Епизода 5

"Медиумска писменост 101“: Онлајн медиуми (bots, deep fake, shallow fake[1])

Најавна шпица

ВОДИТЕЛ : Добре дојдовте назад во „Медиумска Писменост 101,“ радио-програма чија цел е да ги едуцира и оспособи слушателите како да се движат низ медиумскиот простор на критички и информиран начин.

ВОДИТЕЛ : Во денешната епизода, ќе се фокусираме на дигиталната писменост и онлајн безбедноста.

Звук 1: Разбирање на Интернетот и начинот на кој функционира

ВОДИТЕЛ: Интернетот претставува глобална мрежа на компјутери која овозможува споделување на информации и меѓусебна комуникација. Интернетот е моќна алатка која го промени начинот на кој живееме и работиме. Како и да е, важно е да сфатиме како функционира, но и кои се потенцијалните ризици со кои можеме да се соочиме додека го користиме.

Звук 2: Техники кои се користат за ширење на дезинформациите

ВОДИТЕЛ: Дезинформациите најчесто се шират преку социјалните медиуми, најчесто преку „ботови“ и автоматизирани профили. Исто така можат да бидат проширени преку емаил, текстуални пораки, форуми, чет-соби, фотографии, видеа и други форми на онлајн комуникација. Компјутерските програми познати како AI или „Artificial Intelligence“ (Вештачка интелигенција) со способноста која ја имаат да ги заменат оригиналните видеа или слики, задржувајќи го истиот облик, познати и како „**deep fakes“,** претставуваат навистина голем проблем во ширењето на дезинформациите. Доволно е само да ги проверите лажните профили на Инстаграм од Том Круз и Кијану Ривс за да се уверите колку истите изгледаат уверливо и реално. Овие програми можат да реплицираат веќе постоечки личности кои наводно кажуваат или прават нешто што реално ниту го сториле, ниту го кажале. Доколку сретнете видео со политичар или некое лице кое кажува нешто или презема некоја активност, навистина е тешко да процените дали видеото е реално или е монтажа. Тука е моментот каде треба да настапи нашата интиуција и претходно знаење за карактерот на личноста која се наоѓа на видеото. Прво мораме да се запрашаме самите - „Дали сето ова што го прочитав се совпаѓа со се што знам за личноста?“

Shallow Fakes се исто така вознемирувачки, но се креирани од лица кои поседуваат базични

[1] Напомена: Многу од изразите се во изворна форма на англиски јазик поради тоа што нема соодветен превод на македонски јазик. Нивното значење е објаснето во текстот.

способности за едитирање видеа. Веќе постоечка медиумска содржина може да биде целосно изменета, со цел да се прикаже различна приказна или да се пренесе поинаква порака. Целта на **deepfakes** and **shallowfakes** е иста - искривување на реалноста, како и криење и искривување на фактите.

Internet Bots или „Интернет Ботовите“ се софтверски апликации, кои се дизајнирани и програмирани за да извршуваат задачи, автоматски и многу побрзо отколку што тоа би можело да го стори човечко суштество и работат 24/7. Постојат различни видови на ботови, како на пример Алекса и Сири, кои се чет-ботови кои можат да симулираат разговор. Социјалните медиуми имаат таканаречени „**Социјални Ботови“ -Social Bots,** кои можат да учествуваат и да имаат влијание во онлајн дискусии. Доколку купувате онлајн, „**Shopbots**“ (ботовите за шопинг) ќе ви помогнат да ја пронајдете најповолната цена на производот кој го барате.

„Spiders“, исто така познати и како **„Crawlers**“, пребаруваат содржини на ист начин како пребарувачите Google или Firefox. Овие се познати како добри и корисни ботови кои можат да се користат како замена за луѓето во повеќе области - поддршка на клиенти, бизнис, како и на поле забава.

Всушност, чет- ботовите **„chatbots**“ , во денешно време се користат за да им помагаат при извршување на секојдневните активности на постари лица кои најчесто се осамени и на тој начин ја намалуваат нивната социјална изолираност.

Bad bots или „лошите ботови“ се малициозни ботови кои се користат во сајбер криминалот и вклучуваат таканаречени „***Spambots“*** и ги поттикнуваат корисниците на веб-сајтовите преку „pop up“ реклами и „***Hackers***“ кои можат да напаѓаат веб-сајтови и притоа да собираат лични и сензитивни информации.

Звук 3. Како да препознаете малициозни ботови

Постојат повеќе начини на кои можете да препознаете дека вашиот систем е „инфициран“.

- Вашата интернет-конекција е послаба од вообичаено.
- Компјутерот се исклучува без никаква причина.
- Ви одзема подолго време да го исклучите компјутерот или да го рестартирате.
- Постојат додатоци во вашиот пребарувач кои не сте ги инсталирале претходно.

- „Pop up windows“ прозорците се појавуваат постојано, дури и кога не користите Интернет.
- Постојано добивате предупредувачки „popp-up“ прозорци кои ве насочуваат да кликнете на одреден линк, во спротивно компјутерот ќе ви биде инфициран.
- Вашите пријатели добиваат мејлови или пораки од вас кои не сте им ги испратиле.

Звук 4: Совети за креирање на силна лозинка и заштита на вашата приватност онлајн

ВОДИТЕЛ: Заштитата на онлајн приватноста е навистина важна, особено поради тоа што сите наши приватни информации ги споделуваме онлајн. Во наредната епизода подетално ќе ги разгледаме начините за заштита на приватноста онлајн, а во денешната епизода ќе ви предложиме неколку начини за креирање на силна лозинка, а со тоа истовремено и заштита на вашата онлајн приватност:

- Користете мешавина на букви, броеви и специјални карактери во вашите лозинки, Избегнувајте да користите лозинки кои лесно можат да се поврзат со вашето име, датумот на раѓање или било каква друга информација поврзана со вас која лесно може да биде погодена,
- Бидете внимателни при користењето на јавни Wi-Fi мрежи,
- Користете ги поставките за приватност на вашите профили на социјалните медиуми.
-

Звук 5: Како да забележите и спречите Онлајн „scams“ измами

ВОДИТЕЛ: Онлајн „scams“ и измамите можат да бидат во повеќе форми, од фишинг мејлови до лажни веб - страни. Во прилог неколку совети за тоа како да избегнете онлајн измами:

* Секогаш со резерва пристапувајте кон несаканите мејлови и текстуални пораки,

* Бидете внимателни со понуди кои ги среќавате онлајн и кои изгледаат предобро за да бидат вистинити,

* Не давајте лични информации се додека не сте сигурни дека информациите ги давате на вистинско место,

* Секогаш проверувајте ги граматичките и правописните грешки на вебсајтовите и мејловите,

* Користете систем на двојна автентификација кога е возможно.

Звук 6: Гостин говорник

ВОДИТЕЛ: За подетално да го објасниме сето она што го зборувавме денес, би сакале да го поканиме …….

ВОДИТЕЛ: Во следната епизода ќе посветиме внимание на останатите начини за заштита од дезинформации и мануплативни содржини на социјалните медиуми.

ВОДИТЕЛ: Приклучете се и наредната недела во нашата шеста епизода на „Медиумска писменост 101." Во меѓувреме, не заборавајте да го посетите нашиот вебсајт за повеќе информации и корисни извори за медиумска писменост.

Одјавна шпица

ВОДИТЕЛ: Ви благодариме што се приклучивте во нашата емисија „Медиумска писменост 101." До следниот пат, останете информирани, љубопитни и медиумски писмени.

Завршна музика