

The newsletter "Where Do We Draw the Line?" returns with several special editions. In these editions, we will provide a series of practical guides on how to better manage security issues that can affect your organization and the well-being of journalists. In today's edition, Mykola Kostynyan, a digital security consultant, will guide us through the **types of cyberbullying that journalists may experience** and explain how these can pose security risks.



Mykola Kostynyan
digital security consultant

In security theory, risk is defined as an undesirable event that causes real problems and can hinder the achievement of one's goals. Many risks are intentionally caused by someone, especially when they are repeated constantly. These risks can feel like a form of harassment for journalists. Below, we have selected a few examples that occurred to journalists in Moldova during the election period and paired them with advice.

But first of all, **how can we distinguish real risks from "online noise"?**

There are two important parameters of risk: probability and impact. Only the organization can decide how significant a risk is for itself based on these parameters. If a risk makes it impossible for us to operate, then it is significant. Therefore, only we can determine what is real and what is "noise." If a risk affects our operations, then it is real. If we can live with it, however, we may postpone addressing it. For this reason, conducting a risk assessment is useful. You will find some tips on when and how to do this towards the end of the newsletter.

Case 1: What should we do if we find out that our social media pages have been cloned?

When something happens to us on social media, the first thing we should do is report the problem through the platform's internal reporting mechanisms. In the explanation section, we should emphasize that we are a media organization that deserves more attention in this case because we play an important role in society. Additionally, we should seek help from [Access Now](#). The organization has direct contact with major platforms and can expedite our case.

As a preventive measure, it would be helpful to implement meta verification badges so users can more easily distinguish between fake and real accounts. We can also encourage our audience to report fake pages.

In this case, the risks are reputational damage and data leakage if fake accounts request confidential information or documents from someone on behalf of the organization. Cloning could also target journalists' personal pages, for which we follow the same steps.

Case 2: What should we do if our website is cloned?

When it comes to websites, the first thing we look at is the domain name. If there is a site administrator in the editorial office, they can search for the domain name and find its registrar. Next, we identify the web hosting company. While we may not be able to determine this, we could identify that the clone website uses Cloudflare's service, for example. The next step would be to have a lawyer help us draft a request to suspend the website's activity due to abuse and copyright infringement. We can send this letter to Cloudflare or the web hosting company. Even if they are unable to suspend the website, they could blacklist it. Then, when users access the website, they would receive a notification that it is suspicious.

If there is no internal capacity, we can call Access Now or another security service for assistance. The risk in this case is also reputational, but these clones may distribute viruses that infect the computers of those who access them.

In both cases, it is important to communicate these issues to the audience via official channels.

Case 3: How should we respond to emails impersonating authorities or other official organizations?

This is an example of a specific type of cyberattack: phishing. In such an attack, we are typically required to take action, such as accessing a link, downloading something, or opening a file on our computer. Phishing attacks can compromise control of our email or Google Drive accounts and infect our computers with viruses. While these emails are easy to spot at this stage, we must understand that this form of attack is becoming increasingly sophisticated. Phishing is extremely dangerous, and we expect to see more cases like this in the region.

This attack involves psychological and technical aspects. To combat the technical aspect, we must protect our accounts in ways that render phishing ineffective. For example, we can enable multi-factor authentication that includes a security key. Two-step authentication alone is not enough to prevent phishing.

It is equally important to educate team members every six months by providing fresh examples, discussing them, and explaining the signs of suspicion. If you have limited resources but still want to organize security training in your organization, it should focus on phishing because it can occur not only via email but also on messaging services such as Signal, WhatsApp, and Telegram.

Suspicion should arise when we receive an emotional message that frightens us with something, offers us something, for example—exclusive information for an investigation. Newsroom staff need to know how to proceed if they receive such messages. First, they should not interact with the sender. Instead, they should show the message to someone in the newsroom who has more knowledge in this area. While we cannot fully train people to distinguish real messages from fake ones, we can train them to identify suspicious messages. If someone in the newsroom encounters such a case, they should discuss it with the entire team because there is a high probability that colleagues will receive similar messages.

One preventive measure would be to ensure that everyone has access to the latest versions of Windows, Mac, iOS, and Android. All applications must be updated, and unlicensed programs should be avoided. It would also be wise to use corporate antivirus software with a centralized control panel. Through this panel, a designated person could monitor the organization's computer security issues in real time.

Case 3.1: What should we do if someone takes control of our social media accounts or email?

A takeover can only occur through phishing. If emails are secured with multi-step authentication and a security key, as well as Google Advanced Protection, messenger apps cannot be protected with a security key. To prevent this, we need at least two-factor authentication and to educate people through examples. If a takeover has occurred, we can also call on the [Access Now](#) organization for help.

Which platform is the most vulnerable?

The team communication platform should fit the pace of work. First, we choose the platform according to our goals. Then, we make sure to protect it. For Slack, for example, it is a good idea to have a centralized corporate system with a single registration. This way, team members won't need to create separate passwords and logins; they can connect with their Google account, which may be protected by multi-factor authentication.

The most vulnerable platform is the one containing the most important information that we want to protect.

Case 4: How should we respond to coordinated attacks by trolls on social media?

We report troll activity when possible because, in some cases, the platform can detect and shut down their networks. While troll activity does not pose an immediate risk, they could develop their networks, gain certain skills, understand the history of interactions on our account, and create extensive reports that could affect our visibility. This would constitute a direct attack on the organization's operations. Therefore, we should be alert to signs of sudden drops in interactions, views, etc.

Bonus: How do we conduct a risk assessment?

The first step in managing risk within an organization is risk assessment. Encompassing all types of security, it is typically carried out by the management team, though external consultants may also facilitate it. However, management must make the decisions. First, we will define and understand what we want to protect.

The assessment will take place annually. As a result, we must compile a prioritized list of risks for resolution. Risk management may include actions such as prevention, reduction, avoidance, acceptance, transfer, and others.

Then, we will develop a plan to implement the chosen measures. Once the plan is implemented, we can say that we have begun improving the relevant security measures. Next, we will monitor and evaluate the plan to determine its effectiveness.



Opportunity!

1. Google Workspace for nonprofit organizations is now available in Moldova.

With this option, you can create a corporate email system and control the security of your team members' email accounts. You can activate security measures for them, control access, and manage sharing options on Google Drive. [Check the option here.](#)

2. The Association of Independent Press offers consulting services to independent regional and national newsrooms across the country that are facing cybersecurity risks and other issues related to information protection and online security. [Click here](#) for details.



Get Help!

If you are experiencing ongoing stress and anxiety, you can request a free and confidential consultation with a psychologist using [this chatbot](#) or by filling out [this form](#). You will be connected with a specialist within 48 hours.

If you liked what you read, please recommend our newsletter to a colleague. Feedback helps us get better. Let us know what you think about the newsletter at api@api.md.



This newsletter was produced with the financial support of the European Union. Its content represents the sole responsibility of the "TRIMEDIA - Trustworthy reporting, impactful media, engaged communities" project, financed by the European Union and co-funded by the German Federal Ministry for Economic Cooperation and Development (BMZ). The content of the material/publication/video belongs to the authors and does not necessarily reflect the vision of the European Union.

Follow us: [Facebook](#), [Instagram](#)
[Unsubscribe](#)