COVID-19 and digital security: How to organise safe Prides online?

Blog, Covid-19, Pride, Security

> This year, Pride Month will be like no other. Despite the current challenges, it remains as the opportunity of coming together for equality and celebrating our diversity. Many organisations are getting ready for this important month of visibility by organising digital events. Are you wondering how your organisation can prevent possible attacks online this month? ILGA-Europe Programmes & Policy team shared some possible scenarios and tips for you!

With the new physical limitations to manifesting our freedom of expression and making our presence visible, most of our work has moved to online spaces which brings its benefits, but also entails an increased risk of digital security breaches. In recent weeks there have been increased indications that **Pride organisers might be subject to online attacks in a more organised and active manner.**

ILGA-Europe Programmes & Policy team has selected a few of the most likely possible attacks online which could be used to stop or hinder your work. Find out what they are and what you can do to prevent and mitigate them, as well as some ally organisations which might be helpful.

1. Cyberbullying, including cybertrolling and attacks on users profiles online

Individuals, usually using fake accounts or digital identities which cannot be traced to real persons, comment or post negative, or fake information to diminish the importance of your work by shifting the focus and instilling fear. Recently, a Twitter user flagged the plans of the 4chan group.

What you can do as organisers is to discuss this scenario in advance and come up with response strategies; it could be ignoring these messages altogether, deleting or diluting them with supportive messages.

2. Taking down your online resources such as websites and social media pages

These could be done by massively reporting your resources (as having violated the rules of the hosting space) or by the so called DDoS attacks on websites done through simple software available online.

A solution is to create backups with all the content of the website and pages so that it can be restored quickly on your own or alternative pages (these should also be created in advance).

Talk to your hosting providers, informing them that such a scenario is possible due to increased visibility of your group and issues. If the hosting company is international, it might be possible to look into cross-border work on this issue.

3. Attempts to get access to your internal digital resources such as e-mails, cloud storage, organisational servers, and more

This can be done in multiple ways, from phishing attempts to picking weak passwords of team members.

There is quite a lot of information online on how to prevent these types of attacks, but you should not underestimate the need to pay close attention to these types of attacks as they are still some of the most efficient tricks used by our opponents.

Here you can find a useful toolkit that offers a brief and clear visual representation on potential scenarios and ways of preventing and mitigating those.

As general tips, we suggest the following steps:

- **Develop a brief protocol of actions** in case of the above scenarios and inform your teams.
- **Create back-up content for social media pages**; create alternative pages that can immediately replace those taken down.
- **Reach out to local digital security experts and ally organisations or international allies** such as AccessNow's helpline for urgent and complex situations.