July 2016
Volume 11, Issue 7

Going for Gold in Cybersecurity

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

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-a-like 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.

Be aware

We also know that ransomware is currently one of the most popular criminal methods and is sure to be used in conjunction with enticing Olympics-themed email messages. What is ransomware? Ransomware infections may encrypt files on a victim's 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:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™