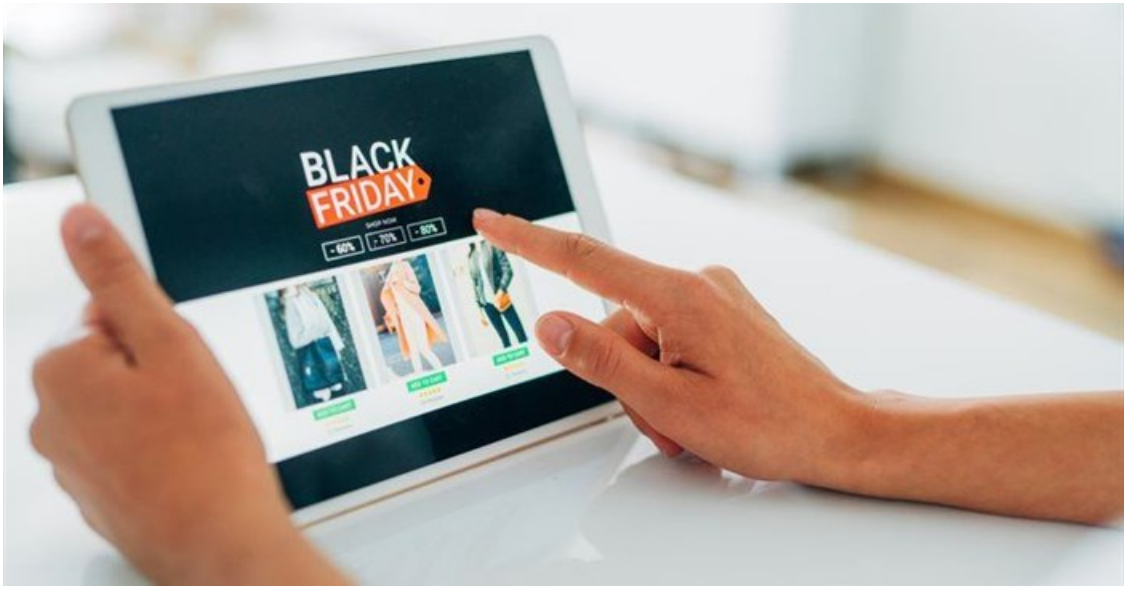
BIZCOMMUNITY

The rise of fake e-commerce sites around Black Friday - and how to spot them

In the lead-up to the blockbuster shopping event that is the Black Friday weekend, FortiGuard Labs has observed an increasing number of scams involving counterfeit websites that "appear" as legitimate e-commerce sites.



Source: Getty

Black Friday and Cyber Monday kick off the holiday shopping season. And since the advent of Cyber Monday, brick and mortar and e-commerce stores alike stand to generate a significant portion of their annual revenue over this shopping "holiday" weekend, often allowing retailers to catch up on revenue and meet goals and sales numbers for the year.

However, FortiGuard Labs notes a proliferation of fake e-commerce sites around this time. To the untrained eye these sites may look safe, but if shoppers aren't paying attention, they can steal payments (and possibly payment information) via a purchase customers thought was legitimate. Fake e-commerce sites are quickly becoming the latest threat to consumers and they cover a wide range of products to lure potential buyers.

FortiGuard Labs recently came across a live, active scam that leverages the look and feel of the world's largest companies and their respective trademarks to compel and lure victims into making purchases from their site. These sites are in no way affiliated with the trademark/IP owner, and are recognisable in part because they use the same template over and over in a digital game of whack-a-mole (meaning that as soon as one site gets shut down another one immediately pops up somewhere else), the company explains.

A challenging, but promising, Black Friday awaits in 2021

2 Nov 2021

Several of the high-profile brands documented include:

• Blink (Amazon)
• Oculus (Facebook)
• Shimano

Other well-known brand names infringed include:

• Coleman (camping gear)
• Ninja (home appliances)
• Nu Wave (home appliances)
• Ryobi (power tools)
• Makita (power tools)

FortiGuard Labs also observed others that have since been taken down:

• Keurig
• Nespresso
• Common Framework

How to recognise counterfeit sites

The websites that were observed have the following characteristics in common:

• The domain names have only been registered for a few days to a few months
• All sites are registered with the same registrar
• They use. TOP and. SHOP top-level domains (.com is also common)
• They use stolen imagery
• They contain numerous grammatical errors and inconsistencies in statements
• Social media buttons do not resolve anywhere or go to accounts that either do not exist or have been deleted
• Their webhosting providers utilise content delivery networks (CDN) to remain anonymous (via an IP address that cannot be traced)