WV Executive Branch Privacy Tip

This week's tip is brought to you by the Identity Theft Resource Center (https://www.idtheftcenter.org/).
Reprinted with permission.

Fireworks and Phishing: How to Avoid 4th of July Scams

With all of the fun and frolic surrounding the Fourth of July, it's easy to forget there can be a downside. Holidays are an especially active time for scammers, and "patriotic" scam attempts can strike in a variety of ways. Scammers can target consumers through different methods of attack, like phishing emails or spam texts, and they often include a variety of premises to lure people. Here's some Fourth of July scams people should be aware of:

1. Patriotic emails and social media posts
Phishing messages and fraudulent social media posts can tug at people's heartstrings on any holiday, and Independence Day is no exception. In this case, the Fourth of July scam may be an active duty or veteran's scam, political or election scam or any other country-specific theme. It's important to remember that charities and organizations do great work all year long. People should avoid these Fourth of July scams and the temptation to impulse-click on an untrustworthy source.

2. Shopping scams
There are retail deals advertised during the Fourth of July holiday, which can also mean bogus web coupons and sales links to click. People should protect themselves from online shopping scams by only doing business with trusted sources, using a secure payment method for purchases and steering clear of "time is running out!" impulse shopping scams.

3. Fireworks scams
People who live in a state that allows citizens to shoot their own fireworks should beware of roadside stands and temporary shops. While they make sense when selling a product that is only popular a few times a year, it means consumers are handing their payment information to someone who may be skipping town in a day or two. If feasible, consumers should use cash instead of giving out payment information. It could lead to a Fourth of July scam.

4. Virus attacks and tech support scams
In years past, there have been reports of malicious software attacks on or around the Fourth of July, playing off of the theme of rebellion, overthrowing tyranny and more. People should be mindful of both genuine cyberattacks and fake ones that pretend to lock up people's computers or inform them that they have already been infected. People should also be aware of phony tech support scams trying to get money and access people's computers in exchange for "cleaning" out a cyberthreat.

Consumers should remember that there are a variety of threats that can have a stronger impact on the holiday, both physically and from a data security standpoint. People should be mindful of Fourth of July scams and fraud, and be safe in whatever summer activities they choose to enjoy.

Note: Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.