mitjà - **Alt** - Molt alt.

Els promotors de la pseudociència sovint adopten el vocabulari de la ciència: descriuen conjectures en forma d'hipòtesis, teories o lleis; aporten "proves" fruit de l'observació i testimonis d'"experts"; o fins i tot desenvolupen el que semblen ser models matemàtics de les seves idees.

Per això, pot ser difícil saber si la informació és de fiar o no, sobretot sense una verificació addicional.

Descripció breu:

La pseudociència consta d'afirmacions, creences o pràctiques declarades científiques i objectives, però que són incompatibles amb el mètode científic.

La pseudociència sovint es caracteritza per afirmacions contradictòries, exagerades o no falsificables; per la dependència del biaix de confirmació enlloc d'intents rigorosos de desmentiment; per la falta de predisposició a l'avaluació feta per altres experts; per l'absència de pràctiques sistemàtiques a l'hora d'elaborar hipòtesis; i per l'adhesió persistent molt temps després d'haver-se desacreditat experimentalment les hipòtesis pseudocientífiques.

Font: https://www.youtube.com/watch?v=-X8Xfl0JdTQ.

Principi de funcionament (què fa i com):

El mot pseudociència suggereix que quelcom s'està presentant com a ciència de manera incorrecta o fins i tot enganyosa.

Quan una idea està molt generalitzada, però és errònia, sovint es pot convertir en un "fet" establert simplement a causa d'haver-se repetit molts cops. A vegades, aquesta desinformació és deguda a la ciència ficció i a la fantasia populars, que es basen o bé en conceptes antics obsolets o bé en una ciència actual però pobra i simple.

Les afirmacions pseudocientífiques *molt* poques vegades s'associen a prediccions científiques específiques i comprovables i, en canvi, es basen en un llenguatge imprecís i ambigu, que sovint inclou arguments ostentosos.

En la medicina dels xarlatans (*quack medicine*), un promotor de pseudociència podria afirmar que un tractament concret "elimina les toxines de l'organisme", sense dir mai *quines toxines*, com s'eliminen o com es pot saber si s'han eliminat. Les toxines són la veritable causa de la malaltia, tot i que mai es diu com la provoquen, i si s'eliminen et curaràs de tots els mals que pateixes.

Exemples:

Llistes d'exemples de pseudociència: https://examples.yourdictionary.com/examples-of-pseudoscience.html i https://rationalwiki.org/wiki/List_of_pseudosciences.

Mètode de comprovació:

La manera més senzilla de distingir el mètode pseudocientífic del científic és mirar si hi ha prediccions comprovables i veure si els experiments s'estableixen amb la intenció de provar la teoria o simplement de confirmar-la.

Pot ser útil saber distingir la ciència de la pseudociència:

CIÈNCIA	PSEUDOCIÈNCIA
L'objectiu principal de la ciència és aconseguir conèixer el món físic d'una manera més completa i unificada.	Les pseudociències tenen més probabilitats de ser impulsades per objectius ideològics, culturals o comercials. Alguns exemples: astrologia (provinent de la cultura babilònica antiga) ufologia (cultura popular i desconfiança en el govern), ciència de la creació (intent de justificar una interpretació literal de la Bíblia), aigües "amb l'estructura alterada" (xarlatanisme comercial).
La major part dels camps científics són objecte d'una investigació exhaustiva que dona lloc a l'ampliació contínua del coneixement en la disciplina.	El camp ha evolucionat molt poc des que es va establir per primera vegada. Generalment, la poca investigació i experimentació que es duu a terme es fa més per justificar la creença que per fer-la créixer.
El professionals del camp acostumen a buscar contraexemples o descobriments que es mostren incompatibles amb les teories acceptades.	En les pseudociències, el qüestionament d'un dogma acceptat sovint es considera un acte hostil, si no heretgia, i porta a controvèrsies rancoroses o fins i tot a cismes.
Les observacions o dades que no són lògiques des del punt de vista de la comprensió científica actual, una vegada s'ha demostrat que són creïbles, generen un gran interès en els científics i estimulen la realització de més estudis.	Les observacions o dades que no són coherents amb les creences establertes tendeixen a ser ignorades o ocultades activament.
La ciència és un procés en què cada principi ha de ser provat en el gresol de l'experiència i segueix sent objecte de qüestionament o rebuig en qualsevol moment.	Els principis fonamentals del camp no solen ser falsables i és poc probable que es modifiquin o que es demostri que són equivocats.
Les idees i els conceptes científics han de fer-se valer per ells mateixos, sobre la base del coneixement i l'evidència existents.	Els conceptes pseudocientífics solen estar determinats per egos i personalitats individuals, gairebé sempre per persones que no estan en contacte amb la corrent dominant

	de la ciència. Se sol recórrer a autoritats (un nom famós, per exemple) per guanyar suport.
Les explicacions científiques s'han de manifestar en termes clars i sense ambigüitats.	Les explicacions pseudocientífiques tenen tendència a ser vagues i ambigües, i sovint fan servir termes científics en contextos discutibles.

Font de la taula: http://www.chem1.com/acad/sci/pseudosci.html.

Dos vídeos per identificar la pseudociència: https://www.youtube.com/watch?v=gaDvroATyjw i https://www.youtube.com/watch?v=h-agrL1gS4c.

Contingut manipulat

Qui ho pot fer:

Professional - Aficionat - **Qualsevol**.

Cada dia, al món es comparteixen milions de fotografies i vídeos a les xarxes socials. Alguns d'aquests continguts estan manipulats, sovint per motius benèvols, com ara fer que un vídeo tingui una imatge més nítida o que un àudio se senti més bé. Però hi ha gent que es dedica a la manipulació de continguts per enganyar.

Les manipulacions es poden fer a través de tecnologia senzilla com Photoshop o mitjançant eines sofisticades que utilitzen tècniques d'intel·ligència artificial o "aprenentatge profund" per crear vídeos que distorsionen la realitat —anomenades habitualment "hipertrucatges" (els hipertrucatges es presenten per separat en aquesta anàlisi).

Grau d'engany:

Baix - Mitjà - **Alt** - Molt alt.

La identitat cada vegada és més difícil de validar, ja que els trols i els bots van adoptant noves maneres d'emmascarar el seu origen real. Els vídeos i les imatges manipulats són molt més difícils de detectar que la desinformació textual.

Les empreses plataforma estan sent cada cop més vigilades i pressionades per a què reaccionin. Algunes prenen mesures i eliminen aquest tipus de continguts. Però, fins i tot en les millors circumstàncies, això requereix un temps després del qual el mal ja està fet.

Descripció breu:

Es parla de "contingut manipulat" quan s'altera part d'un contingut autèntic; molt sovint es tracta de fotografies o vídeos. Els suports visuals es poden transformar mitjançant la manipulació fotogràfica, freqüentment anomenada "photoshopping". La manipulació de vídeo té com a diana d'actuació el vídeo digital i combina tècniques tradicionals de tractament i edició de vídeos amb mètodes auxiliars d' intel·ligència artificial com el reconeixement facial.

Principi de funcionament (què fa i com):

Les noves tècniques per modificar imatges, àudio i vídeo permeten la creació de contingut manipulat. El "photoshopping" pot fer que un producte, una persona o una idea semblin més atractius. S'aconsegueix destacant certes característiques. A més, es poden utilitzar altres tècniques com l'enquadrament o *framing* (es mostra només una part de la foto, cosa que la treu del seu context), que també distorsionen la realitat.

En la manipulació de vídeo típica, es repliquen l'estructura facial, els moviments corporals i la veu d'un subjecte per crear un enregistrament falsificat d'aquest subjecte. Les aplicacions d'aquests mètodes van des dels vídeos educatius fins als vídeos dirigits a la manipulació (massiva) i a la propaganda, una extensió clara de les possibilitats tradicionals de la manipulació fotogràfica.

Exemples:

Exemple de manipulació d'imatges: https://spotlightstories.co/32-examples-media-manipulating-truth/.

Guia del Washington Post sobre els vídeos manipulats: https://www.washingtonpost.com/graphics/2019/politics/fact-checker/manipulated-video-guide/.
Mètode de comprovació: Com comprovar la veracitat dels vídeos virals de les xarxes socials: https://www.youtube.com/watch?v=e91IGj_apsY. Eines en línia per esbrinar si una foto és autèntica: https://www.stopfake.org/en/13-online-tools-that-help-to-verify-the-authenticity-of-a-photo/.

Teoria de la conspiració (ciència marginal)

Qui ho pot fer:

Professional - Aficionat - Qualsevol.

La majoria de persones són consumidores de teories de la conspiració, enlloc de productores. No proposen les seves pròpies teories, sinó que avalen les que ja estan en circulació.

Grau d'engany:

Baix - Mitjà - **Alt** - Molt alt.

La creença en les teories de la conspiració generalment no es basa en proves, sinó en la fe de la persona creient. A la inversa, la teoria de la conspiració planteja l'existència de coalicions secretes d'individus i especula sobre les seves suposades activitats, que poden ser difícils de refutar.

Descripció breu:

Una teoria de la conspiració és una explicació d'un esdeveniment o d'una situació que invoca una conspiració a través d'actors sinistres i poderosos, sovint amb motivació política, quan altres explicacions són més probables. No obstant, a diferència de la pseudociència, la ciència marginal se serveix del mètode científic. Les idees estudiades pels científics marginals no tenen el suport de la ciència tradicional.

Les creences de la conspiració tenen el potencial de causar danys tant a les persones individuals com a la societat. El suport a la conspiració s'associa amb una disminució de la intenció de participar en causes socials i polítiques, una manca de disposició a seguir consells mèdics oficials, un augment de la voluntat de buscar teràpies alternatives i una tendència a rebutjar les dades científiques crítiques.

L'origen d'incomptables teories de la conspiració: https://www.youtube.com/watch?v=88_C-fogY40.

Motiu real pel qual les teories de la conspiració funcionen: https://www.youtube.com/watch?v=tfVgHRPC7Ao.

Principi de funcionament (què fa i com):

Les teories de la conspiració tenen una àmplia presència al web en forma de blocs i vídeos de YouTube, així com a les xarxes socials.

Les teories de la conspiració són, abans que res, formes de propaganda política. Estan dissenyades per denigrar individus o col·lectius específics o per fomentar programes polítics. La teoria que els Clinton estaven, d'alguna manera, involucrats en el suïcidi d'Epstein els denigra. La idea que el govern nord-americà va orquestrar el tiroteig massiu del 2012 a l'escola primària Sandy Hook va ajudar el lobby de les armes a desviar els arguments per obtenir un major control armamentístic. Quina millor manera d'anticipar-se a la crida per a un major control d'armes arran d'un tiroteig en una escola que afirmant que no havia arribat a passar?

Les teories de la conspiració proporcionen explicacions clares i internament coherents que permeten a les persones mantenir les creences davant la incertesa i la contradicció.

Exemples:

Les teories de la conspiració poden basar-se en qualsevol tema, però certs assumptes atreuen més interès que d'altres. Entre els temes preferits hi ha la mort i assassinat de gent famosa, les activitats moralment tèrboles dels governs, la ocultació de certes tecnologies i el terrorisme de "bandera falsa" (incriminar algú altre).

Algunes de les teories de la conspiració més arrelades i reconegudes són les relatives a l'assassinat de John F. Kennedy, l'aterratge a la lluna de l'Apollo el 1969 i els atacs terroristes de l'11 de setembre, així com nombroses teories sobre suposats complots de dominació mundial per part de diversos grups tant reals com imaginaris.

Llista d'articles sobre diferents conspiracions de WIRED (actualitzada): https://www.wired.com/tag/conspiracy-theories/page/1/.

Cinc conspiracions tecnològiques comprovades: https://www.businessinsider.com/facebook-microphone-listening-for-ads-other-tech-conspiracy-theories-explained-2019-9.

Vídeo de YouTube sobre diferents conspiracions: https://www.youtube.com/watch?v=_53cGxAUuDk.

"Fact check: A guide to 9 conspiracy theories Trump is currently pushing": https://edition.cnn.com/2020/09/02/politics/fact-check-trump-conspiracy-theories-biden-covid-thugs-plane/index.html.

Mètode de comprovació:

Llista de pàgines web per verificar fets (*fact-checking*): https://en.wikipedia.org/wiki/List_of_fact-checking_websites.

Iniciativa interessant finançada per la UE sobre la desinformació (s'hi inclouen les teories de la conspiració): https://euvsdisinfo.eu/.

Boles (llegendes urbanes i missatges en cadena)

Qui ho pot fer:

Professional - Aficionat - **Qualsevol**.

Tothom pot fer córrer una bola fent, simplement, declaracions objectives amb l'ús de paraules o d'un context desconeguts; n'és un exemple l'engany del monòxid de dihidrogen (el monòxid de dihidrogen és aigua. Exemple: "Els components atòmics del MODH o DHMO es troben en una sèrie de compostos càustics, explosius i tòxics com l'àcid sulfúric, la nitroglicerina i l'alcohol etílic"- http://www.dhmo.org/facts.html).

Grau d'engany:

Baix - **Mitjà** - Alt - Molt alt.

Les boles sobreviuen gràcies a la pròpia manera que tenim les persones de processar la informació i convertir-la en creences. Quan ens enfrontem amb informació nova, els humans no sempre fem el que és lògic: avaluar-la per si mateixa. Contràriament, sovint prenem decisions precipitades basades en com aquesta informació lliga amb les visions del món que tenim. I això que a través d'una breu cerca a Google de pàgines d'Internet que serveixen per verificar fets (*fast-checkers*) es pot demostrar amb bastanta rapidesa si certa informació és mentida.

Descripció breu:

Una bola és una falsedat articulada de manera deliberada per tal que sigui percebuda com la veritat.

Un aspecte comú de les boles és que totes tenen la finalitat d'enganyar o mentir. Perquè quelcom es converteixi en una bola, la mentida ha d'oferir alguna cosa més: ha de ser escandalosa o dramàtica, però també creïble i enginyosa. Sobretot, ha de ser capaç d'atreure l'atenció de la gent.

Les notícies falses (també conegudes com notícies enganyoses) es publiquen deliberadament amb boles que poden servir per complir l'objectiu propagandístic o desinformatiu — mitjançant l'ús de les xarxes socials per fer créixer el trànsit web i amplificar el seu efecte.

Una llegenda urbana és un gènere modern de folklore. Sol estar integrada per històries de ficció associades a fets macabres, supersticions, "críptids" o animals ocults, "creepypastes" i altres elements narratius dissenyats per fer por. Normalment, les llegendes urbanes provenen de la història local i la cultura popular.

Una carta en cadena és un missatge que intenta convèncer el destinatari que en faci còpies i les passi a un nombre determinat de persones (s'aplica de la mateixa manera als correus electrònics).

Principi de funcionament (què fa i com):

Com s'ha mencionat, una bola és informació falsa o mig certa que es presenta com a precisa i objectiva amb la intenció d'enganyar altres persones. Normalment, és sensacionalista, de manera que difondre-la contribueix a la seva finalitat perquè la gent tendeix a no comprovar la fiabilitat de la informació abans de compartir-la i posar-li un "m'agrada".

Exemples:

Quan un diari o un programa informatiu de ràdio o televisió informen d'una història falsa, aquesta es coneix com una bola. Els trucs publicitaris enganyosos, els fraus científics, les amenaces de bomba falses i les estafes empresarials són exemples de boles o enganys.

Una de les primeres boles registrades als mitjans de comunicació va ser un almanac fals publicat per Jonathan Swift sota el pseudònim d'Isaac Bickerstaff el 1708. Swift va predir la mort de John Partridge, un dels principals astròlegs d'Anglaterra en aquell moment, a l'almanac i, el dia en què se suposava que Partridge havia mort, va fer pública una elegia. Com a conseqüència d'això, la reputació de Partridge va resultar danyada, i el seu almanac astrològic no es va publicar durant els següents sis anys.

Alguns exemples contemporanis: https://www.mentalfloss.com/article/49674/14-greatest-hoaxes-all-time.

Mètode de comprovació:

Llista de pàgines web per verificar fets: https://en.wikipedia.org/wiki/List_of_fact-checking_websites.

Iniciativa interessant finançada per la UE sobre la desinformació (s'hi inclouen les boles): https://euvsdisinfo.eu/.

Pescaclics (*clickbait*)

Qui ho pot fer:

Professional - **Aficionat** - Qualsevol.

A la vegada que hi ha llocs web que prosperen gràcies a milers de clics d'entrada al seu contingut, molts autors veuen l'ús dels pescaclics com un mitjà per envair la psique humana mitjançant la confecció d'aquests titulars cridaners. De vegades els periodistes també utilitzen pescaclics. Un aficionat pot produir bons pescaclics de tant en tant, però els més reeixits i estables requereixen habilitats professionals.

Grau d'engany:

Baix - Mitjà - **Alt** - Molt alt.

El pescaclics s'ha convertit en una forma dominant dels mitjans de comunicació en línia: els titulars dissenyats per temptar la gent a fer-hi clic han esdevingut la norma. Resistir-se a un pescaclics és difícil, ja que el que fa és aprofitar els circuits neuronals que es van anar formant després de milions d'anys d'evolució. El nostre cervell no es va dissenyar per exposar-se a la gran varietat de temptacions que trobem en aquest món hiperconnectat.

Una forma de pescaclics que ja preocupa més és la que apel·la directament a les pors de les persones, especialment quan es relaciona amb una amenaça per a un grup social al qual es pertany: un pescaclics emocional. Aquest tipus de pescaclics compleix un doble propòsit: provocar nerviosisme tot suscitant la rivalitat entre grups i facilitar la difusió a través de les xarxes socials.

Descripció breu:

Un pescaclics és una forma d'anunci fals que fa servir textos o imatges en miniatura enllaçats i està dissenyat per atraure l'atenció de l'usuari i temptar-lo a seguir l'enllaç i llegir, veure o escoltar el contingut en línia que porta vinculat; es defineix per ser enganyós, generalment sensacionalista o fal·laç (font: https://www.cyber.gov.au/acsc/view-all-content/glossary/clickbait). El pescaclics com a efecte també es veu, a vegades, en titulars periodístics que exageren el contingut o en fan escàndol.

En alguns casos, els pescaclics s'utilitzen senzillament per generar ingressos: com més clics, més diners fets amb anunciants. Però aquests titulars i articles també es poden emprar per influir sobre un grup de persones a les xarxes socials. Estan construïts per actuar sobre els biaixos preexistents del grup d'interès i, així, poder difondre's dins de bombolles filtrades.

Principi de funcionament (què fa i com):

Els anomenats anuncis d'intriga tenen com a objectiu explotar la "bretxa de la curiositat", proporcionant la informació suficient per encuriosir els lectors de webs de notícies, però no prou com per deixar-los satisfets sense fer el clic que duu al contingut vinculat. Els titulars pescaclics hi afegeixen un element trampós: utilitzen esquers que no reflecteixen amb precisió el contingut presentat. La part "-bait" del terme en anglès (*clickbait*), que significa "esquer", es fa servir en analogia amb la pesca, en què un ganxo es disfressa amb un element atractiu (l'esquer), i dona la impressió als peixos de ser una cosa desitjable d'empassar.

De vegades el pescaclics s'assembla més a un esquer amb trampa (o *bait and switch*). És a dir, llegim un titular o enllaç enganxós, hi fem clic i el resultat és que ens trobem immersos en un anunci. El contingut apareix en clicar sobre l'enllaç, però queda completament rodejat d'anuncis publicitaris. Així, l'article o vídeo és en realitat un reclam que ens exposa a l'anunci, el *veritable* propòsit del contingut. Si prou persones s'exposen als anuncis, una part esdevindran compradores. Funciona perquè en altres llocs no s'utilitzaria tant.
Font: https://www.youtube.com/watch?v=qskqM9O0FC0.

Exemples:
https://adespresso.com/blog/clickbait-facebook-advertising-examples/
https://www.bluleadz.com/blog/the-scientific-reasons-why-clickbait-actually-works
https://www.reputationx.com/orm/techniques/process/content/orm-guest-posts/click-bait
https://medium.com/zerone-magazine/you-wont-believe-how-these-9-shocking-clickbaits-work-number-8-is-a-killer-4cb2ceded8b6

Mètode de comprovació:
S'han desenvolupat eines per abordar el problema dels pescaclics. Als navegadors s'hi han integrat detectors de pescaclics, mentre que a les plataformes digitals on es comparteixen continguts, com ara Twitter, el que s'ha fet és actualitzar els respectius algorismes per filtrar continguts pescaclics. Alguns grups de xarxes socials, com Stop Clickbait, combaten els pescaclics proporcionant un resum de l'article associat al pescaclics, cosa que tanca la "bretxa de la curiositat". La comunitat investigadora també ha desenvolupat connectors (*plug-ins*) d'explorador informadors de pescaclics per tal de notificar enllaços pescaclics i aconseguir més avenços en el camp basats en algorismes d'aprenentatge supervisat.
Aquí mostrem alguns consells que poden ajudar a no caure en la trampa dels pescaclics:

1. *Pensa en estratègies quan el problema no estigui passant.* Busca idees sobre com resistir als pescaclics quan el problema *no* estigui passant. Posa en pràctica algunes d'aquestes idees i avalua'n els resultats. Comença amb les estratègies més senzilles i fàcils d'implementar. A vegades, fins i tot els petits canvis donen fruits importants.
2. *Fixa't en els patrons de conducta que tens i substitueix-los per d'altres amb una major capacitat d'adaptació*. Potser, a partir d'una petita recopilació de dades, t'adones que tens tendència a endinsar-te al forat de cuc de YouTube (probablement, un subtipus de pescaclics) a la feina, a última hora de la tarda. Per a què serveix? Potser és que necessites un descans? Hi ha alguna altra manera per alleujar l'avorriment o l'angoixa que tens?
3. *Planteja't l'ús d'eines de bloqueig de llocs web*. Hi ha molts instruments que poden ajudar-nos a salvar-nos de nosaltres mateixos. Per exemple, si estem comprovant contínuament si una web concreta ha actualitzat les notícies que conté (i ens enganxen els pescaclics), podem instal·lar un recurs que ens limiti l'accés a aquests llocs temptadors durant períodes de temps definim nosaltres mateixos.

Vídeo de YouTube sobre com detectar pescaclics: https://www.youtube.com/watch?v=8IzfzoZsa-Q.

Publicitat (màrqueting natiu, polític, enganyós, amb influenciadors)

Qui ho pot fer:

Professional - Aficionat - Qualsevol.

Una publicitat eficaç requereix una inversió econòmica i, sovint, l'ús de tècniques sofisticades. Són necessàries certes habilitats per crear el contingut visual o d'àudio d'un anunci. Es disposa de moltes dades de recerca en els camps de la neurociència, la psicologia i l'anàlisi de dades. És important assenyalar que amb vàries eines de creació d'anuncis, tant gratuïtes com de pagament, i plataformes (fàcils d'utilitzar) de publicitat i màrqueting comportamental per a les xarxes socials, fer anuncis cada vegada és més fàcil i està més a l'abast de tothom.

Grau d'engany:

Baix - **Mitjà** - Alt - Molt alt.

La majoria dels anuncis estan identificats com a contingut patrocinat o bé estan col·locats d'una manera que permet al consumidor saber que el material és publicitari. Algunes formes de publicitat (publicitat nativa i publicitat amb influenciadors) són més difícils de reconèixer. Fins i tot quan s'identifiquen, les afirmacions que es presenten als anuncis poden ser bastant enganyoses.

La normativa en matèria de publicitat limita el grau de manipulació; tot i així, existeixen diferents mètodes per intentar enganyar els consumidors que no estan permesos segons les lleis sobre publicitat.

Descripció breu:

La publicitat és una tàctica comercial que implica pagar un espai per promoure un producte, servei o causa. Els missatges promocionals pròpiament dits reben el nom d'anuncis. L'objectiu de la publicitat és arribar a aquelles persones amb més probabilitat d'estar disposades a pagar els productes o serveis d'una empresa i convèncer-les que ho comprin.

Els anuncis es poden posar gairebé a qualsevol lloc: tanques publicitàries a la carretera, laterals d'edificis, llocs web, butlletins d'informació electrònics o impresos, taulers d'anuncis, envasos de productes, cobretaules de paper en restaurants, revistes d'esdeveniments, aparadors, laterals de cotxes, autobusos o vagons de metro, quioscs d'aeroports, estadis esportius, vídeos de YouTube i molts d'altres.

Principi de funcionament (què fa i com):

Als venedors i anunciants els sobren els recursos que ajuden a incitar, persuadir i fins i tot influir en els hàbits de compra de les persones: des dels clàssics com les dades derivades de fonts demogràfiques, geogràfiques i etnogràfiques fins a solucions més emprenedores com el reconeixement facial, la biometria del llenguatge corporal o el màrqueting personalitzat basat en informació psicogràfica (per a més informació: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie).

La publicitat pot utilitzar l'engany mitjançant la millora fotogràfica o *photobleaching* (que dona lloc a resultats falsos i inabastables), la omissió d'informació, l'ocultació de tarifes o

recàrrecs, la manipulació d'unitats de mesura i patrons, l'ús de farciments i envasos de grans dimensions o l'ús d'al·legacions saludables falses.
Els anuncis també poden exagerar el valor d'un producte fent servir termes no demostrats i sense sentit, basats més en l'opinió que en els fets, i en alguns casos a través de la manipulació de dades.
El **màrqueting personalitzat** és una poderosa eina publicitària que permet mostrar anuncis a poblacions específiques o, fins i tot, a persones concretes, en línia. Per exemple, permet als polítics dirigir-se a grups molt reduïts de votants a través de missatges a mida amb el potencial de manipular el debat polític. Funciona així: Durant les campanyes polítiques es creen bases de dades sobre els votants que inclouen informació sobre si una persona està registrada per votar, amb quina freqüència vota, si està afiliada a algun partit, la seva adreça física i de correu electrònic i el seu número de telèfon. Tot seguit, aquests fitxers d'electors es pugen a Google i Facebook per trobar els perfils en línia d'aquestes persones i, a continuació, es mostren anuncis específics per a elles (font: https://www.vox.com/recode/2019/11/27/20977988/google-facebook-political-ads-targeting-twitter-disinformation).
L'**esquer amb trampa (*bait and switch***) és una estratègia de vendes en què el client és atret per l'anunci d'un article de baix preu, però llavors se l'anima a comprar un article més car. O consisteix en el truc d'oferir a una persona quelcom atractiu per guanyar-se-la (p. ex. guanyar-ne el suport polític), i tot seguit, frustrar les seves esperances amb alguna cosa menys desitjable (font: https://www.merriam-webster.com/dictionary/bait%20and%20switch).
El màrqueting natiu és la creació d'anuncis de pagament d'acord amb l'aspecte, l'atmosfera i la funcionalitat del format comunicatiu en què aquests apareixen. La paraula "natiu" fa referència a la coherència del contingut amb els altres materials que es mostren a la plataforma. Són anuncis que es camuflen amb més facilitat amb el contingut digital, de manera que és més difícil d'identificar-ne la naturalesa (font: https://www.outbrain.com/native-advertising/).
El **màrqueting amb influenciadors (*influencers*)** és un tipus de màrqueting de les xarxes socials que se serveix del suport de persones, organitzacions i grups considerats influents o experts en una àrea determinada (font: https://entrepreneurship.babson.edu/what-is-influencer-marketing/).
La publicitat té com a objectiu presentar la millor faceta d'un producte. El procés creatiu gaudeix de certa llibertat d'acció. El problema sorgeix quan la dramatització creua la línia i passa a representar falsament un producte.
La **publicitat política** intenta influir o parlar sobre un tema que, en el moment present, és objecte d'un extens debat polític (font: https://adstandards.com.au/issues/political-and-election-advertising).
Existeix una preocupació generalitzada sobre els efectes que la representació del consum d'alcohol per part dels mitjans de comunicació, l'emplaçament de productes alcohòlics i la publicitat de begudes alcohòliques poden tenir en el consum d'alcohol i l'aparició de problemes relacionats amb la beguda entre el jovent. La televisió, la ràdio, el cinema i la música solen assenyalar-se com a possibles fonts de coneixença de l'alcohol que tenen els joves, així com a possibles agents que influeixen en el consum i en els problemes resultants en aquest grup de població.

Exemples:
Ribena-maker fined $217,500 for misleading vitamin C ads.

Airbrushed make-up ads banned for 'misleading'.
Climbing rope not suitable for climbing.
General election 2019: Ads are 'indecent, dishonest and untruthful'.
Màrqueting amb influenciadors:

- TikTok
- Instagram
- Instagram (2)

Publicitat nativa:
https://www.paldesk.com/spot-native-advertising/
https://www.wordstream.com/blog/ws/2014/07/07/native-advertising-examples

Exemples lituans:
https://www.instagram.com/p/B74tR_UHVk3/?igshid=1nkmddft9w4w2

Mètode de comprovació:
Facebook Political Ad Collector: Aquest recurs mostra als usuaris els anuncis que es troben al seu fil de continguts de Facebook i esbrina quins són polítics. També els mostra els anuncis polítics dirigits a altres usuaris. Tots els anuncis polítics recollits es registren en una base de dades disponible públicament.
Who Targets Me: Aquesta eina permet als usuaris crear un perfil anònim i recopilar informació sobre els anuncis, polítics o no, que els apareixen, juntament amb el motiu pel qual se'ls han enviat aquests anuncis. Aquest instrument pot proporcionar als usuaris estadístiques sobre qui o què els ha tingut com a objectiu i utilitza aquesta informació per construir una base de dades de publicitat i segmentació polítiques.
TV News Fact Check: El TV News Archive és una iniciativa per al desenvolupament d'un arxiu de mitjans digitals que conté, entre d'altres, pàgines web, llibres i textos, enregistraments d'àudio, vídeos, imatges i programari. Un dels seus projectes, el "Political TV AD Archive", és un arxiu d'anuncis polítics del 2016 en combinació amb la comprovació de fets d'una gran varietat de fonts (p. ex. Politifact, Factcheck.com).

Sàtira (paròdia)

Qui ho pot fer:

Professional - Aficionat - Qualsevol.

Tot i que l'humor i la sàtira de qualitat no acostumen a suposar un esforç per al lector, per a l'escriptor sí que exigeixen un treball i una pràctica i requereixen cura i revisió, i és que es diu que la sàtira és un dels tipus d'humor més difícils d'escriure. Normalment, per tal de parlar d'un tema important i fer-ne un comentari seriós de manera que s'interpreti amb una nota d'humor, l'autor ha de destacar en un parell de coses: ha de ser intel·ligent, culte i estar ben informat; i ha de saber ser oportú.

Grau d'engany:

Baix - Mitjà - Alt - Molt alt.

La sàtira no ha de ser fal·laç: quan algú crea una sàtira, busca fer-ho de manera que el lector vegi que es tracta de sàtira.

No obstant, en nombrosos casos, fins i tot els governs, els polítics, els mitjans de comunicació dominants o les agències de notícies són enganyats per la sàtira i la presenten com si es tractés de notícies creïbles.

Descripció breu:

Sàtira: ús de l'humor, la ironia, l'exageració o la burla per exposar i criticar l'estupidesa o els vicis de les persones, especialment en el context de la política contemporània i d'altres temes d'actualitat.

La paròdia és una forma de sàtira en què s'exageren les característiques més destacades de figures públiques, artistes o gèneres, es copia intencionadament l'estil d'algú famós o es copia una situació concreta, fent més evidents i d'una manera còmica les característiques o qualitats de l'original.

La comèdia satírica ridiculitza les polítiques o les doctrines filosòfiques o bé ataca les desviacions de l'ordre social escarnint aquells que en violen els valors morals o de maneres.

La ironia descriu situacions estranyes o gracioses perquè les coses passen d'una manera que sembla ser tot el contrari del que s'esperava (la diferència entre el que es diu o es fa i el que es vol dir).

Principi de funcionament (què fa i com):

La sàtira és una forma d'art influent que pot assenyalar les deficiències de certs comportaments humans i de les qüestions socials que se'n deriven convertint-les en absurdes, fins i tot hilarants; el resultat és que esdevé entretinguda i arriba a un públic ampli. La sàtira també pot protegir els seus creadors de la culpabilitat de la crítica, ja que aquesta s'insinua en lloc de declarar-se obertament; d'aquesta manera, es converteix en una eina poderosa per als dissidents en períodes polítics i socials difícils o opressius.

La sàtira ha perdurat com a tècnica narrativa durant segles perquè ofereix una barreja brillant d'alleujament còmic i crítica social. Combina l'entreteniment amb un propòsit.

Font: https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1065&context=srhonorsprog.

Eines de la sàtira:

1. **Exageració**: Hipèrbole o subestimació. Ampliar, augmentar o representar alguna cosa més enllà dels límits normals, de manera que esdevé ridícula i se'n poden veure els defectes.
2. **Ironia**: Presentar coses fora de lloc o absurdes respecte l'entorn.
3. **Inversió**: Presentar el contrari de l'ordre regular (p. ex., l'ordre dels esdeveniments, l'ordre jeràrquic).
4. **Paròdia**: Imitar les tècniques o l'estil d'una persona, lloc o cosa.
5. **Cinisme**: La capacitat de mirar amb sospita alguna cosa o algú i d'oferir una opinió contrària a l'*statu quo* és una eina excel·lent per a la sàtira
6. **Doble sentit**: Dir una cosa referint-se (clarament) a una altra.

Exemples:

- https://www.thedailybeast.com/fooled-by-the-onion-9-most-embarrassing-fails
- https://www.theonion.com/
- https://www.currantdaily.com/
- https://babylonbee.com/
- https://theconversation.com/too-many-people-think-satirical-news-is-real-121666
- https://preview.redd.it/18bwg09g3zn11.jpg?width=640&crop=smart&auto=webp&s=88def0be2595c89ef9ce12cc2a625218d3fa371f

Programes de televisió, vídeos:

- LastWeek Tonight, The Daily Show with Trevor Noah, The Late Show with Stephen Colbert, Late Night with Seth Meyers.

Mems:

- https://i.chzbgr.com/full/9233889792/hF2226249/meme-about-the-first-picture-of-earth-taken-from-space-being-of-a-turtle-with-grass-on-its-back
- http://www.electomatic.com/political-meme-tracker/
-

Exemples lituans:

- https://1k.lt/r-karbauskis-uzdrausime-kampus-nes-juose-yra-laipsniu/

Mètode de comprovació:

La major part d'obres satíriques tenen en comú les característiques següents:

- La sàtira es basa en l'humor per provocar el canvi social.
- La sàtira gairebé sempre és implícita. El lector ha de captar l'humor per no perdre el caràcter satíric de l'obra.
- La majoria de vegades, la sàtira no se centra en persones específiques. Contràriament, es dirigeix al conjunt de la societat o a tipus de persones en una societat: el polític, l'adúlter, l'altiu, etc.
- L'agudesa i la ironia de la sàtira són exagerades; és en l'exageració que la gent es fa conscient de la seva estupidesa.

Trols, bots i comptes falsos o *puppet accounts*

Qui ho pot fer:

Professional - **Aficionat** - Qualsevol.

El grau de destresa necessari per produir un trol, bot o compte fals actiu varia. Qualsevol pot crear i utilitzar un compte fals senzill, fer servir tècniques de trolejat o comprar bots per construir una granja de clics i m'agrades. Hi ha eines digitals que poden generar tot tipus d'informació personal falsificada, necessàries per crear comptes falsos —des de noms postissos i adreces de correu electrònic temporals fins a la generació i validació de números d'identificació nacional. Es necessiten uns coneixements mínims de programació per crear bots de xarxes socials.

Els efectes més nocius dels trols, els bots o els comptes falsos solen ser provocats per persones amb habilitats professionals. Alguns bots empren tècniques avançades d'AI per tal de semblar més realistes; alguns trols utilitzen tècniques narratives i manipuladores convincents per aconseguir la reacció que volen. Avui dia, la creació de perfils de xarxes socials falsos (o la compra de m'agrades) és una indústria amb un valor superior als 700 milions d'euros.

Grau d'engany:

Baix - Mitjà - **Alt** - Molt alt.

El grau d'engany és molt variable: mentre que alguns trols, bots o comptes falsos es poden identificar fàcilment, d'altres semblen comptes de persones reals i requereixen una investigació més rigorosa per identificar-los.

En un estudi de la School of Systems Engineering de la Universitat de Reading es va observar que al 30% de les persones que hi van participar se les podia enganyar perquè creguessin que era una persona real la que dirigia un compte robot en una xarxa social. Els trols solen enganyar a altres usuaris de les xarxes socials publicant contingut inofensiu i creant perfils i històries realistes.

Descripció breu:

Un trol és una persona que intenta, expressament, molestar o començar una discussió, sobretot mitjançant la publicació de missatges o apunts ofensius o desagradables a Internet (font: https://www.collinsdictionary.com/dictionary/english/troll).

Un bot és un programa informàtic que executa tasques automatitzades a Internet (en el cas que ens ocupa, el que fa és seguir comptes de xarxes socials i interaccionar-hi clicant m'agrada, fent comentaris, compartint publicacions o utilitzant altres funcionalitats de la plataforma). Els bots es comporten de manera autònoma, parcialment o bé del tot, i sovint estan dissenyats per imitar els usuaris humans.

Un compte fals és un compte que algú crea per actuar de maneres que no li estan permeses públicament o per donar suport a quelcom seu (per afavorir el seu propi material, penjar comentaris positius, fer elogis o anunciar la seva feina).

Principi de funcionament (què fa i com):

Algunes **tàctiques que utilitzen els trols** (font: https://medium.com/better-humans/the-complete-guide-to-understanding-and-dealing-with-online-trolls-4a606ae25c2c):

- **Negar-se a fer marxa enrere amb fal·làcies conegudes:** Quan un trol diu una mentida (directament o mitjançant l'ús d'hipèrboles, omissions o tergiversacions), molts d'altres la repetiran, fins i tot si es pot refutar fàcilment.
- **Trol telèfon:** Un trol d'un fòrum diu una bajanada i un altre trol l'adopta com a certa i la repeteix en un altre fòrum. Llavors es converteix en una mentida que es va repetint.
- **Fer de llop marí (*sea-lioning*):** Qüestionament reiterat i incessant, sovint un cop la qüestió s'ha explicat detalladament diverses vegades. L'anomenat lleó marí insistirà que està actuant amb total cortesia, però en realitat està intentant fer-te perdre el temps tant com pugui i desviar la conversa. El nom prové d'un còmic: http://www.muddycolors.com/wp-content/uploads/2017/12/81acd-a5b.jpg.
- **Provocació (*flaming*):** Plantejar temes incendiaris i controvertits per aclaparar un lloc o un moderador, que tracta d'identificar i controlar cada una de les publicacions.
- **Policia ortogràfica o gramatical:** No l'importa el contingut de l'apunt o comentari, però insisteix en què l'ortografia i la gramàtica han de ser perfectes per poder donar arguments vàlids.
- **Bumerang:** Algú que apareix tant com pot per anar comentant un fil. Fins i tot si el bloqueges a les xarxes. Es crearà comptes nous i seguirà fent comentaris per seguir-te fins que et convenci que té raó.
- **Inundació**: Quan algú fa un apunt a la teva pàgina, però repeteix el mateix una vegada i una altra per impedir que tinguis una conversa amb qualsevol altra persona. Normalment es tracta d'abreviacions com LOL (o XD) o NSFW (*Not Safe for Work*, inadequat per a la feina), o simplement de text infantil o burleta.
- **Enemic, odiador o *hatemonger***: Persona que va directament a atacar amb paraules incendiàries o insults —o a amenaçar de mort o violació—, fins i tot quan el fil o els comentaris no justifiquen aquest grau de resposta. Condueix tots els comentadors sensats a un frenesí acalorat i la conversa es converteix immediatament en una baralla.

Perquè els bots socials puguin implementar-se en un canal específic (de les xarxes socials), la plataforma ha de ser accessible a través d'una interfície de programació d'aplicacions (API), oferta, per exemple, per Twitter i Facebook. Mitjançant l'ús d'API, es pot controlar simultàniament i amb poc esforç un gran nombre de comptes bot. A través de cerques senzilles de paraules clau, escanegen les cronologies (o TL, de *timelines*) de Twitter i les publicacions de Facebook per trobar termes o etiquetes específics. Així que troben el que busquen, comenten, comparteixen enllaços o comencen un debat fictici. O bé fan comentaris directament sobre temes específics. En combinació amb altres bots (que formen el que s'anomena una xarxa de zombis o *botnet*), el soroll que fan és cada cop més fort i pot despistar a altres usuaris.

Els **bots de xarxes socials** maliciosos es poden utilitzar per a diversos propòsits (font: https://www.cloudflare.com/learning/bots/what-is-a-social-media-bot/):

- **Augmentar artificialment la popularitat d'una persona o moviment**: Una persona o organització amb milions de seguidors a les xarxes socials es pot considerar important o influent. Un dels usos principals dels bots de les xarxes socials és l'impuls de la popularitat aparent d'altres comptes.

- **Influir en les eleccions**: En un estudi publicat a First Monday, una revista amb revisió científica externa, es va veure que el dia anterior a les eleccions presidencials dels EUA del 2016, un 20% del debat polític a les xarxes socials va ser generat per prop de 400 000 bots de xarxes socials.
- **Manipular els mercats financers**: Els bots de xarxes socials també es poden utilitzar per influir en els mercats financers. Per exemple, els comptes bot poden inundar les xarxes socials amb notícies inventades, bones o dolentes, sobre una empresa, en un intent de manipular la direcció dels preus de les accions.
- **Incrementar els atacs de pesca:** Els atacs de pesca depenen d'un atacant que es guanya la confiança de la seva víctima. Els seguidors falsos de les xarxes socials i la interacció social poden ajudar a convèncer una víctima que el seu estafador es de fiar.
- **Escampar contingut brossa o *spam***: Els bots de xarxes socials s'acostumen a utilitzar amb finalitats publicitàries il·lícites mitjançant la inundació indiscriminada de les xarxes socials amb enllaços a llocs web comercials.
- **Censura de la llibertat d'expressió**: Durant el moviment de la Primavera Àrab de 2010-2012, diversos organismes públics van utilitzar bots a Twitter per omplir els canals de continguts de les xarxes socials. Aquests bots es van utilitzar per dissipar a propòsit els missatges dels manifestants i dels activistes.

Més informació sobre trols: https://www.lifewire.com/types-of-internet-trolls-3485894.

Més informació sobre bots: https://niccs.us-cert.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=ncsam_socialmediabotsoverview_508.pdf.

Exemples:

Trols:

- https://www.rollingstone.com/politics/politics-features/russia-troll-2020-election-interference-twitter-916482/
- https://motherboard-images.vice.com/content-images/contentimage/32137/1459536705346993.png?resize=664:*
- https://motherboard-images.vice.com/content-images/contentimage/32137/1459536758030213.png?resize=638:*
- https://imgur.com/gallery/INtY5SB
- Compte fals de trol de suport als consumidors: https://imgur.com/t/trolling/4yTQWCo

Bots:

- https://www.targetinternet.com/social-media-spam-bots-and-fake-engagement/

Comptes falsos:

- https://socialmediarevolver.com/fake-facebook-accounts-attacking-facebook-groups/
- https://www.hackread.com/google-image-search-social-media-profiles/
- https://www.sbs.com.au/news/thai-click-farm-raided-over-300-000-sim-cards-found
- https://techcrunch.com/2018/08/27/twitter-suspends-more-accounts-for-engaging-in-coordinated-manipulation/

Mètode de comprovació:

Com identificar els diferents tipus de trols i ocupar-se'n: https://www.teamtechnology.co.uk/troll-tactics.html.

Tot i que alguns dels bots de xarxes socials més avançats poden ser difícils de detectar fins i tot per als experts, hi ha estratègies per identificar comptes bot menys sofisticats. Entre elles, s'inclouen les següents:

- Portar a terme una cerca inversa d'imatges a partir de la foto de perfil per veure si s'està utilitzant una foto d'una altra persona treta de la xarxa.
- Mirar les hores de les publicacions. Si hi ha publicacions fetes en hores del dia que no quadren amb el fus horari del compte o penjades cada pocs minuts cada dia, el que ens indica això és que el compte està automatitzat.
- Utilitzar un servei de detecció de bots, com botcheck.me, que fan servir l'aprenentatge automàtic per detectar comportaments típics de bots. Cloudflare Bot Management també usa l'aprenentatge automàtic per reconèixer bots.
- https://botometer.iuni.iu.edu.

Com identificar un compte de xarxa social fals: https://smallbusiness.chron.com/spot-social-media-fake-46150.html.

Establiment d'amistat (i suplantació d'identitat)

Qui ho pot fer:

Professional - **Aficionat** - Qualsevol.

Aconseguir una bona suplantació d'identitat exigeix grans habilitats, però fins i tot els aficionats poden fer-ho de manera creïble i enganyar a altres persones. Fer o establir amistat demana coneixements psicològics bàsics i la capacitat de llegir altres persones.

Grau d'engany:

Baix - **Mitjà** - Alt - Molt alt.

Algunes suplantacions són fàcils de detectar. És possible que alguns delinqüents fingeixin ser una gran organització amb la qual probablement hi fas negocis. Per contra, d'altres investigaran més exhaustivament les teves dades i l'empresa per la qual treballes i intentaran fer-te creure que són executius de l'empresa. És difícil detectar un establiment d'amistat d'aquest tipus al començament d'un procés així, ja que no hi ha cap diferència respecte d'una relació cordial. En etapes posteriors, quan la persona que ha buscat amistat intenta obtenir algun benefici d'aquesta relació, les males intencions esdevenen més fàcils de detectar.

Descripció breu:

Suplantació d'identitat: imitació d'accions o comportaments d'una altra persona. Fingir ser algú altre.

Establiment d'amistat: fer-se passar per una amistat (actual o futura) a les xarxes socials amb l'objectiu d'enganyar o treure algun profit (és a dir, aconseguir informació personal, fotos, vídeos, etc.).

Principi de funcionament (què fa i com):

Sovint, els comptes falsos s'utilitzen per suplantar la identitat d'algú. Aquests comptes imiten celebritats, marques o organitzacions existents o persones aleatòries. De vegades, els comptes poden imitar amics, familiars o d'altres persones properes a la possible víctima. Alguns cops, en lloc de crear comptes falsos, els hackers tenen com a diana comptes d'usuaris inactius i els utilitzen per arribar a amistats que encara són actives a la plataforma.

Quan es creen comptes que imiten celebritats o organitzacions, s'utilitzen llacunes presents a les plataformes de les xarxes socials. Per exemple, és possible imitar un canal popular de YouTube, ja que el nom que es mostra als canals i comptes de YouTube pot ser diferent del nom real del compte. Dins de YouTube, els usuaris poden enviar sol·licituds d'amistat a qualsevol persona de la plataforma. Un cop acceptada una sol·licitud, ja es poden enviar missatges directes a la persona. D'aquesta manera, algú que suplanti la personalitat d'un youtuber famós pot enviar missatges als subscriptors i fer-los creure que la celebritat en persona ha contactat amb ells.

De vegades, s'envien missatges elementals que informen al destinatari que ha guanyat alguna cosa i el conviden a fer clic a enllaços que van a parar a contingut brossa o a llocs maliciosos. En altres ocasions, aquests actors amenaçadors han tret partit de la combinació de tècniques d'imitació creatives per incrementar la legitimitat dels seus missatges i augmentar la probabilitat que els usuaris cliquessin els seus enllaços.

En el cas de l'establiment d'amistat, es poden utilitzar tant comptes falsos com comptes reals. Però això depèn del mitjà en què ocorre; per exemple, en els videojocs en línia normalment s'utilitzen sobrenoms que no donen cap informació sobre la veritable identitat de la persona.
Mitjançant la suplantació d'identitat o l'establiment d'amistat, els estafadors també poden enganyar a la gent aconseguint que faci les següents coses:

- donar diners (fent una transferència o una donació);
- donar informació delicada o confidencial;
- descarregar programari maliciós;
- visitar llocs web que són estafes.

Un intent típic d'imitació que fan els ciberdelinqüents és fer veure que treballen per un dels principals reproductors en línia als quals es paga una quota de subscripció regular. En són exemples habituals Apple Music, Spotify o Netflix. Reps un missatge desconcertant a la safata d'entrada que adverteix d'un problema amb el teu compte. Diu que si no fas clic ràpidament a un enllaç, no tindran més remei que bloquejar-te el compte i no podràs tornar-hi a accedir. Si hi fas clic, se t'enviarà a un lloc web d'imitació que s'assembla (si no és idèntic) a l'empresa suplantada i se't demanarà que proporcionis les teves credencials d'accés.
Un cop accedeixis al lloc fals, se't demanarà que confirmis les teves dades de facturació, però els delinqüents demanen molta més informació de la que hauries de proporcionar. Et demanaran l'adreça de correu completa i la informació de la targeta de crèdit, incloent-hi la data de venciment i el codi CVV. Encara que sembli increïble, alguns et demanaran altres tipus d'informació personal com el nom de la teva mare o el número de la seguretat social; és a dir, tot el que un ciberdelinqüent necessiti per robar-te la identitat, obrir comptes nous al teu nom o apoderar-se d'alguns dels teus altres comptes. Altres ciberdelinqüents utilitzen tècniques similars, però afirmen ser del teu banc o de la teva companyia telefònica.

Exemples:

- https://www.riskiq.com/blog/labs/youtube-impersonation-scams/
- Joc de preguntes i respostes "Find the Fake": https://www.zerofox.com/find-the-fake/

Mètode de comprovació:

Si algú està intentant convence't que és una persona famosa, pren les precaucions següents:

- Verifica la identitat de la persona que ha contactat amb tu. Pots verificar que és qui diu ser? Si no és així, o si no ho tens clar, deixa de contestar-li i no facis el que et demana.
- Si la celebritat es posa en contacte amb tu a través del seu propi compte d'una xarxa social, revisa minuciosament el compte. Inclou la insígnia de verificació blava que confirma que la persona és qui diu que és? La informació del compte coincideix amb notícies sobre aquesta celebritat?
- Fes una cerca a Google escrivint-hi el nom de la persona i la paraula "estafa" o "scam" per veure què surt.
- Planteja't denunciar l'assumpte a la xarxa social on has trobat aquesta persona.

Comprova el perfil de les persones que t'han sol·licitat amistat o que les afegeixis a la teva xarxa, sobretot si només coneixes la persona per Internet. Ves en compte amb el següent:

- Perfils nous amb poc contingut.
- Llistes ocultes d'amics o connexions o llistes plenes de persones del sexe contrari.

- No enviïs diners a ningú que no hagis conegut mai en persona.
- Vigila a l'hora d'enviar fotos o vídeos personals, sobretot si no coneixes el destinatari personalment. Als estafadors se'ls coneix per fer xantatge a les persones que tenen com a objectiu fent servir material comprometedor.
- No passis informació personal a ningú que no hagis conegut mai en persona.
- Fes una cerca d'imatges del teu admirador o admiradora per comprovar si és qui diu que és. Fes servir serveis de cerca d'imatges com Google o TinEye.

RECURSOS

Hem tret la inspiració d'aquí:

https://eavi.eu/ i, concretament, https://eavi.eu/beyond-fake-news-10-types-misleading-info/;

https://firstdraftnews.org/ i, concretament, https://firstdraftnews.org/latest/fake-news-complicated/;

https://euvsdisinfo.eu/;

https://newslit.org/;

https://groundviews.org/2018/05/12/infographic-10-types-of-mis-and-disinformation/;

https://en.unesco.org/sites/default/files/f._jfnd_handbook_module_2.pdf;

https://misinfocon.com/catalogue-of-all-projects-working-to-solve-misinformation-and-disinformation-f85324c6076c;

https://www.ifla.org/publications/node/11174;

https://faktabaari.fi/assets/FactBar_EDU_Fact-checking_for_educators_and_future_voters_13112018.pdf;

http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf;

http://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf.