Cyber Threat Landscape

2026 Winter Olympics – Italy

Prepared by: Robert J Carloff
CYBER NEWS LIVE
Reston VA USA & Canberra ACT AUS

Released: January 2026

Contents

Opening Statement

This is an independent cyber threat analysis for the 2026 Winter Olympic Games in Milano Cortina (Milano Cortina 2026). The Olympic Winter Games are scheduled from February 6 to February 22, 2026, with the Paralympic Winter Games scheduled from March 6 to March 15, 2026. Like previous Olympic Games, Milano Cortina 2026 is anticipated to encounter numerous cyber threats. This report delves into areas including cryptocurrencies, cyber threat actors, emerging technologies, scams, social media, sponsors, and supply chain attacks.

Milano Cortina 2026 marks the first multi-location Winter Olympics and the first since Sarajevo 1984 to have the Opening and Closing Ceremonies held in different cities. The Opening Ceremony will take place on February 6 at Milan's San Siro Stadium, and the Closing Ceremony on February 22 at Verona Arena. Events will be held across Lombardy and Northeast Italy, including Milan, Cortina d'Ampezzo, Valtellina, and Val di Fiemme—an area spanning 22,000 square kilometres, the largest geographic footprint of any Winter Olympics.

Undertaking the cyber threat analysis for the Olympics started to become a passion of ours in 2015 after completing the Cyber Threat Analysis for the 2016 Rio Olympics, where I undertook a leading role in conjunction with industry and government partners. Since then, we have completed every cyber threat analysis for the summer and winter games, including our comprehensive analysis of the Paris 2024 Summer Olympics.

Please feel free to distribute this threat analysis widely, ensuring to provide appropriate credit. For any media inquiries, please contact us at contact@cybernewslive.com.

1. Cryptocurrency

Cryptocurrencies, such as Bitcoin, have gained significant traction in recent years as digital alternatives to traditional currencies. However, along with their growing popularity, these digital assets have become targets for various cyber threats. In this section, we will provide insights into the cyber threats associated with cryptocurrencies, including digital currency, digital wallets, and non-fungible tokens that can have an impact on Milano Cortina 2026.

Cryptocurrency (Bitcoin)

Bitcoin, as the leading cryptocurrency, is a prime target for cyber threats due to its widespread adoption and high market value. Threat actors may employ various tactics to exploit vulnerabilities in Bitcoin networks, including:

- **Ransomware Attacks:** Cyber criminals leverage Bitcoin's anonymity and decentralisation to demand payments in exchange for decrypting encrypted data, evading detection and accountability.
- **Phishing Scams:** Fraudulent websites and emails impersonate legitimate cryptocurrency platforms to deceive users into revealing private keys or login credentials, resulting in theft of funds from digital wallets.
- **Exchange Hacks:** Cyber attackers target cryptocurrency exchanges to pilfer digital assets stored in online wallets, causing substantial financial losses for both users and exchanges.

Digital Currency (National Cryptocurrency in Italy)

Italy, as part of the European Union, is actively involved in the development of the digital euro through the European Central Bank's digital currency initiative. The concept presents its own set of cyber threats:

- **Cyber Espionage:** State-sponsored threat actors may target CBDC infrastructure to gather intelligence or disrupt financial systems, potentially undermining national security and economic stability.
- **Data Privacy Concerns:** The centralised nature of CBDCs raises concerns about data privacy and security, as large-scale data breaches could compromise sensitive financial information of citizens.

Digital Wallets

Digital wallets, used to store and manage cryptocurrencies, are susceptible to various cyber threats:

- **Malware Attacks:** Malicious software can compromise digital wallets, enabling threat actors to steal private keys or manipulate transactions, leading to unauthorized fund transfers.
- **Phishing Attacks:** Cyber criminals employ phishing emails or counterfeit websites to deceive users into divulging their wallet credentials, granting unauthorized access to cryptocurrency funds.

Non-Fungible Tokens (NFTs)

NFTs, which represent unique digital assets such as art, collectibles, and virtual real estate, have emerged as targets for cyber threats:

- **Fraudulent Sales:** Scammers exploit the hype surrounding NFTs by selling counterfeit or plagiarized digital artworks, including fake Olympic memorabilia, deceiving buyers into purchasing illegitimate tokens.
- **Smart Contract Vulnerabilities:** NFT platforms and marketplaces utilizing smart contracts are vulnerable to coding errors or exploits, potentially leading to theft or manipulation of NFT assets.

Conclusion

As cryptocurrencies continue to proliferate and evolve, the cyber threats targeting these digital assets are likely to escalate. To mitigate these risks, stakeholders must remain vigilant against emerging threats, implement robust cybersecurity measures, and educate users about best practices for securely managing and transacting with cryptocurrencies, digital wallets, and non-fungible tokens.

References

- Faulds, Z. (2021) 'These Olympic Champions Get Paid In Cryptocurrency', The Street, 3 June. Available at: https://www.thestreet.com/crypto/investing/olympics-athletes-cryptocurrency (Accessed: 4 June 2021).
- Rodrigues, F. (2022) 'Crypto at the Olympics: NFT skis, Bitcoin bobsledders and CBDC controversy', Cointelegraph, 15 February. Available at: https://cointelegraph.com/news/crypto-at-the-olympics-nft-skis-bitcoin-bobsledders-and-cbdc-controversy (Accessed: 16 February 2022).

2. Cyber Threat Actors

The Milano Cortina 2026 Winter Games will draw attackers of all types, from petty scammers to nation-state actors. According to Unit 42 research from Palo Alto Networks, everything is on the table—from Wi-Fi and digital infrastructure disruptions like those seen at the 2018 Winter Olympics in PyeongChang, to distributed denial-of-service (DDoS) and ransomware attacks of the sort French authorities faced during the Paris 2024 Olympics.

2.1 Nation State Actors

Nation-state and sophisticated cyber threat actors pose significant risks to organisations and governments worldwide. These threat actors are often well-funded, highly skilled, and motivated by political, economic, or strategic interests. They employ a range of tactics, including advanced persistent threats (APTs), social engineering, and zero-day exploits.

Targeting Trade Secrets and Sensitive Information

Nation-state and sophisticated threat actors frequently target organisations to steal trade secrets, intellectual property, and sensitive information. The Unit 42 report identified several state-sponsored groups with demonstrated capabilities:

- **APT28 (Fancy Bear – Russia):** Linked to cyber attacks against various sporting organisations and anti-doping agencies, with a documented history of Olympic-related operations.
- **Mustang Panda (China):** Advanced persistent threat group capable of sophisticated espionage operations targeting geopolitical interests.
- **Kimsuky (North Korea):** State-sponsored outfit with demonstrated capability for strategic intelligence gathering.

Supporting National Interests

Cyber threat actors affiliated with nation-states frequently conduct their operations with the backing or guidance of governmental bodies, aiming to promote their country's national interests, strategic goals, or geopolitical agendas. Given the ongoing conflict in Eastern Europe and the resulting exclusion of certain nations from fielding teams, state-backed cybercriminals may specifically target Italian national interests, considering Rome's foreign policy positions.

Mitigation Strategies

- **Enhanced Cybersecurity Measures:** Implement network segmentation, encryption, intrusion detection systems (IDS), and endpoint protection solutions.
- **Information Sharing and Collaboration:** Foster public-private partnerships and sector-specific information sharing through ISACs and international initiatives.
- **Regulatory Compliance and Cyber Hygiene:** Comply with NIST Cybersecurity Framework, GDPR, and ISO 27001 standards.

Potential Impacts

- **Espionage and Intelligence Gathering:** Theft of sensitive information about athletes, officials, security arrangements, and diplomatic communications.
- **Infrastructure Disruption:** Attacks on critical systems including power, transportation, and communications could disrupt Games operations.
- **Reputational Damage:** Successful nation-state attacks could undermine confidence in Italy's ability to host secure international events.
- **Geopolitical Escalation:** Attribution of attacks could heighten international tensions.

Conclusion

Nation-state and sophisticated cyber threat actors pose significant challenges to Milano Cortina 2026, targeting trade secrets, sensitive information, and critical infrastructure to advance national interests. Given current geopolitical tensions and certain nations' exclusion from the Games providing additional motivation for retaliation, stakeholders must adopt a proactive approach to cybersecurity, leveraging advanced technologies, collaborative partnerships, and regulatory compliance to protect against evolving threats.

References

- Nelson, N. (2024) 'Russia Aims Cyber Operations at Summer Olympics', Dark Reading, 3 June. Available at: https://www.darkreading.com/threat-intelligence/russia-cyber-operations-summer-olympics (Accessed: 4 June 2024).
- Vijayan, J. (2026) 'Cyber Threats Loom Over 2026 Winter Olympics', Dark Reading, 16 January. Available at: https://www.darkreading.com/remote-workforce/winter-olympics-podium-cyberattackers (Accessed: 17 January 2026).

2.2 Organised Crime

Ransomware gangs and other financially motivated actors will look to exploit the Games' complex organisational ecosystem to disrupt critical infrastructure—including ticketing systems, event websites, and point-of-sale (PoS) terminals.

Financially Motivated Activities

- **Data Breaches:** Hacking into computer systems to steal sensitive data, such as credit card information, personal identification details, and intellectual property.
- **Ransomware Attacks:** Encrypting a victim's data and demanding a ransom payment for decryption.
- **Phishing and Smishing:** Sending fraudulent emails or text messages designed to trick victims into revealing personal information or clicking on malicious links.
- **Online Payment Fraud:** Stealing credit card details or using fake accounts to make unauthorized purchases.

Frequent Use of Social Engineering

Social engineering is a manipulative tactic used by cyber criminals to exploit human trust. Common methods include:

- **Pretexting:** Creating a false scenario to gain a victim's trust, such as impersonating a legitimate organisation.
- **Baiting:** Offering something enticing, like a gift or prize, to lure victims into clicking on malicious links.
- **Tailgating:** Physically following authorized individuals into secure areas at Olympic venues.
- **Quid Pro Quo:** Offering to perform a service or provide information in exchange for sensitive details.
- **Shoulder Surfing:** Spying on someone's screen or keyboard while they are using a computer, ATM, or other electronic device.

Potential Impacts

- **Financial Losses:** Individuals can suffer financial hardship due to stolen money or identity theft. Organisations may face significant financial losses from data breaches, ransom payments, and fraudulent activities.
- **Reputational Damage:** Data breaches and other cyber attacks can damage an organisation's reputation, leading to a loss of trust from customers and partners.
- **Operational Disruption:** Cyber attacks can disrupt business operations, leading to downtime, productivity loss, and hindered service delivery.

Recommendations

- **Individuals:** Be cautious when clicking on links or opening attachments in emails or text messages, even if they appear to be from legitimate sources.
- **Organisations:** Implement multi-factor authentication, regularly update software and security systems, and conduct regular security awareness training for employees.
- **Payment Security:** Use secure payment gateways and monitor for unusual transaction patterns across ticketing and retail systems.

Conclusion

Financially motivated cyber crime, particularly when coupled with frequent social engineering tactics, poses a significant threat to individuals and organisations. Remaining vigilant, practicing safe online habits, and implementing robust security measures are crucial to mitigate these risks.

References

- Crisis24 (2025) 'Italian Authorities to Implement Heightened Security for Winter Olympics Through February 2026'. Available at: https://www.crisis24.com/articles/italian-authorities-to-implement-heightened-security-for-winter-olympics-through-february-2026 (Accessed: 10 January 2026).
- Palo Alto Networks Unit 42 (2025) 'Defending the 2026 Milano-Cortina Winter Games'. Available at: https://www.paloaltonetworks.com/resources/research/unit-42-cyber-vigilance-program/2026-winter-games-milano-cortina (Accessed: 10 January 2026).

2.3 Cyber Terrorism

While Italy typically faces a low-to-moderate risk of terrorism, cyber terrorism differs from other forms of cyber crime in its primary motivation—to achieve political or ideological goals through destructive attacks designed to instil fear.

Politically or Ideologically Motivated Actions

- Promoting a specific ideology or agenda
- Undermining government authority and public trust
- Disrupting critical infrastructure and essential services
- Influencing public opinion and sparking social unrest

Goal to Instil Fear through Destructive Attacks

- **Disrupting critical infrastructure:** Targeting power grids, transportation systems, and communication networks.
- **Attacking financial institutions:** Disrupting financial services to cripple economic stability.
- **Spreading misinformation:** Manipulating social media to spread false information and erode public trust.

Recommendations

- Strengthen critical infrastructure protection with redundancy and failover systems
- Establish robust incident response and crisis management protocols
- Foster collaboration with law enforcement and intelligence agencies to identify potential threats
- Develop public communication strategies to counter misinformation and maintain public trust

Conclusion

Cyber terrorism is a growing threat with the potential to cause widespread damage and disrupt critical infrastructure, economies, and societies. Understanding the motivations, goals, and tactics of cyber terrorists is crucial for developing effective mitigation strategies.

References

- Ackerman Group (2025) 'Special Security Assessment: 2026 Winter Olympics'. Available at: https://ackermangroup.com/special-security-assessment-2026-winter-olympics/ (Accessed: 10 January 2026).
- Crisis24 (2025) 'Italian Authorities to Implement Heightened Security for Winter Olympics Through February 2026'. Available at: https://www.crisis24.com/articles/italian-authorities-

to-implement-heightened-security-for-winter-olympics-through-february-2026 (Accessed: 10 January 2026).

- Lambert, E. (2024) 'Islamic State group ad encouraging 'lone wolf' attacks at Olympics', NewsNation, 10 June. Available at: https://www.newsnationnow.com/us-news/sports/olympics/islamic-state-group-ad-paris-olympic-threat/ (Accessed: 11 June 2024).
- Seldin, J. (2024) 'Terror attacks headline threats to upcoming Paris Olympics', VOA News, 4 June. Available at: https://www.voanews.com/a/terror-attacks-headline-threats-to-upcoming-paris-olympics/7642276.html (Accessed: 5 June 2024).

2.4 Hacktivism

The Milano Cortina Winter Games will provide hacktivist groups a perfect venue to try and get their political and social messaging across to an audience estimated to be around 3 billion viewers.

Hacktivism and the Olympics

Environmental activist groups have been particularly active in Italy, with ongoing campaigns denouncing the environmental and economic impact of the Winter Olympics. Milan faces a particular risk of being impacted by civil unrest during the Games. Hacktivist groups may seek to:

- **Raise awareness for a specific cause:** Draw attention to social, political, or environmental issues.
- **Disrupt the event:** Launch cyber attacks on critical infrastructure or operational systems.
- **Embarrass the host nation:** Expose vulnerabilities and undermine public trust.

Disruptive Attacks and Insider Threats

- **DDoS attacks:** Overwhelming websites or online services with traffic, rendering them inaccessible.
- **Website defacement:** Altering the visual appearance of websites with messages promoting the hacktivist's cause.
- **Data breaches:** Stealing or leaking sensitive information such as athlete data or internal communications.
- **Insider threats:** Individuals with authorized access who may be sympathetic to hacktivist causes.

Recommendations

- Deploy robust DDoS mitigation solutions to protect public-facing websites and services
- Implement strict access controls and monitor for insider threat indicators
- Maintain backup systems and rapid recovery capabilities for web properties
- Monitor social media and hacktivist forums for emerging threats and planned actions

Conclusion

Milano Cortina 2026 is vulnerable to hacktivist attacks, which could lead to significant disruption and reputational damage. Understanding the motivations, tactics, and challenges associated with hacktivism is crucial for implementing effective protective measures.

References

- Crisis24 (2025) 'Italian Authorities to Implement Heightened Security for Winter Olympics Through February 2026'. Available at: https://www.crisis24.com/articles/italian-authorities-to-implement-heightened-security-for-winter-olympics-through-february-2026 (Accessed: 10 January 2026).
- Vijayan, J. (2026) 'Cyber Threats Loom Over 2026 Winter Olympics', Dark Reading, 16 January. Available at: https://www.darkreading.com/remote-workforce/winter-olympics-podium-cyberattackers (Accessed: 17 January 2026).

2.5 Advanced Persistent Threats (APTs)

APTs are well-resourced adversaries engaging in sophisticated long-term cyber operations. The high-profile nature of the Olympic Games makes them an attractive target for APTs seeking espionage, data theft, or disruption.

APTs and the Olympics: Historical Precedent

The 2018 PyeongChang Winter Olympics saw significant disruption from the 'Olympic Destroyer' malware, which targeted the Games' IT infrastructure during the opening ceremony, causing Wi-Fi and digital infrastructure disruptions. This demonstrated the real-world impact APTs can have on major sporting events.

Examples of APTs known to target major events include Fancy Bear (Russia), which has been linked to cyber attacks against various sporting organisations and anti-doping agencies.

Risks and Potential Impact

- **Data breaches:** Exposure of sensitive information could damage the reputation of the organising committee, athletes, and sponsors.
- **Disruption of operations:** Compromised critical infrastructure could disrupt ticketing, broadcasting, or essential services.
- **Financial losses:** Data breaches and operational disruptions could result in substantial financial losses.
- **Geopolitical tensions:** Successful attacks could exacerbate international relations depending on the origin.

Recommendations

- Enhance cybersecurity posture with multi-factor authentication, data encryption, and continuous monitoring
- Foster intelligence gathering and threat sharing with international partners
- Develop and rehearse comprehensive incident response plans
- Conduct security awareness training for staff, athletes, and stakeholders

Conclusion

APTs represent one of the most significant cyber threats to Milano Cortina 2026. The documented history of Olympic Destroyer and other APT operations against previous Games demonstrates that these sophisticated adversaries have both the capability and motivation to target the 2026 Winter Olympics. A coordinated, multi-layered defence strategy is essential to detect, prevent, and respond to APT activity.

References

- Dataminr (2025) 'Securing the Slopes: 2026 Winter Olympics Security'. Available at: https://www.dataminr.com/resources/insight/securing-the-slopes-2026-winter-olympics-security/ (Accessed: 10 January 2026).
- Palo Alto Networks Unit 42 (2025) 'Defending the 2026 Milano-Cortina Winter Games'. Available at: https://www.paloaltonetworks.com/resources/research/unit-42-cyber-vigilance-program/2026-winter-games-milano-cortina (Accessed: 10 January 2026).

2.6 Cyber Espionage

In this section, we examine the various cyber espionage threats potentially endangering Milano Cortina 2026. Building upon past examples such as Fancy Bear's intrusion into anti-doping agencies, we can see how international events like the Olympics are prime targets for state-sponsored and independent hacker groups.

Cyber Espionage: Learning from the Past, Preparing for the Future

Espionage targeting the Olympics is not a new phenomenon. Cases like Fancy Bear targeting the United States Anti-Doping Agency (USADA) illustrate the potential for cyber attacks aimed at:

- **Stealing confidential information:** Including athlete training routines, competition strategies, and doping test results.
- **Gaining competitive advantage:** Leaked information could help competing nations gain unfair advantages.
- **Undermining trust and integrity:** Successful attacks can damage public trust in the Olympic Games.

Evolution of Threats: Beyond Traditional Espionage

- **Ransomware:** Attackers could exploit vulnerabilities and encrypt critical infrastructure or data.
- **Destructive malware:** Malicious software designed to destroy or render data and systems inoperable.
- **Website defacement:** Targeting official Olympic websites or sponsor sites with political messaging.

Recommendations

- Implement advanced threat detection systems capable of identifying espionage activities
- Encrypt all sensitive data at rest and in transit
- Establish strict access controls and monitor privileged accounts
- Collaborate with national cybersecurity agencies for threat intelligence sharing

Conclusion

Cyber espionage remains a persistent threat to international sporting events. The targeting of anti-doping agencies, athlete data, and operational systems by state-sponsored groups demonstrates the breadth of espionage objectives. Milano Cortina 2026 must implement robust counterintelligence measures alongside technical defences to protect sensitive information and maintain the integrity of the Games.

References

- Cyware (n.d.) 'Inside Fancy Bear's Arsenal: An Update on the Cyber Tactics of APT28'. Available at: https://cyware.com/resources/research-and-analysis/inside-fancy-bears-arsenal-an-update-on-the-cyber-tactics-of-apt28-5186 (Accessed: 14 May 2024).
- Matsakis, L. (2018) 'Hack Brief: Russian Hackers Release Apparent IOC Emails in Wake of Olympics Ban', Wired, 10 January. Available at: https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/ (Accessed: 11 January 2018).
- Stone, J. (2019) 'Fancy Bear hackers targeted at least 16 athletic organizations ahead of Tokyo Olympics', CyberScoop. Available at: https://cyberscoop.com/fancy-bear-olympics-hacking-tokyo/ (Accessed: 29 October 2019).

3. Emerging Technology Advancements

In this section of the report, we will examine the potential cyber threats posed by emerging technologies like Artificial Intelligence (AI), Machine Learning (ML), and Deepfakes to Milano Cortina 2026. While these technologies offer potential benefits such as enhanced security and personalised experiences, their misuse can create significant challenges.

Artificial Intelligence, Machine Learning, and Deepfakes

Phishing and social engineering scams—boosted by AI and deepfakes—will likely be the tactic of choice for initial access among bad actors at the Games. To make the scams appear legit, adversaries will pose as partner organisations, regulators, or other trusted entities associated with the Winter Olympics.

Emerging Technologies and the Olympics: A Double-Edged Sword

AI and ML offer potential benefits:

- **Enhanced security:** AI can analyse vast amounts of data to identify suspicious activity and potential security threats.
- **Personalised experiences:** ML can personalise the spectator experience based on individual preferences.

Deepfakes pose potential risks:

- **Misinformation and disinformation:** Fabricated videos or audio recordings featuring athletes or officials can spread misinformation and damage reputations.
- **Social engineering:** Deepfakes can be used to impersonate officials in phishing attempts targeting athletes, staff, or sponsors.

Potential Impacts of Misuse

- **Disrupting operations:** AI-powered bots could overwhelm ticketing systems or launch DoS attacks on critical infrastructure.
- **Manipulation and fraud:** Deepfakes could be used to manipulate financial transactions or spread propaganda.
- **Erosion of trust:** Widespread deepfakes could erode public trust in the integrity of the Olympic Games.

Mitigating the Risks

- Implement proactive AI security protocols to detect and prevent malicious AI applications
- Educate staff, athletes, and spectators on how to critically evaluate information online
- Raise public awareness about the potential misuse of AI and deepfakes
- Establish collaborative frameworks with international partners for joint response strategies

Conclusion

Emerging technologies present both opportunities and challenges for Milano Cortina 2026. While AI and ML can enhance security and spectator experiences, their misuse—particularly through deepfakes and AI-powered phishing—poses significant risks. Proactive security measures, public awareness campaigns, and international cooperation are essential to mitigate these evolving threats.

References

- Glanzman, A. (2022) 'Reflecting on 20 years of technology transformation at the Olympic Games', Olympics.com, 10 May. Available at: https://olympics.com/ioc/news/reflecting-on-20-years-of-technology-transformation-at-the-olympic-games (Accessed: 12 May 2024).
- Hak, A. (2021) 'How emerging technologies could shape the 2032 Olympics', The Next Web, 6 August. Available at: https://thenextweb.com/news/emerging-technologies-shape-2032-olympics (Accessed: 12 May 2024).
- Starks, T. (2024) 'Fake Tom Cruise warns of violence at Paris Olympics in pro-Russian info op', CyberScoop, 3 June. Available at: https://cyberscoop.com/russia-tom-cruise-ai-paris-olympics/ (Accessed: 9 May 2024).
- Watts, C. (2024) 'How Russia is trying to disrupt the 2024 Paris Olympic Games', Microsoft On the Issues, 2 June. Available at: https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/ (Accessed: 3 June 2024).

4. Scams

Scams are deceptive marketing schemes that lure victims with the promise of exclusive benefits or scarce resources. The allure of the Olympic Games makes them a prime target for such scams. Increased cyber incidents, such as phishing and scams, may be targeted against travellers to the Games.

Scams: Capitalising on Hype

- **Fake Ticket Lotteries:** Emails or social media posts advertise non-existent lotteries offering a chance to win Olympic tickets, often requiring upfront fees.
- **Ticket Resale Fraud:** Fraudulent online marketplaces offer fake or overpriced tickets to the Olympic Games.
- **Merchandise Scams:** Websites advertise counterfeit or low-quality Olympic merchandise.
- **Accommodation Scams:** Fake listings lure victims into paying for non-existent or overpriced accommodations near Olympic venues.
- **Sports Betting Scams:** Fraudulent schemes aimed at deceiving individuals who engage in sports betting activities.

Identifying Scams

- **Unrealistic promises:** Offers of guaranteed tickets or deeply discounted accommodations are often too good to be true.
- **Urgency and pressure:** Scammers create a sense of urgency, pressuring victims to act quickly.
- **Poor grammar and typos:** Legitimate organisations typically maintain professional communication standards.
- **Suspicious payment methods:** Requests for payment through unusual methods like money transfers are indicative of scams.

Recommendations

- Launch public awareness campaigns educating people on common Olympic scams

- Collaborate with official ticketing platforms to promote secure purchase channels
- Proactively monitor online marketplaces for suspicious activity
- Establish clear reporting mechanisms for suspected scams

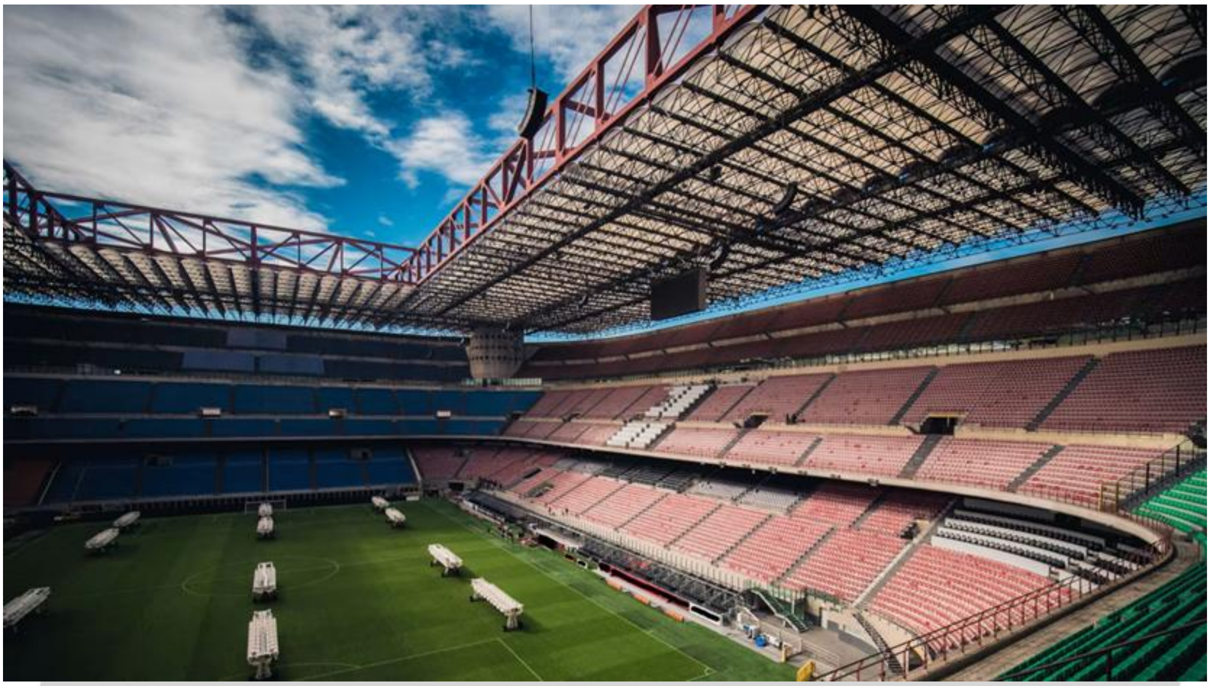
Conclusion

Olympic-themed scams exploit the excitement and urgency surrounding major sporting events. From fake tickets to fraudulent accommodation offers, these schemes target both visitors and remote viewers worldwide. Public awareness, collaboration with official platforms, and proactive monitoring are critical to protecting potential victims and preserving the reputation of Milano Cortina 2026.

References

- Le Figaro (2023) 'Olympic 2024: tickets already sold illegally on the internet, 44 fraudulent sites identified', Ground News. Available at: https://ground.news/article/olympic-2024-tickets-already-sold-illegally-on-the-internet-44-fraudulent-sites-identified_c7e1df (Accessed: 12 May 2023).
- Trend Micro (2021) 'Top 4 Olympic Games Scams – How to Protect Yourself', Trend Micro News. Available at: https://news.trendmicro.com/2021/07/30/top-4-olympic-games-scams-how-to-protect-yourself/ (Accessed: 31 July 2021).

5. Social Media



Social media platforms like Instagram, Meta (Facebook), TikTok, and X (formerly Twitter) will undoubtedly play a significant role at Milano Cortina 2026. While offering opportunities for engagement and information dissemination, these platforms also present potential cyber threats to the estimated 3 billion global viewers.

Social Media: A Powerful Tool for the Olympics

- **Engagement and Community Building:** Social media fosters engagement between athletes, fans, and stakeholders.
- **Information Sharing:** Real-time updates, event highlights, and behind-the-scenes content.
- **Brand Promotion:** Official accounts can be leveraged for promoting sponsorships and merchandise.
- **Global Audience Reach:** Social media allows for wider reach, engaging fans across the globe.

Potential Threats Posed by Social Media

- **Misinformation and Disinformation:** Rapid spread of unverified information creating confusion and damaging reputations.
- **Targeted Harassment and Abuse:** Athletes and officials subjected to online bullying and hate speech.
- **Fake Accounts and Bots:** Malicious actors using fake accounts to manipulate public opinion.
- **Doping Rumours and Scandals:** Fabricated accusations spreading rapidly and tarnishing athletes' reputations.
- **Ticket Scalping and Fraud:** Platforms exploited for selling counterfeit or overpriced tickets.

Recommendations for Milano Cortina 2026

- Develop clear social media guidelines for athletes, officials, and stakeholders
- Establish efficient monitoring and reporting mechanisms

- Foster collaboration with social media platforms to tackle misinformation
- Launch media literacy campaigns educating the public on identifying credible sources

Conclusion

Social media is a double-edged sword for Milano Cortina 2026. While it enables unprecedented global engagement and real-time communication with 3 billion viewers, it also provides channels for misinformation, harassment, and fraud. Clear guidelines, proactive monitoring, and platform collaboration are essential to harness social media's benefits while mitigating its risks.

References

- Barkho, G. (2016) 'How Social Media Changed the Olympics, and What It Means for #Rio2016', Later. Available at: https://later.com/blog/how-social-media-changed-the-olympics-and-rio-2016/ (Accessed: 15 August 2016).
- Forrester, N.W. (2018) 'How social media impacts athletes at the Olympics', Macleans. Available at: https://macleans.ca/olympics/how-social-media-impacts-athletes-at-the-olympics/ (Accessed: 28 February 2018).
- Grabmüllerová, A. (2022) 'Social Media and the Olympics: A Chance for Improving Gender Equality', Frontiers in Sports and Active Living. Available at: https://www.frontiersin.org/articles/10.3389/fspor.2022.825440/full (Accessed: 30 April 2022).
- Starks, T. (2024) 'Fake Tom Cruise warns of violence at Paris Olympics in pro-Russian info op', CyberScoop, 3 June. Available at: https://cyberscoop.com/russia-tom-cruise-ai-paris-olympics/ (Accessed: 9 May 2024).
- Watts, C. (2024) 'How Russia is trying to disrupt the 2024 Paris Olympic Games', Microsoft On the Issues, 2 June. Available at: https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/ (Accessed: 3 June 2024).

6. Sponsor Matrix

Milano Cortina 2026 relies heavily on sponsorships to support the event. The sponsorship plan targets €575 million in revenue, with €400 million secured by early 2025. While official sponsors provide vital financial resources, they also introduce an element of risk to the Olympic Games' overall cybersecurity posture.

Sponsor Matrix: A Complex Ecosystem

Milano Cortina 2026 has secured 52 official partnerships across multiple tiers, including 11 global Olympic and Paralympic partners and 40 national sponsorships. At the top of the domestic pyramid are eight Premium Partners, including major players such as ENEL, Eni, Poste Italiane, Intesa Sanpaolo, Leonardo, and Stellantis.

Potential Risks Associated with Sponsors

- **Supply Chain Attacks:** A cyber attack targeting a sponsor's infrastructure could potentially compromise Olympic systems.
- **Data Breaches:** A data breach at a sponsor company could expose sensitive Olympic information.
- **Brand Hijacking:** Malicious actors could exploit a sponsor's brand for phishing attacks or misinformation.
- **Reputational Risk:** Negative publicity surrounding a sponsor's cybersecurity practices could tarnish the Games' image.

Notable Development: Cloudflare Uncertainty

Cloudflare, a key cybersecurity partner, has threatened to discontinue millions of dollars in pro bono cybersecurity services following a €14 million fine from Italian authorities for alleged anti-piracy law violations. Cloudflare CEO Matthew Prince stated he is considering "discontinuing the millions of dollars in pro bono cyber-security services we are providing the upcoming Milano-Cortina Olympics." This situation creates potential uncertainty around the Games' cybersecurity infrastructure.

Mitigating Sponsor-Related Risks

- **Thorough vetting:** Implement a rigorous vetting process to assess sponsors' cybersecurity posture.
- **Data sharing agreements:** Establish clear data sharing agreements with security protocols.
- **Penetration Testing:** Encourage sponsors to conduct regular penetration testing and security audits.
- **Security Awareness Training:** Collaborate with sponsors on information security awareness training.

Key Partners (Full list in Appendix)

Category	Partners
Worldwide TOP Partners	Airbnb, Alibaba, Allianz, Coca-Cola/Mengniu, Visa, Samsung, P&G, TCL, Deloitte, Corona Cero, Omega
Premium Partners	ENEL, Eni, Poste Italiane, Intesa Sanpaolo, Leonardo, Stellantis, TIM, Gruppo Ferrovie dello Stato Italiane
Official Partners	Accor, Groupe ADP, EA7 Emporio Armani, FNM Group, Fiera Milano, ITA Airways, Salesforce, Technogym
Official Sponsors	Abatable, A2Q, Bauerfeind, Esselunga, Grana Padano, Herbalife, Juniper Networks, Intercom, Dr. Leitner, Salomon, Pirelli, Kiko Milano, Prosecco DOC, Randstad, Fincantieri, Trentino Marketing, IDM Alto Adige
Official Supporters	Airweave, Kässbohrer Italia, Ottobock, RGS Events, Technoalpin, Ticketone, Versalis

Conclusion

The sponsor ecosystem for Milano Cortina 2026 represents both essential financial support and a significant expansion of the attack surface. With 52 partnerships and the ongoing Cloudflare uncertainty, robust vendor security assessments, clear data sharing agreements, and coordinated incident response planning across all partner organisations is critical to maintaining a secure Games environment.

References

- Al Jazeera (2026) 'Milano Cortina Winter Olympics threatened by Cloudflare funding withdrawal'. Available at: https://www.aljazeera.com/sports/2026/1/10/milano-cortina-winter-olympics-threatened-by-cloudfare-funding-withdrawal (Accessed: 11 January 2026).

- Inside the Games (2025) 'Milano Cortina expands sponsorship deals'. Available at: https://www.insidethegames.biz/articles/1154570/milano-cortina-2026-reaches-40-sponsorsh (Accessed: 10 January 2026).
- Jackson, F. (2024) 'Paris Olympics 2024: Cyber Attackers are Targeting Companies Associated With Games, Report Finds', TechRepublic, 4 June. Available at: https://www.techrepublic.com/article/cyber-attackers-target-paris-olympic-games/ (Accessed: 5 June 2024).

7. Supply Chain Attacks

Supply chain attacks, targeting third-party vendors and partners, are a growing threat to large-scale events like Milano Cortina 2026. The Milano Cortina Winter Games will give rise to a large, complex digital ecosystem replete with vulnerabilities both old and new.

Supply Chain Attacks: A Rising Threat Landscape

Supply chain attacks involve compromising a seemingly less secure vendor or partner within an organisation's network to gain access to the main target. The increasing frequency of these attacks can be attributed to:

- **Expanded attack surface:** Organisations rely on an ever-growing network of vendors and partners.
- **Focus on weakest links:** Attackers target less-resourced vendors with weaker cybersecurity posture.
- **Sophisticated techniques:** Attackers leverage social engineering and zero-day exploits to bypass security measures.

Historical Precedent: Tokyo 2020

The Tokyo Olympics became a victim of supply chain compromise when Fujitsu hackers targeted Olympic infrastructure. This incident demonstrated how compromised vendors involved in critical services can disrupt crucial aspects of the Games.

Potential Impact on Milano Cortina 2026

- **Disruption of Critical Services:** Compromised vendors involved in ticketing, broadcasting, or venue management—including digital timings and scoreboards—could disrupt crucial aspects.

- **Data Breaches:** Attackers may steal sensitive information about athletes, spectators, sponsors, or organisational plans.
- **Financial Losses:** Data breaches or operational disruptions can lead to financial losses for organisers and stakeholders.
- **Reputational Damage:** A successful supply chain attack can tarnish the reputation of Milano Cortina 2026.

Mitigating Supply Chain Risks

- **Vendor Risk Management:** Implement robust programs to assess the cybersecurity posture of all vendors.
- **Contractual Obligations:** Incorporate strong cybersecurity clauses into vendor contracts.
- **Security Awareness Training:** Extend training programs to include vendors handling Olympic-related data.
- **Threat Intelligence Sharing:** Foster collaboration among organisers, vendors, and relevant authorities.
- **Multi-factor Authentication:** Encourage vendors to implement MFA for all access points.

Conclusion

Supply chain attacks represent a critical and growing threat vector for Milano Cortina 2026. The precedent set by the Tokyo 2020 Fujitsu compromise demonstrates how adversaries can exploit vendor relationships to access Olympic infrastructure. Given the unprecedented multi-venue footprint of these Games, comprehensive vendor risk management, contractual security obligations, and coordinated threat intelligence sharing are essential to securing the entire supply chain ecosystem.

References

- Greek Reporter (2024) 'Paris Olympics Threatened by Cyberattacks'. Available at: https://greekreporter.com/2024/04/18/paris-olympics-brace-cyberattacks/ (Accessed: 20 April 2024).
- Palo Alto Networks Unit 42 (2025) 'Defending the 2026 Milano-Cortina Winter Games'. Available at: https://www.paloaltonetworks.com/resources/research/unit-42-cyber-vigilance-program/2026-winter-games-milano-cortina (Accessed: 10 January 2026).
- Pierce, F. (2020) 'Supply chain not to blame for Olympic shortages', Supply Chain Digital. Available at: https://supplychaindigital.com/logistics/supply-chain-not-blame-olympic-shortages (Accessed: 25 May 2020).
- Sharma, M. (2021) 'Tokyo Olympics becomes the latest victim of the Fujitsu hackers', TechRadar. Available at: https://www.techradar.com/news/tokyo-olympics-becomes-the-latest-victim-of-the-fujitsu-hackers (Accessed: 15 June 2021).

Final Assessment

In conclusion, the cyber threat analysis for Milano Cortina 2026 underscores the critical importance of robust cybersecurity measures in safeguarding the integrity, security, and success of the event. As with any major international gathering, Milano Cortina 2026 faces a diverse array of cyber threats, ranging from sophisticated cyber espionage tactics to emerging risks posed by AI-enhanced technologies and social engineering scams.

The Milano Cortina 2026 Foundation and Italy's National Cybersecurity Agency (ACN) have signed a cooperation protocol aimed at preventing cyberattacks and securing the technological systems that will support the Games. This agreement builds on experience gained during the Paris 2024 Olympic Games in collaboration with France's National Information Systems Security Agency (ANSSI).

As Bruno Frattasi, Director General of the ACN stated: "The signing of this protocol marks an important moment for our agency. We have been working alongside our French colleagues from ANSSI during the 2024 Summer Olympics and it has been a fruitful opportunity to prepare for the challenges of the upcoming Winter Olympics."

The unique multi-venue nature of these Games, spanning venues across Milan, Cortina d'Ampezzo, Valtellina, and Val di Fiemme—an area of 22,000 square kilometres—presents additional complexity. Events will take place across a bigger area than any previous Olympics, requiring coordinated cybersecurity efforts across multiple regions.

To effectively mitigate these threats, stakeholders must adopt a proactive and collaborative approach, leveraging advanced cybersecurity technologies, sharing threat intelligence, and implementing robust defence strategies. Additionally, continuous monitoring, regular security assessments, and comprehensive incident response planning are essential components of a resilient cybersecurity posture.

By remaining vigilant, adaptive, and united in their efforts to combat cyber threats, organisers, government agencies, sponsors, and other stakeholders can help ensure a safe and secure environment for athletes, spectators, and participants alike during the 2026 Olympic Winter Games in Milano Cortina.

References

- Ackerman Group (2025) 'Special Security Assessment: 2026 Winter Olympics'. Available at: https://ackermangroup.com/special-security-assessment-2026-winter-olympics/ (Accessed: 10 January 2026).
- Al Jazeera (2026) 'Milano Cortina Winter Olympics threatened by Cloudflare funding withdrawal'. Available at: https://www.aljazeera.com/sports/2026/1/10/milano-cortina-winter-olympics-threatened-by-cloudfare-funding-withdrawal (Accessed: 11 January 2026).
- Barkho, G. (2016) 'How Social Media Changed the Olympics, and What It Means for #Rio2016', Later. Available at: https://later.com/blog/how-social-media-changed-the-olympics-and-rio-2016/ (Accessed: 15 August 2016).
- Crisis24 (2025) 'Italian Authorities to Implement Heightened Security for Winter Olympics Through February 2026'. Available at: https://www.crisis24.com/articles/italian-authorities-to-implement-heightened-security-for-winter-olympics-through-february-2026 (Accessed: 10 January 2026).
- Cyware (n.d.) 'Inside Fancy Bear's Arsenal: An Update on the Cyber Tactics of APT28'. Available at: https://cyware.com/resources/research-and-analysis/inside-fancy-bears-arsenal-an-update-on-the-cyber-tactics-of-apt28-5186 (Accessed: 14 May 2024).
- Dataminr (2025) 'Securing the Slopes: 2026 Winter Olympics Security'. Available at: https://www.dataminr.com/resources/insight/securing-the-slopes-2026-winter-olympics-security/ (Accessed: 10 January 2026).
- Faulds, Z. (2021) 'These Olympic Champions Get Paid In Cryptocurrency', The Street, 3 June. Available at: https://www.thestreet.com/crypto/investing/olympics-athletes-cryptocurrency (Accessed: 4 June 2021).
- Forrester, N.W. (2018) 'How social media impacts athletes at the Olympics', Macleans. Available at: https://macleans.ca/olympics/how-social-media-impacts-athletes-at-the-olympics/ (Accessed: 28 February 2018).
- Glanzman, A. (2022) 'Reflecting on 20 years of technology transformation at the Olympic Games', Olympics.com, 10 May. Available at: https://olympics.com/ioc/news/reflecting-on-20-years-of-technology-transformation-at-the-olympic-games (Accessed: 12 May 2024).
- Grabmüllerová, A. (2022) 'Social Media and the Olympics: A Chance for Improving Gender Equality', Frontiers in Sports and Active Living. Available at: https://www.frontiersin.org/articles/10.3389/fspor.2022.825440/full (Accessed: 30 April 2022).
- Greek Reporter (2024) 'Paris Olympics Threatened by Cyberattacks'. Available at: https://greekreporter.com/2024/04/18/paris-olympics-brace-cyberattacks/ (Accessed: 20 April 2024).
- Hak, A. (2021) 'How emerging technologies could shape the 2032 Olympics', The Next Web, 6 August. Available at: https://thenextweb.com/news/emerging-technologies-shape-2032-olympics (Accessed: 12 May 2024).
- Inside the Games (2025) 'Cybersecurity takes control at Milano Cortina 2026'. Available at: https://www.insidethegames.biz/articles/1151217/cybersecurity-control-milano-cortina2026 (Accessed: 10 January 2026).
- Jackson, F. (2024) 'Paris Olympics 2024: Cyber Attackers are Targeting Companies Associated With Games, Report Finds', TechRepublic, 4 June. Available at:

https://www.techrepublic.com/article/cyber-attackers-target-paris-olympic-games/ (Accessed: 5 June 2024).

- Le Figaro (2023) 'Olympic 2024: tickets already sold illegally on the internet, 44 fraudulent sites identified', Ground News. Available at: https://ground.news/article/olympic-2024-tickets-already-sold-illegally-on-the-internet-44-fraudulent-sites-identified_c7e1df (Accessed: 12 May 2023).
- Matsakis, L. (2018) 'Hack Brief: Russian Hackers Release Apparent IOC Emails in Wake of Olympics Ban', Wired, 10 January. Available at: https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/ (Accessed: 11 January 2018).
- Nelson, N. (2024) 'Russia Aims Cyber Operations at Summer Olympics', Dark Reading, 3 June. Available at: https://www.darkreading.com/threat-intelligence/russia-cyber-operations-summer-olympics (Accessed: 4 June 2024).
- Olympics.com (2025) 'Milano Cortina 2026 hosts the International Security Briefing'. Available at: https://www.olympics.com/en/milano-cortina-2026/news/milano-cortina-2026-hosts-the-international-security-briefing (Accessed: 10 January 2026).
- Palo Alto Networks Unit 42 (2025) 'Defending the 2026 Milano-Cortina Winter Games'. Available at: https://www.paloaltonetworks.com/resources/research/unit-42-cyber-vigilance-program/2026-winter-games-milano-cortina (Accessed: 10 January 2026).
- Pierce, F. (2020) 'Supply chain not to blame for Olympic shortages', Supply Chain Digital. Available at: https://supplychaindigital.com/logistics/supply-chain-not-blame-olympic-shortages (Accessed: 25 May 2020).
- Rodrigues, F. (2022) 'Crypto at the Olympics: NFT skis, Bitcoin bobsledders and CBDC controversy', Cointelegraph, 15 February. Available at: https://cointelegraph.com/news/crypto-at-the-olympics-nft-skis-bitcoin-bobsledders-and-cbdc-controversy (Accessed: 16 February 2022).
- Sharma, M. (2021) 'Tokyo Olympics becomes the latest victim of the Fujitsu hackers', TechRadar. Available at: https://www.techradar.com/news/tokyo-olympics-becomes-the-latest-victim-of-the-fujitsu-hackers (Accessed: 15 June 2021).
- Starks, T. (2024) 'Fake Tom Cruise warns of violence at Paris Olympics in pro-Russian info op', CyberScoop, 3 June. Available at: https://cyberscoop.com/russia-tom-cruise-ai-paris-olympics/ (Accessed: 9 May 2024).
- Stone, J. (2019) 'Fancy Bear hackers targeted at least 16 athletic organizations ahead of Tokyo Olympics', CyberScoop. Available at: https://cyberscoop.com/fancy-bear-olympics-hacking-tokyo/ (Accessed: 29 October 2019).
- Trend Micro (2021) 'Top 4 Olympic Games Scams – How to Protect Yourself', Trend Micro News. Available at: https://news.trendmicro.com/2021/07/30/top-4-olympic-games-scams-how-to-protect-yourself/ (Accessed: 31 July 2021).
- Vijayan, J. (2026) 'Cyber Threats Loom Over 2026 Winter Olympics', Dark Reading, 16 January. Available at: https://www.darkreading.com/remote-workforce/winter-olympics-podium-cyberattackers (Accessed: 17 January 2026).
- Watts, C. (2024) 'How Russia is trying to disrupt the 2024 Paris Olympic Games', Microsoft On the Issues, 2 June. Available at: https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/ (Accessed: 3 June 2024).

Appendix – Partners & Sponsors

Worldwide Partners

Company	Website	Facebook	LinkedIn	X (Twitter)
AB InBev	https://www.ab-inbev.com/	AB InBev	AB InBev	@abinbev
Airbnb	https://www.airbnb.com.au/e/olympics	Airbnb	Airbnb	@Airbnb
Alibaba	https://olympics.com/ioc/partners/alibaba	Alibaba Group	Alibaba Group	@AlibabaGroup
Allianz	https://www.allianz.com/en.html	Allianz	Allianz	@Allianz
Coca-Cola	https://www.coca-colacompany.com/	Coca-Cola	The Coca-Cola Company	@CocaCola
Deloitte	https://www.deloitte.com/	Deloitte	Deloitte	@Deloitte
Mengniu	https://www.mengniu.com.cn/	Mengniu	Mengniu Dairy	@MengniuDairy
OMEGA	https://www.omegawatches.com/olympic-games	OMEGA	OMEGA	@OMEGA
P&G	https://us.pg.com/	Procter & Gamble	Procter & Gamble	@ProcterGamble
Samsung	https://www.samsung.com/	Samsung	Samsung Electronics	@Samsung
TCL	https://www.tcl.com/	TCL	TCL Electronics	@TCL_USA
Visa	https://www.visa.com/	Visa	Visa	@Visa

Premium Partners

Company	Website	Facebook	LinkedIn	X (Twitter)
ENEL	https://www.enel.com/	Enel	Enel	@Enel
Eni	https://www.eni.com/	Eni	Eni	@eni
Gruppo FS Italiane	https://www.fsitaliane.it/	FS Italiane	Ferrovie dello Stato Italiane	@FSitaliane
Intesa Sanpaolo	https://www.intesasanpaolo.com/	Intesa Sanpaolo	Intesa Sanpaolo	@IntesaSanpaolo
Leonardo	https://www.leonardo.com/	Leonardo	Leonardo	@Leonardo_live
Poste Italiane	https://www.posteitaliane.it/	Poste Italiane	Poste Italiane	@PosteNews
Stellantis	https://www.stellantis.com/	Stellantis	Stellantis	@Stellantis
TIM	https://www.tim.it/	TIM	TIM	@TIM_Official

Official Partners

Company	Website	Facebook	LinkedIn	X (Twitter)
Accor	https://group.accor.com/	Accor	Accor	@Accor
EA7 Emporio Armani	https://www.armani.com/	Emporio Armani	Armani	@EmporioArmani
Fiera Milano	https://www.fieramilano.it/	Fiera Milano	Fiera Milano	@FieraMilano
FNM Group	https://www.fnmgroup.it/	FNM Group	FNM S.p.A.	@FNMGroup
Groupe ADP	https://www.parisaeroport.fr/	Paris Aéroport	Groupe ADP	@GroupeADP
ITA Airways	https://www.ita-airways.com/	ITA Airways	ITA Airways	@ITAAirways
Salesforce	https://www.salesforce.com/	Salesforce	Salesforce	@salesforce
Technogym	https://www.technogym.com/	Technogym	Technogym	@Technogym

Official Sponsors

Company	Website	Facebook	LinkedIn	X (Twitter)
Abatable	https://www.abatable.com/	Abatable	Abatable	@Abatable_co
Bauerfeind	https://www.bauerfeind.com/	Bauerfeind	Bauerfeind	@bauerfeind
Esselunga	https://www.esselunga.it/	Esselunga	Esselunga	@Esselunga
Fincantieri	https://www.fincantieri.com/	Fincantieri	Fincantieri	@Fincantieri
Grana Padano	https://www.granapadano.it/	Grana Padano	Grana Padano	@GranaPadanoDOP
Herbalife	https://www.herbalife.com/	Herbalife	Herbalife	@Herbalife
IDM Alto Adige	https://www.idm-suedtirol.com/	IDM Südtirol	IDM Südtirol-Alto Adige	@IDM_Suedtirol
Intercom	https://www.intercom.com/	Intercom	Intercom	@intercom
Juniper Networks	https://www.juniper.net/	Juniper Networks	Juniper Networks	@JuniperNetworks
Kiko Milano	https://www.kikocosmetics.com/	KIKO Milano	KIKO Milano	@KikoMilano
Leitner	https://www.leitner.com/	LEITNER ropeways	LEITNER ropeways	@LEITNER_ropeways
Pirelli	https://www.pirelli.com/	Pirelli	Pirelli	@Pirelli
Prosecco DOC	https://www.prosecco.wine/	Prosecco DOC	Consorzio Prosecco DOC	@ProseccoDOC
Randstad	https://www.randstad.com/	Randstad	Randstad	@Randstad
Salomon	https://www.salomon.com/	Salomon	Salomon	@salomon
Trentino Marketing	https://www.visittrentino.info/	Visit Trentino	Trentino Marketing	@VisitTrentino
Valtellina	https://www.valtellinataste.it/	Valtellina	Valtellina Taste	@ValtellinaTaste

Official Supporters

Company	Website	Facebook	LinkedIn	X (Twitter)
Airweave	https://www.airweave.com/	Airweave	Airweave Inc	@airweave

Kässbohrer	https://www.pistenbully.com/	PistenBully	PistenBully	@PistenBully
Ottobock	https://www.ottobock.com/	Ottobock	Ottobock	@ottobock_global
Technoalpin	https://www.technoalpin.com/	TechnoAlpin	TechnoAlpin	@TechnoAlpin
Ticketone	https://www.ticketone.it/	TicketOne	TicketOne	@TicketOneIT
Versalis	https://www.versalis.eni.com/	Versalis	Versalis	@VersalisEni

Hospitality Provider

Company	Website	Facebook	LinkedIn	X (Twitter)
OnLocation	https://www.onlocationexp.com/	On Location	On Location	@OnLocation