The world’s attention will turn to Rio de Janeiro this summer as Brazil will be the first South American venue to host the Olympic Games. This sporting event is sure to generate a vast amount of popular interest with both fans and media alike and this kind of attention holds potential value for those looking to prey upon the attraction of the games to perpetrate cyber fraud schemes.

MAKE SURE IT’S OFFICIAL
The international interest in the Olympic Games, the variety of sports, and the seventeen-day schedule makes for a lengthy window of opportunity for criminals to take advantage of. Fraudsters have the luxury of time and a variety of interest areas to choose from in trying out their schemes to see what works and then to improve upon the effectiveness. How can you avoid being a victim of these schemes? The simplest way is to be cautious and to understand the fraud schemes that you can expect to encounter.

We know that the criminals have already begun trying to entice victims with the lure of false tickets. This type of activity is likely to continue to be targeted to tourist audiences who are in the market to purchase event tickets. To avoid being scammed, only use the official site of the Olympics Games to find the official ticket vendor, the official vendor for the U.S. is CoSport. Criminals are creating very sophisticated, look-alike sites, which are difficult to discern from official ticketing sites. These false sites even mimic expected customer service responses to delay the reporting of the theft.

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.
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.