AMAZON PRIME DAY SPURS SPIKE IN PHISHING, FRAUD ATTACKS

A spike in phishing and malicious websites aimed at defrauding Amazon.com customers aim to make Prime Day a field day for hackers.

October 8, 2020 • ThreatPost • Elizabeth Montalbano

Cybercriminals are tapping into Amazon's annual discount shopping campaign for subscribers, Prime Day, with researchers warning of a recent spike in phishing and malicious websites that are fraudulently using the Amazon brand.

There has been a spike in the number of new monthly phishing and fraudulent sites created using the Amazon brand since August, the most significant since the COVID-19 pandemic forced people indoors in March, according to a Thursday report from Bolster Research.

"As shoppers gear up for two days of great deals, cyber criminals are preparing to prey on the unwary, taking advantage of those who let their guard down to snap up bargains," researchers wrote.

Prime Day actually happens over two days—this year the event falls on Oct. 13 to 14. Amazon Prime customers enjoy special sales and discounts on top brands to mark the biggest shopping event of the year on the online retail giant's site.

Amazon last year yielded over $7 billion in sales during the 36-hour event, which could go even bigger this year due to "the decline of brick and mortar retail and the close proximity to the holidays," researchers noted. Indeed, mandatory stay-at-home orders globally that began with the COVID-19 pandemic in March have significantly boosted Amazon's business, a trend that shows no signs of abating.

Researchers analyzed hundreds of millions of web pages to track the number of new phishing and fraudulent sites using the Amazon brand and logos. Its research shows threat actors taking advantage of both Amazon features and consumer behaviors to try to lure online shoppers to fraudulent sites that can steal their credentials, financial information and other sensitive data.

One new campaign targets "returns" or "order cancellations" related to Prime Day using a fraudulent site, www.amazoncustomersupport[.]net, that mimics a legitimate Amazon site. However, closer examination of the site shows it is clearly designed to defraud consumers, researchers noted.

One clear evidence is its use of a phone number, as "Amazon does not encourage customer service by phone, and takes a great effort to find phone support on the real Amazon site," researchers wrote.

The form on the site also requests

bank or credit card information from customers–a clear intent to steal this information, since Amazon always offers refunds to original form of payment or gift cards. Further, the site also does not ask for a customer password, something Amazon always requires for purchases and returns.

Other smaller issues that might be overlooked—such as broken links attached to the Amazon Prime Logo and a “Get Started” button–also appear on the site. These also are clues to fraudulent behavior that shoppers should look out for in general as they shop on Prime Day, researchers noted.

Another malicious site recently observed by researchers takes advantage of most consumers’ inherent love of a free gift. The site, www.fr-suivre[.]vip, promotes an Amazon loyalty program and offers a free iPhone 11 Pro if people answer a few survey questions. After answering these questions, people are directed to a simple game that they win, after which they’re asked to enter credit card info so the site can charge them $1 to receive the iPhone.

The site even includes a screenshot in which “the free iPhone is validated by many others who have already received their phones,” researchers wrote. “Despite the glowing reviews, the $999 phone will never arrive, and the shopper begins to see strange charges on the credit card number provided,” they warned.

Fortunately for Amazon Prime customers who plan to take advantage of the event this year—or anyone else shopping Amazon these days—avoiding online fraud is not that difficult, researchers said. All shoppers should start directly at the source—Amazon.com—and pay close attention to their experience to ensure that nothing is out of the ordinary.

“Shoppers need to be aware of cyber criminals prepared to take advantage of the situation,” researchers noted. “With some diligence and attention to detail, shoppers will be able to get those deals without getting scammed.”

Amazon, too, can take even more security steps to protect customers as its business continues to boom, with cybercrime inevitably following suit, observed Kevin Beasley, CIO at enterprise management software provider VAI.

“To minimize the risk of data breaches or security issues, retailers, like Amazon, must install additional multi-factor authentication for logins and policies to protect passwords and who has access to data,” he said in an email to Threatpost.

Online retailers across the board also should get out ahead of the busy holiday season by making their platform “a security-first environment,” Beasley said.

This can be done “by installing additional layers of security infrastructure between the operating system and hardware platform, and continuous security testing and automating scans of hardware and software systems to seek out vulnerabilities and patch potential issues as they arise,” he told Threatpost.