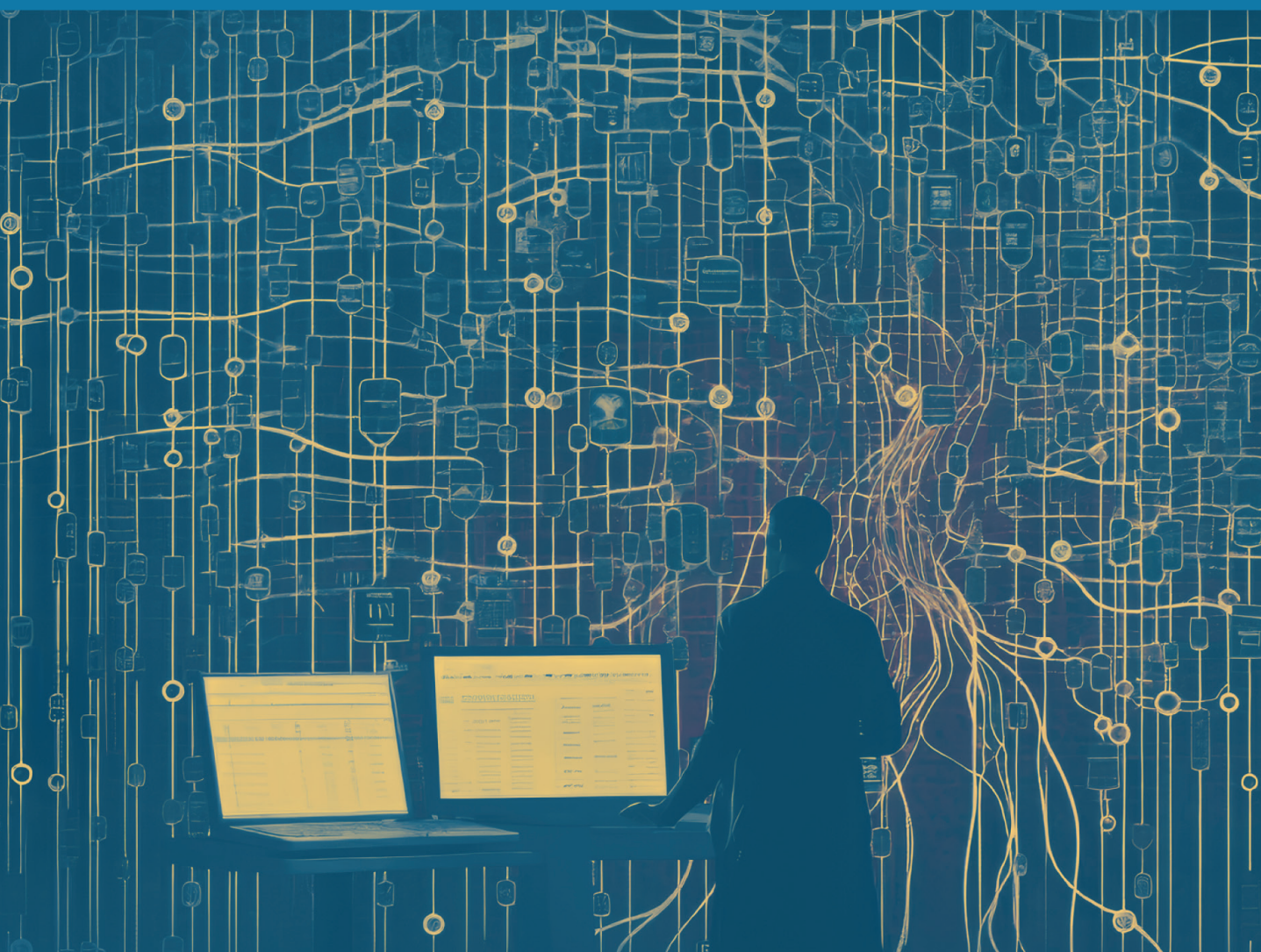
safejournalists.net

Shoqata e Gazetarëve të Maqedonisë

DOKUMENT PËR POLITIKA PUBLIKE

SULME TË KOORDINUARA DIGJITALE NDAJ GAZETARËVE DHE MEDIAVE - PROTOKOLL PRAKTIK PËR REAGIM, RUAJTJE TË PROVAVE DHE VEPRIM

SHKUP, SHKURT 2026



Impresumi
Dokument për politika publike: Sulme të koordinuara digjitale ndaj gazetarëve dhe mediave - protokoll praktik për reagim, ruajtje të provave dhe veprim

Autor
Martin Petrovski

Redaksia
Dragan Sekullovski

Botues
Shoqata e Gazetarëve të Maqedonisë (SHGM)

Projekti
„SafeJournalists Network“

Lektorimi në maqedonisht
Maja Katarova

Përkthim nga maqedonishtja në gjuhën angleze
Olivera Celeska

Përkthim nga maqedonishtja në gjuhën shqipe
Ferikan Iljazi

Dizajni
SHGM

Distancim nga përgjegjegjësia
Ky publikim është përgatitur me mbështetjen financiare të Bashkimit Evropian. Përmbajtja e tij është përgjegjësi vetëm e autorit dhe nuk pasqyron domosdoshmërisht qëndrimet e Bashkimit Evropian.

Shkup, shkurt 2026.

SHËNIM

Ky publikim është i destinuar si udhëzues praktik për redaksitë dhe gazetarët për menaxhimin e sulmeve të koordinuara digjitale, me fokus në sigurinë, ruajtjen e provave dhe përshkallëzimin efektiv. Ai nuk përbën këshillë juridike. Në raste me rrezik të lartë, veçanërisht kur ka kërcënime, doxing ose dyshim për qasje të paautorizuar, rekomandohet konsultim me përfaqësues ligjor dhe raportim në institucionet kompetente.

PËRMBAJTJA

LISTA E AKRONIMEVE

- *2FA* - autentikim me dy faktorë (Two-Factor Authentication)
- *CPJ* - Committee to Protect Journalists (Komiteti për Mbrojtjen e Gazetarëve)
- *BE* - Bashkimi Evropian
- *EUR-Lex* - baza zyrtare e së drejtës së BE-së (portal për legjislacionin dhe aktet e BE-së)
- *FB* - Facebook
- *FIMI* - Foreign Information Manipulation and Interference (ndërhyrje dhe manipulim i huaj i informacionit)
- *IG* - Instagram
- *OSCE* - Organizata për Siguri dhe Bashkëpunim në Evropë (Organization for Security and Co-operation in Europe)
- *SOP* - Standard Operating Procedure (procedurë standarde operative)
- *X* - X (ish - Twitter)

HYRJE

Sulmet e koordinuara digjitale ndaj gazetarëve dhe mediave zakonisht duken si një "valë e shpejtë" ngacmimesh – raportime masive të rreme për të rrëzuar profile, fyerje dhe kërcënime të organizuara, impersonim, kompromet profilesh ose publikim të të dhënave personale me qëllim frikësimi. Këto sulme rrallë janë të rastësishme. Ato janë të dizajnuara për të krijuar panik, për të ndërprerë punën dhe për të cenuar besimin ndaj redaksisë. Në një pjesë të rasteve, sulme të tilla mund të lidhen edhe me operacione më të gjera të ndërhyrjes dhe manipulimit të huaj të informacionit (FIMI - nga anglishtja *Foreign Information Manipulation and Interference*), por udhëzimet më poshtë janë praktike dhe të zbatueshme pavarësisht prejardhjes së sulmit.

Ky dokument ofron hapa praktikë që redaksitë mund t'i zbatojnë menjëherë – si të identifikojnë se bëhet fjalë për një sulm të koordinuar, çfarë të bëjnë në 60 minutat e para dhe në 72 orët e para, si të mbledhin dhe ruajnë prova pa cenuar privatësinë, si të veprojnë ndaj platformave, si të kërkojnë mbështetje nga SHGM dhe kur ka bazë t'u drejtohen institucioneve kompetente.

Qëllimi është që reagimi të jetë i qetë, konsistent dhe i sigurt. Parimi kyç është "do no harm" – të mbrohen njerëzit, të minimizohet përpunimi i të dhënave personale dhe të mos ndërmerren hapa që në mënyrë të panevojshme rrisin dukshmërinë e sulmit ose ekspozojnë ekipin ndaj rreziqeve shtesë.

Kujt i dedikohet ky dokument

Ky dokument është i destinuar për redaktorë, gazetarë, administratorë të profileve në rrjete sociale, menaxhment të redaksive dhe persona përgjegjës për sigurinë dhe çështjet juridike në media.

Metodologjia

Dokumenti është përgatitur mbi bazën e rasteve praktike dhe përvojave nga puna e SHGM me gazetarë dhe redaksi gjatë trajtimit të incidenteve digjitale, si dhe mbi udhëzime relevante për siguri digjitale, ruajtje të provave dhe rregulla zyrtare të platformave për raportim dhe rikthim të qasje.

Si ta përdorni këtë dokument

- Nëse sulmi është në zhvillim, fillimisht përdorni faqen “Reagimi i shpejtë” dhe menjëherë filloni mbajtjen e “incident log“[1].
- Më pas ndiqni procedurën standarde operative (SOP) sipas fazave (60 minutat e para, 24 orët e para, 48 - 72 orë).
- Mblidhni provat në mënyrë sistematike dhe përdorni shabllonin për “paketën e provave” për platforma dhe institucione.
- Nëse ka kërcënime ose “doxing” (doksing)[2], zbatoni protokollin për siguri urgjente dhe veproni pa vonesë.
- Kur është e nevojshme, kontaktoni SHGM për mbështetje, orientim dhe koordinim të hapave të mëtejshëm.

Mesazhe kyçe

- ✓ Një sulm i koordinuar trajtohet si incident – me role, afat kohor dhe vendime të qarta, e jo si “kaos komentesh”.
- ✓ Provat mblidhen menjëherë, por me kujdes – me minimum të dhënash personale dhe me kontroll të qasjes.
- ✓ Veprimi bëhet me hapa – platforma, SHGM, institucione – sipas rrezikut dhe dëmit.
- ✓ Siguria e njerëzve ka përparësi – veçanërisht kur ka kërcënime, “doxing” (doksing) ose profile të kompromentuara.

1 “Incident log” – evidencë e shkurtër kohore e ngjarjeve dhe hapave të ndërmarrë.

2 “Doxing” (doksing) – shpërndarje publike e të dhënave personale pa pëlqim, me qëllim frikësimi, ngacmimi ose nxitjeje dëmi.

ÇFARË ËSHTË NJË SULM I KOORDINUAR DIGJITAL

Një sulm i koordinuar digjital është një aktivitet i qëllimshëm dhe i organizuar i drejtuar ndaj një gazetari, redaktori ose mediumi, me synim të shkaktojë ndërprerje të punës, autocensurë, diskreditim ose frikësim fizik. Sulmi mund të duket si një valë “spontane”, por në praktikë shpesh ka modele të përsëritura, sinkronizim dhe një qëllim të qartë.

Sulmet e koordinuara dallojnë nga kritika “e zakonshme” online sepse synojnë kontrollimin e dukshmërisë dhe qasjes ndaj publikut. Kjo do të thotë se qëllimi nuk është vetëm të lihet një koment, por të rrëzohet një profil, të bllokohen kanalet e komunikimit, të imponohet një kornizë e rreme narrative ose të rrezikohet siguria personale.

Pse kjo është e rëndësishme për redaksitë

Kur sulmi është i koordinuar, reagimi merr strukturë. Improvizimi më së shpeshti çon në tri probleme: humbje të provave, veprim të gabuar ndaj platformave dhe rritje të rrezikut përmes amplifikimit të panevojshëm publik të sulmit. Prandaj dokumenti e trajton sulmin e koordinuar si incident me role të përcaktuara, “incident log” dhe vendime të qarta.

PJESA A - SI TA IDENTIFIKONI PROBLEMIN

Si të dalloni se bëhet fjalë për një sulm të koordinuar

Nuk ka një shenjë të vetme "të sigurt", por kombinimi i disa sinjaleve është një indikator i fortë se sulmi është i organizuar dhe se protokolli duhet të aktivizohet.

- Shfaqet rritje e menjëhershme e komenteve, mesazheve ose reagimeve në një periudhë të shkurtër, me ton të përsëritur dhe formulime identike.
- Disa profile në të njëjtën kohë publikojnë akuza, linqe ose materiale vizuale të njëjta ose shumë të ngjashme.
- Aktivizohet raportim masiv i rremë i profileve, postimeve ose faqeve me qëllim kufizimi ose pezullimi.
- Shfaqen profile të reja me histori minimale, të cilat në mënyrë të koordinuar sulmojnë ose "i përgjigjen" njëra-tjetrës për të krijuar përshtypjen e shumicës.
- Sulmi zhvendoset nga një platformë në tjetrën, me të njëjtin mesazh ose të njëjtin targetim.
- Shfaqen tentativa për impersonim, hakim ose marrje të qasjes administrative.
- Publikohen ose kërcënohet se do të publikohen të dhëna personale, fotografi private, adresa, numra telefoni ose informacione për familjen.
- Përdoret "fshirje konteksti" përmes citateve të shkëputura, screenshot-eve pa burim ose titujve të rremë që më pas "qarkullohen" si provë.

Terma kyç

Raportim masiv i rremë është praktikë e koordinuar ku disa profile raportojnë përmbajtje ose një profil me qëllim që platforma automatikisht të kufizojë arritjen, të heqë përmbajtjen ose të pezullojë profilin.

Impersonim është krijimi ose përdorimi i një profili që paraqitet si gazetar, medium ose anëtar i redaksisë, me qëllim manipulimi, mashtrimi, diskreditimi ose mbledhjeje të të dhënave personale.

Profil i komprometuar nënkupton që një sulmues ka marrë qasje të paautorizuar në një profil ose në mjetet e menaxhimit, si për shembull të drejta administratori, e-mail të lidhur me profilin ose panele

Doksing (doxing) është publikimi publik ose kërcënimi për publikim i të dhënave personale, me qëllim frikësimi, nxitjeje të ngacmimit ose krijimi të rrezikut për sigurinë fizike.

Ngacmim i koordinuar është targetim i organizuar përmes fyerjeve, kërcënimeve, komenteve të seksualizuara, fotografive të manipuluara ose mesazheve të vazhdueshme, me qëllim lodhjeje dhe frikësimi.

Skenarët më të shpeshtë të sulmeve ndaj gazetarëve dhe mediave

Në praktikën redaksionale, është e dobishme që sulmet të grupohen sipas asaj që përpiqen të "rrëzojnë": dukshmërinë, kredibilitetin, identitetin, qasjen ose sigurinë.

Sulme ndaj dukshmërisë	ndodhin kur synimi është të kufizohet arritja, të hiqet përmbajtja ose të pezullohet profili përmes raportimit masiv të rremë dhe abuzimit me mekanizmat e platformave.
Sulme ndaj kredibilitetit	ndodhin kur synimi është diskreditimi përmes pretendimeve të rreme, deklaratave të manipuluara, "provave me screenshot" pa burim ose spinimit të koordinuar të një teme.
Sulme ndaj identitetit	ndodhin kur ka impersonim, profile të rreme "në emër të redaksisë" ose përpjekje për të mashtruar burimet dhe publikun.
Sulme ndaj qasjes	ndodhin kur ka phishing, marrje profilesh, kompromet im të e-mailit ose përpjekje për të siguruar të drejta administrative.
Sulme ndaj sigurisë	ndodhin kur ka kërcënime, doksing, targetim të familjes ose thirrje për përballje fizike, dhe ato gjithmonë kërkojnë prioritetin më të lartë.

PJESA B - SI TË VEPRONI PASI TA KENI IDENTIFIKUAR SULMIN

Nëse identifikoni më shumë se një nga sinjalet e përmendura, kaloni në hapat praktikë më poshtë dhe më pas ndiqni “Reagimin e shpejtë” dhe SOP sipas fazave.

Rregulli bazë për vendimmarrje

Nëse sulmi ndikon në qasjen ndaj profileve, përfshin kërcënime ose doksing, apo krijon rrezik për sigurinë fizike, reagimi trajtohet si incident me rrezik të lartë.
Nëse sulmi është “vetëm” një valë komentesh, por është i koordinuar dhe ndikon në dukshmëri ose besim, protokolli megjithatë aktivizohet, me fokus në mbledhjen e provave, komunikim të kontrolluar dhe veprim të duhur ndaj platformave dhe kanaleve të tjera relevante.

Rolet dhe koordinimi në redaksi

Kur sulmi është i koordinuar, redaksia vepron si ekip me role të qarta. Qëllimi është të reduktohet kaosi, të mos humben provat dhe të merren vendime që ulin rrezikun.

Është më mirë që rolet të caktohen paraprakisht dhe secili rol të ketë zëvendësues. Kur kjo nuk është e mundur, rolet caktohen menjëherë sapo të konstatohet se sulmi është në zhvillim.

- **Koordinatori i incidentit** udhëheq reagimin, vendos prioritetet dhe miraton komunikimin publik.
- **Administratori i platformave** verifikon qasjen, forcon cilësimet e sigurisë, hap raportime dhe ankesa dhe ndjek statusin e tyre.
- **Përgjegjësi për prova dhe “log”** mbledh provat, i emërton dhe arkivon, mban “incident log” dhe përgatit paketën e provave.
- **Përgjegjësi për komunikim** përgatit mesazhe të shkurtra dhe të kontrolluara për publikun dhe partnerët, pa e “amplifikuar” sulmin.
- **Përgjegjësi për siguri dhe hapa juridikë** bën vlerësim të rrezikut nga kërcënimet dhe doksingu, propozon masa mbrojtëse dhe koordinon kontaktin me institucionet kur ka bazë.

Redaksia zbaton një rregull të qartë: vendimet kalojnë përmes koordinatorit, ndërsa secili tjetër i përmbahet planit të dakorduar. Kjo parandalon veprime paralele që krijojnë raportime kontradiktore, humbje provash ose ekspozim shtesë.

“Incident log”

“Incident log” është një regjistrim i thjeshtë që mundëson të ndiqet çfarë ka ndodhur, kur dhe si ka reaguar redaksia. “Log”-u është i dobishëm për veprim ndaj platformave, për institucione dhe për analizë të brendshme pas përfundimit të sulmit.

“Incident log”-u mbahet që nga momenti i parë dhe përditësohet në kohë reale ose çdo 30 - 60 minuta në orët e para. “Log”-u ruhet me qasje të kufizuar dhe ndahet vetëm me personat që kanë rol në incident.

Fushat e mëposhtme janë të mjaftueshme për përdorim praktik:

- Regjistrimi përfshin datën dhe kohën e saktë të ngjarjes ose aktivitetit.
- Regjistrimi tregon se ku ka ndodhur ngjarja, përfshirë platformën, profilin dhe linkun.
- Regjistrimi përshkruan çfarë është vërejtur, për shembull raportim masiv i rremë, kërcënime, impersonim ose qasje e kompromet uar.
- Regjistrimi shënon çfarë veprimi është ndërmarrë dhe nga kush.
- Regjistrimi përmban referencë ndaj provës, për shembull numër dosjeje, emër skedari ose link drejt materialit të arkivuar.
- Regjistrimi ka status, për shembull “në vazhdim”, “i raportuar”, “në procedurë ankese” ose “i mbyllur”.

Reagimi i shpejtë - 60 minutat e para

Ky seksion është i destinuar për situata kur sulmi është në zhvillim dhe redaksia duhet menjëherë të stabilizojë gjendjen. Nëse ka kërcënime të drejtpërdrejta ose doksing, siguria e njerëzve ka prioritet absolut.

1. Aktivizoni procedurën

Menjëherë caktoni një koordinator të incidentit dhe minimumi edhe dy role të tjera, edhe nëse i njëjti person përkohësisht mbulon më shumë detyra. Hapni një kanal të brendshëm për koordinim dhe vendosni rregull që vendimet të kalojnë përmes koordinatorit të incidentit.

2. Bëni një vlerësim të shpejtë të rrezikut

Kontrolloni nëse ka kërcënime për dhunë, doksing, publikim adresash, numrash telefoni ose targetim të familjes. Nëse kjo ekziston, kaloni menjëherë në protokollin për siguri urgjente dhe veproni pa vonesë.

3. Ruani provat para çdo ndryshimi

Para se të fshini, bllokoni ose ndryshoni cilësimet, fillimisht ruani materialin provues. Në 60 minutat e para, më e rëndësishmja është të kapet "pamja" e sulmit ndërsa është aktiv.

Paketa minimale e provave në këtë fazë përfshin:

- Çdo screenshot paraqet ekranin e plotë me datë dhe orë, emër përdoruesi dhe kontekstin e postimit ose profilit.
- Çdo regjistrim video i ekranit tregon si hapet linku dhe si arrihet te përmbajtja e kontestuar, për të ruajtur kontekstin.
- Çdo regjistrim përfshin linkun direkt të përmbajtjes ose profilit, dhe kur është e mundur edhe identifikuesin e postimit ose profilit.
- Çdo profil i dyshimtë që është pjesë e sulmit evidentohet me link dhe një shënim të shkurtër për rolin e tij në sulm.
- Çdo njoftim ose e-mail nga platforma ruhet si provë, përfshirë subjektin, datën dhe përmbajtjen.

4. Stabilizoni profilet dhe qasjen

Administratori i platformave kontrollon nëse ka shenja të qasjes së kompromentuar dhe zbaton masat bazë të mbrojtjes.

- Fjalëkalimet ndryshohen nga një pajisje e sigurt dhe përdoren fjalëkalime unike dhe të forta.
- Autentikimi me dy faktorë (2FA) aktivizohet ose verifikohet që është aktiv për të gjitha profilet dhe e-mail-et kyçe.
- Seancat aktive rishikohen dhe hyrjet e panjohura çkyçen.
- Rolet e administratorëve verifikohen dhe qasjet e panevojshme hiqen gjatë kohëzgjatjes së incidentit.

5. Kufizoni dëmin pa e përshkallëzuar sulmin

Përgjegjësi për komunikim shmang reagimet impulsive publike. Nëse nevojitet një mesazh publik, ai është i shkurtër, faktik dhe i orientuar drejt mbrojtjes së publikut dhe ekipit.

Në 60 minutat e para, prioritet kanë masat që ulin ekspozimin, pa krijuar konflikt shtesë. Moderimi bëhet me kujdes dhe vetëm pasi të jenë ruajtur provat, për të mos humbur gjurmën provuese.

6. Hapni raportim dhe ndiqni procedurën

Administratori i platformave fillon raportimin sipas llojit të sulmit, për shembull impersonim, profil i kompromet uar, doksing ose ngacmim. Përgjegjësi për prova siguron një paketë të rregullt që përdoret në raportime dhe lidhet me “incident log”-un.

7. Kërkoni mbështetje nga SHGM kur ka bazë

Kur sulmi është i koordinuar, kur ka rrezik për sigurinë ose kur reagimi i platformës është joefektiv, redaksia mund të kontaktojë SHGM për orientim dhe koordinim të hapave të mëtejshëm. Kontaktet dhe formati i njoftimit të shkurtër janë dhënë në anekse.

Parimi “do no harm”

- ✓ Të dhënat personale të sulmuesve ose të palëve të treta nuk publikohen, edhe kur ata vetë kanë publikuar më parë të dhëna personale.
- ✓ Kërcënimet nuk përcillen dhe nuk publikohen pa u hequr paraprakisht të dhënat personale që mund të rrisin ekspozimin e personave të targetuar.
- ✓ Mesazhet publike nuk zbulojnë masa të brendshme mbrojtëse dhe detaje operative (për shembull cilësime dhe dobësi) që mund t’i ndihmojnë sulmuesit të përshtaten.

Procedurë standarde operative (SOP) - reagim sipas fazave

Ky protokoll e organizon reagimin në tri faza kohore. Qëllimi është që redaksia të mbetet funksionale, të mbrojë personat e targetuar, të ruajë provat dhe të veprojë sipas një rendi të duhur përmes kanaleve relevante.

Faza 1 - 24 orët e para

Në 24 orët e para prioritet është stabilizimi i qasjes, ruajtja e provave dhe veprimi i shpejtë përmes kanaleve të duhura.

1. Konfirmoni llojin e incidentit dhe vendosni prioritet

Koordinatori i incidentit përcakton nëse sulmi është i drejtuar ndaj dukshmërisë, identitetit, qasjes apo sigurisë. Nëse ka doksing, kërcënime ose qasje të kompromet uar, incidenti trajtohet si me rrezik të lartë.

2. Thelloni mbledhjen e provave

Pas paketës fillestare të provave, përgjegjësi për prova e zgjeron materialin në mënyrë që të mund të përdoret si për veprim ndaj platformave, ashtu edhe për procedim para institucioneve. Çdo provë merr kontekst, shenjë kohore dhe lidhje të qartë me “incident log”-un.

- Provat organizohen në një dosje të strukturuar me nën-dosje të qarta sipas platformave dhe sipas llojit të sulmit.
- Çdo skedar emërtohet duke përfshirë datën, orën, platformën dhe një përshkrim të shkurtër të përmbajtjes.
- Gjatë arkivimit, të dhënat personale të personave të targetuar dhe palëve të treta minimizohen, ndërsa qasja në dosje kufizohet.

3. Aktivizoni procedurat në platforma - raportim, ankesa dhe rikthim qasjeje

Administratori i platformave nis procedurat sipas llojit të sulmit. Çdo paraqitje mbështetet me paketë provash, ndërsa në “incident log” shënohet numri i raportimit ose statusi.

Kur ekziston rrezik për humbje profili ose qasje të kompromet uar, prioritet është rikthimi i kontrollit mbi qasjen, e më pas komunikimi publik.

4. Menaxhoni moderimin dhe komentet pa humbur provat

Moderimi ndjek një rregull: fillimisht prova, pastaj ndërhyrja. Pasi të ruhen provat, redaksia mund të ndërmarrë masa të kufizuara për të ulur dëmin, duke vlerësuar nëse masa mund ta nxisë më tej sulmin.

- *Komentet* dhe mesazhet moderohen sipas një logjike të qartë që dallon kritikën nga ngacmimi dhe kërcënimet.
- Çdo element që përmban kërcënim ose të dhëna personale dokumentohet dhe trajtohet me prioritet më të lartë.
- Fshirja masive shmanget kur ajo shkatërron gjurmën provuese dhe e vështirëson procedimin.

5. Komunikim i kontrolluar

Përgjegjësi për komunikim siguron që redaksia të flasë me një zë, me rrezik minimal për përshkallëzim të mëtejshëm të sulmit. Në 24 orët e para, mesazhi publik është i shkurtër dhe i fokusuar në fakte, jo në debat me sulmuesit.

Kur ka kërcënime ose doksing, komunikimi publik është i kujdesshëm dhe nuk zbulon detaje personale, lokacione, orare ose masa të brendshme mbrojtëse. Në këto raste, komunikimi me institucionet dhe rrjetet mbështetëse merr prioritet.

6. Mbështetje nga SHGM dhe veprim para institucioneve kur ka bazë

Kur sulmi është i koordinuar dhe shkakton dëm të konsiderueshëm, redaksia mund të kontaktojë SHGM me një përmbledhje të shkurtër, “incident log” dhe provat kyçe. Kjo mundëson koordinim më efikas dhe orientim për hapat e mëtejshëm.

Nëse ka kërcënime, doksing, kompromet im profilesh ose keqpërdorim të të dhënave personale, redaksia mund të ndërmarrë veprime para institucioneve kompetente, me një paketë të qartë provash dhe me minimizim të të dhënave personale të panevojshme.

Faza 2 - 48 - 72 orë

Në 48 - 72 orë prioritet është të konsolidohen provat, të ndiqen përgjigjet nga platformat, të ulet ekspozimi dhe të stabilizohet puna e redaksisë.

1. Ndiqni përgjigjet nga platformat dhe mbani status sipas rastit

Administratori i platformave mban një listë me të gjitha raportimet dhe ankesat, me datë, status dhe hapat e radhës. Nëse platforma reagon me sanksione automatike ndaj profilit ose përmbajtjes, redaksia paraqet ankesë me argumentim të qartë dhe paketë të rregullt provash.

2. Konsolidoni "paketën e provave" për institucione dhe partnerë

Përgjegjësi për prova përgatit një paketë të konsoliduar që përmban vijën kohore, provat kyçe, një shpjegim të shkurtër të dëmit dhe kërkesa të qarta. Paketa bëhet e lexueshme dhe e përdorshme pa interpretime shtesë.

3. Ulni ekspozimin dhe mbroni ekipin

Redaksia vlerëson ekspozimin e individëve, veçanërisht gazetarëve që janë drejtpërdrejt të targetuar. Nëse ka rreziqe, shqyrtohen masa si kufizimi i dukshmërisë publike të profileve personale, forcimi i privatësisë dhe mbështetje shtesë për sigurinë psikologjike dhe fizike.

4. Vendosni për vazhdimin e publikimit dhe linjën editoriale

Koordinatori i incidentit, së bashku me ekipin editorial, vendos nëse redaksia vazhdon publikimin e temës që ka nxitur sulmin dhe si ta bëjë këtë pa rritur në mënyrë të panevojshme rrezikun. Vendimi bazohet në vlerësimin e rrezikut dhe në mbështetjen reale që ka redaksia.

5. Përgatitni një analizë të shkurtër "çfarë mësuam" dhe përditësoni masat

Pas qetësimit të valës më të fortë, redaksia bën një analizë të shkurtër të brendshme me tri pyetje: çfarë funksionoi, çfarë nuk funksionoi dhe çfarë duhet të ndryshohet në role, mjete dhe procedura. Kjo analizë është e shkurtër, por çon në përmirësime konkrete.

Matrica “sinjal - reagim - hapat e radhës”

Kjo matricë shërben për orientim të shpejtë dhe mund të përshtatet sipas rastit konkret dhe platformës (për shembull Meta - Instagram/Facebook/Threads, X, YouTube, TikTok).

Sinjal	Reagim (menjëherë)	Hapat e radhës (nëse vazhdon / nëse është serioz)
Raportim masiv i rremë + rënie e arritjes(reach) / kufizim	Ruaj prova (screenshot/ video) + paraqit raportim/ ankesë në platformë	Kontakto SHGM nëse profili është seriozisht i rrezikuar ose ka sanksione të përsëritura
Impersonim (profil i rremë “si media/gazetar”)	Dokumento profilin e rremë + përcakto/publiko cili është kanali zyrtar	Raportim për impersonim në platformë + SHGM nëse ka disa profile / targetim më të gjerë
Profil i komprometuar (hyrje/ndryshime të dyshimta)	Rikthe qasjen + ndrysho fjalëkalimet + 2FA + çkyç seancat e panjohura	Procedurë për rikthim qasjeje në platformë + institucione nëse ka keqpërdorim/kërcënime
Doksing ose kërcënime	Vlerësim urgjent i sigurisë + ruaj prova + ul ekspozimin	Veprim urgjent para institucione-ve + kontakt me SHGM për koordinim
Ngacmim i koordinuar (fyerje/sulm i organizuar)	Ruaj prova + moderim i kuj-desshëm	Raportim i shkeljeve në platformë + SHGM nëse ka dëm të kon-siderueshëm / disa platforma
“Prova” të manipuluara / citate të shkëputura	Arkivo burimin + përgatit korrigjim faktografik	Raportim nëse ka impersonim/ keqpërdorim privatësie + informi

EVIDENTIMI DHE RUAJTJA E PROVAVE

Provat janë thelbësore për dy qëllime: për të siguruar reagim në kohë nga platformat dhe për të krijuar bazë për veprim para institucioneve kompetente kur ka kërcënime, doksing, qasje të kompromentuar ose keqpërdorim të të dhënave personale. Në një sulm të koordinuar, provat shpesh zhduken shpejt – përmbajtjet fshihen, profilet çaktivizohen dhe konteksti humbet. Prandaj mbledhja dhe ruajtja fillon menjëherë dhe bëhet në mënyrë sistematike. Në disa raste, sulme të tilla lidhen me fushata më të gjera manipuluese në hapësirën informative (përfshirë FIMI[3]), ndaj disiplina në menaxhimin e provave është thelbësore edhe për të kuptuar modelin e sulmit.

Parime bazë

- Provat mblidhen para ndërhyrjeve si fshirje, bllokim ose ndryshim cilësimesh, përveç rasteve kur ka rrezik të menjëhershëm për sigurinë.
- Provat ruajnë kontekstin, sepse një screenshot i izoluar pa elementet përreth shpesh nuk është i mjaftueshëm.
- Provat ruhen me qasje të kufizuar dhe me minimum përpunimi të të dhënave personale, në përputhje me parimin “do no harm”.
- Provat lidhen me “incident log”-un, për të siguruar vijë kohore të qartë dhe verifikueshmëri të veprimeve.

Paketa minimale e provave

Paketa minimale e provave është seti që redaksia siguron në orët e para, pavarësisht llojit të sulmit. Ky set zakonisht është i mjaftueshëm për raportime fillestare në platforma dhe për vlerësim të shpejtë të rrezikut.

- Çdo provë përmban datë dhe orë dhe lidhet me një link ose profil konkret.
- Çdo screenshot paraqet ekranin e plotë me emra përdoruesish të dukshëm, kontekst dhe të paktën një pjesë të navigimit.
- Çdo video-regjistrim i ekranit tregon si hapet linku dhe si arrihet te përmbajtja e kontestuar, për të ruajtur kontekstin.

3 Ndërhyrje dhe manipulim i huaj i informacionit.- *Foreign Information Manipulation and Interference*

- Çdo kërcënim dokumentohet me tekst të plotë dhe kontekst përreth, përfshirë shënim nëse kërcënimi përsëritet ose përshkallëzohet.
- Çdo njoftim ose e-mail nga platforma ruhet në formë origjinale, me subjekt, datë dhe përmbajtje.

Paketa e zgjeruar e provave për platforma dhe institucione

Kur sulmi është i koordinuar, paketa minimale zgjerohet në një "paketë provash" që mund të dorëzohet si tërësi. Kjo paketë duhet të jetë e lexueshme dhe të mundësojë veprim të shpejtë, pa nevojë për shpjegime shtesë.

Paketa e provave përfshin:

- Një përmbledhje të shkurtër të incidentit me përshkrim të llojit të sulmit, kohëzgjatjes dhe dëmit.
- Vijë kohore me ngjarjet më të rëndësishme, të lidhura me "incident log"-un.
- Tabelë me linqe, profile dhe postime kyçe, me shënim të shkurtër që tregon ose konfirmon secilin element.
- Prova të përzgjedhura në aneks, të organizuara sipas llojit të sulmit, si raportim masiv i rremë, impersonim, profil i kompromentuar, doksing ose kërcënime.
- Kërkesa të qarta, si rikthim profili, heqje përmbajtjeje, sanksionim të profilit të rremë ose veprim urgjent ndaj kërcënimeve.
- Pikë kontakti në redaksi, me kontakt zyrtar dhe person përgjegjës për ndjekjen e rastit.

Emërtimi, organizimi dhe kontrolli i qasjes

Organizimi sistematik ul rrezikun e humbjes së materialeve dhe mundëson dorëzim dhe përdorim më të shpejtë të provave. Një format i dakorduar është i mjaftueshëm, nëse zbatohet në mënyrë konsistente.

- Dosja kryesore mban datën dhe një emërtim të shkurtër të incidentit.
- Nën-dosjet organizohen sipas platformave dhe sipas llojit të sulmit, për të shmangur përzierjen e materialeve.
- Çdo skedar përmban datë, orë, platformë dhe përshkrim të shkurtër, që të gjendet shpejt pa kërkim të thelluar.
- Qasja në prova kufizohet te personat me rol në incident, ndërsa çdo shpërndarje shënohet në "incident log".

- Provat ruhen me të paktën një kopje rezervë, në një lokacion të sigurt dhe të aksesueshëm edhe për koordinatorin e incidenti

Minimizimi i të dhënave personale

Në sulme të koordinuara shpesh shfaqen të dhëna personale dhe përmbajtje që mund të ekspozojnë më tej personin e targetuar. Redaksia kujdeset që provat të ruhen, duke mos krijuar dëm shtesë.

- Nëse provat ndahen jashtë ekipit të ngushtë të incidentit, përgatiten dy versione – "i brendshëm" dhe "për shpërndarje" – me heqje të të dhënave personale të panevojshme.
- Nëse bëhet mjegullim ose fshehje e të dhënave, ruhet edhe versioni origjinal me qasje të kufizuar, për të mos humbur vlerën provuese.
- Nëse prova përmban adresë, numër telefoni ose të dhëna të ndjeshme, ato nuk përcillen në grupe më të gjera dhe nuk publikohen, edhe kur janë pjesë e sulmit.
- Nëse provat përfshijnë të mitur ose informacione familjare, ato trajtohen si me rrezik të lartë dhe ndahen vetëm kur është e domosdoshme për procedim.

Integriteti i provave dhe konfidencialiteti

Edhe në kontekst praktik, disiplina bazë për integritet dhe konfidencialitet ul mundësinë e kontestimit të autenticitetit.

- Çdo provë ruhet sa më afër "gjendjes origjinale", pa redaktime që ndryshojnë përmbajtjen.
- Çdo provë shoqërohet me shënim se kush e ka siguruar, kur dhe në çfarë mënyre, dhe kjo regjistrohet edhe në "incident log".
- Çdo shpërndarje e paketës së provave evidentohet, me emrin e marrësit dhe qëllimin e shpërndarjes.

PROTOKOLL PËR DOKSING DHE KËRCËNIME[4]

Doksingu dhe kërcënimet trajtohen si situata me rrezik të lartë, sepse mund të kalojnë shpejt nga ngacmim online në rrezik real për sigurinë. Në këto raste, prioritet është mbrojtja e personave të targetuar dhe të afërmve të tyre, e më pas mbrojtja e profileve, përmbajtjes dhe reputacionit.

Ky protokoll aktivizohet kur ekziston të paktën një nga elementet e mëposhtme: publikim i të dhënave personale, kërcënim për dhunë fizike, targetim i shtëpisë/familjes, thirrje për "vizitë", ndjekje, ose kërcënime të përsëritura që përshkallëzohen.

15 minutat e para - stabilizim dhe siguri

Hapi i parë është vlerësimi i shpejtë nëse ekziston rrezik i menjëhershëm. Nëse kërcënimi është konkret, i afërt në kohë ose përmban informacione që tregojnë se sulmuesi e di adresën/rrugën/orarin, veprohet si në një situatë emergjente sigurie.

- ✓ Personi i targetuar njoftohet drejtpërdrejt dhe në mënyrë diskrete, pa e shpërndarë kërcënimin në grupe të gjera.
- ✓ Dakordohet një "status sigurie" i shkurtër – nëse personi është në shtëpi, në lëvizje, vetëm apo me të tjerë, dhe nëse ka ndjesi se po ndiqet.
- ✓ Është e dobishme që personi të mos lëvizë vetëm dhe, kur është e mundur, të ndryshojë rrugën, vendin ose kohën e lëvizjes për të ulur parashikueshmërinë.
- ✓ Caktohet një person kontakti nga redaksia që mbetet i disponueshëm për koordinim derisa situata të qetësohet.
- ✓ Fillon mbledhja e provave, por pa shpërndarë të dhëna personale te persona që nuk janë pjesë e incidentit.

60 minutat e para - kufizim i ekspozimit

Qëllimi në orën e parë është të ulet dukshmëria e të dhënave të ndjeshme dhe të parandalohet dëm shtesë.

4 Fillon mbledhja e provave, por pa shpërndarë të dhëna personale te persona që nuk janë pjesë e incidentit https://www.coe.int/en/web/freedom-expression/-/improvement-of-national-legislation-on-doxing-and-source-protection

- ✓ Verifikohet nëse të dhënat personale shfaqen në më shumë vende dhe platforma, pastaj përgatitet listë me linqe dhe screenshot-e me kontekst.
- ✓ Raportohet përmbajtja që përmban të dhëna personale dhe/ose kërcënime përmes mekanizmave të privatësisë dhe ngacmimit në platformë, duke theksuar qartë se përmbajtja përmban të dhëna personale dhe paraqet rrezik.
- ✓ Rishikohen informacionet publike në profilet e personit të targetuar dhe të redaksisë, dhe detajet e panevojshme hiqen ose kufizohen.
- ✓ Njoftohen persona të afërt vetëm në masën që rrit sigurinë, jo në mënyrë që krijon panik ose shpërndarje të mëtejshme të të dhënave.

Kur kërcënimi duket serioz

Kërcënimi konsiderohet më serioz kur është konkret, i përsëritur, përmban detaje personale, bën thirrje për veprim të menjëhershëm ose vjen nga disa profile në koordinim. Në këto raste, ekziston bazë për kërkim të mbrojtjes institucionale urgjente dhe për procedim me paketë të plotë provash.

- Nëse ka rrezik të menjëhershëm, kontaktohen shërbimet emergjente kompetente.
- Nëse ka kërcënim, doksing ose ndjekje, përgatitet kallëzim pranë institucioneve kompetente me vijë kohore të qartë dhe material provues.
- Nëse është e nevojshme, shqyrtohen masa shtesë për mbrojtje fizike, si shoqërim, ndryshim i përkohshëm i rutinës ose shmangie e përkohshme e paraqitjeve publike.

Prova për doksing dhe kërcënime - çfarë është më e rëndësishme të dokumentohet

Në rastet e kërcënimeve dhe doksingut, provat duhet të tregojnë saktësisht çfarë është thënë ose publikuar, kush e ka publikuar, ku dhe kur, dhe nëse ka përshkallëzim të intensitetit.

- Çdo provë paraqet kontekstin e plotë, përfshirë emrin e përdoruesit, datën/orën dhe linkun.
- Ruhen edhe njoftimet ose mesazhet që tregojnë se përmbajtja ka qenë e dukshme ose e shpërndarë.
- Ruhen përsëritjet dhe variacionet e kërcënimit, sepse përshkallëzimi është indikator i rëndësishëm.
- Shënohet nëse kërcënimi lidhet me një publikim, hulumtim ose temë konkrete, për të kuptuar motivin dhe rrugën e përhapjes.

KOORDINIM DHE VEPRIM

Kontakt me SHGM kur ka bazë

Në raste doksingu dhe kërcënimesh, kontaktimi i SHGM mund të ndihmojë për orientim, koordinim dhe mbështetje publike kur kjo është e sigurt dhe e dobishme. Për njoftim mjafton një përmbledhje e shkurtër, linqe drejt provave kyçe dhe një vlerësim nëse ka rrezik të menjëhershëm.

Veprim para institucioneve kompetente

Kur paraqitet kallëzim, institucioneve u ndihmon një strukturë e qartë. Zakonisht mjafton të dorëzohet:

- Përshkrim i shkurtër i ngjarjes dhe pse konsiderohet kërcënim ose doksing.
- Vijë kohore e ngjarjeve kyçe, e lidhur me “incident log”-un.
- Prova të përzgjedhura që tregojnë kërcënimin ose publikimin e të dhënave personale.
- Informacion nëse ka përsëritje, koordinim ose zhvendosje në disa platforma.
- Pikë kontakti për komunikim të mëtejshëm dhe dorëzim të provave shtesë.

Komunikim në kushte doksingu dhe kërcënimesh

Komunikimi publik në situata të tilla kërkon kujdes të shtuar. Ndonjëherë heshtja dhe komunikimi i kufizuar japin rezultat më të mirë se një debat publik.

- Mesazhi publik, nëse jepet, mbetet i shkurtër dhe faktik dhe nuk përsërit të dhëna personale ose detaje nga kërcënimi.
- Nuk publikohen screenshot-e që përmbajnë adresa, numra telefoni ose të dhëna të tjera të ndjeshme, edhe kur qëllimi është “të tregohet çfarë po ndodh”.
- Nuk paralajmërohen hapat e ardhshëm që mund t’u ndihmojnë sulmuesve të përshtaten, si detaje mbi raportimin, masat e sigurisë ose organizimin e brendshëm.

Çfarë duhet shmangur në situata të tilla

Disa reagime duken “logjike” nën stres, por shpesh përkeqësojnë situatën ose rrisin ekspozimin.

- Nuk hyhet në debat të drejtpërdrejtë me profile që bëjnë kërcënime ose publikojnë të dhëna personale.
- Nuk inkurajohet publiku që “ta kërkojë” sulmuesin, sepse kjo mund të shkaktojë abuzime shtesë dhe rreziqe ligjore.
- Nuk shpërndahen provat në grupe të gjera, veçanërisht kur përmbajnë të dhëna të ndjeshme personale.

MËNYRA PËR RAPORTIM, ANKESA DHE RIKTHIM QASJEJE NË PLATFORMA

Platformat zakonisht reagojnë fillimisht përmes sistemeve të automatizuara. Prandaj rezultati varet nga fakti nëse raportimi është paraqitur në kategorinë e saktë, nëse ka kontekst të mjaftueshëm dhe nëse provat janë të qarta.

Në sulme të koordinuara (përfshirë raste me elemente të FIMI – targetim i sinkronizuar dhe imponim i narrativave të rreme), disiplina në fakte dhe prova është veçanërisht e rëndësishme. Ky seksion ofron rrugë praktike për raportim, ankesa dhe rikthim qasjeje. Linqet janë dhënë në fusnota, në mënyrë që teksti të mbetet i lexueshëm dhe i përdorshëm nën presion.

Rregulla të përgjithshme për raportim dhe ankesa

- Gjithmonë fillimisht ruhen provat, pastaj ndërhyhet me raportim, fshirje ose bllokim.
- Raportimi bëhet në kategorinë më të përshtatshme, sepse kategori e gabuar shpesh sjell refuzim automatik.
- Një raportim i vetëm është më efektiv kur është i plotë dhe konsistent, sesa disa raportime me kontekst të pamjaftueshëm.
- Çdo paraqitje regjistrohet në “incident log”, me datë, orë, link dhe status.
- Në raportime nuk përsëriten të dhëna personale të panevojshme, veçanërisht në raste doksingu dhe kërcënimesh; përdoret përshkrim dhe bashkëngjiten prova.

Check-listë - minimumi që duhet të përmbajë raportimi

- Raportimi fillon me një fjali të qartë që emërton shkeljen dhe çfarë kërkohet të ndërmerret.
- Raportimi përmban linkun direkt të përmbajtjes/profilit dhe të paktën një shembull tjetër që tregon kontekstin.
- Raportimi përfshin një kornizë të shkurtër kohore: kur ka filluar, nëse është në zhvillim dhe nëse ka përshkallëzim në shtrirje/intensitet.
- Raportimi shpjegon pse sulmi konsiderohet i koordinuar (profile të përsëritura, sinkronizim, raportim masiv, zhvendosje ndërmjet platformave).
- Raportimi përfundon me kërkesë konkrete: heqje përmbajtjeje, sanksionim të profilit të rremë, rikthim qasjeje ose veprim urgjent ndaj kërcënimit.

Meta - Instagram, Facebook dhe Threads

1. Raportim masiv i rremë dhe kufizim i arritjes(Reach)

Kur ka dyshim se profili po targetohet përmes raportimeve masive të rreme, është praktike të veprohet në dy drejtime: të ruhen njoftimet/sanksionet dhe të paraqitet ankesë përmes mekanizmave të disponueshëm për "review" ose "appeal". Nëse ndodh kufizim, heqje ose pezullim, është e dobishme të ruhet i gjithë njoftimi nga platforma dhe të përfshihet në paketën e provave. Këto raste shpesh kërkojnë këmbëngulje dhe konsistencë në ankesa.

2. Impersonim

Këto raste shpesh kërkojnë këmbëngulje dhe konsistencë në ankesa.Kur ekziston një profil që paraqitet si gazetar ose media, rruga më e shpejtë është raportimi për impersonim dhe dorëzimi i linkut të profilit zyrtar që po imitohe.

3. Doksing dhe privatësi

Kur publikohen të dhëna personale, përdoren kategoritë për privatësi dhe ngacmim, duke theksuar qartë se bëhet fjalë për keqpërdorim të informacioneve personale. Në tekstin e raportimit shmanget përsëritja e adresave, numrave të telefonit dhe detajeve të tjera të ndjeshme. Në vend të kësaj, bashkëngjiten screenshot-e dhe linqe.

4. Profil i kompromet uar dhe rikthim qasjeje

Kur profili është i kompromet uar ose dyshohet për marrje qasjeje, më e rëndësishmja është të ndiqen rrugët zyrtare të rikuperimit dhe të shmangen "këshillat" nga profile të paverifikuara që ofrojnë "ndihmë". Në këto raste, është e dobishme të fillohet nga një pajisje që është përdorur më parë për hyrje, pasi platformat shpesh e përdorin këtë si sinjal besimi.

Lidhje zyrtare - Meta

- Instagram/Threads - raportim për impersonim (formular): https://help.instagram.com/contact/636276399721841.
- Instagram - udhëzime për raportim impersonimi: https://help.instagram.com/370054663112398.
- Instagram/Threads - raportim për shkelje të privatësisë: https://help.instagram.com/contact/512241091300432.

- Instagram - raportim për ngacmim/bullizëm: https://help.instagram.com/547601325292351.
- Meta Account Recovery Hub (Facebook/Instagram/Threads): https://www.meta.com/account-recovery-support/.
- Instagram - mbështetje për "hacked account": https://www.instagram.com/hacked/.
- Facebook - mjet për "hacked account": https://www.facebook.com/hacked.

X

1. Ngacmim dhe abuzim

Raportimi në X zakonisht bëhet përmes opsionit "Report" nga një postim ose profil, duke zgjedhur kategorinë përkatëse dhe duke shtuar kontekst shtesë.

2. Informacione private dhe doksing

Platforma sociale "X" ka politikë të veçantë për informacione private dhe raportim për abuzim. Në raste doksingu, është e dobishme që raportimi të jetë i qartë, me link drejt postimit dhe një shpjegim të shkurtër pse përmbajtja përbën informacion privat dhe si po përdoret për abuzim.

3. Profil i kompromet uar

Për profil të kompromet uar, X ofron formular për rikthim qasjeje. Nëse profili është "locked" ose "limited", është praktike të ndiqen hapat për verifikim dhe rikthim të funksioneve.

Lidhje zyrtare - X

- Raportim për abuzim: https://help.x.com/en/safety-and-security/report-abusive-behavior.
- Politika për informacione personale: https://help.x.com/en/rules-and-policies/personal-information.
- Formular për "hacked or compromised": https://help.x.com/en/forms/account-access/regain-access/hacked-or-compromised.

YouTube

YouTube i trajton në mënyrë eksplicite kërcënimet dhe doksingun si pjesë e sjelljes së ndaluar në kuadër të politikave për ngacmim dhe cyberbullying. Gjatë raportimit, është e dobishme të bashkëngjitet linku konkret, shenja kohore (timestamp) në video dhe një shpjegim i shkurtër se si përmbajtja targeton një person ose medium.

Lidhje zyrtare - YouTube

- Politika për ngacmim dhe cyberbullying: https://support.google.com/youtube/answer/2802268.

TikTok

TikTok ka një menu të centralizuar "Report a problem" dhe hapa konkretë për raportimin e një profili, përmbajtjeje ose abuzimi. Në sulme të koordinuara, është e dobishme të mblidhen disa shembuj dhe të raportohen duke theksuar qartë se ka përsëritje dhe koordinim. Nëse profili është i kompromentuar, TikTok ofron hapa bazë për rikthimin e sigurisë.

Lidhje zyrtare - TikTok

- „Report a problem": https://support.tiktok.com/en/safety-hc/report-a-problem.
- Si të raportohet një profil: https://support.tiktok.com/en/safety-hc/report-a-problem/report-a-user.
- Nëse llogaria është hakuar: https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked.

Kur raportimet nuk japin rezultat

Ndonjëherë platformat nuk reagojnë shpejt ose vendimet janë jokonsistente. Në raste të tilla, është e dobishme që redaksia të bëjë një "rifreskim" të qasjes:

- ✓ Verifikohet nëse kategoria e raportimit është e saktë dhe nëse ka kontekst të mjaftueshëm.
- ✓ Paraqitet ankesë ose raportim i ri vetëm kur ka fakte të reja ose prova shtesë.
- ✓ Konsolidohet paketa e provave në një tërësi të lexueshme, në vend që të dërgohen fragmente të shpërndara.
- ✓ Shqyrtohet kontakti me SHGM kur ka rrezik të lartë, sanksione të përsëritura ose dëm të konsiderueshëm ndaj punës së redaksisë.

Paketë e shpejtë për raportim dhe kërkesë për mbështetje

Kur sulmi është i koordinuar, koha më e madhe humbet në "mbledhjen e historisë" nga shumë mesazhe dhe skedarë. Prandaj është e dobishme të keni një "paketë të shpejtë" standarde që dërgohet si një **mesazh i vetëm**, me strukturë të qartë dhe **disa prova kyçe**. Dokumentimi dhe regjistrimi (datë, link, çfarë ka ndodhur) është i rëndësishëm sepse përmbajtjet dhe profilet shpesh zhduken ose ndryshojnë.

Kur t'i drejtoheni SHGM-së dhe kur drejtpërdrejt institucioneve

Drejtojuni SHGM-së kur ka nevojë të qartë për koordinim dhe mbështetje më të shpejtë, për shembull:

- profili/fqja është kufizuar, hequr ose realisht rrezikon pezullim për shkak të raportimeve masive të rreme
- impersonim i gazetarit/mediumit (veçanërisht nëse mbledh të dhëna personale ose shpërndan dezinformata të dëmshme)
- qasje e kompromentuar ose tentativa serioze për marrje qasjeje (përfshirë phishing të përsëritur ndaj ekipit)
- publikim i të dhënave personale me qëllim ngacmimi, doksing ose kërcënime për dhunë
- dëm i konsiderueshëm operacional (ndërprerje e publikimit, humbje e qasjes te audienca, goditje serioze ndaj besimit)

Veprimi institucional shqyrtohet kur ka:

- rrezik për sigurinë personale
- publikim të të dhënave personale (doksing), veçanërisht adresë/telefon/të dhëna familjare
- kërcënime për dhunë ose thirrje për "vizitë" / ndjekje
- qasje të paautorizuar në profile dhe indikacione për keqpërdorim të të dhënave personale
- koordinim të organizuar që shkakton dëm të matshëm

Çfarë është "paketa e shpejtë" - 8 elemente që dërgohen në një mesazh

- **Subjekti/titulli:** Sulm i koordinuar - [media/gazetari] - [platforma] - [data]
- **Përmbledhje e shkurtër (4 - 6 fjali):** çfarë po ndodh, si shihet koordinimi, statusi (nëse është në zhvillim)
- **Kornizë kohore:** fillimi + momentet kyçe + statusi aktual
- **Lloji i sulmit:** raportim masiv i rremë / impersonim / marrje qasjeje / doksing / kërcënime / tjetër
- **Kush është i targetuar:** në nivel roli (gazetar, redaktor, admin faqeje), pa detaje personale të panevojshme
- **Çfarë është ndërmarrë:** hapat kryesorë (raportuar, ankuar, ndryshuar fjalëkalime, 2FA, kufizuar qasje)
- **Çfarë kërkohet:** orientim, koordinim, mbështetje ligjore, reagim publik, kontakt me institucione (vetëm çfarë është realisht e nevojshme)
- **Prova:** 3 - 5 linqe kyçe + bashkëngjitje/dosje me "mini-paketë"

Rregull praktik: më mirë **një paketë e plotë** sesa disa mesazhe me "do ta dërgoj më vonë".

"Mini-paketë" provash - çfarë mjafton për fillim

- Disa **screenshot-e me kontekst** (ekran i plotë, emër përdoruesi, link/titull i dukshëm, pjesë e mjedisit përreth)
- Një **video e shkurtër e ekranit** kur konteksti është kritik (si hapet linku dhe ku shihet përmbajtja e kontestuar)
- **Njoftimet/e-mail-et** më të rëndësishme nga platforma (kufizim, paralajmërim, pezullim)
- Një **tabelë e shkurtër** me linqe (3 - 10 rreshta) me kolonë "çfarë provon"
- Nëse ka **e-mail-e** me kërcënime – ruhen në formë origjinale (mos i "forward"-oni si provë e vetme pa nevojë), për të mos humbur të dhëna teknike/kontekst.

Shablloni 1 – Mesazh i shpejtë për SHGM

Lënda: Sulm i koordinuar - [media/gazetari] - [platforma] - [DD.MM.YYYY]

Përmbledhje (4 - 6 fjali):

- ✓ Çfarë po ndodh:
- ✓ Si shihet koordinimi:
- ✓ Statusi: (në zhvillim / i qetësuar / po rishfaqet)
- ✓ Rreziku kryesor: (humbje profili / siguri / tjetër)

Lloji i sulmit: [zgjidhni]
Targeti: [rol – pa të dhëna personale]
Çfarë është ndërmarrë: [3 - 6 pika të shkurtra]
Çfarë kërkojmë nga SHGM: [1 - 2 fjali]

Linqe kyçe (3 - 5):

- ✓ [link] - çfarë tregon
- ✓ [link] - çfarë tregon
- ✓ [link] - çfarë tregon

Bashkëngjitje/dosje(folder): [link me qasje të kufizuar ose "mini-paketë" në bashkëngjitje]
Kontakt: [emër, funksion, telefon zyrtar, e-mail zyrtar]
Kontakt rezervë: [emër + kontakt]

Shablon 2 - "Incident log" (minimal)

Kjo është evidencë e brendshme që ju krijon vijë kohore dhe ju shpëton nga "ku ishte ai link". (Rekomandohet të jetë një tabelë që plotësohet vazhdimisht.)

Emri i incidentit: [shkurt]
Data: [DD.MM.YYYY]
Koordinatori i incidentit: [emër dhe rol]
Statusi: [në zhvillim / i stabilizuar / i mbyllur]

Koha	Platforma	Linku/loka-cioni	Çfarë ndodhi	Çfarë bëmë	Provë
[HH:MM]	[IG/FB/X…]	[link]	[1 fjali]	[1 fjali]	[emri i skedarit/ linku]

Shablloni 3 – Tabela për prova (indeks)

Shenja	Data/koha	Platforma	Link	Çfarë paraqet	Pse është e rëndësishme
D1	[DD. MM.YYYY HH:MM]	[ ]	[ ]	[ ]	[kërcënim/doksing/imper-sonim/marrje qasjeje…]

Shablloni 4 - Format minimal për njoftim drejtuar insti-tucioneve (nëse ka bazë)

Subjekti: Njoftim/kallëzim për [kërcënime / doksing / qasje të paautorizuar / ngac-mim të organizuar] - [DD.MM.YYYY]

1. **Përshkrim i shkurtër: (**5 - 8 fjali: çfarë, kur, ku, kush është i targetuar – në nivel roli)
2. **Pse paraqet rrezik:** (1 - 2 fjali: siguri / privatësi / qasje / dëm)
3. **Prova kyçe:** (D1, D2, D3 + nga një fjali çfarë tregojnë)
4. **Dëmi deri më tani:** (konkret: profil i kufizuar, të dhëna personale të publikuara, kërcënime, qasje e humbur)
5. **Kërkesë për veprim:** (çfarë prisni: konfirmim pranimi, orientim, veprim urgjent, mbrojtje të të dhënave personale)
6. **Kontakt dhe konfidencialitet:** (pikë kontakti + fjali që provat përmbajnë të dhëna të ndjeshme dhe janë për përdorim zyrtar)

Rregulla praktike për privatësi gjatë shpërndarjes

- Në tekst mos përsëritni adresa/numra telefoni – referojuni provës ku ato shihen.
- Nëse dërgoni te më shumë marrës – dërgoni versionin “për shpërndarje” (me të dhëna personale të panevojshme të hequra), ndërsa origjinalin ruajeni me qasje të kufizuar.
- Mos dërgoni prova në grupe të mëdha/chate nëse përmbajnë të dhëna personale.

STUDIM RASTI - “SLOBODEN PEÇAT”

Ky rast tregon si një sulm i koordinuar mund të fillojë si “komente të pazakonta”, e më pas të kalojë në forma të tjera më të vështira për t’u kontrolluar, si pëlqime masive dhe kërkesa për ndjekje, me pasoja në funksionimin e rregullt dhe në dukshmërinë e përmbajtjeve.

Kontekst

Profilet zyrtare në Instagram të “Sloboden peçat” janë @slobodenpecat dhe @slobodenpecat.vesti. Profilet janë mirëmbajtur vazhdimisht rreth tetë vite, me rritje organike dhe pa përdorur promovime të paguara për ndjekës ose arritje.

Përmbledhje e shkurtër e incidentit

Incidenti u zhvillua në periudhën 06.11.2025 – 10.11.2025 në Instagram. Sulmi filloi me komente masive identike, pastaj kaloi në pëlqime masive dhe kërkesa për ndjekje nga profile të dyshimta. Si pasoja kryesore u evidentuan pengim i punës së redaksisë dhe rënie drastike e arritjes, me dyshim për kufizim algoritmik të dukshmërisë.

Si u zhvillua sulmi

Më 06.11.2025 u vërejt vala e parë – një numër i madh komentesh identike me fjalën “like” brenda së njëjtës minutë, nga profile pa ndërveprim të mëparshëm me median dhe me karakteristika tipike për profile të gjeneruara në mënyrë të rreme ose bot. I njëjti fenomen u përsërit nën publikime të tjera në një periudhë të shkurtër.

Gjatë të njëjtës ditë u shfaq vala e dytë – komente masive me përmbajtje politike dhe formulime të përsëritura, ku “Sloboden peçat” akuzohej për censurë dhe fshirje komentesh, me narrativa të lidhura me konflikte ndërkombëtare. Komentet vinin nga profile pa histori ndërveprimi me median, çka sugjeronte koordinim.

Pas aktivizimit të opsioneve mbrojtëse në platformë dhe kufizimeve për komente, komentet masive u ulën, por sulmi u zhvendos. Më 09.11.2025 u vërejt rritje e menjëhershme e pëlqimeve nga të njëjtit lloj profilesh të dyshimta në një publikim me arritje të lartë. Meqë nuk ekziston mekanizëm praktik për “pastrim” selektiv të pëlqimeve masive, profili u bë privat për të mbrojtur vazhdimësinë e punës dhe audiencën e ndërtuar organikisht. Më 10.11.2025 u regjistruan mbi 999 kërkesa për ndjekje, shumica nga profile qartazi të gjeneruara në mënyrë të rreme, gjë që kërkoi pastrim manual.

Gjurmë provash dhe indikatorë

Rasti është shembull se si provat duhet të ruajnë vijën kohore dhe të tregojnë "evoluimin" e sulmit.

- Linqe drejt publikimeve ku shfaqen sinjalet e para, së bashku me screenshot-e që tregojnë kontekstin dhe përsëritjen.
- Vizualizime dhe krahasime statistikash ("views over time") që tregojnë devijim të menjëhershëm në arritje(reach) pas sulmit, si bazë për dyshim për kufizim algoritmik.
- Screen-recording që tregon dinamikën atipike të pëlqimeve dhe ndjekjeve.
- Njoftime nga platforma, kur ekzistojnë, si provë shtesë për statusin dhe masat.

Mësime praktike që mund të zbatohen

1	Sulmi rrallë mbetet në një formë; kufizimi i komenteve mund ta zhvendosë sulmin drejt pëlqimeve, ndjekjeve ose mekanizmave të tjerë të platformës.
2	"Pastrimi" manual shpejt konsumon kapacitetin e redaksisë; është e dobishme të aktivizohet herët regjimi i incidentit me role dhe vijë kohore.
3	Kufizimet për komente dhe moderim janë efektive kur kombinohen me mbledhje sistematike provash dhe raportime konsistente në platformë.
4	Mbyllja e përkohshme (privatësia) mund të jetë masë taktike kur sulmi krijon ngarkesë masive teknike, por është më efektive nëse është paraparë paraprakisht në planin e reagimit.
5	Paketa e provave është më e fortë kur paraqet fazat e sulmit dhe dëmin real, jo vetëm screenshot-e të izoluara pa kontekst.
6	Koordinimi i hershëm me SHGM dhe evidentimi i rastit te institucionet kompetente krijon bazë për mbështetje të mëtejshme dhe reagim më të mirë institucional në raste të ardhshme.

CHECK-LISTË PËR GATISHMËRI NË REDAKSI

A. Role dhe koordinim	✓ Caktoni udhëheqës të incidentit dhe 2 zëvendës (minimum: vendimmarrje, menaxhim profilesh, mbledhje provash). ✓ Dakordoni një kanal të brendshëm për koordinim të shpejtë dhe rregull: vendimet kalojnë përmes udhëheqësit. ✓ Përgatitni listë me kontakte kyçe (të brendshme, IT/admin, mbështetje ligjore, SHGM).
B. Qasje dhe siguri e llogarive	✓ Aktivizoni 2FA (autentifikim me dy faktorë) për profilet kyçe dhe e-mail-et zyrtare; kodet rezervë ruajini në mënyrë të sigurt dhe me qasje të kufizuar. ✓ Kontrolloni rregullisht rolet e administratorëve dhe hiqni qasjet e "harruara". ✓ Përdorni fjalëkalime të forta dhe unike (menaxher fjalëkalimesh, kur është e mundur). ✓ Shmangni hyrjen në profile zyrtare nga rrjete publike dhe pajisje të pasigurta, veçanërisht në periudha rreziku.
C. Zbulim i hershëm dhe moderim	✓ Përcaktoni kush monitoron njoftimet nga platformat dhe kush reagon ndaj paralajmërimeve për aktivitet të dyshimtë/kufizime. ✓ Ndiqni sinjale "alarm": rritje të menjëhershme në komente/ndjekje, fraza të sinkronizuara, profile të përsëritura, zhvendosje të sulmit në platforma të tjera. ✓ Keni rregulla të shkurtra për moderim (çfarë fshihet menjëherë, çfarë dokumentohet dhe raportohet, çfarë lihet si kritikë legjitime). ✓ Mos fshini në mënyrë masive pa siguruar më parë prova (screenshot-e, linqe, vijë kohore).
D. Mbështetje psikologjike dhe ekipore	✓ Bëni një "check-in" të shkurtër me personin e targetuar në 24 – 48 orët e para. ✓ Merrni parasysh rishpërndarje të përkohshme detyrash nëse presioni është i fortë ose ka kërcënime/doksing. ✓ Kur është e mundur, inkurajoni mbështetje profesionale (sidomos në raste sulmesh të përsëritura).
E. Ushtrime dhe përditësim	✓ Realizoni një simulim të shkurtër 30 – 45 minuta (raportim masiv ose impersonim) 1 – 2 herë në vit. ✓ Pas çdo incidenti, shënoni "çfarë mësuam" dhe përditësoni kontaktet, qasjet dhe shabllonet.

Politika dhe mjete të platformave (raportim, ankesa, rikthim profili)

Meta. „Making it Easier to Access Account Support on Facebook and Instagram“. Meta, 04.12.2025. Qasur më 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, pa datë. Qasur më 20.01.2026. https://www.meta.com/account-recovery-support/

Meta. „Inauthentic Behavior (Community Standards)“. Meta Transparency Center, pa datë. Qasur më 20.1.2026. https://transparency.meta.com/policies/community-standards/inauthentic-behavior/

Instagram. „Hacked Instagram Account“. Instagram Help Center, pa datë. Qasur më 20.1.2026. https://help.instagram.com/368191326593075/

Instagram. „Report an Impersonation Account on Instagram or Threads“. Instagram Help Center, pa datë. Qasur më 20.01.2026. https://help.instagram.com/contact/636276399721841

X. „X's Private Information Policy and Doxxing“. X Help Center, pa datë. Qasur më 20.1.2026. https://help.x.com/en/rules-and-policies/personal-information

X. „How to Report Abusive Behavior on X“. X Help Center, pa datë. Qasur më 20.1.2026. https://help.x.com/en/safety-and-security/report-abusive-behavior

YouTube. „Harassment & Cyberbullying Policies“. YouTube Help, pa datë. Qasur më 20.1.2026. https://support.google.com/youtube/answer/2802268

YouTube. „Report Inappropriate Videos, Channels & Other Content on YouTube“. YouTube Help, pa datë. Qasur më 20.01.2026. https://support.google.com/youtube/answer/2802027

TikTok. „My Account Has Been Hacked“. TikTok Support, pa datë. Qasur më 20.01.2026. https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked

Burime praktike për siguri digjitale dhe reagim ndaj incidenteve

Access Now. „Digital Security Helpline“. Access Now, pa datë. Qasur më 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. Qasur më 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. Qasur më 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. Qasur më 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“. Pa datë. Qasur më 20.1.2026. https://onlineviolenceresponsehub.org/

Standarde evropiane dhe ndërkombëtare relevante për mbrojtje praktike

Bashkimi Evropian. “Rregullorja (BE) 2022/2065 e Parlamentit Evropian dhe e Këshillit e 19.10.2022 për tregun unik të shërbimeve digjitale (Digital Services Act)”. EUR-Lex, 19.10.2022. Qasur më 20.01.2026. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Bashkimi Evropian. “Rregullorja (BE) 2022/2065 e Parlamentit Evropian dhe e Këshillit e 19.10.2022 për tregun unik të shërbimeve digjitale (Digital Services Act)”. EUR-Lex, 16.09.2021. Qasur më 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. Qasur më 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. Qasur më 20.1.2026. https://rm.coe.int/pocketguide2023-final/1680ac9318

OSBE – Përfaqësuesi për Lirinë e Mediave. „Guidelines for Monitoring Online Violence Against Female Journalists“. OSCE, komisionuar 2022 (PDF). Qasur më 20.1.2026. https://www.osce.org/files/f/documents/b/0/554098_1.pdf.

www.znm.org.mk