ΔΕΚΑ ΤΥΠΟΙ ΠΑΡΑΠΛΗΡΟΦΟΡΗΣΗΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝΤΑΙ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Ενημερωτικό υλικό για εκπαιδευτικούς

Χρυσανθοπούλου Κ., Γκότση Ειρ., López B., Neuvonen M., Ražinskaitė R., Salo M., Varanauskas A., Zinkevičiūtė G.

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

Περιεχόμενα

Εισαγωγή

Αυτό το έγγραφο προορίζεται να εξοικειώσει τους εκπαιδευτικούς με τους δέκα τύπους παραπληροφόρησης στο διαδίκτυο, που συνήθως συναντώνται στα μέσα κοινωνικής δικτύωσης. Παρέχει πληροφορίες για κάθε επιλεγμένο τύπο παραπληροφόρησης και παρουσιάζει το επίπεδο εξαπάτησης, την αρχή λειτουργίας, παραδείγματα, τις μέθοδους ελέγχου και άλλες σχετικές πληροφορίες.

Οι ενότητες μέσα σε αυτόν τον οδηγό παρέχουν μόνο βασικές πληροφορίες που σχετίζονται με συγκεκριμένο τύπο παραπληροφόρησης, διότι αυτό το έγγραφο προορίζεται να αποτελέσει το πρώτο βήμα για τους εκπαιδευτικούς στο «δρόμο προς τα μέσα ενημέρωσης και γνώσης». Κάτω από κάθε τύπο παραπληροφόρησης ή στο τέλος του προγράμματος ανάγνωσης εγγράφων μπορείτε να βρείτε συνδέσμους για άλλο χρήσιμο υλικό που σας προτείνουμε να διαβάσετε και να χρησιμοποιήσετε επίσης.

Δέκα τύποι παραπληροφόρησης στα μέσα κοινωνικής δικτύωσης επιλέχθηκαν μέσω μιας επαναληπτικής διαδικασίας. Αρχικά αναλύθηκε το υπάρχον υλικό και αναπτύχθηκε ένας μακρύς κατάλογος των τύπων παραπληροφόρησης. Στη συνέχεια, ειδικοί από τους οργανισμούς των εταίρων χαρτογράφησαν και έδωσαν προτεραιότητα σε μερικούς τύπους παραπληροφόρησης για να καταλήξουν σε 15 και να εργαστούν περαιτέρω. Στο τελευταίο βήμα, συλλέχθηκαν τα σχόλια των δασκάλων και των μαθητών κι έτσι η λίστα περιορίστηκε σε ακριβώς δέκα τύπους παραπληροφόρησης που χρησιμοποιούνται στα κοινωνικά μέσα.

Αυτό το εκπαιδευτικό υλικο μπορεί να χρησιμοποιηθεί αυτόνομα (μαζί με διαφάνειες και αφίσες). Ωστόσο, αρκετό υλικό από άλλους οργανισμούς είναι επίσης ελεύθερα διαθέσιμο. Συνεπώς σας ενθαρρύνουμε να το χρησιμοποιήσετε για να προσφέρετε την καλύτερη εμπειρία στους μαθητές σας. Ευχαριστούμε ιδιαίτερα την Ευρωπαϊκή Ένωση για τα Συμφέροντα και την προστασία των Θεατών (EAVI) που ανέπτυξε δέκα τύπους παραπλανητικών ειδήσεων: https://eavi.eu/beyond-fake-news-10-types-misleading-info/ και μια πρώτη προσέγγιση (first draft) εντόπισε τους συγκεκριμένους τύπους παραπληροφόρησης και κακόβουλης πληροφόρησης: https://firstdraftnews.org/fake-news-complicated/). Στο τέλος του εγγράφου θα βρείτε περισσότερες ιδέες και τροφή για σκέψη.

Επιπλέον στο πλαίσιο του έργου gaMEdia, (που συγχρηματοδοτήθηκε από την Ευρωπαϊκή επιτροπή κάτω από την προπαρασκευαστική δράση «Ψηφιακός γραμματισμός για όλους 2018» LC-01234900) ήδη αναπτύσσεται ένα παιχνίδι με κάρτες για παιδιά ηλικίας 12-15 ετών που μπορεί να χρησιμοποιηθεί ως συμπληρωματικό υλικό πάνω στον ψηφιακό γραμματισμό και την πληροφόρηση. Περισσότερες πληροφορίες για το έργο και τα υλικά του θα βρείτε εδώ:

www.checkorcheat.eu.

Πριν προχωρήσουμε στην ανάγνωση των πληροφοριών για τους δέκα επιλεγμένους τύπους παραπληροφόρησης, είναι απαραίτητο να διευκρινήσουμε μερικές έννοιες, καθώς μερικές φορές αυτές χρησιμοποιούνται με διαφορετικό τρόπο. Σε αυτό το έργο, χρησιμοποιούμε τον ακόλουθο

ορισμό και τις διακρίσεις μεταξύ της εσφαλμένης πληροφόρησης, της παραπληροφόρησης και της κακόβουλης πληροφόρησης:

- Εσφαλμένη πληροφόρηση: Όταν κοινοποιούνται ψευδείς πληροφορίες, χωρίς όμως να υπάρχει κάποια πρόθεση για πρόκληση βλάβης·
- Παραπληροφόρηση: Όταν οι ψευδείς πληροφορίες κοινοποιούνται εσκεμμένα για να προκαλέσουν βλάβη·
- Κακόβουλη πληροφόρηση: Όταν κοινοποιούνται γνήσιες πληροφορίες για να προκαλέσουν βλάβη.

Ορισμένα θέματα σε αυτό το έγγραφο δεν παρουσιάζονται στο βαθμό που θα απαιτείτο. Παρ 'όλα αυτά, μένουν εκτός, όχι επειδή είναι ασήμαντα· αντιθέτως, επειδή λόγω της σημασίας τους, θα απαιτούσαν μια ξεχωριστή δημοσίευση. Ένα από τα θέματα είναι και το παραπλανητικό περιεχόμενο στο YouTube. Τα παιδιά όλων των ηλικιών παρακολουθούν πολλά βίντεο, και λόγω αλγορίθμων που παράγουν προτάσεις προβολής, εκτίθενται ευρέως σε τρελές θεωρίες συνωμοσίας και «κομπογιαννίτικες» ιδέες, σε αλλοπρόσαλους ισχυρισμούς υγείας, καθώς και σε ριζοσπαστικοποιημένο περιεχόμενο (*ρητορική μίσους*). Τα θέματα που αναφέρονται παραπάνω καλύπτονται σε αυτό το έγγραφο, όμως, δεν δίνεται προσοχή στην «στρατικοποίηση» των σχολίων, η οποία γίνεται συνήθως από ομάδες που εμπίπτουν στην εναλλακτική δεξιά (alt-right). Ένα άλλο θέμα που δεν παρουσιάζεται είναι το PsyOps (αναφέρεται στις ψυχολογικές επιχειρήσεις: στρατιωτικές επιχειρήσεις που συνήθως στοχεύουν στον επηρεασμό της κατάστασης του εχθρού με μη-μαχητικά μέσα (όπως η διανομή φυλλαδίων), ο οποίος είναι αρκετά περίπλοκος και θα απαιτούσε εκτεταμένη έρευνα και εστίαση στις τεχνικές λεπτομέρειες. Το τελευταίο θέμα που πιστεύουμε ότι πρέπει να αναφερθεί είναι ο διαδικτυακός εκφοβισμός (cyber-bullying), καθώς αποτελεί ένα ευρέως διαδεδομένο πρόβλημα και πολλοί μαθητές το αντιμετωπίζουν εντός του διαδικτυακού περιβάλλοντος. Αρκετές τεχνικές είναι πολύ παρόμοιες με αυτές που χρησιμοποιούνται στην παραπληροφόρηση (δυνατότητα κοινοποίησης για διάδοση φήμων, αλλοιωμένες εικόνες και βίντεο, γυμνές φωτογραφίες, χρήση αστείων μιμιδίων [memes]). Πιστεύουμε ότι ο διαδικτυακός εκφοβισμός καλύπτεται εκτενώς στη συζήτηση επί της σύγχρονης εκπαιδεύσης, ενώ πολλοί συγγραφείς τον έχουν καλύψει καλύτερα από ό,τι θα μπορούσαμε εμείς.

Πριν προχωρήσετε στην ανάγνωση των τύπων παραπληροφόρησης, θα ακολουθήσει μια σύντομη υπενθύμιση για το πώς ο καθένας μας μπορεί να συμβάλλει στον τερματισμό της διάδοσης λανθασμένων ή κακόβουλων πληροφοριών.

1. Μην διαβάζετε μόνο τον τίτλο. Διαβάστε ολόκληρη την ιστορία προτού την κοινοποιήσετε — συμπεριλαμβανομένου του ονόματος του συγγραφέα και της ημερομηνίας δημοσίευσής της. Εάν η ιστορία είναι ψεύτικη, εκεί θα βρείτε τις πρώτες σας ενδείξεις — ειδικά αν ο τίτλος δεν ταιριάζει με το περιεχόμενο.

2. Ελέγξτε αν άλλα συναφή μέσα αναφέρουν την ίδια ιστορία. Εάν μόνο ένα μέσο ενημέρωσης αναφέρει μια ιστορία, ενδέχεται αυτό να συμβαίνει για κάποιον λόγο — θα μπορούσε να είναι αποκλειστική ή να αναφέρει ένα γεγονός που βασίζεται σε διαρροή πληροφοριών ή πηγές

που απαιτούν τη διατήρηση της ανωνυμίας τους. Σε τέτοιες περιπτώσεις, τα άλλα μέσα ενημέρωσης σπεύδουν συνήθως να επαληθεύσουν την ιστορία ή να καλύψουν τις αντιδράσεις στην ιστορία, γεγονός που σας δίνει περισσότερη σιγουριά ότι η ιστορία είναι αληθινή. Στην περίπτωση όμως που κανένα γνωστό μέσο ενημέρωσης δεν έχει καλύψει την ιστορία, και τη βλέπετε μόνο σε ιστολόγια ή σε μέσα ενημέρωσης που απευθύνονται σε πολύ συγκεκριμένο κοινό, μην βιαστείτε να κοινοποιήσετε την ιστορία ή το βίντεο.

3. Πραγματοποιήστε μια γρήγορη αναζήτηση στο Google. Ενδέχεται να μάθετε νέα στοιχεία ή να μάθετε ότι η ιστορία δημοσιεύθηκε πριν από πέντε χρόνια, ή/και ότι ο τίτλος είναι ψευδής.

4. Όταν κάποιοι σας λένε κάτι ή μεταφέρουν κάτι που ενδέχεται να είναι ψευδές, ρωτήστε τους περισσότερα για το πού το άκουσαν, είδαν ή διάβασαν.

Εάν έχετε αμφιβολίες, μην κοινοποιείτε. Δεν είναι κακό να μην κοινοποιήσετε κάτι, μπορεί όμως να αποδειχτεί επιζήμιο να κοινοποιήσετε κάτι που δεν είναι αληθές.

Παραποιημένα βίντεο (Deepfakes)

Ποιοι μπορούν να τα παράγουν:

Επαγγελματίες – **Ερασιτέχνες** – Οποιοσδήποτε.

Ωστόσο, η τεχνολογία εξελίσσεται ραγδαία, γι' αυτό και προβλέπεται ότι στο κοντινό μέλλον θα μπορεί ο καθένας να τα παράγει: https://www.theverge.com/2019/6/10/18659432/deepfake-ai-fakes-tech-edit-video-by-typing-new-words.

Υπάρχουν διαθέσιμες εφαρμογές (https://www.malavida.com/en/soft/fakeapp/#gref) που μπορούν οι χρήστες να κατεβάσουν για να ξεκινήσουν να πειραματίζονται.

Επίπεδο εξαπάτησης:

Χαμηλό – Μέτριο – Υψηλό – **Πολύ υψηλό**.

Ο εντοπισμός των deepfakes αποτελεί ένα μείζον πρόβλημα. Συνήθως, τα ερασιτεχνικά deepfakes μπορούν να εντοπιστούν με γυμνό μάτι, όμως, τα deepfakes γίνονται όλο και καλύτερα, ενώ σύντομα θα αναγκαστούμε να βασιζόμαστε σε ψηφιακά μέσα για τον εντοπισμό τους — εάν βέβαια είμαστε σε θέση να τα εντοπίσουμε.

Σύντομη περιγραφή:

Το deepfake είναι μια τεχνολογία που βασίζεται στην Τεχνητή Νοημοσύνη (AI), η οποία χρησιμοποιείται για την παραγωγή ή την αλλαγή περιεχομένου βίντεο με επεξεργασία προσώπων (εναλλαγή προσώπων ή δημιουργία νέων εκφράσεων προσώπου). Τα πρώτα deepfakes δημιουργήθηκαν με την αντικατάσταση προσώπων σε βίντεο από πρόσωπα διασημοτήτων, κυρίως σε πορνογραφικά βίντεο κλιπ. Έγινε πρώτη φορά τον Δεκέμβριο του 2017 από τον χρήστη του Reddit γνωστό ως deepfakes (ένας συνδυασμός του «deep learning» («βαθιά μάθηση») και της αγγλικής λέξης «fake» («ψεύτικος»), από τον οποίο πήρε το όνομά του αυτός ο τύπος), ο οποίος χρησιμοποίησε τεχνολογία βαθιάς μάθησης για να επεξεργαστεί τα εικονιζόμενα πρόσωπα. Με σκοπό τη διάδοση ψευδών πληροφοριών, χρησιμοποιείται η τεχνολογία βαθιάς μάθησης για τη δημιουργία μιας νέας έκφρασης του προσώπου των διασημοτήτων, η οποία προσομοιώνει τις κινήσεις των μυών του προσώπου, έτσι ώστε να αντιπροσωπεύει την προφορική έκφραση που θα συνόδευε η πηγαία αφήγηση του κατασκευασμένου κειμένου, το οποίο δεν ειπώθηκε ποτέ από το ίδιο το πρόσωπο.

Αρχή λειτουργίας (τι κάνουν και πώς επιτυγχάνουν τον σκοπό τους):

Τα deepfakes δημιουργούνται χρησιμοποιώντας δύο ανταγωνιστικά συστήματα Τεχνητής Νοημοσύνης - το ένα ονομάζεται γεννήτρια (generator) και το άλλο ονομάζεται διαχωριστής (discriminator). Η γεννήτρια δημιουργεί ένα ψεύτικο βίντεο κλιπ και στη συνέχεια ζητά από τον διαχωριστή να προσδιορίσει εάν το κλιπ είναι πραγματικό ή ψεύτικο. Κάθε φορά που ο διαχωριστής αναγνωρίζει με ακρίβεια ένα βίντεο κλιπ ως ψεύτικο, δίνει στη γεννήτρια ένα στοιχείο για το τι δεν πρέπει να κάνει κατά τη δημιουργία του επόμενου κλιπ.

Καθώς η γεννήτρια βελτιώνεται στη δημιουργία ψεύτικων βίντεο κλιπ, ο διαχωριστής γίνεται καλύτερος στο εντοπισμό τους. Αντίστοιχα, καθώς ο διαχωριστής γίνεται καλύτερος στο να εντοπίζει ψεύτικα βίντεο, η γεννήτρια γίνεται καλύτερη στο να τα δημιουργεί.

Μαζί, η γεννήτρια και ο διαχωριστής σχηματίζουν κάτι που ονομάζεται *αναγγενητικό ανταγωνιστικό δίκτυο (ΑΑΔ)*. Το πρώτο βήμα για τη δημιουργία ενός ΑΑΔ είναι να προσδιορίσετε το επιθυμητό αποτέλεσμα και να δημιουργήσετε ένα σύνολο δεδομένων

εκπαίδευσης για τη γεννήτρια. Μόλις η γεννήτρια αρχίσει να δημιουργεί ένα αποδεκτό επίπεδο αποτελεσμάτων, τα βίντεο κλιπ μπορούν να τροφοδοτηθούν στον διαχωριστή.
Πηγή: https://whatis.techtarget.com/definition/deepfake.

Παράδειγμα:
Στο YouTube κανάλι «TheFakening», θα βρείτε πολλά παραδείγματα (ορισμένα σχετίζονται και με την εκπαίδευση): https://www.youtube.com/c/TheFakening/videos.
Άρθρο στο Gizmodo σχετικά με τα deepfakes: https://gizmodo.com/insanely-accurate-lip-synching-tech-could-turn-fake-new-1796843610.
Σύνθεση του βίντεο Obama:
https://www.youtube.com/watch?time_continue=62&v=MVBe6_o4cMI&feature=emb_logo.

Μέθοδος ελέγχου:
Εάν το deepfake δεν είναι επαγγελματικό, μπορεί κανείς να παρατηρήσει ότι οι σκιές δεν απεικονίζονται όπως θα έπρεπε, ή ότι το άτομο δεν ανοιγοκλείνει τα μάτια του. Όμως, εάν το deepfake είναι υψηλής ποιότητας, δεν υπάρχει τρόπος να το εντοπίσετε με γυμνό μάτι. Πολλές εταιρείες προσπαθούν να αναπτύξουν λογισμικό που θα μπορούσε να βοηθήσει στον εντοπισμό των deepfakes: https://techcrunch.com/2020/09/14/sentinel-loads-up-with-1-35m-in-the-deepfake-detection-arms-race/. Ο στρατός των Η.Π.Α. επίσης χρηματοδοτεί μια προσπάθεια εντοπισμού των deepfakes: https://www.technologyreview.com/s/611146/the-us-military-is-funding-an-effort-to-catch-deepfakes-and-other-ai-trickery/.

Ψευδοεπιστήμη

Ποιοι μπορούν να την παράγουν:

Επαγγελματίες – Ερασιτέχνες – **Οποιοσδήποτε**.

Είναι πολύ εύκολη η διάδοση ψευδοεπιστήμης, καθώς αυτή δεν απαιτεί δεξιότητες. Αλλά η δημιουργία ψευδοεπιστημονικής θεωρίας είναι πολύ πιο δύσκολη από ό,τι θα περίμενε κανείς.

Επίπεδο παραπλάνησης:

Χαμηλό – Μέτριο – **Υψηλό** – Πολύ υψηλό.

Οι υποστηρικτές της ψευδοεπιστήμης συχνά χρησιμοποιούν επιστημονικό λεξιλόγιο, παρουσιάζοντας εικασίες ως υποθέσεις, θεωρίες ή νόμους, παρέχοντας «αποδεικτικά στοιχεία» από παρατηρήσεις και μαρτυρίες «ειδικών», ή ακόμη και φαινομενικά μαθηματικά μοντέλα των ιδεών τους.

Εξαιτίας αυτού, μπορεί να είναι δύσκολο να ξεχωρίσει κανείς τις έγκυρες από τις αναληθείς πληροφορίες, ειδικά χωρίς επιπρόσθετη επαλήθευση.

Σύντομη περιγραφή:

Η ψευδοεπιστήμη αποτελείται από δηλώσεις, πεποιθήσεις, ή πρακτικές που ισχυρίζονται ότι είναι επιστημονικές και πραγματικές, παρόλο που δεν είναι συμβατές με την επιστημονική μέθοδο.

Η ψευδοεπιστήμη χαρακτηρίζεται συχνά από αντιφατικούς, υπερβολικούς ή αβάσιμους ισχυρισμούς· αυτοί βασίζονται στην προκατάληψη αυτοεπιβεβαίωσης (confirmation bias) και όχι στις αυστηρές προσπάθειες κατάρριψης ισχυρισμών· χαρακτηρίζονται από έλλειψη διαθεσιμότητας για αξιολόγηση από άλλους ειδικούς, από απουσία συστηματικών πρακτικών κατά την ανάπτυξη υποθέσεων, αλλά και από συνεχή επιμονή επί των ίδιων θέσεων από τους εκφραστές τους, ακόμα και πολύ μετά την κατάρριψή τους από την επιστημονική κοινότητα.

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

Αρχή λειτουργίας (τι κάνει και πώς επιτυγχάνει τον σκοπό της):

Η ψευδοεπιστήμη συναντάται όταν κάτι παρουσιάζεται ως επιστήμη ανακριβώς ή ακόμη και για σκοπούς παραπλάνησης.

Όταν κάτι είναι δημοφιλές, αλλά λανθασμένο, μπορεί συχνά να μετατραπεί σε καθιερωμένο «γεγονός», απλώς και μόνο επειδή επαναλαμβάνεται τόσες πολλές φορές. Μερικές φορές, αυτή η παραπληροφόρηση οφείλεται σε δημοφιλή επιστημονική φαντασία που είτε βασίζεται σε παλιές, ξεπερασμένες έννοιες είτε απλά σε λανθασμένη σύγχρονη επιστήμη.

Οι ψευδοεπιστημονικοί ισχυρισμοί *πολύ* σπάνια εμπεριέχουν συγκεκριμένες, ελέγξιμες επιστημονικές προβλέψεις, και αντ 'αυτού, βασίζονται σε ασαφή και διφορούμενη γλώσσα, η οποία συχνά περιλαμβάνει μεγαλοπρεπείς ισχυρισμούς.

Στην «κομπογιαννίτικη» ιατρική, ένας υποστηρικτής ψευδοεπιστήμης μπορεί να ισχυριστεί ότι μια δεδομένη θεραπεία «αφαιρεί τις τοξίνες από το σύστημά σας», χωρίς να λέει ποτέ *ποιες τοξίνες*, ή πώς αυτές θα αφαιρεθούν, ή πώς μπορείτε να διαπιστώσετε εάν έχουν όντως αφαιρεθεί. Οι τοξίνες είναι η πραγματική αιτία της νόσου, χωρίς όμως να αναφέρεται ποτέ πώς προκαλούν ασθένεια, ενώ παράλληλα υποστηρίζεται ότι η αφαίρεσή τους θα σας θεραπεύσει από όλες τις γνωστές παθήσεις που σας ταλανίζουν.

Παράδειγμα:
Λίστα παραδειγμάτων ψευδοεπιστήμης: https://examples.yourdictionary.com/examples-of-pseudoscience.html και https://rationalwiki.org/wiki/List_of_pseudosciences.

Μέθοδος ελέγχου:

Ο ευκολότερος τρόπος για να ξεχωρίσετε την ψευδοεπιστημονική μέθοδο από την επιστημονική μέθοδο είναι να εξετάσετε αν υπάρχουν ελέγξιμες προβλέψεις, και να δείτε αν τα πειράματα αποσκοπούσαν στο να δοκιμάσουν τη θεωρία ή απλά στο να την επιβεβαιώσουν.

Θα ήταν χρήσιμο να διακρίνουμε την επιστήμη και την ψευδοεπιστήμη:

ΕΠΙΣΤΗΜΗ	ΨΕΥΔΟΕΠΙΣΤΗΜΗ
Ο πρωταρχικός στόχος της επιστήμης είναι να επιτύχει μια πληρέστερη και πιο ενοποιημένη κατανόηση του φυσικού κόσμου.	Οι ψευδοεπιστήμες είναι πιθανότερο να καθοδηγούνται από ιδεολογικές, πολιτιστικές ή εμπορικές σκοπιμότητες. Μερικά παραδείγματα: αστρολογία (από την αρχαία Βαβυλωνιακή κουλτούρα), ουφολογία (UFO) (λαϊκισμός και δυσπιστία έναντι της κυβέρνησης), Δημιουργισμός (απόπειρα να δικαιολογήσει μια κυριολεκτική ερμηνεία της Βίβλου), «δομικά τροποποιημένα» νερά (εμπορικές ανοησίες).
Τα περισσότερα επιστημονικά πεδία αποτελούν αντικείμενο έντονης έρευνας που οδηγεί στη συνεχή διεύρυνση των γνώσεων στον κλάδο.	Το πεδίο έχει εξελιχθεί ελάχιστα από τότε που ιδρύθηκε. Ο μικρός όγκος έρευνας και πειραματισμού που πραγματοποιείται, γίνεται περισσότερο για να δικαιολογήσει την πεποίθηση παρά για να την επεκτείνει.
Οι εργαζόμενοι στον τομέα αναζητούν συνήθως αντιπαραδείγματα ή ευρήματα που φαίνεται να είναι ασυνεπή με τις αποδεκτές θεωρίες.	Στις ψευδοεπιστήμες, μια ένσταση σε ένα αποδεκτό δόγμα θεωρείται συχνά εχθρική πράξη, αν όχι αίρεση, και οδηγεί σε έντονες διαφωνίες ή ακόμη και σχίσματα.
Οι παρατηρήσεις ή τα δεδομένα που δεν συνάδουν με την τρέχουσα επιστημονική κατανόηση, από τη στιγμή που αποδειχθεί ότι είναι αξιόπιστα, δημιουργούν έντονο ενδιαφέρον μεταξύ των επιστημόνων και διεγείρουν επιπλέον μελέτες.	Παρατηρήσεις ή δεδομένα που δεν συνάδουν με τις καθιερωμένες πεποιθήσεις τείνουν να αγνοούνται ή να καταστέλλονται ενεργά.
Η επιστήμη είναι μια διαδικασία στην οποία κάθε αρχή πρέπει να δοκιμάζεται εμπειρικά	Οι κύριες αρχές και παραδοχές του πεδίου συχνά είναι αδιαμφισβήτητες και είναι

και να παραμένει υποκείμενη σε αμφισβήτηση ή απόρριψη ανά πάσα στιγμή.	απίθανο να τροποποιηθούν ή να αποδειχθούν λανθασμένες.
Οι επιστημονικές ιδέες και έννοιες πρέπει να μπορούν να ευσταθούν ή να καραρρίπτονται μεμονωμένα, βάσει των υφιστάμενων γνώσεων και στοιχείων.	Οι ψευδοεπιστημονικές έννοιες τείνουν να διαμορφώνονται από το εγώ και τις προσωπικότητες ορισμένων ατόμων, σχεδόν πάντα από άτομα που δεν έχουν καμία σχέση με την πραγματική επιστήμη. Συχνά επικαλούνται αυθεντίες (το όνομα μιας διασημότητας, για παράδειγμα) για να υποστηρίξουν τους ισχυρισμούς τους.
Οι επιστημονικές εξηγήσεις πρέπει να διατυπώνονται με σαφείς και ξεκάθαρους όρους.	Οι ψευδοεπιστημονικές εξηγήσεις τείνουν να είναι ασαφείς και διφορούμενες, καθώς συχνά επικαλούνται επιστημονικούς όρους σε αμφίβολα πλαίσια.

Πηγή του πίνακα: http://www.chem1.com/acad/sci/pseudosci.html.

Δύο βίντεο σχετικά με τον εντοπισμό της ψευδοεπιστήμης:
https://www.youtube.com/watch?v=gaDvroATyjw και
https://www.youtube.com/watch?v=h-agrL1gS4c.

Αλλοιωμένο περιεχόμενο

Ποιοι το παράγουν:

Επαγγελματίες – Ερασιτέχνες – **Οποιοσδήποτε**.

Καθημερινά, οι χρήστες μοιράζονται εκατομμύρια φωτογραφίες και βίντεο στα μέσα κοινωνικής δικτύωσης. Ένα μέρος αυτού του περιεχομένου έχει υποστεί αλλοίωση, συχνά για καλοήθεις λόγους, όπως για να γίνει πιο ευκρινές το βίντεο ή για να «καθαρίσει» ο ήχος του. Όμως, μερικοί άνθρωποι προβαίνουν στην αλλοίωση μέσων για να παραπλανήσουν.

Οι αλλοιώσεις μπορούν να γίνουν με τη χρήση απλής τεχνολογίας όπως το Photoshop ή μέσω εξελιγμένων εργαλείων που χρησιμοποιούν τεχνικές τεχνητής νοημοσύνης ή «βαθιάς μάθησης», ώστε να δημιουργήσουν βίντεο που στρεβλώνουν την πραγματικότητα – τα οποία συνήθως ονομάζονται «deepfakes» (τα deepfakes παρουσιάζονται ξεχωριστά σε αυτήν την ανάλυση).

Επίπεδο παραπλάνησης:

Χαμηλό – Μέτριο – **Υψηλό** – Πολύ υψηλό.

Η ταυτότητα γίνεται πιο δύσκολο να επικυρωθεί, καθώς τα τρολς και τα bots (μηχανές αυτοματοποιημένης παραγωγής αντιδράσεων/σχολίων) υιοθετούν νέους τρόπους για να καλύψουν την πραγματική τους πηγή. Τα επεξεργασμένα βίντεο και οι αλλοιωμένες εικόνες είναι πολύ πιο δύσκολο να εντοπιστούν, σε σύγκριση με την παραπληροφόρηση σε μορφή κειμένου.

Οι εταιρείες που προσφέρουν τις σχετικές πλατφόρμες κοινωνικής δικτύωσης δέχονται αυξημένη πίεση και έλεγχο για να ανταποκριθούν στο ζήτημα αυτό. Μερικές από αυτές αναλαμβάνουν δράση και καταργούν τέτοιου είδους περιεχόμενο. Όμως, ακόμη και υπό βέλτιστες συνθήκες, απαιτείται χρόνος για ουσιώδη δράση, χρόνος κατά τον οποίο η βλάβη έχει επέλθει ήδη.

Σύντομη περιγραφή:

«Αλλοιωμένο περιεχόμενο» συναντάμε σε περιπτώσεις που τροποποιείται μια πτυχή του γνήσιου περιεχομένου, η οποία σχετίζεται συχνότερα με φωτογραφίες ή βίντεο. Τα οπτικά μέσα μπορούν να μετασχηματιστούν μέσω αλλοίωσης φωτογραφιών, διαδικασία που συχνά αποκαλείται ως «photoshopping». Η αλλοίωση βίντεο στοχεύει ψηφιακά βίντεο χρησιμοποιώντας έναν συνδυασμό παραδοσιακών τεχνικών επεξεργασίας και τροποποίησης βίντεο, και συμπληρωματικών μεθόδων τεχνητής νοημοσύνης, όπως η αναγνώριση προσώπου.

Αρχή λειτουργίας (τι κάνει και πώς επιτυγχάνει τον σκοπό του):

Αρκετές νέες τεχνικές τροποποίησης εικόνων, ήχου και βίντεο επιτρέπουν τη δημιουργία αλλοιωμένου περιεχομένου. Το «photoshopping» μπορεί να κάνει ένα προϊόν, ένα άτομο ή μια ιδέα να φαίνεται πιο ελκυστική. Αυτό γίνεται τονίζοντας ορισμένα χαρακτηριστικά. Επίσης, μπορούν να χρησιμοποιηθούν και άλλες τεχνικές, όπως το καδράρισμα [framing] (με την παρουσίαση μόνο ενός μέρους της εικόνας, χωρίς αυτό να εντάσσεται σε κάποιο συγκείμενο).

Σε περιπτώσεις τυπικής αλλοίωσης βίντεο, η δομή του προσώπου, οι κινήσεις του σώματος και η φωνή του, αναπαράγονται προκειμένου να δημιουργηθεί ένα τεχνητό ντοκουμέντο με

το υποκείμενο. Οι μέθοδοι αυτοί χρησιμοποιούνται σε εκπαιδευτικά βίντεο, καθώς και σε βίντεο που αποσκοπούν στη (μαζική) χειραγώγηση και προπαγάνδα, χρήσεις που αντιπροσωπεύουν μόνο ένα μικρό κομμάτι των εκτεταμένων δυνατοτήτων που κατέχει η αλλοίωση φωτογραφιών.

Παράδειγμα:

Παράδειγμα αλλοίωσης εικόνας: https://spotlightstories.co/32-examples-media-manipulating-truth/.

Ο οδηγός της Washington Post για τα αλλοιωμένα βίντεο: https://www.washingtonpost.com/graphics/2019/politics/fact-checker/manipulated-video-guide/.

Μέθοδοι ελέγχου:

Πώς να επιβεβαιώσετε την εγκυρότητα των ευρέως διαδεδομένων βίντεο στα μέσα κοινωνικής δικτύωσης: https://www.youtube.com/watch?v=e91IGj_apsY.

Διαδικτυακά εργαλεία για την επιβεβαίωση της εγκυρότητας μιας φωτογραφίας: https://www.stopfake.org/en/13-online-tools-that-help-to-verify-the-authenticity-of-a-photo/.

Θεωρίες συνωμοσίας («κομπογιαννίτικη» επιστήμη)

Ποιοι μπορούν να την παράγουν:

Επαγγελματίες – Ερασιτέχνες – Οποιοσδήποτε.

Η πλειονότητα των ανθρώπων είναι καταναλωτές και όχι παραγωγοί θεωριών συνωμοσίας. Δεν επινοούν τις δικές τους θεωρίες συνωμοσίας, αλλά υποστηρίζουν αυτές που ήδη κυκλοφορούν.

Επίπεδο παραπλάνησης:

Χαμηλό – Μέτριο – **Υψηλό** – Πολύ υψηλό.

Κατά γενική ομολογία, η πίστη στις θεωρίες συνωμοσίας δεν βασίζεται σε στοιχεία, αλλά στην πίστη του υποστηρικτή. Μια θεωρία συνωμοσίας υποστηρίζει την ύπαρξη μυστικών ομάδων ισχυρών ατόμων και εικάζει τις υποτιθέμενες δραστηριότητές τους, οι οποίες ενδέχεται να είναι δύσκολο να διαψευστούν.

Σύντομη περιγραφή:

Μια θεωρία συνωμοσίας είναι μια εξήγηση ενός γεγονότος ή μιας κατάστασης, η οποία επικαλείται μια συνωμοσία από απειλητικούς και ισχυρούς παράγοντες, συχνά πολιτικούς με σκοπιμότητες, ενώ υφίστανται άλλες ενδεχόμενες εξηγήσεις που είναι πιο πιθανές. Ωστόσο, σε αντίθεση με την ψευδοεπιστήμη, η «κομπογιαννίτικη» επιστήμη παρουσιάζεται χρησιμοποιώντας την επιστημονική μέθοδο. Οι ιδέες που μελετήθηκαν από τους «κομπογιαννίτες» επιστήμονες δεν λαμβάνουν υποστήριξη από το ευρύ κοινό.

Οι πεποιθήσεις συνωμοσίας δύνανται να είναι επιβλαβείς τόσο για το άτομο όσο και για την κοινότητα. Η υποστήριξη τέτοιων θεωριών σχετίζεται με μειωμένη πρόθεση συμμετοχής στα κοινωνικά και πολιτικά δρώμενα, απροθυμία ακολούθησης έγκυρων ιατρικών συμβουλών, αυξημένη προθυμία αναζήτησης μεθόδων εναλλακτικής ιατρικής και τάση απόρριψης σημαντικών επιστημονικών ευρημάτων.

Η προέλευση αμέτρητων θεωριών συνομωσίας: https://www.youtube.com/watch?v=88_C-fogY40.

Ο πραγματικός λόγος για τον οποίον οι θεωρίες συνωμοσίας έχουν τόση απήχηση: https://www.youtube.com/watch?v=tfVgHRPC7Ao.

Αρχή λειτουργίας (τι κάνουν και πώς επιτυγχάνουν τον σκοπό τους):

Οι θεωρίες συνωμοσίας έχουν σημαντική παρουσία στον Ιστό με τη μορφή ιστολογίων και βίντεο YouTube, ενώ υφίστανται και στα μέσα κοινωνικής δικτύωσης.

Οι θεωρίες συνωμοσίας είναι οι πρώτες και βασικές μορφές πολιτικής προπαγάνδας. Έχουν σχεδιαστεί για να δυσφημίσουν συγκεκριμένα άτομα ή ομάδες, ή να προωθούν μια πολιτική ατζέντα. Η θεωρία ότι οι Κλίντον εμπλέκονταν με κάποιον τρόπο στην αυτοκτονία του Έπσταϊν δυσφημεί τους Κλίντον. Η αντίληψη ότι η κυβέρνηση των Η.Π.Α. σκηνοθέτησε τους μαζικούς πυροβολισμούς το 2012 στο δημοτικό σχολείο Sandy Hook, βοήθησε το λόμπι υπέρ των όπλων να καταφέρει να αποσιωποιήσει τα επιχειρήματα υπέρ του μεγαλύτερου ελέγχου των όπλων. Ποιος καλύτερος τρόπος για να προλάβει κανείς τις εκκλήσεις για μεγαλύτερο έλεγχο όπλων, αμέσως μετά από ένα συμβάν με μαζικούς πυροβολισμούς σε ένα σχολείο, από το να ισχυριστεί ότι αυτό δεν συνέβη ποτέ;

Οι θεωρίες συνωμοσίας φαίνεται να παρέχουν ευρείες, εσωτερικά συνεπείς εξηγήσεις που επιτρέπουν στους ανθρώπους να διατηρούν τις πεποιθήσεις τους ενόψει της αβεβαιότητας και της αντίφασης.

Παράδειγμα:

Μια θεωρία συνωμοσίας μπορεί να πάρει οποιοδήποτε ζήτημα ως κεντρική θεματολογία της, αλλά ορισμένα ζητήματα προσελκύουν μεγαλύτερο ενδιαφέρον σε σχέση με άλλα. Τα πιο δημοφιλή ζητήματα περιλαμβάνουν θανάτους και δολοφονίες διασήμων, ηθικά αμφίβολες κυβερνητικές δραστηριότητες, αποσιωποιημένες τεχνολογίες, και τρομοκρατία «ψευδούς σημαίας» (που κατηγορεί ένα δεύτερο μέρος, αποκρύπτοντας τον πραγματικό υπαίτιο, ο οποίος είναι συνήθως εσωτερικός).

Μεταξύ των πιο μακροχρόνιων και πιο ευρέως αναγνωρισμένων θεωριών συνωμοσίας είναι οι ισχυρισμοί σχετικά με τη δολοφονία του Τζον Φ. Κένεντι, τις προσγειώσεις του Apollo το 1969, και τις τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου, καθώς και πολλές θεωρίες σχετικά με υποτιθέμενα σχέδια για παγκόσμια κυριαρχία από διάφορες ομάδες, τόσο πραγματικές όσο και φανταστικές.

Η λίστα του WIRED με άρθρα πάνω σε διάφορες θεωρίες συνωμοσίας (ενημερωμένη): https://www.wired.com/tag/conspiracy-theories/page/1/.

Πέντε τεχνολογικές συνωμοσίες των οποίων η εγκυρότητα έχει ελεγχθεί: https://www.businessinsider.com/facebook-microphone-listening-for-ads-other-tech-conspiracy-theories-explained-2019-9.

Βίντεο στο YouTube σχετικά με διάφορες θεωρίες συνωμοσίας: https://www.youtube.com/watch?v=_53cGxAUuDk.

Έλεγχος γεγονότων και ισχυρισμών: Ένας οδηγός για 9 θεωρίες συνωμοσίας, τις οποίες ο Τραμπ προωθεί αυτήν τη στιγμή: https://edition.cnn.com/2020/09/02/politics/fact-check-trump-conspiracy-theories-biden-covid-thugs-plane/index.html.

Μέθοδοι ελέγχου:

Λίστα ιστοσελίδων ελέγχου γεγονότων και ισχυρισμών: https://en.wikipedia.org/wiki/List_of_fact-checking_websites.

Αξιοσημείωτη πρωτοβουλία χρηματοδοτούμενη από την Ε.Ε., η οποία αποσκοπεί στην καταπολέμηση της παραπληροφόρησης (συμπεριλαμβανομένων και των θεωριών συνωμοσίας): https://euvsdisinfo.eu/.

Hoaxes (αστικοί μύθοι και chain emails)

Ποιοι μπορούν να τα παράγουν:

Επαγγελματίες – Ερασιτέχνες – **Οποιοσδήποτε.**

Ο καθένας μπορεί να δημιουργήσει ένα hoax προβαίνοντας απλά σε τεκμηριωμένες δηλώσεις και χρησιμοποιώντας ανοίκεια διατύπωση ή συγκείμενο, όπως στο hoax για το μονοξείδιο του διυδρογόνου (το μονοξείδιο του διυδρογόνου είναι νερό. Παράδειγμα: «Τα ατομικά συστατικά του DHMO περιέχονται σε μια σειρά καυστικών, εκρηκτικών και δηλητηριωδών ενώσεων όπως ως το θειικό οξύ, η νιτρογλυκερίνη και η αιθυλική αλκοόλη» - http://www.dhmo.org/facts.html).

Επίπεδο παραπλάνησης:

Χαμηλό – **Μέτριο** – Υψηλό – Πολύ υψηλό.

Τα hoaxes διατηρούν την ισχύ τους λόγω του ιδιότυπου τρόπου με τον οποίο οι άνθρωποι επεξεργάζονται πληροφορίες και υιοθετούν νέες πεποιθήσεις. Όταν έρχονται αντιμέτωποι με νέες πληροφορίες, οι άνθρωποι δεν κάνουν πάντα το λογικό πράγμα, δηλαδή να το αξιολογήσουν αντικειμενικά. Αντ 'αυτού, συχνά λαμβάνουμε γρήγορες αποφάσεις βάσει του τρόπου με τον οποίο οι πληροφορίες ταυτίζονται με τις υπάρχουσες κοσμοθεωρίες μας. Ωστόσο, με μια μικρή έρευνα στο Google και σε διαδικτυακές σελίδες ελέγχου γεγονότων και ισχυρισμών, ενδέχεται να διασταυρώσει κανείς αρκετά γρήγορα εάν μια πληροφορία είναι hoax ή όχι.

Σύντομη περιγραφή:

Το hoax είναι ένα ψέμα που κατασκευάστηκε εσκεμμένα, ώστε να παρουσιάζεται ως αλήθεια. Μια κοινή πτυχή που έχουν τα hoaxes είναι ότι αποσκοπούν στο να παραπλανήσουν ή να διαδόσουν ψέματα. Για να γίνει κάτι hoax, το ψέμα πρέπει να έχει κάτι περισσότερο να προσφέρει. Πρέπει να είναι εξωφρενικό, δραματικό, αλλά πρέπει επίσης να είναι πιστευτό και έξυπνο. Πάνω απ 'όλα, πρέπει να μπορεί να προσελκύσει την προσοχή του κοινού.

Οι ψεύτικες ειδήσεις (fake news) (αναφέρονται επίσης και ως hoax news) δημοσιεύουν σκόπιμα hoaxes που δύνανται να εξυπηρετήσουν τον στόχο της προπαγάνδας ή της παραπληροφόρησης — χρησιμοποιώντας τα μέσα κοινωνικής δικτύωσης για να κατευθύνουν το κοινό στο Διαδίκτυο και να ενισχύσουν την επιρροή τους.

Ο αστικός μύθος είναι ένα μοντέρνο είδος λαογραφίας. Συχνά αποτελείται από φανταστικές ιστορίες που σχετίζονται με μακαβριοτητες, δεισιδαιμονίες, αποκρυφισμούς, creepypasta (τρομακτικά κείμενα που αναπαράγονται ως έχουν) και άλλα αφηγηματικά στοιχεία που προκαλούν φόβο. Οι ρίζες των αστικών μύθων συνήθως εντοπίζονται στην τοπική ιστορία και τη μαζική κουλτούρα.

Ένα μήνυμα chain (chain letter) είναι ένα μήνυμα που προσπαθεί να πείσει τον παραλήπτη να διαβιβάσει αντίγραφα του ιδίου μηνύματος σε έναν ορισμένο αριθμό παραληπτών (το ίδιο ισχύει για τα email).

Αρχή λειτουργίας (τι κάνουν και πώς επιτυγχάνουν τον σκοπό τους):

Όπως αναφέρθηκε, τα hoaxes είναι ψευδείς ή ημιαληθείς πληροφορίες που παρουσιάζονται ως ακριβείς και πραγματικές με σκοπό να παραπλανήσουν άλλα άτομα. Συνήθως, είναι «εντυπωσιακές», γι’ αυτό και εξαπλώνονται γρήγορα, καθώς οι άνθρωποι τείνουν να μην

ελέγχουν την αξιοπιστία των πληροφοριών, προτού πατήσουν like σε αυτές και τις κοινοποιήσουν.

Παράδειγμα:
Όταν μια εφημερίδα ή οι ειδήσεις αναφέρουν μια ψεύτικη ιστορία, αυτή ταυτοποιείται ως ένα hoax. Οι παραπλανητικές ενέργειες που αποσκοπούν στο να τραβήξουν την προσοχή του κοινού, οι επιστημονικές απάτες, οι ψευδείς απειλές για βόμβα και οι επιχειρηματικές απάτες, αποτελούν παραδείγματα περιπτώσεων hoax.
Ένα από τα πρώτα καταγεγραμμένα hoaxes στα μέσα ενημέρωσης ήταν ένα ψεύτικο αλμανάκ που δημοσιεύτηκε από τον Jonathan Swift με το ψευδώνυμο «Isaac Bickerstaff» το 1708. Ο Swift προέβλεψε στο αλμανάκ τον θάνατο του John Partridge, ενός από τους κορυφαίους αστρολόγους στην Αγγλία εκείνη την εποχή, και αργότερα εξέδωσε μια ελεγεία την ημέρα που υποτίθεται ότι πέθανε ο Partridge. Ως εκ τούτου, η φήμη του Partridge καταστράφηκε και το αστρολογικό αλμανάκ του σταμάτησε να δημοσιεύεται για τα επόμενα έξι χρόνια.
Ορισμένα σύγχρονα παραδείγματα: https://www.mentalfloss.com/article/49674/14-greatest-hoaxes-all-time.

Μέθοδος ελέγχου:
Λίστα ιστοσελίδων ελέγχου γεγονότων και ισχυρισμών: https://en.wikipedia.org/wiki/List_of_fact-checking_websites.
Αξιοσημείωτη πρωτοβουλία χρηματοδοτούμενη από την Ε.Ε., η οποία αποσκοπεί στην καταπολέμηση της παραπληροφόρησης (συμπεριλαμβανομένων και των hoaxes): https://euvsdisinfo.eu/.

Παραπλανητικοί σύνδεσμοι/δολώματα (clickbait)

Ποιοι μπορούν να τους παράγουν:

Επαγγεματίες – **Ερασιτέχνες** – Οποιοσδήποτε.

Για ιστότοπους που ευδοκιμούν χάρη στην υψηλή αναλογία κλικ ανά περιεχόμενο που σημειώνουν, πολλοί αρθρογράφοι χρησιμοποιούν το clickbait ως μέσο για να εισέλθουν στην ανθρώπινη ψυχολογία, επινοώντας εντυπωσιακούς τίτλους. Μερικές φορές, το clickbait χρησιμοποιείται επίσης και από δημοσιογράφους. Σε κάποιες περιπτώσεις, ορισμένοι ερασιτέχνες μπορούν να δημιουργήσουν καλά clickbaits, όμως, η επιτυχημένη και συστηματική χρήση του clickbait απαιτεί επαγγελματικά προσόντα.

Επίπεδο παραπλάνησης:

Χαμηλό – Μέτριο – **Υψηλό** – Πολύ υψηλό.

Το «clickbait» αποτελεί μια κυρίαρχη πρακτική στα διαδικτυακά μέσα, με τους τίτλους που έχουν σχεδιαστεί για να προσελκύσουν τους ανθρώπους να κάνουν κλικ, να αποτελούν τον κανόνα. Η αντίσταση στο clickbait είναι δύσκολη, καθώς αυτό εκμεταλλεύεται τα νευρικά κυκλώματα που εξελίχθηκαν για εκατομμύρια χρόνια. Οι εγκέφαλοί μας δεν είχαν σχεδιαστεί για να εκτίθενται στην ποικιλία των πειρασμών που βρίσκονται σε αυτόν τον υπερ-συνδεδεμένο κόσμο. Μια πιο ανησυχητική μορφή του clickbait είναι αυτή που απευθύνεται άμεσα στους φόβους των ανθρώπων, ειδικά επειδή σχετίζεται με μια απειλή προς μια κοινωνική ομάδα στην οποία ανήκουν - συναισθηματικό clickbait. Αυτή η μορφή clickbait εξυπηρετεί τους διττούς σκοπούς της διέγερσης του ενθουσιασμού, χρησιμοποιώντας το αίσθημα του ομαδικού ανταγωνισμού, ενώ διαδίδεται εύκολα μεταξύ των διαδικτυακών μέσων κοινωνικής δικτύωσης.

Σύντομη περιγραφή:

Το clickbait είναι μια μορφή ψεύτικης διαφήμισης που χρησιμοποιεί υπερσυνδέσμους ή συνδέσμους με μικρογραφίες (thumbnails) που έχουν σχεδιαστεί για να τραβούν την προσοχή και να προσελκύουν τους χρήστες να ακολουθήσουν αυτόν τον σύνδεσμο και να διαβάσουν, δουν ή ακούσουν το περιεχόμενο στο οποίο αυτός οδηγεί, έχοντας ως κύρια χαρακτηριστικά τα στοιχεία της παραπλάνησης και της ευαισθητοποίησης/επίκλησης στο συναίσθημα (πηγή: https://www.cyber.gov.au/acsc/view-all-content/glossary/clickbait). Έτσι, ορισμένες φορές, το clickbait συναντάται επίσης με δημοσιογραφικούς τίτλους που σκανδαλίζουν ή υπερβάλλουν για το περιεχόμενό τους.

Σε ορισμένες περιπτώσεις, το clickbait χρησιμοποιείται απλά για κερδοφορία· περισσότερα κλικ ισούνται με περισσότερα χρήματα που παράγονται μέσω διαφημιστών. Αλλά αυτοί οι τίτλοι και τα άρθρα μπορούν επίσης να χρησιμοποιηθούν για να επηρεάσουν μια ομάδα ανθρώπων στα μέσα κοινωνικής δικτύωσης. Κατασκευάζονται για να προσελκύσουν τις προϋπάρχουσες προκαταλήψεις της ομάδας ενδιαφέροντος ώστε να κοινοποιούνται εντός ορισμένων φιλτρόκοσμων (filter bubbles).

Αρχή λειτουργίας (τι κάνουν και πώς επιτυγχάνουν τον σκοπό τους):

Οι επικεφαλίδες των clickbait άρθρων στοχεύουν στο να εκμεταλλευτούν το «χάσμα περιέργειας» (curiosity gap), παρέχοντας στον τίτλο πληροφορίες αρκετές για να κινήσουν

την περιέργεια του αναγνώστη, αλλά όχι αρκετές για να ικανοποιήσουν την περιέργειά του αν δεν κάνει κλικ στον σύνδεσμο που οδηγεί στο περιεχόμενο. Οι επικεφαλίδες των clickbait προσθέτουν ένα στοιχείο ανεντιμότητας, χρησιμοποιώντας δολώματα που δεν αντικατοπτρίζουν με ακρίβεια το περιεχόμενο που παρουσιάζεται. Η λέξη «-bait» (δόλωμα) του όρου χρησιμοποιείται κατ 'αναλογία με το ψάρεμα, όπου ένας γάντζος κρύβεται μέσα σε ένα δόλωμα, δίνοντας την εντύπωση στα ψάρια ότι πρόκειται για επιθυμητό φαγώσιμο πράγμα.

Μερικές φορές, το clickbait μοιάζει περισσότερο με την τεχνική δόλωματος και μεταστροφής (bait and switch). Δηλαδή, διαβάζουμε έναν ελκυστικό τίτλο ή έναν σύνδεσμο, κάνουμε κλικ σε αυτόν, και καταλήγουμε σε μια διαφήμιση. Υπάρχει περιεχόμενο όταν κάνουμε κλικ στον σύνδεσμο, αλλά αυτό περιβάλλεται από μια μεγάλη ποσότητα διαφημίσεων. Έτσι, το άρθρο ή το βίντεο είναι στην πραγματικότητα ένα δέλεαρ που μας εκθέτει στη διαφήμιση, η οποία αποτελεί τον *πραγματικό* σκοπό του περιεχομένου. Όταν εκτίθενται αρκετά άτομα στις διαφημίσεις, θα υπάρξει και ένα ποσοστό που θα γίνουν αγοραστές. Λειτουργεί όπως και οπουδήποτε αλλού· δεν χρησιμοποιούνταν τόσο ευρέως.

Πηγη: https://www.youtube.com/watch?v=qskqM9O0FC0.

Παραδείγματα:

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

Μέθοδοι ελέγχου:

Έχουν αναπτυχθεί διάφορα εργαλεία για την αντιμετώπιση του προβλήματος του clickbait. Η ανίχνευση των clickbaits έχει ενσωματωθεί σε εφαρμογές προγραμμάτων περιήγησης, ενώ οι ψηφιακές πλατφόρμες όπου κοινοποιούνται τα περιεχόμενα, όπως το Twitter έχουν ενημερώσει τους αντίστοιχους αλγόριθμους τους για να φιλτράρουν τα clickbaits. Ομάδες στα μέσα κοινωνικής δικτύωσης, όπως η Stop Clickbait, καταπολεμούν το clickbait παρέχοντας μια σύνοψη του άρθρου clickbait, κλείνοντας έτσι το «κενό περιέργειας». Η ερευνητική κοινότητα έχει επίσης αναπτύξει προσθήκες (plug-ins) προγράμματων περιήγησης για την αναφορά συνδέσμων clickbait, ώστε να σημειωθεί περαιτέρω πρόοδος στον τομέα με τη χρήση αλγορίθμων επιτηρούμενης μάθησης.

Ακολουθούν μερικές συμβουλές που ενδέχεται να σας βοηθήσουν να αντισταθείτε στο clickbait:

1. *Σκεφτείτε στρατηγικές όταν δεν αντιμετωπίζετε το πρόβλημα.* Σκεφτείτε μερικές ιδέες για το πώς να αντισταθείτε στο clickbait όταν *δεν* αντιμετωπίζετε το πρόβλημα. Εφαρμόστε μερικές από αυτές τις ιδέες και αξιολογήστε τα αποτελέσματα. Ξεκινήστε με τις πιο απλές, εύκολες στην εφαρμογή στρατηγικές. Μερικές φορές, ακόμη και οι μικρές αλλαγές οδηγούν σε σημαντικά αποτελέσματα.
2. *Παρατηρήστε τα μοτίβα σας και αντικαταστήστε τα με πιο προσαρμοστικά.* Ίσως μέσω μιας μικρής συλλογής δεδομένων, θα συνειδητοποιήσετε ότι τείνετε να βλέπετε απανωτά πολλά βίντεο στο YouTube (αναμφισβήτητα, μια πρακτική που αποτελεί υποτύπο του clickbait) στη δουλειά τις απογευματινές ώρες. Τι σκοπό εξυπηρετεί αυτό; Μήπως χρειάζεστε ένα

διάλειμμα; Υπάρχει κάτι άλλο που μπορείτε να κάνετε για να ανακουφίσετε την πλήξη ή την αγωνία σας;

3. *Εξετάστε το ενδεχόμενο να χρησιμοποιήσετε ορισμένα εργαλεία αποκλεισμού ιστότοπων*. Πολλά εργαλεία μπορούν να μας βοηθήσουν να σωθούμε από τον εαυτό μας. Για παράδειγμα, εάν συνεχίζουμε να ελέγχουμε έναν συγκεκριμένο ιστότοπο για ενημερώσεις ειδήσεων (και «τσιμπάμε» από το clickbait), μπορούμε να εγκαταστήσουμε ένα εργαλείο που θα περιορίσει την πρόσβασή μας σε αυτούς τους δελεαστικούς ιστότοπους κατά τη διάρκεια περιόδων που εμείς θα ορίσουμε.

Βίντεο στο YouTube πάνω στο πώς να εντοπίζετε clickbaits: https://www.youtube.com/watch?v=8IzfzoZsa-Q.

Ψευδείς διαφημίσεις/καμπάνιες (εγγενείς, πολιτικές, αποπροσανατολισμού, ινφλουένσερ μάρκετινγκ)

Ποιοι μπορούν να τις παράγουν:

Επαγγελματίες – Ερασιτέχνες – Οποιοσδήποτε.

Η επιτυχημένη διαφήμιση απαιτεί οικονομικές επενδύσεις και συχνά χρησιμοποιεί εξελιγμένες τεχνικές. Απαιτούνται ορισμένες δεξιότητες για τη δημιουργία του οπτικού ή ηχητικού περιεχομένου της διαφήμισης. Υπάρχουν πολλά ερευνητικά δεδομένα στους τομείς της νευροεπιστήμης, της ψυχολογίας και της ανάλυσης δεδομένων.

Είναι σημαντικό να σημειωθεί ότι με πολλά δωρεάν εργαλεία ή επί πληρωμή διαφημιστικά εργαλεία και εύχρηστες διαφημίσεις μέσων κοινωνικής δικτύωσης, καθώς και πλατφόρμες στόχευσης, η διαδικασία δημιουργίας διαφημίσεων καθίσταται ευκολότερη και πιο διαθέσιμη στο ευρύτερο κοινό.

Επίπεδο παραπλάνησης:

Χαμηλό – **Μέτριο** – Υψηλό – Πολύ υψηλό.

Οι περισσότερες διαφημίσεις επισημαίνονται ως επιχορηγούμενο περιεχόμενο ή τοποθετούνται με τρόπο που επιτρέπει στον καταναλωτή να γνωρίζει ότι τα μέσα συνιστούν διαφημιστικό υλικό. Ορισμένες μορφές διαφήμισης (εγγενής και διαφήμιση από ινφλουένσερς) είναι πιο δύσκολο να αναγνωριστούν. Ακόμη και όταν εντοπιστούν, οι ισχυρισμοί που παρουσιάζονται σε διαφημίσεις, μπορεί να είναι αρκετά παραπλανητικοί.

Οι νόμοι για τη διαφήμιση περιορίζουν το επίπεδο χειραγώγησης. Ωστόσο, υπάρχουν πολλές διαφορετικές μέθοδοι με σκοπό την παραπλάνηση των καταναλωτών, οι οποίες δεν επιτρέπονται βάσει της διαφημιστικής νομοθεσίας.

Σύντομη περιγραφή:

Η διαφήμιση είναι μια τακτική μάρκετινγκ που περιλαμβάνει την πληρωμή χώρου για την προώθηση ενός προϊόντος, υπηρεσίας ή σκοπού. Τα πραγματικά διαφημιστικά μηνύματα ονομάζονται διαφημίσεις. Ο στόχος της διαφήμισης είναι να προσεγγίσει άτομα που είναι πιο πιθανό να είναι πρόθυμοι να πληρώσουν για προϊόντα ή υπηρεσίες μιας εταιρείας και να τους παρασύρουν να τα/τις αγοράσουν.

Οι διαφημίσεις μπορούν να τοποθετηθούν σχεδόν οπουδήποτε, όπως σε πινακίδες στην άκρη του δρόμου, στις πλευρικές όψεις κτιρίων, σε ιστότοπους, σε ηλεκτρονικά ενημερωτικά δελτία, σε έντυπα ενημερωτικά δελτία, εντός λογαριασμών πληρωμής, σε συσκευασίες προϊόντων, σε σουπλά εστιατορίων, σε δελτία εκδηλώσεων, σε βιτρίνες καταστημάτων, στις πλευρικές αυτοκινήτων και φορτηγών, στους τοίχους των συρμών του μετρό, στα περίπτερα αεροδρομίων, σε αθλητικές αρένες, σε βίντεο στο YouTube, και σε πολλά άλλα μέρη/σημεία.

Αρχή λειτουργίας (τι κάνουν και πώς επιτυγχάνουν τον σκοπό τους):

Οι μαρκετίστες και οι διαφημιστές έχουν ένα εύρος εργαλείων για να ωθήσουν, να πείσουν, ή και να επηρεάσουν τις αγοραστικές συνήθειες ενός ατόμου. Από τα κλασικά, όπως δεδομένα που προέρχονται από δημογραφικές, γεωγραφικές και εθνογραφικές πηγές έως πιο εξελιγμένες λύσεις, όπως η αναγνώριση προσώπου, η βιομετρία της γλώσσας του σώματος ή η μικρο-στόχευση με βάση ψυχογραφικές πληροφορίες (δείτε για περισσότερες πληροφορίες:

https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie).

Η διαφήμιση μπορεί να χρησιμοποιήσει την παραπλάνηση μέσω φωτολεύκανσης [photobleaching] (απεικόνιση ψευδών και μη επιτεύξιμων αποτελεσμάτων), παραλείποντας πληροφορίες, ενέχοντας κρυφές χρεώσεις και επιβαρύνσεις, μέσω έξυπνης χρήσης μονάδων μέτρησης και προτύπων, ουσιών πλήρωσης και υπερμεγέθων συσκευασιών, καθώς και παραπλανητικών ισχυρισμών υγείας.

Οι διαφημίσεις μπορούν επίσης να υπερβάλλουν για την αξία ενός προϊόντος μέσω της χρήσης ασήμαντων, μη τεκμηριωμένων όρων, οι οποίοι βασίζονται περισσότερο σε γνώμες παρά στην πραγματικότητα, και σε ορισμένες περιπτώσεις, μέσω της έξυπνης παρουσίασης των δεδομένων.

Η **μικρο-στόχευση** είναι ένα ισχυρό διαφημιστικό εργαλείο που επιτρέπει τη στόχευση των διαφημίσεων σε συγκεκριμένες ομάδες ατόμων, ή ακόμη και μεμονωμένα άτομα, στο Διαδίκτυο. Για παράδειγμα, επιτρέπει στους πολιτικούς να στοχεύουν πολύ μικρές ομάδες ψηφοφόρων με προσαρμοσμένα μηνύματα που έχουν τη δυνατότητα να χειραγωγούν την πολιτική συζήτηση. Δείτε πώς λειτουργεί: Οι πολιτικές καμπάνιες δημιουργούν βάσεις δεδομένων σχετικά με τους ψηφοφόρους που περιλαμβάνουν πληροφορίες σχετικά με το εάν ένα άτομο έχει δικαίωμα ψήφου, πόσο συχνά ψηφίζει, τη σχέση του με το κόμμα, την ταχυδρομική του διεύθυνση, τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον αριθμό τηλεφώνου του. Έπειτα, μπορούν να ανεβάσουν αυτά τα στοιχεία των ψηφοφόρων στο Google και στο Facebook για να βρουν τα διαδικτυακά προφίλ αυτών των ατόμων και, στη συνέχεια, να διαφημιστούν ειδικά σε αυτά (πηγή: https://www.vox.com/recode/2019/11/27/20977988/google-facebook-political-ads-targeting-twitter-disinformation).

Η τεχνική **δολώματος και μεταστροφής (bait and switch)** είναι μια τακτική πωλήσεων στην οποία ένας πελάτης προσελκύεται από τη διαφήμιση ενός προϊόντος σε χαμηλή τιμή, αλλά στη συνέχεια ενθαρρύνεται να αγοράσει ένα με υψηλότερη τιμή. Ή το τέχνασμα της προσφοράς σε ένα άτομο ενός επιθυμητού πράγματος έναντι υποστήριξης (όπως πολιτική υποστήριξη), όμως, στη συνέχεια, ακολουθεί ανατροπή των προσδοκιών, καθώς το αντικείμενο είναι λιγότερο επιθυμητό σε σχέση με το υποσχόμενο (πηγή: https://www.merriam-webster.com/dictionary/bait%20and%20switch).

Το **εγγενές μάρκετινγκ (native marketing)** αναφέρεται στη χρήση πληρωμένων διαφημίσεων που ταιριάζουν με την εμφάνιση, την αίσθηση και τη λειτουργία της μορφής των μέσων στα οποία εμφανίζονται. Η λέξη «εγγενές» αναφέρεται σε αυτήν τη συνοχή του περιεχομένου με τα άλλα μέσα που εμφανίζονται στην πλατφόρμα. Αυτές οι διαφημίσεις που πιο εύκολα σε ψηφιακό περιεχόμενο, είναι πιο δύσκολο να αναγνωριστούν ως διαφημίσεις (πηγή: https://www.outbrain.com/native-advertising/).

Το **ινφλουένσερ μάρκετινγκ** είναι ένας τύπος μάρκετινγκ μέσων κοινωνικής δικτύωσης που χρησιμοποιεί προτάσεις από άτομα, οργανισμούς και ομάδες που θεωρούνται αυθεντίες ή ειδικοί σε έναν συγκεκριμένο τομέα, και έτσι επηρεάζουν τη γνώμη των ατόμων εντός του τομέα αυτού (πηγή: https://entrepreneurship.babson.edu/what-is-influencer-marketing/).

Η διαφήμιση στοχεύει στην παρουσίαση ενός προϊόντος με τον καλύτερο δυνατό τρόπο. Δίνεται κάποιο περιθώριο «προσωπικής πινελιάς» στη δημιουργική διαδικασία. Το πρόβλημα προκύπτει όταν η δραματοποίηση ξεπερνά το όριο, και έτσι οδηγεί σε εσφαλμένες αναπαραστάσεις του προϊόντος.

Η **πολιτική διαφήμιση** αποπειράται να επηρεάσει ή να σχολιάσει ένα ζήτημα που αποτελεί επί του παρόντος αντικείμενο εκτεταμένης πολιτικής συζήτησης (πηγή: https://adstandards.com.au/issues/political-and-election-advertising).
Υπάρχει ευρεία ανησυχία για τις πιθανές επιπτώσεις που μπορεί να έχει ο τρόπος που παρουσιάζονται στα μέσα ενημέρωσης το ποτό, οι τοποθετήσεις προϊόντων αλκοόλ και η διαφημίσεις αλκοολούχων ποτών στην κατανάλωση αλκοόλ, στα γενικά προβλήματα των νέων. Η τηλεόραση, το ραδιόφωνο, οι ταινίες και η ποπ μουσική συχνά αναγνωρίζονται ως πιθανές πηγές μέσω των οποίων οι νέοι μαθαίνουν για το αλκοόλ και ως πιθανές επιρροές που οδηγούν νέους ανθρώπους στον αλκοολισμό.

Παραδείγματα:
Ribena-maker fined $217,500 for misleading vitamin C ads.
Airbrushed make-up ads banned for 'misleading'.
Climbing rope not suitable for climbing.
General election 2019: Ads are 'indecent, dishonest and untruthful'.
Influencer Marketing:

- TikTok
- Instagram
- Instagram (2)

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

Παραδείγματα από τη Λιθουανία:
https://www.instagram.com/p/B74tR_UHVk3/?igshid=1nkmddft9w4w2

Μέθοδοι ελέγχου:
Facebook Political Ad Collector: Αυτό το εργαλείο εμφανίζει στους χρήστες τις διαφημίσεις στις ροές τους στο Facebook και μαντεύει ποιες είναι πολιτικές. Δείχνει επίσης στους χρήστες πολιτικές διαφημίσεις που απευθύνονται σε άλλους χρήστες. Όλες οι πολιτικές διαφημίσεις που συλλέγονται τοποθετούνται σε μια δημόσια διαθέσιμη βάση δεδομένων.
Who Targets Me: Αυτό το εργαλείο επιτρέπει στους χρήστες να δημιουργήσουν ένα ανώνυμο προφίλ και, στη συνέχεια, να συλλέξουν πληροφορίες σχετικά με τις πολιτικές και άλλες διαφημίσεις που βλέπουν, καθώς και λεπτομέρειες σχετικά με το γιατί στοχεύτηκαν με αυτές τις διαφημίσεις. Το εργαλείο μπορεί να παρέχει στους χρήστες στατιστικά στοιχεία σχετικά με το ποιος/τι τους στοχεύει, ενώ χρησιμοποιεί αυτές τις πληροφορίες για να δημιουργήσει μια βάση δεδομένων πολιτικών διαφημίσεων και στοχεύσεων.
TV News Fact Check: Το TV News Archive είναι μια πρωτοβουλία για την ανάπτυξη ενός αρχείου ψηφιακών μέσων, που κυμαίνεται από ιστοσελίδες, βιβλία και κείμενα, ηχογραφήσεις, βίντεο, εικόνες και προγράμματα λογισμικού. Ένα από τα έργα του, το «Political TV Ad Archive», είναι ένα αρχείο πολιτικών διαφημίσεων του 2016 σε συνδυασμό με έλεγχο γεγονότων από διάφορες πηγές (π.χ. Politifact, Factcheck.com).

Σάτιρα (παρωδία)

Ποιοι μπορούν να την παράγουν:

Επαγγελματίες – Ερασιτέχνες – Οποιοσδήποτε.

Παρόλο που το καλό χιούμορ και η σάτιρα συχνά παρουσιάζονται αβίαστα στον αναγνώστη, από τη μεριά του συγγραφέα απαιτείται προσπάθεια και εξάσκηση. Δεν είναι τυχαία η κοινή παραδοχή που θέλει τη σάτιρα να είναι ένας από τους πιο απαιτητικούς τύπους χιούμορ. Συνήθως, για να πάρει ένα σοβαρό θέμα και να κάνει ένα σοβαρό σχόλιο επ' αυτού με τρόπο που να θεωρείται χιουμοριστικός, ο/η συγγραφέας πρέπει να είναι πετυχημένος/-η σε αρκετούς τομείς: πρέπει να είναι έξυπνος/-η, καλά διαβασμένος/-η, ενημερωμένος/-η και σχετικός/-ή.

Επίπεδο παραπλάνησης:

Χαμηλό – Μέτριο – Υψηλό – Πολύ υψηλό.

Η σάτιρα δεν πρέπει να είναι παραπλανητική – κατά τη δημιουργία ενός σατιρικού έργου, ο/η συγγραφέας θα πρέπει να το δημιουργήσει έτσι, ώστε ο αναγνώστης να καταλαβαίνει ότι πρόκειται για σάτιρα.

Ωστόσο, υπήρξαν πολλές περιπτώσεις που ακόμη και κυβερνήσεις, πολιτικοί, μέσα μαζικής ενημέρωσης ή ειδησεογραφικά πρακτορεία ξεγελάστηκαν από σατιρικό περιεχόμενο και το παρουσίασαν ως αξιόπιστη είδηση.

Σύντομη περιγραφή:

Σάτιρα: η χρήση χιούμορ, ειρωνείας, υπερβολής, ή γελοιοποίησης για την έκθεση και επίκριση της ανοησίας ή των κακών πράξεων/προθέσεων των ανθρώπων, ιδίως στο πλαίσιο της σύγχρονης πολιτικής και άλλων επίκαιρων θεμάτων.

Η παρωδία είναι μια μορφή σάτιρας που εστιάζει στα αξιοσημείωτα χαρακτηριστικά μιας δημόσιας προσωπικότητας, καλλιτέχνη ή είδους τέχνης, αντιγράφει σκόπιμα το στυλ κάποιου διάσημου ή αντιγράφει μια συγκεκριμένη κατάσταση, καθιστώντας τα χαρακτηριστικά ή τις ιδιότητες του/της πραγματικού/-κής ατόμου/κατάστασης πιο αισθητά με χιουμοριστικό τρόπο.

Η σατιρική κωμωδία γελοιοποιεί πολιτικά ή φιλοσοφικά δόγματα, ή αλλιώς επιτίθεται σε αποκλίσεις από την κοινωνική τάξη παρουσιάζοντας ως γελοίους τους παραβάτες των προτύπων ηθικής ή συμπεριφοράς της.

Η ειρωνεία περιγράφει καταστάσεις που είναι περίεργες ή αστείες, επειδή τα πράγματα συμβαίνουν με τρόπο που φαίνεται να είναι ο αντίθετος από αυτόν που θα περιμένατε (η διαφορά μεταξύ του τι λέγεται ή γίνεται, και τι εννοείται).

Αρχή λειτουργίας (τι κάνουν και πώς επιτυγχάνει τον σκοπό της):

Η σάτιρα είναι μια ισχυρή μορφή τέχνης που μπορεί να επισημάνει τις αδυναμίες σε ορισμένες ανθρώπινες συμπεριφορές, καθώς και τα κοινωνικά ζητήματα που προκύπτουν από αυτές με τέτοιο τρόπο, ώστε να γίνουν παράλογες, ακόμη και ξεκαρδιστικές, και ως εκ τούτου, είναι διασκεδαστική και απευθύνεται σε ένα ευρύ κοινό. Η σάτιρα μπορεί επίσης να προστατεύσει τον/τη δημιουργό της από την ευθύνη για την κριτική που ασκείται σε αυτή, καθώς η σάτιρα υπονοείται και σπανίως εκφράζεται ευθέως. Με αυτόν τον τρόπο, γίνεται ένα ισχυρό εργαλείο για τους αντιφρονούντες σε δύσκολες ή πολιτικά καταπιεστικές περιόδους.

Η σάτιρα έχει υπάρξει ως τεχνική αφήγησης για αιώνες επειδή προσφέρει ένα ευφυές μείγμα κωμικής ανακούφισης (comic relief) και κοινωνικής κριτικής. Συνδυάζει την ψυχαγωγία με έναν σκοπό.
Πηγή:
https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1065&context=srhonorsprog.

Εργαλεία της σάτιρας:

1. **Υπερβολή**: υπερβολή ή ευφημισμός. Η μεγέθυνση, αύξηση ή αναπαράσταση ενός πράγματος/ανθρώπου πέρα από τα φυσιολογικά όρια, ώστε να γίνει γελοίο(ς) και να γίνουν προφανή τα λάθη του.
2. **Ειρωνία**: Η παρουσίαση πραγμάτων/ανθρώπων που είναι εκτός τόπου και χρόνου ή παράλογα/-οι σε σχέση με το περιβάλλον.
3. **Αντιστροφή**: Η παρουσίαση του αντίθετου της κανονικής σειράς (π.χ. η σειρά των συμβάντων, ιεραρχική σειρά).
4. **Παρωδία**: Η μίμηση των τεχνικών ή του στυλ κάποιου ατόμου, μέρους ή πράγματος.
5. **Κυνισμός**: Η ικανότητα να κοιτάζουμε κάτι ή κάποιον με καχυποψία, και να προσφέρουμε γνώμη αντίθετη με αυτήν της καθεστηκυίας τάξης, αποτελεί ένα εξαιρετικό εργαλείο για τη σάτιρα.
6. **Διφορούμενα σχόλια**: όταν λέγεται κάτι και εννοείται (σαφώς) κάτι άλλο.

Παραδείγματα:

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

Τηλεοπτικές εκπομπές, βίντεο:

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

Μιμίδια:

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

Παραδείγματα από τη Λιθουανία:

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

Μέθοδος ελέγχου:

Η πλεινότητα του σατιρικού υλικού έχει τα ακόλουθα κοινά χαρακτηριστικά:

- Η σάτιρα βασίζεται στο χιούμορ για να επιφέρει κοινωνικές αλλαγές.
- Ως επί το πλείστον, η σάτιρα υπονοείται. Ο/η αναγνώστης/-στρια πρέπει να «πιάσει» το χιούμορ, διαφορετικά θα του/της ξεφύγει η σατιρική φύση της γραφής.

- Η σάτιρα, τις περισσότερες φορές, δεν ασχολείται με μεμονωμένα άτομα. Αντίθετα, η σάτιρα στοχεύει στην κοινωνία στο σύνολό της, ή σε τύπους ανθρώπων εντός μιας κοινωνίας - τον πολιτικό, τον μοιχό, τον περήφανο κ.λπ.
- Το ύφος και η ειρωνεία της σάτιρας είναι υπερβολικά - μέσω της υπερβολής οι άνθρωποι μαθαίνουν για την ανοησία τους.

Τρολς, bots και ψεύτικοι λογαριασμοί

Ποιοι μπορούν να τα παράγουν:

Επαγγελματίες – **Ερασιτέχνες** – Οποιοσδήποτε.

Το επίπεδο δεξιοτήτων που απαιτείται για τη δημιουργία ενεργών ψεύτικων λογαριασμών, λογαριασμών τρολ, ή bots, ποικίλλει. Ο καθένας μπορεί να δημιουργήσει και να χρησιμοποιήσει έναν απλό ψεύτικο λογαριασμό, να χρησιμοποιήσει τεχνικές τρολ ή να αγοράσει bots για να συλλέξει κλικ και likes. Υπάρχουν διαδικτυακά εργαλεία που μπορούν να δημιουργήσουν κάθε είδους πλαστές προσωπικές πληροφορίες, οι οποίες απαιτούνται για τη δημιουργία ψεύτικων λογαριασμών – από ψεύτικα ονόματα έως προσωρινές διευθύνσεις ηλεκτρονικού ταχυδρομείου και δημιουργία και επικύρωση Αριθμού Δελτίου Ταυτότητας. Απαιτούνται κατ' ελάχιστον κάποιες δεξιότητες προγραμματισμού για τη δημιουργία bots μέσων κοινωνικής δικτύωσης.

Τα πιο επιβλαβή αποτελέσματα των ψεύτικων λογαριασμών, και των λογαριασμών τρολ ή bot, επιτυγχάνονται συνήθως από άτομα που έχουν επαγγελματικές δεξιότητες: ορισμένα bots χρησιμοποιούν προηγμένες τεχνικές τεχνητής νοημοσύνης για να φαίνονται πιο ρεαλιστικά. Ορισμένα τρολς χρησιμοποιούν συναρπαστικές τεχνικές αφήγησης και χειραγώγησης για να επιτύχουν την αντίδραση που αποζητούν. Η δημιουργία ψεύτικων προφίλ στα μέσα κοινωνικής δικτύωσης (ή η αγορά των «likes») είναι πλέον μια βιομηχανία αξίας άνω των 700 εκατομμυρίων €.

Επίπεδο παραπλάνησης:

Χαμηλό – Μέτριο – **Υψηλό** – Πολύ υψηλό.

Το επίπεδο της απάτης ποικίλλει σε μεγάλο βαθμό - ενώ ορισμένα τρολς, bots ή ψεύτικοι λογαριασμοί μπορούν να εντοπιστούν εύκολα, άλλοι μοιάζουν σε μεγάλο βαθμό με λογαριασμούς πραγματικών ανθρώπων και χρειάζεται μια πιο ενδελεχή έρευνα για να εντοπιστούν.

Μια μελέτη από το University of Reading School of Systems Engineering διαπίστωσε ότι το 30% των συμμετεχόντων θα μπορούσε να παραπλανηθεί, και ως εκ τούτου να πιστέψει ότι ένα πραγματικό άτομο διαχειριζόταν έναν λογαριασμό μέσων κοινωνικής δικτύωσης, πίσω από τον οποίον δεν βρισκόταν κανείς, παρά μόνο ένα bot. Τα τρολς συνήθως παραπλανούν άλλους χρήστες των μέσων κοινωνικής δικτύωσης δημοσιεύοντας αβλαβές περιεχόμενο, και δημιουργώντας ρεαλιστικά προφίλ και ιστορίες.

Σύντομη περιγραφή:

Ένα τρολ είναι ένα άτομο που προσπαθεί σκόπιμα να προκαλέσει αναστάτωση ή να ξεκινήσει μια διαφωνία, κυρίως δημοσιεύοντας προσβλητικά ή άσχημα πράγματα στο Διαδίκτυο (πηγή: https://www.collinsdictionary.com/dictionary/english/troll).

Ένα bot είναι μια εφαρμογή λογισμικού που εκτελεί αυτοματοποιημένες εργασίες στο Διαδίκτυο (σε αυτήν την περίπτωση ακολουθεί λογαριασμούς μέσων κοινωνικής δικτύωσης και αλληλεπιδρά με likes, σχόλια, κοινοποιήσεις ή άλλες λειτουργίες της πλατφόρμας). Τα bots συμπεριφέρονται με μερικώς ή πλήρως αυτόνομο τρόπο και συχνά σχεδιάζονται για να μιμούνται ανθρώπινους χρήστες.

Ένας λογαριασμός-μαριονέτα είναι ένας λογαριασμός που δημιουργεί κάποιος είτε για να ενεργεί με τρόπους που δεν μπορεί δημόσια, είτε για να υποστηρίξει το ίδιο του το έργο (για να ψηφίσει το δικό του υλικό και να δώσει θετικά σχόλια, επαίνους ή να διαφημίσει τη δουλειά του).

Αρχή λειτουργίας (τι κάνουν και πώς επιτυγχάνουν τον σκοπό τους):

Ορισμένες **τακτικές που χρησιμοποιούν τα τρολς** (πηγή: https://medium.com/better-humans/the-complete-guide-to-understanding-and-dealing-with-online-trolls-4a606ae25c2c):

- **Επίμονη αναπαραγωγή ψευδών ισχυρισμών**: όταν ένα τρολ λέει ένα ψέμα (είτε άμεσα είτε μέσω της χρήσης υπερβολής, παράλειψης ή της διαστρέβλωσης γεγονότων), πολλοί θα το επαναλάβουν - ακόμη και αν αυτό μπορεί εύκολα να διαψευστεί.
- **Τρολ τηλέφωνο**. Ένα τρολ σε ένα φόρουμ λέει κάτι αναληθές και ένα άλλο τρολ το παίρνει ως αλήθεια και επαναλαμβάνεται και σε άλλο φόρουμ. Τότε δημιουργείται ένα ψέμα που επαναλαμβάνεται (σαν χαλασμένο τηλέφωνο).
- **Τακτική του θαλάσσιου λιονταριού (sea-lioning)**: Επαναλαμβανόμενες και αδιάκοπες ερωτήσεις, συχνά αφότου η εν λόγω ερώτηση έχει ήδη εξηγηθεί λεπτομερώς πολλές φορές. Το θαλάσσιο λιοντάρι θα επιμείνει ότι ενεργεί καθ' όλα ευγενικά, ενώ απλά προσπαθεί να σας καθυστερήσει όσο το δυνατόν περισσότερο, καθώς και να εκτροχιάσει τη συζήτηση. Το όνομα προέρχεται από ένα πλαίσιο webcomic: http://www.muddycolors.com/wp-content/uploads/2017/12/81acd-a5b.jpg.
- **«Εμπρησμός» (flaming)**: Αναφορές σε αμφιλεγόμενα ζητήματα και σε ζητήματα που εγείρουν καβγάδες, έτσι ώστε να «πλημμυρίσει» μια δημοσίευση ή να έρθει σε δύσκολη θέση ο διαχειριστής της, ο οποίος θα κληθεί να εντοπίσει όλες αυτές τις αναφορές και να τις «αστυνομεύσει».
- **Αστυνομία γραμματικής (grammar police)**: Τα τρολς δεν νοιάζονται για το περιεχόμενο της ανάρτησής σας ή του σχολίου σας, αλλά επιμένουν ότι η ορθογραφία και η γραμματική σας πρέπει να είναι τέλειες, διαφορετικά δεν είστε σε θέση να προβάλλετε ένα ισχυρό επιχείρημα.
- **Μπούμερανγκ**: Κάποιος/-α που επιστρέφει με κάθε δυνατό μέσο για να συνεχίσει να σχολιάζει σε ένα νήμα. Ακόμα κι αν τον/την αποκλείσετε στα μέσα κοινωνικής δικτύωσης, αυτός/-ή θα δημιουργήσει νέους λογαριασμούς και θα συνεχίσει να κάνει σχόλια μέχρι να σας πείσει ότι έχει δίκιο.
- **Πλημμύρες**: Όταν κάποιος δημοσιεύει στη σελίδα σας επαναλαμβάνοντας το ίδιο πράγμα ξανά και ξανά για να καταστρέψει την ικανότητα συνομιλίας με οποιονδήποτε άλλο. Συνήθως, αποτελούνται από μηνύματα όπως «lol» ή σεξουαλικού περιεχομένου, ή απλά παιδιάστικα/χλευαστικά μηνύματα.
- **Διασπορά μίσους**: Όταν ένα άτομο χρησιμοποιεί εξαρχής «εμπρηστικές» λέξεις και προσωπικές προσβολές—ή απειλές θανάτου/βιασμού—ακόμη και όταν το νήμα ή τα προηγούμενα σχόλια δεν δικαιολογούν αυτού του είδους τις απαντήσεις. Προκαλεί σε όλους τους λογικούς σχολιαστές σας οργή και η συνομιλία μετατρέπεται αμέσως σε μάχη.

Για να χρησιμοποιηθούν τα κοινωνικά bots σε ένα συγκεκριμένο κανάλι (μέσων κοινωνικής δικτύωσης), η πλατφόρμα πρέπει να είναι προσβάσιμη μέσω μιας διεπαφής προγραμματισμού εφαρμογών (API), όπως δηλαδή, το Twitter και το Facebook. Με τη χρήση API, ένας μεγάλος αριθμός λογαριασμών bot μπορεί να ελεγχθεί ταυτόχρονα με ελάχιστη προσπάθεια. Με απλές

αναζητήσεις λέξεων-κλειδιών, σαρώνουν τα χρονολόγια του Twitter και τις αναρτήσεις στο Facebook, σε αναζήτηση συγκεκριμένων όρων ή hashtag. Μόλις βρουν αυτό που ψάχνουν, σχολιάζουν, κοινοποιούν συνδέσμους ή ξεκινούν μια ψεύτικη συζήτηση. Ή και σχολιάζουν απευθείας επί συγκεκριμένων ζητημάτων. Σε συνδυασμό με άλλα bot (σχηματίζοντας από κοινού ένα botnet), ο θόρυβός τους γίνεται ακόμα πιο δυνατός και μπορεί να παραπλανήσει τους άλλους χρήστες.

Τα κακόβουλα **bots μέσων κοινωνικής δικτύωσης** μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς (πηγή: https://www.cloudflare.com/learning/bots/what-is-a-social-media-bot/):

- **Τεχνητή ενίσχυση της δημοτικότητας ενός ατόμου ή κινήματος**: Ένα άτομο ή μια οργάνωση με εκατομμύρια οπαδούς στα μέσα κοινωνικής δικτύωσης μπορεί να θεωρηθεί σημαντική ή ισχυρή. Μια κλασική περίπτωση χρήσης των bots στα μέσα κοινωνικής δικτύωσης είναι η ενίσχυση της φαινομενικής δημοτικότητας άλλων λογαριασμών.
- **Επηρεασμός της εκλογικής διαδικασίας**: Μια μελέτη του First Monday, ενός επιστημονικού περιοδικού, διαπίστωσε ότι την ημέρα πριν από τις προεδρικές εκλογές των ΗΠΑ το 2016, έως και το 20% των πολιτικών συζητήσεων στα μέσα κοινωνικής δικτύωσης δημιουργήθηκαν από περίπου 400.000 bots μέσων κοινωνικής δικτύωσης.
- **Επηρεασμός χρηματοπιστωτικών αγορών**: Τα bots μέσων κοινωνικής δικτύωσης μπορούν επίσης να χρησιμοποιηθούν για να επηρεάσουν τις χρηματοπιστωτικές αγορές. Για παράδειγμα, οι λογαριασμοί bot μπορούν να πλημμυρίσουν τα μέσα κοινωνικής δικτύωσης με κατασκευασμένα καλά ή κακά νέα για μια εταιρεία, σε μια προσπάθεια ελέγχου της κατεύθυνσης των τιμών των μετοχών.
- **Ενίσχυση επιθέσεων ηλεκτρονικού ψαρέματος (phising attacks)**: Οι επιθέσεις ηλεκτρονικού ψαρέματος βασίζονται σε έναν/μια εισβολέα που κερδίζει την εμπιστοσύνη του θύματός του/της. Οι ψεύτικοι ακόλουθοι στα μέσα κοινωνικής δικτύωσης και η συμμετοχή στα κοινωνικά μέσα μπορούν να συμβάλλουν στο να πειστεί ένα θύμα ότι ο/η απατεώνας/-ισσα του είναι άτομο άξιο εμπιστοσύνης.
- **Διάδοση επανειλλημένων ανεπιθύμητων μηνυμάτων**: Τα bots μέσων κοινωνικής δικτύωσης χρησιμοποιούνται συχνά για παράνομους διαφημιστικούς σκοπούς μέσω προώθησης ανεπιθύμητων μηνυμάτων στον κοινωνικό ιστό με τη μορφή επανειλλημένων συνδέσμων προς εμπορικούς ιστότοπους.
- **Υπονόμευση της ελευθερίας του λόγου**: Κατά τη διάρκεια του κινήματος της Αραβικής Άνοιξης 2010-2012, οι κυβερνητικές υπηρεσίες χρησιμοποίησαν bots στο Twitter για να κατακλύσουν τις ροές του εν λόγω μέσου κοινωνικής δικτύωσης. Αυτά τα bots χρησιμοποιήθηκαν για να «καταπνίξουν» σκόπιμα τα μηνύματα διαδηλωτών και ακτιβιστών.

Περισσότερα σχετικά με τα τρολς: https://www.lifewire.com/types-of-internet-trolls-3485894.

Περισσότερα σχετικά με τα bots: https://niccs.us-cert.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=ncsam_socialmediabotsoverview_508.pdf.

Παραδείγματα:
Τρολς:

- https://www.rollingstone.com/politics/politics-features/russia-troll-2020-election-interference-twitter-916482/
- https://motherboard-images.vice.com/content-images/contentimage/32137/1459536705346993.png?resize=664:*
- https://motherboard-images.vice.com/content-images/contentimage/32137/1459536758030213.png?resize=638:*
- https://imgur.com/gallery/INtY5SB
- Τρολ-ψεύτικος λογαριασμός υποστήριξης πελατών: https://imgur.com/t/trolling/4yTQWCo

Bots:

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

Ψεύτικοι λογαριασμοί:

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

Μέθοδος ελέγχου:

Αναγνώριση και αντιμετώπιση των διαφορετικών τύπων τρολ: https://www.teamtechnology.co.uk/troll-tactics.html.

Ενώ μερικά από τα πιο προηγμένα bots μέσων κοινωνικής δικτύωσης μπορεί να είναι δύσκολο να εντοπιστούν ακόμη και από ειδικούς, υπάρχουν μερικές στρατηγικές για τον εντοπισμό ορισμένων από τους λιγότερο εξελιγμένους λογαριασμούς bot. Αυτές περιλαμβάνουν:

- Την πραγματοποίηση μια αντίστροφης αναζήτησης εικόνας για την εικόνα προφίλ τους για να δείτε εάν χρησιμοποιούν μια φωτογραφία κάποιου άλλου που υπάρχει και αλλού στο Διαδίκτυο.
- Τον έλεγχο του χρόνου των δημοσιεύσεών τους. Αν δημοσιεύουν σε ώρες της ημέρας που δεν είναι λογικές για τη ζώνη ώρας τους ή κάνουν αναρτήσεις κάθε λίγα λεπτά σε καθημερινή βάση, είναι πολύ πιθανό ο λογαριασμός αυτός να είναι αυτοματοποιημένος.
- Τη χρήση υπηρεσίας εντοπισμού bot όπως το botcheck.me που χρησιμοποιεί μηχανική εκμάθηση για τον εντοπισμό συμπεριφοράς bot. Το Cloudflare Bot Management χρησιμοποιεί επίσης μηχανική μάθηση για τον εντοπισμό bot.
- https://botometer.iuni.iu.edu.

Αναγνώριση ενός ψεύτικου λογαριασμού στα μέσα κοινωνικής δικτύωσης: https://smallbusiness.chron.com/spot-social-media-fake-46150.html.

Φιλική προσέγγιση (πλαστοπροσωπία)

Ποιοι μπορούν να τη χρησιμοποιήσουν:

Επαγγελματίες – **Ερασιτέχνες** – Οποιοσδήποτε.

Η καλή πλαστοπροσωπία απαιτεί υψηλές δεξιότητες, αλλά ακόμη και ερασιτέχνες μπορούν να προβούν σε πιστευτή πλαστοπροσωπία και να εξαπατήσουν άλλους ανθρώπους. Η φιλική προσέγγιση απαιτεί βασικές γνώσεις ψυχολογίας, καθώς και να είναι ένα άτομο καλό στην «ανάγνωση» άλλων ανθρώπων.

Επίπεδο παραπλάνησης:

Χαμηλό – **Μέτριο** – Υψηλό – Πολύ υψηλό.

Ορισμένες πλαστοπροσωπίες είναι εύκολο να εντοπιστούν. Μερικοί εγκληματίες θα προσποιηθούν ότι αντιπροσωπεύουν έναν μεγάλο οργανισμό με τον οποίο πιθανώς συνεργάζεστε. Αντίθετα, άλλοι θα προβούν σε μια πιο εμπεριστατωμένη έρευνα για εσάς και την εταιρεία για την οποία εργάζεστε και θα προσπαθήσουν να σας ξεγελάσουν, υποστηρίζοντας ότι είναι στέλεχος της εταιρείας αυτής. Είναι δύσκολο να εντοπίσετε μια τέτοια διαδικασία στο αρχικό της στάδιο, διότι δεν διαφέρει κατά πολύ από μια πραγματική φιλική σχέση. Σε μεταγενέστερα στάδια, όταν το άτομο που σας προσεγγίζει φιλικά θα προσπαθήσει να χρησιμοποιήσει αυτήν τη σχέση προς όφελός του, η τακτική αυτή γίνεται ευκολότερη στον εντοπισμό.

Σύντομη περιγραφή:

Πλαστοπροσωπία – απομίμηση ενεργειών και συμπεριφοράς κάποιου/-ας. Προσποίηση ότι είναι κάποιος/-α άλλος/-η.

Φιλική προσέγγιση – παρουσιάζεται ως φίλος (ή επίδοξος φίλος) στα μέσα κοινωνικής δικτύωσης με σκοπό να εξαπατήσει ή να εκμεταλλευτεί (δηλαδή να αποκτήσει προσωπικές πληροφορίες, φωτογραφίες, βίντεο).

Αρχή λειτουργίας (τι κάνουν και πώς επιτυγχάνουν τον σκοπό τους):

Συνήθως, χρησιμοποιούνται ψεύτικοι λογαριασμοί για πλαστοπροσωπία. Αυτοί οι λογαριασμοί μιμούνται διασημότητες, υπάρχουσες επωνυμίες ή οργανισμούς, ή και τυχαία άτομα. Μερικές φορές, οι λογαριασμοί μπορούν να μιμούνται φίλους, συγγενείς ή άλλα άτομα που βρίσκονται εντός του στενού κύκλου του υποψήφιου θύματος. Μερικές φορές, αντί να δημιουργούν ψεύτικους λογαριασμούς, οι χάκερ στοχοποιούν λογαριασμούς ανενεργών χρηστών και τους χρησιμοποιούν για να στοχεύουν φίλους που εξακολουθούν να είναι ενεργοί στην πλατφόρμα.

Κατά τη δημιουργία λογαριασμών που πλαστοπροσωπούν διασημότητες ή οργανισμούς, χρησιμοποιούνται διάφορα «παραθυράκια» που έχει η κάθε πλατφόρμα μέσων κοινωνικής δικτύωσης. Για παράδειγμα, μπορεί κανείς να μιμηθεί ένα δημοφιλές κανάλι στο YouTube, καθώς το όνομα που εμφανίζεται στα κανάλια YouTube, και οι λογαριασμοί YouTube μπορεί να διαφέρουν από το πραγματικό όνομα λογαριασμού. Στο YouTube, οι χρήστες μπορούν να στείλουν αιτήματα φιλίας στον οποιονδήποτε στην πλατφόρμα. Μόλις αυτά γίνουν αποδεκτά, τότε μπορούν να στείλουν σε αυτό το άτομο άμεσα μηνύματα. Με αυτόν τον τρόπο, κάποιος που πλαστοπροσωπεί έναν/μια διάσημο/-η YouTuber μπορεί να στείλει μηνύματα στους

συνδρομητές του/της, κάνοντάς τους/τις να νομίζουν ότι ο/η ίδιος/-α YouTuber επικοινώνησε μαζί τους.
Μερικές φορές στέλνουν τυποποιημένα μηνύματα που ενημερώνουν τους παραλήπτες ότι έχουν κερδίσει κάτι, προσκαλώντας τους να κάνουν κλικ σε συνδέσμους που ενδέχεται να οδηγήσουν σε απάτη ή σε κακόβουλους ιστότοπους. Σε άλλες περιπτώσεις, αυτοί οι απειλητικοί δρώντες αξιοποίησαν έναν συνδυασμό δημιουργικών τεχνικών πλαστοπροσωπίας, οι οποίες αύξησαν τη σοβαροφάνεια των μηνυμάτων τους και αύξησαν την πιθανότητα οι χρήστες να κάνουν κλικ στους συνδέσμους τους.
Σε περιπτώσεις φιλικής προσέγγισης, μπορεί να χρησιμοποιηθούν τόσο ψεύτικοι όσο και πραγματικοί λογαριασμοί. Αυτό όμως εξαρτάται από το μέσο στο οποίο λαμβάνει χώρα η τακτική αυτή, δηλαδή, για παράδειγμα, στα διαδικτυακά βιντεοπαιχνίδια, συνήθως χρησιμοποιούνται ψευδώνυμα που δεν παρέχουν πληροφορίες σχετικά με την πραγματική ταυτότητα του ατόμου.
Χρησιμοποιώντας πλαστοπροσωπία ή την τεχνική της φιλικής προσέγγισης, οι απατεώνες μπορούν επίσης να εξαπατήσουν τους ανθρώπους και να τους παροτρύνουν να:

- πραγματοποιήσουν μια δωρεά χρημάτων (μεταφέροντάς τα σε αυτούς ή «κάνοντας μια δωρεά»)·
- παρέχουν ευαίσθητες πληροφορίες·
- κατεβάσουν κακόβουλο λογισμικό·
- επισκεφθούν ιστότοπους-απάτη.

Μια τυπική απόπειρα πλαστοπροσωπίας από εγκληματίες στον κυβερνοχώρο περιλαμβάνει την προσποίηση ότι αντιπροσωπεύουν έναν από τους κύριους διαδικτυακούς παράγοντες στους οποίους ενδέχεται να πληρώνετε τακτικά ένα τέλος συνδρομής. Το Apple Music, το Spotify, το Netflix, και άλλα, συναντώνται συχνά. Θα λάβετε ένα επείγον μήνυμα στα εισερχόμενά σας που σας προειδοποιεί για κάποιο πρόβλημα με τον λογαριασμό σας. Και αν δεν κάνετε κλικ αμέσως, δεν θα έχουν άλλη επιλογή παρά να σας κλειδώσουν από τον λογαριασμό σας και να σας αποκλείσουν οποιαδήποτε περαιτέρω πρόσβαση. Εάν κάνετε κλικ, θα οδηγηθείτε σε έναν ιστότοπο «μαϊμού» που μοιάζει (αν δεν είναι πανομοιότυπος) με την πλαστοπροσωπημένη εταιρεία και θα σας ζητηθεί να παράσχετε τα στοιχεία σύνδεσής σας.
Μόλις «συνδεθείτε» στον ψεύτικο ιστότοπο, θα σας ζητηθεί να επιβεβαιώσετε όλα τα στοιχεία χρέωσής σας – όμως, οι εγκληματίες ζητούν πολύ περισσότερες πληροφορίες από αυτές που υποτίθεται ότι πρέπει να παρέχετε. Θα ζητήσουν την πλήρη ταχυδρομική σας διεύθυνση, τα πλήρη στοιχεία της πιστωτικής σας κάρτας, συμπεριλαμβανομένης της ημερομηνίας λήξης και του κωδικού CVV. Μερικοί θα ζητήσουν άλλα πολύ προσωπικά στοιχεία, όπως το πατρικό όνομα της μητέρας σας και το ΑΜΚΑ σας. Δηλαδή, όλα όσα χρειάζεται ένας εγκληματίας στον κυβερνοχώρο για να κλέψει την ταυτότητά σας, να ανοίξει νέους λογαριασμούς στο όνομά σας ή να διαχειριστεί μερικούς από τους άλλους λογαριασμούς σας. Άλλοι εγκληματίες στον κυβερνοχώρο θα χρησιμοποιήσουν παρόμοιες τεχνικές, ισχυριζόμενοι όμως ότι αντιπροσωπεύουν την τράπεζά σας ή τον πάροχο κινητής τηλεφωνίας σας.

Παραδείγματα:

- https://www.riskiq.com/blog/labs/youtube-impersonation-scams/
- Κουίζ «Find the Fake»: https://www.zerofox.com/find-the-fake/

Μέθοδοι ελέγχου:

Εάν κάποιος προσπαθεί να σας πείσει ότι είναι κάποιο δημόσιο πρόσωπο, λάβετε τις ακόλουθες προφυλάξεις:

- Ελέγξτε την ταυτότητα των ατόμων που επικοινωνούν μαζί σας. Μπορείτε να επιβεβαιώσετε ότι είναι αυτοί που λένε ότι είναι; Εάν όχι, ή αν δεν είστε σίγουροι, σταματήστε να απαντάτε και μην κάνετε αυτό που σας ζητούν.
- Εάν επικοινωνείτε με μια διασημότητα από τον δικό της λογαριασμό μέσων κοινωνικής δικτύωσης, εξετάστε προσεκτικά τον λογαριασμό. Περιλαμβάνει την μπλε σήμανση με το τικ που επαληθεύει ότι είναι αυτοί που λένε ότι είναι; Οι πληροφορίες στον λογαριασμό αντιστοιχούν σε πραγματικά γεγονότα που σχετίζονται με αυτήν τη διασημότητα;
- Αναζητήστε στο Google το όνομα της διασημότητας συν τη λέξη «απάτη» για να δείτε τι εμφανίζεται.
- Εξετάστε το ενδεχόμενο να αναφέρετε το ζήτημα στην ομάδα τεχνικής υποστήριξης του μέσου κοινωνικής δικτύωσης στο οποίο ήρθατε σε επαφή με αυτό το άτομο.

Ελέγξτε τα προφίλ των νέων αιτημάτων σύνδεσης ή φιλίας, ειδικά αν τα έχετε γνωρίσει μόνο μέσω διαδικτύου. Να είστε προσεκτικοί όταν συναντάτε:

- νέα προφίλ με περιορισμένο περιεχόμενο·
- κρυμμένες λίστες φίλων ή δικτύων ή λίστες γεμάτες με άτομα του αντίθετου φύλου.
- Μην στέλνετε χρήματα σε οποιονδήποτε δεν έχετε γνωρίσει ποτέ αυτοπροσώπως.
- Να είστε προσεκτικοί όταν μοιράζεστε προσωπικές φωτογραφίες ή βίντεο, ειδικά αν δεν τους έχετε γνωρίσει ποτέ αυτοπροσώπως. Οι απατεώνες πολύ συχνά εκβιάζουν τους στόχους τους χρησιμοποιώντας ευαίσθητο υλικό τους.
- Μην μοιράζεστε προσωπικά στοιχεία με κάποιον που δεν έχετε γνωρίσει ποτέ προσωπικά.
- Κάντε μια αναζήτηση εικόνων του «θαυμαστή» σας για να δείτε αν είναι αυτός που λέει ότι είναι. Χρησιμοποιήστε υπηρεσίες αναζήτησης εικόνων όπως το Google ή το TinEye.

ΠΗΓΕΣ

Αντλούμε έμπνευση από τις παρακάτω πηγές:

https://eavi.eu/ και συγκεκριμένα https://eavi.eu/beyond-fake-news-10-types-misleading-info/;

https://firstdraftnews.org/ και συγκεκριμένα https://firstdraftnews.org/latest/fake-news-complicated/;

https://euvsdisinfo.eu/;

https://newslit.org/;

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

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

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

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

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

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

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