

Cybersecurity at the Olympics

February 18, 2026

Interview with Matteo Rizzi who, with the FBK Center for Cybersecurity, is focusing on the area around Milan-Cortina where hacker attacks on institutions, service centers, and small businesses are on the rise.

These are generally cyberattacks carried out with the intention of creating chaos, making institutional and government websites (38%), Olympic organizations (24%), and critical infrastructure (12%) unavailable. In the opening week of the Olympics alone, from February 2 to 8, 8,000 attacks were recorded across Europe: 42.9% of these occurred in Italy.

These are not actions aimed at stealing data, at least for now, *“but I don’t think these hackers would hesitate if they found a way,”* explains **Matteo Rizzi, Science Ambassador and Security Administrator at the FBK Center for Cybersecurity.**

Rizzi, why does a major event like the Winter Olympics become a prime target for hacktivist groups? And who are these “hacktivists”?

For the most part, Russian hackers are claiming responsibility for the attacks: independent groups driven by geopolitical motives, particularly to protest funding for Ukraine and Russia’s exclusion from the Olympics. Their goal is to gain visibility while demonstrating their strength: they do this by targeting institutional websites or critical infrastructure.

What kind of attacks should we expect?

These are actions aimed at creating disorder, inefficiencies, and making certain services unavailable.

They affect, for example, industrial automation systems, such as those used to regulate heat pumps or turbines, throwing hotels and hospitality facilities like Olympic villages into disarray. Often these systems are not up to date, and a misconfiguration is enough to expose them to risk. Another vulnerable target is CCTV cameras in public and institutional places.

How does FBK support the local area and institutions in preparation for Milan-Cortina 2026?

At Fondazione Bruno Kessler, we have a **Joint Laboratory between the Center for Cybersecurity and the Digital Solutions and IT Infrastructure Service** that manages cybersecurity-related risks, particularly technical risks, through continuous real-time monitoring of the situation. With regard to human risk, the **Joint Lab** conducts training and awareness initiatives for local companies and institutions on potential attacks.

We have seen, in fact, that many of these attacks involve **human error**: an email, a click on the wrong link. It is therefore important to raise collective awareness, warn about dangers, and educate users.

What concrete measures should a company take today to reduce risk?

Italy is made up of small and medium-sized enterprises, which can easily become targets.

The **advice** we give focuses on two fronts: the human side—being very cautious, especially if you are in the Milan-Cortina area—and the technical side. If companies feel they do not have sufficient tools to deal with these attacks, they can rely on larger providers (there are many, even free) that act as a shield by absorbing malicious traffic, serving as a real filter in the case of spam requests.

How can an organization prepare for a possible attack without creating alarm?

Mindfulness matters: the eyes of the whole world are focused on the Olympic area, and knowing you are a target is already a good part of the job—it naturally leads to staying alert and implementing defenses.

Will you be following the Olympics? Any particular discipline?

Not very much; I catch a few moments here and there. I really enjoy downhill skiing and admire the level of skill and expertise in a sport that, personally, I don't know how to practice.

PERMALINK

<https://magazine.fbk.eu/en/news/la-cyber-sicurezza-alle-olimpiadi/>

TAGS

- #ambassador
- #attacks
- #cybersecurity
- #fbkscienceambassador
- #hacker
- #hacktivists
- #jointLab
- #malicious
- #olympics
- #PMI

AUTHORS

- Giovanna Rauzi