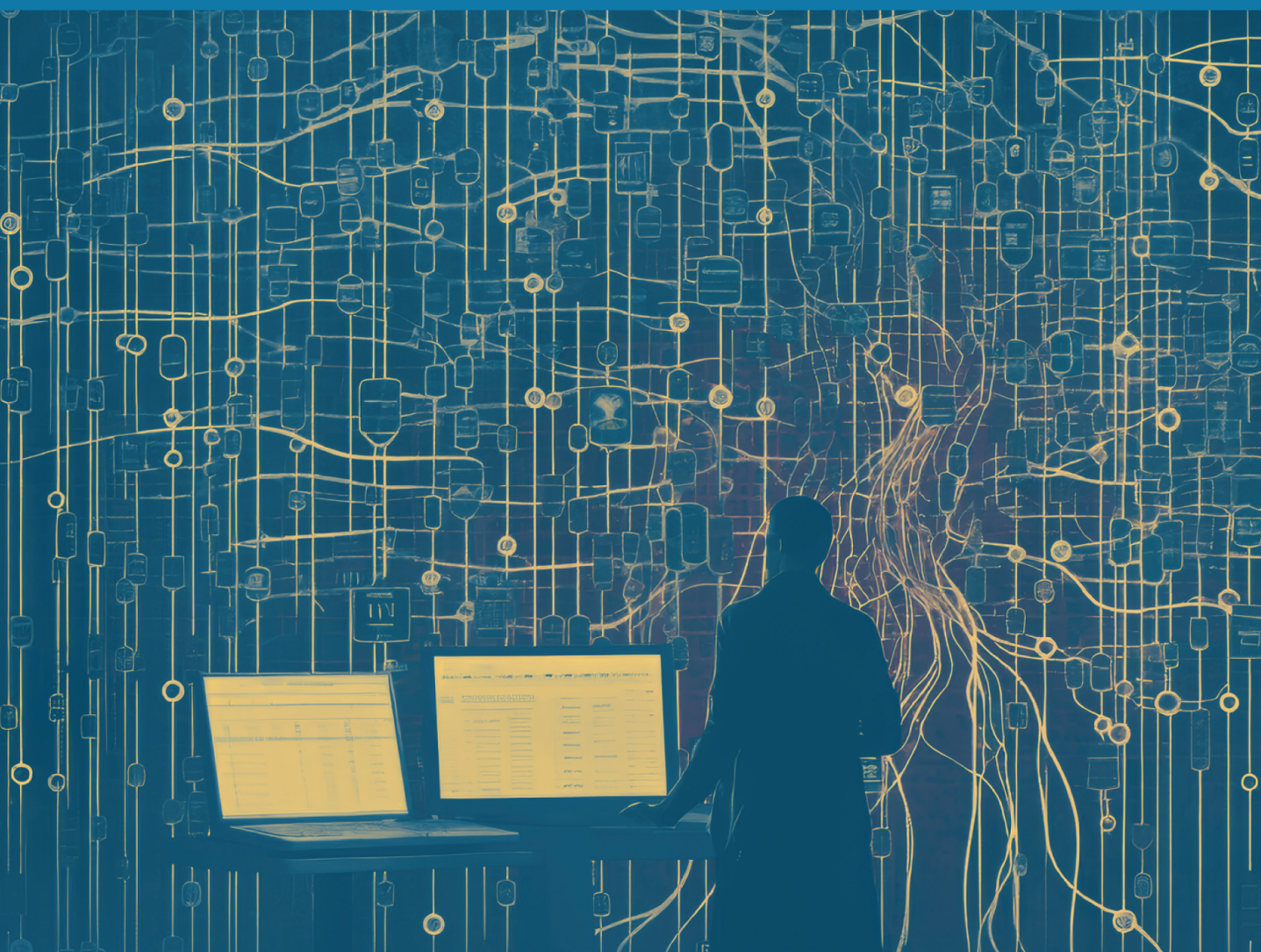
safejournalists.net

Здружение на новинарите на Македонија

ДОКУМЕНТ ЗА ЈАВНИ ПОЛИТИКИ

КООРДИНИРАНИ ДИГИТАЛНИ НАПАДИ ВРЗ НОВИНАРИ И МЕДИУМИ - ПРАКТИЧЕН ПРОТОКОЛ ЗА РЕАКЦИЈА, ЗАЧУВУВАЊЕ ДОКАЗИ И ПОСТАПУВАЊЕ

СКОПЈЕ, ФЕВРУАРИ 2026



Импресум
Документ за јавни политики: Координирани дигитални напади врз новинари и медиуми - практичен протокол за реакција, зачувување докази и постапување

Автор
Мартин Петровски

Редакција
Драган Секуловски

Издавач
Здружение на новинарите на Македонија (ЗНМ)

Проект
„SafeJournalists Network“

Лектура на македонски
Маја Катарова

Превод од македонски на англиски јазик
Оливера Целеска

Превод од македонски на албански јазик
Ферикан Илјази

Дизајн
ЗНМ

Оградување од одговорност
Оваа публикација е изработена со финансиска поддршка на Европската Унија. Нејзината содржина е единствена одговорност на авторот и не ги одразува нужно ставовите на Европската Унија.

Скопје, февруари 2026 г.

НАПОМЕНА

Оваа публикација е наменета како практична насока за редакции и новинари за управување со координирани дигитални напади, со фокус на безбедноста, зачувувањето докази и ефикасна ескалација. Таа не претставува правен совет. Во случаи на висок ризик, особено кога има закани, доксинг или сомнеж за неовластен пристап, се препорачува консултација со правен застапник и пријавување до надлежни институции.

СОДРЖИНА

Импресум 2

Листа на акроними 7

Вовед 8

Кому му е наменет овој документ 8

Методологија 8

Како да го користите овој документ 9

Клучни пораки 9

Што е координиран дигитален напад 10

Зошто ова е важно за редакциите 10

Дел А - Како да го препознаете проблемот 11

Како да препознаете дека станува збор за координиран напад 11

Клучни термини 11

Најчести сценарија на напади врз новинари и медиуми 12

Дел Б - Како да постапите откако ќе го препознаете нападот 13

Основно правило за одлука 13

Улоги и координација во редакција 13

Инцидент „лог“ 14

Следниве полиња се доволни за практична употреба: 14

Брза реакција - првите 60 минути 14

1. Активирајте постапка 14

2. Направете брза процена на ризик 15

3. Зачувајте докази пред какви било промени 15

Минималниот доказен пакет во овој момент вклучува: 15

4. Стабилизирајте ги профилите и пристапот 15

5. Ограничете ја штетата без да го зголемите нападот 16

6. Отворете пријава и следење на постапката 16

7. Побарајте поддршка од ЗНМ кога има основа 16

Принцип „do no harm“ 16

Стандардна оперативна постапка (SOP) - реакција по фази 17

Фаза 1 - првите 24 часа 17

1. Потврдете го типот на инцидент и поставете приоритет 17

2. Продлабочете го собирањето докази 17

3. Активирајте постапки на платформите - пријавување, жалби и враќање на пристапот 17

4. Управувајте со модерација и коментари без да се изгубат докази 18
5. Контролирана комуникација 18
6. Поддршка од ЗНМ и постапување пред институции кога има основа 19
Фаза 2 - 48 - 72 часа 19
1. Следете ги одговорите од платформите и водете статус по предмет 19
2. Консолидирајте „доказен пакет“ за институциите и за партнерите 19
3. Намалете ја изложеноста и заштитете го тимот 19
4. Одлучете за продолжување на објавување и уредничка линија 19
5. Подгответе кратка анализа „што научивме“ и ажурирајте ги мерките 19
Матрица „сигнал - реакција - следни чекори“ 20
Евиденција и зачувување докази 21
Основни принципи 21
Минимален доказен пакет 21
Проширен доказен пакет за платформи и институции 22
Именување, организација и контрола на пристапот 22
Минимизација на личните податоци 23
Интегритет на доказите и доверливост 23
Протокол за доксинг и закани 24
Првите 15 минути - стабилизација и безбедност 24
Првите 60 минути - ограничување на изложеноста 24
Кога заканата изгледа сериозна 25
Докази за доксинг и закани - што е најважно да се фати 25
Координација и постапување 26
Контакт со ЗНМ кога има основа 26
Постапување пред надлежни институции 26
Комуникација во услови на доксинг и закани 26
Што се избегнува во вакви ситуации 26
Начини за пријавување, жалби и враќање пристап кон платформите 28
Општи правила за пријавување и жалби 28
Чек-листа - минимум што треба да содржи пријавата 28
Мета - Инстаграм, Фејсбук и Тредс 29
1. Масовно пријавување и ограничување на досегот 29
2. Имперсонација 29
3. Доксинг и приватност 29
4. Компромитиран профил и враќање на пристапот 29
Официјални линкови - Мета 29
Икс 30
1. Вознемирување и злоупотреба 30

2. Приватни информации и доксинг 30
3. Компромитиран профил 30
Официјални линкови - Икс 30
Јутјуб 31
Официјални линкови - Јутјуб 31
Тик-ток 31
Официјални линкови – Тик-ток 31
Кога пријавите не даваат резултат 32
Брз пакет за пријавување и барање поддршка 32
Кога да се обратите до ЗНМ, а кога директно до институции 32
Што е „брзиот пакет“ - 8 елементи што ги праќате во една порака 33
„Мини пакет“ докази - што е доволно за старт 33
Шаблони 34
Шаблон 1 - Брза порака до ЗНМ 34
Шаблон 2 - „Инцидент лог“ (минимален) 34
Шаблон 3 - Табела за докази (индекс) 35
Шаблон 4 - Мини-формат за известување до институции (ако има основа) 35
Практични правила за приватност при споделување 35
Студија на случај - „Слободен печат“ 36
Контекст 36
Краток преглед на инцидентот 36
Како се развиваше нападот 36
Доказна трага и индикатори 37
Практични лекции што можат да се применат 37
Чек-листа за подготвеност во редакции 38
А. Улоги и координација 38
В. Пристапи и безбедност на сметки 38
С. Рана детекција и модерација 38
D. Психолошка и тимска поддршка 38
Е. Вежбање и ажурирање 38
Клучни извори 39
Платформски политики и алатки (пријавување, жалби, враќање профил) 39
Практични ресурси за дигитална безбедност и одговор на инциденти 40
Европски и меѓународни стандарди релевантни за практична заштита 40

ЛИСТА НА АКРОНИМИ

- *2FA* - (Two-Factor Authentication) двофакторска автентикација
- *CPJ* - Committee to Protect Journalists (Комитет за заштита на новинари)
- *ЕУ/EU* - Европска Унија
- *EUR-Lex* - официјална база на правото на ЕУ (портал за законодавство и акти на ЕУ)
- *FB* - Фејсбук
- *FIMI* - Foreign Information Manipulation and Interference (странско мешање и манипулирање со информации)
- *IG* - Инстаграм
- *ОБСЕ /OSCE* - Организација за безбедност и соработка во Европа (Organization for Security and Co-operation in Europe)
- *SOP* - Standard Operating Procedure (стандардна оперативна постапка)
- *X* - Икс (поранешен Твитер)

ВОВЕД

Координираните дигитални напади врз новинари и медиуми најчесто изгледаат како „брз бран“ на вознемирување - масовни лажни пријави за да се урнат профили, организирано навредување и закани, имперсонација, компромитирање профили или објавување лични податоци со цел заплашување. Овие напади ретко се случајни. Тие се дизајнирани да создадат паника, да го прекинат работењето и да ја нарушат довербата во редакцијата. Во дел од случаите, ваквите напади може да се поврзат и со пошироки операции на странско мешање и манипулирање со информации (FIMI - од англ. *Foreign Information Manipulation and Interference*), но насоките подолу се практични и применливи без разлика на потеклото на нападот.

Овој документ дава практични чекори, кои редакциите можат веднаш да ги применат - како да препознаат дека станува збор за координиран напад, што да направат во првите 60 минути и во првите 72 часа, како да соберат и да ги зачуваат доказите без да ја нарушат приватноста, како да постапат кон платформите, како да побараат поддршка од ЗНМ и кога има основа да се обратат до надлежните институции.

Целта е реакцијата да биде мирна, конзистентна и безбедна. Клучниот принцип е „do no harm“ - да се заштитат луѓето, да се минимизира обработката на лични податоци и да не се преземаат чекори што непотребно ја зголемуваат видливоста на нападот или го изложуваат тимот на дополнителни ризици.

Кому му е наменет овој документ

Овој документ е наменет за уредниците, новинарите, администраторите на профили на социјалните мрежи, менаџментот на редакциите и за лицата задолжени за безбедноста и правните прашања во медиумите.

Методологија

Документот е подготвен врз основа на практични случаи и искуства од работата на ЗНМ со новинарите и редакциите при постапување по дигитални инциденти, како и релевантни насоки за дигитална безбедност, зачувување докази и официјални правила на платформите за пријавување и враќање на пристапот.

Како да го користите овој документ

- Ако нападот е во тек, прво користете ја страницата „Брза реакција“ и веднаш почнете со водење инцидент „лог“[1].
- Потоа следете ја стандардната оперативна постапка (SOP) по фази (првите 60 минути, првите 24 часа, 48-72 часа).
- Доказите собирајте ги систематски и користете го шаблонот за „доказен пакет“, за платформи и институции.
- Ако има закани или „doxxing“ (доксинг)[2], применете го протоколот за итна безбедност и постапете без одлагање.
- Кога е потребно, контактирајте го ЗНМ за поддршка, насочување и координација на следните чекори.

Клучни пораки

- ✓ Координиран напад се третира како инцидент - со улоги, временска линија и јасни одлуки, а не како „хаос на коментари“.
- ✓ Доказите се собираат веднаш, но внимателно - со минимум лични податоци и со контрола на пристап.
- ✓ Постапувањето е по чекори - платформа, ЗНМ, институции - според ризикот и штетата.
- ✓ Безбедноста на луѓето има приоритет - особено кога има закани, „doxxing“ (доксинг) или компромитирани профили.

1 Инцидент „лог“ - кратка временска евиденција на настаните и преземените чекори.

2 „Doxxing“ (доксинг) - јавно споделување лични податоци без согласност, со цел заплашување, вознемирување или поттикнување штета.

ШТО Е КООРДИНИРАН ДИГИТАЛЕН НАПАД

Координиран дигитален напад е намерна и организирана активност насочена кон новинар, уредник или медиум, со цел да се предизвика прекин во работењето, авто-цензура, дискредитација или физичко заплашување. Нападот може да изгледа како „спонтан“ бран, но во пракса често има повторливи обрасци, синхронизација и јасна цел.

Координираните напади се разликуваат од „вообичаената“ онлајн-критика по тоа што се насочени кон контролирање на видливоста и пристапот до публиката. Тоа значи дека целта не е само да се остави коментар, туку да се урне профилот, да се затрупаат каналите за комуникација, да се наметне лажна наративна рамка или да се загрози личната безбедност.

Зошто е важно тоа за редакциите

Кога нападот е координиран, реакцијата добива структура. Импровизацијата најчесто води до три проблеми: губење докази, погрешно постапување кон платформите и зго-лемување на ризикот преку непотребно јавно засилување на нападот. Затоа докумен-тот го третира координираниот напад како инцидент со улоги, инцидент „лог“ и јасни одлуки.

ДЕЛ А - КАКО ДА ГО ПРЕПОЗНАЕТЕ ПРОБЛЕМОТ

Како да препознаете дека станува збор за координиран напад

Не постои еден „сигурен“ знак, но комбинацијата од повеќе сигнали е силен индикатор дека нападот е организиран и дека протоколот треба да се активира.

- Се појавува нагло зголемување на коментари, пораки или реакции во краток период, со повторлив тон и идентични формулации.
- Повеќе профили во исто време објавуваат исти или многу слични обвинувања, линкови или визуелни материјали.
- Се активира масовно лажно пријавување профили, објави или страници, со цел да се ограничат или суспендираат.
- Се појавуваат нови профили со минимална историја, кои координирано напаѓаат или „одговараат“ едни на други за да создадат впечаток на мнозинство.
- Нападот се префрла од една платформа на друга, со истата порака или истото таргетирање.
- Се појавуваат обиди за имперсонација, хакирање или преземање администраторски пристап.
- Се објавуваат или се закануваат да се објават лични податоци, приватни фотографии, адреси, телефони или информации за семејството.
- Се користи „бришење контекст“ преку исечени цитати, скриншоти без извор или лажни наслови, кои потоа се „вртат“ како доказ.

Клучни термини

Масовно лажно пријавување е координирана практика, повеќе профили да пријавуваат содржина или профил, со цел платформата автоматски да го ограничи досегот, да ја отстрани содржината или да суспендира профил.

Имперсонација е креирање или користење профил што се претставува како новинар, медиум или член на редакција, со цел манипулација, измама, дискредитација или прибирање лични податоци.

Компромитиран профил значи дека напаѓачот добил неовластен пристап до профил или до алатки за управување, како на пример администраторски права, е-пошта поврзана со профилот или менаџерски панели.

Доксинг е јавно објавување или закана за објавување лични податоци, со цел заплашување, поттикнување вознемирување или создавање ризик за физичка безбедност.

Координирано вознемирување е организирано таргетирање преку навреди, закани, сексуализирани коментари, манипулирани фотографии или континуирани пораки, со цел исцрпување и заплашување.

Најчести сценарија на напади врз новинари и медиуми

Во редакциската пракса, корисно е нападите да се групираат според тоа што се обидуваат да „срушат“: видливоста, кредибилитетот, идентитетот, пристапот или безбедноста.

Напади врз видливоста	се случуваат кога целта е да се ограничи досегот, да се симне содржина или да се суспендира профил преку масовно лажно пријавување и злоупотреба на платформски механизми.
Напади врз кредибилитетот	се случуваат кога целта е дискредитација преку лажни тврдења, манипулирани изјави, „скриншот докази“ без извор или координирано спинување на една тема.
Напади врз идентитетот	се случуваат кога има имперсонација, лажни профили „во име на редакцијата“ или обиди да се измамат изворите и публиката.
Напади врз пристапот	се случуваат кога има фишинг, преземање профили, компромитирање на е-пошта или обиди за добивање администраторски права.
Напади врз безбедноста	се случуваат кога има закани, доксинг, таргетирање семејство или повици за физичка пресметка и тие секогаш бараат највисок приоритет.

ДЕЛ Б - КАКО ДА ПОСТАПИТЕ ОТКАКО ЌЕ ГО ПРЕПОЗНАЕТЕ НАПАДОТ

Ако препознаете повеќе од наведените сигнали, преминете на практичните чекори подолу и потоа следете ја „Брза реакција“ и SOP по фази.

Основно правило за одлука

Ако нападот влијае врз пристапот до профили, вклучува закани или доксинг, или создава ризик за физичка безбедност, реакцијата се води како високоризичен инцидент. Ако нападот е „само“ бран на коментари, но е координиран и влијае врз видливоста или довербата, протоколот, сепак, се активира, со фокус на доказите, контролирана комуникација и соодветно постапување кон платформите и другите релевантни канали.

Улоги и координација во редакција

Кога нападот е координиран, редакцијата работи како тим со јасни улоги. Целта е да се намали хаосот, да не се изгубат доказите и да се донесат одлуки што ќе го намалат ризикот.

Најдобро е улогите да се назначат однапред и секоја улога да има замена. Кога тоа не е можно, улогите се назначуваат веднаш штом ќе се утврди дека нападот е во тек.

- **Координаторот на инцидентот** ја води реакцијата, ги поставува приоритетите и ја одобрува јавната комуникација.
- **Администраторот на платформите** го проверува пристапот, ги зајакнува поставките, отвора пријави и жалбени постапки и го следи статусот
- **Одговорниот за доказите и „лог“** ги собира доказите, ги именува и ги архивира, води инцидент „лог“ и подготвува доказен пакет.
- **Одговорниот за комуникација** подготвува кратки, контролирани пораки за публиката и партнери, без да го „пумпа“ нападот.
- **Одговорниот за безбедност и правни чекори** прави процена на ризик од закани и доксинг, предлага мерки за заштита и координира обраќање до институциите кога има основа.

Редакцијата применува едно јасно правило: одлуките одат преку координаторот, а секој друг се придржува до договорениот план. Тоа ги спречува паралелните активности, кои создаваат контрадикторни пријави, губење докази или дополнителна изложеност.

Инцидент „лог“

Инцидент „лог“ е едноставен запис, кој овозможува да се следи што се случило, кога и како редакцијата реагирала. „Логот“ е корисен за постапување кон платформите, за институциите и за внатрешна анализа по завршувањето на нападот.

Инцидент „логот“ се води од првиот момент и се ажурира во реално време или на секои 30-60 минути во првите часови. „Логот“ се чува со ограничен пристап и се споделува само со лицата што имаат улога во инцидентот.

Следниве полиња се доволни за практична употреба:

- Записот вклучува датум и точно време на настанот или активноста.
- Записот наведува каде се случува настанот, вклучително и платформа, профил и линк.
- Записот опишува што е забележано, на пример масовно лажно пријавување, закани, имперсонација или компромитиран пристап.
- Записот наведува која акција е преземена и кој ја презел.
- Записот има референца до доказ, на пример број на папка, име на датотека или линк до архивиран материјал.
- Записот има статус, на пример „во тек“, „пријавено“, „во жалбена постапка“ или „затворено“.

Брза реакција - првите 60 минути

Овој дел е наменет за ситуациите кога нападот е во тек и редакцијата треба веднаш да ја стабилизира состојбата. Ако има непосредни закани или доксинг, безбедноста на луѓето има апсолутен приоритет.

1. Активирајте постапка

Веднаш назначете координатор на инцидент и минимум уште две улоги, дури и ако истото лице привремено покрива повеќе задачи. Отворете еден внатрешен канал за координација и договорете правило дека одлуките одат преку координаторот на инцидентот.

2. Направете брза процена на ризик

Проверете дали постојат закани за насилство, доксинг, објавување адреси, телефонски броеви или таргетирање на семејството. Ако постои такво нешто, веднаш преминете на протокол за итна безбедност и постапете без одлагање.

3. Зачувајте ги доказите пред какви било промени

Пред да бришете, да блокирате или да менувате поставки, прво зачувајте го доказниот материјал. Во првите 60 минути, најважно е да се фати „снимката“ на нападот додека е активен.

Минималниот доказен пакет во овој момент вклучува:

- Секој скриншот прикажува целосен екран со датум и време, корисничко име и контекст на објавата или профилот.
- Секоја видеоснимка од екран покажува како се отвора линкот и како се стигнува до спорната содржина, за да се зачува контекстот.
- Секој запис вклучува директен линк до содржината или профилот, а кога има можност и идентификатор на објава или профил.
- Секој сомнителен профил што е дел од нападот се евидентира со линк и со кратка белешка за улогата во нападот.
- Секоја нотификација или е-пошта од платформата се зачувува како доказ, вклучително и предметот, датумот и содржината.

4. Стабилизирајте ги профилите и пристапот

Администраторот на платформи проверува дали има знаци на компромитиран пристап и ги спроведува основните мерки за заштита.

- Лозинките се менуваат од безбеден уред и се користат уникатни и силни лозинки.
- Двофакторската автентикација (2FA) се активира или се потврдува дека е активна за сите клучни профили и е-пошта.
- Активните сесии се прегледуваат и непознатите најави се одјавуваат.
- Администраторските улоги се проверуваат, а непотребните пристапи се отстрануваат додека трае инцидентот.

5. Ограничете ја штетата без да го зголемите нападот

Одговорниот за комуникација ги избегнува импулсивните јавни реакции. Ако е потребна јавна порака, таа е кратка, фактографска и насочена кон заштита на публиката и тимот.

Во првите 60 минути, приоритет имаат мерките што ја намалуваат изложеноста, без да создадат дополнителен конфликт. Модерирањето се прави внимателно и само откако ќе се зачуваат доказите, за да не се изгуби доказната трага.

6. Отворете пријава и следење на постапката

Администраторот на платформи почнува пријавување според типот на нападот, на пример имперсонација, компромитиран профил, доксинг или вознемирување. Одговорниот за докази обезбедува уреден пакет што се користи во пријавите и се поврзува со инцидент „логот“.

7. Побарајте поддршка од ЗНМ кога има основа

Кога нападот е координиран, кога има ризик за безбедноста или кога платформската реакција е неефикасна, редакцијата може да го контактира ЗНМ за насочување и координација на следните чекори. Контактите и форматот на кратко известување се дадени во анексите.

Принцип „do no harm“

- ✓ Личните податоци на напаѓачите или на трети лица не се објавуваат, дури и кога тие први објавиле лични податоци.
- ✓ Закани не се препраќаат и не се објавуваат без претходно да се отстранат личните податоци што можат да ја зголемат изложеноста на таргетираните лица.
- ✓ Јавните пораки не откриваат внатрешни мерки на заштита и оперативни детали (на пример поставки и слабости), кои би им помогнале на напаѓачите да се прилагодат.

Стандардна оперативна постапка (SOP) - реакција по фази

Овој протокол ја организира реакцијата во три временски фази. Целта е редакцијата да остане функционална, да ги заштити таргетираните лица, да ги зачува доказите и да постапува по соодветен редослед преку релевантни канали.

Фаза 1 - првите 24 часа

Во првите 24 часа, приоритет е стабилизација на пристапот, зачувување докази и брзо постапување по соодветни канали.

1. Потврдете го типот на инцидентот и поставете приоритет

Координаторот на инцидентот утврдува дали нападот е насочен кон видливоста, идентитетот, пристапот или безбедноста. Ако има доксинг, закани или компромитиран пристап, инцидентот се третира како високоризичен.

2. Продлабочете го собирањето докази

По првичниот доказен пакет, одговорниот за докази го проширува материјалот за да може да се користи и за постапување кон платформи и за постапување пред институциите. Секој доказ добива контекст, временска ознака и јасна врска со инцидент „логот“.

- Доказите се организираат во структурирана папка со јасни потпапки по платформи и по тип на напад.
- Секоја датотека добива име што вклучува датум, време, платформа и краток опис на содржината.
- При архивирање, личните податоци на таргетираните лица и трети лица се минимизираат, а пристапот до папката се ограничува.

3. Активирајте постапки на платформите - пријавување, жалби и враќање на пристап

Администраторот на платформи почнува постапки според типот на нападот. Секој поднесок се поткрепува со доказен пакет, а во инцидент „логот“ се бележи бројот на пријава или статус.

Кога постои ризик од губење профил или компромитиран пристап, приоритет е враќањето контрола над пристапот, а потоа јавна комуникација.

4. Управувајте со модерацијата и со коментарите без да се изгубат доказите

Модерирањето следи едно правило: прво доказ, потоа интервенција. Откако ќе се зачуваат доказите, редакцијата може да преземе ограничени мерки за намалување на штетата, со процена дали мерката ќе го поттикне нападот.

- *Коментарите* и пораките се модерираат според јасната логика што разликува критика од вознемирување и закани.
- Секој елемент што содржи закана или лични податоци се документира и се третира со повисок приоритет.
- Масовното бришење се избегнува кога ја уништува доказната трага и го отежнува постапувањето.

5. Контролирана комуникација

Одговорниот за комуникација обезбедува редакцијата да зборува со еден глас, со минимален ризик од дополнително поттикнување на нападот. Во првите 24 часа, јавната порака е кратка и насочена кон фактите, а не кон расправа со напаѓачите.

Кога има закани или доксинг, јавната комуникација е внимателна и не открива лични детали, локации, распоред или внатрешни мерки на заштита. Во таквите случаи, комуникацијата со институциите и поддржувачките мрежи добива приоритет.

6. Поддршка од ЗНМ и постапување пред институциите кога има основа

Кога нападот е координиран и предизвикува значајна штета, редакцијата може да го контактира ЗНМ со кратко резиме, инцидент „лог“ и клучни докази. Тоа овозможува поефикасна координација и насочување за следните чекори.

Ако има закани, доксинг, компромитирање профили или злоупотреба на лични податоци, редакцијата може да пристапи кон постапување пред надлежните институции, со јасен доказен пакет и минимизација на непотребни лични податоци.

Фаза 2 - 48 - 72 часа

Во 48 - 72 часа, приоритет е да се консолидираат доказите, да се следат одговорите од платформите, да се намали изложеноста и да се стабилизира работата на редакцијата.

1. Следете ги одговорите од платформите и водете статус по предмет

Администраторот на платформи одржува листа со сите пријави и жалби, со датум, статус и следни чекори. Ако платформата реагира со автоматски санкции кон профилот или содржината, редакцијата поднесува жалба со јасна аргументација и уреден доказен пакет.

2. Консолидирајте „доказен пакет“ за институциите и за партнерите

Одговорниот за докази подготвува консолидиран пакет што содржи временска линија, клучни докази, кратко објаснување на штетата и јасни барања. Пакетот се прави читлив и употреблив без дополнителни интерпретации.

3. Намалете ја изложеноста и заштитете го тимот

Редакцијата ја проценува изложеноста на поединци, особено новинари што се директно таргетирани. Ако постојат ризици, се разгледуваат мерки како ограничување на јавна видливост на лични профили, засилена приватност и дополнителна поддршка за психолошка и физичка безбедност.

4. Одлучете за продолжување на објавување и уредничка линија

Координаторот на инцидент, заедно со уредничкиот тим, носи одлука дали редакцијата продолжува со објавување тема што го предизвикала нападот и како ќе го направи тоа без непотребно зголемување на ризикот. Одлуката се темели на проценатa на ризик и на поддршката што редакцијата реално ја има.

5. Подгответе кратка анализа „што научивме“ и ажурирајте ги мерките

По смирувањето на најсилниот бран, редакцијата прави кратка внатрешна анализа со три прашања: што функционираше, што не функционираше и што треба да се промени во улогите, алатките и процедурите. Оваа анализа е кратка, но води кон конкретни подобрувања.

Матрица „сигнал - реакција - следни чекори“

Оваа матрица служи за брза ориентација и може да се прилагоди на конкретниот случај и платформата (на пример Мета - Инстаграм/Фејсбук/Тредс, Икс, Јутјуб, Тик-ток).

Сигнал	Реакција (веднаш)	Следни чекори (ако продолжи / ако е сериозно)
Масовно лажно пријавување + пад на досег / ограничување	Зачувај докази (скриншоти/видео) + поднеси пријава/жалба на платформата	Контактирај го ЗНМ ако профилот е сериозно загрозен или има повторливи санкции
Имперсонација (лажен профил „како медиум/новинар“)	Документирај лажен профил + утврди/објави кој е официјален канал	Пријава за имперсонација на платформата + ЗНМ ако има повеќе профили / пошироко таргетирање
Компромитиран профил (сомнителни најави/промени)	Врати пристап + смени лозинки + 2FA + одјави непознати сесии	Постапка за враќање пристап на платформата + институции ако има злоупотреба/закани
Доксинг или закани	Итна безбедносна процена + зачувај докази + намали изложеност	Итно постапување пред институции + контакт со ЗНМ за координација
Координирано вознемирување (навреди/организиран напад)	Зачувај докази + внимателна модерација	Пријава на прекршувања на платформата + ЗНМ ако има значајна штета / повеќе платформи
Манипулирани „докази“ / исечени цитати	Архивирај извор + подготви фактографска корекција	Пријава ако има имперсонација/злоупотреба приватност + информирање партнери по потреба

ЕВИДЕНЦИЈА И ЗАЧУВУВАЊЕ ДОКАЗИ

Доказите се клучни за две цели: да се добие навремена реакција од платформите и да се обезбеди основа за постапување пред надлежните институции кога има закани, доксинг, компромитиран пристап или злоупотреба на лични податоци. Во координиран напад, доказите често исчезнуваат брзо - се бришат содржини, се деактивираат профили, а контекстот се губи. Затоа собирањето и зачувувањето почнува веднаш и се прави систематски. Во дел од случаите, ваквите напади се надоврзуваат на пошироки манипулативни кампањи во информацискиот простор (вкл. FIMI[3]), па дисциплината со докази е клучна и за разбирање на образецот.

Основни принципи

- Доказите се собираат пред интервенциите, како бришење, блокирање или промена на поставките, освен кога има непосредна опасност по безбедноста.
- Доказите го задржуваат контекстот, затоа што изолиран скриншот без околни елементи често не е доволен.
- Доказите се чуваат со ограничен пристап и со минимум обработка на личните податоци, согласно принципот „do no harm“.
- Доказите се поврзуваат со „инцидент логот“, за да се обезбеди јасна временска линија и проверливост на активностите.

Минимален доказен пакет

Минималниот доказен пакет е сет што редакцијата го обезбедува во првите часови, без оглед на типот на нападот. Овој пакет обично е доволен за иницијални пријави до платформи и за брза процена на ризикот.

- Секој доказ содржи датум и време и е поврзан со конкретен линк или профил.
- Секој скриншот го прикажува целиот екран со видливи кориснички имиња, контекст и барем дел од навигацијата.
- Секоја видеоснимка од екран прикажува како се отвора линкот и како се доаѓа до спорната содржина, за да се зачува контекстот.

3 Странско мешање и манипулирање со информации - од англ. *Foreign Information Manipulation and Interference*

- Секоја закана се документира со целосен текст и околен контекст, вклучително и белешка дали заканата се повторува или се засилува.
- Секоја нотификација или е-пошта од платформата се зачувува во оригинал, со предмет, датум и содржина.

Проширен доказен пакет за платформи и институции

Кога нападот е координиран, минималниот пакет се проширува во „доказен пакет“ што може да се достави како целина. Овој пакет треба да биде читлив и да овозможи брзо постапување, без потреба од дополнителни објаснувања.

Доказниот пакет вклучува:

- Кратко резиме на инцидентот со опис на типот на напад, времетраење и штета.
- Временска линија со најважните настани, поврзана со „инцидент логот“.
- Табела со клучни линкови, профили и објави, со кратка белешка што го покажува или го потврдува секој елемент.
- Избрани докази во прилог, организирани по тип на напад, како масовно лажно пријавување, имперсонација, компромитиран профил, доксинг или закани.
- Јасно наведени барања, на пример враќање на профилот, отстранување на содржина, санкционирање на лажен профил или итно постапување по закани.
- Контакт точка во редакцијата, со службен контакт и лице задолжено за следење на предметот.

Именување, организација и контрола на пристапот

Систематската организација го намалува ризикот од губење материјали и овозможува побрзо доставување и користење на доказите. Еден договорен формат е доволен, ако се применува доследно.

- Главната папка го носи датумот и краток назив на инцидентот.
- Потпапките се организираат по платформи и по тип на напад, за да се избегне мешање на материјалите.
- Секоја датотека содржи датум, време, платформа и краток опис, за да може да се најде брзо и без пребарување по содржина.
- Пристапот до доказите се ограничува на лица со улога во инцидентот, а споделувањето се бележи во „инцидент логот“.

- Доказите се чуваат со најмалку една резервна копија, на безбедна локација, која е достапна и на координаторот на инцидент.

Минимизација на личните податоци

Во координирани напади често се појавуваат лични податоци и содржини што можат дополнително да го изложат таргетираното лице. Редакцијата внимава доказите да се зачуваат, а истовремено да не се создава дополнителна штета.

- Ако доказите се споделуваат надвор од тесниот инцидент тим, се подготвуваат две верзии - „интерно“ и „за споделување“ - со отстранување непотребни лични податоци.
- Ако се прави замаглување или прикривање, се чува и оригинална верзија со ограничен пристап, за да не се изгуби доказната вредност.
- Ако доказот содржи адреса, телефон или чувствителни податоци, тие не се препраќаат на поширoки групи и не се објавуваат, дури и кога се дел од нападот.
- Ако доказите вклучуваат малолетни лица или семејни информации, тие се третираат како високоризични и се споделуваат само кога е неопходно за постапката.

Интегритет на доказите и доверливост

Дури и во практичен контекст, основната дисциплина за интегритет и доверливост ја намалува можноста за спорење на автентичноста.

- Секој доказ се зачувува што е можно поблиску до „оригиналната состојба“, без уредување што ја менува содржината.
- Секој доказ има белешка кој го прибавил, кога и на кој начин, а ова се бележи и во „инцидент логот“.
- Секое споделување на доказниот пакет се евидентира, со наведен примател и цел на споделувањето.

ПРОТОКОЛ ЗА ДОКСИНГ И ЗАКАНИ[4]

Доксинг и заканите се третираат како високоризични ситуации затоа што можат бргу да преминат од онлајн-вознемирување во реален ризик за безбедност. Во овие случаи, приоритет е заштитата на таргетираните лица и нивните блиски, па потоа заштита на профилите, содржината и репутацијата.

Овој протокол се активира кога има барем еден од следниве елементи: јавнообјавени лични податоци, закана за физичко насилство, таргетирање на дом/семејство, повик за „посета“, следење или повторливи закани што се засилуваат.

Првите 15 минути - стабилизација и безбедност

Првиот чекор е брза процена дали постои непосредна опасност. Ако заканата е конкретна, временски блиска или содржи информации што упатуваат дека напаѓачот знае адреса/рута/распоред, се постапува како за итна безбедносна ситуација.

- ✓ Таргетираната личност се известува директно и дискретно, без споделување на заканата во широки групи.
- ✓ Се договара краток „безбедносен статус“ - дали лицето е дома, на пат, само или со други и дали има чувство дека е следено.
- ✓ Корисно е лицето да не се движи само и, кога е можно, да се промени рутата, местото или времето на движење за да се намали предвидливоста.
- ✓ Се назначува контакт-лице од редакцијата, кое останува достапно за координација додека ситуацијата не се смири.
- ✓ Се почнува со собирање докази, но без препраќање лични податоци на лица што не учествуваат во инцидентот.

Првите 60 минути - ограничување на изложеноста

Целта во првиот час е да се намали видливоста на чувствителни податоци и да се спречи дополнителна штета.

4 Совет на Европа (Council of Europe), „Improvement of national legislation on doxing and source protection“, 2.7.2024, Platform to promote the protection of journalism and safety of journalists, https://www.coe.int/en/web/freedom-expression/-/improvement-of-national-legislation-on-doxing-and-source-protection

- ✓ Се проверува дали лични податоци се појавуваат на повеќе места и платформи, а потоа се прави список со линкови и скриншоти со контекст.
- ✓ Се пријавува содржината што содржи лични податоци и/или закани преку платформските механизми за приватност и вознемирување, со јасно наведување дека содржината содржи лични податоци и претставува ризик.
- ✓ Се преиспитуваат јавните информации на профилите на таргетираната личност и редакцијата, а непотребните детали се тргаат или се ограничуваат.
- ✓ Се известуваат блиски лица само во обем што ја зголемува безбедноста, а не во обем што создава паника или дополнително споделување на податоците.

Кога заканата изгледа сериозна

Заканата се смета за посериозна кога е конкретна, повторлива, содржи лични детали, повикува на непосредно дејство или доаѓа од повеќе профили во координација. Во такви случаи, има основа да се побара итна институционална заштита и да се води постапка со целосен доказен пакет.

- Ако има непосредна опасност, се контактираат надлежните итни служби.
- Ако има закана, доксинг или следење, се подготвува пријава до надлежните институции со јасна временска линија и доказен материјал.
- Ако е потребно, се разгледуваат дополнителни мерки за физичка заштита, како придружба, привремена промена на рутина или привремено избегнување на јавни појавувања.

Докази за доксинг и закани - што е најважно да се фати

Кај закани и доксинг, доказите треба да покажат што точно е кажано или објавено, кој го објавил, каде и кога и дали има засилување во интензитетот.

- Секој доказ прикажува целосен контекст, вклучително и корисничко име, датум/време и линк.
- Се зачувуваат и нотификациите или пораките што покажуваат дека содржината била видлива или распространета.
- Се зачувуваат повторувањата и варијациите на заканата, затоа што засилувањето е важен индикатор.
- Се бележи дали заканата е поврзана со конкретна објава, истражување или тема, за да се разбере мотивот и патеката на ширење.

КООРДИНАЦИЈА И ПОСТАПУВАЊЕ

Контакт со ЗНМ кога има основа

Во случаи на доксинг и закани, контакт со ЗНМ може да помогне за насочување, координација и јавна поддршка кога тоа е безбедно и корисно. При известување, доволно е кратко резиме, линкови до клучни докази и процена дали има непосреден ризик.

Постапување пред надлежните институции

Кога се поднесува пријава, на институциите им користи јасната структура. Најчесто е доволно да се достави:

- Краток опис на настанот и зошто се смета за закана или доксинг.
- Временска линија на клучни настани, поврзана со „инцидент логот".
- Избрани докази што ја покажуваат заканата или објавените лични податоци.
- Информација дали има повторување, координација или префрлање на повеќе платформи.
- Контакт-точка за понатамошна комуникација и достава на дополнителни докази.

Комуникација во услови на доксинг и закани

Јавната комуникација во вакви ситуации бара дополнителна претпазливост. Понекогаш тишината и ограничената комуникација даваат подобар резултат од јавна расправа.

- Јавна порака, ако се дава, останува кратка и фактографска и не повторува лични податоци или детали од заканата.
- Не се објавуваат скриншоти што содржат адреси, телефони или други чувствителни податоци, дури ни кога целта е „да се покаже што се случува".
- Не се најавуваат следни чекори, кои би им помогнале на напаѓачите да се приспособат, како детали за пријавување, безбедносни мерки или внатрешна организација.

Што се избегнува во ваквите ситуации

Одредени реакции изгледаат „логични“ под стрес, но често ја влошуваат состојбата или ја зголемуваат изложеноста.

- Не се влегува во директна расправа со профили што упатуваат закани или објавуваат лични податоци.
- Не се охрабрува публиката да „го бара“ напаѓачот, затоа што тоа може да предизвика дополнителни злоупотреби и правни ризици.
- Не се споделуваат доказите во широки групи, особено кога содржат чувствителни лични податоци.

НАЧИНИ ЗА ПРИЈАВУВАЊЕ, ЖАЛБИ И ВРАЌАЊЕ ПРИСТАП КОН ПЛАТФОРМИТЕ

Платформите најчесто реагираат прво преку автоматизирани системи. Затоа исходот зависи од тоа дали пријавата е поднесена по точната категорија, дали има доволно контекст и дали доказите се јасни. Кај координираните напади (вклучително и случаи што носат елементи на FIMI - синхронизирано таргетирање и наметнување лажни наративи), дисциплината во фактите и доказите е особено важна.

Овој дел дава практични патеки за пријавување, жалби и враќање пристап. Линковите се наведени во фусноти, за да остане текстот читлив и употреблив под притисок.

Општи правила за пријавување и жалби

- Секогаш прво се зачувуваат доказите, па потоа се интервенира со пријавување, бришење или со блокирање.
- Пријавата се поднесува по најсоодветната категорија, затоа што погрешна категорија често носи автоматско одбивање.
- Една пријава е поефикасна кога е комплетна и конзистентна, отколку повеќе пријави со недоволен контекст.
- Секој поднесок се евидентира во „инцидент лог“, со датум, време, линк и статус.
- Во пријавите не се повторуваат непотребни лични податоци, особено кај доксинг и закани, туку се користи опис и приложен доказ.

Чек-листа - минимум што треба да содржи пријавата

- Пријавата почнува со една јасна реченица што го именува прекршувањето и што точно се бара да се преземе.
- Пријавата содржи директен линк до содржината/профилот и најмалку уште еден пример што го покажува контекстот.
- Пријавата наведува кратка временска рамка: кога почнало, дали е во тек и дали има ескалација во обемот/интензитетот.
- Пријавата наведува зошто се смета дека нападот е координиран (повторливи профили, синхронизација, масовно пријавување, префрлање меѓу платформи).
- Пријавата завршува со конкретно барање: отстранување содржина, санкција на лажен профил, враќање пристап или итно постапување по закана.

Мета - Инстаграм, Фејсбук и Тредс

1. Масовно пријавување и ограничување на досегот

Кога има сомнеж дека профилот се таргетира преку масовни лажни пријави, практично е да се реагира на два колосека: да се зачуваат нотификациите/санкциите и да се поднесе жалба преку достапните механизми за „review“ или „appeal“. Ако дојде до ограничување, отстранување или суспензија, корисно е да се зачува целата нотификација од платформата и да се приложи во доказниот пакет. Овој тип случаи често бара упорност и конзистентност во жалбите.

2. Имперсонација

Кога има профил што се претставува како новинар или медиум, најбрзиот пат е пријавување за имперсонација и доставување линк до официјалниот профил што се имитира.

3. Доксинг и приватност

Кога се објавуваат лични податоци, се користат категориите за приватност и вознемирување, со јасно наведување дека станува збор за злоупотреба на лични информации. Во самиот текст на пријавата се избегнува повторување на адреси, телефони и други чувствителни детали. Наместо тоа, се приложуваат скриншоти и линкови.

4. Компромитиран профил и враќање на пристапот

Кога профилот е компромитиран или се сомневате на преземање на пристапот, најважно е да се оди по официјалните recovery патеки и да се избегнуваат „совети“ од непроверени профили што нудат „помош“. Во вакви случаи, корисно е да се почне од уред што претходно се користел за најавување, затоа што платформите често го користат тоа како сигнал за доверба.

Официјални линкови - Мета

- Instagram/Threads - пријавување имперсонација (формулар): https://help.instagram.com/contact/636276399721841.
- Instagram - упатства за пријавување имперсонација: https://help.instagram.com/370054663112398.
- Instagram/Threads - пријавување повреда на приватноста: https://help.instagram.com/contact/512241091300432.

- Instagram - пријавување вознемирување/малтретирање: https://help.instagram.com/547601325292351.
- Meta Account Recovery Hub (Facebook/Instagram/Threads): https://www.meta.com/account-recovery-support/.
- Instagram - „hacked account“ поддршка: https://www.instagram.com/hacked/.
- Facebook - „hacked account“ алатка: https://www.facebook.com/hacked.

Икс

1. Вознемирување и злоупотреба

Пријавувањето на Икс најчесто оди преку „Report“ од пост или од профил, со избор на категорија и дополнителен контекст.

2. Приватни информации и доксинг

Социјалната платформа „Икс“ има посебна политика за приватни информации и пријавување за злоупотреба. Кај доксингот, корисно е пријавата да биде јасна, со линк до постот и кратко објаснување зошто објавеното е приватна информација и како се користи за злоупотреба.

3. Компромитиран профил

За компромитираниот профил, Икс нуди формулар за враќање на пристапот. Ако профилот е „locked“ или „limited“, практично е да се следат чекорите за верификација и враќање на функциите.

Официјални линкови - Икс

- Пријавување злоупотреба: https://help.x.com/en/safety-and-security/report-abusive-behavior.
- Политика за лични информации: https://help.x.com/en/rules-and-policies/personal-information.
- Формулар за „hacked or compromised“: https://help.x.com/en/forms/account-access/regain-access/hacked-or-compromised.

Јутјуб

Јутјуб експлицитно ги третира заканите и доксингот како дел од забрането однесување во рамките на политиките за вознемирување и сајбер-булинг. При пријавувањето, корисно е да се приложи конкретен линк, временска ознака во видеото и кратко објаснување како содржината таргетира личност или медиум.

Официјални линкови - Јутјуб

- Политика за вознемирување и сајбер-булинг: https://support.google.com/youtube/answer/2802268.

Тик-ток

Тик-ток има централизирано „Report a problem“ мени и конкретни чекори за пријавување профил, содржина или злоупотреба. Во координирани напади, корисно е да се соберат неколку примери и да се пријават со јасно наведување дека има повторливост и координација. Ако профилот е компромитиран, Тик-ток дава основни чекори за враќање на безбедноста.

Официјални линкови – Тик-ток

- „Report a problem“: https://support.tiktok.com/en/safety-hc/report-a-problem.
- Како да се пријави профил: https://support.tiktok.com/en/safety-hc/report-a-problem/report-a-user.
- Ако сметката е хакирана: https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked.

Кога пријавите не даваат резултат

Понекогаш платформите не реагираат брзо или одлуките се неконзистентни. Во такви случаи, корисно е редакцијата да направи краток „рифреш“ на пристапот.

- ✓ Се проверува дали категоријата на пријавата е точна и дали има доволно контекст.
- ✓ Се поднесува жалба или повторна пријава само кога има нови факти или дополнителни докази.
- ✓ Се консолидира доказниот пакет во една читлива целина наместо да се праќаат фрагменти.
- ✓ Се разгледува контактот со ЗНМ кога има висок ризик, повторливи санкции или значајна штета по работењето.

Брз пакет за пријавување и барање поддршка

Кога нападот е координиран, најмногу време се губи на „склопување на приказната“ од повеќе пораки и документи. Затоа е корисно да имате стандарден „брз пакет“ што се праќа како **една порака**, со јасна структура и **неколку клучни докази**. Документирањето и логирањето (датум, линк, што се случило) е важно затоа што содржините и профилите често исчезнуваат или се менуваат.

Кога да се обратите до ЗНМ, а кога директно до институциите

Обратете се до ЗНМ кога има јасна потреба од координација и од побрза поддршка, на пример:

- профилот/страницата е ограничена, отстранета или реално ризикува суспензија поради масовни лажни пријави,
- имперсонација на новинар/медиум (особено ако собира лични податоци или шири штетни дезинформации),
- компромитиран пристап или сериозни обиди за преземање (вклучително и повторлив фишинг кон тимот),
- јавнообјавени лични податоци со цел вознемирување доксинг или закани за насилство,
- значајна оперативна штета (прекин на објавувањето, губење пристап до аудиториумот, сериозен удар врз довербата).

Институционално постапување се разгледува кога има:

- ризик за лична безбедност,
- објавени лични податоци доксинг, особено адреса/телефон/податоци за семејството,
- закани за насилство или повик за „посета“/следење,
- неовластен пристап до профили и индиции за злоупотреба на личните податоци,
- организирана координација што создава мерлива штета.

Што е „брзиот пакет“ - 8 елементи што ги праќате во една порака

- **Предмет/наслов:** координиран напад - [медиум/новинар] - [платформа] - [датум];
- **Кратко резиме (4 - 6 реченици):** што се случува, како се гледа координацијата, статус (дали е во тек);
- **Временска рамка:** почеток + клучни моменти + моментален статус;
- **Тип на напад:** масовно лажно пријавување/имперсонација/преземање пристап/ доксинг/ закани/ друго;
- **Кој е таргетиран:** на ниво на улога (новинар, уредник, админ на страница), без непотребни лични детали;
- **Што е преземено:** најважните чекори (пријавено, жалено, сменети лозинки, 2FA, ограничени пристапи);
- **Што барате:** насочување, координација, правна поддршка, јавна реакција, контакт со институциите (само што е реално потребно);
- **Докази:** 3-5 клучни линкови + прилог/фолдер со „мини пакет“.

Практично правило: подобро **е еден комплетен пакет** отколку повеќе пораки „дополнително ќе пратам“.

„Мини-пакет“ докази - што е доволно за старт

- Неколку **скриншоти со контекст** (цел екран, корисничко име, видлив линк/наслов, дел од околината);
- Една **кратка видеоснимка од екран** кога контекстот е критичен (како се отвора линкот и каде се гледа спорната содржина);
- Најважните **нотификации/имејлови** од платформата (ограничување, предупредување, суспензија);
- Кратка **табела со линкови** (3-10 реда) со колона „што докажува“;
- Ако има имејлови со закани - зачувајте ги во оригинал (не ги „препраќајте“ како единствен доказ без потреба), за да не се изгубат техничките податоци/контекстот.

ШАБЛОНИ

Шаблон 1 - Брза порака до ЗНМ

Предмет: Координиран напад - [медиум/новинар] - [платформа] - [DD.MM.YYYY]

Резиме (4-6 реченици):

- ✓ Што се случува;
- ✓ Како се гледа координацијата;
- ✓ Статус: (во тек/смирено/повторно се појавува);
- ✓ Главен ризик: (губење на профилот/безбедноста/ друго)

Тип на напад: [изберете]
Таргет: [улога - без лични податоци]
Што е преземено: [3-6 кратки точки]
Што бараме од ЗНМ: [1-2 реченици]

Клучни линкови (3 - 5):

- ✓ [линк] - што покажува
- ✓ [линк] - што покажува
- ✓ [линк] - што покажува

Прилог/фолдер: [линк со ограничен пристап или „мини пакет“ во прилог]
Контакт: [име, функција, службен телефон, службен имејл]
Резервен контакт: [име + контакт]

Шаблон 2 - „Инцидент лог“ (минимален)

Ова е внатрешна евиденција што ви прави временска линија и ве спасува од „каде беше оној линк“. (Препорачливо е да е една табела што се дополнува.)

Назив на инцидент: [кратко]
Датум: [DD.MM.YYYY]
Координатор на инцидентот: [име и улога]
Статус: [во тек / стабилизиран / затворен]

Време	Платформа	Линк/ локација	Што се случи	Што направивме	Доказ
[HH:MM]	[IG/FB/X…]	[линк]	[1 реченица]	[1 реченица]	[име на фајл/ линк]

Шаблон 3 - Табела за докази (индекс)

Ознака	Датум/ време	Платформа	Линк	Што прикажува	Зошто е важно
Д1	[DD. MM.YYYY HH:MM]	[ ]	[ ]	[ ]	[закана/доксинг/ имперсонација/преземање пристап…]

Шаблон 4 - Мини-формат за известување до институциите (ако има основа)

Предмет: Известување/пријава за [закани/доксинг/неовластен пристап/ организирано вознемирување] - [DD.MM.YYYY]

1. **Краток опис:** (5-8 реченици: што, кога, каде, кој е таргетиран - на ниво на улога).
2. **Зошто е ризик:** (1-2 реченици: безбедност/приватност/пристап/штета).
3. **Клучни докази:** (Д1, Д2, Д3 + по една реченица што покажуваат).
4. **Штета досега:** (конкретно: ограничен профил, објавени лични податоци, закани, изгубен пристап).
5. **Барање за постапување:** (што очекувате: прием, насочување, итно постапување, заштита на лични податоци).
6. **Контакт и доверливост:** (контакт точка + реченица дека доказите содржат чувствителни податоци и се за службена употреба).

Практични правила за приватност при споделување

- Во текст не повторувајте адреси/телефони - упатете на доказот каде што се гледаат.
- Ако праќате на повеќе примателi – праќајте ја верзијата „за споделување“ (со тргнати непотребни лични податоци), а оригиналот чувајте со ограничен пристап.
- Не праќајте докази во големи групи/четови ако содржат лични податоци.

СТУДИЈА НА СЛУЧАЈ - „СЛОБОДЕН ПЕЧАТ“

Овој случај покажува како координиран напад може да почне како „необични коментари“, а потоа да се префрли во други форми што потешко се контролираат, како масовни лајкови и следења, со последици врз редовното работење и видливоста на содржините.

Контекст

Официјалните инстаграм-профили на „Слободен печат“ се @slobodenpecat и @slobodenpecat.vesti. Профилите се одржувани континуирано околу осум години, со органски раст и без користење платени промоции за следбеници или досег.

Краток преглед на инцидентот

Инцидентот се одвиваше во периодот од 6.11.2025 до 10.11.2025 година на Инстаграм. Нападот почна со масовни идентични коментари, а потоа се префрли во масовни лајкови и барања за следење од сомнителни профили. Како главни последици беа наведени попречување на работата на редакцијата и драстичен пад на досегот, со сомнеж за алгоритамско ограничување на видливоста.

Како се развиваше нападот

На 6.11.2025 година беше забележан прв бран - голем број идентични коментари со зборот „like“ во рамки на иста минута, од профили без претходна интеракција со медиумот и со карактеристики типични за лажно генерирани или ботски профили. Истата појава се повтори и под наредните објави, во кус временски период.

Во текот на истиот ден се појави втор бран - масовни коментари со политички обоена содржина и повторливи формулации, во кои „Слободен печат“ се обвинуваше за цензура и бришење коментари, со наративи поврзани со меѓународни конфликти. Коментарите доаѓаа од профили без историја на интеракција со медиумот, што дополнително упатуваше на координација.

По активирањето заштитни опции на платформата и ограничувања за коментирање, масовните коментари се намалија, но нападот се пренасочи. На 9.11.2025 година беше забележан нагол скок на лајкови од истиот тип сомнителни профили на објава со висок досег. Бидејќи не постои практичен механизам за селективно „чистење“ на масовни лајкови, профилот беше направен приватен со цел да се заштити континуитетот на работата и органски изградената публика. На 10.11.2025 година беа регистрирани повеќе од 999 барања за следење, од кои најголемиот дел беа од очигледно лажно генерирани профили, што бараше рачно чистење.

Доказна трага и индикатори

Случајот е пример за тоа како доказите треба да ја задржат временската линија и да ја покажат „еволуцијата“ на нападот.

- Линкови до објавите каде што се јавуваат првите сигнали, заедно со скриншоти што го прикажуваат контекстот и повторливоста.
- Визуализации и споредби на статистики („views over time“), кои укажуваат на нагло отстапување во досегот по нападот, како основа за сомнеж за алгоритамско ограничување.
- Скрин-рекординг што ја покажува атипичната динамика на лајкови и следења.
- Нотификации од платформата, кога ги има, како дополнителен доказ за статус и мерки.

Практични лекции што можат да се применат

1	Нападот ретко останува во една форма, па ограничувањето на коментарите може да го префрли нападот кон лајкови, следења или други механизми на платформата.
2	Рачното „чистење“ бргу го троши капацитетот на редакцијата, па корисно е рано да се активира инцидент режим со улоги и временска линија.
3	Ограничувањата за коментирање и модерација се ефикасни кога се комбинираат со систематско собирање докази и со конзистентни пријави кон платформите.
4	Привременото заклучување (приватност) може да биде тактичка мерка кога нападот создава масовен технички товар, но ваквата мерка е поефикасна ако е предвидена однапред како опција во планот за реагирање.
5	Доказниот пакет е посилен кога ги прикажува фазите на нападот и реалната штета, а не само поединечни скриншоти без контекст.
6	Раната координација со ЗНМ и евидентирањето на случајот кај надлежните институции создаваат основа за понатамошна поддршка и за подобра институционална реакција во идните случаи.

A. Улоги и координација	✓ Назначете водител на инцидент и 2 резерви (минимум: одлуки, управување профили, собирање докази). ✓ Договорете еден внатрешен канал за брза координација и правило: одлуките одат преку водителот. ✓ Подгответе список со клучни контакти (внатрешни, ИТ/админ, правна поддршка, ЗНМ).
B. Пристапи и безбедност на сметки	✓ Активирајте 2FA (двофакторска автентикација) за клучни профили и службени е-пошти; резервните кодови чувајте ги безбедно и со ограничен пристап. ✓ Редовно проверувајте администраторски улоги и отстранувајте „заборавени“ пристапи. ✓ Користете силни и уникатни лозинки (менаџер за лозинки, каде што е возможно). ✓ Избегнувајте најавување на службени профили од јавни мрежи и од несигурни уреди, особено во периоди на ризик
C. Рана детекција и модерација	✓ Договорете кој ги следи нотификациите од платформите и кој реагира на предупредувања за сомнителна активност/ограничувања. ✓ Следете „аларм“ сигнали: нагли скокови во коментари/следења, синхронизирани фрази, повторливи профили, префрлање на нападот на други платформи. ✓ Имајте кратки правила за модерација (што се брише веднаш, што се документира и пријавува, што се остава како легитимна критика). ✓ Не бришете масовно без претходно да обезбедите докази (скриншотови, линкови, временска линија).
D. Психолошка и тимска поддршка	✓ Воведете краток „check-in“ со таргетираната личност во првите 24-48 часа. ✓ Размислете за привремено прераспределување задачи ако притисокот е силен или има закани/доксинг. ✓ Кога е достапно, поттикнете стручна поддршка (особено при повторливи напади).
E. Вежбање и ажурирање	✓ Направете кратка симулација 30-45 минути (масовно пријавување или имперсонација) 1-2 пати годишно. ✓ По секој инцидент, запишете „што научивме“ и ажурирајте ги контактите, пристапите и шаблоните.

КЛУЧНИ ИЗВОРИ

Платформски политики и алатки (пријавување, жалби, враќање профил)

Meta. „Making it Easier to Access Account Support on Facebook and Instagram“. Meta, 04.12.2025. Пристапено на 20.01.2026. https://about.fb.com/news/2025/12/making-it-easier-to-access-account-support-on-facebook-and-instagram/

Meta. „Account Recovery Hub - Facebook, Instagram, Threads“. Meta, без датум. Пристапено на 20.01.2026. https://www.meta.com/account-recovery-support/

Meta. „Inauthentic Behavior (Community Standards)“. Meta Transparency Center, без датум. Пристапено на 20.1.2026. https://transparency.meta.com/policies/community-standards/inauthentic-behavior/

Instagram. „Hacked Instagram Account“. Instagram Help Center, без датум. Пристапено на 20.1.2026. https://help.instagram.com/368191326593075/

Instagram. „Report an Impersonation Account on Instagram or Threads“. Instagram Help Center, без датум. Пристапено на 20.01.2026. https://help.instagram.com/contact/636276399721841

X. „X’s Private Information Policy and Doxxing“. X Help Center, без датум. Пристапено на 20.1.2026. https://help.x.com/en/rules-and-policies/personal-information

X. „How to Report Abusive Behavior on X“. X Help Center, без датум. Пристапено на 20.1.2026. https://help.x.com/en/safety-and-security/report-abusive-behavior

YouTube. „Harassment & Cyberbullying Policies“. YouTube Help, без датум. Пристапено на 20.1.2026. https://support.google.com/youtube/answer/2802268

YouTube. „Report Inappropriate Videos, Channels & Other Content on YouTube“. YouTube Help, без датум. Пристапено на 20.01.2026. https://support.google.com/youtube/answer/2802027

TikTok. „My Account Has Been Hacked“. TikTok Support, без датум. Пристапено на 20.01.2026. https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked

Практични ресурси за дигитална безбедност и одговор на инциденти

Access Now. „Digital Security Helpline“. Access Now, без датум. Пристапено на 20.1.2026. https://www.accessnow.org/help/

Committee to Protect Journalists (CPJ). „Digital Safety: DIY Guides for Better Protecting Against Online Harassment“. CPJ, 04.09.2019. Пристапено на 20.01.2026. https://cpj.org/2019/09/digital-safety-diy-guides/

Committee to Protect Journalists (CPJ). „Digital Safety: Remove Personal Data from the Internet“. CPJ, 04.09.2019. Пристапено на 20.01.2026. https://cpj.org/2019/09/digital-safety-remove-personal-data-internet/

Committee to Protect Journalists (CPJ). „Editors’ Checklist: Protecting Staff and Freelancers Against Online Abuse“. CPJ, 07.07.2022. Пристапено на 20.01.2026. https://cpj.org/2022/07/editors-checklist-protecting-staff-and-freelancers-against-online-abuse/

Coalition Against Online Violence. „Online Violence Response Hub“. Без датум. Пристапено на 20.1.2026. https://onlineviolenceresponsehub.org/

Европски и меѓународни стандарди релевантни за практична заштита

Европска Унија. „Регулатива (ЕУ) 2022/2065 на Европскиот парламент и на Советот од 19.10.2022 за единствен пазар на дигитални услуги (Digital Services Act)“. EUR-Lex, 19.10.2022. Пристапено на 20.1.2026. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Европска комисија. „Recommendation (EU) 2021/… - on the Protection, Safety and Empowerment of Journalists (C(2021) 6650 final)“. EUR-Lex, 16.09.2021. Пристапено на 20.1.2026. https://eur-lex.europa.eu/eli/reco/2021/1534/oj

Council of Europe. „Recommendation CM/Rec(2016)4 on the Protection of Journalism and Safety of Journalists and Other Media Actors“. Council of Europe, 13.04.2016. Пристапено на 20.1.2026. https://rm.coe.int/16806415d9

Council of Europe. „Freedom of Expression and Journalist Safety - A Pocket Guide for Users“. Council of Europe, 09.2023. Пристапено на 20.1.2026. https://rm.coe.int/pocketguide2023-final/1680ac9318

ОБСЕ - Претставник за слобода на медиумите. „Guidelines for Monitoring Online Violence Against Female Journalists“. OSCE, комисионирано 2022 (PDF). Пристапено на 20.1.2026. https://www.osce.org/files/f/documents/b/0/554098_1.pdf.

www.znm.org.mk