



# Olympics Madness

Ensuring Online Security During the Olympic Games

# When the world's attention is on the Olympics, adversary are **Phishing for Gold**



In the majestic city of Paris, the stage is set for the 2024 Olympic Games—a spectacular event destined to captivate hearts and minds worldwide. Spectators from across the globe eagerly anticipate the celebrations and the awe-inspiring athletic feats that will unfold.

Yet, amid the excitement, a shadow lurks. The grandeur of the Olympics has caught the eye of a different kind of participants — **scammers and cybercriminals**, ready to exploit the fervor and media attention. These malicious actors target **enthusiastic viewers and attendees, both online and offline, and athletes, partners, and organizing committees**. Their schemes are as varied as they are insidious, aiming to take advantage of the high-profile event for their gain.



According to Mandiant (Google Threat Intelligence service) Russian threat groups pose the **highest risk to the Olympics**. While **China, Iran, and North Korea state-sponsored actors** also pose a moderate to low risk.

# Potential Threats to Watch For



Phishing attacks

Sports betting websites and Apps

Public Wi-Fi risks



Last-minute travel and hotel booking scams

Installing applications via fake websites and apps

Merchandise and memorabilia scams

Ticket scams



**Ready, Set, Go**

Perform like a gold medalist - Adopt Security Habits!





# 1 Be on the lookout for **scams** **and phishing attempts**

In the guise of the Olympics, scammers may craft **deceptive emails, social media posts, or fraudulent websites**, all aimed at tricking you into divulging your personal information and/or stealing money.

# 1

# Be on the lookout for **scams** and **phishing attempts**



## Spotting Tips

**Verify the source:** Review the sender's email address (not their display name) and verify what you expect. If you receive a message claiming to be from an official Olympic source, verify its legitimacy by checking the official website or contacting the organization directly.

Check for **Typo squatting**: Verify a URL's spelling carefully before clicking on any link. In emails, always double-check the sender's name and address. If you're unsure about the spelling of a website, use a search engine to find its correct URL.

If a link appears in the email, **first hover over it to verify that the URL is recognized** and seems legitimate (on mobile phones, pressing and holding down on the link would reveal the website address).

Look for red flags: **Report emails that contain spelling errors, generic greetings, or urgent requests** for personal information.

Stay Cautious: **Cheap tickets or premium seats at low prices** often signal scams. Verify the source to avoid fraud.



# Common impersonated brands to watch

## (logos, logos, logos)

During the event be on the lookout for any publications from the official partners and sponsors of the Olympic games.

check the official website for more information:



**Official Website**





## 2

# Use **official** sources

When seeking information about the upcoming Olympic Games, like event schedules, results, or live streams, **ensure you rely on official sources.**

Use the official [Olympics website](#) for tickets selling



## 2

# Use **official** sources

## Tips for finding official sources

Visit the **official Olympic website**: For accurate and up-to-date information, visit <https://olympics.com/en/paris-2024>

**Use trusted news outlets**: Stick to reputable news organizations for updates and event coverage.

**Download only official apps**: Install apps only from the Apple Store for iPhones and Google Play for Android. When viewing live streaming ensure you're using the official app recommended by event organizers





# 3 Be cautious of public Wi-Fi connections

While public Wi-Fi networks in places like cafes, sports bars, hotels, and Olympic venues offer convenience, they are often insecure. This vulnerability can allow cybercriminals to intercept any data you send or receive over these connections.



# 3 Be cautious of public Wi-Fi connections

## Tips for using public Wi-Fi securely

Avoid accessing sensitive information: **Do not log into your bank account, email, or other** sensitive accounts while on public Wi-Fi.

Prefer using a **cellular data plan or a personal hotspot over public Wi-Fi**. For Wi-Fi networks with names posted on a wall or note, ensure the network is genuinely associated with your location (this is a common attack vector).

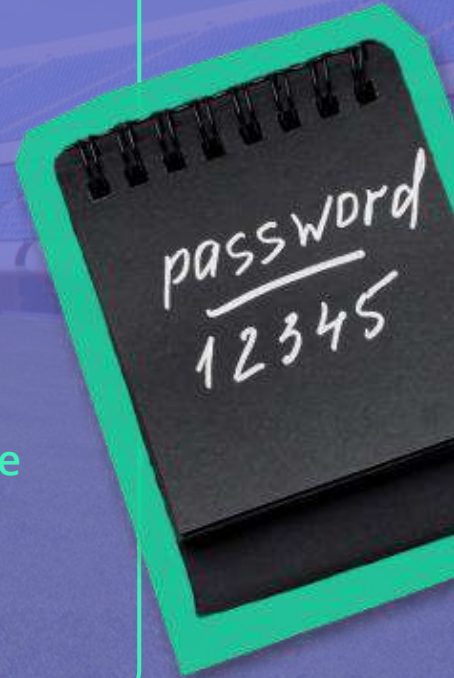
**Turn off file sharing:** Ensure file sharing is turned off and your device is not set to connect to nearby Wi-Fi networks automatically.





# 4 Perform a password audit

- Use **strong and unique passwords** for your online accounts to protect against fraud and unauthorized access to information.
- Don't use a password from one of your **current or past other accounts**.
- **Don't share** the Olympics password with other accounts – current or in the future.
- Prefer using **MFA** when possible.
- When using authentication based on other applications (google, Facebook, etc.), check carefully the **Permissions asked** for in the authentication service.
- When creating new accounts specifically for the Olympic games **don't recycle old passwords**.
- Easily guessable passwords like **"password123"**. **"paris2024"** or **"olympicgames2024"** are **out of the question**.
- **Avoid using your name, date of birth, favorite sports club** or pet's name were probably shared on your social media account. Hackers are watching it closely.





# 4 Perform a password audit

## Tips for creating better passwords

The longer the better. Choose longer passwords (12 characters or more) - long passwords are much harder to crack.

Move to Passphrases: odd and fun phrases like Rainy Green Holes or Talking Dark Bees are easier to remember, yet difficult to guess.

Enable Multi-Factor Authentication. Log into all your important accounts and ensure multi-factor authentication is enabled on each (via account settings).



# Share the message with your **Team members, Family and Friends**



**Stronger Together**

**We are better prepared for the Paris Olympics' cyber threats thanks to our **long-term training program.****

**Many of the cybercriminal manipulations will be familiar to you, but how about **your family and friends?****

**It won't stop if you won't tell – If you see something suspicious **report it to the right security responsible.****

