meediaradar

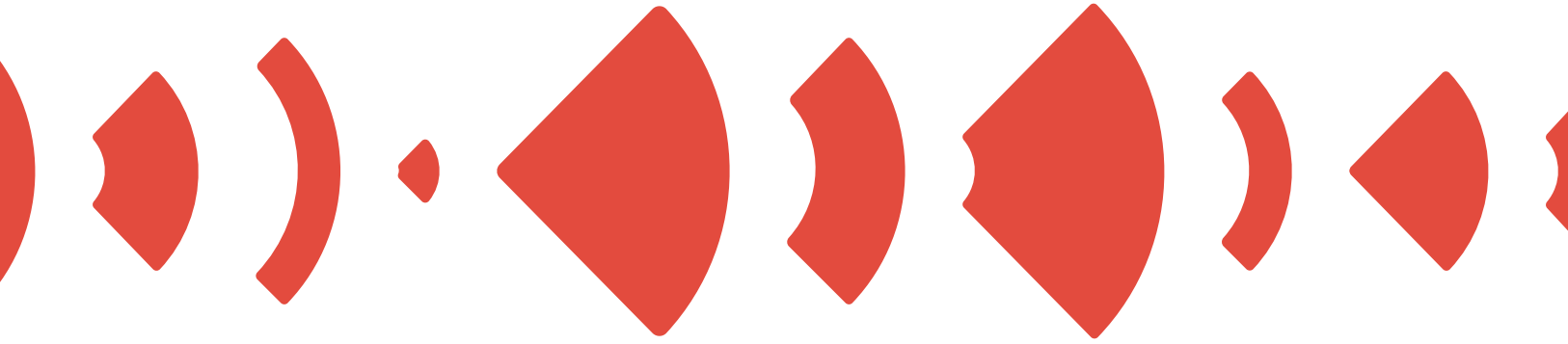
ŠVEITSI–EESTI
koostööprogramm

Kuidas orienteeruda infokülluses

Koostajad: Kateryna Botnar,
Kristiina Kaju, Maret Einmann,
Diana Poudel, Julia Rodina,
Kari Kivinen, Eesti Väitlusselts

Как ориентироваться в большом объеме информации

Составители: Катерина Ботнарь,
Кристийна Каю, Марет Эйнманн,
Диана Поудел, Юлия Родина,
Кари Кивинен, Общество дебатов Эстонии



RaRa EESTI RAHVUS-
RAAMATUKOGU

Sisukord
Оглавление

Sissejuhatus

Sissejuhatuse kirjutamine on alati keeruline, nagu ka millegi uuega alustamine. Õpikuga, mida te käes hoiate, teeme me mõlemat: alustame uut projekti, mis võib paljudele olla sissejuhatuseks meediapädevuse valdkonda.

Meediapädevuse all mõistetakse oskusi, teadmisi ja hoiakuid, mis aitavad eri kanalites esitatud teavet kriitiliselt analüüsida ja hinnata ning kujundada adekvaatseid hinnanguid. Kriitiliselt mõtlev ning analüüsiv inimene oskab eristada tõde valest ning end kriisiolukordades psühholoogiliste rünnakute eest kaitsta (Haridus- ja Teadusministeerium. Meediapädevus).

Kuigi meediapädevuse mõiste on juba hulk aega kasutusel ja kuuldud, ei tähenda see sugugi, et valdkond ei muutu. Vastupidi – see areneb kiiresti, hargneb eri suundadesse ning hõlmab nüüdseks kümmekonda teemat. Suurim saavutus on ehk see, et meediapädevus on jõudnud koolide õppekavva – läbiva teemana ja erikursusena. Ent see ei tähenda, et need, kes pole enam koolieas, jäävad infojagamisest kõrvale. Sugugi mitte! Meie sihtrühm on täiskasvanud: raamatukogude töötajad ja külastajad, õpetajad ja õppijad, aga ka kõik teised meediapädevushuvilised.

Õpiku tutvustamiseks mainime, et selles on kaheksa peatükki, igaüks oma harjutuste ning kuulamis-, vaatamis- ja lugemissoovitustega. Autorid on meediapädevuse spetsialistid Julia Rodina (MTÜ Tuleviku Meedia), Diana Poudel (TÜ), Kristiina Kaju (RaRa) ja Kateryna Botnar (RaRa), abistas Maret Einmann (RaRa). Väljaande kaks osa pärinevad Eesti Väitlusseltsi õpikust „Arutlev haridus" ning Soome MTÜ Faktabaari õppematerjalist – sel viisil on meie õpik saanud juba rahvusvaheliseks ühisloomeks.

Veidi ka projektist. See kannab nime MeediaRadar ning on mõeldud täitma olulist eesmärki muuta Eesti elanikke meedia-, digi- ja infopädevamaks. Vast olete kuulnud mitmeid riigiesindajaid väljendamas soovi, et kõik Eesti elanikud elaksid ühises inforuumis. Aga mis või milline see ühine inforuum on ja kuidas sinna jõuda? Millise trolliga sinna saab? Kas selle trolliga, mis sõitis kunagi mööda Tallinna tänavaid või selle trolli „abiga", kes ohustab teisi lugejaid oma kommentaaridega mõnes digikeskkonnas?

Kateryna Botnar, Kristiina Kaju

Введение

Написать введение всегда непросто, как и начать любое новое дело. Учебник, который вы держите в руках, выполняет обе задачи: мы начинаем новый проект, который для многих может стать введением в сферу медийной грамотности.

Медийная грамотность — это навыки, знания и убеждения, которые помогают критически анализировать и оценивать информацию, представленную в различных каналах, и формулировать адекватные суждения. Критически мыслящий, анализирующий информацию человек способен отличить правду от лжи и защитить себя от психологических атак в кризисных ситуациях (Министерство образования и науки. Медийная грамотность).

Хотя концепция медийной грамотности существует и используется уже давно, это не значит, что эта сфера не будет меняться. Напротив, она стремительно развивается, разветвляется в разных направлениях и уже охватывает десятки тем. Возможно, наибольшим достижением стало то, что медийная грамотность вошла в школьную программу — как сквозная тема и спецкурс. Но это не значит, что те, кто уже не ходит в школу, не могут изучать эту дисциплину. Вовсе нет! Наша целевая аудитория — взрослые: работники и посетители библиотек, преподаватели и учащиеся, а также все, кто интересуется медийной грамотностью.

Наш учебник состоит из восьми глав, каждая из которых содержит упражнения и рекомендации по слушанию, просмотру и чтению. Авторы — специалисты по медийной грамотности Юлия Родина (НКО Tuleviku Meedia), Диана Поудел (Тартуский университет), Кристийна Каю (RaRa) и Катерина Ботнарь (RaRa) при содействии Марет Эйнманн (RaRa). Две части издания взяты из учебника Общества дебатов Эстонии «Дискуссионное образование» и учебного пособия финской некоммерческой организации Faktabaari, получается, что наш учебник — результат международного сотрудничества.

Немного о проекте. Он называется MeediaRadar и призван решить важную задачу — сделать население Эстонии более грамотным в области медиа, цифровых технологий и информации. Наверняка вы не раз слышали, как представители государства выражали пожелание, чтобы все в Эстонии жили в едином информационном пространстве. Но что такое это общее информационное пространство и как его достичь? Увы, в интернет-среде нет ведущих к нему троллейбусов, есть только «тролли», угрожающие своими комментариями другим читателям.

Катерина Ботнарь, Кристийна Каю

Alustuseks: jäämurdmisharjutused

Et mõtteid suunata ja grupiga kontakti luua, soovitame kasutada järgmiseid soojendusharjutusi.

1. **Meediataldrik.**
   Arutelu juht palub igal osalejal kirja panna, milliseid meediakanaleid ta kasutab: TV, veebilehed, sotsiaalmeedia, ajalehed. Koostatakse ühine mõttekaart. Arutleda saab näiteks meediakanalite sarnasuste ja erinevuste üle (nt sotsiaalmeedia ja ajakirjandus), kui palju need meediakanalid igapäevaelu mõjutavad, kuidas meediakasutus muutunud on vm.

2. **Meedia: küsimused ja vastused.**
   Iga osaleja kirjutab ühe küsimuse meedia kohta. Küsimusi arutatakse rühmas ning arutelu juhile esitatakse rühma ühised küsimused.

3. **Kas see on meedias ilmunud?**
   Osalejatele antakse lugeda huvitavaid, naljakaid või kummalisi pealkirju. Harjutuse mõte on ära arvata, kas sellise pealkirjaga artikkel on kunagi päriselt ilmunud.

Harjutuste materjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Для начала: упражнения, чтобы установить контакт

Чтобы установить контакт с группой, рекомендуем использовать следующие упражнения.

1. **Медиатарелка.**
   Ведущий дискуссии просит каждого участника написать, какими медиаканалами он пользуется: телевидение, веб-сайты, социальные сети, газеты. Составляется общая информационная карта. Можно обсудить сходства и различия между медиа (например, социальными медиа и журналистикой), насколько сильно эти медиа влияют на повседневную жизнь, как изменилось использование медиа и т. д.

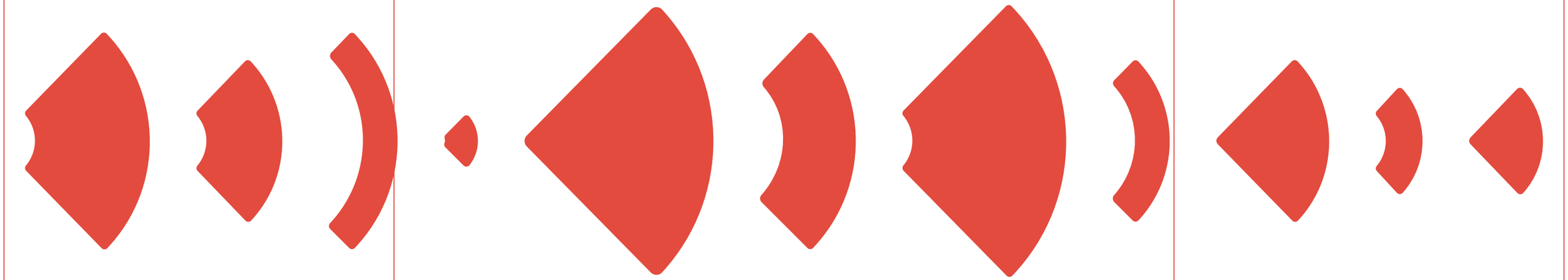
2. **Медиа: вопросы и ответы.**
   Каждый участник пишет один вопрос о медиа. Вопросы обсуждаются в группе, и группа задает ведущему дискуссии общие вопросы.

3. **«Была ли такая публикация?»**
   Участникам раздают интересные, смешные или странные заголовки для чтения. Смысл упражнения в том, чтобы угадать, действительно ли статья с таким заголовком когда-то была опубликована.

Упражнения найдете по ссылке:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

1. Kuidas saada teadlikuks meediakasutajaks

1. Как стать сознательным пользователем медиа



1. Kuidas saada teadlikuks meediakasutajaks

Maret Einmann, RaRa

Peatüki eesmärgid

- Tutvustada teadliku meedia-kasutusega seotud mõisteid.
- Õpetada mõistma meedia rolli demokraatlikus ühiskonnas.
- Selgitada teadliku meedia-kasutuse põhimõtteid.

Igapäevases virvarris ei pane me enamasti tähelegi, kui palju on meediat meie ümber või kui kiiresti jõuavad ka maailma kõige kaugemates paikades toimuvad sündmused otsepildis igaüheni. Elame meediamaailmas – meedia on igal pool ja päriseluga läbi põimunud. Nii teabe saamine, suhtlus kui ka ühiskonnas osalemine on meediast mõjutatud ning toimub info- ja kommunikatsioonitehnoloogia kaudu. Igaüks on pidevalt „sisse lülitatud" ja kättesaadav.

Millest mõtled?

Meil kõigil on õigus avaldada oma mõtteid, vaateid ja arvamusi. Nii noorte kui ka vanemate inimeste elus on oluline üksteisega suhelda ning sageli aitabki just sotsiaalmeedia seda eesmärki täita. Võimalused infot ning oma ideid ja arusaamu paljudele inimestele korraga teatavaks teha ehk sotsiaalmeedia sisu luua ja levitada on tänu erinevatele sotsiaal-meediakanalitele (nt TikTok, Instagram, Facebook jt) otsatud. On oluline, et tunneksime kanalite ja kesk-kondade võimalusi ja häid kasutustavasid.

Kõik see, kui suheldakse suurema auditooriumiga, ongi meedia. Näiteks kui jagad suhtluskeskkonnas avalikult mõnd põnevat videot, saab seda nimetada meediaks. Vaba meedia on osa demokraatlikust ühiskonnast ja mõjutab suhtlemist, kultuuri, poliitilisi hoiakuid, valikuid, majandust ja palju muud.

1. Как стать сознательным пользователем медиа

Марет Эйнманн, Национальная библиотека Эстонии

Цели главы

- Представить понятие сознательного пользования медиаресурсами.
- Научить понимать роль медиа в демократическом обществе.
- Объяснить принципы сознательного пользования медиаресурсами.

В суете повседневной жизни мы не замечаем, как много вокруг нас существует каналов медиа и как быстро события в самых отдаленных уголках мира доходят до каждого человека. Мы живем в медийном мире — медиа повсюду и переплета-ются с реальной жизнью. Доступ к информации, коммуникация и участие в жизни общества — все это зависит от медиа и осуществляется с помощью коммуникационных технологий. Каждый человек постоянно «в сети» и доступен.

О чем вы думаете?

Все мы имеем право выражать свои мысли, взгляды и мнения. И молодежи, и людям постарше важно общаться друг с другом, и социальные сети часто помогают в этом. Различные каналы социальных сетей (например, TikTok, Instagram, Facebook и т. д.) обеспечивают безграничные возможности доносить информацию, идеи и мнения до многих людей одновременно, то есть создавать и распространять контент. Важно знать о возможностях и принципах разумного пользо-вания этими каналами.

К медиа относится любое общение с широкой аудиторией. Например, если вы публично дели-тесь захватывающим видео в социальных сетях, это можно назвать медиа. Свободные медиа являются частью демократического общества и влияют на коммуникацию, культуру, политиче-ские взгляды, выбор, экономику и многое другое.

Meediateadlikkus

Kui sageli mõtleme meediat kasutades sellele, kuidas oma sõnumeid ja olulist infot kõige mõistlikumalt jagada? Missugused võivad olla tagajärjed, kui näiteks kiirustades jagada kontrollimata allika tervisesoovitusi? Kui positiivne on aga mõju, kui levitada asjakohast, vajalikku ja olulist infot? Meedial on autorid ja meedial on mõju. Mõnikord ei tea aga inimene, et ta on autor või kuidas tema loodud sisu teisi mõjutab. Tähtis on mõista, et meedia ei ole lihtsalt tehnoloogia ja sisu, mida me otsustame tarbida, vaid meedia tarbimisega kujunevad seisukohad, mis eneselegi teadvustamata mõjutavad meie valikuid, hoiakuid ja otsuseid elus. Seega on oluline analüüsivalt ja kriitiliselt mõelda, miks ja kuidas on (sotsiaal)meedia sisu loodud. Sõnumid ei ole sotsiaalmeedias sageli neutraalsed. Millal sa viimati mõtlesid, kelle vaatepunktidest või missugustel eesmärkidel sõnumid (sotsiaal)meedias kõlavad? „Maailmas, kus peaaegu igaühel on platvorm oma mõtete edastamiseks ning teaberohkus matab enda alla, vajatakse eelkõige kriitilisi mõtlejaid, kes oskavad hinnata allikate usaldusväärsust, neile allikatele toetudes ise uut sisu luua ja mõtteid loovalt edasi arendada," on öelnud professor Ilona Tragel.

Suur osa infost jõuab inimesteni ka ajakirjanduse kaudu. Ajakirjandus on see osa meediast, mis püüab võimalikult täpselt, tasakaalustatult ja objektiivselt edasi anda infot toimunud sündmustest. Ajakirjandus on faktipõhine. Demokraatlikus ühiskonnas lähtuvad ajakirjandusväljaannete toimetused info objektiivsuse ja tasakaalustatuse põhimõtetest, teevad faktikontrolli ning juhinduvad ajakirjanduseetikast. Ajakirjanduse tähtsaim ülesanne demokraatlikus riigis on pakkuda kodanikele usaldusväärset informatsiooni. Ajakirjandus ei jõua aga tänapäeval enam nii laia publikuni kui varem, kui see oli ainus võimalus avalikkusega suhelda. Sotsiaalmeedia kaudu levivad nii uudised kui ka libauudised kiiremini ja kaugemale.

Soovitusi teadlikuks meediakasutuseks

- Uuri teavet erinevatest allikatest. Loe regulaarselt mitut meediaväljaannet, otsi erinevaid vaatenurki ja tasakaalustatud infot.
- Arutle ja analüüsi. Meediat kasutades ära unusta kriitilist mõtlemist: proovi ära tunda, kas tegu on objektiivse ja tasakaalustatud meediasisuga või tahetakse inimesi panna hoopis teatud viisil käituma või midagi tegema ehk tegu on reklaami, sisuturunduse või poliitilise propagandaga.
- Kontrolli faktide õigsust ning ära jaga mitteusaldusväärset või väärinfot.
- Austa teiste inimeste privaatsust ja õigusi, oma seisukohti jagades kuula ja mõista ka teisi arvamusi, väldi vihakõnet või laimamist.
- Jälgi, et sa ei kulutaks liiga palju aega (sotsiaal)meediale. Väldi ülemäärast infotulva ja sõltuvust, mis võib põhjustada liigset väsimust, stressi või ärevust.

Сознательное пользование медиа

Как часто, пользуясь медиа, мы думаем о том, как наиболее разумно распространять сообщения и важную информацию? Какими могут быть последствия, если, например, вы поспешите поделиться медицинским советом из непроверенного источника? Насколько положительным будет эффект от распространения актуальной, нужной и важной информации? У медиа есть авторы и есть влияние. Однако иногда люди не знают, что они сами являются авторами или как созданный ими контент влияет на других. Важно понимать, что медиа — это не только технологии и контент, которые мы выбираем для потребления, но и взгляды, которые формируются благодаря медиапотреблению и влияют на наш выбор, отношение и решения в жизни, даже если мы этого не осознаем. Поэтому важно аналитически и критически подходить к вопросу о том, почему и как создается контент в (социальных) медиа. Сообщения в социальных сетях часто не нейтральны. Когда вы в последний раз задумывались, с чьей точки зрения и в каких целях создается контент? Профессор Илона Трагел сказала: «В мире, где почти у каждого есть платформа для высказывания своих идей, но они оказываются погребены под лавиной информации, нужны критически мыслящие люди, способные оценивать достоверность источников, создавать на их основе новый контент и творчески развивать идеи».

Много информации доходит до людей и через прессу. Пресса — это часть медиа, которая старается освещать события как можно более точно, сбалансированно и объективно. Она основана на фактах. В демократическом обществе редакторы изданий руководствуются принципами объективности и сбалансированности информации, проверки фактов и журналистской этики. Важнейшая задача прессы в демократическом обществе — предоставлять людям достоверную информацию. Сейчас пресса не охватывает столь широкую аудиторию, как раньше, когда она была единственным способом общения с общественностью. В социальных сетях новости, в том числе фейковые, распространяются куда быстрее и дальше.

Рекомендации по сознательному пользованию медиаресурсами

- Изучайте информацию из разных источников. Регулярно читайте различные издания, ищите разные точки зрения и сбалансированную информацию.
- Рассуждайте и анализируйте. Используя медиа, не забывайте о критическом мышлении. Старайтесь понять, имеете ли вы дело с объективным и сбалансированным контентом или людей пытаются заставить вести себя определенным образом, будь то реклама, контент-маркетинг или политическая пропаганда.
- Проверяйте факты и не делитесь ненадежной или неверной информацией.
- Уважайте частную жизнь и права других людей, выслушивайте и старайтесь понять другие мнения, когда делитесь своим, избегайте проявлений ненависти или клеветы.
- Следите за тем, сколько времени вы проводите в (социальных) медиа. Избегайте информационной перегрузки и зависимости, которые могут привести к усталости, стрессу или беспокойству.

Harjutus

Vali lühike päevakajaline sõnum värskest ajakirjandusväljaandest või sotsiaalmeediast. Loe sõnumit hoolikalt, vajadusel mitu korda. Leia, kelle huvides või kelle vaatenurgast on sinu arvates sõnum koostatud – märgista erinevatele huvidele viitavad kohad tekstis. Aruta tulemust väikeses rühmas.

Lisamaterjal

Eesti meediamaastik 2005–2024 / toim Ragne Kõuts-Klemm.

Nõmm, Tiina. Meedia- ja infopädevuste edendamise hetkeolukorra kaardistus Eesti üldhariduskoolides ning arendusvõimalused. Magistritöö.

Tankler, Lauri; Tisler, Eve. Meedia ja mõjutamine: [gümnaasiumi meediaõpik].

Vehkoo, Johanna. Valede paljastamise käsiraamat.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнение

Выберите короткое актуальное сообщение из недавнего печатного издания или социальных сетей. Внимательно прочитайте текст, при необходимости несколько раз. Подумайте, кто может быть заинтересован в этом тексте или иметь к нему отношение. Отметьте в тексте места, указывающие на этот интерес. Обсудите результаты в небольшой группе.

Дополнительный материал

Вехкоо, Йоханна. Пособие по разоблачению лжи. (Vehkoo, Johanna. Valede paljastamise käsiraamat.)

Интересная книга от финской журналистки. Пропастоп.

Нымм, Тийна. Картирование ситуации с медийной и информационной грамотностью в общеобразовательных школах Эстонии и возможности ее развития. Магистерская диссертация. (Nõmm, Tiina. Meedia- ja infopädevuste edendamise hetkeolukorra kaardistus Eesti üldhariduskoolides ning arendusvõimalused. Magistritöö.)

Танклер, Лаури; Тислер, Эве. Медиа и влияние: [учебник по медиа для гимназии]. (Tankler, Lauri; Tisler, Eve. Meedia ja mõjutamine : [gümnaasiumi meediaõpik].)

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

2. Kuidas leida meediast usaldusväärset infot

Kateryna Botnar, RaRa

Peatüki eesmärgid

- Tutvustada usaldusväärse info kriteeriume.
- Õpetada ära tundma lihtsamaid meediamanipulatsioone.
- Anda praktilisi näpunäiteid faktikontrolliks.

Miks on vaja teada usaldusväärse info tunnuseid?

Meediamaastik on pidevalt muutuv keskkond, kus üsna sageli tekivad uued suundumused ja peaaegu iga päev lisanduvad uued nn kuumad teemad ning mida suuresti mõjutab tehnoloogia areng. Paljudele tundub, et meedia on nagu võsastunud mets, millest enam läbi ei saa, mistõttu otsustatakse enam mitte kedagi või midagi usaldada ning jäädakse nn halli tsooni. Sellised inimesed on haavatavamad võrreldes nendega, kellel on oma kindel seisukoht, kuid nii ühed kui teised võivad lasta ennast petta ning jääda uskuma infot, mis tegelikult ei vasta tõele. Seepärast loetlengi allpool usaldusväärse info tunnuseid, mille tundmine on abiks ükskõik millise artikli või väljaande puhul.

Usaldusväärse info tunnused

- Info allikas. Kontrolli veebilehe aadressi õigsust, vaata rubriiki „Meist" või „Kontakt" – kas see info on lehel olemas?
- Info autor. Kas allikale on lisatud autor(id)? Kas need inimesed on päriselt olemas ja usaldusväärsed? Kas nad kirjutavad oma valdkonna teemadel?

2. Как найти в медиа достоверную информацию

Катерина Ботнарь, Национальная библиотека Эстонии

Цели главы

- Познакомить с критериями достоверной информации.
- Научить распознавать простейшие медиаманипуляции.
- Дать практические советы по проверке фактов.

Почему нужно знать признаки достоверной информации?

Медийный ландшафт — это постоянно меняющаяся среда, где довольно часто появляются новые тенденции и почти каждый день возникают новые горячие темы. На нее в значительной степени влияет развитие технологий. Многим людям средства массовой информации кажутся диким лесом, через который невозможно пробраться, поэтому они решают не доверять никому и ничему и остаются в «серой зоне». Такие люди более уязвимы по сравнению с теми, у кого есть собственное мнение. Тем не менее и тех, и других можно обмануть и заставить поверить в информацию, не соответствующую действительности. Поэтому ниже перечислены признаки достоверной информации, которые помогут при чтении любой статьи или публикации.

Признаки достоверной информации

- Источник информации. Проверьте адрес сайта, загляните в раздел «О нас» или «Свяжитесь с нами» — есть ли эта информация на странице?

- Info ajakohasus. Kas allikale on lisatud kuupäev? Valeuudised võivad käsitleda allikaid, mis on ilmunud aastaid tagasi ja pole enam ajakohased.
- Nn sisetunne. Kas informatsioon tekitab sinus tugevat reaktsiooni? Kas loodad, et info on tõene/vale või on liiga hea, et olla tõsi?
- Pealkiri ja sõnum. Kas pealkirjas on kirjavigu ja liialdusi (trükitähed, hüüumärgid)? Kas pealkiri sobib tekstiga kokku?
- Toetavad allikad. Kas on viidatud faktidele/uuringutele/raamatutele? Kas fakte on võimalik kontrollida?
- Foto- ja videomaterjalid. Kas need on autentsed, näiteks pole kontekstist välja võetud, töödeldud või manipuleeritud? Kas on võimalik, et pildid on genereeritud tehisintellekti abil?
- Nn mitteuudised. Kas tegemist võib olla nalja või satiiriga?

Igaüks meist suudab teha oma teadmiste ja oskuste tasandil faktikontrolli. Kui kahtled artikli või uudise sisus, siis kontrolli juba lugemise käigus selle usaldusväärsust. Harva, aga mõnikord siiski jagatakse uudiseid eelsalvestatud faili või kuvatõmmisena. Sellisel juhul tasub veenduda, et leht on mainitud uudise ka tegelikult avaldanud. Tavaliselt pole meil aega süveneda igasse artiklisse, mida loeme, kuid kahtluse korral soovitame korraks peatuda ning mõelda järgmistele küsimustele:

- Kas teised ajakirjanikud või väljaanded on sama teemat/sündmust kajastanud?
- Kas teemast/sündmusest kirjutatakse uudise või näiteks arvamusloo vormis? Kas teemat/sündmust võidakse kajastada kellegi huvides?
- Kas väljaanded, mida usaldad, on ka sama teemat/sündmust käsitlenud?

Tähtis on veel see, et kui sa ise pole artikli vm materjali sisus kindel, siis parem on seda teistega või avalikult mitte jagada.

Võib-olla oled ise märganud, et vahel ei sobi artikli pealkiri sisuga kokku – esimene on näiteks kutsuvam või otseselt šokeerivam, ning, nagu hiljem selgub, ei ava kuidagi artikli sisu. Selliseid pealkirju nimetatakse ka klikisöödaks või klikimagnetiks (ingl *clickbait*). Sama eesmärgi saavutamiseks mainitakse pealkirjas mõnikord mõnda teadlast (tihti ilma täisnimeta) või tuntud inimest, kes avaldab oma arvamust mõnel tema elu ja erialaga üldse mitte seotud teemal. Oluline on meeles pidada, et väärikas ja usaldusväärne arvamus on kompetentne arvamus.

- Автор информации. Указан ли автор (авторы) источника? Действительно ли эти люди существуют и можно ли им доверять? Пишут ли они на тему, в которой разбираются?
- Актуальность информации. Указана ли дата источника? В фейковых новостях могут использоваться источники, которые были опубликованы много лет назад и уже неактуальны.
- Интуиция. Вызывает ли информация у вас сильную реакцию? Надеетесь ли вы, что информация верна/неверна, или думаете, что это слишком хорошо, чтобы быть правдой?
- Заголовок и суть. Есть ли в заголовке опечатки или попытки привлечь внимание (заглавные буквы, восклицательные знаки)? Соответствует ли заголовок тексту?
- Подтверждающие источники. Есть ли ссылки на факты/исследования/книги? Можно ли проверить факты?
- Фото- и видеоматериалы. Подлинные ли они, например, не вырваны из контекста, не обработаны и не подвергнуты манипуляции? Возможно ли, что изображения сгенерированы с помощью искусственного интеллекта?
- Так называемые «неновости». Может ли это быть шутка или сатира?

Каждый может провести проверку фактов на уровне своих знаний и навыков. Если вы сомневаетесь в содержании статьи или новости, то уже в процессе чтения проверьте, можно ли ей доверять. Изредка новостями делятся в виде сохраненного файла или скриншота. В этом случае стоит проверить, что такая новость действительно была опубликована. Обычно у нас нет времени углубляться в каждую прочитанную статью, но если у вас возникли сомнения, советуем остановиться и подумать над следующими вопросами:

- Освещали ли другие журналисты или издания ту же тему/событие?
- Пишут ли о теме/событии в форме новостей или, например, статьи-мнения? Может ли тема/событие освещаться в чьих-то интересах?
- Освещали ли ту же тему/событие издания, которым вы доверяете?

Еще один важный момент: если вы сами не уверены в содержании статьи или материала, не стоит делиться ими с другими людьми или публично.

Вероятно, вы замечали, что иногда заголовок статьи не соответствует ее содержанию — он может быть завлекательным или шокирующим, но, как выясняется впоследствии, абсолютно не раскрывает, о чем говорится в статье. Такие заголовки называют кликбейтными (от англ. *clickbait*). С той же целью в заголовке иногда упоминается ученый (часто без указания полного имени) или известный человек, который высказывает мнение по вопросу, совершенно не связанному с его жизнью и профессией. Важно помнить, что ценное и заслуживающее доверия мнение — это компетентное мнение.

Harjutused

1. Loe üht neutraalset uudist ja proovi selles üles leida kõik eelmainitud kriteeriumid.
2. Loe üht valeuudist (näiteks RaRa genereeritud valeuudis BBC kuvatõmmisena) ja tee esmane faktikontroll.

Harjutuste materjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Прочитайте нейтральную новостную статью и постарайтесь найти в ней все перечисленные выше критерии.
2. Прочитайте фейковую новость и проведите первичную проверку фактов.

Упражнения найдете по ссылке:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Lisamaterjal

Caulfield, Mike; Wineburg, Sam. Verified : how to think straight, get duped less, and make better decisions about what to believe online.

The critical thinking about sources cookbook / edited by Sarah E. Morris.

Palumbo, Matt. Fact-checking the fact-checkers : how the left hijacked and weaponized the fact-checking industry.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Дополнительный материал

Медиадискурс : анализ медиатекстов. Исследования медиа и культуры / Д. Матисон; [перевод с английского: О. В. Гритчина]

Медиа — адекватное публицирование: содержание, концепция публикаций и презентаций / Ганс В. Гиссен ; [перевод с немецкого: С. С. Димитров]

Медиа: теория массовых коммуникаций / Г. Г. Почепцов

ERR: Meediataip. Юлия Тислер: для многих то, что показано в видеоролике, означает безусловную правду.

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

3. Demagoogia võtted ja saladused

Eesti Väitlusselts

Peatüki eesmärgid

- Õpetada ära tundma erinevaid demagoogiavõtteid.
- Tutvustada demagoogiavõtete kasutamist meedias.

Ajakirjanduses ja sotsiaalmeedias kirjutatul on kindel eesmärk ja soovitakse edasi anda mingit mõtet või ideed. Sageli püütakse oma seisukohti väljendada erinevaid demagoogiavõtteid kasutades. Demagoogia äratundmiseks ja vältimiseks tuleb neid võtteid tunda ja teada, kuidas neid kasutatakse. Alljärgnevalt tutvustame demagoogia selgitamist Eesti Väitlusseltsi koostatud õpikus „Arutlev haridus".

Sihilikult vigaste argumentide esitamist nimetatakse ka demagoogiaks ja tõesena tunduvat vigast loogikat demagoogiavõteteks. Üks võimalus vastaste argumenti ümber lükata ongi tunda ära mõni selles peituv demagoogiavõte ja see kuulajale välja tuua. Samas ei ole demagoogiavõtted midagi erilist – tegemist on vaid vigase loogikaga, mille saab ära tunda ja millele vastu vaielda ka ilma konkreetse võtte nime teadmata. Selle nimekirja tundmine ei ole mingi imerelv. Väitlus, mis taandub teineteise poole ladinakeelsete sententside pildumiseks („Teie argument on puhas *ad hominem*" – „Aga teie oma on *post hoc, propter hoc*") ei ole tavaliselt eriti sisuline.

Poliitikas tihti kasutatav hüüdlause stiilis „Minu oponendi jutt on ju täielik demagoogia! Ja nüüd minu enda mõtete juurde!" on ise paras demagoogia just sellepärast, et ei seletata ära, milles oponendi loogikaviga seisneb, vaid nimetatakse seda nii ilma ühegi põhjenduseta. Selle võtte nimi on sildistamine. Seega on meie soovitus kasutada sõna „demagoogia" ja ladinakeelseid liigitusi pigem harva ning keskenduda rohkem loogikavigade lahtiseletamisele.

3. Приемы и секреты демагогии

Общество дебатов Эстонии

Цели главы

- Научить распознавать различные демагогические приемы.
- Познакомить с использованием демагогических приемов в СМИ.

Тексты, опубликованные в печатных изданиях и социальных сетях, имеют конкретную цель и призваны донести до читателя определенную мысль или идею. Авторы часто пытаются выразить свои взгляды, используя различные демагогические приемы. Чтобы распознать демагогию и научиться избегать ее, необходимо знать эти приемы и то, как они используются. Приведем объяснение демагогии из учебника «Дискуссионное образование», составленного Обществом дебатов Эстонии.

Представление заведомо ошибочных аргументов называется демагогией, а ошибочная логика, выдаваемая за истинную, — демагогическими приемами. Один из способов опровергнуть аргументы оппонента — распознать в них демагогический прием и указать на него слушателю. В то же время в демагогии нет ничего особенного — это просто ошибочная логика, которую можно распознать и оспорить, даже не зная названия конкретного приема. Знание этого списка не панацея. Спор, где оппоненты бросают друг в друга латинскими сентенциями («Ваш аргумент — чистейший *ad hominem*» — «А ваш — *post hoc*, *propter hoc*»), обычно не очень содержателен.

Часто использующееся в политике утверждение: «Речь моего оппонента — сплошная демагогия! А теперь перейдем к моим мыслям!» — само по себе является демагогией именно потому, что не объясняет, в чем заключается изъян в логике оппонента, а называет ее ошибочной безо всякого обоснования. Этот прием называется

Valik demagoogiavõtteid

LÄBI AEGADE…
(*Argumentum ad antiquitatem*)

Mida tähendab:
argument traditsiooni abil ehk öeldakse, et midagi on kogu aeg ühtemoodi olnud ja seepärast peab see ka nii jääma.

Näited:
„Aegade algusest peale on mehed teinud tööd ja naised hoolitsenud perekonna eest.” „Riik peab toetama teatrit, sest seda on Eestis tehtud juba 1865. aastast saadik.”

Kuidas tegeleda:
see, et midagi ajalooliselt on toetatud, ei tee ideed veel õigeks. Orjandus, nõidade põletamine ja mõte, et maakera on lapik, on kõik ajaloolised ja pika traditsiooniga ideed ning sellest hoolimata absoluutselt valed.

VAATA, MILLINE SA ISE OLED!
(*Argumentum ad hominem*)

Mida tähendab:
otsetõlkes argument inimese vastu ehk siis see, kui sisulise argumendi asemel rünnatakse selle esitajat.

Näited:
„Oponent soovib anda naistele rohkem õigusi ainult selle pärast, et ta on ise ka naine.” „Kohtualune on üdini paha ja ebameeldiv tegelane, järelikult tuleb ta mõista süüdi.” „See, mida vastane rääkis, on üks poliitiku jutt ja me ju teame, et poliitikud on väljas ainult enda huvide eest.”

Kuidas vastu vaielda:
seletada, et inimese isikul ei ole enamasti (ja väitluses veel eriti) midagi pistmist tema esitatavate argumentide sisuga. Kui rünnatakse ainult isikut, siis argumendi sisu jääb tähelepanuta ja seega võib eeldada, et vastasel pole selle vastu midagi öelda.

KIIRE ÜLDISTUS

Mida tähendab:
mingi üksik näide üldistatakse tervele grupile või vastupidi: hinnatakse grupi liikmeid sarnaste stereotüüpidena.

Näited:
„Naised on üldiselt nõrgemad kui mehed, seetõttu ei tohi nad osaleda samadel spordialadel kui mehed.” „Ameeriklased, keda me Euroopas turistidena kohtame, tunduvad rumalad, järelikult ongi USA üks rumalate inimeste riik.”

Kuidas tegeleda:
näidata, et ei ole põhjust teha kiireid üldistusi ja et vahed gruppide sees on tihti suuremad kui erinevate gruppide vahel. Näiteks, et väide: „Kõik mustanahalised on laisad” ei pea paika, sest mitmed mustanahalised, näiteks USA president Barack Obama, ei ole üldse laisad.

Demagoogia kohta saab põhjalikumalt lugeda näiteks Eesti Väitlusseltsi õppematerjalide lehelt argument.ee: Haridus > Õppematerjalid > Demagoogia.

навешиванием ярлыков. Поэтому рекомендуем реже использовать слово «демагогия» и латинскую классификацию, а больше внимания уделять развенчанию логических ошибок.

Некоторые демагогические приемы

С НЕЗАПАМЯТНЫХ ВРЕМЕН…
(*Argumentum ad antiquitatem*)

Что это значит:
обращение к традиции, то есть утверждение, что что-то всегда происходило определенным образом, а потому так и должно остаться.

Примеры:
«С незапамятных времен мужчины работали, а женщины заботились о семье». «Государство должно поддерживать театр, потому что в Эстонии оно делает это с 1865 года».

Что возразить:
тот факт, что какая-то идея существовала исторически, еще не делает ее правильной. Рабство, сжигание ведьм и идея о том, что Земля плоская, — все это исторические идеи с долгой традицией, которые, тем не менее, абсолютно ошибочны.

ПОСМОТРИ НА СЕБЯ!
(*Argumentum ad hominem*)

Что это значит:
буквально «аргумент против человека», т. е. вместо критики аргумента по существу — нападение на человека, приводящего аргумент.

Примеры:
«Оппонент хочет дать больше прав женщинам только потому, что она тоже женщина». «Подсудимый — плохой и неприятный человек, поэтому он должен быть осужден». «Слова оппонента — это просто очередная болтовня политика, а мы знаем, что политики преследуют только свои интересы».

Что возразить:
объясните, что личность человека обычно (а тем более в дебатах) не имеет никакого отношения к сути приводимых им аргументов. Когда нападают на человека, суть аргументов игнорируется, и можно предположить, что оппоненту нечего сказать в ответ.

БЫСТРОЕ ОБОБЩЕНИЕ

Что это значит:
один пример обобщается на всю группу или, наоборот, участники группы оцениваются на основе стереотипов.

Примеры:
«Женщины, как правило, слабее мужчин, а потому не могут заниматься теми же видами спорта». «Американские туристы, которых мы встречаем в Европе, кажутся глупыми, поэтому США — страна глупых людей».

Что возразить:
покажите, что нет оснований делать огульные обобщения и что различия внутри групп зачастую больше, чем между группами. Например, утверждение «Все чернокожие люди ленивы» — это неправда, потому что многие чернокожие люди, например президент США Барак Обама, вовсе не ленивы.

Подробнее о демагогии можно прочитать, например, на странице учебных материалов Общества дебатов Эстонии argument.ee: Образование > Учебные материалы > Демагогия.

Harjutus

Rühmatöö: argumendi koostamine

Moodustatakse neljaliikmelised rühmad, kus iga osaleja saab paberilehe. Koolituse läbiviija annab ühe teema. Iga osaleja kirjutab lehele teemaga seotud väite. Seejärel annavad osalejad paberilehe edasi enda kõrval istujale. Saadud paberile kirjutavad osalejad väitega sobiva seletuse. Tegevus kordub argumendi järgmiste osadega (tõestus ja järeldus). Ring liigub pidevalt samas suunas. Kui argument on valminud, antakse see tagasi inimesele, kes algse väite kirjutas. Rühmades arutatakse, kas väite algne autor oleks argumendiga samamoodi jätkanud ning kuidas saaks argumenti täiendada.

Rohkem ülesandeid leiab lehelt argument.ee:

Lisamaterjal

Eesti Väitlusselts. Demagoogia.

ERR: Meediataip. Demagoogia.

Karolin, Anna. Väitlusseltsi kolumn: 15 demagoogiavõtet prügi väljaviimise näitel.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнение

Работа в группах: составление аргумента

Формируются группы по четыре человека, каждый участник получает лист бумаги. Ведущий тренинга задает одну тему. Каждый участник пишет на листе связанное с ней утверждение. Затем участники передают лист бумаги человеку, сидящему рядом. На полученном листе участники пишут пояснение к утверждению.
Это действие повторяют, чтобы добавить следующие части аргумента (доказательство и вывод). Лист все время передают в одном и том же направлении. Когда аргумент готов, его вновь передают участнику, который написал первоначальное утверждение. Группы обсуждают, продолжил ли бы изначальный автор утверждения аргументацию в том же духе и как можно дополнить аргумент.

Упражнения найдете по ссылке:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Дополнительный материал

ERR: Meediataip. Чем факт отличается от мнения?

ERR: Meediataip. Демагогия.

Каролин, Анна. Колонка Общества дебатов: 15 демагогических приемов на примере уборки мусора.

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

4. Meediatekstide liigid ja eesmärgid

Kristiina Kaju, RaRa

Peatüki eesmärgid

- Anda teadmisi erinevatest artikli-tüüpidest ajakirjanduses.
- Õpetada ära tundma meediatekstide erinevaid eesmärke.
- Õpetada meediatekste kriitiliselt lugema ja hindama.

Ajakirjanduse roll

Ajakirjandus ja meediaväljaanded on olulised igas ühiskonnas. Ilma ajakirjanike ja uudismeediata puuduks meil „aken maailma" ning meil oleks väga vähe võimalusi teada saada, mis toimub meie kogukondades või kaugemal.

Ajakirjanduse ja sotsiaalmeedia mitmekesisus pakub lugejatele rohkesti informatsiooni, kuid samal ajal toob kaasa ka mitmeid ohte. Oluline on mõista, kuidas erinevates žanrites võivad esineda manipulatsiooni-võtted, mis mõjutavad meie arusaamu ja otsuseid.

Oluline info liikumise ja vahetamise kanal on sotsiaal-meedia. Ka seal levivad uudised, info sündmuste kohta jne. Kui ajakirjanduses on ajakirjaniku töö osa info ja faktide kontrollimine, et pakkuda oma lugeja-tele tõest teavet, siis sotsiaalmeedias saab postitusi luua ja jagada igaüks ilma infot eelnevalt kontrollimata. Ning seejuures levib (vale)info sotsiaalmeedias väga suure kiirusega. Tasub jälgida, kust pärineb uudis: kas mõnelt sotsiaalmeediaplatvormilt või ajakirjandus-väljaandest.

4. Типы и задачи медиатекстов

Кристийна Каю, Национальная библиотека Эстонии

Цели главы

- Дать начальные знания о различных типах статей в прессе.
- Научить распознавать различные цели медиатекстов.
- Научить критическому чтению и оценке медиатекстов.

Роль прессы

Пресса и средства массовой информации играют важную роль в жизни любого общества. Без журналистов и новостных изданий у нас не было бы «окна в мир», и мы практически не знали бы о том, что происходит в наших сообществах и за их пределами.

Разнообразие прессы и социальных сетей обе-спечивает читателей огромным количеством информации, но в то же время несет в себе и множество рисков. Важно понимать, какие приемы манипуляции, влияющие на наши представления и решения, встречаются в различных жанрах.

Социальные сети — важный канал передачи информации и обмена ею. Здесь также распро-страняются новости, информация о событиях и т. д. В то время как в прессе частью работы журналиста является проверка информации и фактов, чтобы дать читателям правдивую картину, в социальных сетях посты может создавать и распространять любой человек, и информация не всегда проверяется. При этом (ложная) инфор-мация распространяется в социальных сетях с огромной скоростью. Стоит следить за тем, откуда пришла новость: из социальных сетей или журналистского издания.

Uudis

Uudis on ajakirjanduslik tekst, mis kajastab aktuaalseid, hiljuti aset leidnud sündmusi või avalikus elus juhtunut eesmärgiga informeerida lugejat kiiresti ja objektiivselt. Uudises edastatakse uut, märkimist väärt teavet millegi kohta.

Uudise omadused:

- rahuldab infovajaduse;
- vastab põhiküsimustele kes, mis, millal, kus, miks, kuidas;
- annab teada ühiskonnale olulistest protsessidest;
- objektiivsus – ajakirjanik ei esita oma arvamusi või järeldusi, vaid fakte;
- täpsus – faktid on õiged ja kontrollitud;
- tasakaalustatus – sõna saavad kõik teemaga seotud osapooled;
- sõltumatus – autor ei sõltu poliitilistest, majanduslikest või isiklikest mõjutustest, vaid keskendub tõesele ja tasakaalustatud informatsioonile;
- erapooletus – lugejale antakse kogu info, mis olemas on, ja ta teeb ise lõppjärelduse;
- neutraalsus ja emotsioonivabadus.

Uudise keel on tasakaalukas ning ei ürita veenda, vaid edastab informatsiooni; tekst on sõnastatud ratsionaalselt, asjalikult, täpselt ja emotsioonideta.

Mida lähemal toimuvat sündmust uudis kajastab, seda suurem mõju sellel on ja seda suurem on huvi kajastatud teema vastu. Üks uudise liike on reportaaž – sündmuse detailne ja visuaalne kajastus, mis pakub lugejale kohaloleku tunnet.

Kui uudiste puhul eiratakse tasakaalustatust, erapooletust jm aspekte, kaotab väljaanne oma usaldusväärsuse.

Mida tähele panna

Uudised püüavad sageli lugejate tähelepanu šokeerivate pealkirjade, üledramatiseerimise ja emotsioonidel mängimisega. See võib kaasa tuua tasakaalustamata kajastuse, kus esitletakse vaid ühepoolset infot, jättes alternatiivsed vaatenurgad käsitlemata. Samuti on valeuudised ja -info olulised ohud, mida tuleb kriitiliselt hinnata.

Reportaažid võivad lugejate arvamust kallutada, kasutades visuaalseid detaile nagu fotod või stiilivõtteid nagu kõnekujundid, mis kutsuvad esile tugevaid emotsioone. Lisaks võib ajakirjaniku isiklik subjektiivsus mõjutada faktide esitamist, muutes sündmuste kajastuse ebatäpseks või kallutatuks.

Jens Stoltenberg sai Norra rahandusministriks

Jens Stoltenberg sai Norra rahandusministriks. ERR, 4. veebr 2025.

Arvamusartikkel

Arvamusartikkel väljendab kirjutaja isiklikke seisukohti ja sisaldab konkreetse teema analüüsi.

Arvamusartikli omadused:

- subjektiivne, autori arvamusele toetuv, kuid siiski argumenteeritud ja põhjendatud seisukoht;
- sisaldab argumente ja põhjendusi, sageli viidates faktidele ja allikatele;
- pakub analüüsi ja algatab arutelu.

Mida tähele panna

Arvamusartiklid võivad sisaldada faktide väänamist või teadlikku valeinfot, mis eksitab lugejaid. Samuti võib autoriteedi argument ehk tuntud isikute seisukohtade rõhutamine varjutada argumentide tegeliku tugevuse, jättes kriitilise analüüsi tahaplaanile.

Oliver Laas: juturobotid ja kriitiline mõtlemine

Oliver Laas: juturobotid ja kriitiline mõtlemine. ERR, 3. veebr 2025.

Новость

Новость — это журналистский текст, в котором сообщается об актуальных, недавно произошедших событиях либо событиях общественной жизни с целью быстро и объективно проинформировать читателя. Новость передает новую, заслуживающую внимания информацию о чем-либо.

Характеристики новости:

- удовлетворяет потребность в информации;
- отвечает на основные вопросы: кто, что, когда, где, почему, как;
- информирует о важных для общества процессах;
- объективность — журналисты излагают не свои мнения или выводы, а факты;
- точность — факты верны и проверены;
- сбалансированность — все участвующие стороны имеют возможность высказаться;
- независимость — у автора нет политических, экономических или личных мотивов, он сосредоточен на правдивой и взвешенной информации;
- беспристрастность — читателю предоставляется вся доступная информация, и он делает собственные выводы;
- нейтральность и свобода от эмоций.

Язык новостей сбалансирован и не пытается убедить, а передает информацию; текст сформулирован рационально, по делу, точно и без эмоций.

Чем ближе происходящее событие отражает новость, тем большее влияние она имеет и тем выше интерес к освещенной теме. Одним из видов новостей является репортаж — подробный и наглядный отчет о событии, который создает у читателя ощущение присутствия.

Если в новостях игнорируется баланс, беспристрастность и другие аспекты, издание теряет доверие к себе.

На что стоит обратить внимание.

Новости часто стараются привлечь внимание читателей шокирующими заголовками, излишней драматизацией и игрой на эмоциях. Это может привести к неравномерному освещению событий, когда транслируются односторонние мнения, а другие точки зрения игнорируются. К важным рискам, которые необходимо критически оценивать, относятся также фейковые новости и фейковая информация.

Репортажи могут склонять мнение читателей в определенную сторону, используя визуальные детали, например фотографии, или стилистические приемы, например фигуры речи, которые вызывают сильные эмоции. Кроме того, личная субъективность журналиста может повлиять на изложение фактов, сделав освещение событий неточным или необъективным.

Сергей Метлев: не ожидал, что в таком возрасте можно получить такую высокую награду

Сергей Метлев: не ожидал, что в таком возрасте можно получить такую высокую награду. ERR, 5 февраля 2025.

Статья-мнение

Статья-мнение выражает личное мнение автора и содержит анализ конкретной темы.

Характеристики статьи-мнения:

- субъективное высказывание, основанное на мнении автора, но тем не менее аргументированное и обоснованное;
- содержит аргументы и обоснования, часто ссылается на факты и источники;
- предлагает анализ и побуждает к дискуссии.

На что стоит обратить внимание.

Статьи-мнения могут содержать искажения фактов или намеренную дезинформацию, вводящие читателей в заблуждение. Кроме того, аргумент от авторитета, то есть акцент на позиции известных личностей, может затмить реальную силу аргументов, оставляя критический анализ на втором плане.

Juhtkiri

Juhtkiri on toimetuse ametlik seisukohavõtt aktuaalsel ja olulisel teemal. See esindab väljaande ühtset arvamust, sageli on autoriks kollektiiv või peatoimetaja.

Juhtkirja omadused:

- autor on tavaliselt anonüümne või esindab toimetust kui tervikut;
- käsitleb ühiskondlikult olulist küsimust, pakkudes väljaande seisukohta või analüüsi;
- eesmärk on mõjutada avalikku arvamust, suunata diskussiooni või pakkuda lahendusi probleemidele;
- stiil on tõsine ja ametlik, kuid selgelt argumenteeritud ja tihti kaasa mõtlema kutsuv.

Juhtkirja funktsioonid:

- seletamine – mingi sündmuse selgitamine ja selle arengu toetamine; esitab sündmuse põhjused, toob välja kaasnenud muutused ja kuidas nende mõjul hakkab elu muutuma. Oluline on esitada faktid ja ideed objektiivselt, mitte toetuda isiklikule kogemusele või hinnangule;
- veenmine – veenda kedagi midagi tegema või muutma ning anda selleks juhtnööre, aidata lugejail jõuda mingile lahendusele või otsusele;
- kritiseerimine – juhtkirja ülesanne pole üksnes kritiseerida, vaid aidata ka elu parandada. Kriitika peaks olema pigem edasiviiv;
- kiitmine – juhtkirjad pole mitte ainult vastuseisu väljendamiseks, on ka võimalus õnnestumistele ja edusammudele tähelepanu pöörata;
- meelelahutamine – juhtkiri ei pea alati olema tõsine, see võib olla ka kergekaalulisem ja humoorikam;
- tähelepanu juhtimine – väljaanne võib avalikkuses esile kutsuda reaktsioone ja käivitada uusi programme või aktsioone, näiteks teha ettepanekuid kutsuda tagasi poliitilisi liidreid, luua komisjone, ehitada koole, puhastada tänavaid jne.

Mida tähele panna

Juhtkirjad väljendavad väljaande seisukohti, kuid võivad kujundada lugejate arvamusi ühepoolselt, jättes alternatiivsed perspektiivid käsitlemata. Lisaks võivad toimetuse ärilised või poliitilised huvid mõjutada juhtkirja sisu ja tonaalsust.

JUHTKIRI | Hiina näitab tehisaruga võimu (92)

Juhtkiri : Hiina näitab tehisaruga võimu. Eesti Päevaleht, 30. jaan 2025.

Intervjuu

Intervjuu on dialoogiline žanr, kus ajakirjanik küsitleb inimest, et saada infot, arvamusi või lugusid. Toob esile intervjueeritava isikliku vaatenurga ja kogemused.

Intervjuu omadused:

- intervjueeritava suhtes viisakas ja erapooletu;
- ajakirjanik esindab lugejaskonda, auditooriumi;
- intervjueeritava öeldu on edasi antud sõna-sõnalt;
- toimetatud ja intervjueeritavaga kooskõlastatud;
- intervjueerija küsib või juhib tähelepanu lugejatele huvi pakkuvatele teemadele.

Mida tähele panna

Intervjuude puhul võib kaduda kontekst, kui tsitaadid on sellest välja rebitud viisil, mis moonutab intervjueeritava tegelikke seisukohti. Lisaks võivad suunavad küsimused kallutada vastuseid ja viia intervjuu soovitud suunas, vähendades selle objektiivsust.

Teater süstib tolerantsusvedelikku ühiskonna veeni

Ehasalu, Peep; Toikka, Aare. Teater süstib tolerantsusvedelikku ühiskonna veeni. Sirp, 24. jaan 2025.

Каупо Мейель: эстонская литература – это Чак Норрис

Каупо Мейель: эстонская литература – это Чак Норрис. ERR, 30 января 2025.

Редакционная статья

Редакционная статья — это официальная позиция редакции по актуальному и важному вопросу. Она представляет собой единое мнение издания, автором которого часто является коллектив или главный редактор.

Характеристики редакционной статьи:

- автор обычно анонимный или представляет редакцию в целом;
- рассматривает социально значимую проблему, предлагая точку зрения издания или анализ;
- цель — повлиять на общественное мнение, направить дискуссию или предложить решение проблем;
- стиль серьезный и формальный, но четко аргументированный и часто призывающий к размышлениям.

Функции редакционной статьи:

- пояснение — объяснение события и поддержка его хода; объясняет причины события, описывает произошедшие изменения и то, как под их влиянием изменится жизнь. При этом важно объективно излагать факты и идеи, а не полагаться на личный опыт или суждения;
- убеждение — попытка убедить кого-либо сделать или изменить что-либо, а также дать указания, как это сделать, помочь читателю прийти к решению;
- критика — роль редакционной статьи не только в том, чтобы критиковать, но и в том, чтобы помочь улучшить жизнь. Критика должна быть скорее конструктивной;
- похвала — редакционная статья не только способ выразить свое несогласие, но и возможность подчеркнуть успехи и прогресс;
- развлечение — редакционная статья не всегда должна быть серьезной, она может быть легкой и юмористической;
- привлечение внимания — публикация может вызвать реакцию общественности и инициировать новые программы или действия, например внести предложение об отставке политических лидеров, создании комиссий, строительстве школ, уборке улиц и т. д.

На что стоит обратить внимание.

Редакционные статьи выражают точку зрения издания, но могут склонять мнение читателей в определенную сторону, оставляя без внимания альтернативные точки зрения. Кроме того, на содержание и тон редакционной статьи могут влиять коммерческие или политические интересы редакции.

Интервью

Интервью — это жанр диалога, в котором журналист беседует с человеком, чтобы получить информацию, мнение или историю. Интервью выявляет личные взгляды и опыт интервьюируемого.

Характеристики интервью:

- вежливость и беспристрастие в отношении интервьюируемого;
- журналист представляет читателей, аудиторию;
- все сказанное интервьюируемым приводится дословно;
- интервью редактируется и согласовывается с интервьюируемым;
- интервьюер задает вопросы или указывает на темы, интересующие читателей.

На что стоит обратить внимание.

Интервью может лишиться контекста, если цитаты вырваны из него таким образом, что искажают реальное мнение интервьюируемого. Кроме того, наводящие вопросы могут исказить ответы и направить интервью в желаемое русло, снизив его объективность.

Uuriv ajakirjandus

Uuriv ajakirjandus keskendub uuritud teemadele sügavuti ja toob sageli päevavalgele varjatud või keerukaid aspekte.

Omadused:

- põhjalik faktide kogumine, intervjuud ja dokumentide uurimine;
- seotud ühiskondlikult oluliste teemadega;
- pikem formaat, põhjalik taustaanalüüs.

Mida tähele panna

Uurivas ajakirjanduses on keskne allikate usaldusväärsus, sest valesti tõlgendatud või kallutatud info võib viia väärate järeldusteni. Samuti võib esineda hirmutamistaktikaid, kus rõhutatakse emotsionaalseid aspekte faktide arvelt.

Kuidas Twitterist sai Elon Muski propagandamasin?

Kuidas Twitterist sai Elon Muski propagandamasin? Propastop, 9. dets 2024.

Kuidas ennast kaitsta

- Ole kriitiline lugeja. Ära võta infot automaatselt tõena. Küsi endalt: kes selle info avaldas? Miks seda tehakse? Millised tõendeid ja fakte esitatakse?
- Arenda meediakirjaoskust. Harjuta ennast ära tundma erinevaid ajakirjandusžanreid ja nende võimalikke manipulatsioonimeetodeid. Õpi, kuidas uudised sünnivad, millised on nende reeglid ja kus võivad tekkida probleemid.
- Loe ametlikke allikaid. Kui ühiskonnas kerkib üles mõni nn kuum teema, siis on kindlam lugeda ametlikke infoallikaid, avalikku meediat ja arutatavas valdkonnas pädevate inimeste ehk spetsialistide arvamusi. Võib-olla olete märganud nähtust: kui üles kerkib mõni ühiskonnakriitiline teema, mis pälvib rohkelt kajastusi, siis ilmuvad ka eksperdid, kes kipuvad oma arvamust jagama. Infouputuses on raske vahet teha tõe ja eksitava info vahel. Me väsime arvamuste ja uudislugude pidevast voost, uudiste rohkest lugemisest-kuulamisest-vaatamisest ning muutume ükskõikseks. Selle vältimiseks on oluline leida endale uudiste lugemiseks kindel aeg.

ИНТЕРВЬЮ ⟩ Канцлер юстиции: Эстонии нельзя совершать глупостей под влиянием эмоций

ИНТЕРВЬЮ. Канцлер юстиции: Эстонии нельзя совершать глупостей под влиянием эмоций. Postimees, 31 декабря 2024.

Журналистское расследование

Журналистское расследование углубляется в исследуемые темы и часто проливает свет на скрытые или сложные аспекты.

Характеристики:

- основательный сбор фактов, интервью и исследование документов;
- связано с социально значимыми вопросами;
- длинный формат, подробный анализ.

На что стоит обратить внимание. В журналистских расследованиях достоверность источников имеет огромное значение, поскольку неверно истолкованная или предвзятая информация может привести к неверным выводам. Также может использоваться тактика запугивания, когда эмоциональные аспекты подчеркиваются в ущерб фактам.

Какие тайны скрывает закрытый Telegram-чат KOOS?

Какие тайны скрывает закрытый Telegram-чат KOOS? Блог Propastop, 31 декабря 2024.

Как себя защитить

- Будьте критичным читателем. Не принимайте автоматически любую информацию за истинную. Спросите себя: кто опубликовал эту информацию? Зачем это делается? Какие доказательства и факты представлены?
- Развивайте медиаграмотность. Научитесь распознавать различные жанры журналистики и возможные методы манипулирования, которые в них используются. Узнайте, как создаются новости, каковы их правила и где могут возникнуть проблемы.
- Читайте официальные источники. Когда в обществе поднимается «горячая тема», лучше всего читать официальные источники, общественные СМИ и мнения людей, которые являются экспертами в своей области. Возможно, вы замечали такой феномен: когда какой-либо социально значимый вопрос получает широкое освещение, сразу же появляется множество экспертов, которые стремятся поделиться своим мнением. В этом массиве информации трудно отличить правду от лжи. Мы устаем от постоянного потока мнений и новостей и становимся равнодушными. Чтобы избежать этого, стоит выделить для чтения новостей определенное время.

Harjutused

1. Sobita kokku pealkirjad, pildid ja tekstid.
2. Analüüsi näidisartikleid: tuvasta, kas need vastavad faktipõhisuse ja tasakaalustatuse nõuetele ning vaatle, kuidas visuaalne ja keeleline väljendus mõjutab emotsioone ja arusaamu.
3. Leia üks sündmus, mida kirjeldatakse erinevates lugudes, ja kujuta ette, kuidas erinevad kohalikud meediakanalid sama sündmust kajastaksid.
4. Loe mõne ajalehe tänast juhtkirja. Mis on selle teema ja eesmärk?

Harjutuste materjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Lisamaterjal

Botnar, Kateryna. Allikakriitilisus või -skeptilisus? Mõistlik lähenemine tekstile.

ERR: Meediataip. Mis on meedia ja mis ajakirjandus?

Media and information literacy. A practical guidebook for trainers.

Pullerits, Priit. Ajakirjanduse põhižanrid : uudis, olemuslugu, juhtkiri.

Very Verified: Meedia tüübid. Kõneaine kujundamine. Ka vene keeles.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Сопоставьте между собой заголовки, изображения и тексты.
2. Проанализируйте примеры статей: определите, сбалансированы ли они и основаны ли на фактах, а также рассмотрите, как визуальное и языковое выражение влияет на эмоции и восприятие.
3. Найдите событие, которое описывается в разных публикациях, и представьте, как разные местные СМИ осветили бы это событие.
4. Прочитайте сегодняшнюю редакционную статью в какой-либо газете. Какова ее тема и цель?
5. Он-лайн игра Very Verified: Почему это было опубликовано

Упражнения найдете по ссылке:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Дополнительный материал

Материалы Общества дебатов Эстонии на русском языке.

ERR: Meediataip. Что такое СМИ и что такое журналистика?

Very Verified: Типы медиа. Формирование темы для разговора.
EUvsDisinfo. Тактики, методы и приемы дезинформации. Инфошум

Ботнарь, Катерина. Критическое отношение к источникам или скептицизм?
Разумный подход к тексту. (Botnar, Kateryna. Allikakriitilisus või -skeptilisus? Mõistlik lähenemine tekstile.)

Медийная и информационная грамотность. Практическое руководство для преподавателей.
(Media and information literacy. A practical guidebook for trainers.)

Дополнительные материалы:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

5. Tähelepanumajandus

5. Экономика внимания

5.1. Mida sööb klikisööt?

Kateryna Botnar, RaRa

Peatüki eesmärgid

- Tutvustada klikisööda mõistet ja selle väljendusi peavoolu- ja sotsiaalmeedias.
- Anda praktilisi näpunäiteid klikisööda eristamiseks ja oma inforuumi kaitsmiseks.

Paljud valivad oma eelistatud (veebi)lehte lugedes just selle teksti, mille pealkiri tundub kõige kutsuvam/meeldivam/huvipakkuvam. Vahel aga klõpsavad inimesed kõige ebamäärasemal/hirmutavamal/väheusutavamal tekstil – lihtsalt et teada saada, milles on asja mõte. Isegi kui me teame, mis on klikisööt.

Klikisööt (ka klikimagnet, klõpsulõks, ingl *clickbait*) on selline veebisisu, mida püütakse edasi anda emotsionaalsete, sensatsiooniliste ja tihtilugu kallutatud pealkirjade abil. Huvitav on fakt, et kuigi klikisööt nähtusena tekkis enam-vähem koos nn kollase ajakirjandusega, lisasid Oxfordi sõnaraamatu koostajad selle uue sõnana sõnastikku alles 2016. aastal.

Klikisöödalaadsed pealkirjad võivad kõlada näiteks nii: „Seda ei ole võimalik uskuda!", „Kolm varase vananemise põhjust", „See juhtub sinuga, kui…", ehk siis pealkirja sõnastus tekitab vastuolulisi tundeid: paneb justkui kahtlema, ent siiski äratab huvi. Taolised pealkirjad osutuvad isegi väga edukaks, saavad palju klikke ning järelikult toovad sisse palju raha, kuid sisaldavad üsna tihti spämmi, eksitavat ja/või kallutatud infot. Kui spämmiga on asi üsna selge, siis eksitavaks kvalifitseerub info näiteks siis, kui artikli pealkiri ja sisu ei sobi kokku. Kõik me oleme seda kogenud, eks? Vajutad lingile, ning selle asemel, et saada infot näiteks kasemahla tervislikest omadustest, loed hoopis mingit reklaamteksti.

5.1. Что такое кликбейт?

Катерина Ботнарь, Национальная библиотека Эстонии

Цели главы

- Ознакомить с понятием кликбейта и его проявлениями в мейнстримных СМИ и социальных сетях.
- Дать практические советы, как выявить кликбейт и защитить свое информационное пространство.

Многие люди, читая любимое (интернет-) издание, выбирают тексты, заголовки которых кажутся им наиболее интересными/заманчивыми/привлекающими внимание. Однако иногда люди кликают на самый непонятный/пугающий/невероятный заголовок — просто чтобы узнать, о чем там на самом деле пишут. Даже если они знают, что такое кликбейт.

Кликбейт (от англ. *clickbait*) — это интернет-контент, который пытаются передать с помощью эмоциональных, сенсационных и часто предвзятых заголовков. Интересно отметить, что хотя кликбейт как явление возник более или менее одновременно с так называемой желтой прессой, Оксфордский словарь английского языка признал это слово только в 2016 году.

Кликбейтные заголовки могут звучать так: «В это невозможно поверить!», «Три причины раннего старения», «Вот что произойдет с вами, если…». Иными словами, формулировка заголовка вызывает противоречивые чувства: вроде бы заставляет сомневаться, но при этом вызывает интерес. Такие статьи оказываются очень удачными, набирают много кликов и, соответственно, приносят много денег, но довольно часто содержат спам, недостоверную и/или необъективную информацию. Если со спамом все ясно, то вводящая в заблуждение информация — это, например, несоответствие между заголовком статьи и ее содержанием. Все мы встречали такие примеры, правда? Вы переходите по ссылке и вместо, скажем, информации о полезных свойствах березового сока читаете рекламный текст.

Kallutatud pealkirjaks peetakse tavaliselt sellist pealkirja, kus midagi väidetakse üsna ühepoolselt, kinnitatakse, et Eestis (või Euroopas või välismaal) on juhtunud midagi, mida tegelikult pole juhtunud. Näiteks (kõik pealkirjad on autori välja mõeldud): „Loe, mida Angelina Jolie lapsed talle jõulude eel ütlesid" või „Tõeline põhjus, miks suri Michael Jackson" või „... peres juhtus tõeline tragöödia" või „Kes poleks X-i kohtuväitega nõus". Tegelikult me ju ei tahaks kulutada oma aega, et just seda artiklit lugeda, kuid teeme seda ikkagi.

Mis on need tunnused, mida leida osates saaksime klikisöödaks mõeldud pealkirju teistest eristada?

Klikisööda tunnused

- Ebamäärased, detailideta pealkirjad.
- Kummalised, palju- või vähesõnalised sensatsioonilised väited mõne isiku, sündmuse vm kohta.
- Ebareaalne, „liiga hea, et olla tõsi"-tunne.
- Hirmutavad või manipuleerivad fraasid.
- Küsi- või hüüumärkide rohkus.
- Võltsitud või toimetatud reklaampildid.
- Mitteasjakohased veebiaadressid, kuhu lugejat korduvalt ümber suunatakse.
- Uuesti esile tõstetud fakt/sündmus/info, mis ei ole enam ammu ajakohane.

Klikisööda õnge võib langeda igaüks meist, ent kui see juhtub korduvalt, siis võib teiste ohtude kõrval tekkida ka kajakamber. Kajakambriks nimetatakse peamiselt keskkonda, kus korduvad samad ideed ja vaated, leiavad kinnitust samad mõtted. Meie privileeg on elada ühiskonnas, mis võimaldab ligipääsu erinevale infole, nii et ka meie isiklik meediataldrik peaks, kui vähegi võimalik, olema mitmekesine. Parim soovitus siinjuures on ehk see, et tasub alati vaadata, kas mõni uudis huvitab meid päriselt või tunnetame me selle pealkirja taga mingit manipulatsiooni, otsekui mõjutataks meid seda lugema.

Предвзятым заголовком обычно считается заголовок с безапелляционным заявлением, например, о том, что в Эстонии (Европе, за рубежом) произошло то, чего на самом деле никогда не было. Например (все заголовки придуманы автором): «Читайте, что дети Анджелины Джоли сказали ей накануне Рождества», или «Настоящая причина смерти Майкла Джексона», или «В семье ... произошла настоящая трагедия», или «Кто не согласен с судебным спором X». На самом деле, мы не хотели бы тратить время на чтение этих статей, но все равно это делаем.

Признаки кликбейта:

- расплывчатые заголовки без подробностей;
- странные, многословные или, наоборот, короткие сенсационные заявления о человеке, событии или другой теме;
- ощущение нереальности, «слишком хорошо, чтобы быть правдой»;
- запугивающие или манипулятивные фразы;
- обилие вопросительных и восклицательных знаков;
- фальшивые или обработанные рекламные изображения;
- не относящиеся к делу ссылки, по которым читатель неоднократно перенаправляется;
- вновь упомянутый факт/событие/информация, которые уже не являются актуальными.

Любой из нас может попасть в ловушку кликбейта, но если это происходит постоянно, то, помимо прочих опасностей, это может создать эхо-камеру. Эхо-камера — это среда, где повторяются одни и те же идеи и взгляды, подтверждаются одни и те же мысли. Нам повезло жить в обществе, которое обеспечивает доступ к разнообразной информации, поэтому и наш личный медиарацион должен быть по возможности разнообразным. Пожалуй, лучший совет заключается в том, что всегда стоит проверять, действительно ли нам интересна та или иная новость, или мы чувствуем некую манипуляцию, как будто нас заставляют ее прочитать.

Harjutused

1. Tutvu tänase meediavalikuga – kas miski jääb silma? Kas leiad mõne manipulatsiooni?

2. Loe pealkirju ning sobita kokku pealkiri, klikisööda tunnus ja emotsioon.

Harjutuste materjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Lisamaterjal

Botnar, Kateryna. Allikakriitilisus või -skeptilisus? Mõistlik lähenemine tekstile.

Macnamara, Jim. Beyond post-communication: challenging disinformation, deception, and manipulation.

Lisamaterjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Ознакомьтесь с содержанием СМИ за сегодня — привлекло ли что-то ваше внимание? Можете ли вы найти какие-нибудь манипуляции?

2. Прочитайте заголовки и сопоставьте заголовок, признак кликбейта и эмоцию.

Упражнения найдете по ссылке:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Дополнительный материал

ERR: Meediataip. Насколько тесен информационный пузырь, в котором ты живешь?

VeryVerified: Раздел 4. Фальшивые экспертные мнения.

ERR: Meediataip. Видеолекция: как ссылки на науку используются для придания достоверности информации.

Ботнарь, Катерина. Критическое отношение к источникам или скептицизм?
Разумный подход к тексту. (Botnar, Kateryna. Allikakriitilisus või -skeptilisus? Mõistlik lähenemine tekstile.)

Макнамара, Джим. За пределами посткоммуникации: противодействие дезинформации, обману и манипуляциям. (Macnamara, Jim. Beyond post-communication: challenging disinformation, deception, and manipulation.)

Дополнительные материалы:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

5.2. Kunstmurust kui kunstist

Kateryna Botnar, RaRa

Peatüki eesmärgid

- Tutvustada kunstmuru (rohujuurepesu) mõistet ja selle rolli meediamaastikul.
- Näidata, kuidas ja kelle/mille huvides kunstmuru võtet rakendatakse.
- Anda praktilisi näpunäiteid kunstmuru eristamiseks.

Sinu ees on üks vähestest meediaterminitest, millel on lausa mitu eestikeelset vastet, nii et saa tuttavaks: rohujuurepesu ehk kunstmuru (ingl *astroturfing*). Rohujuurepesu on kunstlikult loodud toetus mõnele liikumisele, reklaamikampaaniale, sündmusele või eraisikule. „Rohujuur" viitabki n-ö rohujuuretasandile, kust see toetus justkui pärineb, ent asi pole tegelikult nii lihtne. Sõna „kunstmuru" selgitab paremini, miks toetus on kunstlikult loodud. Kõige paremini saavad sisust aru need, kes on mänginud jalgpalli kunstmuruga väljakul, sest ka meediavaldkonnas võib mõnele ideele vm väljendatud toetus (nagu kunstmuru jalgpalliväljakul) tegelikult olla võlts. Kaugelt paistab nagu päris, aga lähemalt uurides ebaloomulik.

Kunstmuru abil levitatakse ühtesid ja samu vaateid, mõtteid ja ideid suurema mõju omandamiseks. Tavaliselt on rohujuurepesu kampaania ühe osapoole korraldatud, juhitud ja finantseeritud ning seda kasutatakse nii äri- kui ka poliitilistel eesmärkidel, nii turunduses kui ka lihtsalt valeväidete levitamiseks.

5.2. Астротурфинг как искусство

Катерина Ботнарь, Национальная библиотека Эстонии

Цели главы

- Ознакомить с понятием астротурфинга и его ролью в медийном ландшафте.
- Показать, как и в чьих интересах используется прием астротурфинга.
- Дать практические советы, как выявить астротурфинг.

У термина *астротурфинг* нет однозначного перевода на русский язык, но используются также понятия «имитация общественного запроса» и «псевдообщественная инициатива». Астротурфинг — это искусственно сымитированное одобрение движения, рекламной кампании, события или человека. Само понятие указывает на низовой уровень, с которого, как кажется, исходит эта поддержка, но на самом деле все не так просто. Термин произошел от названия американской компании *AstroTurf*, производящей искусственное покрытие для стадионов, которое имитирует траву. Подобно этому сфабрикованная общественная поддержка имитирует настоящую (обозначаемую в английском языке термином *grassroots* — в буквальном переводе «корни травы»). Издалека поддержка выглядит настоящей, но при ближайшем рассмотрении видна ее неестественность.

С помощью астротурфинга распространяют одни и те же взгляды, мысли и идеи, чтобы получить больше влияния. Как правило, астротурфинг организуется, управляется и финансируется одной стороной и используется как в коммерческих, так и в политических целях, для маркетинга или просто для распространения ложных сведений.

Ja kuigi kunstmuru eksisteerib võttena juba ammu, kasvas selle mõju sotsiaalmeedia tekkega palju tõhusamaks. Inimestele meeldivad tooted, kampaaniad jne, mida toetavad teised kasutajad. Näiteks mida rohkem on postitusel laike või tujukujusid, seda suurem on šanss, et teised vaatajad panevad just seda tähele. Teisisõnu meid veendakse, et miski on meie tähelepanu väärt ja kui seda miskit on võimalik soetada, siis me peaksime seda kindlasti tegema. Väga kõnekas näide on siin kuulus McDonald'si reklaam, millesse õnnestus kaasata suur hulk inimesi, kes seisid järjekorras, et uut McDonald'si toodet maitsta.

Turundusvaldkonnas on üsna levinud praktika kaasata otsekui „päris" inimeste kirjutatud, aga tegelikult võltsarvustusi ja -kommentaare muljetavaldavama ja meeldejäävama toetuse näitamiseks. Internetiostud on saanud paljudele meist igapäevaseks tegevuseks ning loomulikult sooviks me enne ostu teada, kas näiteks see näokreem on efektiivne ja oma hinda väärt, ent enamasti ei saa me kindlaks teha, kes need tootearvustused on kirjutanud. Nii et kuigi viis tähte mõne toote hindamisel meelitab meid seda lähemalt uurima, ei pruugi see hinnang olla kvaliteedi tunnuseks. Nii et kui miski tundub kahtlane, tasub pigem usaldada oma sisetunnet.

Poliitikas käivitatakse rohujuurepesu kampaaniaid, et mõjutada valijaskonda olulise sündmuse eel, näiteks enne valimisi; see võib väljenduda poliitiku sotsiaalmeediakonto jälgijate ja kommenteerijate arvu või valijate laialdase toetuse võltsimise näol. Ja meedia ajaloos on teada juhtumeid, kus sotsiaalmeediakasutajate (toetajate) kontod ei kuulunud reaalsetele inimestele.

Kuidas märgata kunstmuru

- Kahtlane tunne teksti/postituse/kommentaari lugemisel.
- Kommentaarid/postitused sotsiaalmeedias on liiga lühikesed ja/või ühesugused.
- Tekstis esinevad grammatilised jm vead.
- Tekstis kasutatakse hästi palju tujukujusid, mis kohati ei vasta teksti sisule.
- Sõnumi kirjutaja konto on suletud või seal on hästi vähe infot.

Kunstmuru ei ole meediamaastikul veel seadusega karistatav nähtus, kuigi selle mõjud võivad olla üsnagi kahjulikud, eriti siis, kui sõnumid jagavad valet või vaenulikku infot. Rohujuurepesu on raske kindlaks teha, kuna see tegevus on aja- ja ressursimahukas. Ent siiski on meil kõigil võimalus panustada selle vähendamisse, näiteks jääda veebis ostlemisel kaine mõistuse juurde ning mitte jagada sotsiaalmeedias kahtlase sisuga sõnumeid.

И хотя астротурфинг как техника существует уже давно, с появлением социальных сетей его влияние стало гораздо эффективнее. Людям нравятся продукты, кампании и т. д., которые поддерживают другие пользователи. Например, чем больше у поста лайков или эмодзи, тем больше вероятность того, что его заметят другие читатели. Иными словами, нас убеждают, что нечто достойно нашего внимания, и если это нечто можно купить, то мы непременно должны это сделать. Очень показательный пример — знаменитая реклама McDonald's, куда удалось привлечь большое количество людей, стоявших в очереди, чтобы попробовать новый продукт McDonald's.

В маркетинговой индустрии довольно распространена практика включения фальшивых отзывов и комментариев, написанных «реальными» людьми, чтобы продемонстрировать более впечатляющую и запоминающуюся поддержку. Покупки в Интернете для многих из нас стали повседневным действием. Естественно, перед покупкой мы хотим узнать, эффективен ли, например, этот крем для лица и стоит ли он своих денег, но чаще всего мы не знаем, кто написал отзывы о продукте. Поэтому, хотя пятизвездочный рейтинг товара может побудить нас присмотреться к нему повнимательнее, он необязательно является показателем качества. Если что-то кажется сомнительным, лучше довериться своей интуиции.

В политике астротурфинг используется с целью повлиять на электорат в преддверии важного события, например выборов; это может выражаться в подделке количества подписчиков и комментариев на странице политика в социальных сетях или имитации широкой поддержки избирателей. В истории СМИ известны случаи, когда аккаунты пользователей социальных сетей (сторонников) не принадлежали реальным людям.

Как выявить астротурфинг

- Подозрительное чувство при чтении текста/поста/комментария.
- Комментарии/посты в социальных сетях слишком короткие и/или повторяющиеся.
- Грамматические и другие ошибки в тексте.
- В тексте используется много эмодзи, которые иногда не соответствуют содержанию текста.
- Аккаунт человека, написавшего сообщение, закрыт или содержит очень мало информации.

Астротурфинг пока не является уголовно наказуемым преступлением в сфере медиа, хотя его последствия могут быть весьма пагубными, особенно когда распространяется ложная или враждебная информация. Выявить астротурфинг бывает сложно, поскольку это требует много времени и ресурсов. Однако мы все можем внести свою лепту в борьбу с ним, например, исходить из здравого смысла при совершении покупок в Интернете и не делиться сомнительными сообщениями в социальных сетях.

Harjutused

1. Osalejad jagatakse kahte gruppi. Ühed kirjutavad kommentaare millegi poolt, teised vastu. Seejärel loetakse kommentaarid ette.

2. Ava mõni kosmeetikat müüv veebipood ning püüa leida vähemalt kolm toodet, mille hinnang on 5+ või mille juures on hästi palju arvustusi.

Lisamaterjal

Botnar, Kateryna. Mis on kunstmuru?

RaRa. Meediapädevus – mis on kunstmuru?

Sperling, Matthew. Astroturf. London : Quercus Publishing, 2019.

Lisamaterjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Участники делятся на две группы. Одни пишут комментарии в поддержку чего-либо, другие — против. Затем по очереди читают их вслух.

2. Откройте сайт какого-либо магазина косметики и постарайтесь найти не менее трех товаров с оценкой 5+, у которых много отзывов.

Дополнительный материал

VeryVerified: Часть 4. Раздел Б. Тролли и боты.

EUvsDisinfo. Понимание. Нарративы и риторика дезинформации. Риторика дезинформации.

Ботнарь, Катерина. Что такое астротурфинг? (Botnar, Kateryna. Mis on kunstmuru?)

RaRa. Медийная грамотность — что такое астротурфинг? (RaRa. Meediapädevus – mis on kunstmuru?)

Сперлинг, Мэттью. Астротурф. Лондон: Quercus Publishing, 2019. (Sperling, Matthew. Astroturf. London : Quercus Publishing, 2019.)

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

6. Mis toimub?!!
Kui te seda peatükki ei loe, siis...

6. Что происходит?!!
Если вы не прочитаете эту главу, то...

6. Mis toimub?!! Kui te seda peatükki ei loe, siis...

Julia Rodina, MTÜ Tuleviku Meedia

Peatüki eesmärgid

- Õpetada mõistma, kuidas emotsioonidega meedias manipuleeritakse.
- Õpetada emotsioonidega seotud riske ära tundma ja ennast kaitsma.
- Aidata olla mõjutustele vastupanuvõimelisem meediatarbija.

Emotsioonid on inimese elu tähtis osa, ilma emotsioonideta oleks elu hall ja igav. Meedias saab emotsioone kasutada, et panna meid reageerima: klikkima, kommenteerima, postitust jagama, toodet ostma, hääletama või muud moodi tegutsema.

Emotsioonid võivad olla erinevad: nii positiivsed kui ka negatiivsed. Aga need kõik võimaldavad meediasõnumi loojal puudutada inimest kui meediatarbijat väga sügavalt. Nunnud kassipildid võivad koguda miljon laiki, küll aga võib suure tõenäosusega öelda, et reageerima ja infot jagama paneb meid just negatiivne postitus või uudis.

Miks öeldakse tihti, et just halvad uudised müüvad? Sest inimese aju reageerib kõige tugevamalt negatiivsele infole. See mehhanism on tekkinud evolutsiooni jooksul, kuna, kui lihtsustatult öelda, siis meie eellased, kes negatiivsele ja ohu eest hoiatavale infole keskkonnas ei reageerinud, tapeti või söödi ära.

Seda mõistavad nii ajakirjanikud kui ka manipuleerijad ja petturid. Uudise või YouTube'i video pealkirja eesmärk on köita sinu tähelepanu, panna sind lingil klikkima, videot vaatama, ajalehte ostma jne. See töötab nii traditsioonilise ajakirjanduse (TV, raadio, ajalehed, uudisteportaalid) kui ka uute meediaformaatide puhul: YouTube'i videod, blogipostitused, (reklaam)bännerid, *reels* ehk lühivideod koos muusikaga jne.

6. Что происходит?!! Если вы не прочитаете эту главу, то...

Юлия Родина, НКО Tuleviku Meedia

Цели главы

- Научить понимать, как происходит манипуляция эмоциями в медиа.
- Научить распознавать риски, связанные с эмоциями, и защищать себя.
- Помочь потребителю медиа приобрести большую устойчивость к манипуляциям.

Эмоции — важная часть жизни человека, без них жизнь была бы серой и скучной. В медиа эмоции используются, чтобы заставить нас реагировать: нажать на ссылку, оставить комментарий, поделиться сообщением, купить товар, проголосовать или предпринять другие действия.

Эмоции могут быть разными: положительными и отрицательными. Но все они позволяют тем, кто создает контент в медиа, глубоко затронуть человека — потребителя этого контента. Фотографии милых котят могут набирать миллионы лайков, но с большой вероятностью отреагировать и поделиться информацией вас заставит негативный пост или новость.

Почему часто говорят, что плохие новости хорошо продаются? Потому что человеческий мозг сильнее всего реагирует на негативную информацию. Этот механизм возник в ходе эволюции, поскольку, попросту говоря, наши предки, которые не реагировали на негативную и угрожающую информацию в окружающей среде, были убиты или съедены первыми.

Это понимают как журналисты, так и манипуляторы и мошенники. Цель заголовка новости или видеоролика на YouTube — привлечь ваше внимание, заставить перейти по ссылке, посмотреть видео, купить газету и т. д. Это работает и для традиционных СМИ (телевидение, радио, газеты, новостные порталы), и для новых медиа: видеоролики на YouTube, посты в блогах, (рекламные) баннеры, *рилзы*, то есть короткие видео с музыкой, и т. д.

Klikimagneti (ehk klikisööda) mõistest räägime lähemalt 5. peatükis. Aga on olemas ka samasuguse mehhanismiga nähtus vihasööt (ingl *ragebait*). *Rage-baiting* on manipuleeriv taktika, mille eesmärk on esile kutsuda pahameelt, et suurendada internetiliiklust, *online*-aktiivsust, tulu ja toetust. Mõtle järele: kas postitus, YouTube'i video või mõni muu sisuühik võib olla loodud selleks, et sind vihastada, et sa jagaksid seda sisu teistega, kirjutaksid kommentaari? Sina saad oma adrenaliinilaksu, raiskad oma aega ja tähelepanu, autor aga saab oma kliki ja võib-olla ka 15 minutit kuulsust või isegi rahalist kasu, sest sotsiaalmeedia algoritmid näevad, et just see sisu on saanud tähelepanu ja hakanud iseseisvat elu elama ehk n-ö lendama. Kahjuks ei hinda algoritm, kas sisu on kasulik ja hea või emotsionaalne ja manipuleeriv. Algoritmidest räägime täpsemalt 8. peatüki viimases osas.

Tänapäeval on inimeste tähelepanu väärtuslik ressurss. Seetõttu saame infoühiskonnas rääkida tähelepanumajandusest – see on süsteem, mis omistab väärtuse võimele pälvida tähelepanu. Ajakirjanikud, blogijad, brändijad, meediaplatvormid, poliitikud – kõik võitlevad selles süsteemis sinu tähelepanu eest. Ja millele inimene veel paremini reageeriks kui mitte sisule, mis tekitab uudishimu, viha, kadedust, ahnust või hirmu?

Hirmu kasutavad nii petturid (kui helistavad ja ütlevad, et sinu või sinu lähedasega tegeleb politsei või kohus), poliitikud kui kahjuks ka meediasisu loojad. Sest kõik tunnevad, et negatiivsus „müüb".

Petukirjades või -kõnedes on alati hirmutamise element või on need lausa üles ehitatud hirmule: „Kui sa kohe ei tegutse/ei anna oma paroole/ ei kanna raha üle, siis jääd kogu oma varast ilma."

Poliitikud teavad, et hirm toimib hästi ja lihtne on tekitada viha konkreetse ühiskonnagrupi või poliitilise konkurendi vastu, et oma valijaid mobiliseerida. Poliitikud hirmutavad oma valijaid sellega, et konkurent või mõni teine suurem ja ohtlikum võim, riik, rahvus vm vaenlane on kõiges süüdi ja ainult nemad on võimelised valijaid selle eest kaitsma. Sellisel juhul õhutatakse viha kindla poliitilise oponendi, ühiskonnagrupi või nähtuse vastu.

Eraldi lugu on artiklite või postituste kommentaaridega. Sealt leiab terve emotsioonide ja manipulatsioonide paketi. Muidugi, pealtvaatajana on mõnikord lõbus seda jälgida, aga püüa mitte sekkuda. Emotsioonid, mida kommentaatorid õhutavad (mõned meelega, mõned lihtsalt seetõttu, et nad on ka ise selles lõksus), ei ole enamasti kõige ratsionaalsema diskussioonini viiv tee.

Kõiki internetikommentaare ei pea alati lugema ja kõigele reageerima. Küsi endalt: miks ma seda loen ja kas ma ilmtingimata pean sekkuma?

Peale hirmu on kadedus ja ahnus veel ühed tugevad motivaatorid, millega on hea manipuleerida. Näiteks tugineb enamik veebipettusi ja üleüldse pettusi kasutajate ahnusele. Internetis ei saa kunagi olla liiga ettevaatlik, tasub alati meeles pidada: peaaegu kõiki pettusi saab vältida, kui järgida põhimõtet „kui see tundub liiga hea, et olla tõsi, siis tõenäoliselt see ei olegi tõsi". See põhimõte kehtib mis tahes võitude, loteriide, isiklike lugude või allahinnatud kaupade kohta.

Концепция магнита для кликов (или кликбейта) подробно рассматривается в главе 5. Но есть явление с похожим механизмом — рейджбейт (англ. *ragebait*). Рейджбейтинг — это манипулятивная тактика, цель которой — вызвать возмущение пользователей, чтобы увеличить интернет-трафик, онлайн-активность, доходы и число подписчиков. Подумайте: возможно, пост, видео на YouTube или любой другой контент был создан для того, чтобы разозлить вас, заставить поделиться им с другими, написать комментарий? Вы получаете дозу адреналина, тратите свое время и внимание, а автор получает свой клик и, возможно, 15 минут славы или даже финансовую выгоду, потому что алгоритмы социальных сетей видят, что именно этот контент привлек внимание и «взлетел». К сожалению, алгоритм не оценивает, является ли контент полезным и хорошим или эмоциональным и манипулятивным. Об алгоритмах соцсетей мы подробно говорим в последней части главы 8.

В наше время внимание людей — ценный ресурс. Именно поэтому в информационном обществе можно говорить об экономике внимания — системе, которая приписывает ценность способности привлекать внимание. Журналисты, блогеры, маркетологи, медиаплатформы, политики — в этой системе все борются за ваше внимание. А на что человек будет реагировать сильнее, если не на контент, вызывающий любопытство, гнев, зависть, жадность или страх?

Страх используют и мошенники (когда звонят и говорят, что вами или вашим близким человеком занялась полиция или суд), и политики, и, к сожалению, создатели медиаконтента. Потому что все они понимают, что негатив «продается».

Мошеннические письма или звонки всегда содержат элемент запугивания или построены на страхе: «Если вы не предпримете никаких действий прямо сейчас, не передадите пароли и не переведете деньги, вы потеряете все свое имущество!»

Политики знают, что страх хорошо работает, и чтобы мобилизовать своих избирателей, достаточно вызвать ненависть к определенной социальной группе или политическому сопернику. Политики запугивают своих избирателей, заставляя их поверить в то, что во всем виноват конкурент или какая-то другая более крупная и опасная сила, государство, нация или иной враг, и что только они могут защитить избирателей от него. Здесь также хорошо сработает ненависть к определенному политическому противнику, социальной группе или явлению.

Отдельная история — это комментарии к статьям или постам. В них можно найти целый спектр эмоций и манипуляций. Конечно, за этим иногда интересно наблюдать, но лучше – со стороны. Эмоции, которые разжигают комментаторы (некоторые намеренно, некоторые просто потому, что сами попались на эту приманку), обычно не ведут к рациональной дискуссии.

Не обязательно читать все комментарии в сети и отвечать на них. Спросите себя: зачем я это читаю и обязательно ли мне нужно вмешиваться?

Помимо страха, мощными мотиваторами, которыми легко манипулировать, являются зависть и жадность. Например, большинство онлайн-мошенников, да и мошенников вообще, полагаются на жадность пользователей. В Интернете никогда нельзя быть слишком осторожным. Почти всех ловушек можно избежать, если следовать принципу «если это звучит слишком хорошо, чтобы быть правдой, то, скорее всего, это неправда». Этот принцип распространяется на любые лотереи, розыгрыши, личные истории или распродажи.

Kuidas ennast kaitsta

- Kõigil on omad nõrkused. Hea on teada, mis on minu omad ja millele ma kõige aktiivsemalt reageerin. Psühholoogilise kerksuse tugevdamine on igapäevane töö, mida ei saa korraga ja ühe tunniga ära teha.
- Loe, mõtle natuke, ja alles siis märgi *like*/*dislike*, jaga või kommenteeri. Leia enda jaoks vastus, kes on selle emotsionaalse sõnumi autor ja miks. Kas postituse, video või artikli autor tahtis, et reageeriksime just nii? Miks?
- Loe teksti edasi. Pealkirjad võivad klikkide meelitamiseks olla väga pilkupüüdvad ja isegi karjuvad. Aga mis on teksti sisu ja mõte tegelikult? Loe pealkirjast edasi ja alles siis otsusta, kuidas teemasse suhtuda.
- Jäta meelde, et mitte kõiki sotsiaalmeediakommentaare ei ole kirjutanud inimesed. Kommentaarid võivad olla loodud manipuleerimiseks ja valeinfo levitamiseks mõeldud tehisintellekti ehk bottide abil.

Как себя защитить

- У всех есть свои слабости. Полезно понимать, каковы именно ваши и на что вы наиболее активно реагируете. Наработка психологической стойкости и защиты — это ежедневная работа, которую нельзя сделать за час.
- Прочитайте, подумайте и только потом поставьте лайк/дизлайк, поделитесь постом или оставьте комментарий. Найдите ответ на вопрос, кто автор этого эмоционального сообщения и почему он его создал. Хотел ли автор поста, видео или статьи, чтобы мы отреагировали именно так? Почему?
- Читайте текст дальше (заголовка). Чтобы собрать клики, заголовки могут быть очень вызывающими и даже кричащими. Но в чем на самом деле состоит суть и идея текста? Прочитайте дальше заголовка и только потом примите решение, как относиться к теме.
- Помните, что не все комментарии в социальных сетях написаны людьми. Комментарии может оставлять ИИ, то есть боты, с целью манипулирования и распространения ложной информации.

Harjutused

1. Leia klikimagneti näiteid: uudisteportaalidest (pealkirjad), reklaamidest, sotsiaalmeediast. Mis oli sinu näidete puhul selle võtte kasutamise eesmärk? Milliste teemade ja emotsioonidega mängiti? Kes oli sihtrühm? Kas tahtsid ka ise pealkirjal klikkida ja miks? Kas nende näidete puhul saaks klikimagneti kui võtte kasutamist vältida? Kuidas kõlaksid need pealkirjad ilma manipulatsioonideta?

2. Ava neutraalne uudis, loe läbi ja kirjuta oma klikisööt-pealkiri. Milliste emotsioonidega mängisid? Kas teised klikkisid sellel pealkirjal?

Lisamaterjal

BBC. What in the world. How content creators make money from rage-baiting.

Davenport, Thomas H.; Beck, John C. The attention economy: understanding the new currency of business.

ERR: Meediataip. Ojamets, Indrek. Ühiskonda võivad lõhestada isegi naljakana tunduvad valeuudised.

Lehrer, Jonah. How we decide. Boston; New York : Mariner Books, 2010.

RaRa. Meediapädevus – mis on *gaslighting* ehk sohutamine?

TEDx Talks. Livingston, Naiya. How social media manipulates your psychology.

Very Verified: Valeinfo ja manipuleerimine. Manipuleerimine.

Wu, Tim. The attention merchants: the epic scramble to get inside our heads.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Найдите примеры магнита для кликов: на новостных порталах (заголовки), в рекламных объявлениях, в социальных сетях. С какой целью этот прием использовался в ваших примерах? На каких темах и эмоциях играли авторы? Кто был целевой аудиторией? Захотелось ли вам самим кликнуть на заголовок и почему? Можно ли было в этих примерах обойтись без использования кликбейта? Как бы звучали эти заголовки и примеры без манипуляций?

2. Откройте нейтральную новость, прочитайте ее и напишите свой кликбейтный заголовок. На каких эмоциях сыграли вы? Кто бы кликнул на этот заголовок?

Дополнительный материал

ERR: Meediataip. Ояметс, Индрек. Даже фальшивые новости, которые кажутся забавными, могут расколоть общество.

Very Verified: Раздел 4. Дезинформация и манипуляции. Манипуляции.

ERR: Meediataip. Почему фейковые новости распространяются?

BBC. Что в мире. Как создатели контента делают деньги на рейджбейте.
(BBC. What in the world. How content creators make money from rage-baiting.)

Бек, Джон К.; Дэвенпорт, Томас Х. Экономика внимания: понимание новой валюты бизнеса.
(Beck, John C.; Davenport, Thomas H. The attention economy: understanding the new currency of business.)

Лерер, Джона. Как мы принимаем решения. Бостон; Нью-Йорк: Mariner Books, 2010.
(Lehrer, Jonah. How we decide. Boston; New York : Mariner Books, 2010.)

RaRa. Медийная грамотность — что такое газлайтинг?
(RaRa. Meediapädevus – mis on *gaslighting* ehk sohutamine?)

TEDx Talks. Ливингстон, Найя. Как социальные сети манипулируют вашей психологией.
(TEDx Talks. Livingston, Naiya. How social media manipulates your psychology.)

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

6.1. Tajuvead ja psühholoogia mõjutamas info tarbimist

Kristiina Kaju, RaRa

Peatüki eesmärgid

- Anda ülevaade levinud vigadest mõtlemises ehk tajuvigadest.
- Tutvustada protsesse, kuidas me ümbritsevat infot ja sündmusi töötleme.
- Näidata, kuidas psühholoogia ja mõtlemine mõjutavad info hankimist ja tarbimist.

Teemat selgitavad mõned psühholoogia mõisted, mis on seotud infoga manipuleerimise, infokäitumise ning info analüüsimisega.

Tajuviga, kognitiivne nihe (ingl *cognitive bias*) on olukord, kus inimeste mõtlemine ja otsused on vastuolus ratsionaalsete ootustega. Meie mõtlemises esinevad tajuvead, mis on küll reeglipärased, kuid mille vältimine on tihti keeruline ja kohati võimatu. Kognitiivsed nihked ehk tajuvead tekivad meil kõigil. Teooria kohaselt teeb inimene otsuseid lähtuvalt oma arusaamast ja seetõttu tekib kõrvalekalle loogilisest otsustusprotsessist. Tajuvigadega kaasneb kalduvus olla millegi poolt või vastu ning inimesel puudub neutraalne vaatenurk. Tajuvigade nimekiri on pikk, sisaldades rohkem kui sadat info vastuvõtmise ja töötlemise puudust.

Mõned näited inimpsühholoogias esinevatest tajuvigadest.

- **Kinnituskalduvus** (ingl *confirmation bias*) — kalduvus teavet otsida või tõlgendada viisil, mis kinnitab inimese eelarvamusi. Lisaks võidakse eirata teavet, mis ei toeta inimese uskumusi. Teisisõnu: inimesed usuvad seda, mida nad tahavad uskuda. Kui nad mõne idee omaks võtavad, jääbki see tihtipeale muutumatuks. Kinnituskalduvus paneb meid soosima infot, mis toetab seda, mida me juba usume. Infot otsides otsime sageli seda, mis sobib meie teadmistega sellel teemal ja toetab neid. Kinnituskalduvus piirab vastuolulise informatsiooni hulka, mida me omaks võtame, piirates

6.1. Ошибки восприятия и психология, влияющие на потребление информации

Кристийна Каю, Национальная библиотека Эстонии

Цели главы

- Дать обзор распространенных когнитивных искажений, то есть ошибок восприятия.
- Ознакомить с процессом обработки информации и событий вокруг нас.
- Показать, как психология и мышление влияют на получение и потребление информации.

Тему поясняют некоторые понятия из психологии, связанные с манипулированием информацией, информационным поведением и анализом.

Ошибка восприятия, когнитивное искажение (англ. *cognitive bias*) — это ситуация, когда мышление и решения людей противоречат рациональным ожиданиям. В нашем мышлении имеются ошибки восприятия, которые подчиняются определенным правилам, но которых зачастую сложно, а то и невозможно избежать. Когнитивные искажения, или ошибки восприятия, есть у каждого из нас. Согласно теории, человек принимает решения, основываясь на собственном восприятии, и поэтому возникают отклонения от логического процесса принятия решений. Ошибки восприятия влекут за собой склонность быть за или против чего-либо и отсутствие нейтральной точки зрения. Список ошибок восприятия длинный и содержит более сотни дефектов приема и обработки информации.

Вот некоторые примеры ошибок восприятия в психологии человека.

- **Предвзятость восприятия** (англ. *confirmation bias*) — тенденция искать или интерпретировать информацию таким образом, чтобы она подтверждала предубеждения человека. Кроме того, человек может игнорировать информацию, не подтверждающую его убеждения. Иными словами, люди верят в то, во что хотят верить. Стоит принять какую-то идею, и она часто остается неизменной. Предвзятость восприятия заставляет нас отдавать предпочтение

nii kognitiivset dissonantsi (vastuoluliste hoiakute tekkimist millegi suhtes). Paraku piirab see ka võimet uusi ideid omaks võtta või muid võimalusi kaaluda. Paljudel veebilehtedel ja sotsiaalmeediaplatvormidel kasutatavad ennustavad otsimisalgoritmid süvendavad kinnituskalduvuse probleemi. See tehnoloogia annab soovitusi asjade kohta, mis sind võiks huvitada, ning teavet, mis on sarnane sellega, mida oled juba näinud, klikkinud, meeldivaks märkinud ja/või jaganud. Ainult algoritmide toodetud ennustavate soovituste kasutamine välistab võimaluse saada uut või vastandlikku teavet mingil teemal. Sotsiaalmeedias liikudes tuginevad inimesed sageli infole, mis neile ette satub, mistõttu muutub nende vaade teemale kitsendatuks ja ühekülgseks. Inimene, kes ei ole teadlik sellistest info esitamise viisidest ja algoritmide toimimisest, võib teha järelduse, et enamik teisi inimesi nõustub tema seisukoha või eelistusega. Seda nimetatakse vale konsensuse efektiks. Selline mõju paneb inimesi üle hindama, kui paljud teised inimesed nendega nõustuvad ning võimaldab teha oletusi, mis ei vasta tõele. On lihtne näha, kuidas kinnituskalduvus ja valekonsensus saavad koos mõjuda, et luua olukord, kus võidakse uskuda vale- ja desinformatsiooni.

- **Motiveeritud arutlus** (ingl *motivated reasoning*) – me kasutame põhjendusi, et uskuda seda, mida me tahame uskuda. Kasutades motiveeritud põhjendusi, võime leida viisi, kuidas end veenda, et miski on tõene, kui tahame, et see oleks tõene.
- **Nn kolmanda isiku efekt** (ingl *third-person effect*) – inimesed eeldavad, et (vale)informatsioon mõjutab teisi rohkem kui neid ennast. Me kõik kipume alahindama, kui palju meid mõjutab väärinfo.
- **Omakasule kallutatus** (ingl *self-serving bias*) – kalduvus tunda oma panust suuremana edu korral ja väiksemana läbikukkumise korral. See võib väljenduda ka mitmeti mõistetava informatsiooni hindamisel hindajale kasulikul viisil.
- **Uskumise kallutatus** (ingl *belief bias*) – argumendi loogilist tugevust hinnates on inimene mõjutatud sellest, kui tõene või väär usub ta selle järelduse olevat.
- **Tagantjäreletarkus** (ingl *hindsight bias*) – kalduvus tajuda minevikusündmusi ennustatavatena. Vahel kutsutakse seda ka olen-seda-kogu-aeg-teadnud-efektiks.
- **Negatiivsuskalduvus või -efekt** (ingl *negativity bias*) – psühholoogiline kalduvus pöörata muude omaduste poolest võrdsete asjaolude korral suuremat tähelepanu negatiivsetele tunnetele, mõtetele, suhtlusolukordadele või sündmustele. Negatiivsuskalduvusega põhjendatakse halbade uudiste eelistamist meedias, sest need pälvivad rohkem tähelepanu ning toovad väljaannetele rohkem lugejaid, kuid see mängib rolli ka kalduvuses kirjalikus internetisuhtluses eelistada sõnumi negatiivset tõlgendust positiivsele ning suurendab konfliktide esinemise tõenäosust.
- **Ankruefekt** (ingl *anchoring bias*) – esimest infokildu võetakse kõige usaldusväärsemana ning lähtutakse edaspidise info töötlemisel sellest.
- **Autoriteedihoiak** (ingl *authority bias*) – autoriteedist tuleneva eelarvamusliku tajuvea tõttu saab positsiooniga isik teiste silmis automaatselt usaldusväärsema tausta ning tema väljaütlemistel on suurem mõju.

Teemaga on seotud ka mõiste **filtrimull** (ingl *filter bubble*) – iga internetikasutaja jaoks kujundatav personaalne unikaalne inforuum, mida koostatakse ja kujundatakse paljude internetiressurssidega seotud erilise tarkvara abil.

информации, которая подтверждает то, во что мы уже верим. Когда мы ищем информацию, то часто ищем то, что соответствует нашим знаниям на данную тему и подтверждает их. Предвзятость восприятия ограничивает количество противоречий, которые мы способны воспринять, тем самым ограничивая когнитивный диссонанс (формирование противоречивого отношения к чему-либо). К сожалению, это также ограничивает способность принимать новые идеи или рассматривать другие варианты. Рекомендательные алгоритмы, используемые на многих сайтах и платформах социальных сетей, усугубляют проблему предвзятости восприятия. Эта технология рекомендует вещи, которые могут вас заинтересовать, и информацию, похожую на ту, которую вы уже видели, открывали, лайкали и/или пересылали другим. Использование только предсказательных рекомендаций, создаваемых алгоритмами, исключает возможность получить новую или противоречивую информацию по какой-то теме. Находясь в социальных сетях, люди часто полагаются лишь на ту информацию, которая им попадается, что делает их взгляд на тему узким и однобоким. Человек, не знающий о таких способах подачи информации и о том, как работают алгоритмы, может прийти к выводу, что большинство других людей согласны с его точкой зрения или предпочтениями. Это называется эффектом ложного консенсуса. Его влияние заставляет людей переоценивать то, сколько других людей с ними согласны, и делать предположения, которые не соответствуют действительности. Легко увидеть, как предвзятость восприятия и ложный консенсус работают вместе, создавая ситуацию, в которой можно поверить в ложь и дезинформацию.

- **Предвзятость рассуждения** (англ. *motivated reasoning*) — мы используем обоснования, чтобы верить в то, во что хотим верить. Используя предвзятые рассуждения, мы можем убедить себя в том, что что-то является правдой, если мы хотим, чтобы это было правдой.
- **Эффект третьего лица** (англ. *third-person effect*) — люди полагают, что (неправильная) информация влияет на других больше, чем на них самих. Все мы склонны недооценивать, насколько сильно мы подвержены влиянию дезинформации.
- **Эгоистическая погрешность** (англ. *self-serving bias*) — склонность преувеличивать свой вклад в случае успеха и преуменьшать его в случае неудачи. Это может проявляться также в оценке неоднозначной информации полезным для оценивающего образом.
- **Предвзятость подтверждения** (англ. *belief bias*) — при оценке логической силы аргумента на человека влияет то, насколько истинным или ложным он считает вывод.
- **Знание задним числом** (англ. *hindsight bias*) — склонность воспринимать события прошлого как пророческие. Иногда это еще называют эффектом «я все время это знал».
- **Негативная предвзятость или эффект** (англ. *negativity bias*) — психологическая тенденция при прочих равных условиях уделять больше внимания негативным чувствам, мыслям, взаимодействиям или событиям. Негативной предвзятостью объясняется предпочтение плохих новостей в СМИ, так как они притягивают больше внимания и привлекают больше читателей к публикациям. Она также играет роль в тенденции отдавать предпочтение негативной интерпретации сообщений в онлайн-переписке и повышает вероятность конфликта.
- **Эффект якоря** (англ. *anchoring bias*) — первая информация воспринимается как наиболее надежная и используется в качестве основы для обработки последующей информации.
- **Эффект авторитета** (англ. *authority bias*) — из-за предвзятости восприятия человек, занимающий авторитетное положение, автоматически воспринимается другими как более заслуживающий доверия, и его высказывания имеют большее влияние.

Kuidas ennast kaitsta

Kui inimesed suudavad neid psühholoogilisi protsesse mõista ja teadlikult juhtida, paraneb nende võime kriitiliselt mõista ja hinnata meedia edastatavat teavet. Järgnevalt mõned tehnikad, mis aitavad piirata psühholoogilise manipulatsiooni mõju.

- Skeptitsism – ole teadlik võimalikust manipuleerimisest. Enne info vastuvõtmist mõtle kasutatud keelele, lisatud taustamuusikale, logodele, kaubamärkidele või fotodele.
- Hoiatus – ole teadlik võimalikust vale- ja desinformatsioonist. Inimesed, kes on teadlikud, et teised võivad levitada väärinformatsiooni, on sellele vähem vastuvõtlikud.
- Analüütiline mõtlemine – peatu ja mõtle saadud info üle. Ära anna kohe võimalust emotsioonidele. Analüüs nõuab aega ja vaeva, sest sellega kaasneb sageli aju kiirreaktsiooni takistamise vajadus.
- Võta aeg maha – ära jaga kohe infot, esmalt tasuks küsida: „Kas see on miski, mida ma tõesti tahan jagada?". Isegi see lihtne kaalutlusmoment võib anda aega, mida aju vajab, et alustada info analüüsimist. Julgusta inimesi mõtlema enne info jagamist või omaks võtmist.
- Valeinfo leviku ennetamine (ingl *prebunking*) – õpi ja õpeta ka teisi ära tundma tehnikaid, mida kasutatakse vale- ja desinformatsiooni levitamiseks.

С этой темой связано и понятие информационного пузыря (англ. *filter bubble*) — уникального персонального информационного пространства для каждого интернет-пользователя, создаваемого и формируемого рядом специализированных программ, связанных со многими интернет-ресурсами.

Как себя защитить

Если люди способны понять эти психологические процессы и осознанно управлять ими, их способность критически понимать и оценивать информацию, передаваемую медиа, улучшится. Вот несколько приемов, которые помогут ограничить влияние психологических манипуляций.

- Скептицизм — будьте готовы к возможным манипуляциям. Прежде чем воспринять информацию, подумайте об используемом языке, фоновой музыке, логотипах, брендах или фотографиях.
- Внимание — будьте готовы к возможной лжи и дезинформации. Люди, которые знают, что другие могут распространять дезинформацию, менее восприимчивы к ней.
- Аналитическое мышление — остановитесь и подумайте над полученной информацией. Не поддавайтесь эмоциям сразу же. Анализ требует времени и усилий, так как зачастую необходимо предотвратить слишком быструю реакцию мозга.
- Не спешите и не делитесь информацией сразу, сначала стоит спросить: «Правда ли я хочу этим поделиться?» Даже этот небольшой момент может дать мозгу время, необходимое для того, чтобы начать анализировать информацию. Побуждайте людей думать, прежде чем делиться информацией или верить ей.
- Предотвращение распространения ложной информации (англ. *prebunking*) — научитесь и научите других распознавать приемы, используемые для распространения лжи и дезинформации.

Harjutused

1. Tajuvigade äratundmise harjutus.

   Igal argumendil on vähemalt kaks poolt. Rühmad kujundavad ühe argumendi puhul poolt- ja teise puhul vastuseisukohad. Otsitakse infot oma seisukohtade tõestuseks. Et argumendi teist poolt ümber lükata, tuleb teada, milline see pool on ja missugusel informatsioonil see põhineb. Kui sa ignoreerid infot, mis ei sobi sellega, mida sa mõtled või ootad, siis leiad sa ainult selle info, mis kinnitab seda, mida sa arvad või ootad.

2. Tartu Ülikool. Digimentorid: Propaganda ja kognitiivsed nihked.

3. Eesti Väitlusselts. Tunnikava tajuvigade mõistmiseks.

4. Eesti Väitlusselts. Tunnikava eelarvamuste mõistmiseks.

Harjutuste materjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Lisamaterjal

52 essential critical thinking : cognitive bias discovery game : improve problem-solving, smarter decision-making.

Burkhardt, Joanna M. Media smart : lessons, tips and strategies for librarians, classroom instructors and other information professionals.

Dobelli, Rolf. Selgelt mõtlemise kunst : [52 mõtlemisviga, mida oleks parem vältida].

Propastop: Tajuvead, tagauks valeinfole.

Very Verified: Isikupärastatud algoritmid ja filtrimullid. Ka vene keeles.

Very Verified: Mis on tajuvead ja miks need tekivad?

Lisamaterjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Упражнение на распознавание когнитивных искажений.

   У каждого аргумента есть как минимум две стороны. Группы формируют мнения «за» для одного аргумента и «против» для другого. Они ищут информацию, чтобы доказать свою точку зрения. Чтобы опровергнуть другую сторону аргумента, нужно знать, что это за сторона и на какой информации она основана. Если вы игнорируете информацию, не соответствующую вашим представлениям или ожиданиям, то найдете только ту, которая подтверждает их.

2. Тартуский университет. Цифровые менторы: Пропаганда и когнитивные искажения. (Tartu Ülikool. Digimentorid: Propaganda ja kognitiivsed nihked.)

3. Общество дебатов Эстонии. План урока по пониманию когнитивных искажений

4. Общество дебатов Эстонии. Факт и мнение. План урока на русском языке.

Упражнения найдете по ссылке: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Дополнительный материал

Very Verified: Персонализированные алгоритмы и информационные пузыри.

Very Verified: Ошибки восприятия.

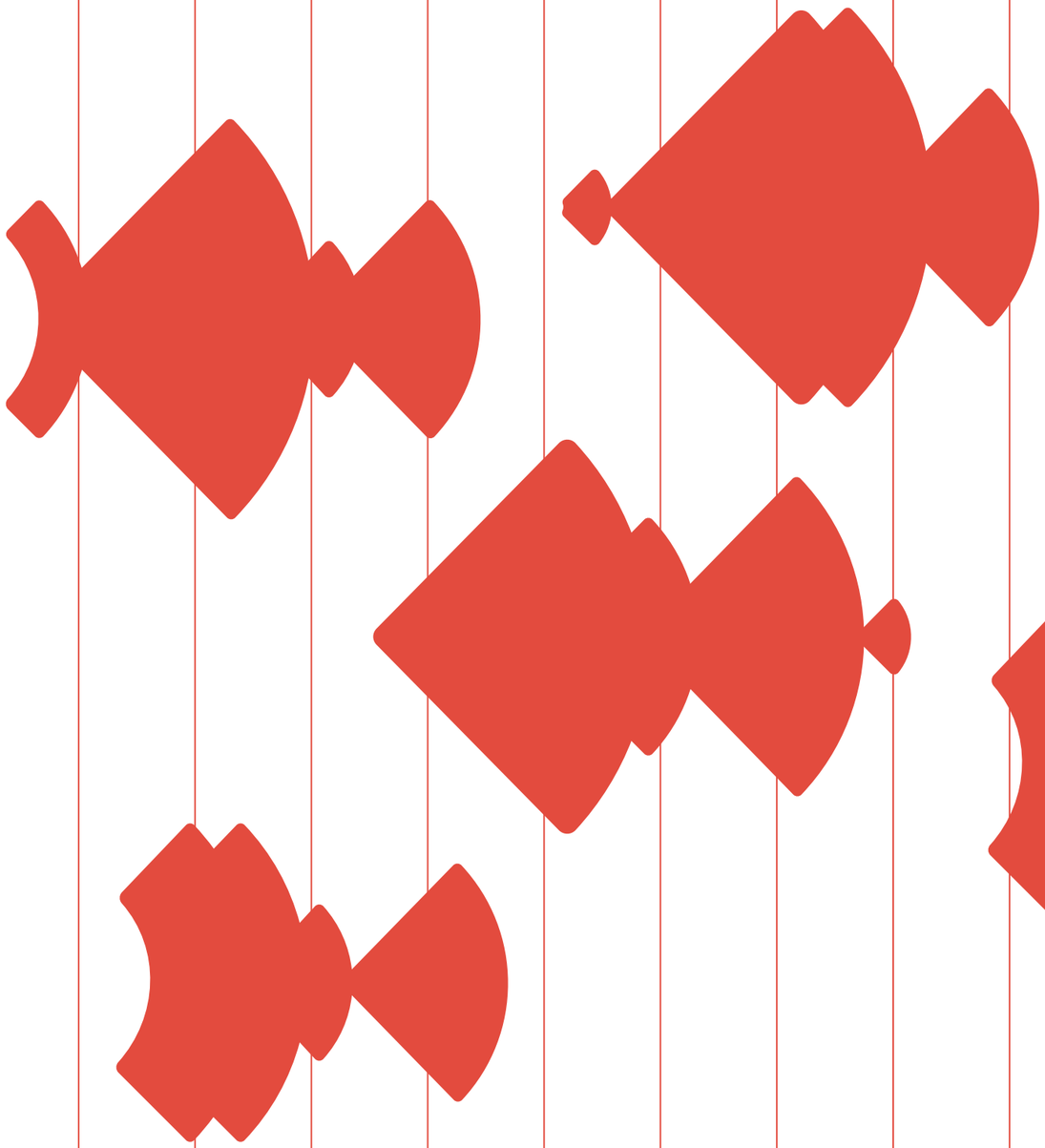
Very Verified: Что такое ошибки восприятия и почему они возникают?

Добелли, Рольф. Искусство мыслить ясно: [52 ошибки мышления, которых следует избегать]. (Dobelli, Rolf. Selgelt mõtlemise kunst : [52 mõtlemisviga, mida oleks parem vältida].)
https://www.ester.ee/record=b4691129

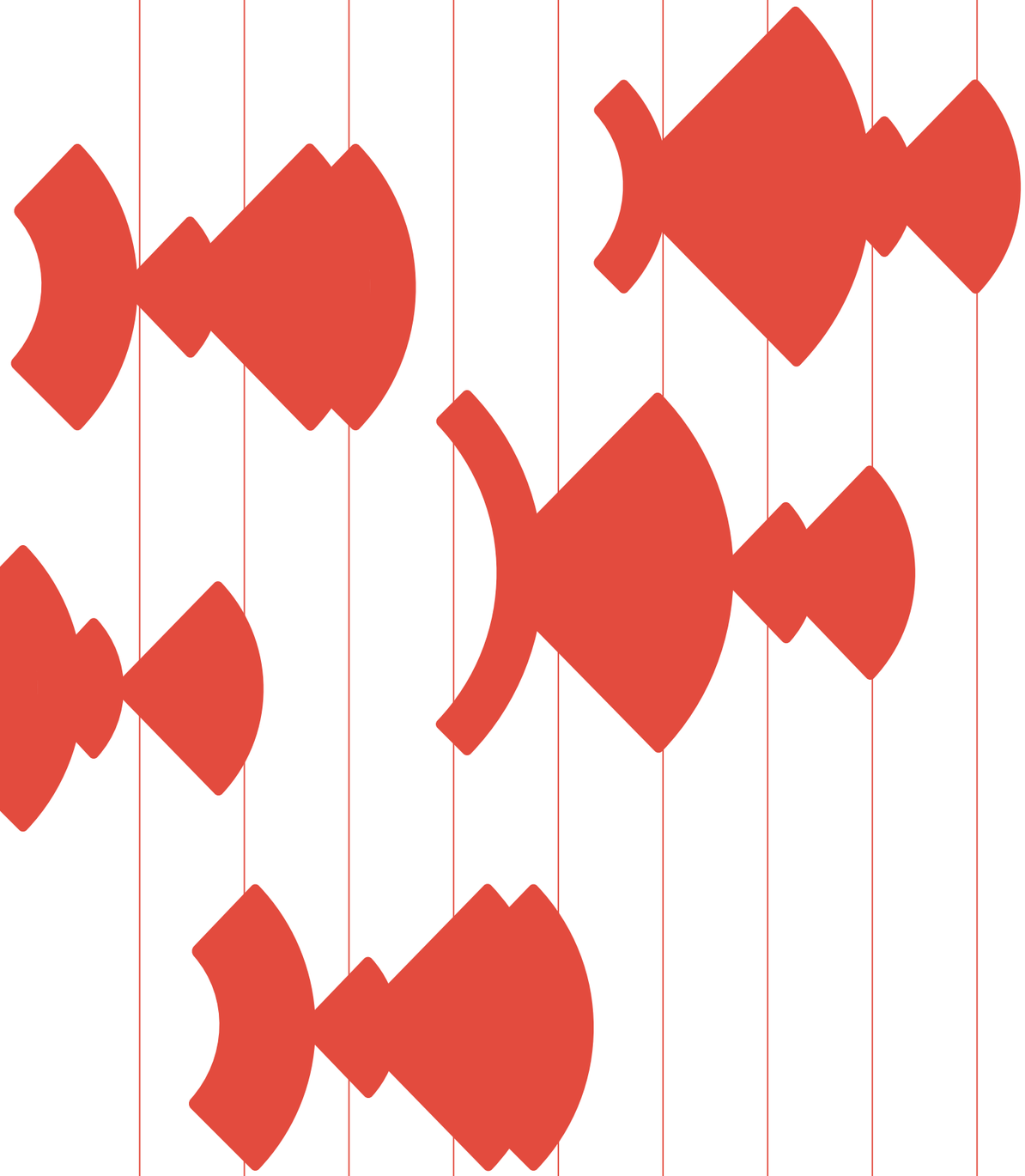
Propastop: Ошибки восприятия и черный ход для дезинформации. (Tajuvead, tagauks valeinfole.)
https://www.propastop.org/2020/10/15/tajuvead-tagauks-valeinfole/

Дополнительные материалы:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

7. Võltsitud 24/7



7. Подделано 24/7



7.1. Valeinfo ja kuidas ennast selle eest kaitsta

Julia Rodina, MTÜ Tuleviku Meedia

Peatüki eesmärgid

- Tutvustada valeinfo mõistet ja näidata, miks see võib ohtlik olla.
- Õpetada, kuidas ennast valeinfo eest kaitsta ja kuidas infot kontrollida.
- Anda näpunäiteid, kuidas saada meediapädevamaks infotarbijaks.

Info kvaliteet, õigsus ja usaldusväärsus võivad olla erinevad. Informatsioon, mis ei vasta tõele, on kogu meie väljaande teema. Nii ajakirjanduses kui ka sotsiaalmeedias võib leida eksitavat infot, mis on tihtilugu vale inimliku või mõne muu juhusliku eksituse tõttu. Sellise informatsiooni eesmärk ei ole meelega kahju tekitada. Hoopis ohtlikum on aga desinfo (ingl *disinformation*), mis on samuti eksitav, aga oluline vahe on selles, et desinfo on sihilikult loodud mõne inimese, ühiskonnagrupi, poliitilise organisatsiooni, riigi vm kahjustamiseks. Samas võib see olla ka osa reklaamistrateegiast, pettus või lihtsalt nali. Enamasti siiski kasutavad pahatahtlikud inimesed valeinfot, et manipuleerida, inimesi ja protsesse mõjutada ning tahtlikult kahju tekitada.

Eriti palju leiab valeinfo näiteid valimis- ja muude poliitiliste kampaaniate ajal, kui mõned poliitikud ei piirdu ainult loosungitega, vaid kasutavad oma esinemistes, sotsiaalmeedias ja valimismaterjalides valeinfot, et valijaskonda mõjutada, oma valijaid mobiliseerida, konkurenti halvustada ja rohkem hääli saada.

7.1. Дезинформация, и как от нее защититься

Юлия Родина, НКО Tuleviku Meedia

Цели главы

- Познакомить с понятием дезинформации и показать, почему она может быть опасна.
- Научить защищаться от дезинформации и контролировать информацию.
- Дать советы, как стать более грамотным потребителем информации.

Качество, правильность и достоверность информации могут разниться. Все наше издание посвящено тому, как распознать информацию, не соответствующую действительности. Недостоверную информацию можно найти как в прессе, так и в социальных сетях, часто из-за человеческой или иной случайной ошибки. Такая информация не преследует цели намеренно причинить вред. Гораздо опаснее *дезинформация* (англ. *disinformation*), которая также вводит в заблуждение, но с той важной разницей, что она создается намеренно, чтобы нанести вред человеку, социальной группе, политической организации, стране и др. Дезинформация также может быть частью рекламной стратегии, мошенничеством или просто шуткой. Однако чаще всего злоумышленники используют дезинформацию для манипуляций, влияния на людей и процессы и намеренного причинения вреда.

Дезинформация особенно часто встречается во время избирательных и других политических кампаний. Некоторые политики не ограничиваются лозунгами, а используют дезинформацию в своих выступлениях, социальных сетях и предвыборных материалах, чтобы повлиять на электорат, мобилизовать избирателей, очернить соперников и получить больше голосов.

Mõisted „valeuudised" (ingl *fake news*) ja „tõejärgne" (ingl *post-truth*) levisid üle maailma seoses USA 2016. aasta presidendivalimiste kampaania ja Brexiti rahvahääletusega. Toona alles kandidaat, praeguseks teist korda USA presidendiks valitud Donald Trump tõi mõiste *fake news* laiaulatuslikku kasutusse ja ringlusse, nimetades valeuudisteks tihti ka infot, mis talle ei sobinud või ei meeldinud. Oma kõnedes esitasid nii Trump kui ka Brexiti ideoloogid ja pooldajad nn alternatiivseid fakte või suisa valet – sisuliselt võibki neid väiteid pidada valeuudisteks.

Nn alternatiivne fakt, aga tegelikult valeinfo võib kahjustada mitte ainult kellegi mainet või mõjutada ühiskondlikku arvamust, vaid võib olla otseselt ka eluohtlik. Mõtleme siin valeinfot, mis puudutab tervist: näiteks vandenõuteooriad vaktsiinide mõju kohta, kinnistes sotsiaalmeediagruppides levivad nõuanded või nn imeravimite retseptid.

Näiteks levis 2024. aastal eestikeelses Facebookis postitus, mis väitis, et mammograafia on ohtlik ja ei aita rinnavähki tuvastada, vaid vähk hoopis tekib pärast seda protseduuri. Tegelikult aitab mammograafia rinnavähki varajases faasis tuvastada ja õigeaegset ravi saada; kiirgushulk, mis protseduuri jooksul saadakse, ei ole ohtlik. Ning Šveits ei ole protseduuri keelustanud, kuigi postitus seda väitis.

Paljudel juhtudel põhineb valeinfo pooltõdedel: vale pannakse kokku ehtsa infoga või ei selgitata lugejale teema konteksti. Nii muutub valeinfo usaldusväärsemaks ja täidab oma ülesande. Sellistes valeinfot sisaldavates artiklites või postitustes tsiteeritakse tihti juhtunu tunnistajaid, valdkonna eksperte või uuringuid, mis võivad olla täielikult võltsitud (neid pole olemas) või on neid valesti tõlgendatud.

Kuidas sulle tundub, milline info levib kiiremini ja miks? Paljud ekspertarvamused ja uuringud näitavad, et valeinfo levib veebis kordades kiiremini kui tõene. Sealjuures mängib olulist rolli asjaolu, et valeinfo pakub alati midagi täiesti uudset ja on tihti esitatud atraktiivselt, tekitab uudishimu, kasutab klikimagneti võtteid, intrigeerib, manipuleerib lugejate hirmude ja teiste emotsioonidega jne.

Tuleb rõhutada, et valeinfo võib esineda eri vormides ja tekst on ainult üks neist. Valeinfo võib levida ka võltsitud heli- ja pildifailide või videotega. Eriti lihtne on see tänapäeval, kui peaaegu iga inimene saab oma nutitelefonis toimetada fotosid või tehisaru abiga genereerida heli, pilte ja videoid.

Kuigi nii Eestis kui ka mujal maailmas tegelevad mitmed toimetused sihikindlalt valeinfo ümber lükkamisega ja teevad näiteks populaarsetele postitustele, poliitilistele väidetele (ka valimiseelsel perioodil) või vaenulikele narratiividele faktikontrolli, ei saa nad kontrollida iga postitust. Valeinfo eest saame me ennast kaitsta ainult ise.

Selleks tasub mõnikord proovida panna ennast uuriva ajakirjaniku rolli, esitada küsimusi ja ka ise tõde otsida. Kahjuks paljud meediatarbijad seda ei tee, kuigi peaksid. Fakte kontrollida on lihtne ning kui oled lugedes korraks mõtlema jäänud ja sul tekib kahtlase artikli või postitusega seoses küsimusi, siis on see juba peaaegu võit. Sinu kriitiline mõtlemine on ärganud!

Pakume läbi väljaande palju kasulikke nõuandeid, kuidas mitte langeda petturite või manipulaatorite ohvriks, kuidas pilte ja infot kontrollida. Siin veel mõned soovitused, mida ette võtta, kui info sinus kahtlust tekitab.

Термины *фейковые новости* (англ. *fake news*) и *постправда* (англ. *post-truth*) распространились по всему миру в контексте президентской кампании 2016 года в США и референдума по Brexit. Дональд Трамп, тогда еще только кандидат, а теперь уже второй раз избранный президентом США, ввел понятие *фейковые новости* в широкое обращение, часто называя информацию, которая ему не нравилась или не подходила, *фейками*. В своих выступлениях идеологи и сторонники Трампа и Brexit представляли т. н. альтернативные факты или по сути откровенную ложь. Именно такие утверждения можно считать дезинформацией.

Так называемые альтернативные факты, а на самом деле дезинформация, могут не только повредить чьей-то репутации или повлиять на общественное мнение, но и представлять прямую угрозу для жизни. Мы имеем в виду дезинформацию, касающуюся здоровья: например, теории заговора о вреде вакцин, советы, распространяемые в закрытых группах соцсетей, или рецепты «чудо-лекарств».

Например, в 2024 году в эстоноязычном пространстве Facebook распространился пост о том, что маммография якобы опасна и именно после этой процедуры развивается рак груди. На самом деле маммография помогает выявить рак груди на ранней стадии и своевременно пройти лечение; доза излучения, получаемая во время процедуры, не опасна. И в Швейцарии эта процедура не запрещена, хотя в посте утверждалось именно это.

Во многих случаях дезинформация основана на полуправде: ложь смешивается с подлинной информацией или читателю не объясняется контекст темы. Так ложная информация выглядит более достоверной и служит своей цели. В подобных дезинформационных статьях и сообщениях часто цитируются свидетели происшествия, эксперты в данной области или исследования, которые могут быть полностью фальсифицированными (несуществующими) или неверно истолкованными.

Как вы думаете, какая информация распространяется быстрее и почему? Многие эксперты и исследования говорят, что ложная информация распространяется в сети в разы быстрее, чем правдивая. Немаловажную роль играет тот факт, что дезинформация всегда предлагает что-то новое, часто подается в привлекательной обертке, вызывает любопытство, использует кликбейт, интригует, манипулирует страхами и другими эмоциями читателей, и т. д.

Следует подчеркнуть, что дезинформация может принимать разные формы, и текст лишь одна из них. Фейковая информация также может распространяться через поддельные изображения, аудиозаписи или видео. Это особенно легко в наше время, когда почти каждый человек может использовать смартфон для редактирования фотографий или генерирования звука, изображений и видео с помощью ИИ.

Хотя многие редакции СМИ как в Эстонии, так и в других странах мира стремятся опровергать дезинформацию и проводить фактчекинг, например, вирусных постов, политических обвинений (в том числе в предвыборный период) или враждебных нарративов, они не могут проверить каждое сообщение. Только мы сами можем защитить себя от дезинформации.

Для этого иногда стоит примерить на себя роль журналиста-расследователя, задавать вопросы и самостоятельно идти на поиски истины. К сожалению, многие потребители медиа не делают этого, хотя могли бы. Проверить факты легко, а если читая статью или пост, вы задумаетесь и начнете задавать вопросы, то это уже почти победа. Ваше критическое мышление на страже!

Во всех главах мы даем множество полезных советов, как не стать жертвой мошенников или манипуляторов, как проверять изображения и информацию. Вот еще несколько советов, что делать, если вы сомневаетесь в правдивости информации.

Kuidas märgata valeinfot?

- Hinda informatsiooni allikat. Uuri selle allika (veebi)lehte, loomise eesmärki ja kontaktinfot. Kas kusagil on märgitud ka väljaandja kui juriidiline isik? Kus ta asub ja kas seda saab kontrollida?
- Loe teksti pikemalt. Pealkirjad võivad klikkide meelitamiseks olla väga pilkupüüdvad ja manipuleerida meie emotsioonidega. Aga mis on teksti sisu tegelikult? Mis tegelikult toimus? Kas meie ees on fakt või arvamus? Vaata pealkirjast kaugemale.
- Kontrolli autorit. Kes loo kirjutas/postitas? Kas ta on päriselt olemas? Kui ta esineb ajakirjanikuna, siis kas ta töötab mõnes toimetuses? Kas autor on usaldusväärne? Mida ta veel on kirjutanud?
- Toetavad allikad tekstis. Millistele allikatele artikkel viitab? Kliki ka nendel linkidel. Uuri, kas info nendes allikates ka tegelikult toetab teksti ja on õigesti tsiteeritud.
- Ekspert. Kas nn vaieldamatu ekspert ehk isik, kes kommenteerib teemat või annab tervisenõu, on selleks tegelikult piisavalt professionaalne? Kas saab kontrollida tema ameti- või aunimetuse tõelevastavust? Guugelda!
- Kontrolli teksti avaldamise kuupäeva. Pane tähele, et vanade uudiste uuesti avaldamine ei tähenda, et need oleksid praegu asjakohased.
- Mõtle, kas tegemist võib olla naljaga. Kui tekst on liiga kummaline, võib see olla mõeldud naljana. Kui kahtled, kontrolli veebilehte ja allikat ning otsi sama infot ka teistest allikatest.
- Mõtle, milline on sinu hoiak teema suhtes. Arvesta sellega, et sinu enda tõekspidamised võivad oluliselt mõjutada sinu hinnangut.
- Kontrolli ka ise fakte, kasuta faktikontrolli tööriistu: näiteks kontrolli, kas pilt postituse või artikli juures on ehtne (kuidas seda teha, saab lugeda 8. peatükist), küsi abi raamatukogust.

Как выявить фейк?

- Оцените источник информации. Изучите сайт источника, цель его создания и контактную информацию. Упоминается ли где-то издатель как юридическое лицо? Где он находится и можно ли его проверить?
- Прочитайте весь текст целиком. Чтобы собрать клики, заголовки могут быть очень вызывающими и могут манипулировать нашими эмоциями. Но каково реальное содержание текста? Что произошло на самом деле? Перед нами факт или мнение? Смотрите дальше заголовка.
- Проверьте автора. Кто написал/разместил эту статью или пост? Существует ли автор на самом деле? Если он представляется как журналист, то работает ли он в каком-то издании? Можно ли доверять этому автору? Что он писал ранее?
- Источники в тексте. На какие источники ссылается статья? Перейдите также по ссылкам на источники. Проверьте, действительно ли информация из этих источников подтверждает написанное в тексте и правильно ли она цитируется.
- Эксперт. Действительно ли так называемый «неоспоримый эксперт», то есть человек, который комментирует тему или дает медицинские советы, достаточно квалифицирован, чтобы делать это? Проверьте, соответствует ли истине его должность или регалии. Погуглите!
- Проверьте дату публикации текста. Обратите внимание, что повторная публикация старых новостей не означает, что они все еще актуальны.
- Подумайте, может ли это быть сатира. Если текст слишком странный, он может быть задуман как шутка. Если вы сомневаетесь, проверьте сайт и источник и поищите ту же информацию в других источниках.
- Подумайте, как вы относитесь к теме материала. Помните, что на нашу оценку могут значительно повлиять наши собственные убеждения.
- Проверьте факты самостоятельно, используя инструменты проверки: например, проверьте, реальна ли фотография под постом или в статье (о том, как это сделать, читайте в следующей главе), обратитесь за помощью в библиотеку.

Harjutused

1. Jaga oma kogemusi: kas oled kunagi avastanud valeinfot? Kas ja kuidas sa seda kontrollisid?
2. Arutle, kes ja miks võiks kirjutada Eestis toimuvate sündmuste kohta valeuudiseid.
3. Arutle, millised tagajärjed võivad olla valeinfol.

Lisamaterjal

Ariely, Dan. Misbelief : what makes rational people believe irrational things.

EPL. Suur aasta kokkuvõte: kuidas kujundas infomõjutustegevus 2024. aastat?

ERR: Meediataip. Himma, Marju. Kuidas kaitsta end ja teisi valeinfo eest?

Global Investigative Journalism Network: introduction to investigative journalism: fact-checking.

O'Connor, Cailin; Weatherall, James Owen. The misinformation age – how false beliefs spread.

Postimees: Haridus. Faktikontroll.

TEDx Talks. Simpson, Blake. Misinformation, the media, and the role you're playing in both.

Very Verified: Valeinfo ja manipuleerimine.

Wolrich, Joshua. Toit pole ravim: kuidas väärinfo kahjustab tervist.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Поделитесь своим опытом: сталкивались ли вы когда-нибудь с дезинформацией? Проверяли ли вы ее и как?
2. Обсудите, кто и зачем может писать фейковые новости о событиях в Эстонии.
3. Обсудите возможные последствия распространения дезинформации.

Дополнительный материал

Ариэли, Дэн. Заблуждения: что заставляет рациональных людей верить в иррациональные вещи.

ERR: Meediataip. Что такое фейковая новость?

ERR: Meediataip. Как определить фейковую новость?

ERR: Novaator. Исследование раскрыло ключевую причину распространения фейков в соцсетях.

VeryVerified: Что такое дезинформация?

Югансоо, Гретел. В помощь учителю — вспомогательные материалы по раскрытию схем мошенничества.

EPL. Большой обзор года: как деятельность в сфере информации повлияла на 2024 год? (Suur aasta kokkuvõte: kuidas kujundas infomõjutustegevus 2024. aastat?)

Postimees: Образование. Проверка фактов. (Postimees: Haridus. Faktikontroll.) https://haridus.postimees.ee/7246269/6-teema-faktikontroll

TEDx Talks. Симпсон, Блейк. Дезинформация, средства массовой информации и роль, которую вы играете в них. (Simpson, Blake. Misinformation, the media, and the role you're playing in both.)

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

7.2. Kas oma silm on kuningas?

Kateryna Botnar, RaRa

Peatüki eesmärgid

- Anda ülevaade, millised võivad olla võltsitud pildid või videod.
- Anda praktilisi näpunäiteid, kuidas eristada võltsitud pilte ja videoid ehtsatest.

Pildimanipulatsioonide maailm on väga mitmekesine ja täis väljakutseid: iga natukese aja tagant ilmuvad uued võltsingud, mis tuleb ümber lükata, nii et faktikontrollijatel tööd jagub. Põhjuseks on nii tehnoloogia areng kui ka inimeste soov muuta pilte paremaks, tavaliselt enda maitse järgi. Pildimanipulatsioon kui mõiste seostub enamasti kaasajaga, kuid nähtus ise eksisteerib juba 19. sajandi lõpust, mil hakati lavastama suure tähtsusega sündmusi ning protsessi kaasati professionaalsed näitlejad. Eelmise sajandi kahekümnendatel aastatel ilmus ajaleht New York Evening Graphic, mille väljaandjad hakkasid ühiskonnas toimunut aktiivselt lavastama: sagedased olid skandaalid vm sellise sisuga uudised, aga ka naiste seksuaalse alatooniga pildid. Seda suundumust võib võrrelda kaasajaga, kus kuulsate näitlejannade nägusid kasutatakse pornofilmide videoid redigeerides. Pildilavastusi on loonud ka kunstnikud, näiteks Alison Jackson, kelle tööd jäävad kindlasti meelde ning kellega ma siiralt soovitan lähemalt tutvuda.

Sõna „pildimanipulatsioonid" Sõnaveebist ei leia, olemas on aga üsnagi sarnase tähendusega sõna „süvavõltsing" (ingl *deep fake*): loodud või manipuleeritud kujutis või audio- või videosisu, mis sarnaneb tegelike isikute, esemete, kohtade, üksuste või sündmustega ning mis näib kasutajale petlikult ehtne või tõene.

7.2. Всегда ли стоит верить своим глазам?

Катерина Ботнарь, Национальная библиотека Эстонии

Цели главы

- Дать обзор того, как можно подделать изображения или видео.
- Дать практические советы, как отличить поддельные изображения и видео от настоящих.

Манипуляции изображениями могут быть очень сложными и разнообразными. То и дело появляются новые подделки, которые нужно опровергать, что создает специалистам по проверке фактов много работы. Это связано как с развитием технологий, так и с желанием людей улучшить изображения — обычно на свой вкус. Манипуляция изображениями как понятие обычно ассоциируется с современностью, но само явление существует с конца XIX века, когда люди начали инсценировать крупные события, привлекая к процессу актеров. В 20-х годах прошлого века выходила газета New York Evening Graphic, которая освещала постановочные события. В ней часто рассказывалось о скандалах и подобных новостях, нередки были и фото женщин с сексуальным подтекстом. Эту тенденцию можно сравнить с сегодняшним днем, когда при создании порнороликов используются лица известных актрис. Постановочные фото создают и художники, например Элисон Джексон, чьи работы, безусловно, запоминаются, и я искренне рекомендую с ними ознакомиться.

Манипуляцию изображениями также коротко называют *дипфейк* (от англ. *deepfake*): это специально созданное или измененное изображение, аудио- или видеоконтент, напоминающий реальных людей, предметы, места, сущности или события и кажущийся пользователю обманчиво реальным или правдивым.

Millistel eesmärkidel aga võltsitakse pilte kaasajal? Esiteks tuleb mainida, et kõik, kes on kasutanud näiteks Instagramis või muus sotsiaalmeediakeskkonnas mõnda filtrit, on sisuliselt loonud (enda kohta) võltsingu. Miks? Sellepärast, et siis näeb inimene pildil teistmoodi välja kui päriselus ja see ongi eesmärk. Teine võimalik põhjus on tahe teiste inimeste arvamust kujundada või mõjutada. Näiteks toimetavad enda tehtud pilte kinnisvarabürood, et saada rohkem oma kodu otsivate huviliste tähelepanu. Muudatused pildil ei pea olema sugugi suured: näiteks on pildil kamin, kus põleb tuli, kuid tegelikkuses ei tööta see kamin juba hulk aega. Taolised väiksed detailid on siin võtmetähtsusega.

Kus veel on võimalik iga päev võltspiltidega kokku puutuda? Õige vastus: sotsiaalmeedias. Realistlike profiilipiltide ja mõnd sündmust kirjeldavate või sügavamat mõtet sisaldavate postituste juures me ei peatugi piisavalt pikalt, et endale selgeks teha, kas pilt on ehtne või mitte. Samas leidub veebiavarustes aina rohkem poliitikute, näitlejate vm pilte, mis ei ole originaalid.

Videote puhul oli viimase ajani natuke lihtsam, sest võltsitud videod olid tavaliselt kehvema kvaliteediga, imelike taustahelidega või ilmselgelt muudetud detailidega. Videovõltsingut saab ära tunda ka jutu järgi, mida kaadris olev inimene räägib: jälgi, kas see on tema tavaline kõnelemisviis, kas jutt tundub loogiline, kas keelekasutus paistab olevat korrektne? Samas tasub tähele panna ka kõnepauside ajal taustal toimuvat: inimes(t)e häält ja muid helisid, kui neid on.

Viimasel paaril aastal on üks populaarseimatest teemadest meediamaastikul piltide genereerimine. Päris mitmed programmid, näiteks OpenAI, Canva, Gemini, DALL-E jt suudavad seda päris hästi, ent siiski on mitmeid tunnuseid, mis eristavad just tehisintellekti abiga loodud pilti lihtsalt võltsitud pildist. Viimast võib pidada katusmõisteks mõlema jaoks.

Kuidas ära tunda süvavõltsingut?

Pööra tähelepanu järgnevale:

- Pildikvaliteet – kas pildil on kõrge resolutsioon, näiteks kas kõiki detaile on näha, kui pilti suurendada.
- Varjude olemasolu.
- Peegelduste olemasolu.
- Valgus – kas see on ühtlane, ere või kontrastne.
- Värvitoonid – kas need tunduvad sulle loomulikud. See on aktuaalne eriti siis, kui tegemist on portreepildiga.
- Kas pilti on lõigatud.
- Jooned ja servad – kas kõik on proportsioonis.

С какими целями подделывают изображения в наши дни? Во-первых, любой, кто пользуется фильтрами, скажем, в Instagram или на любой другой платформе, по сути, подделывает (свое) изображение. Почему? Потому, что на фото человек будет выглядеть иначе, чем в реальной жизни, а это и есть цель подделки. Другая возможная причина — желание сформировать мнение других людей или повлиять на него. Например, агентства недвижимости редактируют фотографии, чтобы привлечь внимание людей, ищущих жилье. Изменения не обязательно должны быть крупными: например, на фото изображен горящий камин, но на самом деле он уже давно не работает. Такие мелкие детали имеют ключевое значение.

Где еще можно столкнуться с поддельными изображениями? Правильный ответ: в социальных сетях. Если фото профиля в посте, где описывается какое-то событие или приводится мысль, реалистичное, мы не станем надолго задерживаться, чтобы понять, подлинное оно или нет. В то же время в сети встречается все больше поддельных фото политиков, актеров и т. д.

С видео до недавнего времени было немного проще, поскольку поддельные видео обычно были низкого качества, со странным звуковым фоном или явно измененными деталями. Видеоподделку можно распознать по тому, как говорит человек в кадре: нужно проанализировать, обычная ли это для него манера речи, кажется ли речь логичной, а язык правильным? Однако стоит обратить внимание и на то, что происходит на заднем плане во время пауз в речи: голоса людей и другие звуки, если они есть.

Одной из самых популярных тем в медиаландшафте в последние несколько лет стала генерация изображений. Достаточно большое количество программ, таких как OpenAI, Canva, Gemini, DALL-E и другие, довольно хорошо генерируют изображения, но все же есть ряд особенностей, которые отличают созданное ИИ изображение от обычного дипфейка. Последний можно рассматривать как зонтичный термин для обоих.

Как распознать дипфейк?

Обратите внимание на следующее:

- качество изображения — насколько высокое разрешение изображения, например, все ли детали видны при его увеличении;
- наличие теней;
- наличие отражений;
- свет — равномерный, яркий или контрастный;
- оттенки цвета — выглядят ли они естественными. Это особенно актуально, когда речь идет о портретной съемке;
- обрезано ли изображение;
- линии и края — все ли пропорционально.

Kuidas ära tunda tehisintellekti abiga genereeritud pilti?

- Vaata, mitu sõrme on pildil kujutatud inimesel: genereeritud kujutisel võib neid olla rohkem kui viis.
- Kui pildil paistab mõni tekst, näiteks poesilt või raamatukaas, siis uuri, mis keeles see on. Mõned tehisintellektil põhinevad programmid tavatsevad teksti ise välja mõelda.
- Tekstuurid ja proportsioonid: kas nahk paistab olevat liiga ideaalne; kas jalad on natuke liiga pikad isegi supermodelli jaoks?
- Detailid – mida rohkem on väidetavalt genereeritud pildil detaile, seda rohkem on ainest, mida uurida. Vaata, millised on käed, kas naeratus on loomulik, milline on inimese asend kõndides, süües jne.
- Taust – vaata, millised on tausta-elemendid. Vahel võib juhtuda, et programm „väsib ära" ja ei näe taustal olevate inimeste või objektide puhul enam kuigi palju vaeva. Sellisel juhul on need vähem kvaliteetsed, hägusad ja isegi ebakorrektsed.

Как распознать изображение, сгенерированное ИИ?

- Посмотрите, сколько пальцев у человека на картинке: на сгенерированном изображении их может быть больше пяти.
- Если на картинке виден какой-то текст, например вывеска магазина или обложка книги, посмотрите, на каком языке он написан. Некоторые программы, основанные на искусственном интеллекте, склонны выдумывать текст.
- Текстуры и пропорции: кожа выглядит слишком идеальной, ноги длинноваты даже для супермодели?
- Детали — чем больше деталей в изображении, которое может быть сгенерированным, тем больше материала для изучения. Обратите внимание на то, как выглядят руки, естественная ли улыбка, в какой позе человек ходит, ест и т. д.
- Фон — обратите внимание на элементы фона. Иногда программа «устает» и не прилагает для генерации людей или объектов на заднем плане особых усилий. В этом случае они окажутся менее качественными, размытыми и даже искаженными.

Harjutused

1. Veebimäng Pildimanipulatsioonide maailm.

2. Veebimäng Tehis *vs.* aru.

Harjutuste materjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Lisamaterjal

Deepfakes : creation, detection, and impact / edited by Loveleen Gaur.

Shu, Kai; Liu, Huan. Detecting fake news on social media.

Van, R. L. Identifying fake news.

Lisamaterjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Онлайн-игра «Мир манипуляций изображениями». (Pildimanipulatsioonide maailm.)

2. Онлайн-игра «Искусственный и интеллект». (Tehis *vs.* aru.)

Упражнения найдете по ссылке:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Дополнительный материал

Very Verified: Раздел 4. Информация, вводящая в заблуждение, и манипуляции.

ERR: Meediataip. Видеолекция: подделывать теперь можно не только фото, но и видео. Как отличить т. н. дипфейк?

Шу, Кай; Лю, Хуань. Обнаружение фейковых новостей в социальных сетях. (Shu, Kai; Liu, Huan. Detecting fake news on social media.)

Ван, Р. Л. Выявление фейковых новостей. (Van, R. L. Identifying fake news.)

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

7.3. Mis on tehisaru?

Kari Kivinen, Faktabaari

UNICEFi definitsiooni kohaselt[1]:

tehisaru viitab masinapõhistele programmidele, mis on võimelised tegema prognoose, soovitusi või otsuseid, mis mõjutavad reaalset või virtuaalset keskkonda, lähtudes inimese määratletud eesmärkidest. Tehisaruprogrammid suhtlevad meiega ja mõjutavad meie keskkonda kas otse või kaudselt. Nad näivad sageli tegutsevat iseseisvalt ja suudavad oma käitumist kohandada, õppides kontekstist.

Lihtsamalt öeldes töötavad tehisaruprogrammid reeglite järgi või õpivad näidete põhjal (juhendatult või juhendamata) või katse ja eksimuse teel (stiimulõpe). Paljud tänapäeval kasutatavad tehisaru rakendused alates soovitussüsteemidest kuni nutirobotiteni tuginevad suurel määral masinõppe tehnikatele mustrite tuvastamise meetodil. Arvutid suudavad andmetest mustreid leides töödelda teksti, heli, pilte või videoid ning vastavalt sellele planeerida ja tegutseda.

Tehisaru tehnoloogia on tõestanud oma kasulikkust, iseäranis andme- ja teabemahukas tervishoiusektoris. Tervishoiusektor muutub kiiresti digitaalseks, kuna andmete parem haldamine ja kogumine võimaldab täpsemaid diagnoose, haiguste ja ravi jälgimist ning ennetavat tervishoidu. Tehisarul põhinevate lahenduste rakendamine tervishoius on juba näidanud, et see võib oluliselt parandada tavasid ja rutiini[2].

Mida peaksid kasutajad teadma tehisaruprogrammidest?

Paljud sotsiaalmeediaplatvormid kasutavad küpsiseid ja mitmesugust tuvastustarkvara, et koguda teavet oma kasutajate kohta[3]. Need võivad jälgida ja salvestada kasutaja välimust (näotuvastus), häält, keskkonda (esemed teie ümber) ning seadmesse salvestatud kontaktandmeid ja pilte.

Kogutud andmete põhjal luuakse kasutaja profiil, et algoritmid saaksid pakkuda kohandatud otsitulemusi, aga eelkõige selleks, et platvormid saaksid võimalikult üksikasjalikke profiile eri eesmärkidel müüa. Näiteks YouTube'i algoritmid soovitavad videoid, Spotify algoritmid muusikat, Netflixi algoritmid filme ja Amazoni algoritmid tooteid, mis kasutajale kõige tõenäolisemalt meeldivad.

Tehisaru kasutatakse üha enam digisisu automaatseks loomiseks ja isegi uudislugude kirjutamiseks. Tüüpilised tehisaru genereeritud tekstid on näiteks ilmaprognoosid. Kasutajatel on tehisaruprogrammidest kasu ka digisisu töötlemisel.

Tehisaru töövahendid võivad pakkuda inimväärset või inimest asendavat suhtlust, nagu seda teevad vestlusrobotid. Otsitulemused, sotsiaalmeedia tegevusvood ja sisusoovitused põhinevad sageli tehisaru algoritmidel ning statistikal. Tehisaruprogrammid võivad kasutada ka isikuandmeid ja digitaalse identiteedi jälgimist, et pakkuda kasutajatele personaalsemaid teenuseid.

7.3. Что такое искусственный интеллект?

Кари Кивинен, НКО Faktabaari

Согласно определению ЮНИСЕФ:

Искусственный интеллект (ИИ) — это машинные системы, способные делать прогнозы, давать рекомендации или принимать решения, влияющие на реальную или виртуальную среду, исходя из поставленных человеком целей. Программы искусственного интеллекта взаимодействуют с нами и прямо или косвенно влияют на наше окружение. Часто кажется, что они действуют независимо и способны адаптировать свое поведение, изучая обстановку[1].

Проще говоря, программы ИИ работают по правилам либо учатся на примерах (обучение с учителем или без учителя) или методом проб и ошибок (обучение с подкреплением). Многие используемые сегодня приложения ИИ, от рекомендательных систем до умных роботов, в значительной степени опираются на методы машинного обучения, способные распознавать закономерности. Находя закономерности в данных, компьютеры могут обрабатывать текст, звук, изображения или видео, а также планировать и действовать в соответствии с этим.

Технология искусственного интеллекта доказала свою пользу, особенно в секторе здравоохранения, отличающемся большими объемами данных. Сектор здравоохранения стремительно переходит на цифровые технологии, поскольку более эффективное управление данными и их сбор позволяют ставить точные диагнозы, отслеживать заболевания и лечение, а также проводить профилактику заболеваний. Использование решений на основе искусственного интеллекта в здравоохранении уже показало, что он может значительно улучшить практику и процессы[2].

Что пользователи должны знать о программах искусственного интеллекта?

Многие платформы социальных сетей используют файлы cookie и различные программы идентификации для сбора информации о пользователях[3]. Они могут отслеживать и сохранять данные о внешности (распознавание лиц), голосе, обстановке (окружающих предметах), а также контактные данные и фотографии, хранящиеся на устройстве.

Собранные данные используются для создания профиля пользователя, чтобы алгоритмы могли выдавать персонализированные результаты поиска, и, прежде всего, чтобы платформы могли продавать наиболее подробные профили пользователей для различных целей. Например, алгоритмы YouTube рекомендуют видео, алгоритмы Spotify — музыку, алгоритмы Netflix — фильмы, а алгоритмы Amazon — товары, которые с наибольшей вероятностью понравятся пользователям.

Искусственный интеллект все чаще используется для автоматического создания контента и даже для написания новостных статей. К типичным текстам, создаваемым ИИ, относится, например, прогноз погоды. Программы искусственного

Koostöö tehisaruprogrammidega

Käskluse sõnastamine tehisaru rakenduste kasutamisel on väga oluline uus oskus, olgu tegemist kõnetuvastusega digiassistendiga või ChatGPTga. Mida täpsem sisend, seda parem tulemus. Kasutajad peaksid olema teadlikud ka sellest, et mõned algoritmid on programmeeritud andma tulemusi, mis toetavad kasutaja arvamust. Sel juhul on oht, et tekib kajakamber. Seepärast peaksid kasutajad kaaluma tehisintellektipõhiste otsimootorite kasutamise plusse ja miinuseid.

Kui kasutaja suhtleb tehisaruprogrammidega, siis ta:

1. Oskab sõnastada otsingupäringuid, et saavutada soovitud tulemus suhtlemisel digiassistentide või nutikõlaritega (nt Siri, Alexa, Cortana, Google Assistant), nt mõistes, et selleks, et programm vastaks soovitud viisil, peab päring olema üheselt mõistetav ja selgelt esitatud, et programm saaks vastata.
2. Saab aru, et mõned tehisaru algoritmid võivad kinnitada digikeskkondades ringlevaid seisukohti, tekitades kajakambri või infomulli (nt kui sotsiaalmeedias eelistatakse teatud poliitilist ideoloogiat, võivad edasised soovitused seda ideoloogiat tugevdada, ilma vastandlikke argumente pakkumata).
3. Kaalub tehisarul põhinevate otsimootorite kasutamise plusse ja miinuseid (nt kuigi need võivad aidata kasutajal leida soovitud teavet, võivad need ohustada eraelu puutumatust ja isikuandmete kaitset või kasutada inimest äri huvides ära).

Et tehisaruprogrammidega usaldatavalt, kriitiliselt ja turvaliselt suhelda, kasutaja:

1. Teab, et isikuandmete töötlemise suhtes kohaldatakse kohalikke eeskirju, näiteks ELi isikuandmete kaitse üldmäärust (GDPR). Näiteks häälsuhtlus virtuaalassistendiga on GDPRi tähenduses isikuandmed ning see võib ohustada kasutaja andmekaitset, eraelu ja turvalisust.
2. Kaalub biomeetriliste tuvastustehnoloogiate (nt sõrmejäljed, näokujutised) kasutamise plusse ja miinuseid, kuna need võivad tahtmatult mõjutada turvalisust. Kui biomeetrilised andmed lekivad või neid häkitakse, on need ohustatud ja võivad viia identiteedipettuseni.
3. On teadlik, et tehisaruprogrammid, mis tuginevad kasutajate isikuandmetele (nt häälassistendid, vestlusrobotid), võivad koguda ja töödelda selliseid andmeid rohkem kui vaja. Seda võib pidada ebaproportsionaalseks ja nii oleks see vastuolus GDPRis määratletud proportsionaalsuse põhimõttega.
4. Kaalub enne virtuaalassistendi (nt Siri, Alexa, Cortana, Google Assistant) või tehisarul põhinevate asjade interneti (IoT) seadmete aktiveerimist plusse ja miinuseid, sest need võivad avaldada isiklikke argirutiine ja eravestlusi.
5. Kaalub plusse ja miinuseid, enne kui lubab kolmandatel isikutel oma isikuandmeid töödelda (nt on teadlik, et nutitelefoni häälassistent, mida kasutatakse robottolmuimejale käskluste jagamiseks, võib anda kolmandatele isikutele – ettevõtetele, valitsustele, küberkurjategijatele – juurdepääsu andmetele).

интеллекта можно использовать для редактирования и обработки цифрового контента.

Инструменты ИИ могут обеспечивать общение, напоминающее общение с человеком или заменяющее его, как это делают чат-боты. Результаты поиска, потоки активности в социальных сетях и рекомендации контента часто основаны на алгоритмах и статистике искусственного интеллекта. Программы искусственного интеллекта также могут использовать персональные данные и цифровую идентификацию, чтобы предоставлять пользователям персонализированные услуги.

Взаимодействие с системами искусственного интеллекта

Формирование запросов при пользовании приложениями ИИ — очень важный новый навык, будь то цифровой помощник с распознаванием речи или ChatGPT. Чем точнее сформулирован запрос, тем лучше будет результат. Пользователи также должны знать, что некоторые алгоритмы склонны выдавать результаты, которые поддерживают мнение человека. При этом существует опасность оказаться в «информационном пузыре». Поэтому пользователям следует взвесить все плюсы и минусы использования поисковых систем на основе ИИ.

Если пользователь взаимодействует с системами искусственного интеллекта, ему нужно...

1. Уметь формулировать поисковые запросы для достижения желаемого результата при взаимодействии с цифровыми помощниками или «умными колонками» (Siri, Alexa, Cortana, Google Assistant), например, понимать, что для того, чтобы система ответила желаемым образом, запрос должен быть однозначным и четко сформулированным.
2. Понимать, что некоторые алгоритмы ИИ могут усиливать существующие в цифровой среде взгляды, создавая эффект «информационного пузыря» (например, если в социальных сетях отдается предпочтение определенной политической идеологии, дальнейшие рекомендации могут подкреплять эту идеологию, не предлагая аргументов против нее).
3. Взвешивать все плюсы и минусы использования поисковых систем на основе ИИ (например, хотя они помогают пользователям найти нужную информацию, они также могут нарушать конфиденциальность и защиту персональных данных или использовать человека в интересах бизнеса).

Чтобы пользование системами искусственного интеллекта было надежным, безопасным и объективным, пользователь должен...

1. Знать, что к обработке персональных данных применяются местные нормы, такие как Общий регламент ЕС по защите данных (GDPR). Например, голосовое взаимодействие с виртуальным помощником в понимании GDPR относится к персональным данным и может представлять угрозу для защиты данных, частной жизни и безопасности пользователя.
2. Взвешивать плюсы и минусы использования технологий биометрической идентификации (например, отпечатков пальцев, изображений лица), поскольку это может влиять на безопасность. Утечка или взлом биометрических данных подвергает их опасности, и это может стать причиной мошенничества с личными данными.

6. Tunneb nii positiivseid kui ka negatiivseid mõjusid, mis kaasnevad kõigi andmete, eelkõige isikuandmete kogumise, kodeerimise ja töötlemisega tehisarul põhinevates digitehnoloogiates, nt rakendustes ja võrguteenustes.

7. On teadlik, et kõike, mida inimesed internetis avalikult jagavad (nt pildid, videod, helid), võib kasutada tehisaruprogrammide treenimiseks. Näiteks võivad tehisaru näotuvastussüsteeme arendavad kommertstarkvarafirmad kasutada internetis jagatud isiklikke pilte (nt perefotosid), et treenida ja parandada tarkvara võimet automaatselt ära tunda neid isikuid teistel piltidel, mis ei pruugi olla soovitav (see võib rikkuda eraelu puutumatust).

Kasutatud allikad

[1] UNICEF (laetud 19.12.2023). Policy guidance on AI for children.

[2] Habli, Ibrahim; Lawton, Tom; Porter, Zoe. (2020). Artificial intelligence in health care: accountability and safety. Bulletin of the World Health Organization, 98 (4), 251–256. World Health Organization.

[3] Clario (laetud 19.12.2023). Which data can companies actually collect?

Originaaltekst: Kivinen, Kari. Tekoäly – mitä meidän pitäisi tietää ja osata?

3. Понимать, что программы искусственного интеллекта, опирающиеся на личные данные пользователей (например, голосовые помощники, чат-боты), могут собирать и обрабатывать больше данных, чем необходимо. Такой сбор данных может быть расценен как непропорциональный и, следовательно, может нарушать принцип пропорциональности, установленный GDPR.

4. Прежде чем активировать виртуального помощника (например, Siri, Alexa, Cortana, Google Assistant) или устройства Интернета вещей (IoT) на базе искусственного интеллекта, взвесить все преимущества и риски, поскольку такие приложения могут раскрыть информацию о личном распорядке дня и частных разговорах.

5. Взвешивать все преимущества и риски, прежде чем разрешать третьим лицам обрабатывать персональные данные (например, нужно помнить, что голосовой помощник на смартфоне, используемый для подачи команд роботу-пылесосу, может дать третьим лицам — компаниям, правительству, киберпреступникам — доступ к данным).

6. Признавать как положительные, так и отрицательные последствия сбора, кодирования и обработки данных, в частности персональных, в цифровых технологиях на основе ИИ, таких как приложения и онлайн-сервисы.

7. Понимать, что все, чем люди делятся в Интернете (например, фотографии, видео, аудиозаписи), может быть использовано для обучения программ искусственного интеллекта. Например, коммерческие компании, разрабатывающие системы распознавания лиц с помощью ИИ, могут использовать личные изображения, размещенные в Интернете (семейные фотографии), для обучения и улучшения способности программного обеспечения автоматически распознавать людей на других изображениях, что может быть нежелательно (так как нарушает неприкосновенность частной жизни).

Использованные источники

[1] UNICEF (laetud 19.12.2023). Policy guidance on AI for children.

[2] Habli, Ibrahim; Lawton, Tom; Porter, Zoe. (2020). Artificial intelligence in health care: accountability and safety. Bulletin of the World Health Organization, 98 (4), 251-256. World Health Organization.

[3] Clario (laetud 19.12.2023). Which data can companies actually collect?

Оригинал: Kivinen, Kari. Tekoäly – mitä meidän pitäisi tietää ja osata?

Harjutused:

1. Proovi vestelda ChatGPTga.
2. Aruta grupis, milleks kasutad või kavatsed hakata kasutama tehisaruprogramme.

Lisamaterjal

Aru, Jaan. Ajust ja arust : unest, teadvusest, tehisintellektist ja muust.

ERR. „AK. Nädal”: kes kontrollib tehisaru ja millised on seejuures inimeste õigused?

ERR. Külli Taro: tehisaru mudelid vajavad kvaliteetset eesti keelt.

ERR: Novaator. Port, Kristjan. Tehisaru asendab tähelepanumajanduse inimeste kavatsuste mudimisega.

Lisamaterjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Попробуйте задать вопрос Chat GPT.
2. Обсудите в группе, для чего бы вам понадобилось использовать программы искусственного интеллекта.

Дополнительный материал

ERR: Meediataip. Роботы могут бороться с фейковыми новостями только с помощью людей.

ERR: Постановление ИИ вступило в силу: запрещены системы, нарушающие основные права человека.

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

8. Patused pettused

8. Мошенничество в Интернете

8. Patused pettused

Diana Poudel, TÜ

Peatüki eesmärgid

- Õpetada ära tundma erinevaid internetipettuseid.
- Õpetada kaitsma oma vara ja mainet digimaailmas.
- Õpetada kontrollima infot avalike tööriistade abil.

Viktoria lugu – tutvumispettus

Viktoria on 62-aastane ja elab Virumaal. Paar aastat tagasi suri tema abikaasa, kellega Viktoria kohtus kunagi ülikoolis esimesel kursusel. Viktorial on kaks last: poeg töötab Tallinnas ja tütar elab mehega Hispaanias. Kuigi lapsed helistavad Viktoriale igal nädalal ning jõulud ja jaanipäevad veedetakse alati koos, tunneb Viktoria end ikkagi väga üksikuna. Ta töötab raamatupidajana ja teeb koostööd mitmete kohalike väikeettevõtjatega, kuid enamiku tööd saab ta teha kodus.

Et end laste ja lastelaste tegemistega paremini kursis hoida, tegi Viktoria endale konto nii Facebookis kui ka Messengeris. Õhtuti veedabki ta tunde Facebookis erinevates gruppides teemasid kommenteerides ja vahel ka mõne tuttavaga sõnumeid vahetades.

Ühel õhtul saab Viktoria kirja tundmatult inimeselt. Profiilipildilt vaatab vastu temaealine mees, kelle nimi on Richard Tammiste.

„Tere. Nägin teie postitust Virumaa grupis ja lootsin, et äkki saate mind aidata. Kas teil on hetk aega suhtlemiseks?”

8. Мошенничество в Интернете

Диана Поудел, Тартуский университет

Цели главы

- Научить распознавать различное мошенничество в Интернете.
- Научить защищать свое имущество и имидж в онлайн-мире.
- Научить проверять информацию с помощью общедоступных инструментов.

История Виктории — романтическая афера

Виктория — 62-летняя бухгалтер из Вирумаа. Пару лет назад умер ее муж, с которым она познакомилась на первом курсе университета. У Виктории двое детей: сын работает в Таллинне, а дочь живет с мужем в Испании. Хотя дети звонят Виктории каждую неделю, а Рождество и Иванов день они всегда отмечают вместе, она все равно чувствует себя очень одинокой. Она работает бухгалтером и сотрудничает с несколькими мелкими предприятиями, но большую часть работы может делать дома.

Для того, чтобы быть в курсе того, что происходит у детей и внуков, Виктория завела аккаунты в Facebook и Messenger. По вечерам она проводит время в Facebook, комментируя темы в разных группах и иногда обмениваясь сообщениями со знакомыми.

Однажды вечером Виктория получила письмо от незнакомца. На фотографии профиля был мужчина ее возраста, которого звали Ричард Таммисте.

«Здравствуйте! Я увидел ваше сообщение в группе Вирумаа и надеюсь, что вы сможете мне помочь. У вас есть минутка, чтобы поговорить?»

Viktoria avas mehe profiili, kuid seal eriti palju infot ei olnud. Tegu on vist piloodiga ja elukohaks oli märgitud Kanada. Lapsed olid Viktoriat hoiatanud erinevate internetipettuste eest, kuid neid pidid tegema Nigeeria petturid ning kuidas mingi nigeerlane eesti keelt saab osata? Viktoria otsustas, et on ettevaatlik, kuid samas – mida halba siis võõras ikka Messengeris teha saab.

„Tere. Ikka on aega. Millega abi on vaja?" kirjutas Viktoria tundmatule vastuseks.

„Vajan inimest, kes aitaks mul leida veidi infot kohalikest allikatest. Nimelt tulid mu vanemad Kanadasse Eestist Teise maailmasõja ajal. Tahaksin teha ühe pikema reisi Eestisse, et veidi uurida oma vanavanemate kohta, kuid vajaksin mõnd kohalikku abilist, kes aitaks veidi seda reisi planeerida ning võib-olla ka veidi uurida mu sugupuu kohta."

Viktoria oli väga põnevil. See tundus nii loogiline ning kuna tal oli aega rohkem kui ideid, mida selle ajaga ette võtta, siis nõustus ta Richardit aitama ning järgnes paar kuud, kus nad iga päev aktiivselt suhtlesid. Viktoria õppis kasutama arhiivide veebilehti ja käis isegi paaris kirikus vanu kirikuraamatuid vaatamas, kuid kahjuks ei õnnestunud Richardi vanemate kohta infot leida. Aga kogu selle suhtluse käigus muutus nende tutvus järjest isiklikumaks ja Viktoria sai teada, et Richard on samamoodi lesk nagu tema. Tema naine oli olnud kohaliku kuulsusega kunstnik ja Richard saatis talle isegi paar fotot naise maalidest. Viktoria saatis samuti palju pilte: kuna Richardit huvitas väga Eestis toimuv, siis avastas Viktoria, et on juba nagu mingi Instagrami suunamudija, kes iga hetke päevast jäädvustab.

Kui nad olid suhelnud umbes kaks kuud, ütles Richard Viktoriale, et armastab teda ja plaanib oma maja Kanadas maha müüa ja Eestisse kolida. Talle väga meeldis väikelinn, kus Viktoria elas ning koos vaadati juba ka kinnisvarakuulutusi, sest Viktoria korter oli üsna väike ning Richard elas Kanadas päris suures ja uhkes majas.

Aga enne kui kolimisplaanid teoks saab teha, tahtis Richard oma praegusel töökohal ühe projekti ära lõpetada. Selleks pidi ta korraks Türki lendama ja hoiatas, et tal võib mobiili ja internetiga probleeme olla ja isegi jagas Viktoriaga oma pangakonto kasutajanime ja parooli, et kui reisi ajal on vaja mingeid ülekandeid teha, siis äkki Viktoria saab aidata.

Kuigi Viktoria ei tahtnud usaldust kuritarvitada, siis otsustas ta ikkagi piiluda korraks Richardi pangakontole, sest sisemuses ikkagi mingi hääl hoiatas, et kõik on liiga ilus, et olla tõsi. Ta isegi polnud lootnud, et leiab veel inimese, kellega koos tahab olla ning Richard oli nii viisakas ja tähelepanelik. Tema kadunud abikaasa oli ka väga hea mees, kuid eestlasele omaselt pigem kinnine ja vähese jutuga. Richard oli empaatiline ja tundis Viktoria tegemiste vastu nii suurt huvi, et isegi ta lapsed ja parimad sõbrad ei teadnud temast nii palju. Kuskil pidi olema mingi konks.

Richardi pangakonto šokeeris Viktoriat. Ta teadis, et Richard on majanduslikult kindlustatud, kuid näha inimese pangakontol 12 miljonit dollarit – Viktoria ei tundnud ühtegi inimest, kellel on nii palju raha. Richardile ta ei maininud, et on kontole sisse loginud, et mees teda nn kullakaevuriks ei peaks.

Järgmisel nädalal lendas Richard Ankarasse. Ta saatis lennujaamast pildi, kuid hiljem rohelist mummukest Messengeris enam ei ilmunud. Viktoria ootas terve päeva, kuid Richard ei andnud endast märku. Ta arvas, et äkki on tõesti internetiga probleeme, nagu Richard hoiatas, ja otsustas mitte kohe muretsema hakata.

Kuid järgmisel hommikul oli Viktoria postkastis kiri Richardilt.

Виктория открыла профиль мужчины, но там было мало информации. Похоже, это был пилот, живущий в Канаде. Дети предупреждали Викторию о различных интернет-мошенничествах, но этим занимались нигерийцы, а разве нигериец может говорить по-эстонски? Виктория решила, что нужно проявить осторожность. С другой стороны, что плохого может сделать незнакомый человек в Messenger?

«Здравствуйте! Конечно, время есть. Чем вам нужно помочь?» — написала Виктория незнакомцу.

«Мне нужно, чтобы кто-то помог найти информацию в местных источниках. Мои родители приехали в Канаду из Эстонии во время Второй мировой войны. Я хотел бы совершить поездку в Эстонию, чтобы поискать информацию о бабушке и дедушке, но мне нужна помощь местного жителя, чтобы спланировать поездку и, возможно, кое-что узнать о моем семейном древе».

Виктории стало очень интересно. Эта история казалась очень логичной, а поскольку времени у нее было больше, чем идей, как его проводить, она согласилась помочь Ричарду. Следующую пару месяцев они активно общались каждый день. Виктория научилась пользоваться сайтами архивов и даже посетила пару церквей, чтобы посмотреть старые церковные книги, но, к сожалению, ей не удалось найти никакой информации о предках Ричарда. Тем не менее в ходе общения их знакомство становилось все более личным, и Виктория узнала, что Ричард тоже вдовец, как и она. Его жена была известной местной художницей, и Ричард даже прислал Виктории пару фотографий ее картин. Виктория тоже отправила ему много фотографий: поскольку Ричард очень интересовался тем, что происходит в Эстонии, она обнаружила, что уже словно звезда Инстаграма снимает каждый момент своей жизни.

Примерно после двух месяцев общения Ричард признался Виктории в любви и сообщил, что планирует продать свой дом в Канаде и переехать в Эстонию. Ему очень понравился городок, где жила Виктория, и они стали вместе смотреть объявления о продаже недвижимости, потому что квартира Виктории была совсем маленькой, а Ричард в Канаде жил в большом шикарном доме.

Но перед тем, как переехать, Ричард хотел закончить проект на своей нынешней работе. Для этого ему нужно было на время улететь в Турцию, и он предупредил, что у него могут возникнуть проблемы с мобильным телефоном и интернетом. Он даже поделился с Викторией логином и паролем от своего банковского счета, чтобы, если во время поездки ему понадобится сделать какой-нибудь перевод, она могла помочь.

Хотя Виктория не хотела злоупотреблять его доверием, она решила взглянуть на банковский счет Ричарда, потому что внутренний голос предупреждал ее, что это слишком хорошо, чтобы быть правдой. Она даже не ожидала, что найдет человека, с которым захочет быть вместе, а Ричард был так вежлив и внимателен. Ее покойный муж тоже был очень хорошим человеком, но, как свойственно эстонцам, довольно замкнутым и неразговорчивым. Ричард сопереживал и проявлял к делам Виктории такой интерес, что даже ее дети и лучшие друзья о ней столько не знали. Где-то здесь должна была быть приманка.

Банковский счет Ричарда поверг Викторию в шок. Она знала, что Ричард финансово обеспечен, но на банковском счете мужчины оказалось 12 миллионов долларов! Виктория не знала никого, у кого были бы такие деньги. Она не сказала Ричарду, что посмотрела его счет, чтобы он не подумал, что ей нужны только деньги.

На следующей неделе Ричард вылетел в Анкару. Он отправил фотографию из аэропорта, но позже зеленой точки в Messenger уже не было. Виктория ждала весь день, но Ричард так ничего и не написал. Она подумала, что у него могут быть проблемы с Интернетом, как он и предупреждал, и решила, что не стоит сразу беспокоиться.

„Mu kallis Viktoria, ma ei tea, kuidas sulle seda öelda, aga olen sattunud hätta. Türgis pangad streigivad ja ma ei saa oma kontole ligi. Lennujaamas varastati mu rahakott ja mul pole isegi raha hotelli eest maksta. Palun, kas sa saaksid mulle natuke raha saata, et ma saaksin oma projekti lõpetada ja koju tagasi tulla? Ma tean, et see on väga suur palve, aga sa oled ainus inimene, keda ma usaldan. Siin on üks konto, millele saad raha kanda."

Viktoria oli kirjast šokeeritud, aga samas teadis, et Richard oli temaga alati aus olnud. Ta oli ju isegi jaganud oma pangakonto andmeid, mis kinnitasid tema jõukust. „See on ajutine probleem," mõtles Viktoria. „Ta maksab kindlasti kõik tagasi, kui koju jõuab."

Richard helistas talle järgmisel päeval ja oli mureliku häälega. Ta tänas Viktoriat usalduse eest ja kinnitas, et maksab raha tagasi kohe, kui saab Kanadasse naasta. Viktoria, kes polnud kunagi osanud kedagi altkäemaksus või pettuses kahtlustada, oli talle üle kandnud 3000 eurot oma säästudest, lootes, et aitab armastatu raskest olukorrast välja. Richard tänas teda veel kord ja saatis uue foto, kus ta paistis hotelli fuajees istuvat.

Nädala pärast tekkis aga uus mure. Richardi sõnul olid Türgis probleemid süvenenud: lennujaamas oli protestide tõttu tekkinud kaos ja ta ei saanud tagasi Kanadasse lennata. Lisaks olid tema pangakontod väidetavalt blokeeritud rahvusvaheliste ülekannete tõttu. „Mul on vaja natuke rohkem raha, et siin edasi olla ja lõpuks koju pääseda," kirjutas Richard. Viktoria süda värises, kuid tema säästud olid juba otsas.

Richard pakkus, et Viktoria võiks ajutiselt võtta välja oma pensionifondi raha. „See on vaid ajutine lahendus," veenis ta. „Kohe, kui saan Kanadasse tagasi, maksan sulle tagasi kahekordselt. Sa oled mu ingel, mu elupäästja!" Tema palved tundusid nii siirad, et Viktoria tegi raske otsuse – võttis välja 12 000 eurot oma pensionifondist ja saatis Richardile.

Richard tänas taas ning saatis isegi video, kus rääkis, kuidas ta unistab nende koosolemisest Eestis. „Viktoria, sa oled ainus inimene, kes mind mõistab. Kohe, kui see kaos möödub, olen ma sinu kõrval," lubas ta.

Aga siis Richard kadus. Ei sõnumeid, ei kõnesid. Viktoria ootas nädalaid, lootes, et tal on lihtsalt internetiprobleemid, kuid sisemiselt hakkas tõde kohale jõudma. Ühel hommikul, pärast öö läbi otsimist internetis, leidis ta foorumi, kus hoiatati selliste skeemide eest. Ta leidis isegi Richardi pildi – sama mees, kes oli tema elu viimastel kuudel nii palju muutnud.

Süda valutas ja pisarad voolasid, kui Viktoria lõpuks tõde tunnistas. Ta oli kaotanud mitte ainult oma säästud ja osa pensionist, vaid ka usalduse iseenda otsustusvõime vastu. Ta tundis end petetu ja häbistatuna.

Järgnevatel kuudel oli Viktorial keeruline toime tulla. Ta pöördus politseisse ja andis kogu info edasi, kuid sai teada, et raha tagasi saada on peaaegu võimatu – selliseid skeeme juhitakse tihti anonüümsete rahvusvaheliste võrgustike kaudu. Viktoria lapsed olid mures ja šokeeritud, kui said teada, mis oli juhtunud. Nad toetasid ema, kuid ka nende usaldus oli löögi saanud.

Lõpuks otsustas Viktoria oma loo avalikustada. Ta andis intervjuu kohalikule ajalehele ja rääkis, kuidas tema üksildus ja vajadus läheduse järele olid ta muutnud pimedaks ilmselgete ohumärkide ees. Tema lugu jõudis paljude inimesteni ja pani neid mõtlema oma internetikäitumise üle. Viktoria alustas ka teavitustööd kogukonnas, et aidata teistel vanematel inimestel ära tunda internetipettusi ja kaitsta end ohtude eest.

Kuigi Viktoria elu ei olnud enam endine, õppis ta sellest kogemusest midagi olulist: üksildus võib teha inimese haavatavaks, kuid teadlikkus ja kogukonna toetus aitavad uuesti jalule tõusta.

Но на следующее утро Виктории пришло электронное письмо от Ричарда.

«Моя дорогая Виктория, я не знаю, как сказать тебе об этом, но у меня проблемы. Банки в Турции бастуют, и я не могу получить доступ к своему счету. У меня украли бумажник в аэропорту, и у меня даже нет денег, чтобы заплатить за гостиницу. Не могла бы ты отправить мне немного денег, чтобы я мог закончить свой проект и вернуться домой? Я знаю, что это большая просьба, но ты единственный человек, которому я доверяю. Вот счет, на который можно перевести деньги».

Виктория была шокирована письмом, но она знала, что Ричард всегда был честен с ней. В конце концов, он даже поделился данными банковского счета, что подтверждало его богатство. «Это временная проблема, — подумала Виктория. — Он обязательно отдаст долг, когда вернется домой».

Ричард позвонил ей на следующий день, и голос у него был встревоженный. Он поблагодарил Викторию за доверие и заверил, что вернет ей деньги, как только сможет вернуться в Канаду. Виктория, которая никогда не подозревала никого во взяточничестве или мошенничестве, перевела ему 3000 евро из своих сбережений, надеясь помочь возлюбленному выйти из сложной ситуации. Ричард еще раз поблагодарил ее и прислал новую фотографию, где он сидит в холле отеля.

Однако неделю спустя возникла новая проблема. По словам Ричарда, проблемы в Турции усугубились: в аэропорту начался хаос из-за протестов, и он не смог вылететь обратно в Канаду. Кроме того, его банковские счета якобы заблокировали из-за международных переводов. «Мне нужно еще немного денег, чтобы жить здесь и наконец вернуться домой», — написал Ричард. Виктория очень переживала за него, но ее сбережения уже закончились.

Ричард предложил Виктории временно взять деньги из ее пенсионного фонда. «Это только временное решение», — заверил он. — Как только я вернусь в Канаду, то верну тебе долг вдвойне. Ты мой ангел, моя спасительница!» Его мольбы казались настолько искренними, что Виктория приняла непростое решение — взяла 12 000 евро из своего пенсионного фонда и отправила их Ричарду.

Ричард еще раз поблагодарил ее и даже прислал видео, где говорил, как он мечтает, чтобы они были вместе в Эстонии. «Виктория, ты единственный человек, который меня понимает. Как только этот хаос закончится, я буду рядом с тобой», — пообещал он.

Но потом Ричард исчез. Ни сообщений, ни звонков. Виктория ждала несколько недель, надеясь, что у него просто проблемы с интернетом, но внутренне начала догадываться, что случилось. Однажды утром после ночи поисков в Интернете она нашла форум, где предостерегали от подобных схем. Она даже нашла фото Ричарда — того самого мужчины, который так изменил ее жизнь за последние месяцы.

Ее сердце сжалось от боли и потекли слезы, когда Виктория наконец признала правду. Она потеряла не только сбережения и часть пенсии, но и уверенность в своей способности принимать решения. Она чувствовала себя обманутой и униженной.

Следующие месяцы были для нее очень сложными. Она обратилась в полицию и передала всю информацию, но узнала, что вернуть деньги практически невозможно — подобные схемы часто проворачиваются через анонимные международные сети. Дети Виктории были обеспокоены и шокированы, когда узнали о случившемся. Они поддержали мать, но их доверию тоже был нанесен удар.

В конце концов Виктория решила рассказать о своей истории людям. Она дала интервью местной газете и рассказала, как одиночество и потребность в близости привели к тому, что она проигнорировала очевидные признаки опасности. Ее историю узнало много людей, которых она заставила задуматься о поведении в Интернете. Виктория начала просветительскую работу,

Alexandri lugu – investeerimispettus

Alexander on Harjumaalt pärit 65-aastane mees, kes läks alles hiljuti pensionile. Pärast aastakümneid kestnud tööd ehituses oli tal lõpuks aega, et nautida elu lihtsaid rõõme: hommikused jalutuskäigud metsas, kalapüük ja ajalehtede lugemine kohvikus. Kuid pensionile jäämine tõi kaasa ka üksinduse, mida Alexander polnud varem tundnud. Tema abielu lõppes aastaid tagasi ning lapsi tal ei olnud.

Ühel õhtul otsustas Alexander proovida midagi uut ja liitus tutvumisportaaliga, mida oli reklaamis näinud. Kuigi esialgu skeptiline, leidis ta mõne päeva pärast oma postkastist sõnumi: „Tere, armas Alexander. Olen Maria. Leidsin su profiili ja tundsin, et pean sulle kirjutama." Sõnum oli soojalt ja sõbralikult kirjutatud ning Alexander tundis kohe uudishimu.

Maria oli 35-aastane naine, kes kirjutas, et töötab rahvusvahelises ettevõttes ja armastab reisida. Tema profiilipildil naeratas tumedapäine kaunitar ning tema sõnades oli midagi siirast ja ligitõmbavat. „Vanus on vaid number," kirjutas Maria. „Ma tunnen, et vanemad mehed on palju elukogenumad ja kindlamad – täpselt sellist partnerit ma otsin." Alexander tundis end erilisena ja hakkas iga päev Mariale kirjutama.

Nende suhtlus muutus kiiresti intiimseks ja isiklikuks. Maria jagas oma unistust reisida ümber maailma ning rääkis, kuidas ta loodab leida kaaslast, kellega seda teha. „Alexander, ma tunnen, et meie vahel on midagi erilist," kirjutas ta ühel õhtul. Alexander tundis end taas noorena ja tema igapäevased vestlused Mariaga täitsid ta elu uue energiaga.

Paar kuud pärast suhtluse algust tõstatas Maria äkitselt investeerimise teema. „Mu kallis, ma olen otsinud viisi, kuidas reisiks raha koguda, ja leidsin ideaalse võimaluse," rääkis ta. Maria selgitas, et on avastanud eksklusiivse investeerimisplatvormi, kus tema kolleegid olevat juba suuri kasumeid teeninud. „Kui me mõlemad paneme sinna raha, kasvab see kiiresti ja saame oma unistuse ellu viia – reisida koos maailma kõige ilusamatesse paikadesse!"

Alexander, kes polnud kunagi varem investeerimisega tegelenud, kahtles alguses. Kuid Maria veenis teda, saates lingi platvormi veebilehele, mis nägi välja professionaalne ja usaldusväärne. Lisaks näitas Maria Alexandrile oma kontojääki platvormil, see oli paari kuuga mitmekordistunud. „Usalda mind, mu arm. See on meie tulevik," kinnitas Maria.

Alexander otsustas proovida. Ta kandis platvormile esmalt 5000 eurot oma säästudest. Maria kiitis teda ja lubas, et see on alles algus. „Kui sa julged panustada rohkem, siis kasvab meie võimalus veelgi kiiremini," rääkis ta entusiastlikult.

Paari nädala pärast ütles Maria, et tal on vaja Alexandri abi, et suurendada nende investeeringut. Alexander müüs oma vana auto ja kandis raha platvormile. Kui Maria ütles, et suuremate kasumite saamiseks tuleks teha viimane panus, otsustas Alexander ka oma pensionifondi raha osaliselt välja võtta. Kokku investeeris ta 25 000 eurot.

Alguses tundus kõik hästi olevat. Platvorm näitas iga päev kasvavat saldot ja Maria saatis talle pidevalt ka kruiiside linke, et Alexander aitaks järgmiseks talveks parima reisi välja valida.

Kuid ühel päeval ei saanud Alexander enam platvormi veebilehele sisse logida. Ta kirjutas Mariale, kuid naine vastas napilt: „Ära muretse, see on ajutine tehniline probleem."

Järgmistel päevadel vaikis Maria aga järjest pikemalt. Tema vastused olid üha harvemad ja lõpuks kadus ta sootuks. Alexander tundis, kuidas mure ja kahtlus teda valdavad. Ta otsustas võtta ühendust pangaga ja uurida, mis toimub. Seal selgus tõde: platvorm, kuhu Alexander oli raha kandnud, oli seotud rahvusvahelise petuskeemiga.

чтобы помочь другим пожилым людям распознать мошенничество в Интернете и защитить себя от опасностей.

Хотя жизнь Виктории уже не была прежней, она вынесла из этого опыта нечто важное: одиночество может сделать человека уязвимым, но осведомленность и поддержка сообщества помогут снова встать на ноги.

История Александра — инвестиционное мошенничество

Александр — 65-летний мужчина из Харьюмаа, который только недавно вышел на пенсию. После многолетней работы в строительной отрасли у него наконец-то появилось время наслаждаться простыми радостями жизни: гулять утром по лесу, ловить рыбу и читать газеты в кафе. Но выход на пенсию принес и одиночество, которого Александр никогда раньше не чувствовал. Его брак распался много лет назад, детей у него не было.

Как-то вечером Александр решил попробовать кое-что новое и зарегистрировался на портале знакомств, который увидел в рекламе. Хотя поначалу он был настроен скептически, через несколько дней он обнаружил в своем почтовом ящике сообщение: «Здравствуйте, дорогой Александр! Меня зовут Мария. Я нашла ваш профиль и почувствовала, что должна написать вам». Сообщение было написано в теплой и дружеской манере, и Александру сразу же стало любопытно.

Мария — 35-летняя женщина, которая написала, что работает в международной компании и любит путешествовать. С фотографии в профиле улыбалась темноволосая красавица, и в ее словах было что-то искреннее и притягательное. «Возраст — это всего лишь цифра, — писала Мария. Мне кажется, что мужчины постарше гораздо опытнее и увереннее в себе — именно такого партнера я и ищу». Александр почувствовал себя особенным и стал писать Марии каждый день.

Их общение быстро стало интимным и личным. Мария поделилась своей мечтой о кругосветном путешествии и рассказала, что надеется найти для этого спутника. «Александр, я чувствую, что между нами есть что-то особенное», — написала она однажды вечером. Александр снова почувствовал себя молодым, а ежедневные беседы с Марией наполнили его жизнь новой энергией.

Через пару месяцев отношений Мария неожиданно подняла тему инвестиций. «Дорогой, я искала способ накопить деньги на поездку и нашла прекрасную возможность», — сообщила она. Мария рассказала, что открыла для себя эксклюзивную инвестиционную платформу, где ее коллеги уже получили большую прибыль. «Если мы оба вложим туда деньги, они быстро вырастут, и мы сможем осуществить нашу мечту — вместе путешествовать по самым красивым местам мира!»

Александр, который никогда раньше не занимался инвестициями, поначалу сомневался. Но Мария убедила его, прислав ссылку на сайт платформы, которая выглядела профессионально и заслуживала доверия. Кроме того, Мария показала Александру баланс своего счета на платформе, который за пару месяцев увеличился в несколько раз. «Доверься мне, любимый. Это наше будущее», — заверила его Мария.

Александр решил попробовать. Сперва он перевел на платформу 5000 евро из своих сбережений. Мария похвалила его и пообещала, что это только начало. «Если ты решишься вложить больше, наши шансы вырастут еще быстрее», — с энтузиазмом сказала она.

Через пару недель Мария сказала, что ей нужна помощь Александра, чтобы увеличить их инвестиции. Александр продал свой старый автомобиль и перевел деньги на платформу. Когда Мария сказала, что для получения большего дохода нужно сделать последний взнос, Александр тоже решил снять часть своего пенсионного фонда. В общей сложности он вложил 25 000 евро.

Alexander tundis, kuidas kogu tema maailm kokku varises. Ta oli kaotanud suurema osa oma säästudest ja pensionifondi raha. Kõige valusam oli aga emotsionaalne pettumus – tunne, et keegi oli kasutanud ära tema üksindust ja usaldust.

Alexander hakkas käima kohalikus pensionäride klubis, leidis uusi sõpru ja otsustas, et enam ta oma üksindusel end nõrgaks muuta ei lase. Elu andis talle õppetunni, kuid ka uue alguse.

Kuidas ennast kaitsta

Kuidas veebituttava tausta kontrollida

- Kasuta pildituvastustehnoloogiat Google Lens, et teada saada, kas profiilil olevaid pilte on ka mujal kasutatud.

  Samasuguste piltide puudumine ei pruugi samas tähendada, et neid ei ole, sest tihti võtavad petturid pildid kellegi sotsiaalmeediakontolt ja neid Google'i otsing ei indekseeri. Samuti kasutatakse järjest rohkem tehisaru abil loodud sisu ning neid pilte otsinguga ka ei leia.

- Tee videokõne.

  Videokõne puhul tuleb väga täpselt jälgida, kas tegu on ikka päris videokõnega või kasutatakse tehisaru abil tehtud videotöötlust: siis näiteks ei liigu huuled koos sõnade ütlemisega, videos vahepeal taust kuidagi väreleb vmt.

- Küsi täiendavat informatsiooni või palu saata link tema mõnele teisele sotsiaalmeediaprofiilile.

  Kui suhtled petturiga, siis ei aita see, kui küsid rohkem infot, sest petturid on endale päris põhjalikud profiilid loonud. Samuti pole petturil keeruline teha endale samasugused kontod Instagrami, Facebooki ja LinkedIn-i.

Kuidas internetis turvaliselt laenu anda

- Tuleb sõlmida leping.

  Aga kui suhtled petturiga, siis pole lepingust kasu.

- Tuleb enne küsida dokumendifotot.

  Internetis on veebilehed, mis müüvad varastatud dokumendifotosid ja samuti on petturitel kombeks oma ohvritelt dokumendipilte välja meelitada – seega dokumendifoto ei garanteeri midagi.

- Kasuta mõnd platvormi, mis on mõeldud laenude vahendamiseks.

  Internetis on lehti, kus saab investeerida oma raha laenude andmiseks, kuid ei ole veebilehti, mis vahendaks/garanteeriks laenu konkreetselt eraisikult konkreetsele eraisikule. Kui keegi väidab, et mingi veebileht sellist teenust pakub, siis on tegu pettusega.

Поначалу все казалось прекрасным. С каждым днем баланс на платформе увеличивался, и Мария присылала ему ссылки на круизы, чтобы Александр помог ей выбрать лучший круиз на следующую зиму.

Но в один прекрасный день Александр больше не смог войти на сайт платформы. Он написал Марии, но женщина коротко ответила: «Не беспокойся, это временная техническая проблема».

Однако в последующие дни Мария молчала все дольше и дольше. Ее ответы приходили все реже и реже, и в конце концов она совсем исчезла. Александр почувствовал, как им овладевают беспокойство и сомнения. Он решил связаться с банком и выяснить, что происходит. Вскрылась правда: платформа, на которую Александр переводил деньги, была связана с международной мошеннической схемой.

Александр почувствовал, как весь его мир рушится. Он потерял большую часть своих сбережений и денег из пенсионного фонда. Но самым болезненным было эмоциональное разочарование — чувство, что кто-то воспользовался его одиночеством и доверием.

Александр начал ходить в местный клуб пенсионеров, завел новых друзей и решил, что больше не позволит одиночеству сделать его слабым. Жизнь преподнесла ему урок, но дала возможность начать все сначала.

Как себя защитить

Как проверить подлинность личности знакомого в Интернете

- Используйте технологию распознавания изображений Google Lens, чтобы узнать, использовались ли фотографии профиля в других местах.

  Однако отсутствие таких изображений не обязательно означает, что их не существует, поскольку мошенники часто берут изображения из чьих-то профилей в социальных сетях, а они не индексируются в поиске Google. Кроме того, все чаще используется контент, сгенерированный ИИ, и такие изображения с помощью поиска не найти.

- Проведите видеозвонок.

  При этом нужно обратить внимание, настоящий ли это видеозвонок или используется обработка видео при помощи ИИ: например, губы не двигаются, когда человек говорит, фон на видео мерцает и т. д.

- Запросите дополнительную информацию или попросите ссылку на другой профиль в других социальных сетях.

  Если вы имеете дело с мошенником, просьба предоставить больше информации не поможет, поскольку мошенники создают себе довольно подробные профили. Мошеннику также не составит труда создать аналогичные аккаунты в Instagram, Facebook и LinkedIn.

- Internetis pole võimalik turvaliselt laenu anda.

  Laenu andmine on alati risk ning kui annad laenu inimesele, keda sa päris-elus ei tunne, siis peaksid suhtuma laenuandmisse pigem kui annetusse või kingitusse.

Kuidas ära tunda investeerimispettust

- Lubatakse kiiresti väga suurt tootlust.
- Püütakse pidevalt survestada suuremaid summasid lisaks investeerima.
- Veebileht on loodud hiljuti või omanik on varjatud.
- Veebileht näeb välja kole või on kehvasti kujundatud.

  Aga tihti näevad petulehed paremad välja kui pärislehed ning on kurjategijaid, kes pakuvadki teistele petturitele kiiret veebilehtede loomise teenust.

Как безопасно одолжить деньги в интернете

- Необходимо заключить договор.

  Но если вы имеете дело с мошенником, от договора пользы не будет.

- Перед этим необходимо попросить фото документа.

  В Интернете есть сайты, продающие краденые фото документов. Мошенники также имеют привычку выманивать фотографии документов у своих жертв, так что фото документа не является гарантией.

- Воспользуйтесь одной из платформ, предназначенных для посредничества при выдаче кредитов.

  В интернете есть сайты, где можно вложить свои деньги, чтобы они использовались для займов, но нет ни одного сайта, который гарантировал бы займ от конкретного человека конкретному человеку. Если кто-то утверждает, что какой-то сайт предлагает такую услугу, это мошенничество.

- Безопасно одолжить деньги в интернете нельзя.

  Займ — это всегда риск, и если вы даете взаймы незнакомому человеку, то относитесь к этому скорее как к подарку или пожертвованию.

Как распознать инвестиционное мошенничество

- Вам очень быстро обещают очень высокую прибыль.
- На вас постоянно давят, чтобы вы инвестировали больше.
- Сайт был создан недавно или его владелец скрыт.
- Сайт выглядит некрасиво или плохо оформлен.

  Тем не менее, часто мошеннические сайты выглядят лучше, чем настоящие, и есть преступники, которые предлагают другим мошенникам услуги по быстрому созданию сайтов.

Harjutused

Harjutuste materjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

Упражнения найдете по ссылке:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

8.1. Miks võltsida veebilehti?

Diana Poudel, TÜ

Internetis on kaks miljardit veebilehte ning väga keeruline on öelda, kui paljud neist on loodud mingil hämaral eesmärgil, kuid kindlasti on petulehti rohkem kui ausaid veebilehti. Seetõttu võib igaüks meist sattuda lehele, mille eesmärk ei ole pakkuda meile tõest infot või meeldivat meelelahutust, vaid lehe omaniku esmane eesmärk on levitada valet, saada ligipääs sinu rahale või õngitseda andmeid.

Väga tihti inimesed arvavad, et petulehe tunneb ära, kuna sealses tekstis on kirjavead või näeb leht kuidagi ebausaldusväärne välja. Tegelikult on nii, et petulehed võivad välja näha usaldusväärsemad kui pärislehed ning neid tuvastada võib olla väga keeruline. Samas on näiteid ka väga kehvasti tehtud petulehtedest, mis ikkagi suudavad inimese ära petta.

Õngitsuslehed

Need lehed üritavad end maskeerida tuntud veebilehtede sarnaseks. Näiteks võib luua õngitsuslehe, mis näeb välja täpselt nagu Facebook. Sealt siis saadetakse inimesele kiri teatega, et keegi üritab tema Facebooki kontot varastada ning ta peaks kohe minema ja Facebooki lehele sisse logima, et seaded üle vaadata. Kirjas on ka link ning kui inimene sellel klikib, siis avaneb leht, mis näeb välja nagu Facebooki sisselogimisleht. Kui inimene nüüd sisestab sinna oma andmed, siis leht lihtsalt suunab inimese õigele Facebooki lehele ning ta ei pruugi isegi mõista, et on oma parooli sisestanud valel lehel. Pätid aga koguvad kontode kasutajatunnused ja paroolid kokku ning müüvad need tumeveebis järgmisele pätile, kes siis inimeste kontod üle võtab.

Sellise pettuse vastu aitab, kui sul on Facebookis vormistatud kaheastmeline autentimine ning samuti soovitan vältida e-kirjades olevatele linkidele klikkimist, avada ise veebilehitseja ja kirjutada sinna ise facebook.com.

Teine väga levinud pettus on panga õngitsusleht. Seal suunatakse inimene näiliselt oma pangakontole sisse logima, kuid tegemist on petulehega. Samal ajal on pätt valvel ja kui inimene sisestab oma kasutajatunnuse, siis pätt sisestab selle õige panga lehele ning kuvab siis ohvrile näiteks Smart-ID kinnituskoodi, mida ta ise näeb veebilehel. Ohvrile tuleb Smart-ID teavitus ning kuna ka ekraanil olev kood on sama, siis lastakse pätt oma kontole sisse. Nüüd hakkab pettur kiiresti ülekandeid vormistama, kuid ohvrile kuvatakse mingi pikk juriidiline dokument, mis siis tuleb PIN2-koodiga allkirjastada. Tegelikult on nii, et kui ohver sisestab PIN2-koodi, siis ta kinnitab need ülekanded, mille pätt tema kontolt tegi.

Sellise pettuse puhul on esmalt väga oluline alati kontrollida veebilehe aadressi, millelt sa sisse logid. Ära kunagi sisene panka e-kirjas oleva lingi kaudu. Samuti aitab pangapettuste puhul oma konto limiitide minimaalseks muutmine. Siis peab pätt sinult mitu korda järjest PIN2-koodi välja petma ja see tundub juba palju kahtlasem.

8.1. Почему подделывают сайты?

Диана Поудел, Тартуский университет

В Интернете насчитывается два миллиарда сайтов, и трудно сказать, сколько из них было создано с какими-либо неблаговидными целями, но мошеннических сайтов точно больше, чем подлинных. Именно поэтому любой из нас может попасть на сайт, который создан не для того, чтобы давать правдивую информацию или развлекать людей, а для того, чтобы распространять ложь, получить доступ к вашим деньгам или выудить данные.

Люди часто думают, что могут распознать мошенничество по опечаткам в тексте или подозрительному облику сайта. На самом деле поддельные страницы могут выглядеть более надежно, чем настоящие, и их очень трудно распознать. Однако есть и примеры очень плохо сделанных мошеннических сайтов, которые все же умудряются обмануть людей.

Фишинговые сайты

Эти страницы маскируются под известные вебсайты. Например, можно создать фишинговый сайт, который будет выглядеть в точности как Facebook. С него людям рассылают сообщения о том, что кто-то пытается украсть их учетную запись и им следует немедленно зайти на свою страницу в Facebook и проверить настройки. В письме есть ссылка, при нажатии на которую открывается страница, похожая на страницу входа в Facebook. Если человек введет свои данные, сайт просто перенаправит его на нужную страницу Facebook, и он может даже не понять, что ввел пароль не на той странице. Мошенники же собирают имена пользователей и пароли и продают их в даркнете следующему мошеннику, который затем крадет учетные записи людей.

Против этого вида мошенничества поможет двухфакторная аутентификация в Facebook. Также советую не нажимать на ссылки в электронных письмах, а открыть браузер и набрать в нем facebook.com.

Еще одно очень распространенное мошенничество — фишинговый сайт, имитирующий страницу банка. Он имитирует перенаправление для входа в банковский счет, но на самом деле это поддельная страница. Мошенник начеку, и когда человек указывает свой идентификатор пользователя, тот вводит его на нужной странице банка, а затем показывает жертве, например, код подтверждения Smart-ID, который видит на сайте. Жертва получит уведомление Smart-ID, и поскольку код на экране совпадает, пускает мошенника в свою учетную запись. Мошенник начинает быстро совершать переводы со счета, а жертве показывают длинный юридический документ, который нужно подтвердить PIN2-кодом. На самом деле, когда жертва вводит PIN2-код, она подтверждает переводы, сделанные преступником с ее счета.

E-poodide pettused

Järjest enam inimesi ostab kaupa internetist ning seetõttu on järjest enam ka pettuseid, kus luuakse e-pood eesmärgiga inimese kaardiandmed kätte saada. Kõige levinum on pettus, kus e-poes pakutakse väga soodsa hinnaga kaupa. Tavaliselt inimesed kahtlustavad, et e-pood ei saada kaupa või saadab ebakvaliteetse kauba, kuid kui mõni ihaldusväärne asi on 90% soodustusega, siis inimene mõtleb, et ta ikkagi riskib selle väikese summaga. Selle peale pätid muidugi loodavadki, sest nende eesmärk on kätte saada ohvri krediitkaardiandmed.

Kui sa hakkad tundmatust e-poest kaupa tellima, siis tee sellele poele alati põhjalik taustakontroll: kontrolli, kellele kuulub selle e-poe veebiaadress. Seda saad teha näiteks päringuga lehel who.is, mis näitab, millal on veebileht registreeritud ja kellele see kuulub. Kui näed, et see domeen on alles hiljaaegu registreeritud või omanik on varjatud, siis kindlasti ära anna oma krediitkaardi andmeid. Samuti võid veebilehtede kontrolliks kasutada ScamAdviseri tööriista.

Tehnilise toe pettused ja viirused

Mõned veebilehed püüavad külastaja arvutisse installida pahavara. Selle vastu üldiselt aitab pidevalt uuendatud viirusetõrje. Aga mõnikord kuvatakse veebilehel mingi tehnilise vea kirjeldus, mis väidab, et kasutaja arvutiga on midagi väga pahasti ning teatele on lisatud ka telefoninumber, kuhu kasutajal palutakse kohe helistada. Kui ohver seda teeb, siis saab ta ühendust pätiga, kes nüüd palub ohvril alla laadida mingi kaughaldustarkvara nagu näiteks AnyDesk, TeamViewer, UltraViewer või mõni muu sarnane programm. Kui ohver seda teeb, siis saab pätt kontrolli ohvri arvuti üle ning sealt edasi püütakse ohvrit pettusega meelitada pangakontole sisse logima, et pätt saaks sealt ülekandeid teha.

Kui sul ilmub arvuti ekraanile mingi veateade, siis esmalt püüa veebileht kinni panna ja siis vajadusel taaskäivita arvuti. Kui veateade püsib, siis küsi nõu mõnelt tuttavalt IT-inimeselt või vii arvuti remonti, kuid ära mitte kunagi helista tundmatul numbril ja veel vähem ära lae alla programme võõra inimese soovitusel.

Loteriid ja loosimised

Inimestele meeldib unistada lotovõidust ja selle peale pätid loodavadki. Tihti on need loteriid kujundatud mõne tuntud brändi järgi: näiteks Telia, Elisa, Kaubamaja, Samsung jne. Ohvril palutakse jätta sellel lehel oma kontaktandmed.

Siit võib pettus hargneda erinevates suundades. Sulle saadetakse näiteks kiri, et oledki võitnud ja edasi manipuleerib pätt sind osavalt hoopis talle raha üle kandma. Sinu veebilehitsejasse võidakse lisada küpsised, mis muudavad sind igasugu järgnevate pettuste sihtmärgiks, kuna sinu andmed müüakse tumeveebis teistele pättidele. Selliseid petuvõimalusi on kindlasti veel palju rohkem.

Pigem püüa vältida loto mängimist kahtlastel lehtedel ning kui tunned, et sul on hetkel Fortuunaga kuidagi väga head suhted, siis mine ja osta üks lotopilet eestiloto.ee lehelt. Suure tõenäosusega sa ei võida, kuid vähemalt piirdub rahaline kahju selle ühe lotopileti hinnaga.

Во избежание такого мошенничества важно всегда сначала проверить адрес сайта, с которого вы входите в систему. Никогда не заходите в банк по ссылке в электронном письме. Чтобы предотвратить банковское мошенничество, стоит также установить для счета минимальные лимиты. Тогда мошеннику придется запрашивать PIN2-код несколько раз, и это будет выглядеть гораздо более подозрительно.

Мошенничество с интернет-магазинами

Все больше людей совершают покупки в Интернете, а потому все чаще появляются мошеннические сайты интернет-магазинов, цель которых — получить данные карты человека. Самый распространенный вид мошенничества — когда интернет-магазин предлагает товар по очень низкой цене. Обычно люди подозревают, что интернет-магазин не отправит покупку или пришлет некачественный товар, но если на него действует скидка 90%, они думают, что это в любом случае невеликий риск. На это, конечно, и рассчитывают мошенники, ведь их цель — получить данные кредитной карты жертвы.

Если вы заказываете товар в неизвестном магазине, всегда тщательно проверяйте информацию о нем: узнайте, кому принадлежит интернет-адрес магазина. Это можно сделать, например, с помощью запроса на странице WhoIs, которая показывает, когда был зарегистрирован сайт и кто является его владельцем. Если вы видите, что домен был зарегистрирован совсем недавно или его владелец скрыт, не стоит сообщать данные своей кредитной карты. Для проверки сайтов также можно использовать инструмент ScamAdviser.

Мошенничество с техподдержкой и вирусы

Некоторые сайты пытаются установить на компьютер посетителя вредоносное программное обеспечение. Обычно против этого помогает регулярное обновление антивируса. Но иногда на сайте видно описание технической ошибки, где говорится, что с компьютером пользователя что-то не так. Сообщение сопровождается номером телефона, по которому пользователя просят немедленно позвонить. Если жертва сделает это, с ней свяжется мошенник, который попросит ее загрузить программу для удаленного управления компьютером, такую как AnyDesk, TeamViewer, UltraViewer или аналогичную. Если жертва сделает и это, компьютер жертвы перейдет под контроль мошенника. Далее жертву обманным путем постараются убедить зайти на сайт банка, чтобы мошенник смог перевести оттуда деньги.

Если на экране компьютера появляется сообщение об ошибке, попробуйте сперва закрыть вебсайт, а затем при необходимости перезагрузить компьютер. Если сообщение сохраняется, спросите совета у знакомого IT-специалиста или отнесите компьютер в ремонт, но никогда не звоните по незнакомому номеру и тем более не устанавливайте программы по совету незнакомых людей.

Лотереи и розыгрыши

Людям нравится мечтать, что они выиграют в лотерею, и мошенники надеются именно на это. В основе таких лотерей часто лежит известный бренд: Telia, Elisa, Kaubamaja, Samsung и т. д. Жертву просят оставить на сайте свои контактные данные.

Далее мошенническая схема может быть разной. Например, вы получаете письмо с сообщением о выигрыше, а затем мошенник ловко манипулирует вами, чтобы вы перевели ему деньги. В ваш браузер добавляют файлы cookie, что делает вас мишенью для всевозможных последующих афер, поскольку ваши данные продали в даркнете другим мошенникам. Безусловно, есть и другие возможности.

Investeerimispettused

Väga jõudsalt kasvav petuskeem, kus luuakse väga uhke veebikeskkond, kuhu siis inimesed meelitatakse „investeerima". Ohvrile lubatakse suurt tulu ja kui ta esimese väikese summa oma kontole paneb, siis näebki, kuidas raha hakkab kasvama nagu kevadine umbrohi. Siis julgustatakse teda aina täiendavalt investeerima ning ka suurem summa kasvab mühinal. Probleemid tekivad, kui inimene hakkab oma investeeringut välja võtma. Siis selgub, et ta peab maksma täiendavaid makse ning kui ta lõpuks aru saab, et langes pettuse ohvriks ja hakkab internetist uurima, kuidas raha tagasi saada, siis tihti satutakse järgmisele petulehele, kus keegi väidab, et suudab petturid tabada. Muidugi on ka see vale, kuid selle lubadusega suudetakse tihti ohvritelt veel täiendavad rahasummad välja petta.

Petulehed on loodud nii, et pettur ise reguleerib, kui palju ohvri raha kasvab või kahaneb ja reaalsusega ei ole seal mingit pistmist. Aga kahjuks võib ka praegusel hetkel olla tuhandeid selliseid ohvreid, kes isegi veel ei tea, et nad on petta saanud, vaid investeerivad iga kuu ja unistavad pensionipõlvest Kariibi mere saartel.

Siin on hästi lihtne reegel see, et pole mõtet investeerida tundmatul lehel ja kui keegi lubab ebamõistlikult suurt tulu, siis see on ilmselge märk pettusest. Kui tahad investeerida, mis on ju igati mõistlik plaan, siis alusta oma III pensionisambast või uuri kodupangast erinevaid investeerimisvõimalusi.

Muud pettused

Tegelikult võibki jääda kirjeldama erinevaid pettuseid. Näiteks saadeti mõned aastad tagasi maksuameti nimel kiri, kus väideti, et inimeselt on liiga palju tulumaksu küsitud ja paluti avaldus teha, et raha tagasi saada. Õngitsusleht nägi väga sarnane välja maksuameti pärislehega ja petturid üritasid inimesi panna seal oma pangaandmeid avaldama.

Väga palju levib praegu ka SMS-pettusi, kus väidetakse, et inimese tellitud pakiga on mingeid probleeme, ja kui inimene klikib lingil, siis suunatakse ta Omniva/DPD/Smartposti petulehele, kus väidetavalt tuleb mingi väike summa juurde maksta. Muidugi ei ole pättide eesmärk mõne euro küsimine, vaid inimese krediitkaardiandmete kätte saamine.

Samuti püüavad inimesed leida võimalusi saada tasuta programme, mis muidu on tasulised ja see on pättidele hea lihtne viis, kuidas pahavara inimese arvutisse sokutada. Ka tööpakkumistega seoses on väga palju erinevaid pettuseid.

Näiteks võib veel tuua ühe ravimipettuse veebilehe analüüsi. Selles pettuses on kasutatud väga palju erinevaid manipulatsioonitaktikaid: identiteedivargus, väljamõeldud ajakirjanik, uskumatud väited, hirmutamine, väljamõeldud tagasiside, tehnilised manipulatsioonid jne.

Избегайте участия в лотереях на сомнительных сайтах, а если вам кажется, что сейчас у вас особенно хорошие отношения с фортуной, лучше купите лотерейный билет на eestiloto.ee. Скорее всего, вы не выиграете, но, по крайней мере, финансовые потери ограничатся стоимостью одного лотерейного билета.

Инвестиционное мошенничество

Очень распространена мошенническая схема, где создают эффектный сайт и заманивают на него людей для «инвестиций». Жертве обещают крупный доход, а когда она вносит на счет первую небольшую сумму, то видит, что деньги растут как на дрожжах. Жертву поощряют вкладывать все больше и больше, и большая сумма тоже стремительно увеличивается. Проблемы возникают, когда человек начинает выводить свои инвестиции. Выясняется, что он должен заплатить комиссию, а когда он наконец понимает, что его обманули, и начинает искать в Интернете, как вернуть свои деньги, то часто попадает на очередной мошеннический сайт, предлагающий помощь с поимкой мошенников. Конечно, это тоже ложь, но такое обещание часто помогает выманить у жертв дополнительные суммы денег.

Мошеннические сайты устроены так, что мошенник сам регулирует, насколько растет или уменьшается вложенная сумма, и это не имеет никакого отношения к реальности. К сожалению, вероятно, что в данный момент тысячи жертв, которые еще даже не подозревают, что их обманули, каждый день вкладывают деньги, мечтая о пенсии на Карибах.

Здесь поможет очень простое правило: нет смысла вкладывать деньги на незнакомом сайте, а если кто-то обещает необоснованно высокие доходы, это явный признак мошенничества. Если вы хотите инвестировать, что очень разумно, начните с III пенсионной ступени или рассмотрите различные варианты инвестирования в своем банке.

Прочие виды мошенничества

Описывать разные виды мошенничества можно бесконечно. Например, несколько лет назад от имени налоговой службы рассылали письмо, в котором утверждали, что с человека сняли слишком большой подоходный налог, и просили написать заявление, чтобы вернуть деньги. Фишинговый сайт был очень похож на настоящую страницу налоговых органов, и мошенники пытались заставить людей сообщить свои банковские данные.

Существует множество мошеннических схем, где человек получает SMS, что с его посылкой возникли проблемы. Когда он нажимает на ссылку, его перенаправляют на мошенническую копию сайта Omniva/DPD/Smartmail, где он должен заплатить небольшую дополнительную сумму. Конечно, цель не в том, чтобы выманить несколько евро, а в том, чтобы получить данные вашей кредитной карты.

Люди также пытаются бесплатно скачать программы, которые обычно продаются за деньги. Для злоумышленников это хороший повод установить на компьютер человека вредоносное ПО. Существует множество видов мошенничества в связи с предложениями работы.

Также можно привести пример анализа сайта с мошенничеством в медицинской сфере. В этой схеме использовались самые разные тактики манипулирования: кража личных данных, выдуманный журналист, неправдоподобные заявления, запугивание, фиктивные отзывы, технические манипуляции и т. д.

Kuidas ennast kaitsta

- Veebilehe omaniku kontroll who.is päringu abil: https://who.is/.

  NB! Ära kunagi jaga oma isiklikke andmeid ega pangakaardi infot veebilehega, mille omanikku pole võimalik tuvastada. Samuti tasub vaadata, millal veebileht on loodud.

- Veebilehe ajaloo vaatamine: http://web.archive.org/.

  Siit on võimalik vaadata, milline on veebileht minevikus olnud. Näiteks saavad pätid mõnikord ligipääsu mõnele täiesti seaduslikule veebilehele, mida siis enda vajadustele vastavaks kohendavad. Veebilehe ajalooga tutvudes näed, milliseid teenuseid ja tooteid on see veebileht enne pakkunud.

- Kui sul on kahtlus, et sind üritatakse petta, siis võta julgelt ühendust veebipolitseinikega, kelle kontaktid leiad siit: https://www.politsei.ee/et/veebipolitseinikud.

Kuidas kontrollida, kas tegu on päris panga veebilehega

- Otsi veebist infot panga kohta.

  Tihti kasutatakse pettustes lehti, mis sarnanevad olemasolevate pankade veebilehtedega. Uuri, kas selline pank on reaalselt olemas ja vaata, kas veebiaadress, mille võimalik pettur saatis, on sama, mis panga ametlikul lehel.

- Võta pangaga ühendust veebilehel oleva meiliaadressi kaudu ja uuri X-i kohta.

  Aga kui tegu on petulehega, siis läheb sinu e-kiri samuti petturitele ja seega ei ole see mõistlik meetod kontrollimiseks.

Mida teha, kui oled sattunud küberpettuse ohvriks

- Teavita politseid.

- Otsi internetist võimalusi, kuidas raha tagasi saada.

  On täiesti eraldi liik pettusi, kus petetakse edasi inimesi, kes on juba ühe pettuse ohvriks sattunud: neile lubatakse, et suudetakse petturitelt raha tagasi saada. Tegelikult on eesmärgiks ohvrilt veel täiendavalt raha välja petta.

- Kahjuks satuvad paroolid petturite kätte mõnikord ka küberrünnakute käigus. Veebilehel haveibeenpwned.com saad kontrollida, kas sinu e-postiga seotud andmed on lekkinud ning kas sinu parool on turvaline (selleks vali ülevalt menüüst *Passwords*).

Как себя защитить

- Проверка владельца сайта с помощью запроса WhoIs: https://who.is/.

  Внимание! Никогда не оставляйте личные данные или данные банковской карты на сайте, владельца которого невозможно идентифицировать. Также стоит проверить, когда был создан сайт.

- Просмотр истории создания сайта: http://web.archive.org/.

  Здесь вы можете увидеть, каким был сайт в прошлом. Например, иногда мошенники получают доступ к вполне легальному сайту, который затем адаптируют под свои нужды. Изучив историю сайта, вы сможете узнать, какие услуги и товары он предлагал раньше.

- Если вы подозреваете, что вас пытаются обмануть, не стесняйтесь обратиться к веб-констеблю, данные которого можно найти здесь: https://www.politsei.ee/et/veebipolitseinikud.

Как проверить подлинность сайта банка

- Поищите информацию о банке в Интернете.

  Мошеннические сайты часто похожи на сайты действующих банков. Выясните, существует ли такой банк на самом деле, и проверьте, совпадает ли веб-адрес, присланный потенциальным мошенником, с официальным адресом сайта банка.

- Свяжитесь с банком по адресу электронной почты, указанному на сайте, и спросите о X.

  Тем не менее, если это мошенничество, ваш адрес эл. почты тоже попадет к мошенникам, поэтому такой способ проверки не является разумным.

Что делать, если вы стали жертвой кибермошенников

- Сообщите в полицию.

- Поищите в Интернете способы вернуть свои деньги.

  Существует совершенно отдельный вид мошенничества, когда людей, уже ставших жертвами аферы, обманывают еще больше: им обещают, что они смогут получить украденные деньги обратно. На самом деле цель заключается в том, чтобы выманить у жертвы дополнительные деньги.

- К сожалению, пароли иногда попадают в руки мошенников во время кибератак. На сайте Have I Been Pwned можно проверить, произошла ли утечка данных вашей электронной почты и надежен ли ваш пароль (для этого выберите пункт *Passwords* в верхнем меню).

Harjutused

1. Otsing veebilehel who.is.

Millal on rara.ee domeen registreeritud?

- 15.10.2016
- 07.01.2019
- 03.03.2021
- 12.07.2022

2. Otsing veebilehel haveibeenpwned.com.

Milline neist paroolidest on kõige rohkem kasutuses?

- Metsamari123
- Maasikas123
- Vaarikas123
- Mustikas123

Lisamaterjal

Cialdini, Robert B. Mõjustamise psühholoogia : teooria ja praktika.

Poudel, Diana. Turvaline internet : digimaailma teejuht.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Поиск на сайте WhoIs.

Когда зарегистрирован домен rara.ee?

- 15.10.2016
- 07.01.2019
- 03.03.2021
- 12.07.2022

2. Поиск на сайте Have I Been Pwned.

Какой из этих паролей используется чаще всего?

- Metsamari123
- Maasikas123
- Vaarikas123
- Mustikas123

Дополнительный материал

ERR: Meediataip. Видеолекция: фишинг и социальная инженерия как отмычки современных мошенников.

PPA: Берегись мошенников.

PPA: Материалы по превенции мошенничества.

Чалдини, Роберт Б. Психология влияния: теория и практика.
(Cialdini, Robert B. Mõjustamise psühholoogia : teooria ja praktika.)

Поудел, Диана. Безопасный интернет: путеводитель по цифровому миру.
(Poudel, Diana. Turvaline internet : digimaailma teejuht.)

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

8.2. Libakontod – kes on pildi taga?

Diana Poudel, TÜ

Internet on imede maa. Seal võib olla igaüks just see, kes soovib ning seetõttu ei tohiks usaldada ühtegi inimest, keda sa päriselus näinud ei ole.

Libakontosid kasutatakse erinevatel eesmärkidel ning väga tihti võib olla isegi nii, et libakonto tegija hakkab ohvriga algul lihtsalt suhtlema ja alles siis, kui ta on ohvri kohta piisavalt infot kätte saanud, hakkab pätt mõtlema, kuidas ohvrit ära kasutada.

Näiteks on väga levinud armupettused. Pätt loob atraktiivsete piltidega libakonto (tihti varastatakse pildid mõnelt reaalselt kontolt või luuakse tehisintellekti abiga) ja hakkab saatma sõbrakutseid. Kui kasutaja uurib, miks talle sõbrakutse saadeti, siis võib pätt väita näiteks, et Facebook soovitas või et kasutaja pilt meeldib või jäi mõni kommentaar positiivselt meelde.

Viimasel ajal on levima hakanud isegi taktika, kus ohvrile saadetakse suvalise sisuga SMS-sõnum ja kui ohver vastab, et see saadeti valele numbrile, siis on pätid väga osavad manipulaatorid ja suudavad ikkagi ka sellelt baasilt vestlust alustada.

Oluline on ka mõista, et pättide jaoks on selliste kontaktide loomine 24/7 töö ja neil ei ole kuhugi kiiret. Tihti tegutsetakse isegi tiimidena, et saaks vahetustega suhelda. Iga ohvri kohta hoitakse eraldi märkmeid, et ohver ei märkaks, et ta suhtleb erinevate inimestega.

Sõltuvalt ohvrist võib selline „mesinädalate periood" kesta nädalaid või kuid. Sulle tundub, et oled kohanud ideaalset inimest. Pätid kasutavad korduvalt testitud stsenaariume ja tunnevad väga suurt huvi vestluspartneri huvide ja tegemiste vastu. Tehakse komplimente, räägitakse ka endast jne. Nüüd, kus usaldus on loodud ja tihti ka päris tugevad tunded tekkinud, algab manipulatsioon.

Kui ohver on empaatilise loomuga, siis väidetakse, et ema/laps/lemmikloom või keegi muu lähedane vajab kiiret haiglaravi ning palutakse lühiajalist laenu. Kui ohver unistab rikkaks saamisest, siis räägitakse, et sugulasel on mingi salajane investeerimiskeskkond, aga ta on nõus lubama ka ohvril sinna investeerida. Kui ohvril üldse raha ei ole, siis palutakse talt hoopis abi mingite ülekannete tegemisel, nii et ohver satub enesele teadmata osalema rahapesus. Kahjuks on ohver selleks ajaks petturiga emotsionaalselt nii seotud, et ei pruugi kuulda võtta ka lähedaste hoiatusi.

Kui keegi hakkab sinuga internetis suhtlema, siis ole ettevaatlik. Kindlasti tee enne suhtlemise algust korralik otsing: otsi inimese nime ja pilti. Kui selgub, et sama nimega konto on olemas ja seal on rohkem sisu/sõpru jne, siis on tegu lihtlabase identiteedivargusega.

8.2. Поддельные профили – кто стоит за фото?

Диана Поудел, Тартуский университет

Интернет — удивительное место. Здесь каждый может быть тем, кем хочет, и именно поэтому не стоит доверять тем, с кем вы не знакомы в реальной жизни.

Поддельные профили используются для разных целей. Очень часто человек с поддельным профилем начинает просто общаться с жертвой, и только когда у него появляется достаточно информации о ней, он задумывается о том, как использовать жертву в своих целях.

Например, очень распространено мошенничество в сфере романтических знакомств. Мошенник создает поддельный профиль с привлекательными фотографиями (часто украденными из профиля реального человека или созданными искусственным интеллектом) и начинает рассылать запросы на добавление в друзья. Если пользователь спросит, почему ему прислали запрос, мошенник может заявить, например, что Facebook порекомендовал его, или что ему понравилась фотография человека, или запомнился какой-то его комментарий.

В последнее время стала популярной схема, где жертве отправляют SMS-сообщение произвольного содержания. Если жертва отвечает, что сообщение отправлено не на тот номер, мошенники умело манипулируют и все равно умудряются завести разговор даже на этой основе.

Важно также понимать, что для мошенников налаживание подобных контактов — это круглосуточная работа, и они никуда не торопятся. Часто они даже работают в командах, чтобы иметь возможность общаться посменно. Для каждой жертвы ведутся отдельные заметки, чтобы жертва не заметила, что общается с разными людьми.

В зависимости от жертвы этот «медовый месяц» может длиться несколько недель или месяцев. Вам кажется, что вы встретили идеального человека. Мошенники используют многократно проверенные сценарии и проявляют живой интерес к увлечениям и занятиям своих собеседников. Они делают комплименты, рассказывают о себе и т. д. Когда доверие установлено и зачастую возникли сильные чувства, начинается манипуляция.

Если жертва обладает эмпатией, мошенник скажет, что мать, ребенок, домашнее животное или кто-то еще из близких нуждается в срочном лечении, и попросит ненадолго одолжить денег. Если жертва мечтает разбогатеть, мошенник сообщит, что у его родственника есть секретная инвестиционная платформа, и он готов позволить жертве вложить туда деньги. Если у жертвы совсем нет денег, ее попросят помочь сделать какой-нибудь перевод, чтобы невольно вовлечь в отмывание денег. К сожалению, к этому моменту жертва настолько эмоционально вовлечена в общение с мошенником, что может не прислушаться к предупреждениям близких.

Proovi ka olla enesekriitiline: kui sinuga tahab hirmsasti suhelda sinust paarkümmend aastat noorem modellivälimusega isik, siis miks ta peaks seda tahtma? Inimestele on loomuomane usaldada atraktiivseid inimesi, kuid kahjuks võib iga Nigeeria pätt olla internetis blond kaunitar või kaunite sinisilmadega arst.

Aga lisaks armupettustele on trollikontodel väga palju rakendusi. Näiteks kasutatakse neid valeinfo levitamisel, kus trollikontode abil laigitakse ja kommenteeritakse algset postitust. Seetõttu ei tasu ka sotsiaalmeedias eeldada, et kui mingil postitusel on palju laike ja kommentaare, siis see on tõsi.

Samuti saab trollikontosid kasutada näiteks e-poodides tagasiside jätmiseks. Isegi kui väidetavalt on tegu tõelise (*verified*) ostjaga, ei tähenda see, et tegu ei võiks olla olematu isikuga.

Kusjuures trollikontodena kasutatakse ka päris inimestelt röövitud kontosid. Näiteks kui sisestad mõnel õngitsuslehel oma kasutajatunnuse ja parooli, siis võtavad pätid su konto üle ja näiteks saadavad su sõpradele mingeid petusõnumeid. Samamoodi ole alati ettevaatlik, kui mõni sõber saadab ootamatult lingi või mingi muu info, mida sa oodata ei oska. Sõprade puhul on kontrollimine muidugi lihtne — võta telefon ja helista.

Kuidas ennast kaitsta

Kui soovid trollikontode loojate teele mitte jääda, siis tee järgmist:

- Ära võta sõbraks inimesi, keda sa päriselus ei tunne.
- Muuda oma sotsiaalmeedia sõbralist privaatseks — nii on väiksem tõenäosus, et trollid leiavad sind sotsiaalmeedia kaudu üles.
- Jaga isiklikku infot pigem ainult sõpradega, sest iga isiklik infokild aitab sinuga paremini manipuleerida. Tihti ütlevad ohvrid hiljem, et usaldust tekitas see, et petturiga oli nii palju ühist. Aga tegelikult oli pettur lihtsalt ohvri sotsiaalmeediakontoga põhjalikult tutvunud.
- Tee esimesel võimalusel videokõne. Petturid üldiselt väldivad videokõnesid, kuid kahjuks hakkab see kontrollimeetod oma efektiivsust kaotama, sest tehisintellekti abiga pole kuigi keeruline videokõnes kellegi nägu enda asemel kuvada.

Если кто-то начинает общаться с вами в Интернете, будьте осторожны. Перед началом общения проведите тщательный поиск: проверьте имя и фотографию человека. Если окажется, что есть профиль с таким же именем и большим количеством контента/друзей и т. д., то это просто кража личности.

Кроме того, постарайтесь быть самокритичными: если человек с модельной внешностью на двадцать лет моложе вас умирает от желания поговорить с вами, почему это так? Людям свойственно доверять привлекательным людям, но, к сожалению, в интернете любой нигерийский мошенник может быть белокурой красавицей или голубоглазым доктором.

Но у поддельных профилей много функций и помимо любовных афер. Например, их используют для распространения дезинформации, когда аккаунты интернет-троллей лайкают и комментируют изначальное сообщение. Поэтому не стоит думать, что если пост в социальных сетях набрал много лайков и комментариев, то это правда.

Аккаунты троллей также можно использовать, например, для создания отзывов в интернет-магазинах. Даже если это якобы подлинный (*verified*) покупатель, это не значит, что это не может быть несуществующий человек.

В качестве аккаунтов троллей используют и учетные записи, украденные у реальных людей. Например, если вы введете свое имя пользователя и пароль на фишинговом сайте, мошенники могут завладеть вашей учетной записью и начать отправлять вашим друзьям сообщения. Точно так же всегда будьте настороже, если друг неожиданно присылает вам ссылку или другую информацию. С друзьями, конечно, все проконтролировать просто — взять телефон и позвонить.

Как себя защитить

Если вы не хотите стать жертвой кражи профиля, поступайте следующим образом:

- Не добавляйте в друзья людей, которых вы не знаете в реальной жизни.
- Сделайте список друзей в социальных сетях приватным — так у троллей будет меньше шансов найти вас в социальных сетях.
- Делитесь личной информацией только с друзьями, потому что каждый кусочек личной информации помогает мошенникам лучше манипулировать вами. Впоследствии жертвы часто говорят, что доверие создавал тот факт, что у них было с мошенником много общего. Но на самом деле мошенник просто внимательно изучил профиль жертвы в социальных сетях.
- При первой же возможности договоритесь о видеозвонке. Мошенники обычно избегают видеозвонков, но, к сожалению, этот способ проверки теряет свою эффективность, ведь с помощью искусственного интеллекта не составляет особого труда сгенерировать чье-то изображение.

Harjutused

Harjutuste materjalid:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

Упражнения найдете по ссылке:
https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Lisamaterjal

Aro, Jessikka. Putini trollid : tõsilood Vene infosõja rindelt.

Catfished.
Ingliskeelne kanal erinevatest pettustest.

ERR. Sõbralik netitroll Diana Poudel: mul oli pool riigikogu sõbralistis.
Ühe trollieksperimendi kajastus.

Jantunen, Saara. Infosõda.

Poudel, Diana. Mõjustamise psühholoogiast. Robert Cialdini raamatu „Mõjustamise psühholoogia" tutvustus ja näiteid internetist.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Дополнительный материал

ERR: Meediataip. Боты и тролли.

Аро, Йессикка. Путинские тролли: реальные истории с фронта информационной войны в России.
(Aro, Jessikka. Putini trollid: tõsilood Vene infosõja rindelt.)

Catfished.
Англоязычный канал о различных видах мошенничества.

ERR. Дружелюбный интернет-тролль Диана Поудел: в списке моих друзей была половина Рийгикогу. Описание эксперимента с интернет-троллями.
(Sõbralik netitroll Diana Poudel: mul oli pool riigikogu sõbralistis. Ühe trollieksperimendi kajastus.)

Янтунен, Саара. Информационная война. (Jantunen, Saara. Infosõda.)

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

8.3. Identiteedivargus – digikuritegude eesmärk ja muukraud

Julia Rodina, MTÜ Tuleviku Meedia

Peatüki eesmärgid

- Anda teadmisi identiteedivarguse riskidest.
- Õpetada ära tundma võimalikke identiteedivarguse tunnuseid ja petturite võtteid.
- Õpetada hindama riske ja ennast identiteedivaraste eest kaitsma.

Selle peatüki käsitluses tähendab identiteet kõiki inimese isikuandmeid alates pildist ja nimest kuni hääle ning dokumendi- ja pangaandmeteni. Lihtsustatult on isikuandmed näiteks sünnikuupäev, postiaadress, krediitkaardi- või kontonumber, isikukood jt. Identiteedivarguse all mõistetakse inimese isikuandmete vargust ja nende kuritarvitamist pettuse eesmärgil.

Identiteedivargus võib toimuda sinu e-posti või sotsiaalmeediakonto kaudu, kuid ka interneti-ostudel või muudes olukordades, kus sa jagad tundlikke andmeid, näiteks postitad oma pilte või jagad krediitkaardi- vm isiklikke andmeid. Ründaja võib varastada sinu nime, fotosid vm andmeid. Tehisaru abiga saab pilti või lühivideot kasutades teha isegi süvavõltsitud pikemaid videoid (ingl *deep fake*), kus sind pannakse tegema just seda, mida identiteedivarastel vaja on. Samamoodi saab salvestada häält ja panna sinu hääle rääkima mida iganes.

Sellise tegevusega otseselt seotud probleem on identiteedi võltsimine, mille puhul pettur kehastab ohvrit sotsiaalvõrgustikes vm sarnases keskkonnas. Identiteedi võltsimise eesmärk sotsiaalmeedias võib ulatuda lihtsast naljast tõsisemate rünnakuteni, mille eesmärk on kellegi sotsiaalvõrgustikus häbistamine või muu kahjustamine.

8.3. Кража личности — цель и средство цифровых преступлений

Юлия Родина, НКО Tuleviku Meedia

Цели главы

- Дать знания о рисках, связанных с кражей личности.
- Научить распознавать признаки кражи личности и методы, используемые мошенниками.
- Научить оценивать риски и защищать себя от кражи личности.

В данной главе под личностью понимаются все личные данные человека, от его фотографии и имени до голоса, документов и банковских реквизитов. Личные данные — это, например, дата рождения, почтовый адрес, номер кредитной карты или банковского счета, личный код и т. д. Кража личности — это кража и неправомерное использование личных данных человека в мошеннических целях.

Кража личности может произойти через электронную почту или аккаунт в социальных сетях, а также при совершении покупок в Интернете или в других ситуациях, когда вы делитесь конфиденциальной информацией, например выкладываете свои фотографии, сообщаете данные кредитной карты или другую личную информацию. Злоумышленник может украсть ваше имя, фотографии или другие данные. С помощью ИИ фотографию или короткий видеоролик можно использовать для создания продолжительных и выглядящих очень достоверными поддельных видео (англ. *deepfake*), где вы делаете именно то, что нужно похитителям личности. Точно так же мошенники могут сгенерировать ваш голос и заставить вас «говорить» то, что им нужно.

Проблема, напрямую связанная с этим видом мошенничества, — подделка личности, когда злоумышленник выдает себя за жертву в социальных сетях или другой подобной среде. Подделка личности в социальных сетях может преследовать разные цели — от простой шутки до более серьезных атак, направленных на то, чтобы опозорить кого-то или навредить иным образом.

Nimevargus viib tihti otseselt või kaudselt mainekaotuseni, kuid põhjuse väljaselgitamine ja ohvrit ähvardavate negatiivsete tagajärgede vältimine põhjustab ka suurt ajakulu. Mõningaid nimevarguse vorme nimetatakse ka (kellegi) teesklemiseks.

Kuidas sellised pettused saavad toimuda? Võib-olla oled kunagi saanud näiteks Facebookis sõbrakutse välismaalasest arstilt või sõjaväelaselt, kes soovib tutvuda, algatab aktiivselt sõnumivahetuse ja tundub väga usaldusväärne ja sümpaatne. Ta võib isegi saata pilte endast koos lastega, rääkida tööst ja armastusest. Kuid mingil hetkel palub ta sul talle raha üle kanda, et osta lennupilet Eestisse, sest soovib kohtuda, aga paraku ei ole tal piisavalt vahendeid, sealjuures kindlasti väga mõjuval põhjusel. Tavaliselt loovad petturid sel puhul võltskonto, kasutades sotsiaalmeediast varastatud pilte. Samamoodi võib sinuga sotsiaalmeedias või tutvumisrakenduses tutvuda väga armas noor naine, kes töötab välismaal ja on isegi valmis videokõnedeks ning pärast usalduse loomise perioodi hakkab jagama oma investeerimissoovitusi.

Sellised tutvumis- ja armupettused on kasutusel juba palju aastaid, kuid kahjuks toimivad siiamaani. Ja petturid kasutavad mitte ainult nn tavainimeste andmeid, vaid varastavad isegi Hollywoodi näitlejate identiteete. Nende ohvriks on langenud näiteks näitlejad Brad Pitt ja Keanu Reeves, aga ka palju nn tavalisi naisi üle maailma, kes on petturitele oma raha üle kandnud.

Identiteedivargus võib esineda ka libareklaami vormis. Näiteks teatasid tuntud perearstid Madis Veskimägi ja Karmen Joller 2023. aastal oma sotsiaalmeediakontodel, et nende fotosid ja nime kasutades reklaamitakse veebis tundmatuid ravimeid. Petturid kasutasid nende autoriteeti inimestele „imeravimi"/ toidulisandi reklaamimiseks, lootes, et tarbijad kindlasti usuvad, kui soovitusi annab tuntud isik.

Skeemid võivad olla erinevad. Näiteks võis 2023. aastal Facebookis näha tuntud teleajakirjaniku Anu Välba osalusega reklaami, mis pakkus investeerimisvõimalust. Kui Facebooki kasutaja klikkis reklaamil, siis avanes veebileht, kuhu paluti jätta oma kontaktid, et väga kiiresti ja tulusalt investeerida. Kui inimene ei olnud piisavalt kriitiline ja meediapädev ning jättis oma kontaktid, siis võttis temaga kauplemisplatvormil kohe ühendust lahke „nõustaja", kes aitas teha ülekandeid. Üks selline juhtum jättis ühe Eesti elaniku ilma rohkem kui 9000st eurost. Võib arvata, et ohvreid oli rohkem.

Aga ka mõne sinu tuttava inimese identiteeti on võimalik kuritarvitada: näiteks on eriti kerge võltsida e-posti aadressi. Petturid võivad luua aadressi, mis tundub kuuluvat usaldusväärsele kirjavahetuspartnerile — näiteks vahetades e-posti aadressis ainult mõned tähed. Lisaks lubab tänapäeva tehnoloogia petturitel võltsida telefoninumbrit ja häält nii, et sulle võib tunduda, et helistab inimene, keda sa tunned.

Кража имени часто прямо или косвенно приводит к репутационному ущербу, а на то, чтобы выявить причину и предотвратить негативные последствия, нужно много времени. Некоторые формы кражи имени также называются имперсонацией.

Как происходят такие случаи мошенничества? Например, вы получаете запрос на добавление в друзья в Facebook от иностранного врача или военного, который хочет познакомиться с вами, активно инициирует переписку и кажется очень надежным и симпатичным. Он даже может присылать свои фотографии, фото с детьми, рассказывать о работе и говорить о любви. В какой-то момент он просит вас перевести ему деньги, чтобы купить билет на самолет в Эстонию, потому что хочет встретиться с вами, но по очень веской причине у него недостаточно средств. Мошенники обычно создают фальшивый аккаунт, используя изображения, украденные в социальных сетях. Точно так же вы можете познакомиться в социальных сетях или в приложении для знакомств с очень симпатичной девушкой, которая работает за границей и даже готова созвониться и поговорить по видеосвязи. Когда между вами возникает доверие, она начинает делиться инвестиционными советами.

Такие схемы мошенничества в сфере знакомств существуют уже много лет и, к сожалению, до сих пор работают. При этом мошенники используют не только данные «обычных» людей, они даже крадут личности голливудских актеров. Их жертвами стали, например, Брэд Питт и Киану Ривз, а также в итоге множество обычных женщин по всему миру, которые перевели деньги мошенникам.

Кража личности может также принимать форму фальшивой рекламы. Например, известные семейные врачи Мадис Вескимяги и Кармен Йоллер в 2023 году сообщили в своих соцсетях, что в Интернете с использованием их фотографий и имен рекламируются неизвестные лекарства. Мошенники использовали авторитет конкретных врачей, рекламируя «чудо-лекарства» и пищевые добавки, в надежде, что потребители поверят, если рекомендации дает известный человек.

Схемы могут быть разными. Например, в 2023 году в Facebook можно было увидеть рекламу с участием известной тележурналистки Ану Вяльба, якобы предлагающей возможности для выгодных инвестиций. Когда пользователь Facebook нажимал на рекламу, открывался сайт с предложением оставить контактные данные, чтобы быстро и удачно вложить деньги. Если человек оказывался недостаточно критичным и медиаграмотным и оставлял свои контакты, с ним тут же связывался любезный «консультант» платформы для торгов, который помогал ему сделать перевод. В одном из таких случаев житель Эстонии лишился более 9000 евро. Можно предположить, что жертв было больше.

Использовать могут и личность знакомого вам человека: например, очень легко подделать адрес электронной почты. Мошенники могут создать адрес, который покажется вам подлинным, например, изменив всего несколько букв в email-адресе. Кроме того, современные технологии позволяют мошенникам подделывать телефонные номера и голоса так, что может показаться, будто звонит кто-то из ваших знакомых.

Kuidas ennast kaitsta

- Paroolid kaitsevad kõiki meie kontosid ja andmeid. Ja peaksid ka päriselt kaitsma: 1234567 ei ole turvaline parool. Sinu sünniaasta ega lemmiklooma nimi ka ei ole. Veebiparoolis peaks olema vähemalt kaheksa tähte ja/või numbrit. Turvalises paroolis on nii tähed kui ka numbrid, kasuta nii väikseid kui suuri tähti. Eriti turvalises paroolis ei ole sõnu, mida saab sõnastikust leida.
- Kus tehniliselt võimalik, kasuta kaheastmelist autentimist. Näiteks e-posti rakendustes (Gmail jt), sotsiaalmeediakontodel vm. Sellega saad ennetada oma kontole sisenemist teisest nutiseadmest, sest saad sellise tegevuse kohta sõnumi.
- Ära hoia PIN-koode koos panga- ja/või ID-kaardiga. Ära jaga oma PIN-koode vm selliseid andmeid teistega.
- Enne tellimist veendu, et e-pood on usaldusväärne ja alles siis sisesta enda ja oma krediitkaardi andmed.
- Enne mõtle ja alles siis postita! Näiteks infot enda (ja oma lähedaste) kodu või auto(numbri) kohta, fotosid, videoid vm isiklikku infot. Ja kontrolli, kes näeb sinu postitusi sotsiaalmeedias. Kas kõik kasutajad üle maailma või on ligipääs piiratud ainult nendega, keda sa tead? Kontrolli oma sotsiaalmeediakontode privaatsusseadeid.
- Enne mõtle ja alles siis lisa uusi Facebooki sõpru ja kontakte teistel sotsiaalmeediaplatvormidel.
- Kui keegi on loonud sinu nimega libakonto või oled muul moel langenud identiteedivarguse ohvriks, siis anna sellest kindlasti teada sotsiaalmeediaplatvormile ja politseile.
- Kui näed, et keegi on loonud libareklaami tuntud tegelasega (ja oled veendunud, et see on libareklaam) või libakonto, kasutades varastatud isikuandmeid, teata sellest vähemalt sotsiaalmeediaplatvormile, vajutades nuppu „Report” või muul sarnasel viisil.

Как себя защитить

- Все наши учетные записи и данные защищены паролями. И пароли должны действительно их защищать: 1234567 — это ненадежный пароль. Так же, как и год вашего рождения или кличка вашего питомца. Пароль в Интернете должен содержать не менее восьми букв и/или цифр. Надежные пароли состоят как из букв, так и из цифр, в них используются как прописные, так и строчные буквы. Особенно надежный пароль не содержит слов, которые можно найти в словаре.
- Там, где это технически возможно, используйте двухфакторную аутентификацию. Например, в почтовых приложениях (Gmail и др.), аккаунтах социальных сетей и т. д. Это поможет предотвратить вход в вашу учетную запись с другого смарт-устройства, так как вы получите сообщение о такой активности и сможете ее пресечь.
- Не храните PIN-код вместе с банковской и/или ID-картой. Не сообщайте свои PIN-коды или подобную информацию другим людям.
- Прежде чем сделать заказ, убедитесь, что э-магазину можно доверять, и только потом вводите данные кредитной карты.
- Сперва подумайте, а потом постите! Например: ваш адрес и номер автомобиля, фотографии, видео или другую личную информацию (то же относится и к данным ваших близких). Проверьте, кто может видеть ваши посты в соцсетях. Все пользователи по всему миру или доступ имеют только те, кого вы знаете? Проверьте настройки конфиденциальности своих учетных записей.
- Прежде чем добавить кого-то в друзья в Facebook или на других платформах, хорошо подумайте.
- Если кто-то создал поддельную учетную запись с вашим именем или вы стали жертвой кражи личности, обязательно сообщите об этом администрации социальной сети и в полицию.
- Если вы видите, что кто-то создал фальшивую рекламу с известным человеком (и вы уверены, что это именно фальшивая реклама) или поддельный аккаунт с украденной личной информацией, сообщите об этом администрации соцсети, нажав кнопку «Report» или другим подобным способом.

Harjutused ja praktiline eneseanalüüs

1. Ava oma sotsiaalmeediakonto ja vaata läbi oma sõprade nimekiri. Kas sa tegelikult tead, kes need inimesed on, kes sind jälgivad? Kas keegi neist ei ole kahtlaselt oma profiilipilti või -nime muutnud?

2. Jaga oma kogemusi: kas oled ise näinud sotsiaalmeediapostitusi, mis kuritarvitasid teiste inimeste identiteeti? Kas tead mõnda identiteedivarguse juhtumit või on petturid pöördunud ka sinu poole?

Упражнения и практический самоанализ

1. Откройте свой аккаунт в социальных сетях и проверьте список друзей. Действительно ли вы знаете людей, которые на вас подписаны? Не сменил ли кто-то из них подозрительным образом свое фото или имя?

2. Поделитесь своим опытом: видели ли вы когда-нибудь посты в социальных сетях, где используется личность других людей? Знаете ли вы о случаях кражи личности или связывались ли с вами мошенники?

Lisamaterjal

Anu Välba nime kasutanud veebikelm pettis noorelt naiselt välja üle 9500 euro.

Holmes, Becky. Keanu Reeves is not in love with you : the murky world of online romance. Ashland : Blackstone Publishing, 2024.

Levin, Adam. Swiped : how to protect yourself in a world full of scammers, phishers, and identity thieves. New York : PublicAffairs, 2016.

Lomp, Loora-Eliisabet. Identiteedivargus. Tuntud perearstid avastasid ennast „imeravimit" reklaamimast.

MEAWW. $360,000 scam involving Brad Pitt's name leaves women heartbroken.

Postimees: Haridus. Avaliku info olemus. Poolavalik ja privaatne sfäär.

Vaitmaa, Ester jt. Libainfo eksperiment. Vaata, kui lihtne on tehisaruga luua täielikku jama! „Minu identiteediga tehakse äri teiste inimeste haiguste arvelt".

VICE TV. How scammers steal your identity. Black Market.

Weisman, Steve. 50 ways to protect your identity in a digital age : new financial threats you need to know and how to avoid them. Upper Saddle River : FT Press, 2012.

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Дополнительный материал

Онлайн-мошенник, использовавший имя Ану Вяльба, выманил у молодой женщины более 9500 евро.

IREX. Инструкция тренера по медиаграмотности. Фейковые профили в социальных сетях. 198-210.

Riigiportaal: Защита личных данных и частной жизни.

Ломп, Лоора-Элийзабет. Эстонские семейные врачи стали жертвами преступников

MEAWW. Афера на 360 000 долларов с именем Брэда Питта разбивает женщинам сердце. (MEAWW. $360,000 scam involving Brad Pitt's name leaves women heartbroken.)

VICE TV. Как мошенники крадут вашу личность. Черный рынок. (How scammers steal your identity. Black Market.)

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

8.4. Sotsiaalmeedia algoritmid – kas kontrollivad kasutajat või vastupidi?

Julia Rodina, MTÜ Tuleviku Meedia

Peatüki eesmärgid

- Selgitada, mis on sotsiaalmeedia algoritmid ja milline on nende mõju.
- Õpetada mõistma, kuidas algoritmid võivad meie käitumist muuta ja meiega manipuleerida.
- Õpetada tundma sotsiaalmeedia kasutamise ohte.

Sotsiaalmeedia algoritmid on tehnilised vahendid, mis aitavad sotsiaalmeediaplatvormil postitusi (sisu) sorteerida. See protsess toimub mitte näiteks avaldamisaja, vaid selle alusel, kui asjakohased need postitused just konkreetse kasutaja jaoks on. Algoritmist sõltub, millist sisu sa esimesena näed. Eesmärk on valida ja näidata sulle postitusi, mis suurima tõenäosusega tekitavad sinus huvi, soovi neid meeldivaks märkida (laikida), kommenteerida või jagada.

Näiteks määratakse algoritmide abil, milliseid postitusi sa näed Instagrami voogu sirvides või millised sinu sõprade postitused (*story*'d) ilmuvad esimesena. Tihti on oluline, kelle ja millise sisuga postitusi oled varem meeldivaks märkinud ja jaganud.

Sotsiaalmeedia algoritmid on loodud nii, et kasutajad veedaksid platvormidel võimalikult palju aega tarbides ehk sisu luues ja kommenteerides. Ühelt poolt võib algoritm tõesti aidata sul leida rohkem infot teemal, mis sind huvitab, teiselt poolt aga, kui sellega passiivselt kaasa minna, siis riskid sattuda filtrimulli ja jääda olulisest osast infost ilma.

Algoritmid kasutavad ära inimeste endi antud sotsiaal-demograafilist teavet, mis on vajalik profiili loomisel, kuid õpivad lisaks ka kasutajate sotsiaalmeediakäitumisest, uurides põhjalikult, mis neid huvitab ja millise sisuga nad kõige rohkem juba aega veedavad. See võimaldab sotsiaalmeedial suunata kasutajatele reklaame, mis võiksid neile huvi pakkuda, teenides niiviisi raha.

8.4. Алгоритмы соцсетей — они контролируют пользователя или наоборот?

Юлия Родина, НКО Tuleviku Meedia

Цели главы

- Объяснить, что такое алгоритмы социальных сетей и каково их влияние.
- Научить понимать, как алгоритмы могут менять наше поведение и манипулировать нами.
- Рассказать о рисках, связанных с пользованием социальными сетями.

Алгоритмы социальных сетей — это набор технологических правил и шагов, которые помогают платформам социальных сетей сортировать посты (контент). Сортировка может происходить, например, не на основе времени публикации, а на основе релевантности постов для конкретного пользователя. Алгоритм определяет, какой контент вы увидите первым. Цель — выбрать и показать вам те посты, которые с большой вероятностью заинтересуют вас, заставят поставить лайк, прокомментировать или поделиться ими.

Например, алгоритмы определяют, какие посты вы увидите, просматривая свою ленту Instagram, или какие *story* ваших друзей появятся в ленте первыми. Часто имеет значение то, какие посты вы лайкнули и чем делились раньше.

Алгоритмы социальных сетей разработаны так, чтобы пользователи тратили на потребление, создание и комментирование контента как можно больше времени. С одной стороны, алгоритм может действительно помочь найти больше информации по интересующей вас теме, но с другой стороны, если пассивно следовать ему, можно попасть в информационный пузырь и упустить значительную часть информации.

Sotsiaalvõrgustikud soovivad hoida meid oma platvormidel võimalikult kaua ja seetõttu püüavad meid aina rohkem panna otsima, vaatama, laike märkima ja sisu kommenteerima. See omakorda tähendab, et me näeme oma infovoogudes suure tõenäosusega ainult seda, mida me tahame näha, mitte seda, mis meile ei meeldi või millest me ei hooli. Sotsiaalmeediaettevõtted (näiteks Meta, kellele kuuluvad Facebook ja Instagram, Google, kellele kuulub YouTube ning TikToki omanik ByteDance) on õppinud näitama kasutajatele seda, mida nad tahavad näha, lähtudes sellest, millist sisu nad varem on vaadanud.

Sinu kohta kogutud andmete (vanus, sugu, elu- või asukoht, huvid, sulle meeldiv sisu jne) põhjal loob sotsiaalmeediaplatvorm sinu profiili, mis sisaldab nii sinu andmeid kui ka veebikäitumise iseloomu. Iga kord, kui külastad sotsiaalmeediaplatvormi, täiendatakse ja ajakohastatakse ka sinu profiili. Sotsiaalmeedia algoritmid kasutavad loodud profiili, et kuvada sulle sisu ja reklaame, mis on kooskõlas just sinu andmete ja huvidega.

Kas oled kunagi tähele pannud, et kui hakkad postitusi meeldivaks märkima või otsima infot mõnel teemal, mis sind varem eriti ei huvitanud, hakkab sotsiaalmeedia sulle saatma laviinina infot ja reklaame, mis on sellega otseselt seotud? Näiteks kui kirjutad sotsiaalmeedias otsingusse „siiami kassid", hakkab sinu sealne infovoog täituma postituste, fotode ja videotega kassidest (tõenäoliselt just sellest tõust) ning kasside ja lemmikloomadega seotud reklaamidega.

Aga kui kõik, mis sind ei huvita või on vastuolus sinu tõekspidamistega, filtreeritakse sotsiaalmeediaplatvormil välja, siis satud filtrimulli (või infomulli, ingl *filter bubble*). Selle termini autor on interneti-aktivist Eli Pariser. Filtrimullis olemine tähendab, et oled intellektuaalses isolatsioonis. Aga demokraatliku ja avatud ühiskonna toimimiseks peavad inimesed asju üksteise vaatenurgast nägema.

Infomulli teine oht on, et võid hakata arvama, et peaaegu kõik mõtlevad nii nagu sina. Seda aga juhtub harva ja suure tõenäosusega oled lihtsalt muude vaatenurkade eest kaitstud, kuna need asuvad väljaspool mulli. See aga süvendab ühiskonna polariseerumist.

Sotsiaalmeedia algoritmid on mõjus tööriist turunduses ja müügis – see on osa tähelepanumajandusest, milles tänapäeval on inimese tähelepanu, aeg, klikk ja laik väärtuslik ressurss. Sotsiaalmeediaplatvormid teenivad oma tulu, näidates kasutajatele reklaame ja nende kliendid ehk reklaami ostjad tahavad näidata oma reklaame just teatud ehk valitud kasutajaskonnale. Ja platvormid saavad neile seda pakkuda, näiteks just kindlas piirkonnas elavatele kindla profiiliga (vanus, sugu, keel, huvid jne) kasutajatele. Seega, algoritmid võivad reklaamiostjal aidata tarbijate käitumist mõjutada.

Samamoodi võime algoritmide mõju all sattuda sotsiaalsesse või poliitilisse filtrimulli, mis omakorda mõjutab ka meie käitumist, kuna me ei näe terviklikku infopilti.

Алгоритмы используют социально-демографическую информацию, предоставленную самими пользователями, для создания их профилей, а также изучают их поведение в социальных сетях, внимательно следя, чем пользователи интересуются и на какой контент тратят больше всего времени. Это позволяет соцсетям показывать вам таргетированную рекламу, которая может заинтересовать именно вас, и таким образом зарабатывать деньги.

Социальные сети хотят удержать нас на своих платформах как можно дольше и поэтому ведут себя так, чтобы мы постоянно искали, просматривали, лайкали и комментировали контент. Это, в свою очередь, означает, что мы с большей вероятностью увидим в своей ленте то, что хотим видеть, а не то, что нам не нравится или неинтересно. Компании, создавшие социальные сети (такие как Meta, владеющая Facebook и Instagram, Google, владеющая YouTube, и ByteDance, владеющая TikTok), научились показывать пользователю именно то, что он хочет увидеть, основываясь на контенте, который он просматривал в прошлом.

На основе собранной о вас информации (возраст, пол, местоположение, интересы, понравившийся контент и т. д.) платформа социальных сетей создает ваш профиль, который будет включать ваши данные и характер поведения в Интернете. Каждый раз, когда вы заходите на платформу социальных сетей, ваш профиль обновляется и пополняется. Алгоритмы социальных сетей используют созданный вами профиль, чтобы показывать вам контент и рекламу, соответствующие вашим данным и интересам.

Замечали ли вы, что когда вы начинаете ставить лайки или искать информацию по теме, которая вас раньше не особенно интересовала, социальные сети обрушивают на вас лавину информации и рекламы, непосредственно связанной с ней? Например, если вы наберете в поиске соцсети «сиамские кошки», ваша лента заполнится постами, фотографиями и видео с кошками (скорее всего, именно этой породы), а также рекламой, связанной с кошками и домашними животными.

Но если все, что вас не интересует или противоречит вашим убеждениям, отфильтровывается, вы рискуете оказаться в информационном пузыре (или «пузыре фильтров», англ. *filter bubble*). Этот термин предложил интернет-активист Илай Парайзер. Пузырь фильтров означает интеллектуальную изоляцию. Но для того, чтобы общество функционировало как демократическое и открытое, люди должны уметь взглянуть на вещи и с позиции других.

Еще одна опасность информационного пузыря заключается в том, что вы можете посчитать, что почти все думают так же, как и вы. Однако в жизни такое случается редко, и, скорее всего, вы просто ограждены от других мнений, так как они остались за пределами пузыря. Это усугубляет поляризацию общества.

Алгоритмы социальных сетей служат мощным инструментом маркетинга и продаж — частью экономики внимания, где человеческое внимание, время, клики и лайки являются самым ценным ресурсом. Платформы социальных сетей зарабатывают на показе рекламы своим пользователям, а их клиенты, или покупатели рекламы, хотят показывать свои объявления определенной, то есть выбранной аудитории. И платформы могут им это предложить — например, показать рекламу пользователям с определенным профилем (возраст, пол, язык, интересы и т. д.), проживающим в определенном месте. Таким образом, алгоритмы могут помочь покупателям рекламы влиять на поведение потребителей.

Точно так же под влиянием алгоритмов мы можем попасть в пузырь социальной или политической изоляции, что, в свою очередь, влияет на наше поведение, поскольку мы не видим всей картины.

Kuidas ennast kaitsta

- Alusta kriitilisest mõtlemisest. Aga ära unusta ka tehnilist poolt: ava sotsiaalmeediaplatvormidel oma kontode seaded ja leia aega lugeda läbi privaatsusreeglid.
- Vaata oma seaded üle. Näiteks: kes saab Facebookis näha sinu sünnipäeva ja elukohta? Aga sinu fotosid ja postitusi (*story*'sid)? Kas kõikidel platvormi kasutajatel peab olema ligipääs sinu andmetele?
- Vaata üle andmed, mida oled lubanud sotsiaalmeediarakendustel enda kohta koguda. Kas sa tegelikult soovid, et nad saaksid kasutada näiteks näotuvastusvahendeid, mis võimaldavad neil sinu nägu fotodel tuvastada? Kui midagi ei sobi, siis loobu sellest kohe. Kõike seda saab sotsiaalmeediaplatvormide privaatsusseadetest vaadata ja muuta.

Как себя защитить

- Начните с критического мышления. Но не забывайте и о технической стороне: откройте свои аккаунты в соцсетях и найдите время, чтобы прочитать правила конфиденциальности.
- Проверьте настройки. Например, кто может видеть в Facebook день вашего рождения и место проживания? А фотографии, посты и *story*? Все ли пользователи платформы должны иметь доступ к вашим данным?
- Просмотрите данные, которые вы разрешили приложениям социальных сетей собирать о вас. Вы действительно хотите, чтобы они могли использовать, например, технологию распознавания лиц, позволяющую идентифицировать ваше лицо на фотографиях? Если вам что-то не подходит, откажитесь от этого. Все это можно посмотреть и изменить в настройках приватности.

Harjutused

1. Palu sõbral, kolleegil või pereliikmel näidata oma sotsiaalmeediavoogu. Võrdle reklaame ja sisu, mida sina oled näinud. Mille järgi on algoritmid otsustanud, et miski võib just sulle või sõbrale meeldida?

2. Tee eksperiment. Vali teema või sisu, mis sind varem ei ole sotsiaalmeedias huvitanud ja proovi märkida meeldivaks 5–7 sellise sisuga postitust. Jälgi, mis hakkab sinu infovoos toimuma.

Lisamaterjal

ERR: Meediataip. Hellerma, Juhan. Meediaekspert: meediaplatvormide andmeäri tekitab üha enam tõrksust.

ERR: Novaator. Ühismeedia takistab igavusest uute kirgede leidmist.

IREX Media Literacy in the Baltics. Kuidas väljuda filtrimullist?

Lanier, Jaron. Kümme põhjust, miks otsekohe kustutada kõik oma sotsiaalmeedia kontod.

Lembke, Anna. Dopamine nation: finding balance in the age of indulgence._

Pariser, Eli. The filter bubble: what the Internet is hiding from you.

Postimees: Haridus. Algoritmid ja personaliseeritud sisu.

Veebikonstaabel Maarja Punaku avalik loeng „Sotsiaalmeediasse postitatud sõna kaal või kaalutus".

Very Verified: Sotsiaalmeedia. Kuidas sotsiaalmeedia toimib?

Lisamaterjalid: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

Упражнения

1. Попросите друга, коллегу или члена семьи показать вам свою ленту в социальных сетях. Сравните рекламу и контент, которые вы видели. Как алгоритмы определили, что вам или вашему другу может понравиться именно это?

2. Проведите эксперимент. Выберите тему или контент, которым вы раньше не интересовались в социальных сетях, и поставьте лайк 5—7 постам с такой тематикой и контентом. Проследите за тем, что происходит в вашей ленте, как она меняется.

Дополнительный материал

Учебная программа ЮНЕСКО по медийной и информационной грамотности для педагогов и учащихся. 219-228.

ERR: Новатор. Хеллерма, Юхан. Медиаэксперт: бизнес по обработке данных на медиаплатформах все чаще вызывает отторжение. (ERR: Novaator. Hellerma, Juhan. Meediaekspert: meediaplatvormide andmeäri tekitab üha enam tõrksust.)

ERR: Новатор. Социальные сети не позволяют людям впасть в скуку и находить новые идеи. (ERR: Novaator. Ühismeedia takistab igavusest uute kirgede leidmist.)

IREX: Медиаграмотность в странах Балтии. Как не попасть в информационный пузырь? (IREX Media Literacy in the Baltics. Kuidas väljuda filtrimullist?)

Ланье, Джарон. 10 аргументов удалить все свои аккаунты в социальных сетях. (Lanier, Jaron. Ten arguments for deleting your social media accounts right now.)

Лембке, Анна. Дофаминовая нация. Поиск равновесия в эпоху излишеств. (Lembke, Anna. Dopamine nation: finding balance in the age of indulgence.)

Парайзер, Илай. За стеной фильтров. Что интернет скрывает от вас. (Pariser, Eli. Filter bubble: what the Internet is hiding from you.)

Postimees: Образование. Алгоритмы и персонализированный контент. (Postimees: Haridus. Algoritmid ja personaliseeritud sisu.)

Публичная лекция веб-констебля Маарьи Пунак «Вес или невесомость слов в социальных сетях» (Sotsiaalmeediasse postitatud sõna kaal või kaalutus).

Дополнительные материалы: https://www.rara.ee/uuri/desinformatsioon/meediaradar/

MeediaRadar:
kuidas orienteeruda infokülluses

Koostajad:
Kateryna Botnar, Kristiina Kaju, Maret Einmann,
Diana Poudel, Julia Rodina, Kari Kivinen,
Eesti Väitlusselts

Soome keelest tõlkinud ja tõlke toimetanud
Luisa Tõlkebüroo

Vene keelde tõlkinud ja tõlke toimetanud
Luisa Tõlkebüroo

Keeletoimetaja: Gerli Randjärv

Kujundajad: Viktor Gurov, Margit Plink

Kirjastaja: Eesti Rahvusraamatukogu

Trükikoda: Printon

Väljaanne on valminud
MeediaRadari projekti raames,
rahastus Šveitsi-Eesti koostööprogrammi
toetusmeetmest „Sotsiaalse kaasatuse toetamine”

Võrguväljaanne:
ISBN 978-9949-413-81-2 (pdf)

Trükis:
ISBN 978-9949-413-80-5

MeediaRadar:
как ориентироваться в большом объеме информации

Составители:
Катерина Ботнарь, Кристийна Каю, Марет Эйнманн,
Диана Поудел, Юлия Родина, Кари Кивинен
и Общество дебатов Эстонии

Перевод на русский язык и редактура:
бюро переводов Luisa

Редактура текста на эстонском языке:
Герли Рандярв

Дизайнер: Виктор Гуров, Маргит Плинк

Издатель: Национальная библиотека Эстонии

Печать: Printon

Издание подготовлено в ходе проекта «MeediaRadar»
при помощи швейцарско-эстонской программы
сотрудничества «Поддержка социальной
вовлеченности»

Сетевое издание:
ISBN 978-9949-413-81-2 (pdf)

Издание:
ISBN 978-9949-413-80-5