Cyber Monday: it's the most wonderful time of year for cyber-attackers

Holiday shopping triggers spike in cybercrime, experts say, so ignore dodgy-looking emails and social media posts and verify orders on retailers' websites

Jared Lindzon

Sat 28 Nov 2015 07.09 EST

This weekend kicks off the busiest shopping season in many parts of the world – and, starting Cyber Monday, the most popular season for cyber-attacks.

Malicious attacks on shoppers increased 40% on Cyber Monday in 2013 and 2014, according to EnigmaSoftware.com, an anti-malware and spyware company, compared to the average number of attacks on days during the month prior. Other cybersecurity software providers have identified the December holiday shopping season as the most dangerous time of year to make online purchases.

"The attackers know that there are more people online, so there will be more attacks," said Christopher Budd, Trend Micro's global threat communications manager. "Cyber Monday is not a one-day thing, it's the beginning of a sustained focus on attacks that go after people in the holiday shopping season."

Budd adds that cyber-attacks often target the hottest items of that holiday shopping season.

“If you’re reading about it in the mainstream press as far as what’s really hot this year, the hackers are too,” he said. “Whatever the latest hot gadget is, that’s almost always going to be used as a spam or phishing or social media scam lure, and that’s something that has longevity through the shopping season.”

Apple products as well as PlayStation and Xbox-related items have been key targets in years past. Attackers will often advertise deals that may seem too good to be true, either through spam emails, hacked social media posts or fake websites, said Budd.

“Instead of going to Amazon.com, someone might go to Google and search ‘great deals on an Xbox One’,” said Ryan Gerding, a spokesperson for EnigmaSoftware.com. “There are bad guys who are particularly sophisticated and can make it so that pretty high up in the Google search results there might be a page that promises a ridiculously low price for an Xbox, and someone might click on that and in turn get an infection when they do.”

Gerding added that while the risk of attack is ongoing, Cyber Monday marks the beginning of an annual shift in focus for cyber-attackers.

“The bulk of infections during the rest of the year that our customers get, quite honestly, comes because of them visiting adult websites and clicking on areas they probably shouldn’t,” he said. “This time of year it seems as though a greater percentage are just folks that are trying to do some shopping.”

One of the primary modes of attack, according to cybersecurity experts, are social media hacks that send links through direct messages, tweets and wall posts, advertising online discounts. These attacks are particularly successful because users tend to trust recommendations that are posted or sent directly from friends and trusted sources, without considering that their accounts may have been hacked.

“You can send out hundreds of thousands of emails, or you can get one person on social media [to click on a malicious link], and they end up infecting all of their friends,” said Kevin Haley, a security expert for Norton. “It goes on all their friends’ walls, and a small percentage of those people will click on it, and it cascades through very quickly.”

Another common attack during the holiday season takes advantage of the fact that more people are expecting deliveries this time of year, including gifts they may not have purchased themselves.

“You send out a set of spam emails that says ‘We had a package that we couldn’t deliver. If you want to find out the details, click on this attachment,’ pretending to be UPS or FedEx,” said Haley. “It works because people really want to know about a package they weren’t expecting. Think about how effective that is during the holiday season, when people are getting lots of packages delivered to their door.”

Attackers also use the increase in package deliveries following Cyber Monday to send false emails that appear to be sent from Amazon, Best Buy and other online retailers.

“If you get an email telling you that there’s a problem with one of your online orders, instead of clicking the link in the email, just launch your web browser and type in the address for that retailer, log in and check your shopping cart,” said Gerding. “There are times when there very well could be a reason for you to get an email telling you there’s a problem with your order, but you can confirm that if you visit the website directly as opposed to clicking on a link [in an email].”

Here are 10 more ways to protect yourself online during the holiday season, according to cybersecurity experts:

1 Enable two-step email verification

2 Be wary of suspicious social media posts

3 Don’t click on links in emails and on social media without confirming that they were sent intentionally, no matter the sender

4 Only make online purchases from websites with SSL certificates (usually indicated by a small icon of a lock in the lower right-hand side of the window)

5 Do not download mobile apps outside the Apple App Store, Amazon App Store and Google Play Store

6 Do not use the same password for more than one website, especially banking and email sites

7 Use anti-spyware and anti-malware software

8 Confirm order history and shipping information via the online retailer’s website directly, not through email links

9 Be wary of any online shopping deals that seem too good to be true

10 Keep your applications and operating systems up to date

Topics

Cyber Monday

Cybercrime / Internet / Email / Computing / news

View all comments >

Most viewed