COMPÀS

Desinformació a les xarxes socials:

Què és i com identificar-la

Check or Cheat

fcri
Fundació Catalana per a la Recerca i la Innovació

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

Elaborat per:

López, B. (Fundació Catalana per a la Recerca i la Innovació, Catalunya)

Carrillo, N. (Universitat Autònoma de Barcelona, Catalunya)

Chryssanthopoulou, K., Gotsi, I. (Media Literacy Institute, Grècia)

Neuvonen, M., Ražinskaitė, R., Salo, M. (Avoin Yhteiskunta RY, Finlàndia)

Varanauskas, A., Zinkevičiūtė, G. (Knowledge Economy Forum, Lituània)

Coordinació i edició versió en català:

López, D., Sastre, D. (Fundació Catalana per a la Recerca i la Innovació)

Barcelona, 2021

Índex

Presentació

Aquestes darreres dècades el terme postveritat (Steve Tesich, 1992, Guerra del Golf) s'ha popularitzat força i alhora ha obert un encès debat sobre que entenem per "veritat", aspecte aquest que els pensadors postmoderns, entre molts d'altres temes, ja havien iniciat amb anterioritat.

Postveritat, com a concepte que implica que s'ha superat la "veritat" i que ja no es pot discernir entre la validesa d una afirmació basada en el pensament racional, com el mètode científic, front d'una altra basada en les emocions i creences personals, comporta un desprestigi dels arguments que es recolzen en una "realitat objectiva", i legitima que son les persones que opinen, en funció de la seva pròpia visió i interessos, les que defineixen les veritats dels fets. Com ja albirava i diu la locució llatina *Mundus vult decepi* (el món vol ser enganyat).

La pandèmia de la Covid-19 i les seves conseqüències sanitàries i socioeconòmiques, han estat narrades en bona part des d'una perspectiva racional i científica, però també han estat acompanyades per l'esclat de la desinformació: la generació i la distribució massiva de notícies falses, establint d'aquesta manera uns relats i contrarelats constants que poden induir fàcilment a la confusió general sobre els fets que succeeixen. Si fins no fa gaire, quan ens miràvem les xarxes socials i internet ens mostràvem preocupats per la sobreinformació i pèrdua de qualitat de continguts implícita, ara l'abrupta irrupció del SARS-CoV-2 ha estat envoltada d'un creixement exponencial de la informació falsa sobre el virus, els seus tractaments, expansió, mesures preventives i vacuna, que va afectar severament la població, però també, els periodistes i mitjans de comunicació i la classe política.

La persistència de l'entorn pandèmic, i l'elevada dependència ciutadana de xarxes socials i apps de missatgeria massives, ha fet que enquestes molt diverses mostrin, percentatges socials alts, fregant o superiors al 50% segons països, de persones que es consideren seriosament afectades per les notícies falses i, en especial per les relacionades amb aquesta malaltia. La desconfiança s'estén de les xarxes socials a Internet, on els percentatge de ciutadans que desconfien de la veracitat de la informació que hi troben via web és encara més elevat. Paradoxalment, l'ús dels mitjans web i xarxes socials per a informar-se, s'ha generalitzat en detriment de la televisió i els mitjans tradicionals, configurant un bucle socioinformatiu de difícil gestió.

Davant d'això, no tan sols els i les periodistes i disseminadors tenen un repte, sinó també els acadèmics i els legisladors, per a formar noves generacions preparades per enfrontar-se a les notícies falses i ensenyar l'actual població a saber distingir informació d'opinió, discernir sobre la fiabilitat de les diverses fonts que emeten informació i construir una arquitectura legislativa que protegeixi millor la societat front a la infoxicació massiva.

De fet, cadascú de nosaltres té un paper rellevant a jugar en el desafiament que significa aprendre a ser veraços, no deixar-nos enganyar i a detectar les notícies falses. Ajudar en aquesta tasca, no menor, tant a la societat en general com els preceptors i organitzacions del sector de la recerca potencialment afectades per la desinformació, la informació errònia o la maliciosa, és l'objectiu d'aquest informe que us posa a mans la Fundació Catalana per a la Recerca i la Innovació (FCRI), seguint el seu objectiu de proporcionar al nostre país una disseminació i comunicació científica de qualitat.

Esperem us sigui d'utilitat i generi el vostre interès i complicitat davant aquests grans reptes.

Jordi Portabella
Fundació Catalana per a la Recerca i la Innovació
Director general

Desinformació a Catalunya: com ens afecta i com hi lluitem

La desinformació, i fins i tot la informació errònia i la mala informació, no són fenòmens recents, tot i que en els darrers anys han experimentat una viralitat i un impacte social que preocupen els poders públics i la societat. Tant els polítics com la ciutadania han pres consciència de la necessitat de combatre aquests desordres informatius que poden tenir —i estan tenint— conseqüències per a la salut, la democràcia, l'economia i altres àmbits.

La desinformació, que ha estat una constant en la propaganda política durant la Segona Guerra Mundial i altres conflictes (Posetti, Matthews, 2018), ha viscut una expansió a partir del Brexit i les eleccions dels EUA de 2016 (CAC, 2018; Vosoughi, Roy, Aral, 2018). Però també s'ha accelerat a partir d'altres esdeveniments posteriors, com ara el referèndum de l'1-O a Catalunya el 2017, la pandèmia de la covid-19 i les diverses cites electorals dels darrers anys.

Les xifres no conviden a l'optimisme. Ja a la fi de 2017, la consultora Gartner, en el seu informe sobre tendències tecnològiques per al 2018, preveia que el 2022, consumirem més informació falsa que verídica (Gartner, 2017). Un informe més recent subratlla que el 2020, un total de 81 països van emprar les xarxes socials per estendre desinformació sobre política, una xifra que representa un creixement important respecte l'any anterior, on aquesta activitat de *cyber troop* es va identificar a 70 països (Bradshaw, Hailey i Howard, 2021).

No només preocupa el creixement que la desinformació i els altres desordres informatius estan experimentant, sinó també i sobretot les conseqüències que aquesta contaminació de l'ecosistema informatiu pugui tenir en la democràcia, la salut (física i mental; individual i pública), la ciència, l'economia i altres àmbits. La Comissió Europea, n'alertava el 2018, en un informe en què subratllava que la desinformació "erosiona la confiança en les institucions i en els mitjans digitals i tradicionals i fa mal a les nostres democràcies, tot obstaculitzant l'habilitat dels ciutadans per prendre decisions informades" (Comissió Europea, 2018:1). La preocupació ciutadana al voltant de la desinformació se situa en xifres destacables. Segons el Digital News Report de 2021, un 67% dels usuaris de l'Estat Espanyol es mostra preocupat per la desinformació, una xifra molt superior al 58% de mitjana entre els 46 països que analitza l'estudi (Newman et al., 2021).

Les mentides del segle XXI: una diagnosi

Tenir una visió acurada i actualitzada de les característiques i les formes de la desinformació resulta clau fer-hi front de manera eficient, coordinada i constant. Pel que fa a les plataformes, tot i que la desinformació i la resta de desordres informatius s'estenen per tots els espais (Twitter, Facebook, Tik-tok, Instagram, etc.), existeix consens en el fet d'assenyalar WhatsApp com una de les plataformes en què la desinformació es viralitza més (Magallón, Sánchez-Duarte, 2020). Això malgrat els esforços de la plataforma per posar-hi fre. Aquesta preponderància de WhatsApp en la desinformació es pot explicar no només per la dificultat de rastrejar l'inici de la falsedat, sinó també perquè funciona amb la nostra agenda telefònica, és a dir, amb l'entorn més pròxim format per familiars i amistats i, per tant, s'evidencia així la importància del component emocional i interpersonal de la desinformació. De vegades, les fonts de confiança o amb qui tenim un lligam afectiu es confonen amb fonts confiables.

Respecte a la temàtica de la desinformació, cal destacar que les falsedats sobre salut i política han estat les més habituals darrerament. Segons el *Digital News Report 2021*, un 60% dels enquestats a Espanya assegura que ha trobat desinformació relacionada amb la covid-19, una xifra que no dista molt dels qui asseguren que n'han trobat sobre política, que se situa en el 51%. Més enllà del record o la percepció ciutadana, diversos estudis assenyalen que en la desinformació sobre la covid-19 també predomina aquella que té un caràcter polític, és a dir, destaquen les informacions en què les falsedats estan relacionades amb les mesures polítiques adoptades pels diferents governs o les declaracions d'institucions com l'OMS (Brennen et al. 2020; Salaverría et al. 2020).

Els formats, les fonts de la desinformació i la vulnerabilitat a aquests desordres constitueixen altres aspectes d'interès. Pel que fa als formats, hi ha consens en què el majoritari és la veritat a mitges, també anomenat contingut enganyós o "reconfiguració" (Brennen et al. 2020). Sobre les fonts d'informació, pel que fa a la desinformació relacionada amb la ciència i la salut, destaca la preponderància de les fonts suplantades i anònimes (Salaverría et al. 2020). La ciutadania té la percepció que qui més desinforma són els polítics. Segons el *Digital News Report 2021*, un 42% dels enquestats espanyols confessa preocupació per la desinformació procedent dels polítics i dels partits polítics, una xifra que s'allunya del 29% de la mitjana de l'estudi i que reflecteix la desconfiança i la manca de credibilitat en els polítics i els partits en el cas de l'Estat Espanyol. En segon lloc, se situa la preocupació per la desinformació atribuïda als periodistes i els mitjans, que és de l'11%. Pocs, un 9% mostren preocupació per aquella desinformació distribuïda per la "gent normal i corrent", una xifra sensiblement inferior al 16% de mitjana.

Tot i que ningú és immune a la desinformació, el cert és que aquest fenomen presenta també una dimensió sociològica i no afecta tothom per igual. Hi ha més inquietud per les informacions falses entre la gent gran —un 73% dels espanyols de 65 anys i més grans s'hi mostren preocupats mentre que la xifra baixa al 56% en la franja de 18 a 24 anys (Newman et al. 2021)— i hi ha també estudis que asseguren que les persones majors de 65 anys comparteixen més enllaços a pàgines de notícies falses (Guess et al., 2019). Pel que fa a l'Estat Espanyol, les persones conservadores són més susceptibles a la desinformació (Roozenbeek et al. 2020). Altres estudis relacionen un baix nivell educatiu i econòmic, així com un malestar emocional amb una major vulnerabilitat per tal de creure's les teories conspiranoiques (Goertzel, 1994; van Prooijen et al. 2018; Freeman et al. 2020).

Verificació digital contra la desinformació

La verificació digital i els verificadors viuen un moment d'efervescència i expansió. La International Fact-Checking Network, que, des de 2015, agrupa els verificadors més rellevants a escala internacional, compta ja amb més de 80 membres que s'han adherit al seu Codi de Principis, uns compromisos ètics de bones pràctiques. Catalunya participa d'aquesta tendència internacional i compta amb diverses iniciatives que treballen per contrastar les informacions falses de les xarxes socials i del discurs polític, entre les quals, destaquen els projectes de *fact-checking* "Verificat", "Fets o Fakes" de Catalunya Ràdio i també altres iniciatives com ara seccions de reflexió a diferents mitjans de comunicació com ara El món a *RAC 1* o al programa *Aquí, amb Josep Cuní,* de la Cadena SER, entre d'altres.

"Verificat" va néixer a principis de 2019 per tal de contrastar la informació al voltant dels comicis municipals de Barcelona. Es tracta d'un *fact-checker* català, membre de l'IFCN, constituït com una associació sense ànim de lucre i amb fonts provinents majoritàriament de l'Open Society Foundations. Amb un equip creixent, que en l'actualitat se situa al voltant de la desena de persones, "Verificat" va fer durant el primer trimestre de 2021 un total de 120 verificacions. A aquesta tasca de fact-checking, cal sumar l'activitat educativa a través d'un programa educatiu a l'Escola Llor de Sant Boi de Llobregat. Cal destacar la seva aliança amb Newtral per tal de verificar les eleccions catalanes del 14 de febrer i també les sinergies encetades amb El Periódico de Catalunya per tal d'ampliar el públic a què arriben les seves verificacions. En els darrers mesos, aquest verificador català ha impulsat dos projectes dignes d'esment: "Les mentides alimenten l'odi", encarregat per la Secretaria d'Igualtat, Migracions i Ciutadania del Departament de Treball, Afers Socials i Família de la Generalitat de Catalunya per tal de contrastar mites relatius a la immigració; i les verificacions sobre la covid-19 finançades amb una beca de Google i pel qual compten amb la col·laboració de l'Institut de Salut Global de Barcelona, la comunitat catòlica Aleteia i l'Observatori Blanquerna de Comunicació, Religió i Cultura.

"Fets o Fakes" és una iniciativa de verificació impulsada per un equip de periodistes dels informatius de Catalunya Ràdio i que té un espai fix en l'antena de l'emissora al programa informatiu Catalunya migdia. També va iniciar la seva activitat l'any 2019 i, tot i que no forma part de la IFCN, aplica el seu codi de principis a l'hora de treballar la verificació de la informació. Aquest 2021, "Fets o fakes" s'enfronta a un procés de consolidació. Ambiciona esdevenir un equip estable i passar de ser un projecte circumscrit a Catalunya Ràdio a ser-ho de tota la Corporació Catalana de Mitjans Audiovisuals. A aquestes dues iniciatives catalanes, se sumen, a l'àmbit de l'Estat Espanyol, els verificadors Newtral, Maldita, EFE Verifica i també RTVE Verifica.

Ciència en temps de pandèmia de desinformació

La ciència i la recerca són dos camps en què es combat la desinformació, tant amb verificació digital com amb divulgació de coneixement científic per tal de prevenir els enganys. Les iniciatives específiques relacionades amb la verificació científica són prèvies a la pandèmia: l'any 2018 van néixer "Maldita Ciencia", iniciativa específica per verificar contingut científic dins del paraigua del verificador Maldita, i també "Salud sin Bulos", un projecte relacionat amb la verificació d'informació sobre salut creat per professionals sanitaris. El cert és, però, que la situació generada per la covid-19 ha esperonat el sorgiment de nous projectes de verificació de la informació sobre salut, i, en especial de tot allò relacionat amb el virus.

A més del projecte específic de "Verificat", destaquen, entre d'altres, la iniciativa de Newtral "Vacúnate contra los bulos" o el projecte "VacunaCheck" en què EFE i les farmàcies de l'Estat Espanyol intenten lluitar contra la desinformació relacionada amb la covid-19. La pandèmia, però, també la desinformació al voltant del canvi climàtic i d'altres temes científics, han posat en evidència la necessitat d'una alfabetització científica.

Des de la Fundació Catalana per a la Recerca i la Innovació, es participa en un projecte europeu sobre Media Literacy des de 2018 per a la detecció i anàlisi de les fake news i les paraciències, tot identificant i alertant d'aquelles relatives a l'àmbit de la ciència.

Amb aquest propòsit estan sorgint algunes iniciatives. Una de les més recents en l'àmbit català és "Neurones fregides", una aliança de diversos divulgadors per tal d'impulsar la divulgació de la ciència en català.

A banda del sector científic, cal remarcar l'interès i la contribució d'altres actors per tal de minimitzar els desordres informatius —la desinformació, però també la informació maliciosa. Destaquen, entre d'altres, la iniciativa #PacifiquemlesXarxesSocials, un projecte de FundiPau amb l'Institut Català Internacional per la Pau, i també la crida de Digital Future Society Lab, de la Mobile World Capital, per tal de trobar solucions tecnològiques que ajudin i empoderin la ciutadania davant la desinformació.

Alfabetització digital per empoderar la ciutadania

L'educació mediàtica en verificació digital resulta clau per tal d'empoderar la ciutadania en la societat de la desinformació en què vivim. Es tracta d'educar els joves en particular i la ciutadania en general per tal que puguin accedir, analitzar, avaluar, crear i actuar amb les diverses formes i mitjans de comunicació. A Catalunya treballen en aquesta línia iniciatives com ara el programa eduCAC (educac.cat), promogut pel Consell de l'Audiovisual de Catalunya (CAC); el programa "Premsa a les escoles", del Col·legi de Periodistes de Catalunya amb el suport de l'Obra Social "la Caixa"; "Júnior Report", una iniciativa de caràcter empresarial; o el projecte "Learn to Check", nascut l'any 2020 a partir del treball de diverses periodistes i amb el suport del Consolat dels EUA a Catalunya.

L'FCRI organitza un curs d'estiu sobre alfabetització digital especialment adreçat a professorat d'educació secundària perquè contribueixi, des de l'àmbit escolar, a la formació de ciutadania responsable i amb capacitat crítica.

El programa eduCAC es va posar en marxa el 2017 amb la voluntat d'oferir recursos didàctics a professorat i famílies per tal de reflexionar i apostar per l'educació en comunicació. La desinformació s'aborda en una de les moltes unitats didàctiques que s'inclouen a la seva web i que es poden obtenir amb registre previ. A banda d'aquest recurs, el CAC també ha implementat altres línies de treball al voltant de la desinformació. El 2019 s'aprova la creació de la Plataforma per a l'Educació Mediàtica de Catalunya que agrupa entitats, experts i expertes i altres actors que treballen al voltant de l'educació mediàtica. A més, ha elaborat informes sobre el negacionisme, els productes que suposadament curen la covid-19 i continguts falsos sobre la vacunació; també ha elaborat recomanacions conjuntes amb el departament de Salut, el Consell del Col·legi de Metges de Catalunya i el Col·legi de Periodistes de Catalunya sobre la desinformació.

Pel que fa al Col·legi de Periodistes, cal assenyalar que treballa la desinformació i l'educació en verificació digital com un dels temes que s'aborden als tallers de "Premsa a les escoles" que es van engegar l'any 2009 amb el suport de l'Obra Social "la Caixa" i que l'any 2019 van arribar a uns 3.600 alumnes de tot Catalunya. També treballen en el camp de l'educació mediàtica "Junior Report", una iniciativa que es proposa acostar l'actualitat al jovent i que se situa sota el paraigua de l'empresa Blue Globe Media SL, i Learn to Check. Aquesta darrera iniciativa, nascuda el setembre de 2020, és un projecte educatiu i divulgatiu per tal de reflexionar sobre la desinformació i acostar la verificació digital a la ciutadania. "Learn to Check" inclou una web en obert en català, castellà i anglès amb recursos per tal d'aprendre a verificar i també tallers per a joves, docents, periodistes, bibliotecàries, famílies i altres públics. Té com a objectiu promoure el pensament crític i empoderar la ciutadania.

Nota metodològica i recomanacions

El consum d'informació en el món actual, s'ha incrementat exponencialment els darrers anys, amb l'eclosió de les xarxes socials i la facilitat per elaborar, publicar i transmetre continguts.

Podem accedir a tot tipus d'informació, pel que fa a formats, orientació o procedència, sense cap filtre que ens permeti identificar quins corresponen a continguts veraços i quins corresponen a continguts poc confiables, inexactes o malintencionats. Aquesta situació es veu reforçada pel fet que els mateixos algoritmes que hi ha darrera de les aplicacions que gestionen les xarxes socials, tendeixen a mostrar-nos com a rellevants simplement aquells resultats més "populars": aquells que marquen tendència, per ser els més compartits o els que generen més resposta. No acostuma a haver-hi una correlació entre la rellevància d'aquests resultats i la qualitat i el grau de certesa de la informació que contenen, i sovint els usuaris no tenen el grau d'alfabetització digital necessari per a investigar, analitzar i contrastar la veracitat de tota aquesta informació ni disposen d'eines de suport que els facilitin aquesta tasca. El resultat és el que s'anomena desinformació, és a dir, l'aparició de notícies enganyoses, provocades per una suma de factors com ara la sobreabundància de dades, l'anonimat dels continguts, l'accés sense control a les xarxes, i la manca de regulació per publicar a Internet.

Aquest document vol introduir al lector en el concepte de *desinformació* i familiaritzar-lo amb els 10 principals tipus de desinformació que acostumem a trobar en les xarxes socials. L'informe, generat en un primer moment com una eina d'ús pràctic per al professorat d'ensenyament secundari, dins del marc del projecte MediaLiteracy,[1] finançat per la Comissió Europea, s'obre ara al conjunt de la ciutadania, i molt especialment a totes aquelles persones interessades a prendre consciència de l'existència i les formes de transmissió de les notícies falses o enganyoses en un entorn tan incert com les xarxes socials.

En primer lloc, cal comentar que a nivell conceptual, la terminologia sobre les notícies falses o enganyoses, varia segons els diferents actors que les utilitzen. En aquest informe s'ha optat per utilitzar els termes informació errònia, desinformació i malinformació, en funció de la intencionalitat que hi ha darrera de cada notícia enganyosa, la definició dels quals seria la que mostra el següent quadre:

	Informació errònia	Informació falsa que es difon sense la intenció de fer mal
	Malinformació	Informació vertadera que es difon per fer mal
	Desinformació	Informació falsa que es difon per fer mal

[1] Media Literacy for All, 2018

La selecció dels tipus de desinformació presents a les xarxes socials es va fer mitjançant procés acurat i exhaustiu en el qual 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, un grup d'experts, mitjançant activitats de catalogació i triatge, van preseleccionar 15 tipus de desinformació sobre els quals seguir treballant. En el darrer pas, tenint en compte que els joves són el col·lectiu que fa un major ús de les xarxes socials i, per tant, els que més sovint es troben amb informacions intencionadament falses o enganyoses, en un procés de co-creació, es van recollir aportacions de docents i alumnat de secundària. Les seves contribucions van ajudar a reduir la llista fins a deixar-la en els 10 tipus de desinformació més usats a les xarxes socials.

Tota la informació es presenta en format fitxa per a facilitar-ne l'ús. Cada fitxa està estructurada en 6 apartats que abracen continguts essencials relacionats amb el tipus concret de desinformació, des de la descripció i funcionament de cada tipus de desinformació fins al perfil d'aquells que els usen, el nivell d'engany que comporta, clarament lligat amb el grau de perillositat que representa, o el mètode de comprovació, en cas de dubte, sempre complementats amb informació addicional que fan encara més entenedor el concepte explicat. A més, les fitxes inclouen l'accés a un conjunt de vídeos elaborats per l'FCRI, en què s'explica, de forma molt visual, amb exemples reals i utilitzant un llenguatge per a joves, els diferents tipus de desinformació.[2]

Finalment s'ofereixen un seguit de recomanacions per als usuaris de xarxes socials que vulguin contribuir a no difondre informació falsa o pensada per fer mal, així com algunes propostes que excedeixen l'acció individual.

[2] Media Literacy - Check or Cheat https://www.youtube.com/playlist?list=PLxyLc6Orw5S2aKz9y5ORJsovYHvjmhVoD

Recomanacions

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. De vegades, encara que el titular no sigui fals, pot ser enganyós o pot no donar tota la informació. Cal context i més dades per interpretar. Llegeix la peça, reflexiona sobre qui ha emès aquella informació, de quines fonts beu, si hi ha o no errors en el contingut o si la informació és incompleta o esbiaixada.

2. Comprova l'autoria. Analitza si la informació s'està publicant en un mitjà de comunicació fiable o bé en una pàgina web que difon teories de la conspiració. Estudia si aquella publicació que no et sembla fiable és un mitjà de comunicació satíric. Cal veure qui n'és l'autor/ra i on es publica. Si la informació es publica en un mitjà no creïble o no confiable, espereu-vos abans de difondre la història o el vídeo.

3. Examina si estàs davant d'un contingut nou. 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. També pot ser molt útil fer una cerca inversa d'imatges amb eines com ara TinEye, Google Imatges o Yandex. De vegades circulen fotografies i vídeos que són antics; és l'anomenada desinformació per context fals.

4. Analitza les evidències. És clau accedir a la informació primària d'on s'ha extret i elaborat la informació. Hi ha evidències? Hi ha dades? Ens donen enllaços? Tenim proves d'aquell fet o d'aquella dada? Cal contrastar la informació amb les evidències.

5. Si sospites, no comparteixis. 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. No compartir informació no contrastada és un comportament responsable i ètic a xarxes socials.

6. Ajuda't dels verificadors. Si tens dubtes, pots consultar les verificacions publicades per verificadors com ara Verificat, Fets o fakes, Maldita, Newtral, RTVE Verifica o EFE Verifica. La majoria també contrasten rumors i continguts sota demanda. Pots demanar feina periodística a aquests professionals.

7. Aposta pel periodisme de qualitat. Estar ben informat/da ajuda a prevenir la desinformació. Si tenim informació prèvia, podem reconèixer ràpidament alguns enganys que ens arriben, estarem millor preparats/des per no caure en els paranys de la desinformació.

8. Demanda transparència. Cal exigir transparència a les institucions públiques, als partits polítics, a les empreses i a altres actors. Amb les evidències posades a l'abast del públic, contrastar i defensar-nos de la desinformació esdevé més fàcil.

9. Actua de forma responsable. La desinformació exigeix una acció coordinada, eficaç i duradora. Com a ciutadans/nes, podem demanar als partits polítics que no desinformen; a les xarxes socials, que no fomentin la polarització i l'odi amb uns algoritmes més ètics; a l'escola, que incorpori l'educació en comunicació i les competències digitals i, com a mares i pares, també podem fomentar valors ètics i responsables en les nostres creacions a xarxes socials.

Fitxes

Hipertrucatge (*Deepfake*)

Qui ho pot fer: aficionat

Actualment existeixen aplicacions[3] que els usuaris es poden descarregar per començar a experimentar. No obstant això, l'avenç de la tecnologia és incontrolable i, en un futur proper, es preveu que qualsevol podria fer-ho.[4]

Grau d'engany: molt alt

Si estan 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 intentar detectar-los.

En què consisteix?

L'hipertrucatge és una tecnologia basada en la Intel·ligència Artificial (IA) que s'usa per crear o alterar el contingut d'un vídeo mitjançant la modificació de les cares (intercanvi de cares o creació de noves expressions facials). 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.

Orígens.

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.

Com funciona?

L'hipertrucatge de vídeo s'aconsegueix mitjançant l'ús de dos sistemes d'IA 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 s'ha de 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. [5]

Com detectar-ho?

Si l'hipertrucatge no és professional, és fàcil veure que les ombres no quadren o que la persona no parpelleja. 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.[6] L'exèrcit nord-americà també està finançant un projecte per descobrir-los. [7]

Per saber-ne més:

Clark, Adam. (2017). "Insanely Accurate Lip Synching Tech Could Turn Fake News Videos Into a Real Problem", Gizmodo, [en línia]. [Consulta: 26 maig 2021]. Disponible a: <https://gizmodo.com/insanely-accurate-lip-synching-tech-could-turn-fake-new-1796843610>.

Supasorn Suwajanakorn, Steven M. Seitz, Ira Kemelmacher-Shlizerma. (2017) Teaser - Synthesizing Obama: Learning Lip Sync from Audio [en línia]. [Consulta: 26 maig 2021]. Disponible a: <https://youtu.be/MVBe6_o4cMI>.

The Fakening (2018) Canal de Youtube [en línia]. [Consulta: 26 maig 2021]. Disponible a: <https://www.youtube.com/c/TheFakening/videos>.

FCRI (2021) Hipertrucatge (*Deep fake*) [en línia]. [Consulta: 27 maig 2021].
Disponible a: <https://youtu.be/rjjINA-2lY8>.

[3] https://www.malavida.com/en/soft/fakeapp/#gref
[4] https://www.theverge.com/2019/6/10/18659432/deepfake-ai-fakes-tech-edit-video-by-typing-new-words
[5] https://whatis.techtarget.com/definition/deepfake
[6] https://techcrunch.com/2020/09/14/sentinel-loads-up-with-1-35m-in-the-deepfake-detection-arms-race
[7] https://www.technologyreview.com/s/611146/the-us-military-is-funding-an-effort-to-catch-deepfakes-and-other-ai-trickery

Pseudociència (*Pseudoscience*)

Qui ho pot fer: qualsevol 

La pseudociència és molt fàcil de difondre i no requereix cap tipus d'habilitat. Però l'elaboració de teories pseudocientífiques resulta molt més complexa del que podríem esperar.

Grau d'engany: alt 

Els promotors de la pseudociència sovint adopten el vocabulari de la ciència: descriuen conjectures en forma d'hipòtesis,[8] teories[9] o lleis científiques;[10] aporten "evidències" fruit de l'observació i testimonis "d'experts";[12] 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.

En què consisteix?

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

La pseudociència consta d'afirmacions, creences o pràctiques declarades científiques i objectives, però que són incompatibles amb el mètode científic. Sovint es caracteritza per afirmacions contradictòries, exagerades o no refutables;[13] per la dependència del biaix de confirmació[14] 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 la seva persistència molt temps després d'haver-se desacreditat experimentalment les seves hipòtesis.

Com funciona?

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.[15] 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. Concretament, en medicina, existeix el terme *xarlatanisme* [16] per a referir-se a aquells que promouen tractaments sense una base científica sòlida (pseudociència). Per exemple, podrien afirmar que un tractament concret "elimina les toxines de l'organisme", sense concretar de *quines toxines es parla*, com s'eliminen o com es pot saber si s'han eliminat.

[8] https://rationalwiki.org/wiki/Hypothesis
[9] https://rationalwiki.org/wiki/Scientific_theory
[10] https://rationalwiki.org/wiki/Scientific_law
[11] https://rationalwiki.org/wiki/Anecdotal_evidence
[12] https://rationalwiki.org/wiki/Expert_for_hire
[13] https://en.wikipedia.org/wiki/Falsifiability
[14] https://en.wikipedia.org/wiki/Confirmation_bias
[15] https://rationalwiki.org/wiki/Argument_by_assertion
[16] https://rationalwiki.org/wiki/Quackercy

Com detectar-ho:

La manera més senzilla de distingir el mètode pseudocientífic del mètode 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.

La següent taula[17] mostra 7 diferències entre ciència i pseudociència que ens poden ajudar a distingir-les:

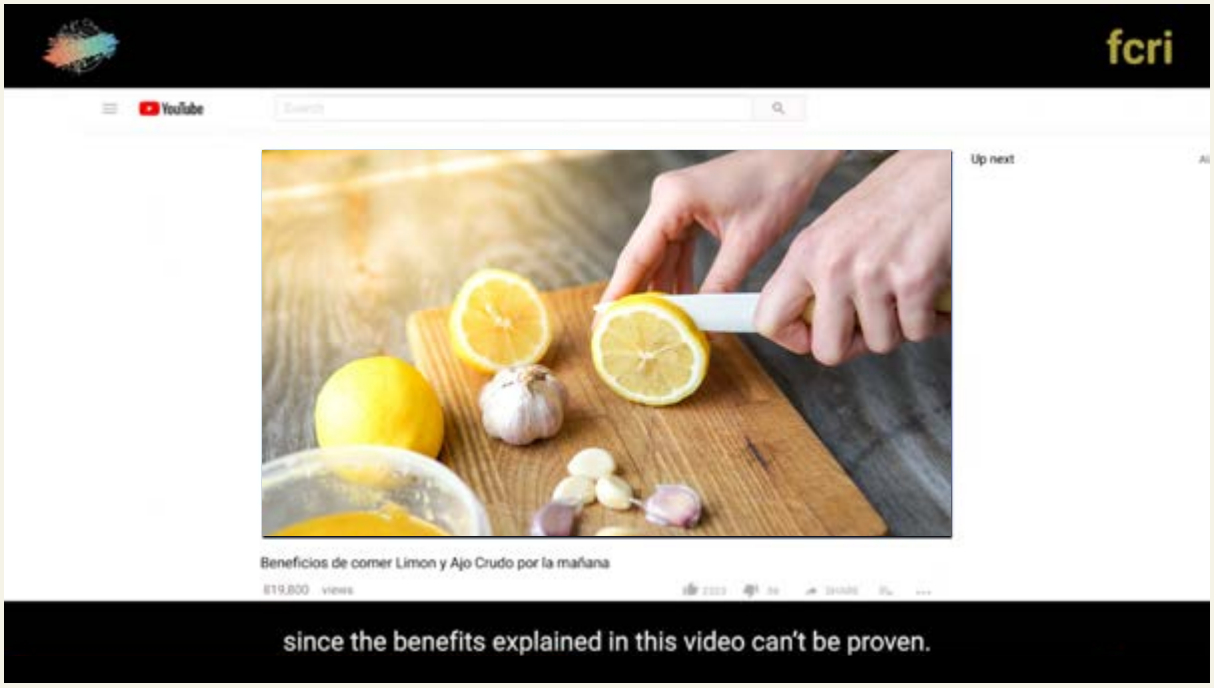
CIÈNCIA	PSEUDOCIÈNCIA
L'objectiu principal és aconseguir conèixer el món físic d'una manera més completa i unificada.	Tenen més probabilitats de ser impulsades per objectius ideològics, culturals o comercials (com p. e.: l'astrologia, provinent de la cultura babilònica antiga; la ufologia, cultura popular i desconfiança en el govern); o la ciència de la creació, és a dir, l'intent de justificar una interpretació literal de la Bíblia).
La major part dels camps científics són objecte d'una investigació exhaustiva que dona lloc una contínua expansió i evolució del coneixement en la disciplina.	El camp ha evolucionat molt poc des que es va establir per primera vegada. Generalment, la petita quantitat de recerca i experimentació que es duu a terme es fa més per justificar la creença que per ampliar-la.
Les ciències avancen incorporant la nova informació que s'obté. S'acostumen a buscar contraexemples o descobriments que semblin incompatibles amb les teories acceptades, per tal de confrontar-les.	El qüestionament d'un dogma acceptat sovint es considera un acte hostil, o fins i tot heretgia, i porta a controvèrsies rancoroses o 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 activament ocultades.
Cada principi ha de ser testejat i provat, i tot i així pot ser qüestionat o rebutjat en qualsevol moment.	Els principis fonamentals no solen ser falsables i és poc probable que es modifiquin o que es demostri que són equivocats, sense que això demostri la seva validesa.
Les idees i els conceptes científics es fan valer per ells mateixos, sobre la base del coneixement i l'evidència existents.	Els conceptes solen estar determinats per egos i personalitats individuals, gairebé sempre per persones que no estan en contacte amb el corrent dominant de la ciència. S'acostuma a recórrer a autoritats (personatge famós, per exemple) per guanyar suport.
Les explicacions es manifesten en termes clars i sense ambigüitats.	Les explicacions tenen tendència a ser vagues i ambigües, i sovint fan servir termes científics en contextos discutibles.

Per saber-ne més:

Crash Course (2016) *Karl Popper, Science, & Pseudoscience: Crash Course Philosophy, 8*. [en línia]. [Consulta: 26 maig 2021].
Disponible a: <https://youtu.be/-X8Xfl0JdTQ>.

"Examples of Pseudoscience in Different Fields". A: *YourDictionary.com* [en línia]. LoveToKnow, 2020. [Consulta: 26 Maig 2021].
Disponible a: <https://examples.yourdictionary.com/examples-of-pseudoscience.html>.

"List of pseudosciences". A: *RationalWiki* [en línia]. RationalMedia Foundation, 2021. [Consulta: 26 Maig 2021].
Disponible a: <https://rationalwiki.org/wiki/List_of_pseudosciences>



FCRI (2021) Pseudociència (*Pseudoscience*) [en línia]. [Consulta: 27 maig 2021]. Disponible a: <https://youtu.be/0p5Mnh7gzdw>.

[17] http://www.chem1.com/acad/sci/pseudosci.html

Contingut manipulat (*Manipulated content*)

Qui ho pot fer: 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 ara 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: alt 

La identitat cada vegada és més difícil de verificar, 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 plataformes socials cada cop estan sent més vigilades i pressionades perquè 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.

En què consisteix?

Es parla de "contingut manipulat" quan s'altera part d'un contingut autèntic, molt sovint fotografies o vídeos. Els suports visuals es poden transformar[18] mitjançant la manipulació fotogràfica, sovint anomenada "fotoparament" (*photoshopping*). La manipulació de vídeo té com a diana d'actuació el vídeo digital[19] i combina tècniques tradicionals de tractament[20] i edició de vídeos[21] amb mètodes auxiliars d'intel·ligència artificial[22] com ara el reconeixement facial.[23]

Com funciona?

Les noves tècniques per modificar imatges, àudio i vídeo permeten la creació de contingut manipulat. El fotoparament 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 orientats a la manipulació massiva[24] i a la propaganda,[25] una extensió clara de les possibilitats tradicionals de la manipulació fotogràfica.[26]

Com detectar-ho?

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/.

[18] https://en.wikipedia.org/wiki/Image_editing
[19] https://en.wikipedia.org/wiki/Digital_video
[20] https://en.wikipedia.org/wiki/Video_processing
[21] https://en.wikipedia.org/wiki/Video_editing
[22] https://en.wikipedia.org/wiki/Artificial_intelligence
[23] https://en.wikipedia.org/wiki/Face_recognition
[24] https://en.wikipedia.org/wiki/Crowd_manipulation
[25] https://en.wikipedia.org/wiki/Propaganda
[26] https://en.wikipedia.org/wiki/Photo_manipulation

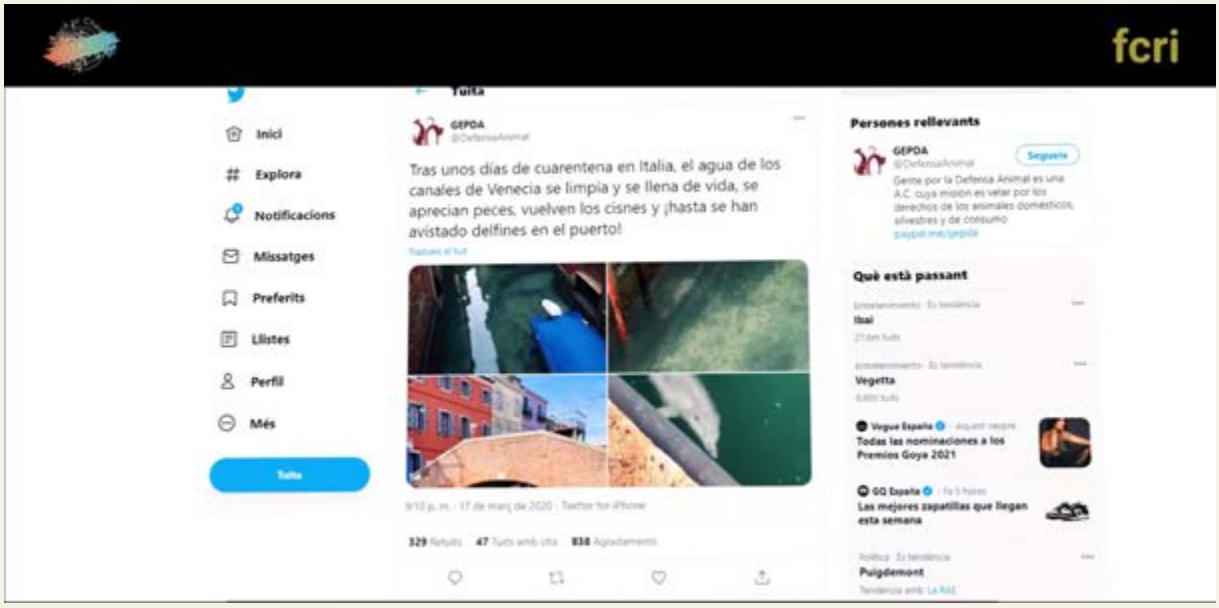
Per saber-ne més:

"Conspiracy Theories". A: *Wired* [en línia] Condé Nast, 2020. [Consulta: 26 maig 2021]. Disponible a: <https://www.wired.com/tag/conspiracy-theories/page/1/>.

Dale, Daniel. "Fact check: A guide to 9 conspiracy theories Trump is currently pushing". A: CNN [en línia]. Cable News Network, 2020 [Consulta: 26 maig 2021]. Disponible a: <https://edition.cnn.com/2020/09/02/politics/fact-check-trump-conspiracy-theories-biden-covid-thugs-plane/index.html>.

Dawson, Shane. (2018) *Mind blowing conspiracy theories* [en línia]. [Consulta: 26 maig 2021]. Disponible a: <https://youtu.be/_53cGxAUuDk>.

Holmes, Aaron. "We fact-checked 5 popular conspiracy theories about tech companies, from Apple making iPhones obsolete to Facebook secretly activating your microphone". A: *Business Insider* [en línia] Insider Inc, 2019. [Consulta: 26 maig 2021]. Disponible a: <https://www.businessinsider.com/facebook-microphone-listening-for-ads-other-tech-conspiracy-theories-explained-2019-9>.



FCRI (2021) Contingut manipulat (*Manipulated content*) [en línia]. [Consulta: 27 maig 2021]. Disponible a: <https://youtu.be/efjbbSkWl20>.

Teoria de la conspiració (ciència marginal)

Qui ho pot fer: professional

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

Grau d'engany: 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.

En què consisteix?

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. Tanmateix, 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 teories 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.

Com funciona?

Les teories de la conspiració tenen una àmplia presència al web[27] en forma de blocs[28] i vídeos de YouTube,[29] així com a les xarxes socials.[30]

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.

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, l'ocultació de certes tecnologies i el terrorisme de "bandera falsa"[31] (incriminar algú altre).

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

Algun exemples:

- 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 l'afirmació que no havia arribat a passar?
- Altres teories de la conspiració molt conegudes són: 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.
- També són populars nombroses teories sobre suposats complots de dominació mundial per part de diversos grups tant reals com imaginaris.

Com detectar-ho:

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

NATURALEZA 20-06-2019

'Chemtrails': ¿en serio nos fumigan los aviones?

Esta es la explicación a una de las más famosas teorías conspiratorias.

Más sobre:
Actualidad, Curiosidades, Aviones y aeropuertos

No, no nos fumigan desde el aire

© Getty Images

Tiempo de lectura **5 minutos**

Por si aún queda alguien que no haya escuchado la palabra **'chemtrail'** y todo lo que conlleva su pronunciación, haremos un breve repaso.

La denominada como **teoría conspiratoria de los 'chemtrails'** (palabra que se compone de dos palabras, *chemical* y *trails*, o lo que es lo mismo, estelas químicas) se inicia en Estados Unidos, después de que su ejército del aire,

FCRI (2021) Teories de la conspiració (*Conspiracy theories*) [en línia]. [Consulta: 27 maig 2021]. Disponible a: <https://youtu.be/lrCR7d80T-w>.

[27] https://en.wikipedia.org/wiki/World_Wide_Web
[28] https://en.wikipedia.org/wiki/Blog
[29] https://en.wikipedia.org/wiki/YouTube
[30] https://en.wikipedia.org/wiki/Social_media
[31]https://en.wikipedia.org/wiki/False_flag

Llegendes urbanes (i missatges en cadena)

Qui ho pot fer: qualsevol

Tothom pot fer circular una llegenda urbana, simplement, fent afirmacions que usen paraules o contextos desconeguts. Un cas conegut és la llegenda urbana del monòxid d'hidrogen (MODH). Aquest nom químicament correcte per l'aigua, és descriu a Internet com si es tractés d'un component perillós, com en aquest exemple: "Els components atòmics del MODH es troben en una sèrie de compostos càustics, explosius i tòxics com l'àcid sulfúric, la nitroglicerina i l'alcohol etílic".[32]

Grau d'engany: mitjà

Les llegenda urbana 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, enlloc d'intentar verificar-la de manera sistemàtica.

En què consisteix?

Quan un diari o un programa informatiu de ràdio o televisió informen d'una història falsa, aquesta es coneix com una llegenda urbana. Una llegenda urbana és una falsedat articulada de manera deliberada per tal que sigui percebuda com la veritat.

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

Les notícies falses es publiquen deliberadament amb llegendes urbanes que poden servir per complir l'objectiu propagandístic[33] o desinformatiu,[34] mitjançant l'ús de les xarxes socials[35] per fer créixer el tràfic web[36] i amplificar-ne l'efecte.

D'altra banda, les llegendes urbanes són mentides que normalment provenen de la història local i la cultura popular. Sovint està integrada per històries de ficció associades a fets macabres, supersticions i altres elements narratius dissenyats per fer por.

Per últim, els missatges en cadena són mentides que intenten convèncer la persona destinatària que en faci còpies i les passi a un nombre determinat de persones (s'aplica de la mateixa manera als correus electrònics).

Com funciona?

Com s'ha dit prèviament, una llegenda urbana 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:

Llegendes urbanes amb història: una de les primeres llegendes urbanes registrades als mitjans de comunicació va ser un almanac fals[37] publicat per Jonathan Swift[38] sota el pseudònim d'Isaac Bickerstaff el 1708. Swift va predir la mort de John Partridge,[40] 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 malmesa, i el seu almanac astrològic no es va publicar durant els següents sis anys.

Llegendes urbanes modernes: els trucs publicitaris enganyosos, els fraus científics,[41] les amenaces de bomba falses[42] i les estafes[43] empresarials són exemples de llegendes urbanes o enganys.

Com detectar-ho:	A Internet podem trobar pàgines que serveixen per verificar fets. Son les anomenades *fast-checkers*, que permeten demostrar amb força rapidesa si certa informació és mentida.[44]
Per saber-ne més:	"The 14 Greatest Hoaxes of All Time". A: *Mental Floss* [en línia]. Pro Sportority, 2019. [Consulta: 26 maig 2021]. Disponible a: <https://www.mentalfloss.com/article/49674/14-greatest-hoaxes-all-time>. "List of fact-checking websites": https://en.wikipedia.org/wiki/List_of_fact-checking_websites

FCRI (2021) Boles (*Hoax*) [en línia]. [Consulta: 28 maig 2021].
Disponible a: <https://www.youtube.com/watch?v=SKtzuNixdIE>

[32] http://www.dhmo.org/facts.htm
[33] https://en.wikipedia.org/wiki/Propaganda
[34] https://en.wikipedia.org/wiki/Disinformation
[35] https://en.wikipedia.org/wiki/Social_media
[36] https://en.wikipedia.org/wiki/Web_traffic
[37] https://en.wikipedia.org/wiki/Almanac
[38] https://en.wikipedia.org/wiki/Jonathan_Swift
[39] https://en.wikipedia.org/wiki/Isaac_Bickerstaff
[40] https://en.wikipedia.org/wiki/John_Partridge_(astrologer)
[41] https://en.wikipedia.org/wiki/Scientific_fraud
[42] https://en.wikipedia.org/wiki/Bomb_threat
[43] https://en.wikipedia.org/wiki/Scam
[44] ttps://en.wikipedia.org/wiki/Fact-checking

Pescaclics (*Clickbait*)

Qui ho pot fer: aficionat

Cada vegada hi ha més llocs web que prosperen gràcies a milers de clics d'entrada al seu contingut, els anomenats pescaclics, que són vistos per molts autors com un mitjà per envair la psique humana mitjançant la confecció de titulars cridaners. De vegades, fins i tot els periodistes utilitzen aquests "titulars-esquer". Un aficionat pot produir bons pescaclics de tant en tant, però els més bons i consistents requereixen d'habilitats professionals.

Grau d'engany: alt

Els pescaclics s'han 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 explota el circuit neuronal que va evolucionar al llarg de milions d'anys. Els nostres cervells no es van dissenyar per exposar-se a la gran varietat de temptacions que trobem en aquest món hiperconnectat.

Una de les variants de pescaclics que més preocupa, són els pescaclics emocionals, els quals apel·len directament a les pors de les persones, especialment quan es relaciona amb una amenaça per a un grup social al qual es pertany. 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.

En què consisteix?

Un pescaclics és una forma de publicitat falsa que fa servir textos o imatges en miniatura enllaçats i està dissenyat per cridar l'atenció i atraure l'usuari a seguir l'enllaç i llegir, visualitzar o escoltar el contingut en línia que porta vinculat; es caracteritza per ser enganyós, generalment sensacionalista o fal·laç.[45] Els pescaclics com a efecte també es veuen, de vegades, a titulars periodístics que exageren o tracten de forma escandalosa un contingut.

En alguns casos, els pescaclics s'utilitzen senzillament per generar ingressos: com més clics, més diners es guanyen amb els anunciants. Però aquests titulars i articles també es poden usar per influir sobre un grup de persones a les xarxes socials.[46] Estan construïts per actuar sobre els biaixos preexistents[47] del grup d'interès i, així, ser compartits dins de filtres bombolla.[48]

Com funciona?

Les anomenades campanyes d'intriga[49] tenen com a objectiu explotar la "bretxa de la curiositat" i proporcionar la informació suficient per encuriosir qui llegeix webs de notícies, però no prou com per satisfer aquesta curiositat 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.

De vegades el pescaclics s'assembla més a un esquer amb trampa (en analogia amb la pesca). És a dir, llegim un titular o enllaç atractiu, 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 a un determinat anunci, una part n'esdevindran compradores.

Com detectar-ho:

Per lluitar contra els pescaclics s'han desenvolupat diferents eines i recursos: els navegadors han integrat aplicacions que detecten pescaclics, mentre que les plataformes socials on es comparteixen continguts, com ara Twitter, han actualitzat els respectius algoritmes per filtrar continguts pescaclics. Alguns grups de xarxes socials, com ara Stop Clickbait, combaten els pescaclics tot proporcionant un resum de l'article associat al pescaclics, cosa que tanca la "bretxa de la curiositat". La comunitat investigadora, per la seva banda, ha desenvolupat connectors (plug-ins) que identifiquen possibles pescaclics i notifiquen els enllaços associats, per tal d'aconseguir més avenços en el camp basats en algorismes d'aprenentatge supervisat.

Alguns consells que poden ajudar als usuaris a no caure en la trampa dels pescaclics:

1. Pensar en idees o estratègies sobre com resistir la temptació de fer clics en qualsevol titular o anunci quan el problema no estigui passant.
2. Fixar-se en els patrons de conducta que tenim i substituir-los per d'altres que evitin la navegació "per avorriment" o per "desconnectar".
3. Plantejar-se l'ús d'eines de bloqueig de llocs web. Per exemple, podem instal·lar un recurs que ens limiti l'accés a aquests llocs per evitar accedir-hi.

Per saber-ne més:

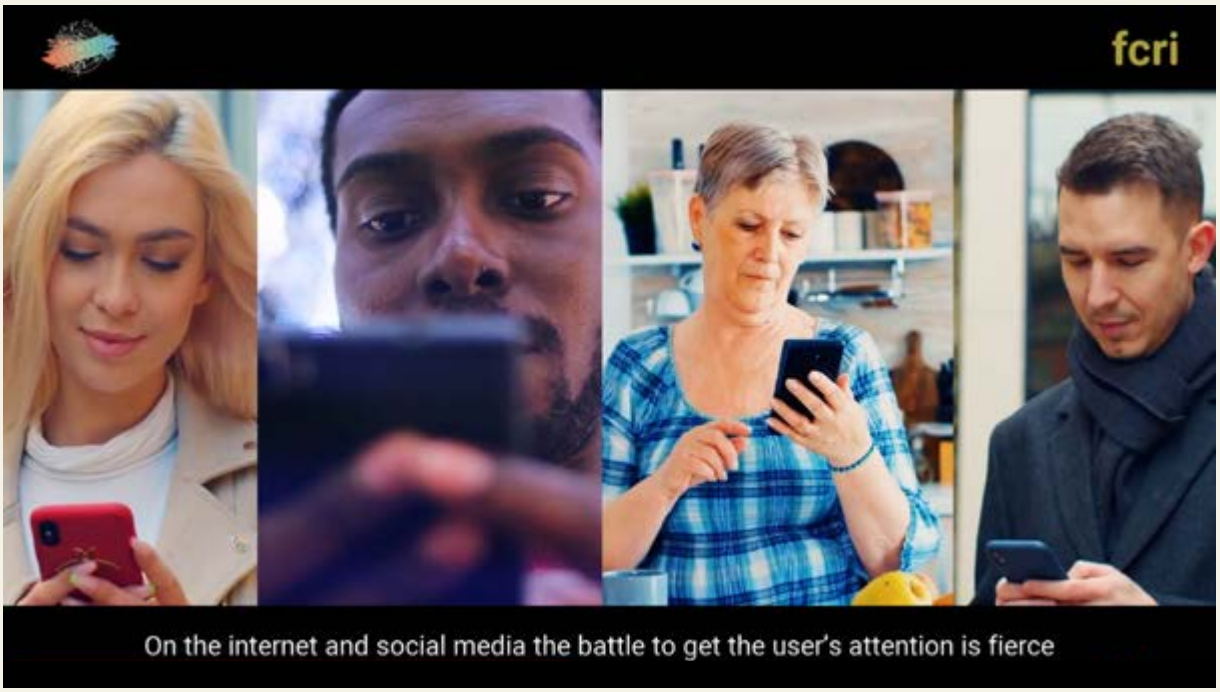
Ashuta. "You won't believe how these 9 shocking clickbaits work! (number 8 is a killer!)". A: *The Zerone Magazine* [en línia]. Medium, 2017. [Consulta: 26 maig 2021]. Disponible a: <https://medium.com/zerone-magazine/you-wont-believe-how-these-9-shocking-clickbaits-work-number-8-is-a-killer-4cb2ceded8b6>.

"Clickbait examples: Headlines and images explained". A: *Reputation X* [en línia]. Reputation X, 2021. [Consulta: 26 maig 2021]. Disponible a: <https://blog.reputationx.com/clickbait>.

Lally, Micah. "10 Clickbait Examples That Will Make You Cringe". A: *Bluleadz.com* [en línia]. Bluleadz, 2019. [Consulta: 26 maig 2021]. Disponible a: <https://www.bluleadz.com/blog/the-scientific-reasons-why-clickbait-actually-works>.

Smith, Brad. 2Clickbait Copycat: How Can You Resist Clicking these 10 Facebook Ads? (Part 2)2. A: *AdEspresso.com* [en línia]. AdEspresso, 2016. [Consulta: 26 maig 2021]. Disponible a: <https://adespresso.com/blog/clickbait-facebook-advertising-examples/>.

Techquickie (2016) *How Does Clickbait Work?* [en línia] [Consulta: 26 maig 2021]. Disponible a: <https://youtu.be/qskqM9O0FC0>.



FCRI (2021) Pescaclics (*Clickbait*) [en línia]. [Consulta: 27 maig 2021]. Disponible a: <https://youtu.be/ltj6hYK8No0>.

[45] https://www.cyber.gov.au/acsc/view-all-content/glossary/clickbait
[47] https://en.wikipedia.org/wiki/Confirmation_bias
[49] https://en.wikipedia.org/wiki/Teaser_campaign
[46] https://en.wikipedia.org/wiki/Social_media
[48] https://en.wikipedia.org/wiki/Filter_bubble

Publicitat (*Advertising*)

Qui ho pot fer: professional

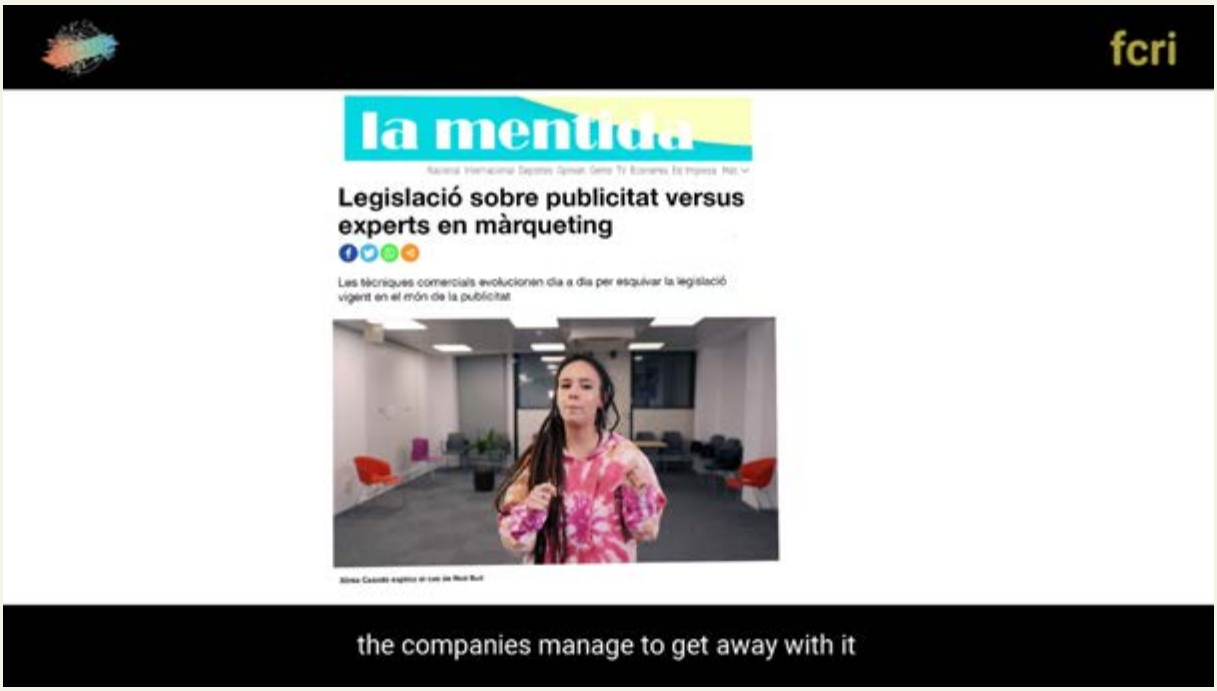
Habitualment una publicitat eficaç requereix una inversió econòmica i, sovint, l'ús de tècniques sofisticades. Són necessàries certes habilitats per crear el contingut visual o d'àudio d'un anunci. Cal tenir coneixements en els camps de la neurociència, la psicologia i l'anàlisi de dades. Però amb l'aparició d'eines de creació d'anuncis, tant gratuïtes com de pagament, i plataformes de publicitat i màrqueting comportamental per a xarxes socials, fer anuncis cada vegada és més fàcil i està més a l'abast de tothom.

Grau d'engany: mitjà

La majoria dels anuncis s'identifiquen de forma explicita, bé com a contingut patrocinat o bé perquè estan col·locats d'una manera que permet al consumidor saber que el material és publicitari. Ara bé, algunes formes de publicitat (publicitat nativa i publicitat amb influenciadors [*influencers*])[50] són més difícils de reconèixer. Fins i tot quan s'identifiquen, les informacions que presenten aquests anuncis poden ser bastant enganyoses. La normativa en matèria de publicitat limita el grau de manipulació, tot i així, existeixen diferents mètodes per provar d'enganyar els consumidors.

En què consisteix?

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 pels productes o serveis d'una empresa i convèncer-les que ho facin. A nivell digital els anuncis es poden posar gairebé a qualsevol lloc: pàgines web, correus electrònics, publicacions en línia, canals de YouTube, xarxes socials, etc.



FCRI (2021) Publicitat (*Advertising*) [en línia]. [Consulta: 27 maig 2021]. Disponible a: <https://youtu.be/AVI46PXk3bE>.

Com funciona?

La publicitat en general té com a objectiu presentar la millor faceta d'un producte, amb un cert marge de maniobra justificat pel procés creatiu. El problema sorgeix quan la dramatització creua la línia i passa a representar falsament un producte.

La publicitat pot utilitzar l'engany mitjançant la millora i manipulació fotogràfica, l'omissió d'informació, l'aplicació de càrrecs i recàrrecs ocults, la manipulació d'unitats de mesura i patrons, o l'ús d'afirmacions enganyoses sobre salut. Els anuncis també poden exagerar el valor d'un producte tot fent servir explicacions no demostrades i sense sentit, basades més en l'opinió que en els fets, i en alguns casos a través de la manipulació de dades.

Els professionals del màrqueting i els anunciants tenen molts recursos per ajudar a impulsar, persuadir i, fins i tot, influir en els hàbits de compra d'una persona. Des dels recursos clàssics com ara les dades derivades de fonts demogràfiques, geogràfiques i etnogràfiques fins a solucions més avançades com per exemple el reconeixement facial, la biometria del llenguatge corporal o el màrqueting personalitzat basat en informació psicogràfica.[51]

El **màrqueting personalitzat** és una poderosa eina publicitària que permet apuntar a grups específics de persones, o fins i tot persones, en línia. Per exemple, permet als polítics adreçar-se molt estretament a grups d'electors amb missatges personalitzats que poden manipular el debat polític. Així es com funciona: durant les campanyes polítiques es creen bases de dades sobre els votants que inclouen informació sobre 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 serveixen per a trobar els perfils d'aquestes persones a les xarxes socials i mostrar-los.[52]

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 oferir a una persona quelcom atractiu per guanyar-se-la (p. e. guanyar-ne el suport polític), i tot seguit, frustrar les seves esperances amb alguna cosa menys desitjable.[53]

El **màrqueting natiu** és l'ús d'anuncis de pagament que coincideixen amb l'aspecte, la sensació i la funció del format multimèdia en què apareixen. La paraula "natiu" fa referència a aquesta coherència del contingut amb la resta de suports que apareixen a la plataforma. Aquests anuncis que es combinen més fàcilment amb contingut digital i que són més difícils d'identificar com a anuncis.[54]

El **màrqueting mitjançant influenciadors** és un tipus de màrqueting de xarxes socials que utilitza recomanacions de persones, organitzacions i grups considerats influents o experts en una àrea determinada.[55]

La publicitat política intenta influir o comentar un afer que actualment és objecte d'un ampli debat polític.[56]

Quins són els efectes adversos de la publicitat? Existeix una preocupació generalitzada sobre els efectes que la representació del consum d'alcohol per part dels mitjans de comunicació i la publicitat de begudes alcohòliques poden tenir en el consum d'alcohol i l'aparició de problemes relacionats amb aquesta beguda entre els joves.

Com funciona?	Facebook Political Ad Collector: recurs que 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: eina que 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.
Per saber-ne més:	"Airbrushed make-up ads banned for 'misleading'". A: *BBC News* [en línia] BBC, 2011. [Consulta: 26 maig 2021]. Disponible a: <https://www.bbc.com/news/uk-14304802>. Maškarić, Nikolina. "How to Spot Native Advertising?". A: Paldesk.com [en línia] Paldesk, (n.d.). [Consulta: 26 maig 2021]. Disponible a: <https://www.bbc.com/news/technology-50726500>. Ribena-maker fined $217,500 for misleading vitamin C ads. A: *NZ Herald* [en línia] NZME Publishing Limited, 2007. [Consulta: 26 maig 2021]. Disponible a: <https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=10431119>. Shewan, Dan. "Native Advertising Examples: 5 of the Best (and Worst)". A: *The WordStream Blog* [en línia] WordStream, 2020. [Consulta: 26 maig 2021]. Disponible a: <https://www.wordstream.com/blog/ws/2014/07/07/native-advertising-examples>. Tidy. Joe; Schraer, Rachel. "General election 2019: Ads are 'indecent, dishonest and untruthful'". A: *BBC News* [en línia] BBC, 2019. [Consulta: 26 maig 2021]. Disponible a: <https://www.bbc.com/news/technology-50726500>.

[50] https://ca.wikipedia.org/wiki/Influencer
[51] https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie
[52] https://www.vox.com/recode/2019/11/27/20977988/google-facebook-political-ads-targeting-twitter-disinformation
[53] https://en.wikipedia.org/wiki/Bait-and-switch
[54] https://www.outbrain.com/native-advertising/
[55] ttps://entrepreneurship.babson.edu/what-is-influencer-marketing/
[56] https://adstandards.com.au/issues/political- publicitat electoral

Sàtira (*satire/parody*)

Qui ho pot fer: professional

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

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. Tanmateix, en nombrosos casos, fins i tot els governs, els polítics, els mitjans de comunicació o les agències de notícies són enganyats per la sàtira i la presenten com si es tractés de notícies creïbles.

En què consisteix?

La sàtira consisteix en l'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.

Com funciona?

La sàtira es caracteritza per 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 esdevé entreteniment i així pot arribar a un públic ampli. També pot protegir els seus creadors de la culpabilitat de la crítica, ja que aquesta s'insinua enlloc de declarar-se obertament; d'aquesta manera, esdevé una eina poderosa per als dissidents en períodes polítics i socials difícils o opressius. 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.[57]

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. e., 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.

Com detectar-ho:

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.

Com funciona?

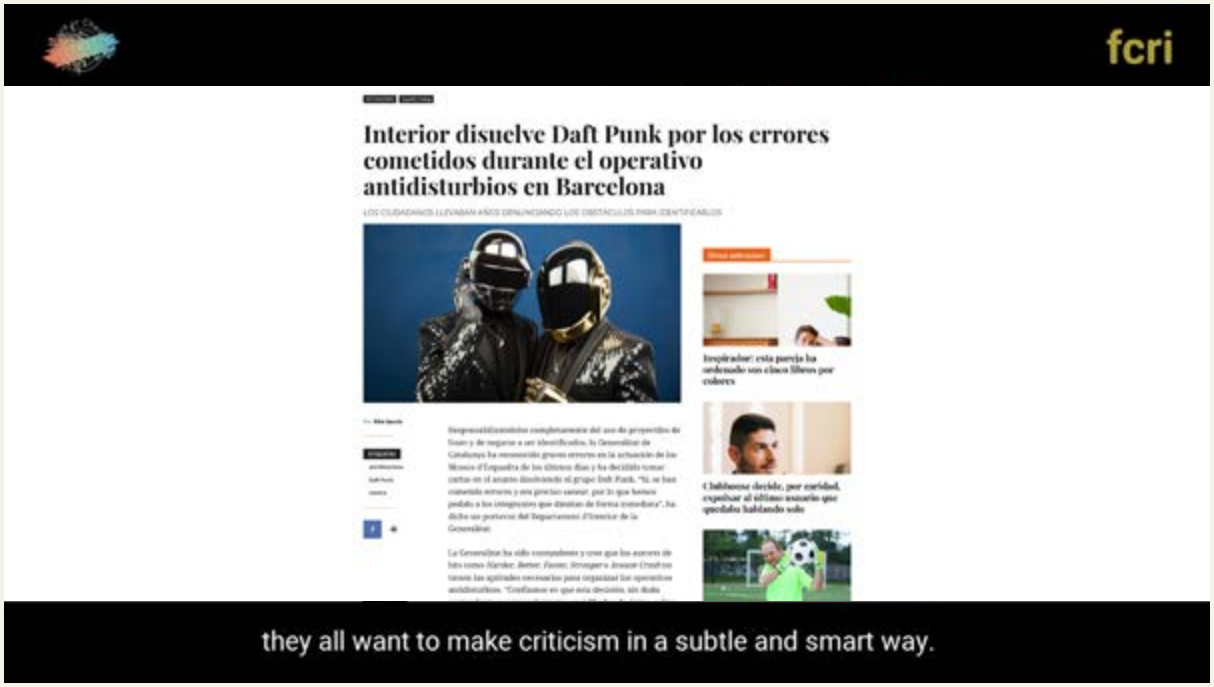
Fallon, Kevin. "Fooled by 'The Onion': 9 Most Embarrassing Fails". A: *The Daily Beast* [en línia] The Daily Beast Company, 2017. [Consulta: 26 maig 2021]. Disponible a: <https://www.thedailybeast.com/fooled-by-the-onion-9-most-embarrassing-fails>.

Political Meme Tracker. A: *Electomatic* [en línia] MSS Media, 2021. [Consulta: 26 maig 2021].
Disponible a: <https://www.electomatic.com/political-meme-tracker/>.

The Babylon Bee [en línia] The Babylon Bee, 2021. [Consulta: 26 maig 2021]. Disponible a: <https://babylonbee.com/>.

The Onion [en línia] G/O Media, 2021. [Consulta: 26 maig 2021]. Disponible a: <https://www.theonion.com/>.

"Too many people think satirical news is real". A: T*he Conversation* [en línia] Asociación The Conversation España, 2019. [Consulta: 26 maig 2021]. Disponible a: <https://theconversation.com/too-many-people-think-satirical-news-is-real-121666>.



FCRI (2021) Sàtira (*Satire/Parody*) [en línia]. [Consulta: 27 maig 2021].
Disponible a: <https://youtu.be/Pp0r51osR4Y>.

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

Trols, bots i comptes falsos o comptes titella

Qui ho pot fer: aficionat

El grau d'habilitat necessari per produir trols, bots o compte falsos actius, varia força.

Qualsevol pot crear i utilitzar un compte fals senzill, fer servir tècniques per trolejar o comprar bots per fer clics o aconseguir "m'agrades". Hi ha eines digitals que poden generar tot tipus d'informació personal falsificada, necessària per crear comptes falsos —des de noms falsos i adreces de correu electrònic temporals fins a la generació i validació de números d'identificació nacional. Però calen uns coneixements mínims de programació per crear bots de xarxes socials.

Els efectes més nocius dels trols, els bots o els comptes falsos acostumen a ser provocats per persones amb habilitats professionals. Alguns bots empren tècniques avançades d'intel·ligència artificial per tal de semblar més realistes; alguns trols utilitzen convincents tècniques de narració i manipulació 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: 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.

En què consisteix?

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.[58]

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.[59]

Un **compte fals** o **compte titella** 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).[60]

[58] https://en.wikipedia.org/wiki/Internet_troll
[59] https://en.wikipedia.org/wiki/Internet_bot
[60] https://en.wikipedia.org/wiki/Sock_puppet_account

Com funciona?

Tàctiques que utilitzen els trols:

- **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 (*sealioning*)**: 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.
- **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 ara 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 assenyats 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:

- **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 és 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.

Com detectar-ho:

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 o Cloudflare Bot Management que també usa l'aprenentatge automàtic per reconèixer bots.

- Utilitzar l'eina anomenada "botòmetre",[61] que comprova l'activitat d'un compte de Twitter i li dona una puntuació. Les puntuacions més altes signifiquen més activitat semblant als bots.

[61] https://botometer.iuni.iu.edu

Per saber-ne més:

"Identifying Fake Social Media Profiles Possible with Google Image Search". A: *HackRead.com* [en línia] HackRead, 2015. [Consulta: 26 maig 2021]. Disponible a: <https://www.hackread.com/google-image-search-social-media-profiles/>.

Chastain, Ragen. "The Complete Guide to Understanding and Dealing With Online Trolls". A: *Better Humans* [en línia], Better Humans, 2018. [Consulta: 26 maig 2021]. Disponible a: https://betterhumans.pub/the-complete-guide-to-understanding-and-dealing-with-online-trolls-4a606ae25c2c

"Cybersecurity and Infrastructure Security Agency (2018)". *Social Media Bots Overview* [en línia]. [Consulta: 26 maig 2021] Disponible a: <https://niccs.cisa.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf>

"What is a social media bot? Social media bot definition". A: Cloudflare [en línia], Cloudflare, 2018. [Consulta: 26 maig 2021]. Disponible a: <https://www.cloudflare.com/es-es/learning/bots/what-is-a-social-media-bot/>

"Recognising And Dealing With Trolls". A: Team Technology [en línia] Team Technology, 2021. [Consulta: 26 maig 2021]. Disponible a: <https://www.teamtechnology.co.uk/troll-tactics.html>

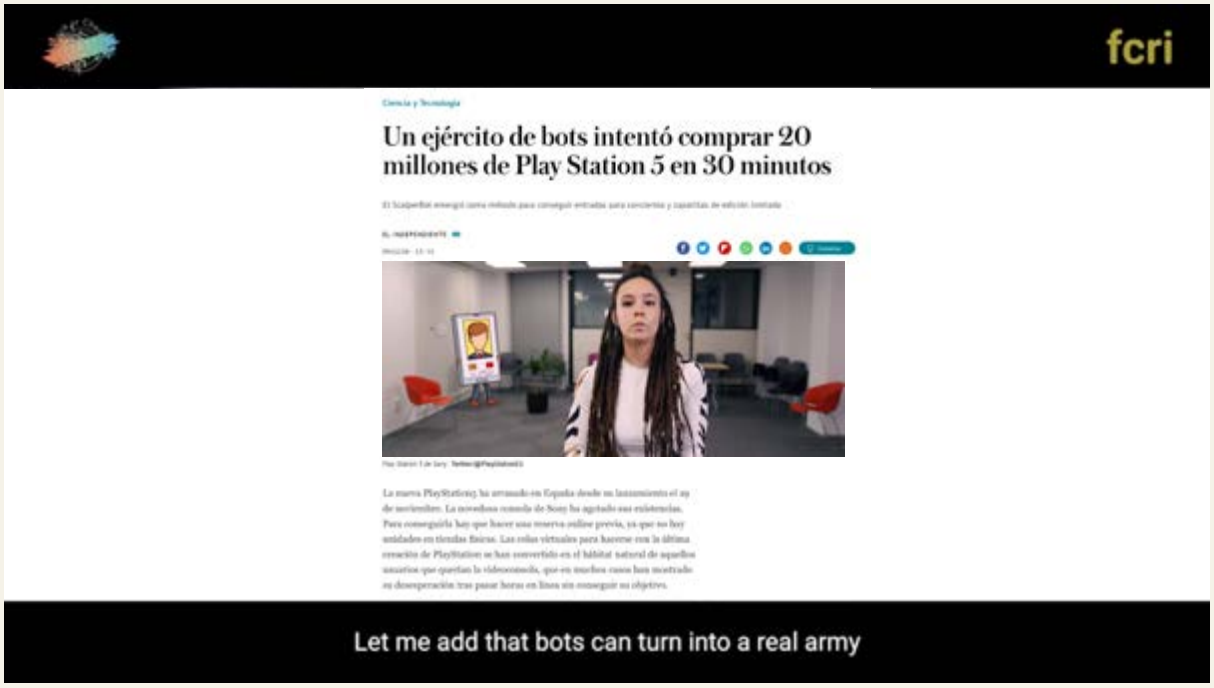
Linvill, Darren; Warren, Patrick. "That Uplifting Tweet You Just Shared? A Russian Troll Sent It". A: *Rolling Stone* [en línia] Rolling Stone LLC, 2019. [Consulta: 26 maig 2021]. Disponible a: <https://www.rollingstone.com/politics/politics-features/russia-troll-2020-election-interference-twitter-916482/>.

Olin, Kris. "Exposed! Fake Facebook Accounts Attacking Facebook Groups". A: Social Media Revolver [en línia] Social Media Revolver, 2013. [Consulta: 26 maig 2021]. Disponible a: <https://socialmediarevolver.com/fake-facebook-accounts-attacking-facebook-groups/>.

Shu, Catherine. "Twitter suspends more accounts for engaging in coordinated manipulation". A: *Techno Crunch* [en línia] Verizon Media, 2018. [Consulta: 26 maig 2021]. Disponible a: <https://techcrunch.com/2018/08/27/twitter-suspends-more-accounts-for-engaging-in-coordinated-manipulation/>.

"Social media spam bots and fake engagement". A: Target Internet [en línia] Target Internet, 2021. [Consulta: 26 maig 2021]. Disponible a: <https://www.targetinternet.com/social-media-spam-bots-and-fake-engagement/>.

"Thai 'click farm' raided, over 300,000 SIM cards found". A: *SBS News* [en línia] SBS, 2017. [Consulta: 26 maig 2021]. Disponible a: <https://www.sbs.com.au/news/thai-click-farm-raided-over-300-000-sim-cards-found>.



FCRI (2021) Trols i bots (*Trolls/bots/fake, puppet accounts*) [en línia]. [Consulta: 27 maig 2021]. Disponible a: <https://youtu.be/zAG1aWXJaD8>.

Establiment d'amistat (i suplantació d'identitat)

Qui ho pot fer: aficionat 

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. Establir amistat demana coneixements psicològics bàsics i saber comprendre a les altres persones.

Grau d'engany: mitjà 

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.

En què consisteix?

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'n algun profit (aconseguir informació personal, fotos, vídeos, etc.).

Com funciona?

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 legals presents a les plataformes 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 persona famosa ha contactat amb ells.

De vegades, s'envien missatges elementals que informen a la persona destinatària 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, els estafadors 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 cliquin 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 utilitzat; per exemple, en els videojocs en línia normalment s'utilitzen sobrenoms que no donen cap informació sobre la veritable identitat de la persona.

Qui ho pot fer: aficionat

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 a 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 accedeixes 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.

Com detectar-ho:

Si algú està intentant convèncer-te 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 persona famosa 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 aquest personatge famós?
- 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 demanes que les afegeixis a la teva xarxa, sobretot si només coneixes la persona per Internet. Ves amb 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 la persona destinatària personalment. Els estafadors poden utilitzar-les per fer xantatge.
- 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 ara Google o TinEye.

Per saber-ne més:

Find the Fake [en línia] ZeroFOX, 2019. [Consulta: 27 maig 2021]. Disponible a: <https://www.zerofox.com/find-the-fake/>.

Klijnsma, Yonathan. "YouTube Impersonation Scams Offering Fake Rewards are Running Wild ".A: Riskiq.com [en línia] RiskIQ, 2019. [Consulta: 27 maig 2021]. Disponible a: <https://www.riskiq.com/blog/labs/youtube-impersonation-scams/>.

FCRI (2021) Amistat (*Befriending and impersonation*) [en línia]. [Consulta: 27 maig 2021]. Disponible a: <https://youtu.be/ZVYe54DcQOU>.

Bibliografia

Consell de l'Audiovisual de Catalunya. (2018). Fake news o desinformació en línia: respostes a l'amenaça de la societat connectada. En *Informe 2017. L'audiovisual a Catalunya* (p. X-XII). https://www.cac.cat/sites/default/files/2018-07/Ac.72-2018_%20ANNEX%20Informe%20audiovisual%202017.pdf

DemTech | Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. (2021). DemTech. https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/

European Commission. (2018). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling online disinformation: A European approach*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018DC0236

Freeman, D., Waite, F., Rosebrock, L., Petit, A., Causier, C., East, A., Jenner, L., Teale, A. L., Carr, L., Mulhall, S., Bold, E., & Lambe, S. (2020). Coronavirus conspiracy beliefs, mistrust, and compliance with government guidelines in England. *Psychological Medicine*, 1–13. https://doi.org/10.1017/s0033291720001890

Gartner Reveals Top Predictions for IT Organizations and Users in 2018 and Beyond. (2017). Gartner. https://www.gartner.com/en/newsroom/press-releases/2017-10-03-gartner-reveals-top-predictions-for-it-organizations-and-users-in-2018-and-beyond

Goertzel, T. (1994). Belief in Conspiracy Theories. *Political Psychology*, 15(4), 731. https://doi.org/10.2307/3791630

Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, 5(1), eaau4586. https://doi.org/10.1126/sciadv.aau4586

International Center for Journalists. (2018). *A Short Guide to the History of «Fake News» and Disinformation: A Learning Module for Journalists and Journalism Educators*. https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf

Reuters Institute for the Study of Journalism. (2021). *Reuters Institute Digital News Report 2021*. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf

Roozenbeek, J., Schneider, C. R., Dryhurst, S., Kerr, J., Freeman, A. L. J., Recchia, G., van der Bles, A. M., & van der Linden, S. (2020). Susceptibility to misinformation about COVID-19 around the world. *Royal Society Open Science*, 7(10), 201199. https://doi.org/10.1098/rsos.201199

Salaverría, R., Buslón, N., López-Pan, F., León, B., López-Goñi, I., & Erviti, M. C. (2020). Desinformación en tiempos de pandemia: tipología de los bulos sobre la Covid-19. *El Profesional de la Información*, 29(3). https://doi.org/10.3145/epi.2020.may.15

Sánchez-Duarte, J. M., & Magallón Rosa, R. (2020). Infodemia y COVID-19. Evolución y viralización de informaciones falsas en España. *REVISTA ESPAÑOLA DE COMUNICACIÓN EN SALUD*, 31. https://doi.org/10.20318/recs.2020.5417

Types, sources, and claims of COVID-19 misinformation. (2020). Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation

van Prooijen, J. W., Staman, J., & Krouwel, A. P. (2018). Increased conspiracy beliefs among ethnic and Muslim minorities. *Applied Cognitive Psychology*, 32(5), 661–667. https://doi.org/10.1002/acp.3442

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

fcri

Fundació
Catalana per a
la Recerca i la
Innovació

Fundació Catalana per a
la Recerca i la Innovació

Passeig Lluís Companys, 23
08010 Barcelona

T. +34 93 268 77 00
info@fundaciorecerca.cat

fundaciorecerca.cat