One of the early schemes targeting interest in the 2016 Olympics occurred approximately one year ago, just as the Olympic ticket market was taking shape. The fraudsters sent out false messages purporting to be from the Brazilian government and the International Olympic Committee (IOC) claiming that recipients had won a ticket lottery. All one had to do was provide the criminal with banking or personal information. This information was then used to steal money from the individual.
computer and demand a ransom be paid to allow the victim to regain access to the files. Malvertising is one of the most common gateways for malicious software to be installed on a device. Malvertising, or malicious advertising, is the use of online, malicious advertisements to spread malware and compromise systems. The advertisement, or email and its attachment will be carefully designed to draw upon your interest in the hope of getting you to open them. You can learn to spot these messages by being mindful, being observant, and being aware of attachments.

The fraudulent messaging around the Olympics will look identical to what you would expect to receive from a sales or promotion around these games. Do not respond to, or click links in unsolicited emails. If you are interested in an offer being advertised, a safer alternative is to use a search engine to find the official vendor’s site and to visit it directly to look for the offer. If the deal is available, then it is likely going to be promoted on the vendor’s website. Fraudsters may also use other attention-getters surrounding the Olympic games, such as “Zika outbreak at the Olympics!”

The Rio Olympics will begin on August 5 and last until August 21, with more than 10,000 athletes competing in 306 events. Careful attention to the sites that you visit for your Olympics purchases or to watch the games online will make them more enjoyable. Go Team USA!

**Recommendations**

- Do not visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open attachments from unknown or untrusted emails.
- Use up-to-date anti-virus.
- Patch all systems and applications.

**Provided By:**

![Multi-State Information Sharing & Analysis Center](image)

The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.