February 2018
Volume 13, Issue 2

Spotting and Avoiding Olympic Scams

MS-ISAC
Multi-State Information Sharing & Analysis Center

Enterprise Information Security Program

Tacoma

From the Desk of Ron Jimerson, Chief Information Security Officer

In February, the best athletes from around the world will gather in PyeongChang to test their skills against one another at the Winter Olympics. Entire countries will wait with excitement to see the outcomes of individual competitions and count the medals. However, as with any high-profile event, cybercriminals and scammers will also focus on the Games, using your interest in the Olympics to try to trick you into visiting malicious websites, opening malicious spam, downloading malware, and falling for scams. Below we will explore these tactics and techniques, and provide recommendations on how to spot and avoid them, so you can safely enjoy the Games!

Malicious Olympic Websites and Apps

Cybercriminals commonly create convincing but fraudulent websites as a means to distribute malware or gather information about you. This year there will also likely be many suspicious and, possibly, malicious Olympic-themed mobile apps intended to compromise your smartphones and tablets. Whether you're looking to find out the current medal count, who won the bobsled race, see an amazing figure skating routine, or find out what curling is, these malicious websites and apps will be there for you.

You can start protecting yourself by being careful what websites you visit and emails you open. As with any high-profile event, it's always safest to get your news from websites you already know and trust. When you get that email with the link to the video you just have to see or the fascinating story of the amazing win, remember to *Hover to Discover*. This means to hover your mouse over the link and see where the link is really sending you. If you don't recognize the website, don't click on the link. Instead, go to the official Olympics website or another online website that you trust and look for the video or news there.

You can also like/friend/follow the official Olympics accounts on your favorite social media platforms (GooglePlus, YouTube, Twitter, and Facebook) and get the news directly from the source, instead of waiting for potentially suspicious links to appear later. As the Games get

closer, many social media apps will also likely role out news feeds and other special features, related to the Games. Keep an eye out for those so you can safely stay in the know!

Of course, there's also an official Olympic app for your smart device! The Olympics website says the app will contain real-time updates and news, as well as images, videos, and the medal count. The app is available in the Google Play Store and iOS App Store. Since there are a-lot of other Olympic apps, some of which are malicious, make sure you're careful to download the right one! You can check the app against the app images on the Olympics.org website.

Olympic Games Related Scams

When it comes to high-profile events like the Olympics, cybercriminals always seek to trick you with scams, too. Many of these scams may involve websites that sound and look legitimate. This is because criminals often register these domains with names similar to the event, so that the website name adds credibility to their scams. Two very common Olympic scams are:

Trip and Lottery/Sweepstakes Scams

With this year's Winter Olympics occurring in PyeongChang, South Korea, it is a bit pricey to head over to view the Games in person. Scammers commonly send phishing emails during and leading up to Olympic Games identifying the recipient of the email as the winner of a sweepstakes or lottery for tickets to the Games and travel arrangements. You just have to pay a "fee" or "tax" first and provide a few details… maybe including your Social Security Number or credit card number. Whether they seek your payment information to take your money or your personally identifiable information for identity theft, these notices are always false and should be avoided, as you cannot win a lottery that you have not entered!

Olympic Merchandise Offers

As with lots of other events, there will be Olympic merchandise for sale so you can display your pride and support your favorite athletes. This is great, just be careful where you buy from as you may receive emails or see online advertisements enticing you to purchase fraudulent or counterfeit items from less than reputable vendors. At best, by clicking on these advertisements and offers you will open yourself to the risk of purchasing counterfeit merchandise and at the worst, you open yourself to the risk of having your payment information or identity stolen. Display your team pride by ignoring these suspicious offers and purchasing your merchandise through a known, trusted, and authorized retailer.

It's also a good idea to make all online purchases through an alternative or more secure payment system, such as Visa Checkout, Mastercard Securecode, or PayPal. Otherwise consider using one credit card (not a debit card!) for all online purchases. As always, remember to look for the "HTTP**S**" in the URL and the little lock icon in the browser bar to ensure your communication with the trusted vendor is safe. If you don't see these, don't submit sensitive information to that website. Lastly, remember to always make your purchases on a trusted, secure network, never through public, unsecured Wi-Fi.

We hope you safely enjoy the 2018 PyeongChang Winter Olympics.

Go Team USA!

The information provided in the MS-ISAC 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.