PENNSYLVANIA STATE POLICE
COMMUNITY AWARENESS BULLETIN
CAB 003-2018 February 9, 2018

2018 OLYMPICS SCAMS: BE ALERT

On February 8, 2018, the Winter Olympics in PyeongChang, South Korea, began and the world's attention is on this magnificent sporting event. As the games get underway, criminals will likely capitalize on the high-profile occasion by utilizing various techniques to steal cash and personal information from victims. Criminals may use the stolen personal information to create fraudulent accounts to conduct further illegal activity. Listed below are some of the Olympics-related scams:

PyeongChang 2018™

Car Decoration

An email is sent that appears to come from the United States Olympic Committee. The sender of the email offers to pay the victim $350 a week to display Olympic material on their vehicle. Victims who respond to the email are sent a check for an amount greater than $350. The victims are instructed to deposit the check into their bank account and wire transfer any amount over $350 back to the company. Sadly, the checks sent by the scammer are counterfeit and the money that is wired back to the sender is deducted from the victim's bank account.

Gold-Medal Malware

Many people will also receive emails and text messages appearing to contain updates, photos, and videos of Olympic events. Unfortunately, when a victim clicks on a link or downloads an attachment sent by a scammer, the victim may inadvertently download ransomware or malware used to steal information from their computer or smart device. This information can then be used to steal the victim's identity for other fraudulent activity.

2018 Olympic Online Lottery Promotion

Scammers may send emails advising recipients they won cash and a trip to South Korea through the Olympic lottery. The emails appear to be legitimate and may purport to come from a known Olympic sponsor such as McDonalds or Coca-Cola. The email will instruct the victim to pay income taxes or some type of administrative fee to claim the prize. The scammer keeps the payment and no prize money is awarded to the victim.

Malware Apps

There are legitimate applications (apps) available including the official PyeongChang 2018 app, which is available at the Google Play Store and the iOS App Store. People may utilize these apps to obtain valuable information regarding the games. Unfortunately, many other Olympic-related apps appear genuine but are loaded with malware, including keystroke logging malware and ransomware.

Social Media

Scammers are also turning to social media, such as Facebook, to send out links to photos and videos of important Olympic moments. The links may appear valid, but when they are clicked, malware is downloaded.

Counterfeit Olympic Merchandise

Olympics-related merchandise, particularly apparel, is extremely popular. Unfortunately, many websites are selling counterfeit Olympics apparel and merchandise. Authentic Team USA merchandise is offered on the Team USA website and can purchased through secure payment methods.

To Avoid Becoming the Victim of a Scam:

- Do not cash a check that is for more than an amount you are owed and comes with a request to send back the overpayment.
- Never click on a link or download an attachment unless you are positive it is legitimate. Even if the address of the sender appears correct, the address may have been "spoofed" to appear genuine.
- Recognize lottery taxes are either deducted before the prize is awarded or the entire prize is awarded to the winner, who is then personally responsible to pay the taxes which are due.
- Be cognizant that lottery winners are not typically charged administrative fees.
- Only download apps from authorized stores.
- When shopping online, use a credit card rather than a debit card because credit cards give you much greater consumer protection if your information is stolen.

If You Have Been the Victim of a Scam:

- Contact your local law enforcement agency.
- File a complaint with the Internet Crime Complaint Center (IC3) at http://www.ic3.gov.
- File a complaint with the Federal Trade Commission at www.ftccomplaintassistant.gov or 1-877-FTC-HELP. If possible, be prepared to provide:
    - Your contact information: name, address, phone number, email address
    - The type of product or service involved
    - Information about the caller: business name, address, phone number, website, email address, representative's name
    - Details about the transaction: amount paid, how paid, date of transaction

Sources:

Weisman, S. (2018, January 16). Scam of the day – January 17, 2018 – Winter Olympic scams. *WordPress.* Retrieved 02/06/2018 from https://scamicideblog.wordpress.com/2018/01/16/scam-of-the-day-january-17-2018-winter-olympic-scams/.
Dunklebarger, P. (2018, February 1). Watch out for these three scams during the 2018 Winter Olympics. *Delta News Web.* Retrieved 02/06/2018 from http://www.deltanewsweb.com/2018/02/01/watch-out-for-these-three-scams-during-the-2018-winter-olympics/.
Weisman, S. (2018, January 31). Con Watch: 6 Winter Olympics scams. *Saturday Evening Post.* Retrieved 02/06/2018 from http://www.saturdayeveningpost.com/2018/01/31/health-and-family/con-watch-6-winter-olympics-scams.html.