ВЛИЈАНИЕТО НА ДИГИТАЛНИТЕ ТЕХНОЛОГИИ ВРЗ БЕЗБЕДНОСТА НА НОВИНАРИТЕ ВО СЕВЕРНА МАКЕДОНИЈА

ИСТРАЖУВАЊЕ

СПРОВЕДЕНО ОД:
Здружение на Новинари за човекови права

ИСПИТАНИЦИ:
118 новинари и медиумски работници

ПЕРИОД НА ИСТРАЖУВАЊЕ:
2024 година

Влијанието на дигиталните технологии врз безбедноста на новинарите во Северна Македонија

Издавач: Новинари за човекови права
Ул. Венијамин Мачуковски 2А-3/16 Скопје
Електронска пошта: detstvo@detstvo.org.mk
Подготвил: Наташа Доковска / Александра Радевска
Графичка обработка: Каракиров ДОО
Лектура: Стојан Спировски
Скопје, Јуни 2024

Вовед

Во современото општество дигиталните технологии имаат големо влијание врз секојдневниот живот и врз различни професии, а особено врз новинарството. Со развојот на интернетот, социјалните мрежи и дигиталните платформи, новинарите добија можност побрзо да собираат, обработуваат и пренесуваат информации до јавноста. Денес информациите можат да се споделат за само неколку секунди, што овозможува граѓаните навремено да бидат информирани за настаните во државата и светот.

Дигиталната ера донесе бројни предности за новинарите, како што се полесен пристап до информации, комуникација со извори, онлајн интервјуа, директен контакт со публиката и поголема достапност на медиумските содржини. Социјалните мрежи овозможуваат новинарите побрзо да ги следат случувањата и да добијат информации од различни извори. Покрај тоа, современите технологии овозможуваат создавање мултимедијални содржини преку фотографии, видеа и аудио материјали кои го подобруваат квалитетот на известувањето.

Сепак, покрај позитивните страни, дигиталните технологии носат и многу предизвици и опасности. Со зголемената употреба на интернетот се појавуваат нови форми на закани кои можат сериозно да влијаат врз безбедноста и работата на новинарите. Онлајн нападите, говорот на омраза, заканите преку социјалните мрежи, дигиталниот надзор, хакерските напади и злоупотребата на личните податоци стануваат сè почести проблеми.

Во Северна Македонија овие проблеми стануваат сè позабележителни. Истражувањето спроведено од Здружението на Новинари за човекови права покажува дека голем број новинари се соочуваат со различни форми на дигитални закани кои негативно влијаат врз нивната професионална работа, лична сигурност и психолошка состојба. Особено загрижувачки е фактот што жените новинари се изложени на поголем ризик од онлајн малтретирање и дискриминација.

Целта на ова истражување е да се анализира влијанието на дигиталните технологии врз безбедноста на новинарите во Северна Македонија, да се прикажат резултатите од спроведеното истражување и да се предложат можни мерки за подобрување на дигиталната безбедност и заштита на новинарите.

Резултати од истражувањето

Истражувањето е спроведено од Здружението на Новинари за човекови права во Северна Македонија со цел да се анализира влијанието на дигиталните технологии врз безбедноста на новинарите и да се утврдат главните ризици со кои тие се соочуваат во текот на нивната професионална работа.

Во истражувањето учествувале **118 испитаници**, односно новинари и медиумски работници од различни медиуми во Северна Македонија. Во примерокот биле вклучени испитаници од различни медиумски области, со цел да се добие поширока слика за состојбата со дигиталната безбедност.

Испитаниците биле дел од:

- телевизиски медиуми;
- интернет портали;
- печатени медиуми;
- радио станици;
- независни медиумски организации.

За спроведување на истражувањето бил применет **квантитативен метод**, преку анкетен прашалник кој содржел повеќе прашања поврзани со искуствата и безбедносните предизвици на новинарите во дигиталната средина.

Прашањата биле насочени кон:

- онлајн малтретирање;
- закани и говор на омраза;
- дигитален надзор;
- фишинг напади;
- хакерски обиди;
- безбедност на лични податоци;
- заштита на дигиталната комуникација.

Добиените резултати биле обработени со статистичка и процентуална анализа. Истражувањето покажало дека **60% од испитаниците се соочиле со онлајн малтретирање**, **35% изразиле загриженост за дигитален надзор**, а **25% пријавиле фишинг или хакерски обиди за пристап до нивните профили или уреди**.

Резултатите покажуваат дека дигиталната безбедност на новинарите претставува значајно прашање кое бара поголемо внимание, дополнителна заштита и развој на мерки за спречување на ваквите закани.

Анализа на онлајн малтретирањето

1. Онлајн малтретирање на новинарите

Истражувањето покажува дека 60% од испитаниците изјавиле дека биле изложени на онлајн малтретирање преку социјалните мрежи и дигиталните платформи. Овој резултат укажува дека повеќе од половина од новинарите се соочуваат со различни форми на психолошки притисок и напади во дигиталниот простор.

Онлајн малтретирањето претставува форма на насилство што се одвива преку интернет и вклучува навредливи пораки, закани, ширење невистинити информации и јавно омаловажување. Денес социјалните мрежи се место каде што новинарите често ги споделуваат своите информации и ставови, но истовремено стануваат и цел на напади.

Најчестите форми на онлајн малтретирање се:

- навредливи коментари;
- говор на омраза;
- закани по личната безбедност;
- дискредитација на професионалниот углед;
- ширење лажни информации;
- јавни навреди и исмејување.

Последиците од ваквите напади можат да бидат сериозни. Кај многу новинари се појавуваат стрес, анксиозност, страв и намалена самодоверба. Во одредени случаи, новинарите почнуваат да избегнуваат известување за чувствителни теми поради страв од дополнителни напади.

Особено загрижувачки е фактот што жените новинари се изложени на поголем ризик. Освен професионалните напади, тие често добиваат навреди поврзани со нивниот физички изглед, пол или приватен живот. Таквите напади можат дополнително да влијаат врз нивната психолошка состојба и работна мотивација.

2. Дигитален надзор и чувство на несигурност

Според резултатите од истражувањето, 35% од новинарите изразиле загриженост дека нивната комуникација може да биде предмет на следење или надзор.

Дигиталниот надзор претставува процес на следење на електронската комуникација, интернет активностите или личните податоци на корисниците. Новинарите секојдневно комуницираат со извори на информации и често работат со доверливи податоци, па затоа безбедноста на комуникацијата е од големо значење.

Стравот од дигитален надзор може да се појави поради:

- сомнеж за прислушување на комуникацијата;
- следење на електронска пошта;
- следење на профили на социјални мрежи;
- неовластен пристап до лични податоци;
- можност за следење на мобилни уреди.

Кога новинарите чувствуваат дека нивната комуникација не е безбедна, тие можат да почнат да избегнуваат одредени теми или да се воздржуваат од комуникација соизвори.
Последиците од ваквата ситуација се:

- намалена слобода на изразување;
- губење доверба во дигиталните алатки;
- чувство на страв и несигурност;
- намалена професионална независност.

Ова може да има негативно влијание и врз квалитетот на новинарската работа, бидејќи новинарите може да избегнуваат истражување чувствителни теми.

3. Фишинг напади и хакерски обиди

Истражувањето покажува дека 25% од испитаниците пријавиле дека биле цел на фишинг напади или хакерски обиди за пристап до нивните уреди и профили.
Фишинг нападите претставуваат еден од најчестите облици на интернет измами. Напаѓачите се претставуваат како доверливи лица или организации со цел да добијат чувствителни информации.
Најчесто овие напади се вршат преку:

- електронска пошта;
- пораки на социјални мрежи;
- лажни интернет страници;
- СМС пораки;
- непознати линкови.

Целта на овие напади е да се добијат:

- лозинки;
- лични информации;
- банкарски податоци;
- пристап до профили;
- доверливи документи.

Доколку новинар стане жртва на ваков напад, последиците можат да бидат сериозни:

- губење важни информации;
- кражба на податоци;
- злоупотреба на лични профили;
- нарушување на приватноста;
- компромитирање на новинарски извори.

Поради ова, новинарите треба да користат безбедносни мерки како што се:

- силни лозинки;
- двофакторска автентикација;
- редовно ажурирање на уредите;
- внимателност при отворање линкови;
- користење безбедни комуникациски платформи.

Дигитален надзор

Според резултатите од истражувањето, **35% од новинарите** изразиле загриженост дека нивната дигитална комуникација може да биде предмет на надзор или следење. Овој податок покажува дека значителен број новинари чувствуваат несигурност при користењето на дигиталните алатки и комуникациски платформи во нивната секојдневна работа.

Дигиталниот надзор претставува процес на следење, собирање и анализа на дигитални податоци и активности на корисниците. Тој може да опфаќа следење на телефонски разговори, електронска пошта, пораки на социјални мрежи, интернет пребарувања, како и пристап до лични податоци или документи зачувани на електронски уреди.

За новинарите, овој проблем е особено важен бидејќи нивната работа често подразбира комуникација со доверливи извори и работа со чувствителни информации. Во многу случаи, изворите сакаат да останат анонимни заради лична безбедност или страв од последици. Доколку постои сомневање дека комуникацијата може да биде следена, тоа може да доведе до намалување на довербата меѓу новинарите и нивните извори.

Дигиталниот надзор може да се појави во различни форми:

- следење на електронска пошта;
- следење на комуникација преку социјални мрежи;
- прислушување на телефонски разговори;
- пристап до лични податоци;
- следење на интернет активностите;
- неовластен пристап до уреди и профили.

Стравот од ваков вид надзор може да предизвика сериозни психолошки и професионални последици кај новинарите. Тие можат да почнат да чувствуваат стрес, несигурност и страв при извршување на својата работа. Во одредени ситуации, новинарите може да избегнуваат обработка на чувствителни теми или да се воздржуваат од контактирање на извори поради страв дека нивната комуникација не е доволно безбедна.

Последиците од дигиталниот надзор можат да бидат:

- намалување на слободата на изразување;
- нарушување на приватноста;
- намалување на довербата во дигиталните технологии;
- ограничување на професионалната работа;
- чувство на страв и несигурност;
- психолошки притисок и стрес.

Поради овие причини, потребно е новинарите да користат безбедносни мерки како што се криптирана комуникација, двофакторска автентикација, силни лозинки и

редовна едукација за дигитална безбедност. Со подобра заштита може да се намали ризикот од злоупотреба на личните информации и да се овозможи побезбедна работна средина за новинарите

Сајбер напади

Според резултатите од истражувањето, 25% од испитаниците изјавиле дека се соочиле со обиди за фишинг напади или хакерски обиди за пристап до нивните уреди и профили. Овој резултат покажува дека сајбер нападите претставуваат сериозна закана за новинарите и нивната безбедност во дигиталниот простор. **Сај**бер нападите претставуваат намерни активности кои имаат цел да предизвикаат штета, да украдат информации или да добијат неовластен пристап до компјутерски системи, профили или лични податоци. Со развојот на технологијата и сè поголемата употреба на интернетот, овие напади стануваат почести и пософистицирани.

Новинарите се особено ранлива група бидејќи секојдневно работат со чувствителни информации, доверливи извори и документи од јавен интерес. Во случај на успешен напад, може да се загрози не само безбедноста на новинарот, туку и безбедноста на неговите извори и медиумската организација. Најчестите видови сајбер напади се:

- Фишинг напади – испраќање лажни пораки или е-пошта со цел добивање лозинки и лични податоци;
- Хакерски обиди – неовластен пристап до профили, електронска пошта или уреди;
- Малициозен софтвер (Malware) – програми кои можат да оштетат систем или да украдат податоци;
- Вируси и ransomware напади – програми кои блокираат пристап до податоци и бараат плаќање за нивно враќање;
- Кражба на идентитет – злоупотреба на лични информации и профили.

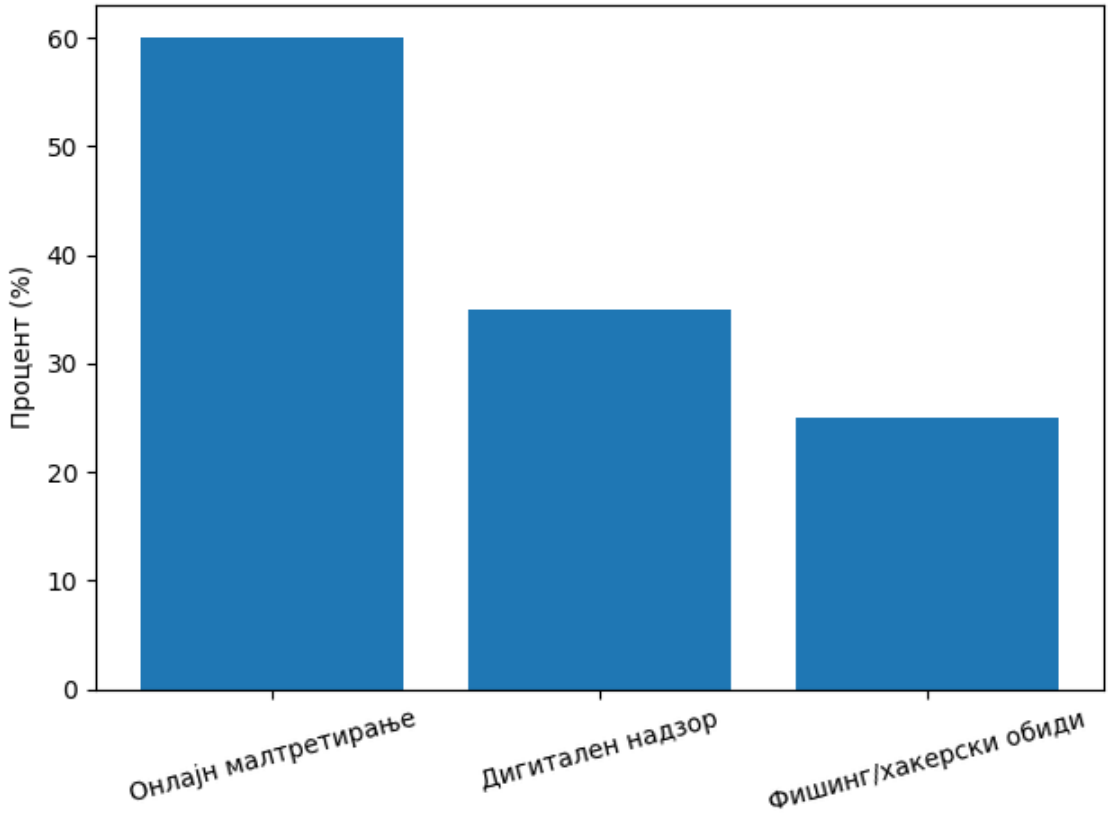
Последиците од сајбер нападите можат да бидат многу сериозни:

- губење на важни информации и документи;
- Кражба на лични и професионални податоци;
- компромитирање на доверливи извори;
- нарушување на приватноста;
- финансиска штета;
- психолошки стрес и чувство на несигурност;
- нарушување на професионалниот углед.

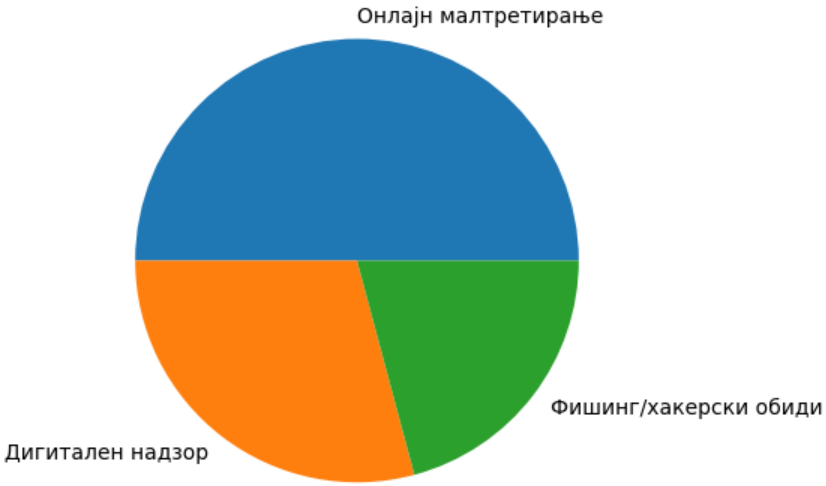
За да се намалат ризиците од сајбер напади, потребно е новинарите да применуваат соодветни мерки за дигитална безбедност. Таквите мерки вклучуваат:

- користење силни и сложени лозинки;
- двофакторска автентикација;
- редовно ажурирање на софтверот и уредите;
- внимателност при отворање линкови и прилози;
- користење безбедни комуникациски платформи;
- редовна едукација за сајбер безбедност.

Со примена на овие мерки, новинарите можат значително да го намалат ризикот од дигитални закани и да создадат побезбедна работна средина.



Графикон 1: Процентуален приказ на проблемите.



Графикон 2: Споредба на резултатите од истражувањето.

Заклучок

Врз основа на резултатите од истражувањето може да се заклучи дека дигиталните технологии имаат големо влијание врз работата и безбедноста на новинарите во Северна Македонија. Иако современите технологии овозможуваат побрзо ширење на информации, полесна комуникација и подобар пристап до различни извори, тие истовремено создаваат нови ризици и предизвици за новинарската професија.

Резултатите покажуваат дека голем број новинари се соочуваат со различни форми на дигитални закани. Дури **60% од испитаниците** пријавиле онлајн малтретирање, **35% изразиле загриженост поради можен дигитален надзор**, а **25% се соочиле со фишинг или хакерски обиди**. Овие податоци укажуваат дека дигиталната безбедност претставува сериозен проблем кој може да влијае врз професионалната работа, приватноста и психолошката состојба на новинарите.

Онлајн нападите и заканите можат да предизвикаат чувство на страв, несигурност и намалување на слободата на изразување. Исто така, сајбер нападите и можноста за дигитален надзор можат да доведат до губење доверливи информации и нарушување на безбедноста на новинарските извори. Поради тоа, потребно е да се посвети поголемо внимание на заштитата на новинарите и создавање побезбедна дигитална средина.

Препораки

За подобрување на безбедноста на новинарите се препорачува:

1. **Организирање обуки за дигитална безбедност** – новинарите треба редовно да посетуваат едукации за препознавање на сајбер закани и заштита на личните податоци.
2. **Користење силни лозинки и двофакторска автентикација** – оваа мерка значително го намалува ризикот од неовластен пристап до профили и уреди.
3. **Користење безбедни комуникациски платформи** – криптирани апликации и безбедни системи за комуникација можат да обезбедат поголема приватност.
4. **Поголема институционална поддршка** – медиумските организации и надлежните институции треба да обезбедат помош и заштита за новинарите кои се жртви на дигитални закани.
5. **Подобрување на законската регулатива** – потребно е зајакнување на законите поврзани со онлајн насилството, сајбер нападите и заштитата на новинарите.
6. **Подигнување на јавната свест** – преку кампањи и јавни активности да се укаже на важноста на безбедноста на новинарите и почитувањето на човековите права.

Со спроведување на овие мерки може да се придонесе кон создавање посигурна и побезбедна работна средина за новинарите, што ќе овозможи слободно и професионално извршување на нивната работа.