Vaša *digitálna* bezpečnosť

PRÍRUČKA PRE ŽENY VO VEREJNOM PRIESTORE

Ako sa chrániť pred online obťažovaním, manipulatívnymi útokmi a rodovo podmienenými dezinformáciami

Mgr. Rasťo Kužel
Mgr. Marek Mračka
prof. PhDr. Alexandra Bitušíková, CSc.

OBSAH

O tejto príručke a ako s ňou *pracovať*

> *„Viditeľnosť nesmie znamenať zraniteľnosť."*

Táto príručka vznikla v rámci projektu „**Fighting gendered disinformation online**", ktorý realizuje MEMO 98 s cieľom posilniť digitálnu bezpečnosť a odolnosť voči online útokom.

Projekt bol realizovaný s podporou Holandského kráľovstva. Za obsah publikácie nesú zodpovednosť jej autori, pričom názory uvedené v texte nemusia nevyhnutne odrážať stanoviská donorov.

Táto príručka je určená najmä ženám, ktoré pôsobia vo verejnom priestore alebo sú viditeľné online. Užitočná však môže byť aj pre organizácie, redakcie, občianske združenia a neformálne komunity, ktoré chcú lepšie chrániť ľudí vo svojom tíme.

Cieľom tejto príručky je ponúknuť **praktickú orientáciu**: stručne vysvetliť, čo sú rodovo podmienené dezinformácie, ako vyzerajú v praxi, čo robiť po útoku, ako chrániť svoje účty a súkromie, ako reagovať bezpečne a ako si nastaviť základný plán prevencie. Príručka je navrhnutá ako praktický sprievodca – môžete sa k jednotlivým častiam vracať podľa potreby, bez nutnosti čítať ju od začiatku do konca.

Táto príručka vychádza z presvedčenia, že **viditeľnosť nesmie znamenať zraniteľnosť**. Verejný aj online priestor by nemal byť miestom, kde sa ženy a ďalšie zraniteľné skupiny boja slobodne vyjadrovať z dôvodu rizika útokov, zastrašovania či znevažovania.

> ***Tip:*** *Tento materiál môžete použiť aj v krízovej situácii – jednotlivé časti sú navrhnuté tak, aby sa dali čítať samostatne (napríklad len sekcia o prvých 30 minútach po online útoku). Ak sa nachádzate v situácii, ktorá vás zneisťuje alebo ohrozuje, môžete začať práve touto časťou.*

Verejný aj online priestor patrí ženám rovnakým dielom. Bezpečnosť preto nevnímame ako prekážku v účasti na verejnom živote, ale ako základnú podmienku slobody. Zároveň ponúka konkrétne kroky a odporúčania, ktoré pomáhajú túto bezpečnosť aktívne posilňovať v každodennej praxi.

Čo sú *rodovo podmienené* dezinformácie?

01

Rodovo podmienené dezinformácie sú falošné, zavádzajúce alebo manipulatívne naratívy, ktoré útočia na človeka alebo skupinu na základe rodu, rodových rolí, sexuality alebo stereotypov spojených s tým, aká žena „má byť" a aké miesto jej „patrí".

Často sa tvária ako názor, vtip, kritika alebo len „tvrdšia debata". V skutočnosti však nejde o vecnú polemiku, ale o útok na dôveryhodnosť, dôstojnosť, identitu a právo človeka verejne vystupovať. Takéto útoky sa nezameriavajú na argumenty, ale na vzhľad, hlas, materstvo, sexualitu, morálku, ženskosť, „slušnosť" alebo „správne miesto ženy v spoločnosti".

> ***Dôležité:*** *cieľom týchto útokov nie je vyhrať diskusiu, ale oslabiť vašu dôveryhodnosť, vyvolať tlak a odradiť vás od ďalšieho vystupovania.*

Rodovo podmienené dezinformácie sa často prepájajú s ďalšími škodlivými naratívmi. **Môžu byť súčasťou širších útokov proti rodovej rovnosti, ľudským právam, občianskemu aktivizmu, nezávislým médiám či verejne angažovaným ľuďom a inštitúciám.** Niekedy pracujú so strachom z údajných spoločenských zmien, inokedy vykresľujú konkrétne ženy ako hrozbu pre rodinu, tradície, stabilitu alebo morálne hodnoty.

V praxi často nejde o jednotlivý komentár, ale o kombináciu viacerých útokov (komentáre, príspevky, memy, videá), ktoré sa navzájom posilňujú a zvyšujú tlak.

Nejde len o verbálne útoky. V skutočnosti môže ísť o stratégiu, ktorej cieľom je znevideteľniť verejne pôsobiace osobnosti a spraviť z verejného priestoru miesto, kde ich hlas prestáva byť počuť.

Výsledkom býva, že človek začne sám seba obmedzovať – menej píše, menej vystupuje alebo sa z verejného priestoru stiahne úplne.

Prečo je to *problém?* 02

Rodovo podmienené dezinformácie neškodia len jednej osobe. Ich cieľom býva často vyvolať širší efekt: **zastrašiť, vyčerpať, zneistiť, spochybniť dôveryhodnosť a odradiť ďalšie ženy od toho, aby verejne vystupovali.** Cieľom nie je len útok na jednotlivca, ale vytvorenie prostredia, v ktorom je pre ženy a menšiny náročnejšie alebo riskantnejšie byť verejne aktívne.

> *„človek prestane hovoriť nie preto, že nesmie, ale preto, že je to príliš vyčerpávajúce, alebo nebezpečné."*

Človek, ktorý je cieľom útoku, sa môže cítiť ohrozený, unavený, ponížený alebo dlhodobo pod tlakom. Môže začať obmedzovať svoje vystupovanie, zrušiť verejné podujatia, prestať publikovať, vyhýbať sa témam, ktoré vyvolávajú útoky, alebo sa úplne stiahnuť z online priestoru. Tak vzniká autocenzúra, ktorá nie je slobodnou voľbou, ale reakciou na nepriateľské prostredie.

Tento efekt sa často označuje ako „umlčiavanie bez zákazu" – človek prestane hovoriť nie preto, že nesmie, ale preto, že je to príliš vyčerpávajúce, alebo nebezpečné.

Keď sa to deje opakovane, nejde len o individuálny problém. Mení sa tým verejná diskusia. Ak útoky umlčiavajú ženy, novinárky, odborníčky alebo aktivistky, verejný priestor prichádza o dôležité hlasy, skúsenosti a perspektívy. Oslabuje sa pluralita, narúša sa dôvera a prehlbuje sa polarizácia.

Rodovo podmienené dezinformácie preto nezasahujú len jednotlivé osoby, ale aj kvalitu verejnej diskusie a demokratickej účasti.

Ako tieto útoky *vyzerajú v praxi?* 03

Tieto útoky môžu mať mnoho podôb. Niekedy ide o jednotlivé komentáre alebo príspevky, inokedy o koordinované kampane naprieč platformami. **V mnohých prípadoch sa kombinujú rôzne formy útoku tak, aby sa navzájom posilňovali.** To znamená, že jeden útok môže rýchlo prerásť do širšej kampane, najmä ak sa začne zdieľať alebo preberať ďalšími účtami.

Najčastejšie formy útokov

- zosmiešňovanie vzhľadu, hlasu alebo prejavu
- sexualizované urážky a ponižujúce narážky
- spochybňovanie odbornosti, inteligencie či kompetencií
- nálepkovanie a vykresľovanie žien ako „bábok“, „agentiek“ či „hrozieb“
- manipulácia s obsahom cez upravené fotky, memy a vytrhnuté výroky
- morálne súdy a agresívne útoky na súkromný život
- koordinovaný tlak prostredníctvom organizovaných komentárov a zdieľaní
- šírenie klamstiev o financovaní, motiváciách či osobných vzťahoch
- zverejňovanie súkromia (doxing) a zastrašovanie odhalením identity

Niektoré z týchto útokov môžu na prvý pohľad pôsobiť nevinne (napr. ako vtip alebo meme), no v skutočnosti **sú súčasťou širšieho vzorca znevažovania.**

Na Slovensku sa tieto útoky často prelínajú s ideologickými a geopolitickými témami. Ženy sa tak stávajú terčom nielen za svoje slová, ale aj za to, čo symbolicky reprezentujú: verejnú angažovanosť, ochranu práv, profesionálnu integritu či schopnosť kriticky čeliť manipulatívnym naratívom. Útok sa tak často presúva z konkrétneho výroku na to, čo osoba „ “ v očiach útočníkov predstavuje.

Útok často nezačína argumentom. Začína stereotypom. A stereotyp sa potom používa ako zbraň.

Kto býva najčastejšie *terčom?* 04

Najčastejším terčom sú ženy, ktoré sú viditeľné, aktívne a verejne vystupujú.

Typicky ide o novinárky, političky, kandidátky, aktivistky, odborníčky, komentátorky, pracovníčky občianskych organizácií a ženy, ktoré sa angažujú vo svojich komunitách.

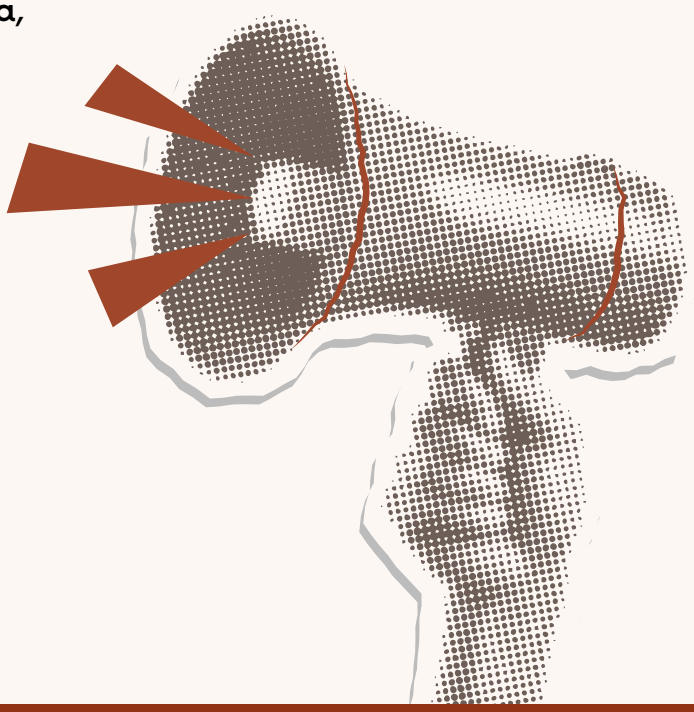
Vysokému riziku čelia ženy, ale aj muži, ktorí sa venujú témam, ako sú rodová rovnosť, ľudské práva, reprodukčné práva, postavenie menšín, korupcia, extrémizmus alebo dezinformácie. Práve tieto témy bývajú polarizované a často sa stávajú zámienkou na osobné útoky.

Rodovo podmienené útoky sa však netýkajú len žien. **Zasahovať môžu aj ďalšie verejne viditeľné alebo zraniteľné skupiny a niekedy aj mužov, ak na nich útočníci cielia cez stereotypné predstavy o tom, ako sa má správať „správny" muž alebo žena.** V praxi sa teda tieto dezinformácie dotýkajú širšieho okruhu ľudí, ktorých verejná prítomnosť, identita alebo postoje nezapadajú do úzkych stereotypných predstáv.

Zvýšenému riziku čelia najmä ľudia, ktorí sa odlišujú – napríklad svojimi názormi, identitou alebo verejným postojom.

Netýka sa to len verejne známych osobností. Útoky v lokálnom prostredí - či už v rámci komunity, kampane alebo na pracovisku - bývajú často osobnejšie a o to zraňujúcejšie.

Netreba podceňovať ani drobné, dlhodobé prejavy nepriateľstva, keďže ich následky sú často rovnako vážne.



Kedy *nejde* o bežnú kritiku? 05

Nie každá ostrá reakcia je koordinovaný útok. Vo verejnom priestore je normálne, že ľudia nesúhlasia, polemizujú alebo aj ostrejšie kritizujú. **Dôležité je vedieť rozlíšiť, kedy ide ešte o vecnú kritiku a kedy už o manipulatívny tlak, zastrašovanie alebo cielenú kampaň.**

Rozlíšenie je dôležité: nie každú kritiku treba riešiť, ale niektoré situácie si vyžadujú rýchlu reakciu.

Najčastejšie varovné signály

- v krátkom čase sa objaví veľké množstvo podobných komentárov,
- rôzne účty používajú rovnaké alebo veľmi podobné formulácie,
- útok sa nezameriava na obsah vášho výroku, ale na to, kým ste,
- objavuje sa sexualizácia, hanobenie alebo morálne súdy,
- niekto zverejňuje alebo naznačuje osobné údaje,
- komentáre majú za cieľ vyvolať hanbu, strach alebo mlčanie,
- útok sa rýchlo šíri cez viacero profilov, skupín alebo platforiem,
- objavujú sa výzvy na „odhalenie“, zosmiešnenie, alebo potrestanie.

Ak sa objaví viacero týchto signálov naraz, pravdepodobne nejde o bežnú kritiku, ale o koordinovaný alebo manipulatívny útok.

Užitočnou pomôckou môže byť jednoduchá otázka: smeruje útok na to, čo hovoríte, alebo na to, kým ste? Bežná kritika sa týka názoru, rozhodnutia, či konkrétneho konania. Manipulatívny útok však cieli na vašu identitu, dôstojnosť a samotné právo byť prítomná vo verejnom priestore.

> ***Rýchly test:*** keby ste ten istý komentár počuli na pracovnom stretnutí, alebo verejnej diskusii, považovali by ste ho za primeraný?

Ak máte pocit, že nejde len o nesúhlas, ale o snahu zastrašiť, vyčerpať alebo umlčať, berte situáciu vážne. Netreba čakať, kým sa ešte zhorší. Intuícia je dôležitá – **ak sa necítite bezpečne, je to dostatočný dôvod konať.**

Čo robiť v *prvých 30 minútach* po útoku?

06

> ***Dôležité:*** *Keď sa útok začne, je prirodzené chcieť reagovať okamžite. Najlepším prvým krokom však býva spomaliť a získať kontrolu nad situáciou. To, čo urobíte v prvých minútach, môže výrazne ovplyvniť ďalší priebeh.*

Základný postup:

Stop → Ulož → Posúď → Kontaktuj → Zabezpeč → Rozhodni

Zastavte impulz odpovedať hneď

Nereagujte v šoku, hneve ani v panike. Aj krátka pauza vám môže pomôcť vyhnúť sa reakcii, ktorá by pod tlakom mohla zbytočne zvýšiť dosah útoku. Aj 10 či 15 minút môže výrazne zmeniť kvalitu vašej reakcie.

Uložte dôkazy

Spravte screenshoty, uložte odkazy, mená účtov, čas a platformu. Ak sa útok rýchlo šíri, nespoliehajte sa na to, že obsah zostane online. Screenshoty robte tak, aby bolo vidieť aj meno účtu, dátum a URL adresu.

Zistite, o aký typ útoku ide

Položte si základné otázky: ide o urážku, koordinovaný nátlak, hrozbu, zverejnenie osobných údajov (doxing), pokus o kompromitáciu alebo známku hacknutia? Typ útoku určuje ďalší postup, pričom nie všetky situácie sa riešia rovnako.

Dajte vedieť niekomu dôveryhodnému

Kolegyňa, editor, koordinátorka, kamarátka alebo iný blízky človek vám môže pomôcť situáciu posúdiť a niesť ju s vami. Nemusíte to riešiť sama. Zapojenie ďalšieho človeka znižuje stres aj riziko unáhlených rozhodnutí.

Skontrolujte, či nejde o bezpečnostné riziko

Ak útok obsahuje hrozby, osobné údaje alebo známky narušenia účtu, riešte ho ako bezpečnostný incident. V takom prípade je prioritou ochrana účtov, súkromia a fyzickej bezpečnosti.

Uložte dôkazy

Nie každý útok si vyžaduje verejnú odpoveď. Najprv bezpečie, potom komunikácia. Reakcia by mala byť premyslená, nie unáhlená pod tlakom.

Ako si útok *zdokumentovať?* 07

Dobre zdokumentovaný incident sa ľahšie rieši. Pomáha pri internom nahlásení, pri komunikácii s platformou, aj pri zvažovaní právnych krokov.

Čím presnejšie máte dôkazy, tým jednoduchšie sa situácia rieši a posudzuje.

Pri každom incidente si skúste uložiť

- screenshot alebo videozáznam obrazovky,
- presný odkaz na obsah,
- dátum a čas,
- názov profilu, stránky alebo skupiny,
- platformu, na ktorej sa útok objavil,
- stručný opis toho, čo sa stalo a prečo je to problém,
- informáciu, či sa útok opakuje, alebo šíri ďalej,
- poznámku, či sa objavili hrozby, osobné údaje, alebo známky koordinácie.

Tipy

- Screenshoty robte tak, aby bolo vidieť meno účtu, dátum a ideálne aj URL adresu.

- Ak ide o viac príspevkov, vytvorte si jednoduchý incident log. Môže to byť tabuľka, poznámka v dokumente, alebo priečinok s dôkazmi. Dôležité je, aby ste vedeli spätne zachytiť rozsah, intenzitu a vývoj útoku. Aj jednoduchý zoznam (dátum – čo sa stalo – kde – kto) výrazne pomáha udržať prehľad.

- Uchovávajte dôkazy mimo platformy. Obsah môže byť vymazaný, nahlásený, zablokovaný alebo zmenený. Ideálne je mať kópie uložené na zariadení alebo úložisku, ku ktorému máte bezpečný prístup.

Čo potom: *ignorovať, moderovať, nahlásiť* alebo *eskalovať?*

08

Nie každý útok si vyžaduje rovnakú reakciu. Niekedy postačí nereagovať, alebo skryť komentár. Inokedy je nevyhnutné zapojiť tím, situáciu zdokumentovať, kontaktovať platformu, alebo pristúpiť k formálnemu nahláseniu. **Neexistuje jedna správna reakcia – dôležité je zvoliť postup podľa závažnosti situácie.** Pomôcť môže jednoduchá séria otázok:

Je to len jedna urážka bez širšieho dosahu?

Ak áno, zvyčajne postačí nereagovať, komentár skryť alebo účet zablokovať.

Opakuje sa to, alebo sa to šíri koordinovane?

Ak áno, situáciu dokumentujte a zapojte tím, či organizáciu. Sledujte, či nejde o cielene zosilňovanú kampaň. Pri opakovaných útokoch je dôležité nenechať to bez reakcie a začať situáciu systematicky sledovať.

Obsahuje to hrozbu, osobné údaje, alebo známky zverejnenia osobných údajov (doxxing)?

Ak áno, ide o bezpečnostný incident - situáciu bezodkladne eskalujte a zapojte ďalšiu pomoc. Nečakajte, ale konajte okamžite.

Zasahuje to do práce, reputácie, alebo psychickej pohody?

Ak áno, nenechávajte to na seba. Vyhľadajte podporu, využite interné mechanizmy a podľa potreby aj odbornú pomoc. Aj psychický dopad je dostatočný dôvod na riešenie situácie.

Má verejná reakcia zmysel?

Verejná odpoveď je spravidla vhodná vtedy, ak môže situáciu upokojiť, pomenovať manipuláciu, alebo ochrániť ďalších. Nie vždy je potrebná. Niekedy je najlepšou reakciou nereagovať a nešíriť útok ďalej. Platí jedno základné pravidlo: ak ide o vyhrážky, doxing, pokus o hacknutie alebo cielené zastrašovanie – konajte okamžite. Ak si nie ste istá, radšej situáciu konzultujte. Je to vždy lepšie, ako ju podceniť.

Chráňte svoje *účty* a *zariadenia* 09

Digitálna bezpečnosť nezačína až po útoku. Začína ešte predtým - pri základných nastaveniach, ktoré znižujú riziko hacknutia, prevzatia účtu, alebo zneužitia osobných údajov.

Prevencia je najjednoduchší spôsob, ako znížiť dopad prípadného útoku.

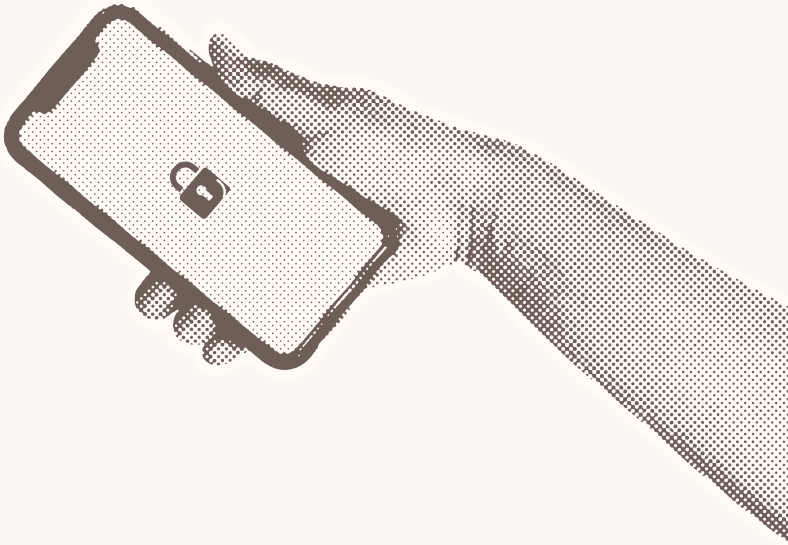
Základné minimum zahŕňa

- silné a jedinečné heslá pre každú službu,
- dvojfaktorové overenie,
- pravidelné aktualizácie telefónu, počítača a aplikácií,
- kontrolu prihlásených zariadení a aktívnych relácií,
- opatrnosť pri podozrivých správach, odkazoch a prílohách,
- oddelenie súkromných a verejných účtov,
- priebežnú kontrolu toho, kto má k vašim účtom prístup.

Ak používate rovnaké heslo na viacerých miestach, stačí jeden útok a ohrozené môžu byť viaceré účty naraz.

Ak čelíte online útokom, bezpečnosť účtov nie je technický detail. Je to súčasť vašej ochrany. V niektorých prípadoch môžu po dezinformačnej kampani nasledovať aj technické pokusy o narušenie účtov, zneužitie prihlasovacích údajov, alebo iné formy útoku. Útok na reputáciu sa môže rýchlo premeniť na útok na vaše účty, alebo súkromie.

Ak je to možné, používajte správcu hesiel a urobte si aspoň raz za čas krátky bezpečnostný audit. Dve minúty prevencie dnes môžu znamenať hodiny ušetreného stresu neskôr. Stačí si raz za pár mesiacov prejsť nastavenia účtov a skontrolovať, či je všetko aktuálne a bezpečné.



Chráňte svoje *súkromie* 10

Pri online útokoch býva zraniteľným miestom nielen obsah, ktorý zdieľate, ale aj informácie, ktoré sa o vás dajú jednoducho nájsť. Preto sa oplatí urobiť si základný audit súkromia.

Útočníci často pracujú práve s verejne dostupnými informáciami – nemusia nič „hacknúť".

Skontrolujte si:

- aké kontaktné údaje sú verejne dostupné,
- či sa vaša adresa, alebo miesto pobytu, nenachádza online,
- čo sa dá zistiť o vašej rodine, deťoch, škole či dennom režime,
- či fotografie neodhaľujú polohu, auto, dom, alebo pracovné miesto,
- ktoré staršie príspevky dnes zbytočne zvyšujú riziko,
- ktoré účty, alebo aplikácie, majú prístup k vašim osobným údajom.

> ***Tip:*** *Skúste si vygoogliť samu seba a prejsť si, čo všetko je o vás verejne dostupné.*

Cieľom nie je zmiznúť z online priestoru. Cieľom je obmedziť množstvo informácií, ktoré možno zneužiť na zastrašovanie, doxing alebo reputačné útoky. Menej dostupných informácií znamená menej možností na zneužitie.

Pomáha aj jedno jednoduché pravidlo: **zverejňujte vedome. Nie všetko, čo je pravdivé, musí byť aj verejné.** Platí to najmä pri informáciách o rodine, deťoch, cestách, presnej polohe, či každodennom režime. Najmä pri zdieľaní v reálnom čase (napr. z dovolenky alebo domova) zvážte, či je to bezpečné.

Kde je to možné, oddeľte pracovné a súkromné kontakty. Ak sa útok rozšíri do iných oblastí vášho života, budete môcť reagovať s väčším odstupom - a väčším pokojom. Oddelenie kontaktov vám dáva väčšiu kontrolu nad tým, kto a ako vás môže kontaktovať.

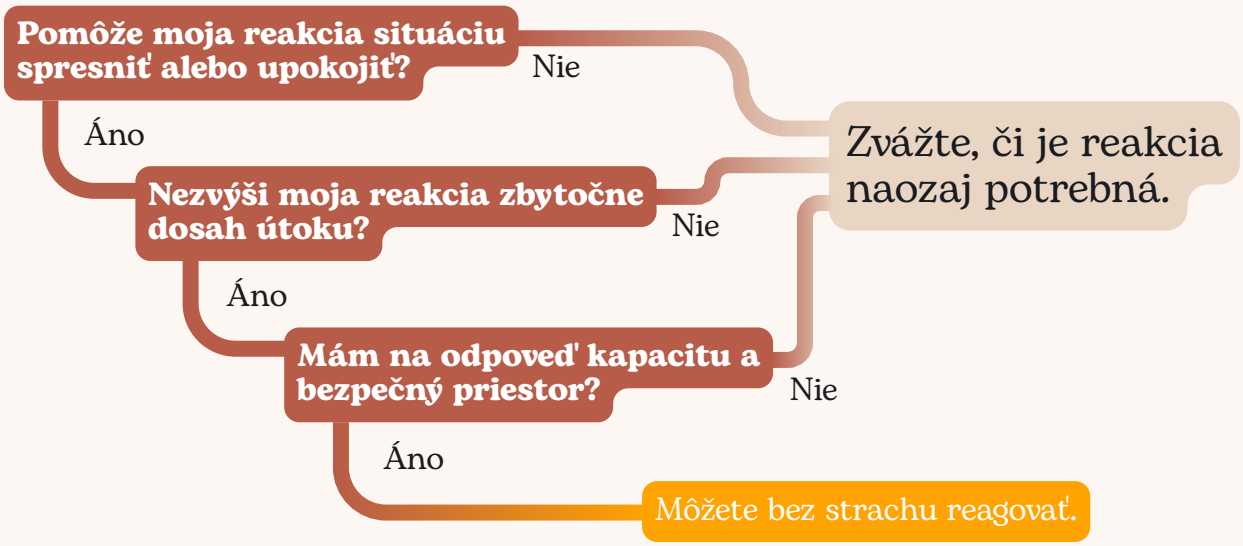
Kedy reagovať *verejne*, a kedy radšej *nie*

11

Nie každý útok si vyžaduje verejnú odpoveď. Niekedy je najlepšou reakciou nereagovať vôbec. Inokedy pomôže krátke a vecné pomenovanie manipulácie. Dôležité je, aby reakcia chránila vás, nie logiku útoku.

Cieľom reakcie nie je presvedčiť útočníka, ale nastaviť hranice a ochrániť seba (a prípadne aj publikum).

Skôr než odpoviete, položte si tri otázky:



Dobrá reakcia nemusí byť dlhá. Musí byť bezpečná, presná a vedomá. A niekedy je tou najlepšou reakciou to, že sa rozhodnete nehrať hru, ktorú nastavili útočníci. Rozhodnutie nereagovať je tiež aktívna a legitímna voľba.

Ak sa rozhodnete reagovať, držte sa týchto zásad:

- reagujte až po krátkom odstupe,
- držte sa faktov,
- nevysvetľujte donekonečna svoju dôstojnosť, ani právo byť prítomná vo verejnom priestore,
- neodpovedajte na každý komentár,
- ak je to vhodné, nechajte hovoriť aj organizáciu, redakciu alebo tím,
- ak je cieľom útoku vyprovokovať vás, nenechajte sa vtiahnuť do hry.

Keď útok zasiahne *tím,* alebo *organizáciu*

12

Ak sa útok netýka len jednej osoby, ale aj organizácie, redakcie alebo kampane, veľmi pomáha mať aspoň jednoduchý dohodnutý postup. V strese sa rozhoduje ťažšie a chaos zvyšuje tlak na napadnutú osobu, ale aj na celý tím.

Postup, ktorý je dopredu dohodnutý, znižuje stres a urýchľuje reakciu.

Je dobré vedieť:

- kto monitoruje situáciu,
- kto archivuje dôkazy,
- kto komunikuje navonok,
- kto je v kontakte s dotknutou osobou,
- kto rieši technickú bezpečnosť účtov,
- kto rozhoduje o eskalácii a ďalších krokoch.

Keď je jasné, kto čo robí, situácia sa zvláda pokojnejšie a bez zbytočného tlaku na jednotlivcov. Pri silnejšom útoku je dôležité, aby človek, ktorý je terčom, nemusel niesť všetko sám. **Organizácia mu vie pomôcť tým, že prevezme monitoring, triedenie komentárov, prípravu odpovede, komunikáciu s platformami, alebo posúdenie, či je potrebné zapojiť právnu či psychologickú pomoc.**

Najväčšou pomocou býva prevzatie časti zodpovednosti – aby napadnutá osoba nemusela riešiť všetko sama. **Dobrý tímový postup nemusí byť zložitý.** Dôležité je, aby bol vopred premyslený, zrozumiteľný a použiteľný. Krízová komunikácia nie je len o verejnom vyhlásení. Je aj o tom, ako v tíme rozdelíte úlohy, znížite tlak a ochránite človeka, ktorý je práve pod útokom.

Aj jednoduchý interný dokument môže výrazne zlepšiť pripravenosť tímu.

Psychologická podpora je súčasť bezpečnosti

13

Online útok môže spôsobiť šok, hnev, únavu, pocit hanby, strach aj bezmocnosť. Takéto reakcie sú normálne. Nie sú znakom slabosti. Sú prirodzenou reakciou na nepriateľské a zaťažujúce správanie.

Každý človek reaguje inak – neexistuje „správny" spôsob, ako sa cítiť.

Pomôcť môže:

- vypnúť notifikácie a získať odstup,
- obmedziť čítanie komentárov,
- zveriť monitoring niekomu inému,
- hovoriť s blízkou osobou alebo kolegyňou,
- požiadať o odbornú psychologickú pomoc,
- neprenášať zodpovednosť za útok na seba,
- dopriať si spánok, pohyb a základný režim aj v období tlaku.

Aj krátky odstup od online priestoru môže výrazne pomôcť znížiť stres.

Útok, ktorý sa odohráva online, môže mať veľmi reálne dôsledky offline. Dlhodobý tlak, nenávisť a pocit neustáleho sledovania sa môžu prejaviť na psychickom zdraví, sústredení aj schopnosti pracovať. Dlhodobé vystavenie útokom môže viesť k vyčerpaniu, alebo vyhoreniu. **Je v poriadku spomaliť a dať si priestor.**

To, že vás útok zasiahol, neznamená, že ste zlyhali. Znamená to, že išlo o útok. Aj psychologická podpora patrí k zodpovednej reakcii. Nie je to niečo navyše. Je to súčasť ochrany. Postarať sa o seba nie je slabosť – je to súčasť vašej bezpečnosti.

Kedy už *nestačí* riešiť to sama 14

Niektoré incidenty sa dajú zvládnuť moderovaním, blokovaním, alebo internou podporou. Iné si vyžadujú širšiu pomoc.

Nie je vašou povinnosťou zvládnuť všetko sama.

Skontrolujte si:

- útok obsahuje vyhrážky,
- sú zverejnené osobné údaje,
- ide o stalking alebo opakované zastrašovanie,
- objavia sa známky hacknutia, alebo prevzatia účtu,
- útok zasahuje rodinu, deti alebo kolegov,
- útok má výrazný dopad na psychické zdravie, alebo prácu,
- situácia presahuje kapacity vás, alebo vášho tímu.

Ak si nie ste istá, či je situácia „dostatočne vážna", je v poriadku sa poradiť.

Externá pomoc môže mať rôzne podoby. Môže ísť o právnu pomoc, IT bezpečnostnú podporu, psychologickú pomoc, alebo o kontaktovanie polície, ak ide o hrozby, stalking, zverejnenie osobných údajov, alebo iný závažný incident.

Vyhľadanie pomoci neznamená, že situáciu nezvládate – znamená to, že ju riešite zodpovedne.

Nie vždy je jednoduché rozhodnúť sa, či niečo nahlásiť. Mnohí ľudia majú skúsenosť s tým, že sa necítili vypočutí alebo že pomoc prišla neskoro. To však nemení nič na tom, že pri vážnych hrozbách treba myslieť aj na formálne kroky.

Dôležité je mať pri tom podporu, nezostať na to sama a postupovať čo najpokojnejšie a systematicky. Aj malé kroky (konzultácia, uloženie dôkazov, rozhovor s odborníkom) môžu byť začiatkom riešenia.

Môj osobný *bezpečnostný checklist*

15

Skúste si prejsť tento zoznam a označiť, čo už máte nastavené a čo si ešte potrebujete doplniť.

Nemusíte mať všetko splnené – cieľom je vedieť, kde ste a čo je ďalší krok.

- ☐ Mám silné a jedinečné heslá.
- ☐ Mám zapnuté dvojfaktorové overenie.
- ☐ Viem, kto mi pomôže pri technickom probléme.
- ☐ Mám oddelené súkromné a verejné účty.
- ☐ Viem, ako ukladať dôkazy o útoku.
- ☐ Viem, kedy útok ignorovať a kedy eskalovať.
- ☐ Mám obmedzené množstvo osobných údajov dostupných online.
- ☐ Viem, komu sa ozvem, keď sa niečo stane.
- ☐ Neostávam na online útok sama.
- ☐ Viem, kde hľadať psychologickú, alebo právnu pomoc.

Tento checklist nie je test. Je to orientačná pomôcka. Nemusíte mať všetko vyriešené naraz. Dôležité je vedieť, kde ste dnes, a postupne si budovať väčšiu istotu a pripravenosť

Bezpečnosť sa často buduje sériou menších krokov.

Aj drobné zmeny v nastavení účtov, alebo návykoch môžu mať veľký efekt.

Je naša *organizácia* pripravená? 16

Online útoky nie sú len individuálny problém. Organizácia môže výrazne ovplyvniť, či sa človek cíti chránený, alebo osamelý.

To, ako organizácia reaguje, má priamy vplyv na to, či sa človek cíti bezpečne, alebo pod tlakom.

Skúste si v tíme prejsť tento základný zoznam:

- ☐ Máme jasné pravidlá, čo sa považuje za incident?
- ☐ Vieme, kto monitoruje a archivuje útoky?
- ☐ Máme dohodnuté prahy eskalácie?
- ☐ Vieme, kedy kontaktovať políciu, alebo odbornú pomoc?
- ☐ Chránime napadnutú osobu pred preťažením?
- ☐ Máme základný plán krízovej komunikácie?
- ☐ Máme bezpečnostné minimum pre účty a zariadenia?
- ☐ Máme spôsob, ako filtrovať nenávistné komentáre?
- ☐ Vieme poskytnúť psychologickú, alebo peer podporu?
- ☐ Učíme sa z incidentov a priebežne upravujeme postupy?

Ak si na viacero otázok odpoviete „nie“, je to dobrý moment na začatie s jednoduchými krokmi.

Nemusíte mať rozsiahly bezpečnostný manuál. Veľký rozdiel často urobí aj jednoduchý interný dokument, v ktorom je jasne napísané, kto čo robí, ako sa uchovávajú dôkazy a kedy sa situácia eskaluje. Aj krátky, zrozumiteľný dokument môže výrazne zlepšiť pripravenosť tímu.

Pripravená organizácia nevyrieši všetko. Môže však výrazne znížiť chaos, urýchliť pomoc a ukázať ľuďom, že na útok nie sú sami.

Podpora zo strany organizácie je kľúčová – nikto by nemal čeliť útokom sám.

Ako *budovať odolnosť* dlhodobo 17

Reakcia na incident je dôležitá, no rovnako dôležitá je aj dlhodobá odolnosť. Tá nevzniká len individuálne. Vzniká v prostredí, kde ľudia vedia rozpoznať škodlivé naratívy, navzájom sa podporujú a majú k dispozícii praktické nástroje, kontakty a základné postupy.

Odolnosť nie je jednorazový krok, ale proces, ktorý sa buduje postupne.

Dlhodobej odolnosti pomáha napríklad:

- pravidelné vzdelávanie o digitálnej bezpečnosti,
- výmena skúseností medzi ženami, novinárkami, aktivistkami a miestnymi líderkami,
- podpora peer sietí a kontaktov dôvery,
- zdieľanie dobrých príkladov reakcie,
- budovanie spolupráce medzi médiami, občianskou spoločnosťou a odborníkmi,
- pomenúvanie škodlivých naratívov skôr, než sa stanú „normálnou“ súčasťou online prostredia.

Veľkú úlohu zohráva aj pocit, že v tom nie ste sama. Odolnosť neznamená, že človeka útoky prestanú bolieť. Znamená, že na ne nie je sám, rozumie im lepšie a má k dispozícii mechanizmy, ktoré znižujú ich dopad. Práve v tom je sila komunitného a organizačného prístupu.

Spoločná skúsenosť a podpora môžu výrazne znížiť dopad aj opakovaných útokov.

Verejný priestor *patrí aj vám*

Rodovo podmienené dezinformácie a online útoky majú často jediný cieľ: znížiť vašu istotu, oslabiť váš hlas a vytlačiť vás z priestoru, v ktorom máte právo byť prítomná. Cieľom útoku nie je diskusia, ale to, aby ste prestali hovoriť.

Táto príručka nevyrieši všetko. Môže však pomôcť získať väčšiu orientáciu, pripravenosť a oporu. Bezpečnosť nie je prejav slabosti. Je to podmienka toho, aby ľudia mohli hovoriť, pracovať a zapájať sa do verejného života bez strachu.

Silnejšia odolnosť nevzniká len individuálne. Vzniká aj cez solidaritu, pripravené organizácie, bezpečnejšie komunity a lepšie nástroje podpory. Práve preto má zmysel hovoriť o digitálnej bezpečnosti vecne, prakticky a bez zbytočného zľahčovania.

Čím viac ľudí je pripravených, tým menší dopad majú útoky.

Na útok nemusíte zostať sama. Verejný priestor patrí aj vám. A vaša bezpečnosť je jeho súčasťou. **Máte právo byť v ňom prítomná – a byť v ňom v bezpečí.**

MEMO 98 je nezávislá organizácia založená v roku 1998, ktorá sa venuje monitorovaniu médií, volebným procesom a boju proti dezinformáciám. Realizovala viac ako 150 projektov v približne 60 krajinách v spolupráci s partnermi ako OBSE, Európska únia, Organizácia spojených národov (OSN) či UNESCO. V posledných rokoch sa zameriava aj na výskum rodovo podmienených dezinformácií (vrátane spoločného výskumu v SR a ČR) a tvorbu praktických nástrojov na posilnenie odolnosti voči online útokom.

Bibliografia

MEMO 98 / Ženy v médiích. Gendered Disinformation in Slovakia and Czechia.
Dostupné na: https://memo98.sk/article/gendered-disinformation-in-slovakia-and-czechia
Access Now. Digital Security Helpline: FAQ.
Dostupné na: https://www.accessnow.org/help/helpline-faq/
Committee to Protect Journalists (CPJ). Digital Safety Kit.
Dostupné na: https://cpj.org/2019/07/digital-safety-kit-journalists/
Committee to Protect Journalists (CPJ). Safety Notes.
Dostupné na: https://cpj.org/safety-notes/
Committee to Protect Journalists (CPJ). Digital safety: Using online platforms safely as a journalist.
Dostupné na: https://cpj.org/2022/11/digital-safety-using-online-platforms-safely-as-a-journalist/
Center for Information Resilience (CIR). Holding Our Digital Ground: Addressing Gendered Disinformation During Elections and Beyond.
Dostupné na: https://www.info-res.org/cir/reports/holding-our-digital-ground-addressing-gendered-disinformation-during-elections-and-beyond/
Center for Information Resilience (CIR). Gender Lens.
Dostupné na: https://www.info-res.org/about-the-gender-hub/
PEN America. Online Harassment Field Manual.
Dostupné na: https://onlineharassmentfieldmanual.pen.org/
PEN America. Prepare for Online Harassment.
Dostupné na: https://onlineharassmentfieldmanual.pen.org/prepare-for-online-harassment/
PEN America. Federal Laws & Online Harassment.
Dostupné na: https://onlineharassmentfieldmanual.pen.org/federal-laws-online-harassment/
UNESCO. Online violence against women journalists: a global snapshot of incidence and impacts.
Dostupné na: https://www.unesco.org/en/world-media-trends/online-violence-against-women-journalists-global-snapshot-incidence-and-impacts
UNESCO. Safety of Women Journalists.
Dostupné na: https://www.unesco.org/en/safety-journalists/safety-women-journalists
UNESCO. How to combat online gendered disinformation? (Global Dialogue recommendations, 2023).
International Media Support. Digital misogyny: Why gendered disinformation undermines democracy. 2021.
United Nations (Irene Khan). Gender disinformation and online gender-based violence. Report of the UN Special Rapporteur on freedom of expression.
European Parliament. Women's rights and democracy: combatting stereotypes, disinformation, violence in the digital age. Briefing requested by the FEMM Committee. 2023.
UK Government. Quick Read: Gender and Countering Disinformation.
Organization for Security and Co-operation in Europe Office for Democratic Institutions and Human Rights. Addressing Violence against Women in Politics in the OSCE Region: Toolkit. Warsaw: OSCE/ODIHR, 2022.

— Addressing Violence against Women in Parliaments (Tool 2)
— Addressing Violence against Women in Political Parties (Tool 3)
— Support and Encouragement for Women in Politics (Tool 5)
— The Role of Civil Society and Women's Movements (Tool 6)
**UK Government. Quick Read: Gender and Countering Disinformation. **

Poznámka
Táto príručka je praktický orientačný materiál. Nejde o právne stanovisko, ani akademickú štúdiu. Text vychádza z verejne dostupných praktických manuálov, metodických materiálov a publikácií zameraných na online násilie, digitálnu bezpečnosť a ochranu žien vo verejnom priestore, vrátane verejne dostupnej správy MEMO 98 a Žien v médiích o rodovo podmienených dezinformáciách v slovenskom a českom prostredí. Zároveň čerpá z medzinárodných odporúčaní a výskumov organizácií ako OSCE, UNESCO, OSN či ďalších expertíznych platforiem zameraných na bezpečnosť novinárok, aktivistiek a verejne činných osôb.