

Your phone is the first thing you pick up when you wake up and the last thing you put down when you go to bed. It's a digital copy of your daily life, with personal and work information often mixed in with private or shared conversations. Some of the information we deal with on a daily basis becomes public, and what becomes public about us is of interest to us because every cyber-attack starts with **open source information**.

In this issue, we talk about the digital hygiene that every journalist needs to work safely.

“Young journalists starting out in investigative reporting have the hardest time coping with stress.”

Following an investigation published a few years ago, she was confronted with a huge wave of hate and messages attacking her personally. In another case, she was stalked and intimidated. For **Liuba Sevcluc**, these episodes came at a time when she was already experienced, which helped her overcome the challenges more easily. But the support of her managers made all the difference, and she advises all newsrooms to offer that support when their journalists are under attack. In her 17 years of journalism, Liuba has been part of several journalistic teams at Publika TV, Radio Free Europe, and Rise Moldova. Five years ago, she founded and still runs the investigative journalism project “Cu Sens,” which gives her the experience to guide young investigative journalists through the risks of the profession.

“Cu Sens” does video journalism, and from the start that means more exposure than other types of journalism. It is harder to protect your identity, and you have to take risks. However, Liuba says that she and the team try to keep as little information about their personal activities on their personal social media accounts as possible. “Instead, we use our social media pages to promote the materials we produce.”

Young journalists starting out in investigative reporting have the hardest time dealing with the stress, Liuba explains. “First, because investigative material is complex and requires more depth to analyze the data and make connections between them; second, because when you work with video, you are physically exposing yourself to the characters you are writing about, and 90 % of the time, the people you are interviewing don’t want to talk to you. That usually means you’re doing stories where the characters in your journalistic material have a negative attitude. This can be quite traumatic for less experienced colleagues, but we try to train them as much as possible. The more often they go out in the field, the more they develop a certain immunity, and they react differently to the next shoot.”

Liuba and her colleagues have a set of rules they follow in the newsroom. “When we talk about online security, everyone has two-step authentication enabled, two recovery emails, antivirus programs. We don’t use unlicensed software, we only talk on Signal, which is a secure chat, we don’t click on dubious links, and we change our passwords regularly. When we have more sensitive information, we use encrypted email to send it. For certain sensitive documents, we work offline. It all depends on how sensitive the information is. We don’t have to be paranoid either, because fortunately Moldova is still quite safe and we can do investigative journalism safely.” On field trips, Liuba says it’s important that another person from the newsroom accompany the reporter. Reporters are also always monitored by the newsroom when they go on such trips, and they are trained on how to react if they are in danger. “If everyone follows these rules, things go a little smoother.”

The most common pressure on investigative journalists in our country is being sued, Liuba says. In such situations, it is necessary to have the newsroom’s support, which has to provide journalists with legal assistance. At the same time, it is also difficult for the newsroom because a court case takes time and money. “We have won all such cases so far but it’s hard for a newsroom that’s barely surviving on grants to go through courts with dozens of cases.”



Mykhailo Koltsov
 Ukrainian cybersecurity expert

Five good things to know about your data

Distinguish between private and public life

It can be challenging for a journalist to separate his or her private life from their public life, because being a public figure is part of the job. However, it is important to learn how to protect certain information. One of the biggest mistakes is to try to communicate in the same environment with both people close to you and people in your work environment. You need to separate your communication media. Use one platform for personal communication, another for communication with colleagues, and another for communication with sources.

Be careful where and how you share your personal information

If a service is free, it does not mean it is really free; it just means you are paying for it in some other way. Open source is the best way to get information about you. Be careful about what you share and how you share it to avoid becoming vulnerable to potential attacks. A journalist can expect someone to know your address, phone number, activities and location, and this information can easily be turned into a physical threat.

Security is not free, but that does not mean we have to pay for it

It is important to evaluate the digital tools that help you communicate and understand which ones are worth paying for and which ones are fine with the free versions. If we are talking about data storage, it is important to be able to retrieve your data quickly, so you need cloud services (iCloud or Google Drive) that you should pay for. Another example is Proton email, which is very good for private communication, but it is a paid service. However, it can be complicated to use because both you and your source have to be Proton users. A valuable tool worth paying for is the physical security key, which acts as a secondary authentication factor. Even if someone knows your password, they would not be able access your accounts without this stick.

Maintain security hygiene

The first tip is to try to use a secondary authentication factor whenever possible. The second tip is to always create backups, as it is important to be able to quickly access your data. The third tip is to use as few communication platforms as possible in your work. If you use too many platforms and applications, you become vulnerable, not because of you, but because of the vulnerabilities of those platforms. The fourth tip is to always check what you share, especially personal information. Check your social applications and find out what kind of information is visible in your accounts, because every cyber-attack starts with information available in open sources. The fifth tip is to be aware of suspicious activity on the Internet. Phishing (a cyber-attack that steals your personal information) is the main way databases are hacked. The only way to protect yourself is to avoid clicking on dubious links.

Communicate using secure platforms

- Signal – Good for communicating with sources.
- WhatsApp/Messenger – Suitable for personal communication.
- Viber – Useful for personal communication, but inconvenient to use due to the large number of ads.
- E-mail – Gmail or Outlook accounts are safe to use. Other email services that do not have two-factor authentication, protection algorithms, and teams that monitor suspicious activity and protect you from exposure are not safe.

Where does Telegram rank?

Telegram can be used for both work and personal communication, as long as you do not exchange sensitive information, because it has some security issues. One of them is the lack of an account and data recovery mechanism. Even though it has two-step authentication, it only consists of an additional password which does not provide a very high level of security.



We explain

OSINT (open-source intelligence) – a method of collecting and analyzing information from open and public sources. These sources can include information available on the Internet, in the media, in public documents, and on social networks, and are used by governments, security services, journalists, business people, and researchers.



Useful tip!

Three criteria that define a secure communications platform
 You need to make sure that the application you are using has end-to-end encryption. The second thing to check is whether the platform offers a timer, i.e. whether you can control how long the message is available after it has been sent. You also need to be aware of the information that the platform collects about you and understand that it should not collect sensitive information such as your address, fiscal code, etc.



Opportunities!

- Media and civil society organizations working on human rights and digital security can receive grants of up to €17,000 to strengthen their organizational capacity. Read more [here](#).
- Local media outlets in the North, South, Center, ATU Gagauzia and Transnistrian region can receive grants worth €6000 to produce quality media content on issues such as social cohesion, defense of human and minority rights, and fight against corruption. Read more [here](#).

If you'd like us to include one of your announcements or opportunities for journalists that fit into the topics of this newsletter, send us a message at info@api.md.



Get Help!

Ask for 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 to 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.



Funded by the European Union



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.

