Your *digital* safety

A GUIDEBOOK FOR WOMEN IN PUBLIC LIFE

How to Protect Yourself from Online Harassment, Manipulative Attacks, and Gendered Disinformation

Rasťo Kužel, MA
Marek Mračka, MA
Prof. Alexandra Bitušíková, PhD.

TABLE OF CONTENTS

3.....About This Guide and How to Use It
4.....What Is Gendered Disinformation?
5.....Why Is It a Problem?
6.....What Do These Attacks Look Like in Practice?
7.....Who Is Most Commonly Targeted?
8.....When Is It More Than Ordinary Criticism?
9.....What to Do in the First 30 Minutes After an Attack
10.....How to Document an Attack
11.....What Next: Ignore, Moderate, Report, or Escalate?
12.....Protect Your Accounts and Devices
13.....Protect Your Privacy
14.....How to Respond Publicly, and When Not To
15.....When an Attack Targets a Team or Organization
16.....Psychological Support Is Part of Safety
17.....When It Is No Longer Enough to Handle It Alone
18.....My Personal Safety Checklist
19.....Is Our Organization Prepared?
20.....How to Build Long-Term Resilience
21.....Public Space Belongs to You Too and About MEMO 98
22.....Bibliography

About This Guide and *How to Use It*

> *"Visibility must not mean vulnerability."*

This guide was developed as part of the project **Fighting Gendered Disinformation Online**, implemented by MEMO 98 with the aim of strengthening digital safety and resilience against online attacks.

The project was carried out with the support of the Embassy of the Kingdom of the Netherlands. The authors are solely responsible for the content of this publication, and the views expressed do not necessarily reflect those of the donors.

This guide is primarily intended for women who are active in public life or visible online. However, it may also be useful for organizations, newsrooms, civil society groups, and informal communities seeking to better protect people within their teams.

The purpose of this guide is to provide **practical guidance**: to briefly explain what gendered disinformation is, how it manifests in practice, what to do after an attack, how to protect your accounts and privacy, how to respond safely, and how to establish a basic prevention plan. The guide is designed as a practical resource — you can return to individual sections as needed, without having to read it from beginning to end.

This guide is based on the belief that **visibility must not mean vulnerability**. Public and online spaces should not be places where women and other vulnerable groups are afraid to express themselves freely because of the risk of attacks, intimidation, or humiliation.

> ***Tip:*** *You can also use this guide in a crisis situation - the individual sections are designed to be read independently (for example, only the section on the first 30 minutes after an online attack). If you find yourself in a situation that feels threatening or overwhelming, you can start there.*

Public and online spaces belong equally to women. We therefore do not see safety as an obstacle to participation in public life, but as a fundamental condition of freedom. This guide also offers concrete steps and recommendations to help actively strengthen that safety in everyday practice.

What Is *Gendered Disinformation*?

01

Gendered disinformation refers to false, misleading, or manipulative narratives that target a person or group based on gender, gender roles, sexuality, or stereotypes about what a woman "should be" and what place she "belongs" in society.

These attacks often present themselves as opinions, jokes, criticism, or simply "tough debate." In reality, however, they are not aimed at meaningful discussion, but at undermining a person's credibility, dignity, identity, and right to participate publicly. Such attacks do not target arguments, but rather appearance, voice, motherhood, sexuality, morality, femininity, "decency," or the "proper place of women in society."

> **Important:** *The goal of these attacks is not to win a debate, but to undermine your credibility, create pressure, and discourage you from speaking out further.*

Gendered disinformation is often intertwined with other harmful narratives. **It may form part of broader attacks against gender equality, human rights, civic activism, independent media, or publicly engaged individuals and institutions.** Sometimes these narratives exploit fears of alleged social change; at other times, they portray specific women as threats to family, tradition, stability, or moral values.

In practice, this is often not just a single comment, but a combination of multiple attacks — comments, posts, memes, and videos — that reinforce one another and increase pressure on the targeted person.

These are not merely verbal attacks. In reality, they can form part of a broader strategy aimed at making publicly active individuals less visible and turning public space into an environment where their voices are no longer heard.

As a result, people may begin to limit themselves — posting less, speaking out less often, or withdrawing from public space altogether.

Why Is It a *Problem*?

02

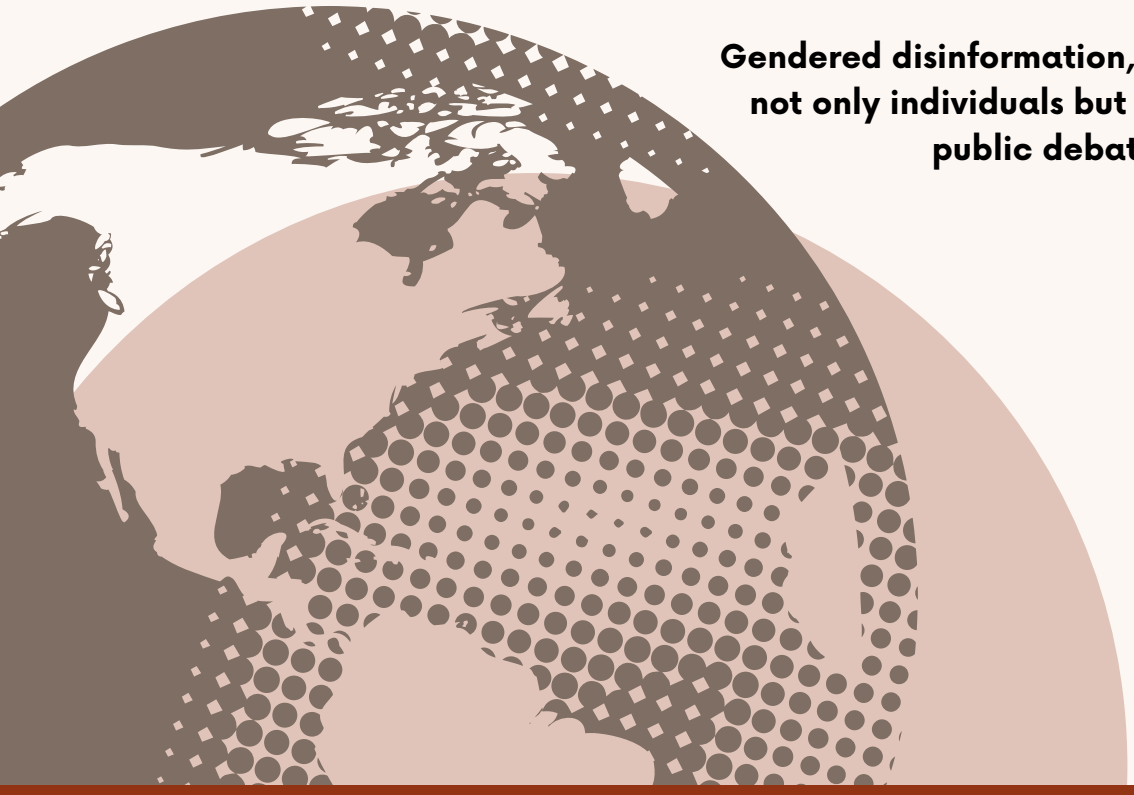
Gendered disinformation does not harm only one individual. Its aim is often to create a broader effect: to intimidate, exhaust, unsettle, undermine credibility, and discourage other women from speaking out publicly. The goal is not only to attack an individual, but to create an environment in which it becomes more difficult or risky for women and minorities to participate in public life.

> *"A person stops speaking not because they are forbidden to, but because it becomes too exhausting or too dangerous."*

A person who becomes the target of an attack may feel threatened, exhausted, humiliated, or under long-term pressure. They may begin to limit their public engagement, cancel public events, stop publishing, avoid topics that trigger attacks, or withdraw from online spaces entirely. This leads to self-censorship, which is not a free choice, but a reaction to a hostile environment.

This effect is often described as "silencing without prohibition" - a person stops speaking not because they are forbidden to, but because it becomes too exhausting or too dangerous.

When this happens repeatedly, it is no longer just an individual problem. It changes public discourse itself. When attacks silence women, journalists, experts, or activists, public space loses important voices, experiences, and perspectives. Pluralism is weakened, trust is eroded, and polarization deepens.



Gendered disinformation, therefore, affects not only individuals but also the quality of public debate and democratic participation.

What Do These Attacks *Look Like in Practice*?

03

These attacks can take many forms. Sometimes they involve individual comments or posts; other times, they are coordinated campaigns spanning multiple platforms. **In many cases, different forms of attack are combined in ways that reinforce one another.** This means that a single attack can quickly escalate into a broader campaign, especially once it begins to be shared or amplified by other accounts.

The Most Common Forms of Attacks

- mocking appearance, voice, or manner of expression
- sexualized insults and degrading remarks
- questioning expertise, intelligence, or competence
- labeling and portraying women as "puppets," "agents," or "threats"
- manipulating content through edited photos, memes, and quotes taken out of context
- moral judgments and aggressive attacks on private life
- coordinated pressure through organized comments and shares
- spreading falsehoods about funding, motives, or personal relationships
- exposing private information (doxxing) and intimidation through threats of revealing someone's identity

Some of these attacks may appear harmless at first glance (for example, as a joke or meme), but in reality they are often part of a **broader pattern of humiliation and degradation.**

In Slovakia, these attacks are often intertwined with ideological and geopolitical narratives. Women thus become targets not only because of what they say, but also because of what they symbolically represent: public engagement, the defense of rights, professional integrity, or the ability to critically challenge manipulative narratives. As a result, the attack often shifts from a specific statement to what the person is perceived to represent in the eyes of the attackers.

An attack often does not begin with an argument. It begins with a stereotype. And that stereotype is then used as a weapon.

Who Is Most Commonly *Targeted*?

04

The most common targets are women who are visible, active, and publicly engaged.

This typically includes women journalists, politicians, candidates, activists, experts, commentators, civil society workers, and women active in their communities.

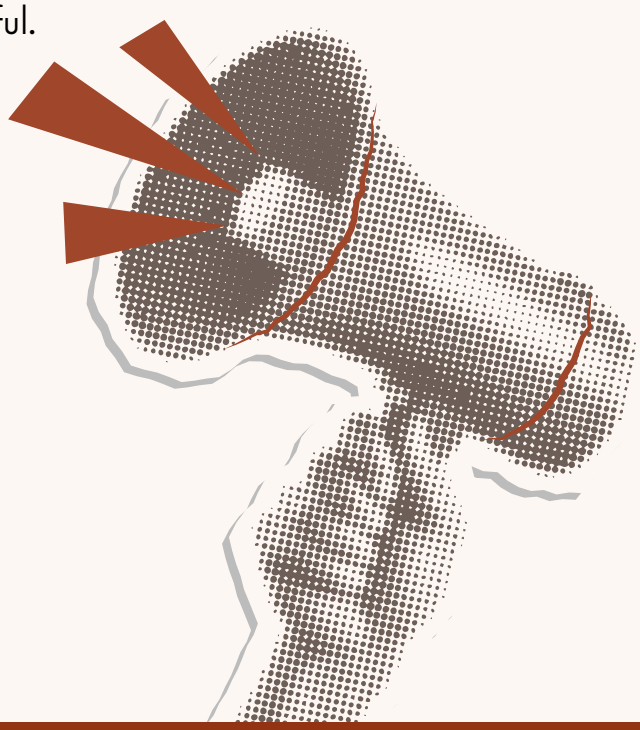
Women - but also men - who work on issues such as gender equality, human rights, reproductive rights, minority rights, corruption, extremism, or disinformation face particularly high risks. These topics are often highly polarized and frequently become a pretext for personal attacks.

However, gender-based attacks do not affect only women. **They can also target other visible or vulnerable groups, and sometimes men as well, especially when attackers rely on stereotypical ideas about how a "proper" man or woman should behave.** In practice, these forms of disinformation therefore affect a broader range of people whose public presence, identity, or views do not fit narrow stereotypical expectations.

People who stand out - for example because of their opinions, identity, or public stance - are particularly at risk.

This does not concern only well-known public figures. Attacks in local environments — whether within a community, campaign, or workplace - are often more personal and therefore even more hurtful.

Even subtle, long-term expressions of hostility should not be underestimated, as their consequences can be equally serious.



When Is It *More Than Ordinary* Criticism?

05

Not every harsh reaction is a coordinated attack. In public life, it is normal for people to disagree, debate, or even criticize sharply. **What matters is being able to distinguish between legitimate criticism and manipulative pressure, intimidation, or a targeted campaign.**

This distinction is important: not every criticism requires a response, but some situations require quick action.

The Most Common Warning Signs

- a large number of similar comments appear within a short period of time
- different accounts use identical or very similar wording
- the attack does not focus on what you said, but on who you are
- sexualization, humiliation, or moral judgment appear in the comments
- someone shares or hints at personal information
- the comments are intended to provoke shame, fear, or silence
- the attack spreads quickly across multiple profiles, groups, or platforms
- there are calls to "expose," ridicule, or punish the targeted person

If several of these warning signs appear at the same time, it is likely not ordinary criticism, but a coordinated or manipulative attack.

A useful guiding question can be: is the attack directed at what you are saying, or at who you are? Legitimate criticism focuses on an opinion, decision, or specific action. A manipulative attack, however, targets your identity, dignity, and your very right to be present in public space.

> **Quick test**: If you heard the same comment during a workplace meeting or a public discussion, would you consider it acceptable?

If you feel that the situation is not simply about disagreement, but about an attempt to intimidate, exhaust, or silence you, take it seriously. There is no need to wait for it to escalate further. **Your intuition matters - if you do not feel safe, that alone is a sufficient reason to act.**

What to Do in the *First 30 Minutes* After an Attack

06

> ***Important**: When an attack begins, it is natural to want to respond immediately. However, the best first step is usually to slow down and regain control of the situation. What you do in the first few minutes can significantly influence what happens next.*

Basic Response Steps

Stop → Save → Assess → Contact → Secure → Decide

Stop the Urge to Respond Immediately

Do not respond while in shock, anger, or panic. Even a short pause can help you avoid a reaction that might unintentionally amplify the attack under pressure. Even 10 or 15 minutes can significantly improve the quality of your response.

Save the Evidence

Take screenshots and save links, account names, timestamps, and the platform where the attack appeared. If the attack is spreading quickly, do not assume the content will remain online. Make sure your screenshots include the account name, date, and URL whenever possible.

Assess the Type of Attack

Ask yourself some basic questions: Is this an insult, coordinated harassment, a threat, the exposure of personal information (doxxing), an attempt to discredit you, or a sign of hacking? The type of attack determines the next steps, as not all situations should be handled in the same way.

Tell Someone You Trust

A colleague, editor, coordinator, friend, or another trusted person can help you assess the situation and support you through it. You do not have to handle it alone. Involving another person can reduce stress and lower the risk of making rushed decisions.

Check Whether It Is a Security Risk

If the attack includes threats, personal information, or signs that an account has been compromised, treat it as a security incident. In such cases, protecting your accounts, privacy, and physical safety should become the priority.

Decide on Your Response

Not every attack requires a public response. Safety comes first, communication second. Any response should be thoughtful and deliberate, not rushed under pressure.

How to *Document* an Attack? 07

A well-documented incident is easier to address. It can help with internal reporting, communication with platforms, and the consideration of possible legal steps.

The more precise your evidence is, the easier it becomes to assess and respond to the situation.

For Every Incident, Try to Save

- a screenshot or screen recording
- the exact link to the content
- the date and time
- the name of the profile, page, or group
- the platform where the attack appeared
- a brief description of what happened and why it is problematic
- information on whether the attack is recurring or spreading further
- notes on whether threats, personal information, or signs of coordination appeared

Tips

- Make sure your screenshots include the account name, date, and ideally the URL address as well.

- If the incident involves multiple posts, create a simple incident log. This can be a spreadsheet, a document note, or a folder containing evidence. The important thing is to be able to track the scope, intensity, and development of the attack over time. Even a simple list (date – what happened – where – who) can help you maintain a clear overview.

- Store evidence outside the platform itself. Content may be deleted, reported, blocked, or altered. Ideally, keep copies saved on a device or secure storage location that only you can access.

What Next: *Ignore*, *Moderate*, *Report*, or *Escalate*?

08

Not every attack requires the same response. Sometimes it is enough not to engage or to hide a comment. In other cases, it is necessary to involve your team, document the situation, contact the platform, or proceed with formal reporting. **There is no single correct response — what matters is choosing an approach that matches the seriousness of the situation.**

A simple series of questions can help guide your decision:

Is it just a single insult without a broader impact?

If so, it is usually enough to not respond, hide the comment, or block the account.

Is it recurring or spreading in a coordinated way?

If so, document the situation and involve your team or organization. Monitor whether it may be part of a deliberately amplified campaign. In cases of repeated attacks, it is important not to leave the situation unaddressed and to begin tracking it systematically.

Does it contain threats, personal information, or signs of doxxing?

If so, this should be treated as a security incident - escalate the situation immediately and involve additional support. Do not wait; act right away.

Does it impact your work, reputation, or psychological well-being?

If so, do not handle it alone. Seek support, use internal mechanisms, and, if necessary, professional help. Psychological impact alone is a sufficient reason to address the situation.

Is a Public Response Helpful?

A public response is generally appropriate if it can help calm the situation, identify the manipulation, or protect others. However, it is not always necessary. Sometimes the best response is not to engage and not to amplify the attack further. One basic rule applies: if the situation involves threats, doxxing, hacking attempts, or targeted intimidation — act immediately. If you are unsure, consult someone about the situation. It is always better to seek advice than to underestimate the risk.

Protect Your *Accounts* and *Devices*

09

Digital safety does not begin only after an attack occurs. It starts beforehand — with basic settings and habits that reduce the risk of hacking, account takeover, or misuse of personal information.

Prevention is the simplest way to reduce the impact of a potential attack.

The Basic Minimum Includes

- strong and unique passwords for every service
- two-factor authentication
- regular updates of your phone, computer, and applications
- checking logged-in devices and active sessions
- caution when dealing with suspicious messages, links, and attachments
- separating private and public accounts
- regularly reviewing who has access to your accounts

If you use the same password in multiple places, a single breach can put several accounts at risk at once.

If you are facing online attacks, account security is not just a technical detail — it is part of your protection. In some cases, disinformation campaigns may be followed by technical attempts to compromise accounts, misuse login credentials, or carry out other forms of attack. An attack on your reputation can quickly turn into an attack on your accounts or privacy.

Whenever possible, use a password manager and carry out a brief security check from time to time. Two minutes of prevention today can save hours of stress later. Every few months, take a moment to review your account settings and make sure everything is up to date and secure.

Protect Your *Privacy* 10

During online attacks, the vulnerable point is often not only the content you share, but also the information about you that can be easily found online.

That is why it is worth carrying out a basic privacy audit. Attackers often rely on publicly available information - they do not necessarily need to "hack" anything.

Check the Following:

- What contact information is publicly available?
- Can your address or place of residence be found online?
- What information can be discovered about your family, children, school, or daily routine?
- Do photos reveal your location, car, home, or workplace?
- Which older posts may unnecessarily increase your risk today?
- Which accounts or applications have access to your personal data?

> *Tip: Try googling yourself and review what information about you is publicly available.*

The goal is not to disappear from online spaces. The goal is to limit the amount of information that can be misused for intimidation, doxxing, or reputational attacks. The less information that is publicly available, the fewer opportunities there are for abuse.

One simple rule can also help: **share consciously. Not everything that is true needs to be public.** This is especially important when it comes to information about your family, children, travel, exact location, or daily routine. In particular, when sharing in real time (for example from a vacation or from home), consider whether it is safe to do so.

Whenever possible, separate your professional and private contacts. If an attack spreads into other areas of your life, this separation can help you respond with greater distance - and greater peace of mind. Keeping contacts separate gives you more control over who can contact you and how.

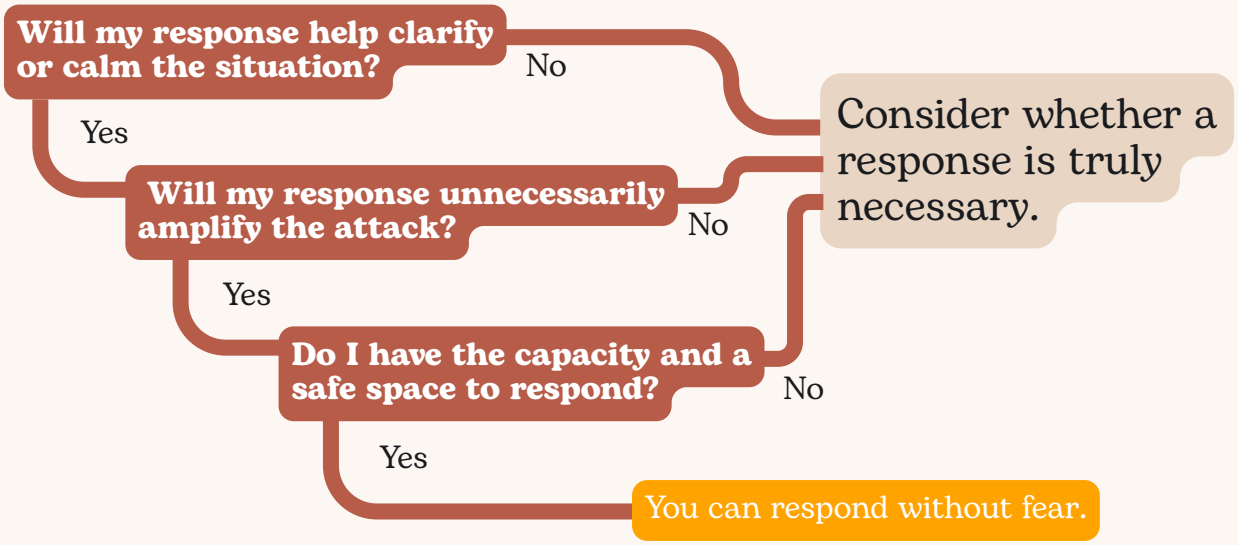
When to *Respond Publicly*, and When *Not To*

11

Not every attack requires a public response. Sometimes the best reaction is not to respond at all. In other situations, a brief and factual acknowledgment of the manipulation may help. What matters most is that your response protects you — not the logic of the attack.

The purpose of a response is not to convince the attacker, but to set boundaries and protect yourself (and potentially your audience as well).

Before responding, ask yourself three questions:



A good response does not need to be long. It needs to be safe, accurate, and intentional. And sometimes, the best response is choosing not to play the game set by the attackers. Deciding not to respond is also an active and legitimate choice.

If You Decide to Respond, Follow These Principles

- respond only after taking a short pause
- stick to the facts
- do not endlessly justify your dignity or your right to be present in public space
- do not respond to every comment
- when appropriate, allow your organization, newsroom, or team to speak as well
- if the goal of the attack is to provoke you, do not let yourself be drawn into the game

When an Attack Targets a *Team* or *Organization*

12

If an attack affects not only one individual, but also an organisation, newsroom, or campaign, it is extremely helpful to have at least a simple agreed procedure in place. Under stress, decision-making becomes more difficult, and chaos increases pressure not only on the targeted person, but on the entire team as well.

A procedure agreed upon in advance reduces stress and helps speed up the response.

It Is Important to Know:

- who monitors the situation
- who archives evidence
- who communicates externally
- who stays in contact with the affected person
- who handles the technical security of accounts
- who decides on escalation and further steps

When it is clear who is responsible for what, the situation can be handled more calmly and without unnecessary pressure on individuals. In the case of a more serious attack, it is important that the targeted person does not have to carry the entire burden alone. **An organization can help by taking over monitoring, sorting comments, preparing responses, communicating with platforms, or assessing whether legal or psychological support should be involved.**

One of the most valuable forms of support is sharing responsibility — so that the targeted person does not have to manage everything alone. **An effective team procedure does not need to be complicated.** What matters is that it is thought through in advance, understandable, and practical to use. Crisis communication is not only about making a public statement. It is also about how tasks are divided within the team, how pressure is reduced, and how the person under attack is protected.

Even a simple internal document can significantly improve a team's preparedness.

Psychological Support Is Part of Safety

13

An online attack can cause shock, anger, exhaustion, shame, fear, or helplessness. These reactions are normal. They are not a sign of weakness. They are a natural response to hostile and distressing behavior.

Everyone reacts differently - there is no "right" way to feel.

What May Help:

- turn off notifications and create some distance
- limit how much you read comments
- ask someone else to monitor the situation
- talk to a trusted person or colleague
- seek professional psychological support
- avoid blaming yourself for the attack
- make sure you get sleep, movement, and maintain basic daily routines, even during stressful periods

Even a short break from online spaces can significantly help reduce stress.

An attack that takes place online can have very real offline consequences. Long-term pressure, hatred, and the feeling of being constantly watched can affect mental health, concentration, and the ability to work. Prolonged exposure to attacks may lead to exhaustion or burnout. **It is okay to slow down and give yourself space.**

The fact that an attack affected you does not mean you failed. It means that it was an attack. Psychological support is also part of a responsible response. It is not something extra - it is part of protection. Taking care of yourself is not a weakness; it is part of your safety.

When It Is *No Longer Enough* to Handle It Alone

14

Some incidents can be managed through moderation, blocking, or internal support. Others require broader assistance.

It is not your responsibility to handle everything alone.

Consider Seeking Additional Help If:

- the attack contains threats
- personal information has been exposed
- the situation involves stalking or repeated intimidation
- there are signs of hacking or account takeover
- the attack affects your family, children, or colleagues
- the attack has a serious impact on your mental health or work
- the situation exceeds your or your team's capacity to handle it

If you are unsure whether the situation is "serious enough," it is completely okay to seek advice.
External support can take many forms. It may include legal assistance, IT security support, psychological help, or contacting the police in cases involving threats, stalking, the exposure of personal information, or another serious incident.

Seeking help does not mean you are unable to cope with the situation - it means you are handling it responsibly.

It is not always easy to decide whether to report something. Many people have experienced not feeling heard or receiving help too late. However, this does not change the fact that serious threats should also be considered from a formal and legal perspective.

What matters is having support, not facing the situation alone, and proceeding as calmly and systematically as possible. Even small steps - such as consulting someone, saving evidence, or speaking with a professional - can be the beginning of a solution.

My Personal *Safety Checklist*

15

Go through this checklist and mark what you already have in place and what still needs to be improved.

You do not need to have everything completed - the goal is to understand where you are now and what your next step should be.

- ☐ I use strong and unique passwords.
- ☐ I have two-factor authentication enabled.
- ☐ I know who can help me with a technical problem.
- ☐ I keep my private and public accounts separate.
- ☐ I know how to save evidence of an attack.
- ☐ I know when to ignore an attack and when to escalate it.
- ☐ I limit the amount of personal information available about me online.
- ☐ I know who to contact if something happens.
- ☐ I do not face online attacks alone.
- ☐ I know where to seek psychological or legal support.

This checklist is not a test. It is a practical guide. You do not need to solve everything at once. What matters is understanding where you are today and gradually building greater confidence and preparedness.

Safety is often built through a series of small steps.

Even small changes in your account settings or daily habits can make a significant difference.

Is Our *Organization* Prepared? 16

Online attacks are not just an individual problem. An organization can significantly influence whether a person feels protected or isolated.

The way an organization responds has a direct impact on whether someone feels safe or under pressure.

As a team, try going through this basic checklist:

- ☐ Do we have clear rules defining what is considered an incident?
- ☐ Do we know who monitors and archives attacks?
- ☐ Do we have agreed escalation thresholds?
- ☐ Do we know when to contact the police or seek professional assistance?
- ☐ Do we protect the targeted person from overload?
- ☐ Do we have a basic crisis communication plan?
- ☐ Do we have minimum security standards for accounts and devices?
- ☐ Do we have a way to filter hateful comments?
- ☐ Are we able to provide psychological or peer support?
- ☐ Do we learn from incidents and continuously improve our procedures?

If you answered "no" to several of these questions, this is a good moment to start with simple steps.

You do not need a complex security manual. Even a simple internal document that clearly defines who is responsible for what, how evidence is stored, and when situations should be escalated can make a major difference. A short and understandable document can significantly improve a team's preparedness.

A prepared organization will not solve everything. However, it can greatly reduce chaos, speed up support, and show people that they are not facing attacks alone.

Support from the organization is crucial - no one should have to face attacks on their own.

How to Build *Long-Term* Resilience

17

Responding to an incident is important, but long-term resilience is equally important. Resilience is not built only on an individual level. It grows in environments where people are able to recognize harmful narratives, support one another, and have access to practical tools, trusted contacts, and basic procedures.

Resilience is not a one-time step, but a process that is built gradually.

Long-Term Resilience Can Be Strengthened Through

- regular education and training on digital safety
- sharing experiences among women, journalists, activists, and local leaders
- supporting peer networks and trusted contacts
- sharing good examples of effective responses
- building cooperation between media, civil society, and experts
- identifying and naming harmful narratives before they become a “normal” part of the online environment

A strong sense that you are not facing the situation alone also plays an important role. Resilience does not mean that attacks stop being painful. It means that a person is not left alone to face them, understands them better, and has access to mechanisms that reduce their impact. This is where the strength of community and organizational approaches lies.

Shared experience and mutual support can significantly reduce the impact even of repeated attacks.

Gendered disinformation and online attacks often have a single goal: to undermine your confidence, weaken your voice, and push you out of spaces where you have every right to be present. The purpose of the attack is not discussion - it is to make you stop speaking.

This guide will not solve everything. But it can help provide greater clarity, preparedness, and support. Safety is not a sign of weakness. It is a condition that allows people to speak, work, and participate in public life without fear.

Stronger resilience is not built only individually. It is also built through solidarity, prepared organizations, safer communities, and better support mechanisms. That is why it is important to speak about digital safety in a practical, clear, and serious way - without downplaying the problem.

The more prepared people are, the smaller the impact of attacks becomes.

You do not have to face attacks alone. Public space belongs to you too. **And your safety is part of it. You have the right to be present in that space - and to be safe in it.**

MEMO 98 is an independent organization founded in 1998 that focuses on media monitoring, electoral processes, and countering disinformation. It has implemented more than 150 projects in approximately 60 countries in cooperation with partners such as the Organization for Security and Co-operation in Europe, the European Union, the United Nations, and UNESCO.

In recent years, MEMO 98 has also focused on research into gendered disinformation (including joint research conducted in Slovakia and the Czech Republic) and on developing practical tools to strengthen resilience against online attacks.

Created with the support of the Embassy of the Kingdom of the Netherlands.

Kingdom of the Netherlands

Bibliography

MEMO 98 / Ženy v médiích. Gendered Disinformation in Slovakia and Czechia.
Available at: Gendered Disinformation in Slovakia and Czechia
Access Now – Digital Security Helpline: FAQ
Committee to Protect Journalists (CPJ) – Digital Safety Kit
Committee to Protect Journalists (CPJ) – Safety Notes
Committee to Protect Journalists (CPJ) – 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
Center for Information Resilience (CIR) – Gender Lens
PEN America – Online Harassment Field Manual
PEN America – Prepare for Online Harassment
PEN America – Federal Laws & Online Harassment
UNESCO – Online Violence Against Women Journalists: A Global Snapshot of Incidence and Impacts
UNESCO – Safety of 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)

Note
This guide is a practical reference resource. It is not a legal opinion or an academic study. The text is based on publicly available practical manuals, methodological materials, and publications focused on online violence, digital safety, and the protection of women in public space, including the publicly available report by MEMO 98 and Ženy v médiích on gendered disinformation in Slovakia and Czechia.
It also draws on international recommendations and research by organizations such as the Organization for Security and Co-operation in Europe, UNESCO, the United Nations, and other expert platforms focused on the safety of women journalists, activists, and public figures.