












## *Suspect/Counterfeit Items (S/CI) & Security During the Holidays*



The start of the holiday season means shoppers across the country may be participating in the biggest shopping days of the year. Whether shoppers are looking for the newest electronics, computers, tablets, or computing equipment for work, they'll be searching for the best deals. While it's tough to turn away from low prices, shoppers need to remain vigilant. Included in the list of the most counterfeited items seized by U.S. Customs and Border Patrol are consumer electronics and electrical products such as those that may be purchased commonly for gifts or for computing such as working from home. Not only could counterfeit consumer electronics and electrical products pose a significant electrical hazard as they can lead to fire, shock, or explosion which may result in deaths, injuries, and substantial property loss, they also pose significant security risks to organizations. Below are some tips to help keep you and your family safe and secure this holiday season!

### **Shopping Tips to Keep You Safe Online and Prevent Buying S/CIs<sup>1</sup>**

-  Purchase from the online stores you already know, trust, and have done business with previously.
-  Be suspicious of prices that are significantly better than those you see at the established online stores. If the deal sounds too good to be true, it may be S/CI.
-  Type the name of the online store or its web address into a search engine to see what others have said about it. Look for terms like "fraud," "scam," "never again," and "fake."
-  Look for changes in a company's domain name. For instance, you know the web address is energy.gov but now it is energygov.com.
-  Avoid websites that lack contact information, have broken contact forms, or those that use personal email addresses.
-  Use a unique password for each of your online accounts. Can't remember all your passwords? Consider storing them in a secure location or in a password manager.
-  Be wary when purchasing new products on social media<sup>2</sup> marketplaces as many items may be stolen or counterfeit.
-  Look for the "connection is secure" lock on websites when purchasing online to verify that transactions are secure.
-  To avoid phishing or other malicious attacks, don't click on links but rather type key information into a search engine.

<sup>1</sup> Tips Reference SANS Newsletter OUCH! [Shopping Online Securely](#), Mark Orlando, 11/01/2021

<sup>2</sup> <https://www.controlrisks.com/our-thinking/insights/social-media-influencers-the-newest-players-in-counterfeit-risk>

### **S/CI and Security Scenario**

You decide to procure a brand-new keyboard and mouse for working at home. You have struggled with finding items that are ergonomically correct and meet your needs. The items will be connected to your Department of Energy (DOE) laptop or computer. These items seem innocuous enough and you decide to use a P-Card to procure the items online. During the buying process, you notice that the supplier may be located outside the U.S. but seems to be using a warehouse in the U.S. to sell items; therefore, the items will technically ship from inside the U.S. The items are priced much lower than the manufacturer's suggested retail price (MSRP) as listed on the manufacturer's website, but you decide to buy the items from this supplier since the items are more affordable.

Upon receipt of the items, you notice that the keyboard and mouse packaging is not what you expected. It is not in the manufacturer's packaging, the items are much lower quality than they appeared in the online photos, and the packaging stated that they were "only intended to be sold in Asia".

Would you use these items? Are there any potential indications of S/CI?

See the answer at bottom of page.

### **S/CI Resources for DOE Employees & Contractors**

- ✿ Suspect/Counterfeit Items [webpage](#) (energy.gov)
- ✿ Suspect/Counterfeit Powerpedia [website](#)
- ✿ Contact the S/CI Subject Matter Expert by emailing [gabrielle.holcomb@hq.doe.gov](mailto:gabrielle.holcomb@hq.doe.gov)



#### **Answer:**

You should not use the items or connect them to your DOE computing device. There are multiple indications of potential S/CI that were encountered during the buying process and during receipt of the items. For instance, the supplier is actually located outside the U.S. but primarily uses private or contract warehousing in the U.S. This could be an indication that the supplier is a counterfeiter. Using various warehousing methods in the U.S. is a common tactic used to elude customs, while building stock to sell to consumers. Other key indicators of potential S/CI are the price being below MSRP, the items not being in the manufacturer's packaging, the general appearance and quality of the items, and the items stating that they were *only intended to be sold in Asia*.

Figure 1: Photo courtesy of *Supposed NIB "OEM" keyboard from Lenovo - how to identify a counterfeit/replica*. Posted on [Thinkpads.com Support Community](#) 01/23/2021